3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 004.056; 004.052.4; 004.057.4

ПРЕВЕНТИВНІ ТА РЕАКТИВНІ МЕХАНІЗМИ БЕЗПЕКИ В БЕЗДРОТОВИХ ТРАДИЦІЙНИХ ТА AD-HOC МЕРЕЖАХ

Сергій Гладиш
Одеська національна академія зв'язку ім. О. С. Попова (Україна), за підтримки Visegrad Fund (фонд урядів Угорщини, Словаччини, Чехії, Польщі)

Анотація: **Традиційні та нові (Ad-Hoc, Mesh, сенсорні) архітектури бездротових мереж ідентифіковано зі складностями в захисті інформації; класифіковано механізми безпеки як превентивні та реактивні; вказано особливі характеристики та вразливості мереж, зокрема атаки на багатокрокову (multi-hop) маршрутизацію; наведено висновки та пропозиції.**
Summary: **Traditional and new (Ad-Hoc, Mesh, sensor) architectures of wireless networks were identified to security complexities; security mechanisms were classified as preventive and reactive; special features and vulnerabilities were shown, including multi-hop routing security; summary and proposals were given.**
Ключові слова: **Ad-Hoc мережа, архітектура безпеки, бездротова мережа, виявлення вторгнень, інформаційна безпека, механізми безпеки, multi-hop маршрутизація, реагування на інцидент.**

I Постановка задачі

Бездротові мережі (БМ) є технологією передавання/прийому інформації (голосу, даних, мультимедіа) за допомогою радіозв'язку (модульованих електромагнітних хвиль, що поширюються у відкритому просторі). Багато сучасних БМ (умовно назвемо їх «традиційними») зараз широко використовуються, наприклад: мобільний стільниковий зв'язок (GSM/GPRS/EDGE, CDMA); мережі Wi-Fi (IEEE 802.11), Wi-Max (IEEE 802.16) тощо. Але також розроблено і розвивається інший за принципом організації зв'язку клас технологій (в західній термінології: Ad-Hoc мережі) з динамічною самоорганізацією та багатокроковою (англ.: multi-hop) маршрутизацією, який призначено для децентралізованих, динамічних, розподілених застосувань. Специфіка таких новітніх інфокомунікаційних застосувань та майбутніх сценаріїв [1–3], потенційні технічні обмеження з боку кінцевих пристроїв – все це висуває загальну проблему теоретико-концептуального плану щодо архітектури механізмів, принципів та організації безпечного інформаційного обміну в БМ; та накладає нові інженерно-технічні вимоги, в першу чергу до інформаційної безпеки (ІБ).

Складність завдань ІБ в БМ, й особливо в Ad-Hoc мережах, (неможливість вирішити всі проблеми лише превентивними (запобігаючими) технологіями безпеки, необхідність виявлення та реагування на інциденти) [4, 5] – це вирішуючі фактори, які стримують поки що подальший розвиток нових архітектур БМ та обмежують можливості їхнього широкого використання для передачі інформації з обмеженим доступом (ІзОД) в оперативних динамічних сценаріях. Отже, забезпечення ІБ в Ad-Hoc мережах є актуальним завданням, від вирішення якого в значній мірі залежить темп та масштаб їхнього впровадження.

Більшість отриманих на сьогодні результатів [6, 7] щодо ІБ в БМ стосуються перш за все превентивних технологій безпеки в БМ через використання механізмів автентифікації та контролю доступу, симетричних та асиметричних криптографічних схем для забезпечення конфіденційності та цілісності, VPN, інфраструктури ключів та сертифікатів, міжмережних екранів, тощо.

Однак, превентивні технології безпеки не завжди можуть перекрити всі вразливості БМ і не захищають від всіх можливих загроз [8]. Необхідно створювати другий рубіж захисту – реактивний: направлений на виявлення та реагування на ті інциденти, які виникатимуть в БМ. Але на сьогодні реактивні технології безпеки в БМ є найменш дослідженими в проблемній підгалузі безпеки БМ. Що стосується пострадянського простору досліджень, – в більшості публікацій стосовно безпеки БМ мова йшла лише про безпеку «традиційних» БМ [9]. В Україні ж взагалі недостатньо уваги приділяється такому перспективному напрямку телекомунікацій, як тенології Ad-Hoc мереж. Декілька публікацій зробелно автором [1, 4, 5, 8].

Мета даної статті – розробка архітектури ІБ, що включає превентивні та реактивні механізми, з урахуванням вимог та обмежень динамічних розподілених застосувань (сценаріїв) та нових класів БМ.

Задачами дослідження є: аналіз традиціних та нових бездротових архітектур; виявлення їхніх особливих характеристик з точки зору ІБ; класифікація превентивних та реактивних механізмів безпеки; виділення

вразливостей та співвідношення до них певних механізмів безпеки, зокрема розробка реактивних механізмів безпеки для багатокрокової маршрутизації в бездротових Ad-Hoc мережах.

ІІ Перспективні застосування, нові архітектури БМ та вимоги щодо ІБ

Розвиток традиційних БМ відзначають тенденції [1] в напрямку зростання абонентської бази, розширення зон покриття, розширення спектру частот, підвищення ефективності використання спектру, пропускної спроможності та швидкостей, а також еволюція до мереж наступного покоління 3G та 4G:

- впровадження нових видів інтелектуальних, інфокомунікаційних та телематичних послуг, що зумовлює мультисервісність мережі;
- одночасне використання декількох цифрових пакетних технологій передачі на базі різних аппаратних платформ, що зумовлює гетерогенність мережі;
- впровадження програмно-керованих систем керування мережею та окремими її елементами на базі комп'ютерних платформ, систем комутації – Softswitch;
- інтеграційні рішення з мережею Інтернет, які на транспортному та мережному рівнях спираються на стек протоколів TCP/IP, що зумовлює конвергентність мережі.

Крім того логічно перебачити, що в найближчому майбутньому використання та застосування БМ, в особливості Mesh мереж, сенсорних та інших Ad-Hoc мереж (БМДС – бездротових мереж з динамічною самоорганізацією й багатокроковою multi-hop маршрутизацією), дедалі збільшуватиметься, отримуючи нових форм, таких як «всепроникаючі обчислення» (ubiquitous computing), сенсорні та наносенсорні мережі отримання та розподіленого зберігання інформації, інтегруючі мережі телеметрії, радіочастстної ідентифікації (RFID), телебіометрії, мережі роботів та нанороботів, мережі віртуальної реальності тощо.

Характерними особливостями та вимогами багатьох майбутніх застосувань БМ буде: повна (або часткова) децентралізаціїя, самоорганізація, розподіленість, паралельність, динамічність в режимі реального часу, мобільність та технічні обмеження з боку кінцевих пристроїв. Такі напрямки розвитку БМ спрямовані на поступову адаптацію наявних технічно-обмежених телекомунікаційних можливостей до майбутніх постійно зростаючих інформаційних та телематичних потреб людства. Обов'язково при цьому має бути забезпечено як гарантований рівень якості обслуговування (QoS), так і певний припустимий ріень безпеки БМ.

Для того, щоб відповідати аналогічним вимогам військових застосувань та сценаріїв (децентралізація, самоорганізація, розподіленість, динамічність, мобільність) в 1970-х роках в США були розроблені перші прототипи Ad-Hoc мереж [10]. І хоча вони значально розроблялися лише для задовольняння таких потреб НАТО, як стеження за підводними човнами СРСР та Китаю, організація оперативного зв'язку в бойових умовах, зараз їхні переваги роблять їх дуже привабливими і для сучасних невійськових застосувань, таких як:

- зв'язок у надзвичайних ситуаціях (рятівні, антитерористичні операції);
- швидка організація оперативного тимчасового зв'язку між різними типами пристроїв (конференції, виїзні роботи, аварійно-ремонтні бригади);
- дешевий доступ до Інтернет (там, де невигідно будувати інфраструктуру);
- місцеві, муніципальні, відомчі, університетські мережі (community networks);
- мережі зв'язку між транспортом, що рухається (vehicular networks);
- збір та моніторинг даних сенсорних мереж: телеметрія, телебіометрія, RFID.

Ad-Hoc (лат. – для спеціального призначення) – це технологогія організації бездротового зв'язку за принципом динамічної самоорганізації.

Як свідчать публікації [1, 6, 7], вже сьогодні можна казати про цивільне впровадження Ad-Hoc мереж: Wireless Mesh Networks (WMN), Mobile Ad-Hoc Networks (MANET), Vehicular Ad-Hoc Networks (VANET), Wireless Sensor Networks (WSN). Перспективність Ad-Hoc мереж підтверджується як вже існуючими, так і потенційними застосуваннями, а також особливою увагою з боку науковців. За останні роки було реалізовано ряд промислових проектів з практичного втілення різних типів Ad-Hoc мереж, опубліковано значну кількість досліджень. Розпочато розробки з використання Ad-Hoc мереж для самоорганізації зв'язку між нанопристроями (наносенсорами, нанороботами) [3].

Для нових застосувань та сценаріїв перевагами Ad-Hoc архітектури БМ є:

- можливість оперативного швидкого розгортання;
- мінімальні вимоги, дешевість пристроїв, відсутність вимог до попередньо існуючої інфраструктури і завдяки цьому низька загальна вартість;
- можливість більшого покриття, масштабованості, живучості.

III Характеристики та класифікація архітектур БМ з точки зору ІБ

БМ дозволяють розширювати можливості, спектр послуг та зону осяжності традиційних дротових телекомунікаційних мереж (ТМ) завдяки використанню модульованих електромагнітних хвиль як носіїв сигналу та радіоефіру як середовища передачі (або оптичних частот в інфрачервоному диапазоні спектру). Але сам принцип передачі інформації в БМ зумовлює складність забезпечення ІБ в них:

- незахищений характер та відкритість бездротового середовища передачі;
- вразливості, пов'язані з мобільністю пристроїв користувачів, мобільністю сервісів та застосувань;
- розподіленістю, змінами у топології (особливо для децентралізованих Ad-Hoc мереж, див. п. 5 далі);
- недоліками або помилками під час проектування протоколів (наприклад WEP);
- принциповою неможливістю реалізації деяких механізмів безпеки через структурні особливості БМ;
- наявністю специфічних технічних обмежень.

На сьогодні розроблено значну кількість бездротових технологій. Залежно від обраного критерія можна запропонувати той чи інший спосіб їхньої класифікації.

В даній роботі виділимо класифікацію на традиційні БМ та Ad-Hoc (БМДС - з динамічною самоорганізацією та багатокроковою маршрутизацією):

- традиційні БМ, в яких радіоефір використовується лише для організації надання доступу мобільним (рухомим) чи стаціонарним абонентам до інформаційно-телекомунікаційних послуг (передача голосу, даних, Інтернет) та ресурсів фіксованих (дротових) магістральних ТМ;
- Ad-Hoc (БМДС), в яких радіоефір використовується як для абонентського доступу, так і для динамічного утворення (самоутворення самими абонентськими пристроями або виділеними вузлами мережі) розділюваної та розподіленої бездротової магістралі (wireless backbone).

Таблиця 1 – БМ залежно від типу та способу організації абонетської та магістральної частин (класифікація автора)

Тип мереж	«Традиційні» БМ	Бездротові Ad-Hoc мережі			
		Mesh	MANET	VANET	Сенсорні
Тип абонетських пристроїв	залежно від стандарту зв'язку: термінал з бездротовим інтерфейсом (телефон, рація, пейджер, PDA, ноутбук, КПК, ПК)	термінал з бездротовим інтерфейсом IEEE802.11s, рідше IEEE802.16 (ноутбук, нетбук, PDA, КПК, ПК, смартфон з Wi-Fi)	рухомий мобільний термінал з бездротовим інтерфейсом	вбудований в автомобіль термінал (ПК) з бездротовим інтерфейсом	сенсор з бездротовим інтерфейсом
Функції абонентських пристроїв	лише виконують функцію кінцевих пристроїв з прийому/передачі інформації	- інфраструктурна Mesh: кінцеві пристрої з прийому/передачі; - абонентська Mesh: і як кінцеві пристрої, і як проміжні вузли (роутери)	одночасно як кінцеві пристрої та як проміжні вузли (роутери), які власно й (само-)утворюють мережу		
Тип магістральної частини мережі	фіксована (дротова) інфраструктура, задані точки радіо-доступу абонентів	фіксована (бездротова) інфраструктура	відсутня будь-яка постійна інфраструктура, вся мережа повністю складається з кінцевих абонетських пристроїв		
Спосіб утворення магістральної частини мережі	задані точки радіо-доступу абонентів; статична детермінована топологія мережі	задані точки радіо-доступу абонентів; динамічна самоорганізація топології мережі	будь-які випадкові вузли динамічно самоутворюють тимчасову бездротову топологію		
Роутинг	у бездротових сегментах роутинг відсутній, роутинг здійснюється починаючи з фіксованих (дротових) сегментів	багатокроковий (multi-hop) роутинг з динамічною самоорганізацією (Ad-Hoc) у бездротовому сегменті			

В табл. 2 наведено класифікацію БМ залежно від зони осяжності (радіуса дії мережі) [9]:

Таблиця 2 – БМ залежно від зони осяжності (радіуса дії) [9]

Класс	Приклади стандартів	Радіус
Wireless Wide Area Networks (WWAN)	супутникові; стільникові: CDMA, UMTS, GSM, NMT, AMPS; радіальні; транкінгові: TETRA	глобальні
Wireless Metropolitan Area Networks (WMAN)	IEEE 802.16 (Wi-MAX)	декілька км
Wireless Local Area Networks (WLAN)	IEEE 802.11 (Wi-Fi)	~100м – 1км
Wireless Personal Area Networks (WPAN)	802.15.1 (Bluetooth); 802.15.4a (сенсорні ZigBee);	~10м

Розробка стандартів для WWAN, в тому числі й рекомендацій щодо безпеки WWAN, виконується такими організаціями, як ITU-T та ETSI. Значну кількість стандартів БМ меншого радіуса дії, які використовуються на практиці, розроблено IEEE.

Для стандартів БМ розроблено спеціальні технології захисту (802.11i, WPA, WEP, 802.1X) [6, 7, 9]. В цих технологіях реалізовано превентивні засоби та механізми безпеки, такі як: протоколи, програмне та апаратне забезпечення, що реалізує криптографічні перетворення, автентифікацію, керування доступом, контроль цілісності повідомлень; міжмережні екрани; технологія VPN.

Однак тенденції розвитку бездротових телекомунікацій, підвищуючи складність БМ як об'єкта керування та захисту, неодмінно призводять до зростання кількості вразливостей та загроз, які наслідуються від усіх попередніх інтегрованих технологій та підсистем. Це спричиняє потенційну можливість виникнення більшої кількості ***інцидентів безпеки*** в сучасних та майбутніх БМ.

IV Архітектура Ad-Hoc мереж з точки зору ІБ

Ad-Hoc мережі за принципами організації відрізняється від традиційних мереж. Цими принципами є:
- можливість утворення мережі випадковими абонентами;
- децентралізація, відсутність інфраструктури (наприклад, базових станцій);
- самоорганізація (пристрої з'єднуються «на льоту»);
- багатокрокова маршрутизація з перенаправленням (forwarding) пакета від вузла до вузла.

Останній принцип має на увазі, що кожен вузол мережі може відігравати роль бездротового маршрутизатора-посередника (intermediate router), що перенаправляє IP пакети до наступного (next-hop) вузла, який в свою чергу може бути або кінцевим отримувачем (destination) або також посередником.

На відміну від класичних бездротових мереж абонентського доступу, (таких як GSM/GPRS/EDGE, CDMA, Wi-MAX, Wi-Fi в режимі інфраструктури, тощо) – Ad-Hoc мережах радіозв'язок використовується не лише для надання доступу кінцевим абонентам, але й для динамічної самоорганізації бездротової магістральної мережі (wireless backbone) з багатокроковою маршрутизацією між бездротовими роутерами (точками доступу), якими можуть бути й самі абонетські пристрої.

На сьогоднішній день Ad-Hoc мережі (за виключенням сенсорних мереж) будуються на базі існуючого програмно-апаратного забезпечення, фізичного та канального інтерфейсів в рамках стандартів бездротового зв'язку (Табл. 3).

Таблиця 3 – Класифікація стандартів фізичних та канальних інтерфейсів Ad-Hoc мереж (класифікація автора)

Тип Ad-Hoc мережі	Клас бездротової технології	Стандарт	Радіус
Mesh Networks	Wireless Metropolitan Area Networks (WMAN)	IEEE 802.16 (Wi-MAX)	декілька км
MANET; Mesh Networks	Wireless Local Area Networks (WLAN)	IEEE 802.11 (Wi-Fi)	~100м – 1км
MANET	Wireless Personal Area Networks (WPAN)	802.15.1 (Bluetooth);	~10м
Sensor Networks		802.15.4a (ZigBee);	

Як мережний рівень використовується стандартний стек інтернет-протоколів, останнім часом – версія IPv6, спеціально розроблена з урахуванням потреб мобільних пристроїв та безпеки. Транспортний рівень зазвичай не відрізняється від стандартного стеку TCP/IP і використовує - TCP та UDP.

Як правило для переключення мережі в режим Ad-Hoc достатньо лише встановити в системних настройках клієнтського програмного забезпечення (драйвер бездротового мережного адаптеру) опцію роботи в режимі однорангової мережі (Ad-Hoc). Таким чином, можна створити клієнтську Ad-Hoc мережу або MANET (Mobile Ad-Hoc Network), з'єднавши портативні комп'ютери (ноутбуки), КПК, PDA, комунікатори, мобільні телефони або інші мобільні пристрої, в яких присутні адаптери стандартних фізичних та канальних інтерфейсів IEEE 802.11 (Wi-Fi) або IEEE 802.15.1 (Bluetooth).

За Ad-Hoc архітектурою організується зв'язок між ***сенсорами***, які збирають та передають дані моніторингу фізичних параметрів навколишнього середовища (акустичних, оптичних, інфрачервоних, тиску, температурних, хімічних, радіочастотних тощо) або параметрів біологічних організмів, зокрема людини (телебіометрія). В більшості ***сенсорних мереж*** як фізичний та канальний інтерфейс використовується спеціально розроблений стандарт ZigBee. Найрозповсюдженою операційною системою, під керуванням якої працюють сенсори є TinyOS.

Принцип організації зв'язку в ***Mesh мереж*** хоча і наслідує більшість підходів Ad-Hoc мереж, однак спирається на інфраструктуру у вигляді бездротових стаціонарних маршрутизаторів (Mesh-роутерів), які відіграють роль точок бездротового доступу з певним обмеженим радіусом дії. Mesh-роутери не підключаються до фіксованої мережі (як традиційні точки доступу Wi-Fi), а натомість з'єднані один з одним за допомогою бездротового зв'язку за принципом Ad-Hoc мережі, тобто пересилають пакети через радіоканали від одного роутера до іншого.

Ті ж самі принципи, які забезпечують Ad-Hoc мережам ефективність та привабливість, роблять складною і критичною проблему безпеки [1].

По-перше, це незахищеність радіоефіру як відкритого середовища передачі надає порушнику можливості прослуховування, зашумлення каналів зв'язку, закладання або модифікації пакетів. Ця проблема є спільною для всіх бездротових мереж і вирішується зазвичай на різних рівнях моделі OSI:

на мережному рівні (IPv6): VPN; IPSec з криптографічним шифруванням пакетів з використанням блочних симетричних алгоритмів (3DES, AES-128, ГОСТ 28147) та контролю цілісності пакета шляхом розрахунку значення імітовставки HMAC на основі значень геш-функцій SHA-1 або MD5;

на канальному рівні: шифрування потоковими симетричними криптоалгоритмами інформації, що передається через відкритий канал радіозв'язку (RC4, CCMP RFC2610); застосування широкосмугового сигналу, завадостійке та помилкокорегуюче кодування, геш-функція CRC32;

на фізичному рівні: направленими антенами та контролем меж поширення радіосигналу.

Однак у випадку Ad-Hoc мереж використання вказаних заходів ускладнене. Навіть якщо в тій мірі, в якій це дозволяє децентралізована динамічна топологія, використовувати механізми безпеки, які запропоновані в базових стандартах (наприклад IEEE 802.11.i), все одно залишаються критичні вразливості, які дуже важко перекрити.

Зокрема, криптографічні засоби мають спиратися на механізми розподілу ключів, такі як інфраструктура відкритих ключів (PKI) з сервером сертифікатів ключів. Але в багатьох випадках Ad-Hoc мережі повністю децентралізовані та не мають постійної інфраструктури, тому використання центральних серверів може бути неможливе.

Навіть якщо є певна централізована структура (захищений сервер), все одно існує можливість компрометації незахищених вузлів мережі та отримання таким чином несанкціонованого доступу до ключової інформації.

Крім того, можливість відносно легкої компрометації вузла (наприклад, шляхом фізичного доступу) створює додаткові внутрішні загрози, так звані Візантійські атаки (Byzantine attacks). В зв'язку з цим виникає ситуація, коли неможливо довіряти будь-якому внутрішньому вузлу, який може бути інсайдером (Byzantine attacker), тобто авторизованим вузлом, який має автентифікаційну інформацію (ключі) і є «легалізованим» учасником інформаційного обміну.

Як можна побачити, навіть механізми шифрування, контролю цілісності, розподілу ключів та керування доступом шляхом автентифікації не вирішують повністю проблему безпеки Ad-Hoc мереж.

Ще більше загострює проблему той факт, що будь-який (навіть компрометований) вузол мережі потенційно може відігравати роль маршрутизатора, який має пересилати пакети, призначені іншим вузлам. В зв'язку з легкістю компрометації будь-якої кількості таких маршрутизаторів, та вразливістю існуючих протоколів маршрутизації в Ad-Hoc мережах виникає безліч можливостей для реалізації Візантійських атак як на рівні контролю (control plane), так і на рівні даних (data plane, forwarding) маршрутизації.

V Перший рубіж захисту БМ – превентивні (запобігаючі) технології безпеки

Розділимо всі технології безпеки на ***превентивні*** та ***реактивні***.

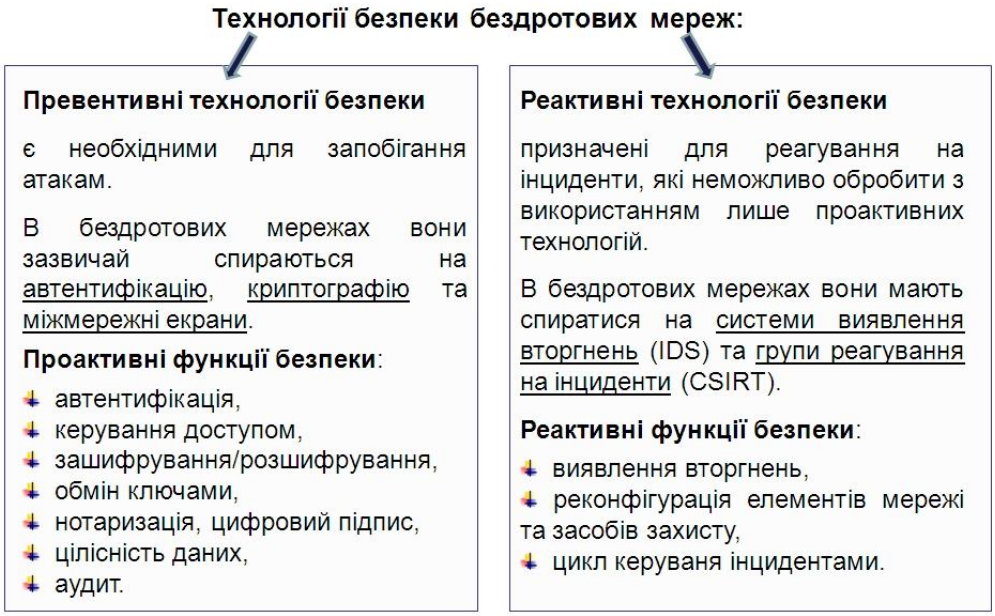

Рисунок 1 – Класифікація технологій безпеки БМ

Превентивні технології безпеки є необхідними для запобігання атакам. В БМ вони зазвичай спираються на криптографічні механізми та гарантують функції безпеки, такі як: зашифрування/розшифрування, обмін ключами, цифровий підпис, керування доступом, цілісність даних, автентифікація, нотаризація.

В таблиці 4 наведено деякі приклади окремих елементів превентивних технологій, що реалізують відповідні функції безпеки в БМ стандартів IEEE 802.11i та GSM:

Таблиця 4 – Приклади елементів превентивних технологій, що реалізують функції безпеки в БМ

Стандарт / Функція	WLAN IEEE 802.11	WLAN IEEE 802.11i	WWAN GSM
автентифікація	802.1X, RADIUS	802.1X, RADIUS	SIM-card, IMSI, Ki, A3, SRES, RAND, A8, Kc, BTS, MSC, AUC
керування доступом	міжмережні екрани, VPN	міжмережні екрани, VPN	IMEI, MSC, HLR, VLR, EIR
конфіденційність	WEP, RC4	WPA2, CCMP, AES-128	Kc, A5, BTS, MSC

Розглянемо *ITU-T X.1121* [11] як офіційну рекомендацію щодо загально-абстрактної архітектури безпеки в бездротових мобільних мережах. Згідно з нею в БМ має бути впроваджена багаторівнева *система інформаційної безпеки*, яка має реалізовувати певні *функції безпеки*, щоб задовольнити встановленим *вимогам безпеки*.

Наступним кроком проаналізуємо загальну модель безпеки OSI. Згідно з *ITU-T X.800* [12] *механізми безпеки* забезпечують *сервіси безпеки*, останні, в свою чергу, надають *функції безпеки*. Для того щоб практично реалізувати в БМ функції безпеки та задовольнити вимогам безпеки, в X.1121 рекомендуються певні *технології безпеки*.

Рівень ІБ, який сьогодні може бути гарантовано традиційними технологіями превентивного захисту інформації (ЗІ) в БМ, не завжди можна визнати як цілком прийнятний, особливо для таких категорій ІзОД, як оперативна інформація критичного змісту (стосовно керування кризовими ситуаціями, інцидентами), телемедицина, критичні інфокомунікаційні інфраструктури, персональні дані тощо. При цьому треба підкреслити, що саме ці нові типи та застосування БМДС є й будуть найбільш актуальними для динамічних оперативних сценаріїв найближчого майбутнього, в яких має передаватись ІзОД вказаних

категорій безпеки.

VI Необхідність другого рубежу захисту БМ – реактивних технологій безпеки

Специфіка БМ, наявність в них великої кількості вразливостей та поява інцидентів призводять до необхідності створювати другий рубіж захисту, який має створюватись *реактивнми технологіями ІБ* [1, 4, 5]:

- бездротових систем виявлення вторгнень (Wireless Intrusion Detection Systems – WIDS);
- груп з реагування на інциденти (Computer Security Incidents Response Team – CSIRT);
- автоматизованих систем обробки інцидентів (Incident Handling Systems – IHS);
- розслідування інформаційних злочинів (Forensics).

Реактивні технології безпеки призначені для виявлення, реагування й обробки атак та інцидентів, яких не вдалось запобігти з використанням лише проактивних технологій. Одними з типічних для БМ прикладів таких інцидентів є :

- ушкодження або компрометація бездротового обладнання (маршрутизаторів, точок доступу) шляхом несанкціонованого фізичного або логічного доступу;
- внесення несанкціонованих змін до таблиць маршрутизації або іншої керуючої інформації протоколів;
- DDoS або DoS атаки, зокрема шляхом навмисного порушення правил MAC-доступу та «засмічення» каналів передачі тощо.

Реактивні технології безпеки в БМ мають спиратися на механізми виявлення вторгнень та реагувати на виялені інциденти шляхом реконфігурації бездротової мережної інфраструктури.

На сьогодні вже проведено значну кількість досліджень, присвячених механізмам виявлення вторгнень та реагуванню на інциденти в «звичайних» дротових телекомунікаційних мережах. Однак, при цьому треба відмітити, що БМ характеризуються певними особливостями [9] (наприклад, істотно обмежена смуга пропускання, істотна зміна якості каналу в часі тощо), які не дозволяють в повній мірі застосовувати вже розроблені підходи та реактивні технології безпеки в БМ без відповідної адаптації та модифікації.

На момент проведення даного дослідження існує одне офіційне керівництво щодо розробки та оцінки бездротових систем виявлення вторгнень (IDS), розроблене Агенством національної безпеки США - *SNAC NSA "Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems" (2005)* [13]. Цей документ, хоча він стосується лише мереж IEEE 802.11 та не відображає всіх можливостей сучасних бездротових IDS, може бути використаний як основа для розробки та оцінки більш повної та сучасної реактивної технології безпеки БМ в частині виявлення вторгнень.

VII Безпека багатокрокової маршрутизації в Ad-Hoc мережах

Даний підрозділ статті спирається на дослідження, проведене автором в період наукової стажировки в Будапештському технічному університеті (Угорщина), яке було підтримано Вишеградським фондом.

Найвразливішою ланкою бездротових Ad-Hoc мереж є багатокрокова маршрутизація [8, 14] як базова функція мережного рівня, що забезпечує доставку пакетів даних від роутера-джерела (source) до роутера-призначення (destination) через динамічно (само-)утворюваний маршрут, що включає проміжні роутери, динамічно з'єднані бездротовими каналами радіозв'язку за принципом саморганізації та реконфігурації залежно від змін в топології мережі.

Головні складнощі: динамічність змін топології; відкритість середи передачі; фізична незахищеність бездротових роутерів, розміщених на неконтрольованії території з можливістю здійснення несанкціонованого фізичного доступу до обладнання, фізичного отримання ключової криптографічної інформації, та подальшої компрометації роутера з його використанням як інсайдера («Візантійска атака»); відносна відкритість мережі для включення нових вузлів (роутерів); непередбаченість маршрутів та учасників інформаційного обміну (роутерів-посередників) тощо.

Основний зміст робіт автора [8, 14] присвячено робастності багатокрокової маршрутизації до «Візантійських помилок». В центрі уваги – слабкості (вразливості) протоколів маршрутизації в площині форвардингу даних, а також стратегічні «Візантійські атаки». Проведено аналіз та показано обмеження декількох протоклів маршрутизації. Виявлено критичні помилки в протоколах та запропоновано ефективні сценарії атак. Піддано критиці існуючу методологію розробки протоколів.

Результатом [8, 14] є обгрунтування необхідності кардинально нового підходу щодо виявлення та реагування на інциденти безпеки (в першу чергу стратегічні «Візантійські» атаки) на площині форвардингу даних багатокрокової маршрутизації в бездротових Ad-Hoc мережах.

VII Висновки

Більшість розроблених технологій безпеки БМ направлено на запобігання порушенням безпеки на базі криптографічних механізмів в ***традиційних*** БМ. Однак лише ці механізми не завжди можуть ефективно перекрити специфічні вразливості ***Ad-Нос мереж*** і не захищають від всіх можливих загроз.

Однак, ті частини завдання, що стосуються власне архітектури та механізмів реактивних технологій безпеки Ad-Нос мереж, особливо механізмів та заходів з реагування на інциденти та Візантійські атаки в площині форвардингу даних багатокрокової маршрутизації, на сьогодні залишаються майже невирішеними, або ці рішення не є придатними для практичного завстосування.

Тому найбільш перспективним напрямком є створення другого рубежу захисту, направленого на виявлення, реагування та обробку вторгнень (інцидентів).

Література: ***1.*** *Гладиш С. Проблеми та перспективи безпеки Ad-Нос мереж // Зб. наук. праць НАУ «Захист інформації». Спец. вип. – 2008. – с. 143 - 148.* ***2.*** *Кононович В., Тардаскін М. Парадигма інформаційної безпеки телебіометрики та сенсорних телекомунікаційних мереж // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - №12. – 2006. – с. 56 - 66.* ***3.*** *Тардаскіна І. В. Перколяційні моделі протидії функціонуванню несанкціонованої наносенсорної мережі // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - №16. – 2008. – с. 40 -48.* ***4.*** *Гладиш С. В. Реактивні технології безпеки бездротових мереж // Зб. пр. XI Міжн. наук.-практ. конф. "Безпека інформації в інформаційно-телекомунікаційних системах". - 2008. - Пуща Озерна - с 102 - 103.* ***5.*** *S. Gladysh. Reactive security technologies for wireless networks // Зб. тез. конф. «Захист в інформаційно-комунікаційних системах» – 2008. – НАУ, Київ. – с. 52 – 53.* ***6.*** *L. Buttyan, J.-P. Hubaux. Security and Cooperation in Wireless Networks. -Cambridge University Press, 2007. – 496 p.* ***7.*** *L. Buttyan, V. Gligor, D. Westhoff. Security and Privacy in Ad Hoc and Sensor Networks. Lecture Notes in Computer Science No. 4357. – Springer, 2007. - 193 p.* ***8.*** *Gladysh S. V. Strategical attacking on data forwarding plane of routing protocols with Byzantine failure robustness // Radio-Electronic and Computer Systems. – №5. - 2009. – p. 96 – 101.* ***9.*** *Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей. – М.: Горячая Линия – Телеком, 2008. – 288 с.* ***10.*** *Інтернет ресурс. Офіційний веб-сайт DARPA: http://www.darpa.mil* ***11.*** *ITU-T X.1121 Recommendation. Framework of security technologies for mobile end-to-end data communications. – Geneva, 2004. – 27 pp.* ***12.*** *ITU-T X.800 Recommendation. Security architecture for Open Systems Interconnection for CCITT applications. – Geneva, 1991. – 48 pp.* ***13.*** *SNAC NSA Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS). – USA, 2005. – 24 pp.* ***14.*** *Кононович В. Г., Гладиш С. В. Виявлення та реагування на нциденти безпеки маршрутизац в бездротових Ad-Нос мережах // Зб. пр. XII Міжн. наук.-практ. конф. "Безпека інформації в інформаційно-телекомунікаційних системах". - 2009. - Пуща Озерна, 19 - 22 травня 2009 р. - с. 102 - 103.*

УДК 534.21:004.56.5(045)

АКУСТИЧЕСКАЯ СИСТЕМА ДЛЯ АДАПТИВНОГО ПОДАВЛЕНИЯ СИГНАЛОВ РЕЧЕВОГО ДИАПАЗОНА

Борис Журиленко, Владимир Недашковский, Надежда Николаева, Ольга Сачук
Национальный авиационный университет

Анотація: **Проведені теоретичні дослідження можливості застосування адаптивних методів компенсації акустичних сигналів для захисту інформації.**
Summary: **The conducted theoretical researches of possibility of application of adaptive methods of compensation of acoustic signals for defence of information.**
Ключевые слова: **Акустические каналы утечки информации, адаптивные системы, защита информации, компенсация волн, плоские волны, сферические волны.**

I Введение

За последние годы в результате исследований по «адаптивным системам» появились различные адаптивные автоматы, свойства которых в некотором смысле напоминают определенные свойства живых систем и биологических адаптивных процессов.

Задачи адаптивных систем достаточно разнообразны, однако их объединяет общая идея. По определению Я. З. Цыпкина [1] – это системы, уменьшающие первоначальную неопределенность на основе информации, получаемой в процессе управления. Для них характерна априорная неопределенность самой структуры