УДК 621.396

Шаціло П.В., Сова О.Я., Симоненко О.А., Жук П.В.

АНАЛІЗ ОСНОВНИХ АСПЕКТІВ БЕЗПЕКИ ФУНКЦІОНУВАННЯ МОБІЛЬНИХ РАДІОМЕРЕЖ З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ

Анотація:

У статті проводиться аналіз основних аспектів безпеки функціонування мобільних радіомереж з динамічною топологією,що відносяться до класу MANET.

Аннотация:

В статье осуществляется анализ основных аспектов безопасности функционирования мобильных радиосетей с динамичной топологией, которые относятся к классу MANET.

Abstract:

The article the analysis of the main aspects of the cafety of the mobile radio networks with dynamic topology which belonig to the class MANET.

Динамічна топологія побудови мобільних радіомереж (МР) або *MANET* (*Mobile Ad-Hoc Networks*) припускає відсутність фіксованої мережевої інфраструктури (базових станцій) і централізованого управління [1]. В останні роки спостерігається підвищений науковий інтерес до дослідження МР через наявність недорогих бездротових мережевих технологій (стандарти IEEE 802.11, IEEE 802.11*g*, IEEE 802.11*n*, Bluetooth). Класичним прикладом застосування МР є перспективні мережі радіозв'язку тактичної ланки управління військами [3]. Виділимо основні особливості цих мереж:

– відсутність фіксованої інфраструктури (стаціонарних базових станцій);

– децентралізоване управління (кожен вузол автономний, виконує функції хоста та маршрутизатора);

– динамічна топологія (всі вузли мобільні); значна розмірність (сотні й тисячі вузлів);

– низька пропускна здатність радіоканалів (у порівнянні зі стаціонарними мережами);

– неоднорідність вузлів (по мобільності, ресурсам потужності й продуктивності); обмежена фізична безпека й ін.

Одним із завдань управління МР є забезпечення її безпеки [4–6].

Порушення безпеки МР розглядається як інцидент безпеки інформаційно-аналітичного процесу оперативного управління МР через втрату конфіденційності, цілісності і доступності її інформаційних ресурсів. Атакою на МР називається дія або послідовність зв'язаних між собою дій порушника, які приводять до реалізації *погрози* шляхом використання її уразливостей [7].

Погрози за метою впливу поділяються на погрози порушення конфіденційності, цілісності і доступності (або відмови в обслуговуванні) [8]. Погроза порушення конфіденційності полягає в тім, що інформація стає відомою особам без відповідних повноважень доступу. Погроза цілісності містить у собі будь-яке навмисне перекручування (модифікацію або навіть видалення) інформації, що зберігаються у вузлах мережі або при її передачі мережею. Погроза відмови в обслуговуванні виникає щоразу, коли в результаті навмисних дій знижується продуктивність або блокується доступ до

деякого ресурсу мережі або вузла. Результативність реалізації погроз залежить від такої характеристики МР як *уразливість*.

Уразливості МР у порівнянні зі стаціонарними мережами визначаються особливостями її архітектури та протоколів функціонування [5, 6]:

1. Обмеженість фізичної безпеки радіоканалу. Широкомовна природа радіоканалу дозволяє супротивникові ставити активні й пасивні завади, здійснювати прослуховування передач вузлів, аналізувати мережевий трафік і, як наслідок, розкривати існуючу систему управління військами.
2. Вузол може бути захоплений на полі бою супротивником або скомпрометований.
3. Динамічна топологія й колективна робота вузлів припускають уразливість функціонування протоколів канального, мережевого та інших рівнів, а також методів управління топологією, радіоресурсом і т.д. [4].
4. Обмеженість ресурсів елементів мережі: ємність батареї, обсяг пам'яті, продуктивність процесора вузла; пропускна здатність радіоканалу та ін.

Реалізація погроз на практиці здійснюється противником шляхом проведення атак. Можна виділити наступні основні типи атак:

1. Аналіз мережевого трафіка (з метою ідентифікації топології мережі, ідентифікації вузлів та їх ролі, ідентифікація протоколів обміну (маршрутизації, адресації та ін.), ідентифікація операційних систем, визначення вразливостей вузла та ін.).
2. Підміна довіреного об'єкта мережі.
3. Впровадження помилкового об'єкта мережі (наприклад, за допомогою помилкового маршруту) з подальшою селекцією (модифікацією) або підміною потоку інформації, який проходить через нього.
4. Відмова в обслуговуванні (насичення смуги пропускання, переповнення буферів та ін.).
5. Порушення прав доступу.
6. Завантаження невірних даних (модифікація інформації при її передачі мережею або в процесі обробки та зберігання на вузлі, порушення конфіденційності інформації та ін.).

Безпека в безпроводових радіомережах забезпечується за допомогою різних сервісів та механізмів, які повинні враховувати особливості МР з метою захисту від атак. Сервіси безпеки зазвичай включають такі основні поняття [4]:

– таємність (*confidentiality*) – неможливість ознайомлення противником зі смисловим змістом переданого повідомлення;

– справжність (аутентифікація, *authentication*) – впевненість у тому, що дані відправлені саме тією особою, від чийого імені вони отримані;

– цілісність (*integrity*) – впевненість у тому, що прийняті дані не були змінені на шляху від відправника до одержувача;

– контроль доступу (*access control*) – запобігання доступу користувача до об'єкта (ресурсу) без відповідних повноважень;

– неспростовність (*non-repudation*) – механізм, що гарантує неможливість відмови від факту отримання або відправлення повідомлення;

– доступність (*availability*) – властивість ресурсу системи, що полягає в можливості його використання на вимогу користувача, що має відповідні повноваження, незважаючи на можливі атаки [8, 9, 10].

У табл. 1 показані механізми реалізації зазначених сервісів. Захист від зовнішніх атак включає шифрування інформації, використання цифрового підпису та забезпечення інших сервісів безпеки. Так цифровий підпис дозволяє перевірити справжність, цілісність повідомлення, а також забезпечити його неспростовність (забезпечує захист від атак типу відмова, підміна і модифікація переданих даних). Електронний цифровий підпис (ЕЦП) – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних. ЕЦП – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. ЕЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. ЕЦП є ефективним рішенням при передачі даних у МР під час управління бойовими підрозділами. Всі учасники електронного документообігу отримують рівні можливості незалежно від їх фізичного розташування. Документи, підписані електронним цифровим підписом, можуть бути передані до місця призначення за лічені секунди з гарантією їх справжності та цілісності.

Таблиця 1

Сервіси механізмів реалізації безпеки

Сервіси безпеки	**Механізми реалізації**
таємність	шифрування
справжність	цифровий підпис
цілісність	шифрування, хеш-функція
контроль доступу (ідентифікація)	блок ідентифікації абонента, протоколи ідентифікації вузлів
неспростовність	цифровий підпис
доступність	засоби фізичної безпеки,

Для захисту від внутрішніх атак передбачається використовувати систему виявлення атак (СВА або IDS) – програмний засіб, призначений для контролю чи виявлення фактів неавторизованого доступу в радіомережу. Украй важлива характеристика СВА – те, як вона аналізує накопичені нею дані.

Сьогодні існує кілька різних типів СВА, що відрізняються різними алгоритмами моніторингу даних і підходами до їх аналізу. Кожному типу системи відповідають ті або інші особливості використання. Існує дві основні категорії методів виявлення атак: виявлення аномалій і виявлення зловживань.

Виявлення аномалій використовує моделі передбачуваної поведінки користувачів і додатків, інтерпретуючи відхилення від „нормальної" поведінки як потенційне порушення захисту.

Основний постулат виявлення аномалій полягає в тому, що атаки відрізняються від нормальної поведінки. Скажемо, певну „нормальну" активність мобільного вузла можна змоделювати досить точно. Допустимо, конкретний мобільний вузол авторизується в МР приблизно в один і той же час доби, передає певні типи інформації із певною частотою, тривалістю та до певних абонентів, використовує певний набір методів маршрутизації, тощо. Якщо ж система визначить суттєві відхилення від „норми" – вона позначить цей вузол як підозрілий і продовжить моніторинг його стану та діяльності.

Головна перевага систем виявлення аномалій полягає в тім, що вони можуть виявляти раніше невідомі атаки. Визначивши, що таке „нормальна" поведінка, можна виявити будь-яке порушення, не залежно від того, передбачене воно моделлю

потенційних погроз чи ні. У реальних системах перевага виявлення раніше невідомих атак зводиться нанівець великою кількістю фіктивних тривог. До того ж, системи виявлення аномалій важко налагодити коректно, якщо їм доводиться працювати в середовищах, для яких характерна значна мінливість та невизначеність.

Системи виявлення зловживань визначають, що відбувається не так, як повинно відбуватися. Вони містять описи атак (сигнатури) і у відповідності до цих описів перевіряють потоки даних, з метою виявлення проявів відомої атаки [11]. Основна перевага систем виявлення зловживань полягає в тому, що вони зосереджуються на перевірці даних, аналізують їх і, зазвичай, породжують дуже мало фіктивних тривог.

Головний недолік систем виявлення зловживань пов'язаний з тим, що вони можуть визначати тільки відомі атаки, для яких існує певна сигнатура. При виявленні нових атак розроблювачі повинні будувати відповідні їм моделі, додаючи їх до бази сигнатур [12].

Системи виявлення вторгнень, створені для проводових мереж неефективні або не можуть бути застосовані в МР. Виділимо основні відмінності між безпроводовими й стаціонарними СВА і визначимо пропозиції щодо побудови СВА в МР.

1. Так як трафік у радіомережі по своїй природі не може бути сконцентрований в одній точці, то мережева реалізація СВА не прийнятна для МР. Тому IDS-агент повинен бути активованим на кожному вузлі МР і виконуватися незалежно (рис. 1).

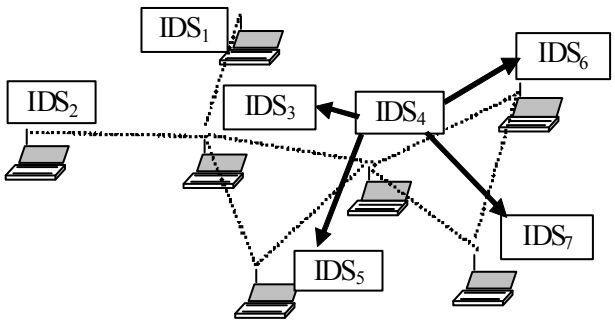

Рис. 1. Архітектура багатоагентної СВА для мобільних радіомереж

Варіант архітектури IDS-агента представлений на рис. 2. Вся інформація, що надходить у вузол, проходить у реальному масштабі часу аудит і реєстрацію в модулі моніторингу й зберігається у відповідній базі даних. Модулі локального й кооперативного виявлення аналізують інформацію на предмет атак. Модуль безпеки здійснює криптографічні методи захисту при передачі службових повідомлень між IDS-агентами. Модулі реакції разом із системою управління мережею планують і здійснюють відповідні дії.

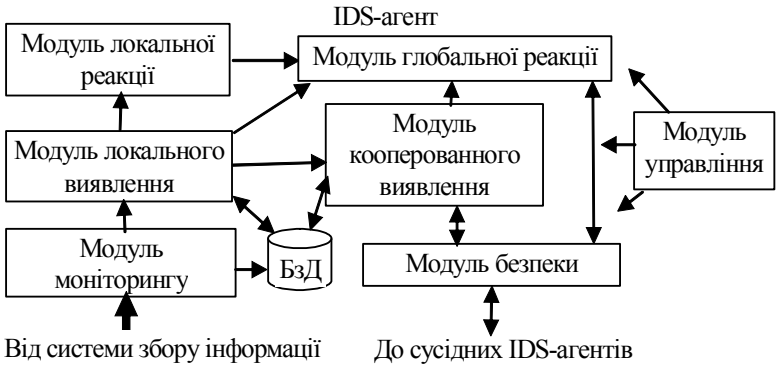

Рис. 2. Концептуальна модель IDS-агента

Реакцією на ідентифікацію або виявлення захоплених (скомпрометованих) вузлів може бути:

– виключення даних вузлів із процесу обміну інформацією (наприклад, побудова обхідних маршрутів) або їхнє придушення;

– зменшення впливу даних вузлів за рахунок передачі декількома незалежними маршрутами передачі;

– зміна ключової інформації у вузлах мережі.

2. При кооперованій роботі СВА окремо взятий вузол не може повністю довіряти сусіднім вузлам, внаслідок можливої їхньої компрометації або захоплення.

Загальний підхід до аналізу поведінки сусіднього вузла полягає в реалізації принципу „сторожового собаки" [13, 14, 15]. Кожен вузол створює профілі нормальної й аномальної поведінки сусіда за певними параметрами: мобільність, протоколи, що використовуються канальним і мережевим рівнями, частота перебудування або втрати маршруту, частота скидання пакетів, якість маршрутів тощо. За певний період часу здійснюється перерахунок контрольованих параметрів й уточнення ступеня довіри до сусіда. Остаточне рішення про компрометацію певного вузла може бути прийняте після узгодження свого ступеня довіри з іншими вузлами. Необхідно відзначити, що мобільність вузлів створює додаткові труднощі в розрізненні їх нормального й аномального функціонування.

3. Обмеженість ресурсів МР. Необхідність аналізу реального трафіка вимагає значної продуктивності комп'ютера, що входить у суперечність із наявними ресурсами вузлів МР. Тому реалізація багатоагентних СВА можлива в мобільних базових станціях, а в мобільних вузлах – реалізація окремих функцій цих систем [2].

4. Виділимо основні вимоги до СВА в МР:

–децентралізованість функціонування;

–чутливість у певній області мережі (на відстані декількох ретрансляцій);

–низька величина помилкових спрацьовувань;

–мінімізація зв'язних й обчислювальних ресурсів;

–інтеграція модулів СВА на різних рівнях ЕМ ВВС і за функціями управління МР[4];

–наявність механізмів реакції на атаку.

Крім того, з метою організації коректної роботи СВА в середовищах, для яких характерна значна мінливість та невизначеність, а також для забезпечення здатності СВА до самонавчання на основі отриманого досвіду в процесі моніторингу мережі пропонується інтелектуалізувати роботу СВА, шляхом використання технологій обробки знань. Так, на рис. 3 зображена узагальнена модель інтелектуальної системи управління вузлом МР, центральне місце в якій займає база знань та база методів управління, які відповідають різним функціям вузлової системи управління, в тому числі забезпечення безпеки.

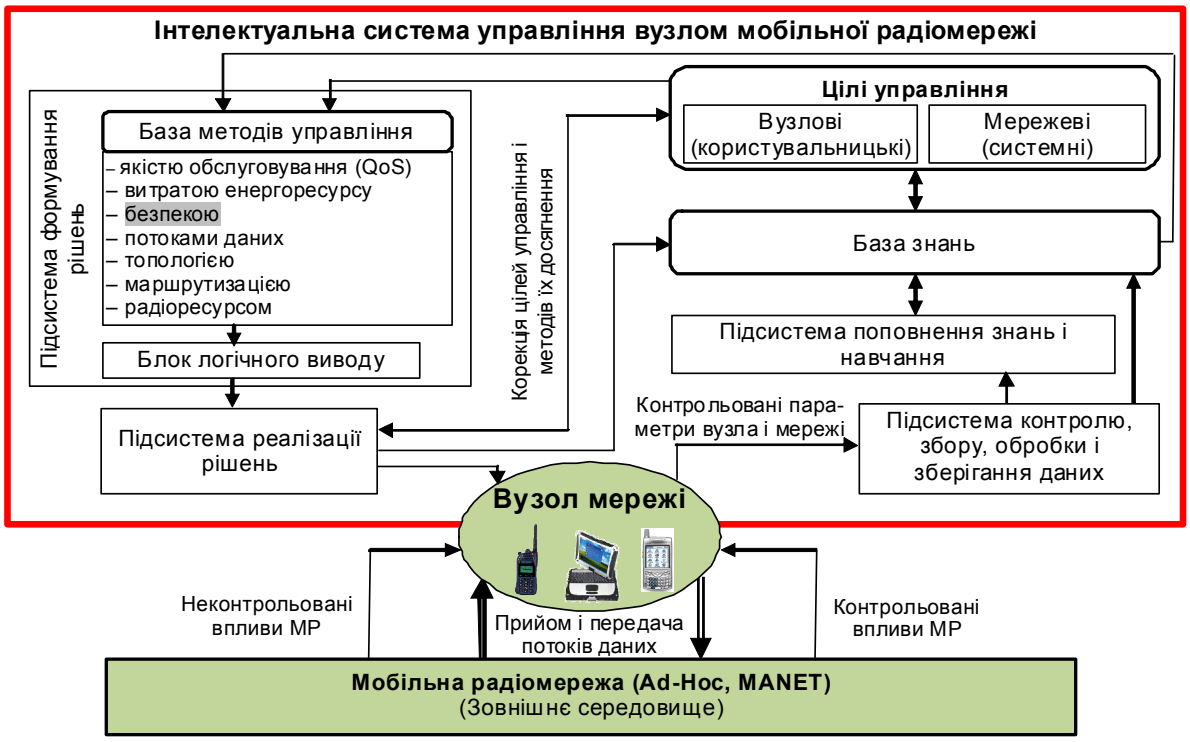

Рис. 3. Узагальнена модель інтелектуальної системи управління вузлом МР

Зважаючи на те, що різні вузли МР вирішуватимуть суміжні завдання, пов'язані із організацією безпечного функціонування радіомережі, пропонується реалізувати СВА у вигляді множини інтелектуальних агентів (ІА), котрі знаходяться в кожному вузлі МР. ІА – програмний продукт, здатний діяти в інтересах поставленої мети і володіти наступними властивостями: активність; мобільність; кооперованість і можливість комунікації з іншими агентами; сумісна робота на досягнення загальної мети. При цьому, головною властивістю ІА є інтелектуальність – здатність до самонавчання, логічної дедукції чи конструювання моделей навколишнього середовища для знаходження оптимальних способів поведінки [16].

Таким чином, захист від зовнішніх атак у МР повинен здійснюватися методами криптографічного захисту, внутрішніх атак – застосуванням СВА. З урахуванням особливостей МР а також можливих варіантів побудови СВА пропонується:

– крім компонентів традиційних моделей захисту, які використовуються в стаціонарних мережах зв'язку (розмежування доступу та виявлення несанкціонованого доступу, аутентифікація та криптографічний захист), пропонується ввести до складу вузлової системи управління підсистему виявлення атак;

– вузлова СВА повинна функціонувати в децентралізованому режимі і мати можливість приймати колективні рішення із забезпечення безпеки МР;

– для реалізації СВА у складі вузлової системи управління пропонується використовувати технологію інтелектуальних агентів, побудованих з використанням технологій обробки знань.

В ході подальших досліджень будуть розроблені методи та моделі прийняття рішень інтелектуальними агентами, пов'язані з виявленням атак в МР та відповідною реакцією на них.

Література:

1. *Григорьев В.А., Лагутенко О.И., Распаев Ю.А.* Сети и системы радиодоступа. – М.: Эко-Трендз, 2005. – 384 с.

2. *Романюк В.А.* Мобильные радиосети – перспективы беспроводных технологий // Сети и телекоммуникации. – 2003. – № 12. – С. 62 – 68.

3. *Романюк В.А.* Напрямки розвитку тактичних систем зв'язку // II Науково-технічна конференція ВІТІ "Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення". – К.: ВІТІ НТУУ "КПІ". – 2004. – С. 22 – 32.

4. *Миночкин А.И., Романюк В.А.* Методология оперативного управления мобильными радиосетями // Зв'язок. – 2005. – № 2. – С. 53 – 58.

5. *Міночкін А.І., Романюк В.А.* Безпека мобільних радіомереж // Збірник наукових праць № 5. – К.: ВІТІ НТУУ "КПІ". – 2004. – С. 116 – 126 .

6. *Лукацкий А.В.* Обнаружение атак. – СПб: БХВ–Петербург, 2003. – 608 с.

7. *Максим М.*, *Полино Д.* Безопасность беспроводных сетей. – М.: ДМК Пресс, 2004. – 288 с.

8. *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атаки через Internet. – М.: НПО "Мир и семья", 1997.

9. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв'язок. – 2004. – № 2. – С. 46 – 50.

10. *Миночкин А.И., Романюк В.А.* Управление энергоресурсом мобильных радиосетей // Зв'язок. – 2004. – № 8.

11. *Миночкин А.И., Романюк В.А.* Протоколы маршрутизации в мобильных радиосетях // Зв'язок. – 2001. – №1. – С. 31 – 36.

12. *Zhang Y., Lee W.* Intrusion Detection in Wireless Ad-Hoc Networks // In Proceedings of IEEE MOBICOM, 2000. – pp. 275 – 283.

13. *Котенко И.В., Карсаев О.И.* Использование многоагентных технологий для компьютерной защиты информационных ресурсов в компьютерных сетях // Перспективные информационные технологии и интеллектуальные системы, 2001. – № 3.

14. *Marti S., Guuli T.J., Lai K., Baker M.* Mitigating Routing Misbehavior in Mobile Ad Hoc Networks // In Proceedings of IEEE MOBICOM, 2000.

15. *Huang Y., Lee W.* A Cooperative Intrusion Detection System for Ad Hoc Networks // In Proceedings of the ACM Workshop on Security of Ad hoc and Sensor Networks, 2003.

16. *Романюк В.А., Сова О.Я., Жук П.В., Романюк А.В.* Концепция иерархического построения интеллектуальных систем управления тактическими радиосетями класса MANET: сборник тезисов докладов и выступлений участников XXII Международной Крымской конференции ["СВЧ-техника и телекоммуникационные технологии"], (КрыМиКо). / – Севастополь, 2012. – С. 265.