УДК 621.391

В. В. Сальник, С. В. Сальник, Е. М. Бовда

АНАЛІЗ МЕТОДІВ ЗАПОБІГАННЯ ВТОРГНЕННЯМ У МОБІЛЬНІ РАДІОМЕРЕЖІ КЛАСУ MANET

Проведено аналіз існуючих методів запобігання вторгненням в мобільні радіомережі класу MANET. Визначено перелік вимог до таких методів для застосування їх у мобільній радіомережі. Запропоновано напрями створення сучасних методів запобігання вторгненням у мобільні радіомережі, визначено напрям подальших досліджень.

К л ю ч о в і с л о в а : забезпечення безпеки мобільної радіомережі, MANET, система запобігання вторгненням, IPS.

Постановка проблеми. Останнє десятиліття мобільні радіомережі (МР) класу MANET (Mobile Ad-Hoc Networks) все більше застосовуються у повсякденному житті та військовій галузі, а саме, в тактичній ланці управління військами [1]. Тому основним питанням під час побудови МР є забезпечення її безпеки. Актуальність вирішення цієї проблеми пов'язана з характеристичними особливостями МР, такими як передавання інформації в радіосередовищі, динамічна топологія, масштабованість, що може бути використано противником для вторгнення у МР. Метою вторгнення у МР може бути: порушення цілісності, доступності, достовірності інформації на рівнях мережевої моделі OSI (Open Systems Interconnection), вплив на функціонування програмної, апаратної та інформаційної складових МР.

Таким чином, МР повинна містити в собі підсистему управління безпекою (ПУБ), робота якої буде спрямована на виявлення та запобігання вторгненням у МР. Для цього ПУБ повинна мати в своєму складі систему виявлення та запобігання вторгненням, функціонування якої ґрунтується на основі методів виявлення вторгнень та методів запобігання вторгненням (МЗВ) [2].

Аналіз останніх досліджень і публікацій. Організація безпеки МР, захист мережі від вторгнень, а також питання проектування та побудови системи запобігання вторгненням розглядалися у працях [12–18].

Мета статті. Проаналізувати існуючі методи запобігання вторгненням у МР з метою визначення можливостей їх застосування в МР класу MANET.

Об'єктом розгляду у статті є процес забезпечення безпеки інформації, яка передається в МР.

Предметом дослідження є МЗВ противника в МР, які використовуються на сьогоднішній день.

Виклад основного матеріалу. Забезпечення безпеки МР має комплексний характер і включає в себе теоретичну та практичну складові.

До теоретичної складової віднесено визначення переліку критеріїв та стандартів, вивчення розвитку, вдосконалення та впровадження нових підходів до забезпечення безпеки МР.

До критеріїв безпеки даних віднесено конфіденційність, яка передбачає доступність тільки для осіб або інтелектуальних систем, що мають відповідні на це повноваження; цілісність інформації, яка передбачає її незмінність в процесі передавання від відправника до одержувача; достовірність, яка передбачає відповідність цієї інформації її явному опису та змісту.

Стандарти висувають такі вимоги до забезпечення безпеки інформації [6, 9]: забезпечення інформаційної безпеки, фізична безпека, адміністративна безпека, проведення аудиту безпеки та ін.

До практичної складової відноситься впровадження та застосування алгоритмів, протоколів і технологій, на яких ґрунтується побудова ПУБ для управління МР, а саме:

– протоколів безпеки (SRP, SAODV, TAODV, SAR, ARAN, Confidant, SLSP та ін.);

– стандартів безпеки (WEP, WPA, WPA2, TKIP, WRAP, CCMP та ін.).

Основними інструментами забезпечення безпеки у безпроводових мережах стандартів 802.11 є протоколи WEP та WPA. Однак ці протоколи мають недоліки, пов'язані з криптографічними ключами. Так, ще у 2001 році С. Флурером, І. Мантіні та А. Шаміром було встановлено, що ключ шифрування довжиною 40 бітів та 104 біта може бути взламаний після аналізу чотирьох мільйонів фреймів. Для безпроводової локальної мережі це відповідає трьом годинам роботи, після чого ключ взламується завдяки пасивно зібраним фреймам у мережі.

Виходячи з цього, для усунення недоліків стандарту WEP був розроблений стандарт WPA (Wi-Fi Protected Access). WPA перевершує WEP завдяки додаванню протоколу TKIP (Temporal Key Integrity Protocol) та механізму аутентифікації на базі 802.1x і протоколу EAP (Extensible Authentication Protocol). Шифруванням даних у WPA займається протокол TKIP, який використовує динамічні ключі шифрування. При всіх посиленнях безпеки інформації та контролю доступу, вразливості знаходяться і в протоколі WPA. Е. Тьюзі та М. Бек за допомогою розробленого підходу провели успішну атаку на ключі TKIP [7].

З аналізу предметної області випливає, що забезпечення безпеки МР на інформаційному, програмному та апаратному рівнях вимагає застосування інтелектуалізації підсистеми забезпечення безпеки (ПЗБ). Вказана необхідність обґрунтована характеристичними особливостями вторгнень та функціональними можливостями ПЗБ.

ПЗБ поєднує у собі рішення щодо захисту від вторгнень, які на сьогоднішній день знайшли відображення у системі виявлення вторгнень (СВВ) та системі запобігання вторгненням (СЗВ). У даній статті розглянемо існуючі МЗВ, які забезпечують роботу СЗВ з метою їх застосування в МР класу MANET.

СВВ призначена для виявлення вторгнень в МР, проведення класифікації та кластеризації вторгнень і надання пропозицій щодо управлінських рішень відносно кожного окремого вторгнення в МР.

СЗВ – інформаційна, програмна або апаратна система безпеки, яка не тільки виявляє вторгнення або порушення безпеки, а й вживає заходів для захисту мережі та реагування на вторгнення.

СЗВ поділяють на мережеві, які відстежують трафік у мережі та блокують підозрілі потоки даних і системи для безпроводових мереж, які перевіряють активність в безпроводових мережах. Зокрема виявляють невірно сконфігуровані точки бездротового доступу до мережі; аналізують мережевий трафік, ідентифікують нетипові потоки, наприклад DoS і DDoS атаки. СЗВ для окремих вузлів – це програми, які виявляють підозрілу активність у вузлі.

МЗВ являє собою програмно-апаратний елемент МР, який аналізує трафік на таких рівнях моделі OSI: прикладному, представлення, сеансовому, транспортному, мережевому, канальному та фізичному, а також виявляє та реагує на вторгнення. Виходячи із характеристичних особливостей МР, для підтримання безпеки мережі МЗВ повинні відповідати вимогам точності, застосування в мобільному середовищі, самонавчання, запобігання нововиявленим вторгненням, прогнозування, роботи в умовах нечіткої мережевої активності, роботи в режимі реального часу та ін.

На відміну від стаціонарних мереж, середовищем передавання інформації в МР є радіоканал, а елементами МР – мобільні вузли, які взаємодіють між собою та з вузлами стаціонарної мережі. У зв'язку з цим, з одного боку, кількість варіантів здійснення вторгнень у МР збільшується порівняно з проводовими мережами, а з іншого боку, весь спектр вторгнень, які застосовуються у проводовій мережі, може бути застосований у МР [2,11].

Тому, розглядаючи вплив противника на інформаційні, програмні та апаратні засоби МР, варто зазначити, що об'єктами атак є правила і технічні процедури, які здійснюють з'єднання, і обмін даними в мережі, що відносяться до різних рівнів мережевої моделі OSI. Об'єктами проведення вторгнень (атак) є: керування передаванням даних; обмін пакетами; організація з'єднань; програмні, технічні, енергетичні характеристики засобів зв'язку; керування інформацією або вузлом та ін. Приклади вторгнень у МР, які можуть бути застосовані на різних рівнях мережевої моделі OSI, наведено в табл. 1.

Даний вплив може здійснюватись під час вторгнення, яке реалізується за допомогою множини різнонаправлених атак [11]. Під вторгненням розуміється несанкціонований вхід в інформаційно-телекомунікаційну систему в результаті дій, що порушують політику безпеки або обходять систему захисту [8, 10].

Через те, що кожен тип атак характеризує множину цілей при проведенні вторгнень у МР, дії яких направлені на відповідні рівні мережевої моделі OSI, при виявленні вторгнення кожному типу атаки присвоюється характеристична терма, що характеризує вплив атак на рівнях мережевої моделі OSI.

Мета атаки може не збігатися з метою реалізації загроз, вона може бути спрямована на отримання проміжного результату, необхідного для досягнення подальшої реалізації загрози. У разі такої невідповідності атака розглядається як етап підготовки до вчинення дій, спрямованих на реалізацію загрози. Результатом атаки є наслідки, які є реалізацією загрози або сприяють такій реалізації [10].

Таблиця 1

Види застосовуваних атак на рівнях мережевої моделі OSI

Рівень моделі OSI	MANET		Тип реалізації	Основні види атак
Прикладний рівень (Application)	Прикладний рівень (Application)		програмний	відмова в доступі до прикладних програм; отримання (або зміна) пріоритету обслуговування окремих видів трафіка, відмова у сервісі, порушення з'єднання мережі
Рівень представлення (Presentation)			програмний	впровадження шкідливих програм троянів
Сеансовий рівень (Session)			програмний	відмова в обслуговуванні
Транспортний рівень (Transport)	Транспортний рівень (Transport)		програмний	порушення доставки великих пакетів даних, побудова фальшивих пакетів, переповнення буфера, порушення в обслуговуванні шляхом частого відправлення запитів, надсилання великої кількості пакетів запитів
Мережевий рівень (Network)	Мережевий рівень (Network)	Роутинговій рівень (Ad-Hoc Routing)	програмний	порушення доставки повідомлень, порушення маршрутизації, відмова в обслуговуванні певного класу трафіка, надсилання неправдивих повідомлень, атака ICMP-запитами, підроблення адрес
Канальний рівень (Data Link)	Канальний рівень (Data Link)		апаратний	порушення синхронізації, відмова в доступі, відмова в сервісі, підтримка MAC-адреси, самостійна розсилка даних
Фізичний рівень (Physical)	Фізичний рівень (Physical)		апаратний	відмова в сервісі, розрив зв'язку, встановлення шуму, відмова у перетворенні сигналів, перехоплення та прослуховування

В основу існуючих на сьогодні МЗВ в бездротових мережах покладені принципи функціонування аналогічних методів, розроблених для проводових мереж зв'язку, реалізація яких представлена в стандарті IEEE 802.11b; протоколах WEP, WEP, WPA, TKIP; ідентифікаторі SSID; системі аутентифікації OSA та ін. Тому з метою визначення характеристичних особливостей методів виявлення вторгнень було проведено їх аналіз, у якому розглянуто методи, які застосовуються у проводовому та безпроводовому середовищі.

1. R. Janakiraman, M. Waldvogel, Q. Zhang [13], якій застосовується у проводовому середовищі. Основою методу є використання базової сигнатури, базової аномалії та проведення самонавчання. Побудова методу підтримує можливість децентралізації та взаємодії з іншими підсистемами безпеки і компонентами МР. Даний метод виконує моніторинг та аналіз стану мережі в межах зв'язності та зони відповідальності. У разі виявлення вторгнення у мережі МЗВ застосовує управлінське рішення відповідно до бази знань.

Перевагами методу є збирання та оновлення інформації про загрози вторгнень та способи запобігання вторгненням на рівні сигнатур та мережевих аномалій. Недоліками методу є неможливість використання у безпроводовому середовищі, динамічній топології, нечіткій мережевій активності та малий об'єм пам'яті.

2. O. Awodele, S. Idowu, O. Anjorin, J. Joshua [14]. Основою запропонованого МЗВ, який застосовується у проводовому середовищі, є мультибагаторівневий підхід до системи виявлення та запобігання вторгненням, яка складається з трьох окремих шарів: файл аналізатор, системний ресурс та об'єднані шари нейронної мережі. Кожен з цих шарів об'єднав обидва критерії основних методик виявлення: аномалію та підпис. Метод включає в себе профілактику та можливість виявлення вторгнень на основі класифікації та кластеризації вхідних даних у шарі нейронної мережі. У разі виявлення вторгнення у мережу МЗВ застосовує управлінське рішення відповідно до бази знань.

Перевагами методу є: робота в режимі реального часу, самонавчання та широкий спектр виявлення аномалій в мережі. Недоліками методу є неможливість використання у безпроводовому середовищі, динамічній топології, нечіткій мережевій активності; забезпечення безпеки тільки на рівні аномалій.

3. S. Khanum, M. Usman, A. Alwabel [4, 5]. Запропонований МЗВ застосовується у безпроводовому середовищі. Основою методу є MUSK архітектура та мобільні агенти. Архітектура складається з трьох агентів: аналізатора агент, координатора агента та агента управління, що дозволяє самонавчатися. Метод підтримує можливість виявлення та запобігання сигнатури в МР. Мобільний агент встановлюється на кожному вузлі в мережі, який взаємодіє з іншими вузлами. У разі виявлення вторгнення у мережу МЗВ приймає управлінське рішення відповідно до бази знань.

Перевагами методу є робота в безпроводовому середовищі та реальному режимі часу, самонавчання системи і широкий спектр виявлення сигнатур в мережі. Недоліками методу є неможливість використання у динамічній топології, нечіткій мережевій активності; забезпечення безпеки тільки на рівні сигнатур.

4. K. Vieira, A. Schulter, C. Westphall [6]. В основі запропонованого МЗВ, якій застосовується у безпроводовому середовищі, покладене хмарне обчислення та поведінковий шаблон, що дозволяє об'єднувати існуючу базу знання з метою виявлення аномалій та сигнатур вторгнення з подальшим їх запобіганням. МЗВ включає додаткові заходи безпеки, аналіз поведінки та аналіз знань. Метод побудований на штучних нейронних мережах та здатний оцінювати поведінку невеликих відхилень. МЗВ може самонавчатись, визначати вторгнення за допомогою поширення своїх алгоритмів та існуючої бази знань. Основа методу полягає у виявленні вторгнення за поведінковим шаблоном, що дозволяє охопити ширший спектр невідомих атак.

Перевагами методу є використання у безпроводовому середовищі, самонавчання, виявлення сигнатур та мережевих аномалій. Недоліками методу є неможливість використання у мережі з динамічною топологією, нечіткою мережевою активністю та відсутність управлінського рішення.

5. M.-L. Shyu and V. Sainani [7]. Запропонований МЗВ також застосовується у безпроводовому середовищі. В його основу покладено розподілену архітектуру мультиагентної СЗВ за компонентами класифікатора. Ця інтеграція інтелектуального агента дозволяє швидко реагувати на вторгнення та запобігати вторгненню в режимі реального часу. За допомогою інтелектуального аналізу даних розподілені архітектури виявлення вторгнення використовують багатоагентні підходи та аналіз даних.

Перевагами методу є використання у безпроводовому середовищі з динамічною топологією, виявлення сигнатур та аномалій, інтелектуалізація, децентралізація, самонавчання. Недоліками методу є неможливість використання у нечіткій мережевій активності, відсутнє управлінське рішення, великий час відгуку.

6. M.-Y. Su, G.-J. Yu and C.-Y. Lin Sainani [19]. Запропонований МЗВ, який також застосовується у безпроводовому середовищі, заснований на нечітких асоціативних правилах із застосуванням інтелектуального аналізу даних, що не задовільняє вимоги до роботи в режимі реального часу. За допомогою нечітких асоціативних правил рішення приймається кожні дві секунди.

Перевагами є робота в режимі реального часу, інтелектуальний аналіз даних, запобігання атакам на основі аномалій, використання нечітких асоціативних правил. Недоліками методу є неможливість використання у безпроводовому динамічному середовищі, великий час реагування, забезпечення безпеки тільки на рівні аномалій.

У таблиці 2 наведена порівняльна характеристика розглянутих МЗВ, яка дозволяє визначити їх напрямки роботи та основні переваги і недоліки.

Таблиця 2

Порівняльна характеристика методів запобігання вторгненням

Автор	Метод	Запобігання аномаліям/ сигнатурі	Недоліки	Переваги
Реалізовані в проводовому середовищі				
R. Janakirman M. Waldvogel Q. Zhang	базова сигнатура, базова аномалія	так/так	не використовується у безпроводовому середовищі, нечіткій мережевій активності	постійне оновлення інформації про загрози вторгнень та способи запобігання атакам
O. Awodele S. Idowu O. Anjorin J. Joshua	базова сигнатура, базова аномалія	так/так	не використовується у безпроводовому середовищі, нечіткій мережевій активності	робота в режимі реального часу, самонавчання та широкий спектр виявлення аномалій
S. Khanum M. Usman A. Alwabel	метод сигнатур	ні/так	неможливість використання у динамічній топології, нечіткій мережевій активності	робота в режимі реального часу, самонавчання
Реалізовані в безпроводовому середовищі				
K. Vieira A. Schulter C. Westphall	гібридний (сигнатура і аномалії)	так/так	неможливість використання в мережі з динамічною топологією, нечіткій мережевій активності, відсутнє управлінське рішення	низькі обчислювальні витрати, використання у безпроводовому середовищі, самонавчання
M.-L. Shyu V. Sainani	інтелек-туальний аналіз даних	так/так	неможливість використання при нечіткій мережевій активності, відсутнє управлінське рішення, великий час відгуку	використання у мережі з динамічною топологією, інтелектуалізація, децентралізація, самонавчання
M.-Y. Su G.-J. Yu C.-Y. Lin	нечіткі правила асоціації	так/ні	неможлива робота у безпроводовому динамічному середовищі	робота в режимі реального часу, інтелектуальний аналіз даних, використання нечітких асоціативних правил

Таким чином, найбільше висунутим вимогам відповідають методи M.-L. Shyu, V. Sainani та M.-Y. Su, які реалізовані для використання в мобільному середовищі, що може бути масштабоване. Дані методи побудовані на протоколах маршрутизації та мають технології прийняття рішень. Однак запропоновані методи не реалізують можливість самонавчання до запобігання новим типам вторгнень, не пристосовані до застосування у випадках непередбачуваної, неповної та нечіткої мережевої активності.

Висновки

Проведений аналіз показав, що існуючі методи в основному здатні вирішувати завдання із запобігання вторгненням у проводову або стаціонарну радіомережі, що своєю чергою не задовольняє вказані вище вимоги до застосування даних методів при побудові СЗВ для використання у МР та мережах тактичної ланки управління військами.

Враховуючи постійно змінювану природу атак, відсутність можливості концентрування трафіка МР в одній точці, самонавчання, прийняття управлінського рішення, а також мобільність елементів МР, динамічність топології та масштабованість, можливим рішенням може бути побудова інтелектуальних МЗВ на основі комплексного застосування нечіткої логіки, сенсорних та нейронних

мереж. При цьому основне завдання при розробленні інтелектуальних методів полягає у можливості створення на їх основі СЗВ, здатних працювати з різнорідними типами трафіка, великим об'ємом даних, розпізнавати нові типи вторгнень, надавати управлінське рішення, та можливості взаємодії з СЗВ інших вузлів МР.

У ході подальших досліджень будуть розроблені модель функціонування СЗВ у МР класу MANET та методи запобігання вторгненням із застосуванням нечіткої логіки, сенсорних та нейронних мереж.

Список використаних джерел

1. Романюк, В. А. Мобильні радіомережі – перспективи безпроводових технологій [Текст] / В. А. Романюк // Сети и телекоммуникации. – 2003. – № 12. – С. 62–68.

2. Міночкін, А. І. Виявлення атак в мобільних радіомережах [Текст] / А. І. Міночкін, В. А. Романюк, П. В. Шаціло // Збірник наукових праць ВПІ НТУУ "КПІ" № 1. – К. : ВІТІ НТУУ "КПІ", 2005. – С. 102–111.

3. Jangra1, A. Goel, N. Priyanka and Bhati, K. Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering. – 2010. – pp. 189–196.

4. B. Sun, K. Wu, U. W. Pooch. "Alert Aggregation in Mobile Ad Hoc Networks". The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03). – 2003. – pp. 69–78.

5. Чевардин, В. Е. Анализ угроз безопасности информации в сетях [Текст] / В. Е. Чевардин, А. В. Романюк, И. Н. Диянчук // Збірник наукових праць ВІТІ НТУУ "КПІ" № 1. – К. : ВІТІ НТУУ "КПІ", 2012.

6. Hoeper, K. Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks / K. Hoeper, G. Gong // Proceedings of the 5th International Conference on Ad-Hoc, Mobile, and Wireless Networks - ADHOC-NOW 2006, ser. LNCS 4104. – 2006. – pp. 224–237.

7. Климов, С. М. Противодействие компьютерным атакам. Методические основы [Текст] / С. М. Климов, М. П. Сычёв, А. В. Астрахов. – М. : МГТУ им. Н. Э. Баумана, 2013. – 108 с.

8. Лукацкий, А. Обнаружение атак [Текст] / А. Лукацкий. С Пб. : изд-во БХВ, 2003. – 596 с.

9. Yun J.-H. WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks / J.-H. Yun, I.-H. Kim, J.-H. Lim, S.-W. Seo. // In Ubiquitous Convergence Technology (ICUCT 2006). – 2007. – pp. 200–209. LNCS 4412.

10. Макаренко, С. И. Информационная безопасность [Текст] : учеб. пособие / С. И. Макаренко. – Ставрополь : СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

11. Сальник, С. В. Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET [Текст] / С. В. Сальник, О. Я. Сова, Д. А. Міночкін // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 1. – С. 103–111.

12. Ramaprabhu Janakiraman, Marcel Waldvogel, Qi Zhang. Indra: A peer-to-peer approach to network intrusion detection and prevention, Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2003.

13. Awodele, Oludele; Idowu, Sunday; Anjorin, Omotola; Joshua, Vincent J., "A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)", Academic journal article from Issues in Informing Science & Information Technology, Vol. 6.2009

14. S. Khanum, M. Usman, and A. Alwabel. "Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks," International Journal of Computer Science Issues, IJCSI, vol. 9, 2012.

15. S. Khanum, M. Usman, K. Hussain, R. Zafar, and Dr M. Sher. "Energy-Efficient Intrusion Detection System for Wireless Sensor Network Based on MUSK Architecture" HPCA 2009, LNCS 5938, pp. 212–217, Springer-Verlag Berlin Heidelberg 2010

16. K. Vieira, A. Schulter, and C. Westphall. "Intrusion Detection for Grid and Cloud Computing" IT Professional, vol. 12, pp. 38–43, 2010.

17. M.-L. Shyu and V. Sainani. "A Multiagent-based Intrusion Detection System with the Suppor t of Multi-Class Supervised Classification" in Data Mining and Multi-agent Integration , L. Cao, Ed., ed: Springer US, 2009, pp. 127–142.

18. M.-Y. Su, G. -J. Yu, and C.-Y. Lin. "A real- time network intrusi on detection system for large-scale attacks based on an incremental mining approach" Computers & Scurity, vol. 28, pp. 301–309, 2009.

Стаття надійшла до редакції 16.12.2015 р.