УДК 621.391

[1]*Сергій Васильович Сальник*
[1]*Олег Ярославович Сова (канд. техн. наук, с.н.с.)*
[2]*Дмитро Анатолійович Міночкін (канд. техн. наук, с.н.с.)*

[1]*Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій, Київ, Україна*
[2]*Інститут телекомунікаційних систем Національного технічного університету України "Київський Політехнічний Інститут", Київ, Україна*

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ У МОБІЛЬНІ РАДІОМЕРЕЖІ КЛАСУ MANET

В статті проведено аналіз існуючих методів виявлення вторгнень в мобільні радіомережі, також здійснено класифікацію методів виявлення вторгнень. В ході проведення аналізу було розглянуто види застосовуваних атак на рівнях мережевої моделі OSI. Також вказані архітектури на базі яких можуть бути побудовані системи виявлення вторгнень, та визначені вимоги до методів виявлення вторгнень при їх застосуванні в мобільних радіомережах. Розкрито класифікацію методів виявлення вторгнень в мобільні радіомережі та розглянуто їх основні напрямки. Проаналізовано переваги та недоліки вказаних методів. Розглянуто існуючі авторські методи виявлення вторгнень, в ході чого з'ясовано перелік методів що найбільше задовольняють вимогам для застосування в мобільних радіомережах. Запропоновано напрями вдосконалення існуючих методів з метою використання в мережах типу MANET та забезпечення безпеки інформації, яка передається в них. Визначені завдання щодо подальших досліджень, в яких буде розроблено метод виявлення вторгнень із застосуванням нечіткої логіки та нейронних мереж.

Ключові слова: *мобільні радіомережі; MANET; забезпечення безпеки інформації; система виявлення вторгнень; методи виявлення вторгнень.*

Вступ

Постановка проблеми. В останні десятиліття мобільні радіомережі (МР) або мережі класу MANET (*Mobile Ad-Hoc Networks*) стають все більш вживаними як у повсякденному житті, так і у військовій галузі, особливо в тактичній ланці управління військами [1]. Одним з найважливіших питань, які необхідно вирішити в процесі їх проектування, є забезпечення безпеки зв'язку. Важливість вирішення цього питання пов'язана з тим, що в МР є вразливості, які зумовлені передачею інформації в радіосередовищі, динамічною топологією і масштабованістю МР, необхідністю збору значної кількості службової інформації про стан мережі для функціонування методів та протоколів на різних рівнях мережевої моделі OSI. Зазначені вразливості можуть бути використані противником для здійснення вторгнень у МР з метою порушення цілісності інформації, яка передається в МР, або організації деструктивного впливу на сам процес функціонування МР.

Таким чином, у МР має бути передбачена можливість як щодо виявлення вторгнень, так і щодо їх запобігання. Для забезпечення такої можливості вузлова система управління повинна містити у своєму складі підсистему управління безпекою [2], функціонування якої повинно здійснюватися на основі відповідних методів виявлення вторгнень (МВВ) та методів запобігання вторгненням. У даній роботі будуть розглянуті МВВ, які застосовуються для побудови систем виявлення вторгнень (СВВ) на сьогодні.

Аналіз останніх досліджень і публікацій. Організація безпеки МР, захист мережі від вторгнення, а також проблемні питання, пов'язані з побудовою СВВ, розглядалися в роботах [3-5, 18-23]. Більш детальний розгляд питання застосування зазначене у розділі – "Реалізація методів".

Мета статті. Проведення аналізу існуючих методів виявлення вторгнень в МР для визначення можливості їх застосування в МР, оцінки необхідних сервісів безпеки та механізмів їх реалізації.

Об`єкт розгляду статті. Процес забезпечення безпеки інформації, яка передається в МР.

Предмет дослідження. Методи виявлення вторгнень противника в МР, які використовуються на сьогоднішній день.

Виклад основного матеріалу дослідження

Аналіз предметної області. Під вторгненням розуміється несанкціонований вхід в інформаційно-телекомунікаційну систему, в результаті дій, що порушують політику безпеки або обходять систему захисту [6], метою якого є порушення цілісності, конфіденційності та доступності даних, які циркулюють в системі [7].

Відповідно, питання захисту будь-якої інформаційно-телекомунікаційної системи, в тому

числі МР, від вторгнення являє собою комплексну задачу, забезпечення яка покладається на:

систему виявлення вторгнень (СВВ) – попереджає про початок атак на інформаційно-телекомунікаційну систему;

систему запобігання вторгнень (СЗВ) – яка не тільки попереджує, але й вживає заходів для блокування вторгнення (атаки).

Сучасні рішення щодо захисту від вторгнення поєднують в собі функціональність двох типів систем СВВ і СЗВ, а їх об'єднання іноді називають системою виявлення і запобігання вторгнень. Однак у даній статті ми обмежимося розглядом існуючих сьогодні методів виявлення вторгнень для визначення можливості їх застосування в СВВ, реалізованих у вузлах МР класу MANET.

СВВ являє собою програмно-апаратний елемент вузла МР, призначений для виявлення фактів несанкціонованого доступу в МР або систему управління нею. Приймаючи до уваги те, що МР застосовуються в тактичній ланці управління військами, де існує висока загроза попадання мобільного вузла до рук противника, метою несанкціонованого доступу до МР може бути приховане управління вузловими та мережевими ресурсами, а також неавторизований вплив на програмні та апаратні засоби МР.

Розглядаючи неавторизований вплив на програмні і апаратні засоби МР, варто зазначити, що об’єктами атак противника є правила і технічні процедури, які здійснюють з'єднання і обмін даними в мережі, і відносяться до різних рівнів мережевої моделі OSI (*Open Systems Interconnection*). До них відносяться: управління передачею даних, обмін пакетами, організацію з’єднань, міжмережевий обмін, механічні та електричні характеристики засобів зв'язку, доступ до кодування, управління інформацією, вплив на файлову систему і. т.д. Приклад атак, які можуть бути застосовані на різних рівнях мережевої моделі OSI, наведено в табл. 1.

Таблиця 1

Види застосовуваних атак на рівнях мережевої моделі OSI

Рівень моделі	Тип реалізації	Основні види атак
Прикладний рівень (*Application*)	програмний	Відмова в доступі до прикладних програм; отримання (або зміна) пріоритету обслуговування окремих видів трафіка
Рівень представлення (*Presentation*)	програмний	Впровадження шкідливих програм троянів
Сеансовий рівень (*Session*)	програмний	Відмова в обслуговуванні
Транспортний рівень (*Transport*)	програмний	Порушення в обслуговуванні шляхом частої відправки запитів SYN, на підключення відповідно протоколу TCP, надсилання великої кількості пакетів запитів ICMP
Мережевий рівень (Network)	програмний	Відмова в обслуговуванні певного класу трафіка, надсилання неправдивих повідомлень про помилки під час передачі даних, атака ICMP-запитами (ICMP *Flooding*), підроблення адрес
Канальний рівень (*Data Link*)	апаратний	Відмова в доступі, підтримка MAC-адреси (MAC *Flooding*)
Фізичний рівень (*Physical*)	апаратний	Відмова в доступі, перехоплення та прослуховування

В основу побудови СВВ можуть бути покладені наступні архітектури:

1. Автономний агент – використовує невеликі окремі програми (агенти), для виконання функції моніторингу на хостах (вузлах) мережі. Автономний агент використовує ієрархічну структуру, яка координується агентом-координатором, для збору інформації з кожного мобільного вузла, або групи вузлів. Таким чином, виявляється будь-яка підозріла активність в МР.

2. Агент-менеджер – розташований в різних ділянках мережі, з метою централізованого збору та аналізу реєстрованих даних.

Існуючі сьогодні СВВ (зокрема, *VIPNet IDS*, система виявлення атак *“Форпост”, StoneSoft, Arbor Networks, Cisco Systems, Juniper Networks, PaloAlto, Check Point, StoneGate IPS* та ін.), використовують множину МВВ, які не враховують особливостей функціонування МР у тактичній ланці управління військами. Способи проведення вторгнень в мережу можуть включати в себе широкий спектр різнонаправлених атак, спрямованих на наведені вище вразливості МР [8]. Це, в свою чергу, визначає наступні вимоги до МВВ при їх застосуванні в МР класу MANET:

можливість як автономного так і кооперованого функціонування;

самонавчання (виявлення нових типів вторгнень, оновлення баз даних сигнатур);

можливість проведення аналізу (вторгнень, атак, правил, протоколів);

застосування при непередбачуваній, нечіткій мережевій активності;

наявність технології прийняття рішень, інтелектуалізації тощо;

можливість застосування навчального імітатора;

можливість оптимізації підсистем і оснащення СВВ на інших вузлах.

Проведемо аналіз існуючих МВВ з метою визначення можливості їх застосування при

побудові СВВ у мобільних радіомережах класу MANET, з урахуванням наведених вимог.

Аналіз методів виявлення вторгнень в МР.

Класифікація методів виявлення вторгнень в МР вказані на рис. 1.

Методи СВВ класифікуються:

І. За способом збору інформації про вторгнення:

1. Засновані на протоколі – використовуються для відстеження трафіка, що порушує правила певних протоколів або синтаксис мови і являє собою систему (або агента), яка відстежує та аналізує комунікаційні протоколи з пов'язаними системами або користувачами.

2. Засновані на прикладних протоколах – ведуть спостереження і аналіз даних, переданих з використанням специфічних для певних додатків протоколів.

3. На рівні додатків – засновані на пошуку проблем в певному додатку (прикладній програмі).

4. На рівні хоста (вузла) – встановлюються на вузлах і здійснюють спостереження за цілісністю файлової системи, системних журналів, додатків і т.д. Використання цього класу методів дозволяє виробити ефективні заходи запобігання аналогічних вторгнень у майбутньому [9].

Перевагою хостових методів є: менша кількість помилкових спрацьовувань; не вимагається постійне оновлення сигнатур; менша схильність до обману; вимагають меншого обслуговування і налаштування.

Недоліки хостових методів: необхідність завантаження і управління програмним забезпеченням на кожному вузлі, який захищається; сигнали тривоги надходять після успішної атаки; мережеві системи іноді забезпечують більш раннє попередження.

5. На рівні мережі – аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил (експертні системи). Мережеві системи виявлення вторгнення функціонують на мережевому рівні моделі OSI.

Мережеві системи в свою чергу поділяються на такі методи:

на основі сигнатур – в таких системах події, що відбуваються в мережі, порівнюються з ознаками відомих атак, які і називаються сигнатурами;

на основі бази знань – стежать за мережею, збирають статистику про поведінку мережі, виявляють відхилення і позначають їх як підозрілі;

гібридна СВВ – поєднує кілька підходів до розробки СВВ для створення найбільш повного уявлення про безпеку мережі. Гібридні СВВ, що представляють собою комбінацію різних типів систем, як правило, включають в себе можливості декількох категорій [10,11].

До недоліків використання системи на рівні мережі відноситься: неможливість генерування великої кількості сигналів, відсутність видимості внутрішнього трафіка, неспроможність до розпізнавання нових атак.

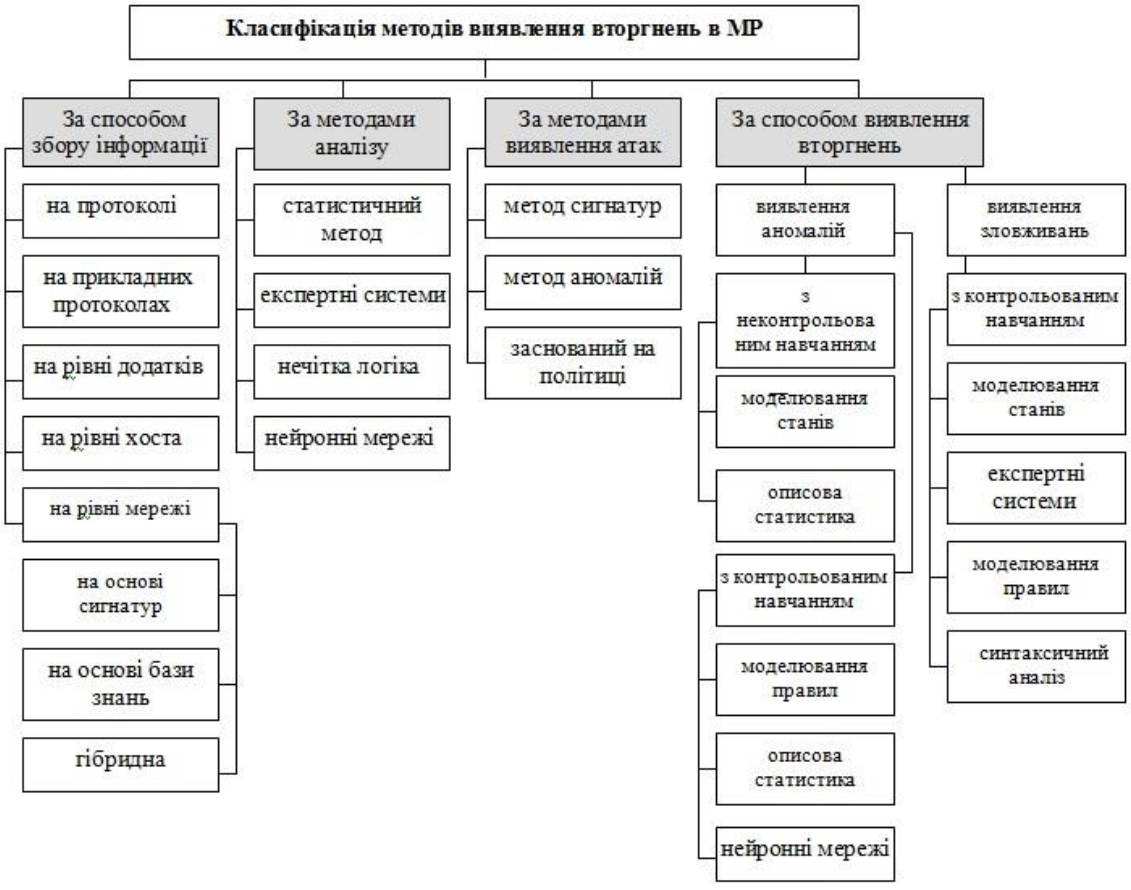

Рис. 1. Класифікація методів виявлення вторгнень в МР

II. За методами аналізу. Від даних методів багато в чому залежить ефективність СВВ. В даний час до них відносяться:

1. Статистичний метод – є універсальним, оскільки для проведення аналізу не потребує знань про можливі вторгнення і використовувані ним вразливості.

Основні переваги – використання розробленого апарату математичної статистики, який себе зарекомендував, та адаптація до поведінки суб'єкта.

Недоліки методу пов'язані з тим, що їх можна "навчити" сприймати несанкціоновані дії як нормальні.

2. Експертні системи – складаються з набору правил, які охоплюють знання експерта. Використання експертних систем являє собою поширений метод виявлення вторгнень, при якому інформація про вторгнення формулюється у вигляді правил. При виконанні цих правил приймається рішення про наявність несанкціонованої діяльності.

Перевагою підходу є повна відсутність помилкових тривог.

Недоліком є неможливість відображення невідомих вторгнень, оновлення сигнатур.

3. Нечітка логіка – нечітка класифікація є розвитком підходу експертних систем. Основна відмінність і перевага нечіткої класифікації – це можливість формулювання достовірних класифікаційних висновків виходячи з неповних і не цілком достовірних вхідних посилок. При виявленні загроз і атак нечітка логіка використовуються спільно з нейронними мережами або експертними системами, так як сама нечітка система дозволяє лише виносити припущення про можливу загрозу.

Недоліками нечітких систем є: відсутність стандартної методики конструювання нечітких систем; неможливість математичного аналізу нечітких систем існуючими методами.

Однак, недоліки нечіткої логіки не можуть переважити її переваги, саме тому перспективи нечіткої логіки, а значить, нейромережевих підходів до вирішення прикладних і погано формалізованих задач величезні і потребуючі.

4. Нейронні мережі – можуть проводити аналіз інформації, надаючи можливість оцінити, чи узгодяться дані з характеристиками, які вона навчена розпізнавати. Спочатку нейромережу навчають правильної ідентифікації на попередньо підібраній вибірці прикладів вторгнення. Реакція нейромережі аналізується і система налаштовується таким чином, щоб досягти необхідних результатів. На додаток, нейромережа може набиратися досвіду по мірі того, як вона проводить аналіз даних, пов'язаних з виявленням вторгнень.

Перевагою нейронних мереж при виявленні вторгнень є їх здатність вивчати характеристики умисних вторгнень та ідентифікувати елементи, які не схожі на ті, що спостерігалися в мережі раніше [12].

III. Методи виявлення вторгнень, реалізація яких ґрунтується на методах виявлення атак:

1. Метод сигнатур – заснований на пошуку сигнатури атаки, при якому програма, переглядаючи файли або пакети, звертається до словника з вірусами. Під сигнатурою атаки розуміється деякий шаблон, який відповідає даній атаці.

До переваг методу сигнатур відносяться: ефективне визначення атак і відсутність великої кількості помилкових повідомлень; надійна діагностика використання конкретного засобу або технології атаки; можливість початку процедури обробки інциденту і корекція заходів забезпечення безпеки.

Недоліками є: оновлення баз даних для отримання сигнатур нових атак.

2. Метод аномалій (відхилення від нормальної моделі дій користувача) – заснований на пошуку аномалій, де визначення нестандартної поведінки на вузлі або в МР покладається на детектор аномалій, що працює з інтелектуальною системою, яка відстежує відмінності.

Перевагами методу є: визначення атаки без знання конкретних деталей (сигнатури); детектори аномалій можуть створювати інформацію, яка в подальшому буде використовуватися для визначення сигнатур атак.

Недоліками методу є: велика кількість хибних сигналів при непередбаченій поведінці користувачів і мережевої активності; значні витрати на етапі навчання системи.

3. Метод, заснований на політиці – полягає в написанні правил мережевої безпеки, що визначають взаємодію елементів мережі між собою і використання протоколів.

Переваги методу: використання при виявленні нових (невідомих) атак.

Недоліки методу: трудомісткість створення бази політик [10, 13].

IV. За способом виявлення вторгнень в мережу:

1. Методи виявлення аномалій – процес виявлення атаки на основі порівняння дій користувачів з шаблонами нормальної активності. Метод призначений для розпізнавання процесу, що викликав зміни в роботі системи в результаті дій противника.

Методи виявлення аномалій поділяються на дві групи методів:

1.1. З контрольованим навчанням ("навчання з учителем"), до них належать:

метод моделювання правил – система виявлення протягом процесу навчання формує набір правил, що описують нормальну поведінку системи;

описова статистика – навчання полягає в зборі простої описової статистики системи, яка захищається, на основі множини показників, об'єднаних у спеціальну структуру;

нейронні мережі – структура застосовуваних нейронних мереж різна. Але у всіх випадках

навчання виконується даними, що представляють нормальну поведінку системи. Отримана навчена нейронна мережа використовується для оцінки аномальності системи.

1.2. З неконтрольованим навчанням (“навчання без учителя”), до них належать:

моделювання множини станів – нормальна поведінка системи описується у вигляді набору фіксованих станів і переходів між ними;

описова статистика – метод відповідає методу в контрольованому навчанні.

Основна відмінність між підгрупами методів полягає в тому, що методи контрольованого навчання використовують фіксований набір параметрів оцінки і якісь апріорні відомості про значення параметрів оцінки. Час навчання є фіксованим. У неконтрольованому навчанні множина параметрів оцінки може змінюватися з плином часу, а процес навчання відбувається постійно.

Перевагою технології виявлення аномалій являється орієнтування на виявлення нових типів вторгнень.

Недолік – необхідність постійного навчання.

2. Метод виявлення зловживань – процес виявлення атаки на основі порівняння поточного стану контрольованих ознак з апріорними відомостями про характеристики атак і полягає в описі вторгнення у вигляді сигнатури і пошуку даної сигнатури в контрольованому просторі. Дана технологія може виявити всі відомі вторгнення. Однак системи даного типу не можуть виявляти нові, ще невідомі види вторгнень [14].

Метод зловживань має одну реалізацію – з контрольованим навчанням (“навчання з учителем”) в яку входять:

метод моделювання станів – де вторгнення представляється як послідовність значень параметрів оцінки системи, яка захищається;

експертні системи – процес вторгнення представляється у вигляді різного набору правил;

моделювання правил – простий варіант експертних систем;

синтаксичний аналіз – системою виконується синтаксичний розбір з метою виявлення певної комбінації символів, які передаються між підсистемами і системами захищеного комплексу.

Основна перевага методу зловживань полягає в тому, що вони зосереджуються на аналізі перевірки даних і зазвичай породжують малу кількість помилкових тривог.

Основний недолік пов'язаний з тим, що метод може визначати тільки відомі атаки, для яких існує певна сигнатура [15].

Таким чином, кожен з описаних методів має низку переваг і недоліків, які визначають їх ефективність за різних умов застосування. Тому, при побудові реальних СВВ проводиться комбінування методів виходячи з вимог, які визначаються особливостями функціонування того чи іншого класу мереж.

Реалізація методів

В основу існуючих на сьогодні методів вторгнень в безпроводових 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 інше. Розглянемо детальніше окремі з них.

1. Y. Zhang, W. Lee та Y. Huang [16, 17] прийшли до висновку, що СВВ і СПВ повинні виконувати свої функції узгоджено. У запропонованій ними моделі, кожен вузол самостійно відповідає за виявлення вторгнень, а також передбачена можливість їх взаємодії. Розміщена на вузлах СВВ повинна відстежувати стан мережі в межах забезпечення зв'язку окремого вузла. Агент, який розміщений на вузлі виявляє порушення і ініціює відповідь щодо даної події. При виявленні аномалії під час передачі даних між вузлами передбачене підключення сусідніх агентів для ідентифікації вторгнень. Індивідуальні ідентифікатори (агенти) в сукупності утворюють комплексну систему захисту МР.

Згодом даний метод був удосконалений (Y. Zhang, та інші [23]) шляхом додавання можливості виявлення аномалій за допомогою класифікатора, який навчається на основі отриманих даних. Метою функціонування класифікатора є встановлення можливої найближчої події пов’язаної з вторгненням, з урахуванням послідовності попередніх подій.

2. P. Albers та O. Camp [18] запропонували використання розподілених і спільних архітектур СВВ за допомогою локального мобільного агента (ЛМА). ЛМА реалізується на кожному вузлі для забезпечення безпеки, проте її можливості можуть бути розширені для вирішення загальномережевого завдання. Після виявлення локального порушення, вузлова СВВ ініціює відповідь у СПВ та інформує інші вузли мережі.

Вказаний метод також був удосконалений (C. Manikopoulos та Li Ling [22]). Була запропонована архітектура для мереж типу MANET, де СВВ також виконувалась на кожному вузлі, але з метою збору та обробки даних зі свого вузла та сусідніх вузлів залучалися ідентифікатори стану.

3. O. Kachirsk та R. Guha [19] запропонували використання датчика в СВВ на основі технології mobile agent. У запропонованій ними моделі СВВ може бути розділена на три основних модулі, кожен з яких представляє мобільний агент з певною функціональністю. До даних модулів відносяться: модуль моніторингу; модуль прийняття рішень; модуль ініціювання відповіді.

Подібне розділення функцій було зроблено K. Nadkarni та A. Mishra [24] і передбачало наявність схеми з виявлення вторгнень, побудованої на принципі виявлення зловживань, котрі можуть відповідати значенням атак.

4. D. Sterne [20] запропонував динамічну модель, яка потенційно може масштабуватися, а при використанні у великих мережах використовується кластеризація. Даний метод визначення вторгнень реалізовувався кожним вузлом, в результаті чого вузол має можливість контролювати, аналізувати і реагувати відсиланням сповіщень на інші вузли. Також методом передбачено виконання фільтрації даних, відстеження вторгнень, і управління безпекою системи.

Питання кластеризації в подальшому досліджувалось N. Marchang та R. Datta [25], які запропонували новий алгоритм для виявлення вторгнень в кластері. Алгоритми використовують сумісні зусилля декількох різних вузлів для виявлення пошкоджених атакою вузлів шляхом моніторингу. Повідомлення щодо стану мережі передається між вузлами і, в залежності від отриманих повідомлень, вузли встановлюють пошкоджений вузол. Алгоритм працює таким чином, щоб надати можливість групі вузлів, ґрунтуючись на аналіз даних мережі, прийняти рішення щодо реакції на вторгнення.

5. B. Sun [21] запропонував метод Zone Based IDS (ZBIDS) який так само встановлюється на окремі вузли і при визначенні вторгнення розділяє зону пошуку на ділянки, які не перективаються. У застосуванні методу вузли мережі умовно поділяються на внутрішні і зовнішні зони. Кожен вузол має ідентифікатори (агенти). Ці агенти подібні агентам запропоновані Zhang та Lee, Y. Huang. До складу додаткових компонентів у вузловий СВВ входять: модуль збору даних, модуль оповіщення.

Підхід з кооперуванням вузлів в подальшому розглядалися M. Chatterjee, S.K. Das та D. Turgut [26], які розробили алгоритм, де прийняття рішень щодо виявлення вторгнення в мережу покладається на об'єднанні зусилля усіх вузлів мережі. Аналіз стану проводиться вузлом, після чого відбувається відправка інформаційних пакетів про стан вузла на інші вузли, де інформація знаходиться у стадії розгляду для виявлення безпечного вузла. У разі підозри щодо вторгнення вузол відзначається як підозрілий. СВВ мережі аналізує стан вузлів для побудови маршруту передачі даних з використанням безпечних вузлів.

У таблиці 2 наведена характеристика розглянутих методів, яка дозволяє визначити їх відповідність зазначеним вище вимогам.

Таблиця 2

Порівняльна характеристика методів виявлення вторгнень

Метод	Архітектура побудови	Аутентифікація	Маршрутизація	Джерело даних	Метод виявлення	Протокол маршрутизації	Середовище застосування	Спосіб побудови
Y. Zhang, W. Lee, Y. Huang	розподілена та об'єднана	ні	так	аудит (журнал подій)	аномалія	AODV, DSR, DSDV	моделювання	СВВ на агентах виявлення
P. Albers, O. Camp	розподілена та об'єднана	ні	ні	аудит (журнал подій)	зловживання , аномалія	-	моделювання	локальна СВВ на мобільних агентах
O. Kachirski, R. Guha	ієрархічна	ні	ні	аудит (журнал подій)	аномалія	-	моделювання	ієрархічна СВВ на мобільних агентах
D. Sterne	ієрархічна	ні	ні	аудит (журнал подій)	зловживання , аномалія	-	моделювання	ієрархічна модель для динамічності
B. Sun, K.Wu, U. Pooch	розподілена та об'єднана	ні	так	аудит (журнал подій)	аномалія	DSR	моделювання	на протоколах маршрутизації

Таким чином в найбільшій мірі представленим вимогам відповідають методи D. Sterne та B. Sun (та інші), які реалізовані для динамічної мережі, що має схильність до масштабування, побудована на протоколах маршрутизації та має технології прийняття рішень. Однак, запропоновані методи не реалізують можливість самонавчання щодо виявлення нових типів вторгнень та не пристосовані до застосування при непередбачуваній, нечіткій мережевій активності.

Висновки й перспективи подальших досліджень

Проведений аналіз показав, що існуючі методи в основному здатні вирішувати завдання з виявлення вторгнень у проводовій мережі або у стаціонарній радіомережі, що в свою чергу не задовольняє вказаним вище вимогам щодо застосування даних методів при побудові СВВ МР, а також не враховує особливості використання МР в тактичній ланці управління військами.

Враховуючи постійно змінювану природу атак, відсутність можливості концентрування трафіка МР в одній точці, а також мобільність елементів МР, динамічність топології та масштабованість, можливим рішенням може бути побудова інтелектуальних методів на основі комплексного застосування нечіткої логіки і нейронних мереж. При цьому основне завдання при розробці інтелектуальних методів полягає в можливості створення на їх основі СВВ здатних працювати з різнорідними типами трафіка великих об'ємів, розпізнавати нові типи атак, приймати рішення щодо забезпечення безпеки як в автономному режимі, так і у взаємодії з СВВ інших вузлів МР. Основними перевагами застосування зазначеного підходу є можливість швидкої адаптації СВВ до динамічних умов функціонування МР, а також можливість самонавчання що є важливим при роботі систем в режимі реального часу.

У ході подальших досліджень буде розроблена модель функціонування СВВ в МР класу MANET та методи виявлення вторгнень із застосуванням нечіткої логіки та нейронних мереж.

Література

1. Романюк В. А. Мобильні радіомережі – перспективи безпроводових технологій / Сети и телекоммуникации. – 2003. – № 12. – С. 62–68. **2. Міночкін А. І.,** Романюк В. А., Шаціло П. В. Виявлення атак в мобільних радіомереж / Збірник наукових праць № 1. – К.: ВІТІ НТУУ "КПІ". – 2005. – с. 102–111. **3. Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. / В.Ф. Шаньгин, Москва: ДМК Пресс, 2015. – 592 с. **4. Максим М.** Безопасность беспроводных сетей / пер. с англ. Семенова А. В. – М.: Компания АйТи; ДМК Пресс, 2004. – 288 с. **5. Владимиров А. А.** Wi–fi: "боевые" приемы взлома и защиты беспроводных сетей / А. Владимиров, В. Гавриленко, А. Михайловский; пер. с англ. А. А. Слинкина. М.: НТ Пресс, 2005. – 463 с. **6. Платонов В. В.** Программно–аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования / В. В. Платонов. – М.: издательский центр "Академия", 2013. – 336 с. **7. Лукацкий А.** Обнаружение атак: издательство БХВ / Санкт–Петербург, серия : "Мастер систем", 2003. – 596 с. **8. Макаренко С. И.** Информационная безопасность: учебное пособие / Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. **9. Гриняев С.** Системы обнаружения вторжений и реагирование на компьютерные инциденты на основе программ – агентов: Аналитический доклад / С. Гриняев, Москва: Центр стратегических оценок и прогнозов, 2005. – 46 с. **10. Ptacek T.,** Newsham T. Insertion, evasion, and denial of service: eluding network intrusion detection. Secure Networks, 2008. **11. Пролетарский А. В.,** Баскаков И. В., Чирков Д. Н. Беспроводные сети WI–FI / учебное пособие. – Москва: Интернет – университет информационных технологий, Бином. Лаборатория знаний , 2013. – 216 с. **12. Галицкий А. В.,** Рябко С. Д., Шангин В. Ф. Защита информации в сети – анализ технологий и синтез решений, – М.:ДМК Пресс, 2009. – 616 с. **13. Костров Д.** Системы обнаружения атак. – СПб.: БВХ–Петербург, 2008. **14. T. D. Garvey,** T. F. Lunt, Model–based Intrusion Detection / Proceeding of the 14 th Nation computer security conference, Baltimore, MD, October 1991. **15. J. Allen, A.** Christie, W. Fithen, J. McHuge, J. Pickel, E. Stoner, State of Practice of intrusion detection technologies / Technical Report CMU/SEI–99–TR–028. Carnegie Mellon Software Engineering Institute. 2000. **16. Y. Zhang,** W. Lee, and Y. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". Wireless Networks Journal (ACM WINET), 9(5): 545–556, 2003. **17. Y. Zhang,** W. Lee, "Intrusion detection in wireless ad–hoc networks", The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283, 2000. **18. P. Albers,** O. Camp, et al. "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches". Proceedings of the 1st International Workshop on Wireless Information Systems (WIS–2002), pp. 1–12, April 2002. **19. O. Kachirski,** R. Guha. "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks." Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2003 **20. D. Sterne,** P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs". In Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57–70, 2005. **21. B. Sun,** K.Wu, and 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), pp. 69–78, 2003. **22. C. Manikopoulos,** Li Ling: Architecture of the mobile adhoc network security (MANS) system, in: Proceedings of the IEEE. International Conference on Systems, Man and Cybernetics, vol. 4, October 2003, p. 312. **23. Y. Zhang,** W. Lee, Y. Huang : Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET. **24. K. Nadkarni,** A. Mishra: Intrusion detection in MANETs – the second wall of defense, in: Proceedings of the IEEE Industrial. Electronics Society Conference'2003, Roanoke, Virginia, USA, November 2–6, 2003, pp. 1235–1239. **25. N. Marchang,** R. Datta: Collaborative techniques for intrusion detection in mobile ad–hoc networks, 2007. .**26. M. Chatterjee,** S.K. Das, D. Turgut, WCA: a weighted clustering algorithm for mobile ad hoc networks, Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks) 5 (2002). pp. 193–204.

АНАЛИЗ МЕТОДОВ ОПРЕДЕЛЕНИЯ ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ КЛАССА MANET

[1]Сергей Васильевич Сальник

***[1]Олег Ярославович Сова** (канд. техн. наук, с.н.с.)*

***[2]Дмитрий Анатольевич Миночкин** (канд. техн. наук, с.н.с.)*

[1]Военный институт телекоммуникаций и информатизации Государственного университета телекоммуникаций, Киев, Украина

[2]Институт телекоммуникационных систем Национального технического университета Украины "Киевский Политехнический Институт", Киев, Украина

В статье проведен анализ существующих методов определения вторжений в мобильные радиосети, также произведена классификация методов определения вторжений. В ходе проведения анализа были рассмотрены виды применяемых атак на уровнях сетевой модели OSI. Также указаны архитектуры, на базе которых могут быть построены системы определения вторжений и определены требования к методам определения вторжений при их применении в мобильных радиосетях. Раскрыта классификация методов определения вторжений в мобильные радиосети и рассмотрены их основные направления. Проанализированы достоинства и недостатки указанных методов. Рассмотрены существующие авторские методы определения вторжений, в ходе чего определен перечень методов наиболее удовлетворяющих требованиям для применения в мобильных радиосетях. Предложены направления усовершенствования существующих методов с целью применения в сетях класса MANET и обеспечения безопасности информации, передающейся в них. Определены задания относительно дальнейших исследований, в которых будет разработан метод определения вторжений с применением нечеткой логики и нейронных сетей.

Ключевые слова: *мобильные радиосети; MANET; обеспечение безопасности информации; система определения вторжений; методы определения вторжений.*

METHODS ANALYSIS OF INTRUSION DETECTION IN MANET CLASS MOBILE RADIO NETWORKS

[1]Serhii V. Salnyk
[1]Oleh Y. Sova ***(Candidate of Technical Sciences, Senior Research Fellow)***
[2]Dmitro A. Minochkin ***(Candidate of Technical Sciences, Senior Research Fellow)***

[1]Militarv Institute of Telecommunications and Informatization of State Universitv of Telecommunications. Kviv. Ukraine
[2]Institute of Telecommunication Systems of National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine

The analysis of existing methods of mobile radio networks intrusion detection was performed in the article and classification of intrusion detection methods was produced. Types of applied network model OSI attacks were considered in the course of the analysis. Architectures which can be used as bases for building intrusion detection systems were specified and requirements for intrusion detection methods when applying them in mobile radio networks were defined. Classification of mobile radio networks intrusion detection methods was discovered and their main directions were observed. The advantages and disadvantages of these methods were analyzed. Existing proprietary methodology of intrusion detection were considered and method list which meets requirements for the applying in mobile radio networks was determined. Directions of existing methods improvement for using in MANET networks and security directions of transmitted information were suggested. Tasks of further research were defined.

Keywords: *mobile radio network; MANET; security information; system intrusion detection; methods of intrusion detection.*

References

1. Romanyuk V.A. (2003), The mobile radio network – wireless technology prospects. [*Mobilnyie radioseti – perspektivyi bezprovodnyih tehnologiy*], Seti i telekommunikatsii, Vol. 12, pp. 62–68. **2. Minochkin A.I.,** Romanyuk V.A., Shatsilo P.V. (2005), Attack detection in mobile radio networks. [*Viyavlennya atak v mobilnyih radiomerezhah*], Zbirnyik naukovih prats VITI NTUU "KPI", Vol. 1, pp. 102–111. **3. Shangin V.F.** (2015), Protection of information in computer systems and networks [*Zaschita informatsii v kompyuternyih sistemah i setyah*], Moscow, DMK Press, 592 p. **4. Maksim M.** (2004), Security for wireless networks. [*Bezopasnost besprovodnyih setey*], Moscow, Kompaniya AyTi; DMK Press, 288 p. **5. Vladimirov A.A.** (2005), Wi-fi: "fighting" techniques of hacking and wireless security". [*Wi–fi: "boevyie" priemyi vzloma i zaschityi besprovodnyih setey*], Moscow, NT Press, 463 p. **6. Platonov V.V.** (2013), Hardware and software data protection. [*Programmno–apparatnyie sredstva zaschityi informatsii*], Moscow, izdatelskiy tsentr "Akademiya", 336 p. **7. Lukatskiy A.** (2003), Attack detection. [*Obnaruzhenie atak*], BHV – Sankt–Peterburg, seriya "Master sistem", 596 p. **8. Makarenko S.I.** (2009), Information security: a training manual. [*Informatsionnaya bezopasnost: uchebnoe posobie*], SF MGGU im. M.A. Sholohova, 372 p. **9. Grinyaev S.** (2005), System intrusion detection and response for computer incidents based on software agents. [*Sistemyi obnaruzheniya vtorzheniy i reagirovanie na kompyuternyie intsidentyi na osnove programm–agentov*], Analiticheskiy doklad, Moscow, Tsentr strategicheskih otsenok i prognozov, pp. 46. **10. Ptacek T.,** Newsham T. (2008), [*Insertion, evasion, and denial of service: eluding network intrusion detection. Secure Networks*], 276 p. **11. Proletarskiy A.V.,** Baskakov I.V., Chirkov D.N. (2013), Wireless networks WI–FI. [*Besprovodnyie seti WI–FI*], uchebnoe posobie, Binom. Laboratoriya znaniy, 216 p. **12. Galitskiy A.V.,** Ryabko S.D., Shangin V.F. (2009), Information security in network analysis technologies and synthesis solutions. [*Zaschita informatsii v seti – analiz tehnologiy i sintez resheniy*], DMK Press, 616 p. **13. Kostrov D.** (2008), System intrusion detection. [*Sistemyi obnaruzheniya atak*], BVH-Peterburg, 357 p. **14. Garvey T.D.,** Lunt T.F., (1991), Model–based Intrusion Detection, Proceeding of the 14 th Nation computer security conference, Baltimore, MD. **15. Allen J.,** Christie A., Fithen W., McHuge J., J. Pickel, E**.** Stoner (2000), State of Practice of intrusion detection technologies, Technical Report CMU/SEI–99–TR–028. Carnegie Mellon Software Engineering Institute. **16. Zhang Y.,** Lee W., and Huang Y**.** (2003), Intrusion Detection Techniques for Mobile Wireless Networks,

Wireless Networks Journal (ACM WINET), № 9(5), pp. 545–556. **17. Y. Zhang,** W Lee, (2000), Intrusion detection in wireless ad–hoc networks, The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283. **18. P. Albers,** O. Camp, et al. (2002), Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches, Proceedings of the 1st International Workshop on Wireless Information Systems (WIS–2002), vol. April, pp. 1–12. **19. O. Kachirski,** R. Guha. (2003), Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE. **20. D. Sterne,** P. Balasubramanyam, et al. (2005), A General Cooperative Intrusion Detection Architecture for MANETs, In Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57–70. **21. B. Sun,** K.Wu, and U. W. Pooch. (2003), 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), pp. 69–78. **22. C. Manikopoulos,** Li Ling. (2003), Architecture of the mobile adhoc network security (MANS) system, Proceedings of the IEEE. International Conference on Systems, Man and Cybernetics, vol. 4, p. 312. **23. Y. Zhang,** W. Lee, Y. (2002), Huang : Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET. **24. K. Nadkarni,** A. Mishra (2003), Intrusion detection in MANETs – the second wall of defense, in: Proceedings of the IEEE Industrial, Electronics Society Conference, Roanoke, Virginia, USA, № November 2–6, pp. 1235–1239. **25. N. Marchang,** R. Datta (2007), Collaborative techniques for intrusion detection in mobile ad–hoc networks. **26. M. Chatterjee,** S.K. Das, D. Turgut, (2002), WCA: a weighted clustering algorithm for mobile ad hoc networks**,** Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks), vol. 5, pp. 193–204.

Отримано: 03.02.2015 року