УДК 621.391

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

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

АТАКИ ПРИ ПРОВЕДЕННІ ВТОРГНЕНЬ У МОБІЛЬНІ РАДІОМЕРЕЖІ КЛАСУ MANET

В статті проведено аналіз існуючих атак, які застосовуються для вторгнень в мобільні радіомережі класу MANET. Здійснено класифікацію категорій та типів вторгнень, а також з'ясовано варіанти їх впливу на мобільну радіомережу на різних рівнях мережевої моделі OSI. Розглянуто можливість використання відомих вторгнень в процесі навчання на основі навчальної множини вторгнень та при побудові методів виявлення вторгнень. Також було розглянуто перелік параметрів, якими характеризуються вторгнення в мобільну радіомережу. Визначено перелік вимог до методів виявлення вторгнень для застосування їх у мобільній радіомережі. Наведена порівняльна характеристика використовуємих на сьогоднішній день методів виявлення вторгнень. З метою забезпечення безпеки мережі запропоновано напрями побудови сучасних методів виявлення вторгнень у мобільних радіомережах на основі нейронних мереж при використанні в умовах нечіткої мережевої активності. Також було визначено напрям подальший досліджень.

Ключові слова: *забезпечення безпеки мобільної радіомережі; MANET; система виявлення вторгнень; вторгнення в мережу; атака.*

Вступ

Постановка проблеми. Актуальність дослідження. В останні десятиліття мобільні радіомережі (МР) 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 на різних рівнях мережевої моделі OSI (*Open Systems Interconnection*). Зазначені вразливості можуть бути використані противником для здійснення вторгнень у МР з метою порушення цілісності інформації, яка передається в МР, або для 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).

В даній статті ми обмежимося розглядом типів атак, які найчастіше використовуються супротивником, та параметрів цих атак, які застосовуються в процесі навчання МВВ.

Метою статті є аналіз існуючих атак при проведенні вторгнень у МР для застосування їх в проведенні навчання МВВ.

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

Предметом дослідження є атаки противника на МР, які використовуються при проведенні вторгнень.

Виклад основного матеріалу дослідження

Аналіз предметної області. Під вторгненням розуміється несанкціонований вхід в інформаційно-комунікаційну систему, в результаті дій, що порушують політику безпеки або обходять систему захисту [3]. Метою даних дій є порушення цілісності, конфіденційності та доступності даних, які передаються в системі [4].

Питання захисту будь-якої інформаційно-комунікаційної системи, в тому числі МР, від вторгнень являє собою задачу, забезпечення якої покладається на МВВ. В наслідок чого при побудові МВВ необхідно враховувати широкий спектр атак, які здатні впливати на МР практично на всіх рівнях мережевої моделі OSI. Робота даних методів вивчалася багатьма дослідниками та описана в [1–16].

На відміну від стаціонарних мереж, середовищем передачі інформації в МР є радіоканал, а елементами МР є мобільні вузли, які можуть взаємодіяти як між собою, так і з вузлами

стаціонарної мережевої інфраструктури. У зв'язку з цим, з одного боку, кількість варіантів здійснення вторгнень (атак) у МР суттєво збільшується в порівнянні з проводовими мережами, а з іншого боку, практично весь спектр атак які застосовуються з метою впливу на проводові мережі може бути застосований у МР [2, 11].

На підставі вказаного доцільно визначити перелік вимог до МВВ, з метою їх застосування у МР тактичної ланки управління. До даного переліку віднесемо: високу точність виявлення вторгнень; застосування в мобільному середовищі; можливість самонавчання; можливість виявлення нових вторгнень; мінімальне використання вузлових та мережевих ресурсів (енергетичних, обчислювальних та ін.); робота в умовах нечіткої мережевої активності; функціонування в режимі реального часу та ін.

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 та відносяться до різних рівнів мережевої моделі OSI. До об`єктів проведення вторгнень (атак) відносяться: управління передачею даних; обмін пакетами; організацію з'єднань; програмні, технічні, енергетичні характеристики засобів зв'язку; управління інформацією або вузлом та інше.

Виходячи з вказаного, вплив атаки на МР здійснюється у відповідності з метою проведення вторгненні та на основі функціональних можливостей атак. Відповідно до своїх характеристик та можливостей, атаки у МР поділяються на 4 категорії [6,11]. Кожна з категорій має множину типів атак, які використовуючи свої функціональні можливості по різному впливають на МР.

Метою здійснення вторгнення у МР може бути комплекс дій, якій складається з декількох етапів. На першому етапі – проникнення до програмного або інформаційного ресурсу мережі з метою впливу на них. На другому етапі – вплив на апаратну частину мережі (зміну маршрутної таблиці, протоколів маршрутизації, вплив на енергосистему або систему безпеки тощо).

Тому з метою з`ясування видів впливу категорій та типів атак на мережу розглянемо склад категорій:

1. *DoS* атаки – це мережеві атаки, спрямовані на виникнення ситуацій, коли у системі, що піддається вторгненню, відбувається відмова в обслуговуванні. Вказані атаки характеризуються генерацією великого об`єму трафіка, що призводить до перенавантаження та блокування сервера. До найбільш відомих типів DoS атак відносять:

– *Back* атака – дозволяє віддалено керувати вузлом за допомогою графічного інтерфейсу. Атака може бути реалізована для генерації мережевого трафіка. Здійснює вплив на працездатність процесора, у наслідок чого тривалість обробки даних збільшується, що в свою чергу впливає на системи життєдіяльності вузла. Атака використовує протокол HTTP який призначений для передачі довільних даних.

– *Land* атака – полягає в передачі на відкритий порт вузла жертви TCP-пакетів з встановленням мітки SYN, причому вихідний адрес та порт такого пакету співпадають з адресою та портом атакуємого вузла. Це призводить до намагання жертви встановити з`єднання із собою, що провокує завантаження процесору, втрату енергоресурсу, помилки мережі. Дана атака ефективна для використання у маршрутизаторах, так як може вивести із ладу всю мережу. Атака використовує протоколи TCP/IP, HTTP які призначені для передачі довільних даних та обміну повідомленнями.

– *Neptune* атака – направлена на моніторинг мережевого трафіка або вплив на нього. Також атака проводить відмову в обслуговуванні портів. Атака використовує протокол TCP який призначений для управління передачею даних в мережах та під мережах TCP/IP.

– *Pod* атака – тип мережевої атаки при якій вузол-жертва отримує підроблені запити направлені на вузол, після чого вузол перевантажується та перестає відповідати на них. Атака також здійснює направлення зміщеної фрагментації пакетів на вузол, що провокує помилки та зупинку передачі даних. Атака використовує протоколи TCP, ICMP, які призначені для управління передачею даних в мережах та під мережах TCP/IP, а також передачі повідомлень про похибки та інші непланові ситуації які виникають при передачі даних.

– *Smurf* атака полягає в передачі в мережу запитів від імені вузла – жертви. В наслідок чого вузли отримувачі відповідають відправнику, тим самим аналізується трафік повідомлень та відбувається зменшення пропускної здатності каналу зв`язку жертви, що призводить до ізоляції вузла. Атака використовує протокол ICMP який призначений для передачі повідомлень про похибки та інші непланові ситуації, які виникають при передачі даних.

– *Teardrop* атака впливає на порядок перегрупування фрагментів пакетів, або встановлення пробілів у фрагментах, що може призвести до помилок при отриманні даних. Атака може завантажувати стек протоколів фрагментами з дублюючими друг друга полями, що уповільнює роботу мережі або призводить до збоїв у роботі. Атака використовує протокол TCP/IP, які призначені для обміну повідомленнями.

2. *U2R* атаки – пропонують отримання зареєстрованим користувачам привілей локального суперкористувача (мережевого адміністратора). Дані атаки представлені наступними типами:

– *Buffer_overflow* – програма, яка для прориву в інформаційну систему вузла та отримання

привілей суперкористувача використовує неточність в контролі розмірів строк та буферів. Здійснює переповнення буферу.

– *Loadmodule* – атака проводиться для отримання контролю над мережею. Розрахована на погану захищеність системи.

– *Perl* – програма, яка використовує вразливості у програмному забезпеченні та застосовується для проведення атак на обчислювальну систему вузла, сервісні або клієнтські додатки, модулі операційної системи. Метою атаки може бути захват контролю над системою та порушення її функціонування.

– *Rootkit* – набір програмних засобів для забезпечення: маркування об`єктів (процесів, файлів, директорій); контролю подій, які відбуваються в системі або вузлі; збору даних щодо параметрів системи; приховування слідів противника в мережі шляхом модифікації стека протоколів TCP/IP. Атака використовує протоколи обміну даними API, TCP/IP, які призначені для обміну повідомленнями та виклику функцій сервісу.

3. *R2L* атаки, характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяються на:

– *Ftp_write* – сервіс для створення підроблених файлів для записів у каталогах даних. Противник завдяки цьому здатен віддалено відкривати систему та керувати нею не вводячи ідентифікуючих паролів. Сервіс використовує протокол FTP, який призначений для передачі файлів по TCP мережам.

– *Guess_passwd* – програма призначена для взлому веб-сайтів, та повідомлень. Взлом та взяття під контроль системи відбувається в наслідок проведення підбору логінів та паролів. Після взлому програма поширює шкідливі програми, спам, фішинг тощо. Програма використовує протоколи Telnet, Rlogin, які призначені для реалізації текстового інтерфейсу.

– *Imap* атака – за допомогою влаштованих помилок дозволяє отримувати повідомлення з поштового серверу, в наслідок чого встановлюється віддалений контроль над системою та вузлом. Атака використовує протоколи Imap та TCP які призначені для доступу до повідомлень.

– *multihopp* – багатоступенева атака, призначена для отримання доступу з боку віддаленої станції. Вона призначена для обміну маршрутної інформацією між доменами мережі. Впливає на формування маршрутів мережі та контролює час життя пакетів інформації. Атака використовує протокол динамічної маршрутизації BGP, який призначений для обміну інформацією про зв`язність між автономними підсистемами.

– *Phf* атака – призначена для отримання файлів, паролів, віддаленого підбору паролів та інше. Програма використовує протокол HTTP який використовується для передачі довільних даних.

– *Spy* програма – для віддаленого спостереження за вузлом, перехоплення пакетів, сканування та керування вузлом. Атака також змінює записи реєстру, змінює налаштування та розповсюджує шкідливі повідомлення. Програма використовує протокол FTP, який призначений для передачі файлів по TCP мережам.

– *Warezclient* представляє собою програму для здійснення локальних атак в мережі. Програма впливає на порядок передачі файлів, також здійснює заборону користувачеві системи робити записи на FTP-сервері. Програма використовує протокол FTP, який призначений для передачі файлів по TCP мережам.

– *warezmaster* атака – обмежує можливість завантаження файлів, пакетів та обмежує користування власною системою. Також атака надає можливості віддаленому користувачу завантажувати паролі та мати доступ до інформації. Програма використовує протокол FTP, який призначений для передачі файлів по TCP мережам.

4. *Probe*-атаки – полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. Найбільш часто застосовані типи *Probe*-атак на МР:

– *Ipsweep* атака – полягає у підміні одної IP-адреси на іншу, використовуючи зловживання. Також атака здійснює відправку пакетів – запитів різним адресатам під час певного часу, тим самим компрометує свій вузол. Використовує протоколи IP, ICMP, які призначені для доставки пакетів між вузлами мережі, передачі повідомлень про похибки та інші непланові ситуації, які виникають при передачі даних.

– *Nmap* – програма для сканування та аналізу мережі, яка в скритому режимі використовуючи зловживання, ідентифікує віддалені операційні системи та вузли. Програма використовує протокол IP, який призначений для забезпечення доставки пакетів між вузлами мережі.

– *Portsweep* атаки – використовуючи зловживання, визначають експлуатовані канали зв`язку на віддалених вузлах шляхом направлення з`єднання декільком портам TCP. Атака використовує протоколи IP, TCP, які призначені для управління передачею даних в мережах, під мережах TCP/IP та для забезпечення доставки пакетів між вузлами мережі.

– *Satan* – програма для пошуку вразливостей власної підмережі з метою передачі даних противнику. Програма використовує протоколи IP, FTP, які призначені для забезпечення доставки пакетів між вузлами мережі та передачі файлів по TCP мережам.

Враховуючі перераховану класифікацію атак та її вплив на мережу слід зазначити, що існуючі МВВ, передбачають прийняття рішень, щодо

виявлення вторгнень на основі навчання. Процес навчання відбувається на основі навчальної множини вторгнень (атак). В якості навчальної множини існуючі МВВ використовують конкретні різновиди вторгнень, які представлені в базі даних (БД) KDD-99 [7]. Ця БД налічує близько 5000000 відомостей щодо аномальних з`єднань та близько 1000000 відомостей про нормальний тип з`єднання.

Варіантом підбору навчальної множини атак можуть бути види нормальної поведінки та види аномальної поведінки до яких входять розглянуті у [8, 9] та статті типи атак. Так як кожен тип атак характеризує множину цілей при проведенні вторгнень у МР, дії яких направлені на відповідні рівні мережевої моделі OSI, то при проведенні навчання кожному типу атаки присвоюється терма, що характеризує вплив атак на рівнях мережевої моделі OSI (табл. 1).

Після проведення навчання МВВ відбувається включення його в роботу у складі системи виявлення вторгнень (СВВ). Робота СВВ характеризується направленням вхідного трафіка до МВВ з метою його аналізу на предмет виявлення вторгнень.

Таблиця 1

Вплив атак на МР за рівнями мережевої моделі OSI

Категорії атак	Типи атак	Рівні мережевої моделі OSI				
		Прикладний	Транспортний	Мережевий	Канальний	Фізичний
DoS	*back*	+	+	+	+	+
	land	+	+	+	+	+
	neptune		+	+		
	pod		+	+	+	+
	smurf			+	+	+
	teardrop	+	+	+	+	+
U2R	*buffer_ overflow*		+	+		+
	loadmodule		+	+		+
	perl	+	+	+		+
	rootkit	+	+	+	+	
R2L	*ftp_write*	+			+	
	guess_passwd	+	+		+	
	imap	+	+		+	
	multihop	+		+		+
	phf	+	+			
	spy	+			+	
	warezclient	+			+	+
	warezmaster	+				+
Probe	*ipsweep*			+	+	
	nmap			+	+	
	portsweep		+	+		
	satan	+		+		

Отже при вході трафіка до СВВ кожному потоку даних надається запис, який являє собою образ вхідного мережевого з`єднання. Даний запис включає в себе 41 параметр мережевого трафіка (табл. 2), який містить у собі символьні, логічні та числові ознаки. У загальному вигляді ознаки містять інформацію про: тривалість з'єднання, тип протоколу, кількість спроб реєстрації тощо [10].

Параметри трафіка, під час проходження МВВ, аналізуються та кластеризуються внаслідок чого відбувається перевірка на наявність заборонених з'єднань, та маркування цих з`єднань як „вторгнення" або „не вторгнення".

Запис маркування складається з 42 полів. Перші 41 поле описує ознаки мережевого трафіка, а останнє 42-е поле вказує на тип трафіка, який аналізується. Вказане 42-е поле може приймати значення „*normal*", якщо дане мережеве з`єднання відноситься до нормального стану трафіка, або найменування типу вторгнення (наприклад, „*smurf*"). У результаті на виході МВВ, у разі виявлення конкретної атаки буде з`являтися відповідне значення, щодо виявлення впізнаного вторгнення, його класифікації та пропозицій для підсистеми реалізації рішень (на основі присвоєної характеристичної терми) відносно варіантів реагування на виявлене вторгнення.

Таблиця 2

Параметри мережевого трафіка

№ з/п	Параметр	Опис
1.	*duration*	Тривалість (у секундах) з'єднання
2.	*protocol_type*	Тип протоколу (TCP, UDP, etc.)
3.	*service*	Атакований сервіс
4.	*src_bytes*	Кількість байтів від джерела до призначення
5.	*dst_bytes*	Кількість байтів відповіді клієнту
6.	*flag*	Прапорці з'єднання
7.	*land*	1, якщо з'єднання від/до того самого хоста/порта
8.	*wrong_fragment*	Кількість „хибних" фрагментів
9.	*urgent*	Кількість термінових пакетів
10.	*hot*	Кількість „гарячих" індикаторів
11.	*num_failed_logins*	Кількість невдалих спроб реєстрації
12.	*logged_in*	1, якщо успішний вхід в систему; 0 неуспішне
13.	*num_compromised*	Кількість „компроментуючих" умов
14.	*root_shell*	1, якщо root shell отриманий; інакше 0
15.	*su_attempted*	1, якщо виконувалась„su root" ; інакше 0
16.	*num_root*	Кількість „root" доступів
17.	*num_file_creations*	Кількість операцій створення файлів
18.	*num_shells*	Кількість запитів на надання оболонки
19.	*num_access_files*	Кількість операцій на доступ до контролю файлів
20.	*num_outbound_cmds*	Кількість вихідних команд для FTP сесії
21.	*is_hot_login*	1, якщо логін належав до „гарячого" списку
22.	*is_guest_login*	1, якщо „гостьовий" вхід
23.	*count*	Кількість з'єднань на хост в поточній сесії за останні 2с.
24.	*serror_rate*	% з'єднань що мали „SYN" помилки
25.	*rerror_rate*	% з'єднань що мали „REJ" помилки
26.	*same_srv_rate*	% з'єднань що мали однаковий сервіс
27.	*diff_srv_rate*	% з'єднань на різні сервіси
28.	*srv_count*	Кількість з'єднань на такий самий сервіс за останні 2с.
29.	*srv_serror_rate*	% з'єднання з помилкою в „SYN" пакеті
30.	*srv_rerror_rate*	% з'єднання, що мають „REJ" помилки
31.	*srv_diff_host_rate*	% з'єднання від інших хостів
32.	*dst_host_count*	Кількість з`єднань до локального хоста, встановлених віддаленою стороною
33.	*dst_host_srv_count*	Кількість з`єднань до локального хоста, встановлених віддаленою стороною та використовуючих одну службу
34.	*dst_host_same_srv_rate*	% з`єднань до локального хоста, встановлених віддаленою стороною та використовуючих одну службу
35.	*dst_host_diff_srv_rate*	% з`єднань до локального хоста, встановлених віддаленою стороною та використовуючих різні служби
36.	*dst_host_same_src_port_rate*	% з`єднань до даного хоста при поточному номері порту джерела
37.	*dst_host_srv_diff_host_rate*	% з`єднань до служби різних хостів
38.	*dst_host_serror_rate*	% з`єднань з помилкою типу SYN для даного хост-приймача
39.	*dst_host_srv_serror_rate*	% з`єднань з помилкою типу SYN для даної служби приймача
40.	*dst_host_rerror_rate*	% з`єднань з помилкою типу REJ для даного хост-приймача
41.	*dst_host_srv_rerror_rate*	% з`єднань з помилкою типу REJ для даної служби приймача

Використовуючи множину типів атак у якості навчальної вибірки та принцип пошуку вторгнень на основі параметрів мережевого трафіка, існує цілий ряд розроблених МВВ. Однак представлені на сьогоднішній день методи не враховують вимоги щодо їх застосування у МР тактичної ланки управління військами (ТЛУВ).

У табл. 3 наведена порівняльна характеристика використовуємих на сьогоднішній день МВВ, для проводових (стаціонарних) мереж та МР, що дозволяє визначити їх відповідність зазначеним вимогам для застосування у ТЛУВ.

Таблиця 3

Порівняльна характеристика методів виявлення вторгнень

№ п/п	Метод	Вид середовища	Математичний апарат	Робота при нечіткості	База даних	К-ть вхідних параметрів	Пошук вторгнень та нормальної поведінки, %	Пошук нових вторгнень
1	Y. Yang, D. Jiang, M. Xia [12]	Проводове, стаціонарне	Ієрархічна самоорганізуюча карта	-	KDD-99	41	Norm- 96,4 DoS-96,2 U2R-37,1 R2L-43,1 Probe-94,3	-
2	H.F.Eid, A.Darwis, A.E.Hassanien, A.Abraham [13]	Проводове, стаціонарне	Метод опорних векторів	-	KDD-99	41	Norm-99,8 DoS-97,5 U2R-86,6 R2L-81,3 Probe-92,8	-
3	М.П. Комар, Д.І. Боднар, А.О. Саченко [10]	Проводове, стаціонарне	Нейрон Kohonen	-	KDD-99	41	Norm- - DoS-98 U2R-30,8 R2L-36,5 Probe-92,8	-
4	H.Alipour, E.Khosrowsh, M.Esmaeili, M.Nourhossein [14]	Мобільна радіомережа	Нейроний класифікатор	-	KDD-99	41	Norm-98,5 DoS-98,5 U2R-76,3 R2L-89 Probe-82,5	-
5	W. Sharafat, R. Naoum [15]	Мобільна радіомережа	Генетичний нейронний алгоритм	+	KDD-99	41	Norm-96,3 DoS-97,3 U2R-29,8 R2L-9,6 Probe-88,7	-
6	MS. Abadeh, J. Habibi [16]	Мобільна радіомережа	Гібридна нейрона мережа	+	KDD-99	41	Norm-96 DoS-98,8 U2R-72,8 R2L-33,45 Probe-86,2	-

Як зазначалося, основна класифікаційна ознака МВВ полягає у їх відношенні до виду середовища, в якому відбувається передача інформації. Тому, з метою з`ясування принципів побудови та функціональних можливостей МВВ, розглянемо методи призначені для проводових (стаціонарних) та безпроводових мереж, які використовують однакову базу даних KDD-99 для проведення навчання методу та однакову кількість вхідних параметрів трафіка, на основі яких відбувається пошук вторгнень.

1. Метод, запропонований Y. Yang, D. Jiang, M. Xia [12], призначений для використання у проводових (стаціонарних) мережах. У якості математичного апарату метод застосовує ієрархічну самоорганізуючу карту. Даний метод здійснює пошук вторгнень та класифікує типи нормальної поведінки. До недоліків методу відноситься: неможливість використання при нечіткій мережевій активності; не пристосованість до самонавчання та пошуку нових типів вторгнень.

2. Запропонований H.F. Eid, A. Darwis, A.E. Hassanien, A. Abraham [13], МВВ призначений для використання у проводових (стаціонарних) мережах. У якості математичного апарату метод застосовує – метод опорних векторів. Запропонований метод здійснює пошук вторгнень та класифікує типи нормальної поведінки. До недоліків методу відноситься: неможливість використання при нечіткій мережевій активності; не пристосованість до самонавчання та пошуку нових типів вторгнень.

3. Метод що запропонований М.П. Комар, Д.І. Боднар, А.О. Саченко [10], призначений для використання у проводових (стаціонарних) мережах. У якості математичного апарату метод застосовує нейронну мережу Кохонена. Запропонований метод здійснює пошук вторгнень. До недоліків методу відноситься: неможливість використання при нечіткій мережевій активності; не пристосованість до самонавчання, пошуку нових типів вторгнень та класифікації типів нормальної поведінки.

4. H. Alipour, E. Khosrowsh, M. Esmaeili, M. Nourhossein [14], запропонували метод призначений для використання у безпроводових мережах. У якості математичного апарату метод застосовує нейронний класифікатор. Даний метод здійснює пошук вторгнень та класифікує типи нормальної поведінки. До недоліків методу відноситься: неможливість використання при нечіткій мережевій активності; не пристосованість до самонавчання та пошуку нових типів вторгнень.

5. Запропонований W. Sharafat, R. Naoum [15], МВВ призначений для використання у

безпроводових мережах, даний метод може бути застосований при нечіткій мережевій активності, отриманні неточних та неповних вхідних даних. У якості математичного апарату метод застосовує генетичний нейронний алгоритм. Запропонований метод здійснює пошук вторгнень та класифікує типи нормальної поведінки. У зв'язку з особливостями функціонування у МР, запропонований метод характеризуються низькою точністю виявлення вторгнень. Також до недоліків методу відноситься: не пристосованість до самонавчання та пошуку нових типів вторгнень.

6. Метод, запропонований MS. Abadeh, J. Habibi [16], призначений для використання у безпроводових мережах, як і попередній метод також враховує можливості використання при нечіткій мережевій активності. У якості математичного апарату метод застосовує гібридну нейронну мережу. Запропонований метод здійснює пошук вторгнень та класифікує типи нормальної поведінки. До недоліків методу відноситься: не пристосованість до самонавчання та пошуку нових типів вторгнень; низька точність виявлення вторгнень.

Як видно з вказаного: проводові (стаціонарні) МВВ за своїми функціональними можливостями не можуть бути застосовані в МР, але вони мають більшу точність виявлення вторгнень. В свою чергу безпроводові МВВ можуть бути використані в МР, деякі з них здатні працювати при нечіткій мережевій активності, однак мають низьку точність виявлення вторгнень в порівнянні з стаціонарними МВВ.

Таким чином, з метою використання МВВ в МР класу MANET, та з урахуванням вимог висуваємих до МВВ, для застосування в МР, в найбільшій мірі відповідають розглянуті методи (5, 6), які реалізовані для мобільної радіомережі та враховують можливість застосування при неточності, неповноті вхідних даних та нечіткій мережевій активності. Однак, запропоновані методи не реалізують можливість самонавчання, виявлення нових типів вторгнень та характеризуються не високою точністю виявлення вторгнень.

Висновки й перспективи подальших досліджень

Проведений аналіз методів виявлення вторгнень показав, що вони здатні вирішувати покладені на них завдання у проводових або безпроводових мережах зв'язку. Однак, існуючі методи не враховують особливостей функціонування МР класу MANET, що призводить до неможливості їх використання для побудови систем виявлення вторгнень в радіомережі даного класу.

Тому враховуючи вказане, можливим рішенням, щодо виконання висунутих вимог по побудові МВВ може бути, використання методів на основі нейронних мереж з використанням при нечіткій мережевій активності. Це дозволить підвищити точність виявлення вторгнень та забезпечить виявлення вторгнень в МР, в режимі реального часу.

У ході подальших досліджень буде розроблено метод виявлення вторгнень на основі нейронних мереж, а також буде проведене моделювання можливих загроз противника при вторгненні в МР класу MANET.

Література

1. Романюк В. А. Мобильные радиосети - перспективы беспроводных технологий / Сети и телекоммуникации, 2003. № 12. С. 62-68. **2. Міночкін А. І.,** Романюк В. А., Шацило П. В. Виявлення атак в мобільних радіомережах / Збірник наукових праць № 1. – К.: ВІТІ НТУУ "КПІ", 2005. С. 102-111. **3. 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. **4. 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. **5. Сальник С. В.**, Сова О. Я., Міночкін Д. А. Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET // науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони" № 1(22)2015 – К.: Національний університет оборони України імені Івана Черняховського, 2015. С. 103-112. **6. Лукацкий А. В.** Обнаружение атак. 2-е изд., – СПб.: БХВ-Петербург, 2003. **7. KDD Cup 1999 Data** / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999. **8. S. Akbar**, K.Nageswara Rao, J.A.Chandulal. "Intrusion Detection System Methodologies Based on Data Analysis." International Journal of Computer Applications (0975 – 8887), Volume 5– No.2, August 2010. **9. Васильев В. И.**, Шарабыров И. В., Обнаружение атак в локальных беспроводных сетях на основе интеллектуального анализа даннях / Известия ЮФУ. 2012. С. 57-66. **10. Комар М. П.**, Боднар Д. І., Саченко А. О. Інтелектуалізована інформаційна технологія виявлення комп'ютерних атак / Вимірювальна та обчислювальна техніка в технологічних процесах. 2010. – № 2. С. 133-137. **11. Меріт М.**, Полино Д. Безопасность беспроводных сетей. – М.: ДМК Пресс, 2004, 288 с. **12. Yahui Yang**, Dianbo Jiang, Min Xia Using Improved GHSOM for Intrusion Detection, Journal of Information Assurance and Security 5, 2010, 232-239. **13. Heba F. Eid**, Ashraf Darwish, Aboul Ella Hassanien, Ajith Abraham, Principle Components Analysis and Support Vector Machine based Intrusion Detection System, 10th International Conference on Intelligent Systems Design and Applications, 2010, 363-367. **14. H. Alipour**, E. Khosrowshahi, M. Esmaeili, M. Nourhossein. ACOFCR: applying ACO-based algorithms to induct FCR. In: Proceedings of the World Congress on Engineering (IWCE), 2008, 12-17. **15. W. S. Sharafat**, R. Naoum, Development of Genetic-based Machine Learning for Network Intrusion Detection GBML-NID).World Academy of Science, Engineering and Technology, 2009, pp. 20-24. **16. MS. Abadeh**, J. Habibi, A hybridization of evolutionary fuzzy systems and ant colony optimization for intrusion detection. The ISC International Journal of Information Security 2010, 2(1):33-46.

АТАКИ ПРИ ПРОВЕДЕНИИ ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ КЛАССА MANET

[1]Сальник Сергей Васильевич
[1]Сова Олег Ярославович (канд. техн. наук, с.н.с.)
[1]Сальник Владимир Васильевич
[2]Миночкин Дмитрий Анатольевич (канд. техн. наук, с.н.с.)
[1]Военный институт телекоммуникаций и информатизации, Киев, Украина

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

В статье проведен анализ существующих атак, которые применяются для вторжений в мобильные радиосети класса MANET. Осуществлено классификацию категорий и типов вторжений, а также установлены варианты их влияния на мобильную радиосеть на разных уровнях сетевой модели OSI. Рассмотрена возможность использования известных вторжений в процессе обучения на основе обучающего множества вторжений и при построении методов обнаружения вторжений. Также был рассмотрен перечень параметров, которыми характеризуются вторжения в мобильную радиосеть. Определен перечень требований к методам обнаружения вторжений для применения их в мобильной радиосети. Приведена сравнительная характеристика используемых на сегодняшний день методов обнаружения вторжений. С целью обеспечения безопасности сети, предложены направления построения современных методов обнаружения вторжений в мобильных радиосетях на основе нейронных сетей при использовании в условиях нечеткой сетевой активности. Также было определено направление дальнейших исследований.

Ключевые слова: *обеспечение безопасности мобильной радиосети; MANET; система обнаружения вторжений; вторжение в сеть, атака.*

ATTACKS DURING INTRUSION REALIZATION IN THE MANET MOBILE RADIONETWORKS

Serhii V. Salnyk
Oleh Y. Sova *(Candidate of Technical Sciences, Senior Research Fellow)*
Volodymyr V. Salnyk
Dmytro A. Minochkin *(Candidate of Technical Sciences, Senior Research Fellow)*

[1]Military institute of telecommunications and information, Kyiv, Ukraine
[2]Institute of telecommunication systems National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine

In the article the analysis of existent attacks is conducted which are used for intrusion in the MANET. Classification of category and types of intrusions, also the variants of their influence are found out on a mobile radio network on the different levels of network model of OSI is realized. Possibility of the intrusions is considered during organization of studies on the basis of teaching great number intrusions and construction methods of detection intrusions. The list of parameters that intrusions are characterized in a mobile radio network are also considered. The list of requirements to methods of detection of intrusions for their application in a mobile radio network is defined. Directions of construction modern methods of finding out intrusions offer in mobile radio networks on the basis of neural networks at the use in the conditions of unclear network activity with the purpose providing of safety network are proposed. The direction of further researches is also determined.

Keywords: *security mobile radio network; system of detection of invasions; invasion into a network; attack.*

References

1. Romanyuk V.A. (2003), The mobile radio network - wireless technology prospects. [*Mobilnyie radioseti – perspektivyi bezprovodnyih tehnologiy*], Seti i telekommunikatsii, No 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", No 1 pp. 102–111. **3. Platonov V.V.** (2013), Hardware and software data protection. [*Programmno - apparatnyie sredstva zaschityi informatsii*], Moscow: izdatelskiy tsentr "Akademiya", 336 p. **4. 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. **5. Salnik S.V., Sova O.Y., Minochkin D.A.** Analysis methods for intrusion detection in mobile radio class MANET [*Analiz metodov obnaruzheniya vtorzheniy v mobil'nyye radioseti klassa MANET*], nauchnyy zhurnal "Sovremennyye informatsionnyye tekhnologii v sfere bezopasnosti i oborony " No 1 (22) 2015, Moscow: Natsional'nyy universitet oborony Ukrainy , 2015 pp. 103-112. **6. Lukatskiy A.V,** (2003) Attack detection. [*Obnaruzhenie atak*], 2nd edition, SPb.: BHV Peterburg.. **7. KDD Cup 1999 Data** / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999. **8. S. Akbar,** K.Nageswara Rao, J.A.Chandulal**.** (2010) "Intrusion Detection System Methodologies Based on Data Analysis." International Journal of Computer Applications (0975 – 8887), Volume 5, No.2. **9. Vasilyev V.I.,** Sarabyrov I.V., (2012) attack detection in wireless local area networks based on data mining, Izvestiya YuFU. pp. 57-66. **10. Komar M. P.,** Bodnar D. I., Sachenko A.O. (2010) Intelligent information technology of exposure of computer attacks VimIryuvalna ta obchislyuvalna tehnIka v tehnologIchnih protsesah. No 2. pp. 133-137. **11. Merit M.**, Polino D. (2004) Wireless Security. [*Bezopasnost besprovodnyih setey*], Moscow: DMK Press, p 288. **12. Yahui Yang,** Dianbo Jiang, Min Xia (2010) Using Improved GHSOM for Intrusion Detection, Journal of Information Assurance and Security 5, pp. 232-239. **13. Heba F. Eid,** Ashraf Darwish, Aboul Ella Hassanien, Ajith Abraham (2010) Principle Components Analysis and Support Vector Machine based Intrusion Detection System, 10th International Conference on Intelligent Systems Design and Applications, pp. 363-367. **14. H. Alipour,** E. Khosrowshahi, M. Esmaeili, M. Nourhossein. (2008) ACOFCR: applying ACO-based algorithms to induct FCR. In: Proceedings of the World Congress on Engineering (IWCE), pp. 12-17. **15. W. S. Sharafat**, R. Naoum, (2009) Development of Genetic-based Machine Learning for Network Intrusion Detection GBML-NID).World Academy of Science, Engineering and Technology, pp. 20-24. **16. MS. Abadeh**, J. Habibi**,** (2010) A hybridization of evolutionary fuzzy systems and ant colony optimization for intrusion detection. The ISC International Journal of Information Security, No 2(1), pp. 33-46.

Отримано: 14.10.2015 року