УДК 621.391

С.В. Сальник, В.В. Сальник, О.А. Симоненко, О.Я. Сова

Військовий інститут телекомунікацій та інформатизації, Київ

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ В МОБІЛЬНІ РАДІОМЕРЕЖІ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ

В статті представлено удосконалений нейромережевий метод виявлення вторгнень в мобільні радіомережі класу MANET, в основі якого знаходиться існуючий метод виявлення вторгнень у стаціонарних комп'ютерних мережах з використанням нейронної мережі Кохонена. Удосконалення полягає в зменшенні кількості нейромережевих аналізаторів, структурній зміні роботи нейромережевих аналізаторів з послідовної на паралельну, що забезпечило роботу методу в режимі реального часу. З метою покращення можливостей конкурування та навчання нейронної мережі Кохонена, впроваджено проведення підрахунку потенціалу кожного нейрона мережі та підрахунок похибки мережі. Проведено експериментальні дослідження та з`ясовано рівень виявлення вторгнень розробленим методом.

Ключові слова: *мобільні радіомережі, MANET, забезпечення безпеки мобільної радіомережі, метод виявлення вторгнень, мережа Кохонена.*

Вступ

Актуальність дослідження. В останнє десятиліття спостерігається стрімкий розвиток та поширення мобільних радіомереж (МР) або радіомереж класу MANET [1], які стають все більш вживаними як у повсякденному житті, так і у військовій галузі, особливо в тактичній ланці управління військами. Основними особливостями побудови та застосування МР є: мобільність усіх вузлів; динамічна топологія; децентралізоване управління МР; спільний доступ вузлів до середовища передачі, у якості якого виступає радіоканал; масштабованість; необхідність збору значної кількості інформації про стан мережі на різних рівнях мережевої моделі OSI. Зазначені особливості МР обумовлюють множину вразливостей, які можуть бути використані зловмисниками для здійснення вторгнень у МР з метою порушення цілісності інформації, яка передається в МР, або організації деструктивного впливу на сам процес функціонування МР.

Тому, саме з метою забезпечення безпеки мережі застосовують системи виявлення вторгнень (СВВ) які ґрунтуються на роботі методів виявлення вторгнень (МВВ). Дані методи застосовуються з метою організації безпеки мережі, забезпечення безпеки даних та обмеження несанкціонованого входу в інформаційну систему або систему захисту. Робота даних методів вивчалася багатьма дослідниками та описана в [2–11]. Основними недоліками існуючих СВВ є відсутність можливості самонавчання та прогнозування подій, неможливість застосування при непередбачуваній мережевій активності, нерозвиненість технології прийняття рішень та управління, також погана пристосованість до роботи в реальному режимі часу та за умов децентралізованого управління МР [12].

Аналізуючи можливості існуючих методів виявлення вторгнень, у роботі [9] було запропоновано нейромережевий метод виявлення вторгнень (атак) який в ході проведення досліджень показав добрі показники. Однак даний метод не задовольняє особливостям побудови МР, та не враховує вимоги, що висуваються до методів, які можуть бути використані в МР та у військовій сфері. Тому одним із варіантів усунення вказаних недоліків є вдосконалення існуючого методу для забезпечення роботи в режимі реального часу та в умовах якими характеризується функціонування МР.

Метою статті є вдосконалення існуючого нейромережевого методу виявлення вторгнень (атак) для застосування в МР.

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

Предметом дослідження є нейромережевий метод виявлення вторгнень (атак) в МР.

Аналіз предметної області

У зв`язку з тим що СВВ потрібно виявляти вторгнення як у МР так і у систему управління нею [12], то СВВ повинна відслідковувати весь трафік (службовий та інформаційний), що циркулює в МР. Для цього СВВ повинна функціонувати на всіх рівнях моделі OSI, здійснюючи при цьому контроль з`єднань, аналіз структури та вмісту мережевих пакетів, контроль власного трафіка. Джерелом вхідних даних для пошуку вторгнень СВВ може бути образ різних за своєю природою об`єктів: символів тексту, зображення, звуку, пакетів інформації, сигналів та інше. Ці дані надходять із підсистеми збору інформації, у вигляді вектору параметрів вхідного трафіка які відображають щільність передачі, кількість пакетів, об`єм даних, тривалість з`єднання, кількість з`єднань тощо.

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 стаціонарними мережами [2], а з іншого боку, обмежені обчислювальні можливості мобільних вузлів не дозволяють проводити аналіз мережевої активності в режимі реального часу, використовуючи при цьому значну кількість параметрів, якими описується вхідний трафік (як інформаційний, так і службовий).

Враховуючи зазначене, можна виділити наступні вимоги до методів, які будуть використовуватися при побудові СВВ у МР класу MANET:

– здатність до самонавчання;
– забезпечення роботи у режимі реального часу;
– скорочення часу пошуку вторгнень;
– збільшення швидкості навчання;
– невисока обчислювальна складність, обумовлена низькими обчислюваними можливостями мобільних вузлів.

Існуючі СВВ передбачають прийняття рішень щодо виявлення вторгнень на основі навчання. Інформація, під час проходження системою, аналізується за відповідними параметрами на предмет виявлення аномалій. У результаті чого на виході СВВ з`являється ознака рішення щодо відсутності, або наявності вторгнення у мережу.

В якості навчальної множини існуючі СВВ використовують конкретні різновиди вторгнень (атак), представлені в базі даних (БД) KDD-99 [14]. Ця БД налічує близько 5000000 записів щодо аномальних з`єднань та близько 1000000 відомостей про нормальний тип з`єднання. Кожен запис являє собою образ мережевого з`єднання, включає 41 параметр мережевого трафіка (табл. 1), серед яких міститься три типи ознак: символьні, логічні та числові. У загальному вигляді вони містять інформацію про тривалість з'єднання, тип протоколу, кількість спроб реєстрації тощо [8]. На основі вхідних параметрів з'єднання відбувається перевірка на наявність заборонених з'єднань та маркування їх як „вторгнення" або „не вторгнення". Вказаний запис складається з 42 полів. Перші 41 поле описують ознаки мережевого трафіка, а останнє 42-е поле вказує на тип трафіка, який описується. Вказане поле може приймати значення „*normal*", якщо дане мережеве з`єднання відноситься до „нормального" стану трафіка, або найменування типу вторгнення (наприклад, „*ipsweep*"). Дане поле також необхідне для виконання процесу навчання та аналізу ефективності роботи моделі.

Вирішуючи задачу кластеризації, СВВ ставить у відповідність наведеним вище параметрам мережевого трафіка 22 типи найбільш часто застосованих атак, які поділяються на 4 категорії [15]:

– 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 найчастіше застосованих DoS атак належать: *back*, *land*, *neptune*, *pod*, *smurf*, *teardrop* атаки.

– U2R атаки – пропонують отримання зареєстрованим користувачам привілей локального суперкористувача (мережевого адміністратора). До U2R атак відносять наступні типи атак: *buffer_overflow*, *loadmodule*, *perl*, *rootkit*.

– R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяють R2L атаки на: *ftp_write*, *guess_passwd*, *imap*, *multihop*, *phf*, *spy*, *warezclient*, *warezmaster* та інші атаки.

– *Probe*-атаки – полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. *Probe*-атак поділяються на наступні типи: *ipsweep*, *nmap*, *portsweep*, *satan та інші.*

Таким чином, для побудови математичної моделі СВВ необхідно враховувати значну кількість параметрів функціонування мережі зв'язку, які відносяться до різних рівнів моделі OSI і мають різну фізичну природу. Одним із варіантів вирішення даного завдання є використання апарату нейронних мереж. Відповідно, при розробці запропонованого у [9] нейромережевого методу виявлення вторгнень (атак) у комп'ютерних мережах було використано нейронну мережу Кохонена. Дана нейронна мережа представляє собою математичну модель [13], важливою особливістю якої є можливість паралельної обробки інформації та здатність до самонавчання. Натренована на множині даних з БД мережа здатна узагальнювати отриману інформацію та показувати добрі результати щодо виявлення вторгнень, знаходження нових видів вторгнень та прогнозування можливих подій [5].

Однак, запропонований у [9] метод потребує повної інформації про значну кількість параметрів функціонування мережі зв'язку, збір та обробка якої в умовах динамічної природи функціонування МР неможлива. Тому в даній статті буде здійснено удосконалення існуючого методу з урахуванням особливостей функціонування МР та наведених вище вимог до методів виявлення вторгнень (МВВ) у даних мережах.

Позначення вихідних даних: Розглядається ситуація рівноімовірнісного знаходження системи у стані протікання вторгнення в МР. В один і той же час відбуваються як вторгнення у трафік так і у компоненти вузла зв`язку. Для моделювання такої ситуації слід побудувати навчальну вибірку, яка має в собі 20 %

нормальних з`єднань та 80% аномальних, які містять зазначені типи вторгнень (атак), що відповідає кількості нормальних та аномальних з`єднань. 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. Дана вибірка буде представляти шаблон поведінки порушника. Під час проведення вторгнення, в якості вхідних даних застосовується параметри бази даних KDD Cup 1999 Data.

Таблиця 1

Параметри мережевого трафіка

№	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 2 с.
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 2 с.
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

Вхідний трафік який несе в собі (мову, відео, передачу даних тощо) складається з параметрів мережевого трафіка. При входженні трафіка до першого шару мережі Кохонена параметрам надається відповідне векторне значення $x_i = (x_1,...,x_m)$, $m = \overline{1,M}$. По проходженню першого шару кожен параметр описується відповідним ваговим коефіцієнтом $\omega_m = (\omega_{m1},...,\omega_{mn})$, де m – кількість вхідних векторів які надходять на n – нейрон другого шару для проведення кластеризації. Після проходження другого шару на виході має з`явитися векторне значення проаналізованої поведінки у вигляді $Y_n = 1$ – „аномальне" з`єднання, або $Y_n = 0$, „нормальне" з`єднання. Також на виході отримуються класифікаційні параметри виявленого вторгнення та пропозицій для підсистеми реалізації рішень (на основі присвоєної терми) відносно варіантів реагування на виявлене вторгнення (атаку).

Обмеження та допущення: В роботі розглядаються штучні вторгнення (атаки) порушників з бази даних KDD Cup 1999 Data, що є загрозами для МР. Пошукова вибірка вторгнень обмежена кількістю навчальної вибірки, тому практичне знаходження нових видів вторгнень проводитись не буде. Однак в можливостях мережі передбачене фіксування кожної аномальної поведінки як нововиявленого вторгнення. Вважатимемо, що у складі кожного мобільного вузла функціонує система управління (СУ), що складається з множини підсистем, які виконують функції управління вузловими та мережевими ресурсами відповідно до рівнів моделі OSI [17].

***Необхідно*:** провести удосконалення існуючого методу виявлення вторгнень, який побудований на основі нейронної мережі Кохонена, для забезпечення можливості його використання в умовах характеризуючих МР або мережі класу MANET.

Суть удосконалення запропонованого методу

Як зазначається в [16], збільшення кількості нейронів у нейронній мережі призводить до зменшення швидкості її навчання та сповільнення процесу реакції нейронної мережі на зовнішні впливи. Також з (рис. 1) видно що в процесі навчання, мережа буде навчатися параметрам вторгнень (атак), які відповідають 22 типам атак, що відносяться до 4 категорій. Тому в процесі виявлення вторгнень як у 22 так і у 4 аналізаторах буде аналізуватися одна і таж сама вибірка параметрів, однак в першому випадку буде витрачатися зайвий час на проходження циклу пошуку вторгнень на всіх 22 аналізаторах. Також враховуючи можливість паралельної обробки інформації у МК [13] та з метою покращення швидкості виявлення вторгнень пропонується проводити направлення вхідного сигналу на аналізатори паралельно, а не послідовно (циклічно) як вказано у [9]. У зв'язку з цим, суть удосконалення запропонованого нейромережевого методу полягає у зменшенні кількості нейромережевих аналізаторів з 22 до 6. Тобто, замість аналізаторів, які відповідають 22 типам атак, пропонується введення чотирьох аналізаторів, які відповідають чотирьом категоріям вторгнень (атак), одного аналізатора для фіксації нових типів виявлених атах та одного еталонного аналізатора, який визначає параметри „нормального" впливу на мережу. Вказані два різновиди аналізаторів не були представлені у роботі [9], що обмежувало можливість СВВ до навчання новим видам вторгнень (атак) або „нормального" стану трафіка. Також, з метою виконання вимог до МВВ та покращення можливостей конкурування та навчання нейронів мережі Кохонена пропонується проведення підрахунку потенціалу кожного нейрона, що буде представлено введенням блоку до алгоритму навчання. А впровадження підрахунку похибки мережі на основі визначення швидкості навчання за допомогою введення блоку швидкості забезпечить підвищення точності виявлення вторгнень.

Таким чином, процес функціонування системи виявлення вторгнень в МР можна представити у вигляді алгоритму, який складається з наступних етапів [17].

Етап 1. Підсистемою контролю (збору, обробки, аналізу і зберігання даних) відбувається збір, вимірювання та розпізнавання параметрів встановленого з'єднання, аналіз розпізнаних параметрів та направлення їх на аналізатори підсистеми формування рішень.

Етап 2. Підсистемою формування рішень яка складається з шести нейромережевих аналізаторів (рис. 1) та побудована на мережі Кохонена, відбувається перевірка виконання умов для встановлення аномальної поведінки, шляхом відповідності вихідних параметрів навчальній вибірці:

– якщо вихідне значення n-го нейромережевого аналізатора рівне $Y_n = 1$, то встановлене з'єднання оцінюється як – „аномальне".

– якщо вихідне значення n-го нейромережевого аналізатора рівне $Y_n = 0$, то встановлене з'єднання оцінюється як – „нормальне".

– якщо встановлюється вихідне значення еталонного аналізатора $Y_1 \neq 1$, або для аналізаторів виявлення вторгнень (атак) $Y_{2,3,4,5} \neq 0$, то це значення надходить на інтерпретатор третього шару, якій надсилає сигнал на вхід аналізатора нововиявлених аномалій з параметрами нового сигналу для фіксації нового виду вторгнень (атак) A. Таким чином відбувається навчання аналізатора Y_6 в наслідок чого на його виході буде отримане відповідне значення щодо виявлення нового вторгнення $Y_6 = 1$.

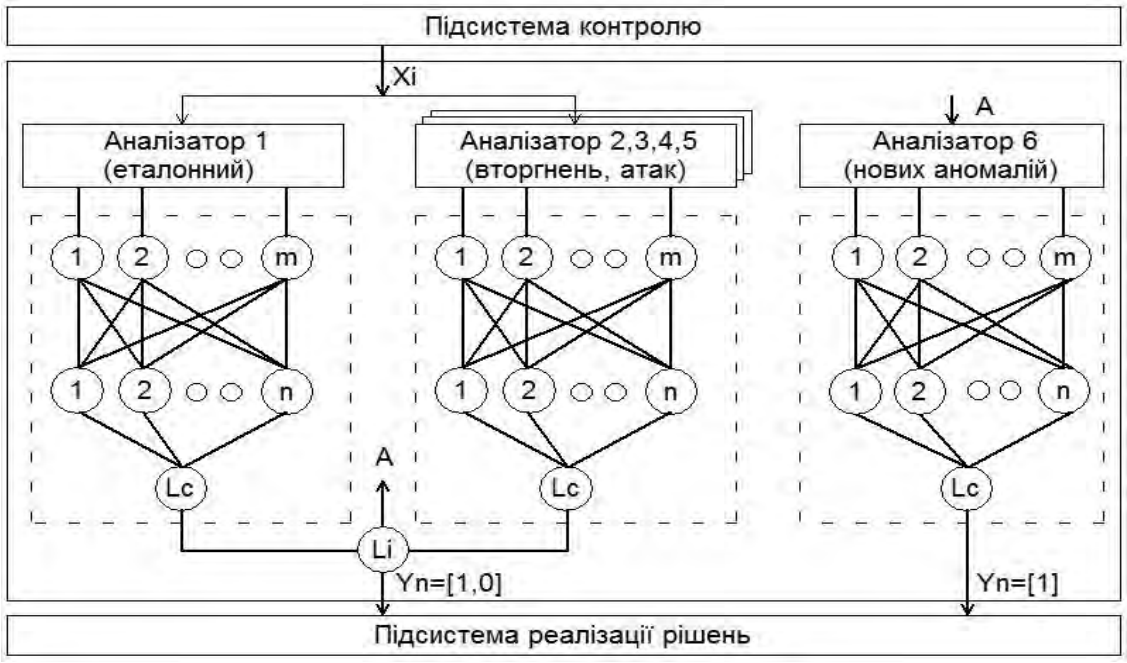

Рис. 1. Структура підсистеми формування рішень

Після проходження підсистеми формування рішень, до підсистеми реалізації рішень буде надсилатися повідомлення щодо виявлення впізнаного вторгнення (атаки), або щодо встановленого невідомого об`єкту, та пропозицією щодо дій відносно відповідного трафіка.

У даній роботі приділяється увага удосконаленню методу, якій забезпечує роботу даної підсистеми.

Етап 3. Підсистема реалізації рішень надає данні щодо стану захищаємої системи, параметрів трафіка, виду виявленого вторгнення, та вживає відповідні заходи щодо виявленого вторгнення.

Побудова удосконаленої архітектури та алгоритму навчання нейромережевої підсистеми виявлення вторгнень в МР

Так як основним інструментом методу є нейронна мережа Кохонена (МК), то варто зазначити, що вона відноситься до самоорганізуючої нейронної мережі та складається з двох шарів: вхідний та вихідний [11,18].

МК це мережа де кожен нейрон з`єднаний з іншими компонентами n - мірного вхідного вектору. МК здатна функціонувати в умовах перешкод, так як число класів вторгнень фіксовано, ваги модифікуються повільно, та настроювання ваг закінчується після навчання. МК також дозволяє виявляти кластери в навчальних даних та відносити данні до тих або інших кластерів.

Якщо після навчання мережа зустрічається з набором даних, несхожим з відомими зразками, то вона не може класифікувати такий набір і тим самим завдяки відповідності ваг виявляє його новизну. Загальна структура мережі Кохонена показана на (рис. 2).

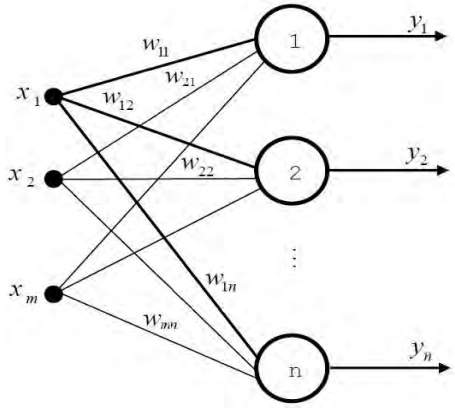

Рис. 2. Загальна структура мережі Кохонена

Перший шар нейронних елементів, призначений для розподілу вхідних сигналів X_m на нейрони шару Кохонена, в якості яких виступають параметри мережевого з'єднання. Як зазначалося вище, мережеве з'єднання оцінюється за 41 параметром, тому кількість нейронних елементів розподільного шару буде рівною m = 41.

Другий шар Кохонена складається з n = 41 нейронів Кохонена, та відіграє ключову роль в класифікації даних і здійснює кластеризацію вхідного простору образів, в результаті чого утворюються кластери різних образів, кожному з яких відповідає свій нейронний елемент. Кількість нейронів шару Кохонена дорівнює – n_K , причому:

$$n_K = f + 1, \qquad (1)$$

де f – кількість нейронів шару Кохонена, які відповідають категоріям атак (вторгнень);

l – кількість нейронів шару Кохонена, які відповідають видам нормального з'єднання.

У зв'язку з тим, що в шарі Кохонена використовується поділ нейронів, які характеризують або нормальне з'єднання, або вторгнення, то коректна класифікація відбувається, якщо при подачі на вхід мережі параметрів вторгнення переможцем буде один з f нейронів шару Кохонена, або, якщо при подачі на вхід мережі параметрів нормального з'єднання переможцем буде l нейрон шару Кохонена. В інших випадках відбувається некоректна класифікація.

Для навчання шару Кохонена використовується конкурентний метод навчання [10]. Суть даного методу навчання полягає в тому, що в процесі навчання відбувається конкуренція між нейронними елементами, в результаті чого визначається нейронний елемент-переможець, який і характеризує категорію або вид даних. З метою пошуку аномальних значень у багатомірних даних та проведення аналізу ступеня подібності об`єктів на основі міри відстаней, а також для визначення „нейрона-переможця" використовується Евклідова відстань (ЕВ) між вхідним і ваговими векторами i-го нейронного елемента шару Кохонена. В основі визначення ЕВ є оцінка відстані між усіма спостереженнями у n-му просторі даних. ЕВ між пошуковими точками є геометричною відстанню та визначається наступним чином:

$$d_i = \left|X - \omega_m\right| = \sqrt{\left(x_1 - \omega_{m1}\right)^2 + \left(x_2 - \omega_{m2}\right)^2 + \ldots + \left(x_m - \omega_{mn}\right)^2}, \qquad (2)$$

де ω_{mn} – ваговий коефіцієнт між m-м нейроном розподільного шару і n-м нейроном другого шару Кохонена; $x_i = \left(x_1, \ldots, x_m\right)$ – вхідний образ.

У процесі навчання синаптичні зв'язки для „нейрона-переможця" посилюються, а для решти нейронів не змінюються. Таким чином, після навчання нейронної мережі, при подачі вхідного сигналу активність „нейрона-переможця" приймається рівною одиниці, а решта нейронів рівні нулю. Таке правило навчання відомо під назвою „Переможець бере все" [10,11].

При навчанні мережі Кохонена може виникати проблема так званих „мертвих нейронів". Одне з обмежень будь якого конкуруючого слою полягає в тому, що деякі нейрони можуть бути не задіяні. Тобто, нейрони, які мають початкові вагові вектори, значно віддалені від векторів входу, ніколи не виграють конкуренції, не залежно від терміну навчання. Як наслідок, такі вектори не використовуються при навчанні та відповідні нейрони ніколи не перемагають (мертві). Тому з метою надання можливості перемогти іншим нейронам, в алгоритмі навчання передбачена можливість втрати „нейроном-переможцем" своєї активності. З цією метою проводиться облік активності нейронів на основі підрахунку потенціалу p_i кожного нейрону в процесі виявлення вторгнення та навчання нейрона [13]. Перш за все нейронам другого шару надається потенціал

$$p_i(0) = \frac{1}{n},$$

де n – кількість нейронів (кластерів).

Якщо значення потенціалу p_i опускається нижче рівня p_{min}, то нейрон виключається з розгляду.

Якщо $p_{min} = 0$, то нейрони не виключаються з розгляду.

Якщо $p_{min} = 1$, то нейрони перемагають по черзі, так як в кожен цикл пошуку тільки один з них готов до розгляду.

В k-му циклі навчання потенціал обчислюється за правилом:

$$p_i(k) = \begin{cases} p_i(k-1) + \dfrac{1}{n}, & i \neq j; \\ p_i(k-1) - p_{min}, & i = j, \end{cases} \qquad (3)$$

де j – номер „нейрона-переможця".

Ваги „нейрона - переможця" та інших нейронів, що знаходяться в межах радіусу навчання, навчаються за правилом Кохонена:

$$\omega_i^{(k+1)} = \omega_i^{(k)} + \eta_i^{(k)}\left[x - \omega_i^{(k)}\right], \qquad (4)$$

де x – вхідний вектор, k – номер циклу навчання, $\eta_i^{(k)}$ – коефіцієнт швидкості навчання i-го нейрона з радіусу навчання в k-ому циклі навчання.

Ваги нейронів, що знаходяться за межами радіусу навчання, не змінюються.

Коефіцієнт швидкості навчання $\eta_i^{(k)}$ поділяється на дві частини: функцію сусідства $\eta_i(d,k)$ та функцію швидкості навчання $a(k)$:

$$\eta_i^{(k)} = \eta_i \cdot (d,k) \cdot a(k). \qquad (5)$$

В якості функції сусідства застосовується Гаусова функція

$$\eta_i(d,k) = e^{\frac{d_i}{2\sigma(k)}}, \qquad (6)$$

де d_i – відстань між i-им нейроном та „нейроном-переможцем". При цьому $\sigma(k)$ – функція, лінійно збігаюча від номеру циклу навчання.

Функція швидкості навчання $a(k)$ представляє собою, збігаючу від номеру циклу навчання, та використовуються як лінійно або зворотно-пропорційна від номеру циклу навчання виду:

$$a(k) = \frac{A}{k + B}\ , \qquad (7)$$

де A и B це константи. Використання цієї функції призводить до того, що всі вектори з навчаємої вибірки вносять приблизно рівний внесок в результат навчання.

Навчання буде складатись з двох етапів:

– на початковому обирається велике значення швидкості навчання та радіус навчання, що дозволяє розташувати вектори нейронів у відповідності з розподільним прийомом у виборці.

– на заключному проводиться більш точне налаштування ваг, коли значення параметрів швидкості навчання набагато менше початкових.

Навчання продовжуватиметься до тих пір, поки похибка мережі при P вхідних векторах не стане найменшою величиною (ω_j – вектор вагів „нейрона-переможця").

$$E = \frac{1}{P}\sum_{i=1}^{P}\left\|x_i - \omega_j\right\|^2\ . \qquad (8)$$

Після надання рівних можливостей для перемоги нейронів, та підрахунку похибки нейронний елемент переможець з номером k визначатиметься:

$$d_k = \min_j d_j\ . \qquad (9)$$

З метою перевірки коректності проведення класифікації при визначенні „нейронів-переможців", відбувається визначення ваг нейронів у області класифікації за допомогою перевірки наступних умов:

– якщо, у разі подачі на вхід мережі нормального з`єднання переможцем є один з l нейронів або при подачі на вхід мережі аномального з`єднання переможцем є один з f нейронів мережі Кохонена. То проводиться модифікація вагових коефіцієнтів „нейрона-переможця" у відповідності з виразом:

$$\omega_{mk}(t+1) = \omega_{mk}(t) + \gamma(x_m - \omega_{mk}(t))\ , \qquad (10)$$

де γ – параметр норми навчання, t – номер ітерації навчання.

– якщо, у разі подачі на вхід мережі нормального з`єднання переможцем не є один з l нейронів або при подачі на вхід мережі аномального з`єднання переможцем не є один з f нейронів мережі Кохонена. То проводиться модифікація вагових коефіцієнтів „нейрона-переможця" у відповідності з виразом:

$$\omega_{mk}(t+1) = \omega_{mk}(t) - \gamma(x_m - \omega_{mk}(t))\ . \qquad (11)$$

З урахуванням проведенням підрахунку потенціалу та похибки удосконалений алгоритм навчання МК можна представити у вигляді (рис. 3).

Етап 1. Реалізується ініціалізація вагових коефіцієнтів ω_{mn} нейронів Y_n шару Кохонена згідно виразу (1).

Рис. 3. Алгоритм навчання шару Кохонена

Етап 2. Обчислюється Евклідова відстань між вхідним образом і ваговими векторами нейронних елементів шару Кохонена на основі співвідношення (2).

Етап 3. Проводиться підрахунок потенціалу p_i, за допомогою виразу (3).

Етап 4. Виконується проходження швидкісного блоку. Етап буде виконуватись поки похибка мережі при вхідних векторах не стане найменшим значенням (4-8).

Етап 5. Визначається нейронний елемент переможець з номером k (9).

Етап 6. Проведення модифікування вагових коефіцієнтів „нейрона-переможця" у відповідності з умовою для (10) та (11) на підставі перевірки коректності проведення класифікації при визначенні „нейронів-переможців".

Етап 7. Відбувається відповідність вхідних та вагових образів, процес повторюється для всіх вхідних образів, починаючи з етапу 2, до найвищого ступеня узгодження між вхідними і ваговими векторами.

Третій шар МК складається з лінійного нейронного елемента L_c – суматора якій розташований у кожному аналізаторі, та одного інтерпретатора L_i якій розташований на виході з суматорів. Суматори при отриманні $Y_n = 1$ або $Y_n = 0$ встановлюють „аномальне" або „нормальне" значення кожного окремого аналізатора.

Інтерпретатор аналізує отримані данні з суматорів та:

– якщо отримується з еталонного аналізатора значення $Y_n = 1$, а з аналізаторів вторгнень $Y_n = 0$ або навпаки з еталонного аналізатора значення $Y_n = 0$, а з одного з аналізаторів вторгнень $Y_n = 1$, то буде виявлена стандартна поведінка параметри якої надсилаються через інтерпретатор до підсистеми реалізації рішень;

– якщо отримується з еталонного аналізатора значення $Y_n = 1$ та хоча б з одного із аналізаторів вторгнень також $Y_n = 1$ або навпаки з еталонного аналізатора значення $Y_n = 0$, а з аналізаторів вторгнень також $Y_n = 0$, то буде виявлена нова аномальна поведінка A, а її параметри надсилаються до інтерпретатора який слугує відправником параметрів нової поведінки на аналізатор нових аномалій для проведення навчання. По проведенню навчання на виході аналізатора нових аномалій формується лише одне значення $Y_n = 1$ яке направляється відразу до підсистеми реалізації рішень.

У результаті проходження параметрів у методі, у разі виявлення конкретної атаки, як вже зазначалось, на його виході буде з`являтися відповідне значення щодо виявлення впізнаного вторгнення, його класифікації та пропозицій для підсистеми реалізації рішень (на основі присвоєної терми) відносно варіантів реагування на виявлене вторгнення (атаку).

Результати експериментальних досліджень

Для проведення дослідження нейромережевого МВВ в якості вхідних даних застосовується база KDD Cup 1999 Data, яка представляє собою набір даних для систем виявлення вторгнень. Так як і у [9], було сформовано навчальну вибірку, яка має в собі 20% нормальних з`єднань та 80% аномальних, які містять зазначені типи вторгнень (атак). Результати проведеного моделювання показали, що:

– отримані результати підтверджують той факт, що якість класифікації залежить від кількості еталонів окремих класів в навчальній виборці. Також при невеликій кількості еталонів помилки виявляються, однак даний показник не перевищує 10 %;

– кількість виявлених вторгнень по классам атак в нашому випадку покращились. Результати виявлення вторгнень за категоріями атак вказані у табл. 2.

– даний метод показав, що в режимі реального часу метод здатний обраховувати складні операції в МР з високою продуктивністю.

Таблиця 2

Результати виявлення вторгнень за категоріями атак

Клас атаки	Середнє значення виявлення атаки, %
Normal	99,5
DoS	99,2
Probe	93,1
R2L	64,4
U2R	55,4

Висновок

У статті представлено удосконалений метод виявлення вторгнень в мобільні радіомережі класу MANET на основі нейронних мереж. Суть удосконалення методу, яка визначає його новизну та відмінність від існуючих методів, полягає у: зменшенні кількості нейромережевих аналізаторів; організації паралельної роботи аналізаторів; удосконаленні процедури навчання нейронної мережі, яка полягає в проведенні обліку активності нейронів мережі на основі підрахунку потенціалу кожного нейрону в процесі виявлення вторгнень та навчання; підрахунку похибки мережі на основі визначення швидкості навчання.

Вказане удосконалення було застосовано вперше, та на відміну від існуючих методів виявлення вторгнень дозволило покращити швидкість навчання нейронної мережі, підвищити точність виявлення вторгнень у МР та забезпечило роботу методу в режимі реального часу. Експериментальні дослідження показали, що в середньому значення виявлення вторгнень удосконаленим методом покращилось на 13,5 %, що задовольняє мету даної роботи.

У ході подальших досліджень буде розроблено модель загроз противника при вторгненні в МР класу MANET, що дозволить проводити аудит, аналіз ситуацій та прогнозування подій (вторгнень) в МР і, таким чином, підвищить ефективність запропонованого методу виявлення вторгнень.

Список літератури

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

2. Міночкін А.І. Виявлення атак в мобільних радіомереж / А.І. Міночкін, В.А.Романюк, П.В. Шацило // Збірник наукових праць № 1. – К.: ВІТІ НТУУ "КПІ", 2005. – С. 102 – 111.

3. Мерит М. Безопасность беспроводных сетей / М. Мерит, Д. Полино; пер. с англ. А.В. Семенова. – М.: Компания АйТи; ДМК Пресс, 2004. – 288 с.

4. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А.А. Владимиров; пер. с англ. А. А. Слинкина. – М.: НТ Пресс, 2005. – 463 с.

5. Осовский С. Нейронные сети для обработки информации / С. Оссовский; пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.

6. Kachirski O. Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks / O. Kachirski, R. Guha // Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2003.

7. A General Cooperative Intrusion Detection Architecture for MANETs / D. Sterne, P. Balasubramanyam, et al. // Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), 2005. – P. 57 – 70.

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

9. Комар М.П. Інтелектуалізована інформаційна технологія виявлення комп'ютерних атак / М.П. Комар, Д.І. Боднар, А.О. Саченко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2010. – № 2. – С. 133-137.

10. Головко В.А. Нейронные сети: обучение, организация, применение / В.А. Головко. – Нейрокомпьютеры и их применение: учеб. пособие – М., 2001. – 256 с.

11. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.

12. 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.

13. Вежневец А. Популярные нейросетевые архитектуры/ Компьютерная Графика и Мультимедиа. Сетевой журнал — 2004. — №2 (1).

14. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.

15. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий; 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2003. – 624 с.

16. Заенцев И.В. Нейронные сети: основные модели Учебное пособие к курсу Нейронные сети" для студентов 5 курса магистр. к. электроники физического ф-та / И.В. Заенцев. – Воронеж, 1999. – 76 с.

17. Романюк В.А. Інтелектуальні мобільні радіомережі: збірник матеріалів V науково-технічної конференції [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / В.А. Романюк. – К.: ВІТІ НТУУ „КПІ", 2010. – С. 28 – 36.

18. Кохонен Т. Самоорганизующие карты / Т. Кохонен. – М.: БИНОМ. Лаборатория знаний, 2008. – 655 с.

19. Чевардін В.Є. Аналіз загроз безпеки інформації в мережах MANET / В.Є .Чевардін, А.В. Романюк, І.М. Діянчук // Збірник наукових праць № 1. – К.: ВІТІ НТУУ "КПІ", 2012. – С. 125 – 134.

Надійшла до редколегії 2.09.2015

Рецензент: д-р техн. наук проф. О.В. Кувшинов, Військовий інститут телекомунікацій та інформатизації, Київ.

МЕТОД ОПРЕДЕЛЕНИЯ ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

С.В. Сальник, В.В. Сальник, О.А. Симоненко, О.Я. Сова

В статье представлен усовершенствованный нейросетевой метод определения вторжений в мобильные радиосети класса MANET, в основе которого находиться существующий метод определения вторжений в стационарные компьютерные сети с использованием нейронной сети Кохонена. Усовершенствование заключается в уменьшении количества нейросетевых анализаторов, структурном изменении работы нейросетевых анализаторов с последовательной на параллельную, что обеспечило работу метода в режиме реального времени. С целью улучшения возможностей конкурирования и обучения нейронной сети Кохонена внедрено проведение подсчета потенциала каждого нейрона сети и подсчет погрешностей сети. Проведены экспериментальные исследования и определен уровень определения вторжений разработанным методом.

Ключевые слова: *мобильные радиосети, MANET, обеспечение безопасности мобильной радиосети, метод определения вторжений, сеть Кохонена.*

METHOD OF INTRUSION DETECTION IN MOBILE RADIO NETWORKS ON THE BASIS OF NEURALS NETWORKS

S.V. Salnyk, V.V. Salnyk, O.A. Symonenko, O.Y. Sova

An advanced neural network method of intrusion detection in MANET class mobile radio networks is introduced in the article. It is based on an existing method of intrusion detection in fixed computer networks using self-organizing map. The improvement involves quantity reduction of neural network analyzers and serial-to-parallel structural operation change of neural network analyzers which enabled operation of the method in real-time mode. In order to improve competition capabilities and studying of self-organizing map, counting works of each network neuron potential and network errors have been implemented. Experimental studies have been conducted and level of intrusion detection using the established method have been defined.

Keywords: *mobile radio network, MANET, security mobile radio network, method of detection, Kohonen network.*