УДК 621.391

[1]Сергій Васильович Сальник
[1]Володимир Васильович Сальник
[1]Едуард Миколайович Бовда (канд. техн. наук)
[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

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ В МОБІЛЬНІ РАДІОМЕРЕЖІ КЛАСУ MANET НА ОСНОВІ ГІБРИДНОГО НЕЙРО-НЕЧІТКОГО КЛАСИФІКАТОРА

В статті представлено гібридний нейро-нечіткий класифікатор виявлення вторгнень в мобільні радіомережі класу MANET, з використанням нечітких мереж на основі нейронів, які реалізують нечіткі операції. Розробка методу полягала в побудові алгоритму функціонування системи виявлення вторгнень в мобільній радіомережі, покращенні можливостей конкурування та навчання нейронів мережі та розробці алгоритму навчання нейро-нечіткої підсистеми виявлення вторгнень в мобільну радіомережу. Це забезпечило роботу методу виявлення вторгнень в режимі реального часу, при нечіткій мережевій активності, умовах мобільності, динамічній топології та умовах, що характеризують мобільні радіомережі військового призначення. Проведено експериментальні дослідження та з'ясовано рівень виявлення вторгнень розробленим методом. Визначені завдання, щодо подальших досліджень, в яких буде розроблено модель вторгнень в мобільні радіомережі класу MANET та метод навчання нечітких баз правил.

Ключові слова: *мобільні радіомережі; MANET; забезпечення безпеки мобільної радіомережі; методи виявлення вторгнень; гібридний нейро-нечіткий класифікатор.*

Вступ

Актуальність дослідження. Останнім часом спостерігається динамічний розвиток та поширення мобільних радіомереж (МР) класу MANET, які стають більш вживаними у повсякденному житті та у військовій галузі, особливо в тактичній ланці управління військами [1]. Основними особливостями побудови та застосування МР є: мобільність усіх вузлів; динамічна топологія; децентралізоване управління МР; спільний доступ вузлів до середовища передачі даних; 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 для здійснення вторгнень у МР з метою порушення безпеки 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 [1–14]. Основними недоліками існуючих СВВ є обмежені можливості: самонавчання, прогнозування подій, застосування при непередбачуваній та нечіткій мережевій активності; нерозвиненість технології прийняття рішень; погана пристосованість до роботи в реальному режимі часу [3].

Аналізуючи можливості існуючих МВВ, зазвичай пропонується метод, який не завжди задовольняє особливостям побудови МР, та не враховує вимоги, що висуваються до методів, які можуть бути використані в МР військової сфери. Тому одним із варіантів усунення вказаних недоліків є розробка методу для забезпечення роботи в умовах якими характеризується МР.

Метою статті є розробка гібридного нейро-нечіткого методу виявлення вторгнень для застосування в МР.

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

Предметом дослідження є метод виявлення вторгнень в МР побудований на основі гібридного нейро-нечіткого класифікатора.

Аналіз предметної області. У зв'язку з тим, що СВВ потрібно виявляти вторгнення як у МР так і у систему управління нею [3], то СВВ повинна відслідковувати весь трафік, 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 контролю та збору інформації, у вигляді векторів параметрів вхідного трафіка, які відображають щільність передачі даних, 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 множину параметрів, якими описується вхідний трафік.

Враховуючи зазначене, можливо 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; можливість прогнозування вторгнень в мережу; невисока обчислювальна складність. Таким чином, для побудови СВВ необхідно враховувати значну кількість параметрів функціонування МР, які відносяться до різних рівнів моделі OSI, мають різну фізичну природу та можуть містити у собі неточні, неповні або нечіткі данні вхідного трафіка [4].

Одним із варіантів вирішення даного завдання є використання апарату нейронної мережі, сформованої на основі нечітких нейронів з нечіткими входами, а також чіткою активаційною функцією. Зазвичай подібний підхід називається гібридним. Враховуючи необхідність проведення методом класифікації вхідних образів, основаних на попередній кластеризації навчаємих прикладів та віднесення їх до заданих класів, надає підстави називати даний метод – гібридним нейро-нечітким класифікатором (ГНК). Даний підхід застосовується для додатків, які характеризуються нечіткими межами між класами, та забезпечує досить просте подання складного розподілу простору ознак. Крім того ГНК характеризується можливістю навчання при отриманні нової інформації (параметрів). Завдання нечіткої класифікації полягає у виконанні відповідного нечіткого розподілу ознакового простору. При цьому кількість помилково класифікованих образів буде наближуватись до мінімуму у зв'язку з тим, що база нечітких правил буде оптимізована шляхом проведення самонавчання [5].

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

Натренована на множині даних з відповідної бази даних мережа здатна узагальнювати отриману інформацію, виявляти вторгнення, знаходити нові види вторгнень, що в свою чергу задовольняє вимогам щодо розробки та застосуванню МВВ в МР класу MANET [6].

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). 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 характеристична терма t, що характеризує вплив атак на рівнях мережевої моделі OSI.

Вхідний трафік, який несе в собі (мову, відео, передачу даних тощо) складається з параметрів мережевого трафіка. В якості вхідних даних застосовується параметри бази даних (БД) KDD Cup 1999 Data, які характеризують вищевказані параметри [7].

Тобто при подачі на вхід першого шару мережі, вектору $\left(\grave{x}_1,...,\grave{x}_m\right)$, відбувається розподіл його на три рівнозначні потоки. Дані потоки являються вхідними даними для другого шару, якій аналізує ці данні на предмет нечіткості, та визначає її повноту виходячи з нечіткої відповідності {висока, середня, низька} вхідних даних. На виході другого та третього шару формується значення нечіткої повноти вхідних параметрів.

Виходи нейронів нечіткого шару застосовуються у якості входів нейронного шару. Кількість нейронів нечіткого шару визначається кількістю кластерів, тобто відповідає категоріям вторгнень, та становить шість.

Кожен з нейронів нейронного шару навчений виявленню вторгнень, розпізнаванню їх у відповідності до їх типів та характеристичних можливостей впливу на МР та її компоненти. Нейронний шар складатиметься з прихованих шарів, які за своєю функцією проводять: класифікацію та кластеризації вхідного простору, конкурентний спосіб навчання та виявлення вторгнень, облік активності нейронів на основі підрахунку їх потенціалу, визначення "нейрона-переможця" та надання значенню параметра відповідної характеристичної терми.

Під час виявлення вторгнень у нейронному шарі буде застосовуватись механізм нечіткого логічного виводу для опису бази вхідних параметрів. На підставі співставлення вхідних

параметрів, у системі правил буде формуватись рішення, щодо нейро-нечіткої класифікації. Вихідним значенням системи правил може бути:

значення проаналізованої поведінки у вигляді $Y_n = 1(t)$ – "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 t) відносно варіантів реагування на виявлене вторгнення.

Обмеження та допущення: В роботі розглядаються штучні вторгнення (атаки), 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 [11]. Вказана СУ здатна проводити виявлення нечіткості, неточності та неповноти даних вхідного трафіка та направляти його через підсистему контролю до підсистеми формування рішень, де і відбуватиметься виявлення вторгнень.

Необхідно: Провести розробку МВВ, який побудований на основі гібридного нейро-нечіткого класифікатора, та матиме можливість використання в МР тактичної ланки управління військами.

Суть розробки методу: В якості навчальної множини існуючі СВВ використовують конкретні різновиди вторгнень (атак), представлені в базі даних [7]. 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, 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 [4,8].

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 описує 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 навчання та аналізу ефективності роботи методу. Процес побудови та тестування МВВ на основі навчальної вибірки атак розглядалося у [4,8,9]. 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.

В процесі навчання та вирішуючи задачу кластеризації, мережа буде ставити у відповідність параметри мережевого трафіка, тобто 22 типи найбільш часто застосованих атак, які поділяються на 4 категорії, вказані у таблиці 1. Виходячи з цього 22 типам атак будуть відповідати нейрони (класифікатори) та додатково один класифікатор для фіксації нових типів виявлених вторгнень та один еталонний класифікатор, який визначає параметри "нормального" впливу на мережу [4,10].

Таблиця 1

Категорії та типи найбільш часто застосованих атак

№ з/п	Категорії атак	Типи атак
1	DoS	back, land, neptune, pod, smurf, teardrop
2	U2R	buffer_overflow, loadmodule, perl, rootkit
3	R2L	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster
4	Probe	ipsweep, nmap, portsweep, satan

Також, з метою виконання вимог до МВВ та покращення можливостей конкурування та навчання нейронів мережі пропонується проведення підрахунку потенціалу кожного нейрона, що буде представлено введенням відповідного блоку до алгоритму навчання.

Таким чином, функціонування СВВ в МР можливо представити у вигляді алгоритму, який складається з наступних етапів [11].

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 до підсистеми формування рішень.

Етап 2. Підсистемою формування рішень, яка складається з ГНК, відбувається перевірка виконання умов для встановлення аномальної поведінки на основі нечітких правил та шляхом відповідності вихідних параметрів навчальній вибірці.

Після проходження підсистеми формування рішень, до підсистеми реалізації рішень буде надсилатися повідомлення щодо виявлення впізнаного вторгнення, його класифікації та пропозицій для підсистеми реалізації рішень (на основі присвоєної терми) відносно варіантів реагування на виявлене вторгнення.

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

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

Побудова архітектури та алгоритму навчання нейро-нечіткої підсистеми виявлення вторгнень в МР.

З метою вирішення задачі класифікації, найбільш часто застосовуються нейронні мережі та системи з нечіткою логікою, які здатні доповнювати один одного в рішенні складно обчислювальних завдань. Тому буде розглядатися модель нейро-нечіткої мережі ANFIS (Adaptive-Network-Based Fuzzy Inference System), яка була запропонована Янгом (Jang). Дана мережа за своєю структурою являє собою багатошарову нейронну мережу прямого поширення сигналу особового типу.

Основна ідея, яка покладена в основу ANFIS, полягає у використанні навчальної вибірки даних для визначення параметрів функцій належності, які найкраще відповідають системі нечітких міркувань. При цьому для знаходження параметрів функцій належності використовуються відомі процедури навчання нейронної мережі. Це дозволяє застосовувати для налаштування нейро-нечітких мереж швидкі алгоритми навчання нейронних мереж, засновані на методі зворотного поширення помилки.

Гібридна мережа адаптивної нейро-нечіткої системи виведення ANFIS являє собою нейронну мережу з одним виходом та кількома входами, які є нечіткими лінгвістичними змінними. При цьому терми вхідних лінгвістичних змінних описуються стандартними функціями належності, а терми вихідних змінних представляються лінійним виразом або константною функцією належності [5].

Для рішення задачі класифікації вторгнень в МР у статті запропонована модифікація моделі ANFIS, яка входить до складу підсистеми формування рішень та представлена на (рис. 1). Зазвичай модель ANFIS реалізує систему нечіткого виводу Сугено, у вигляді відповідної кількості шарів нейронної мережі прямого поширення. Враховуючі необхідність пошуку мережею нововиявлених вторгнень та проведення навчання мережі в алгоритм методу буде адаптовано зворотне поширення похибки (виявленого нового вторгнення).

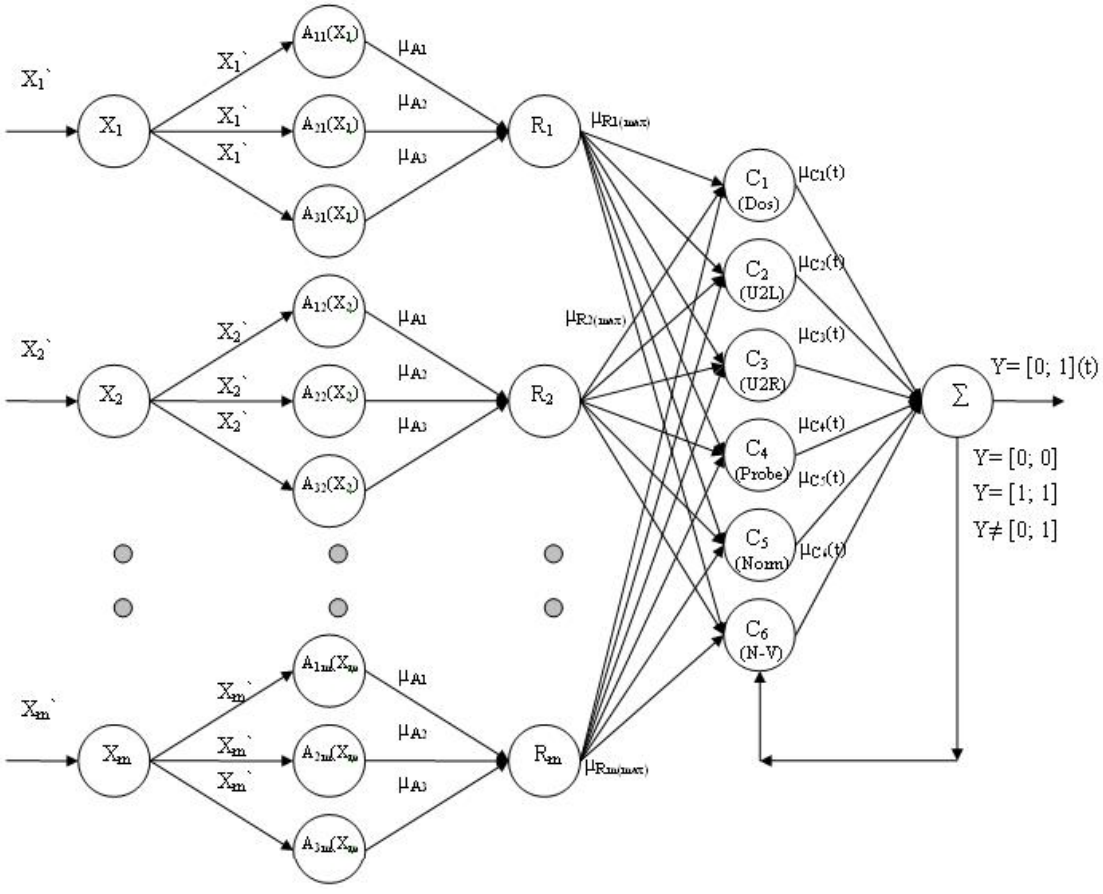

Рис. 1. Структура гібридного нейро-нечіткого класифікатора

Розроблена адаптована модель гібридного нейро-нечіткого виводу складатиметься з п'яти шарів:

– **перший шар** – представляє собою вхідний шар, який отримує вектор вхідних значень, який характеризує параметри трафіка. Тобто з системи контролю надходять вхідні данні $X = (x_1, ..., x_m)$, де m - кількість параметрів мережі, яка дорівнює 41. Після чого нейронний елемент розподіляє та надсилає вхідне значення трьома рівнозначними потоками на другий шар мережі.

– **другий шар** – представляє собою розподіл кожного вхідного значення на лінгвістичні вхідні терми. Кожна терма відповідає повноті отриманих значень вхідних параметрів у нечіткій відповідності {висока, середня, низька}, тобто відповідатиме (A_1, A_2, A_3), нейронам шару. Кожен з нейронів отримує вхідні значення та визначає ступень належності їх нечіткій множині. Вихід кожного (A_1, A_2, A_3), нейрона m - го параметру має вигляд:

$$A_{im}(x_m) = \mu_{Ai}(x_m), \qquad (1)$$

де x_m – вхідний сигнал m - го елемента, A_i – лінгвістична змінна, яка відповідає нечіткій відповідності, μ_{Ai} – функція належності.

Кожен нейрон шару відповідає одному нечіткому правилу, а вихідне значення з m нейронних елементів являє собою завершення та визначатиметься:

$$R_m = \mu_{A1}(x_1) \times ... \times \mu_{Am}(x_m), \qquad (2)$$

Сумарне значення термів лінгвістичних змінних вузла відповідає вхідному значенню параметра та визначається:

$$M = X_m = \sum_{i=1}^{3} A_{im}, \qquad (3)$$

– **третій шар** – являє собою процедуру збору ступенів належності вхідних параметрів відповідним нечітким правилам та визначення переможного значення рівня відповідності {висока, середня, низька}. Кількість нейронів шару R_m відповідає кількості вхідних значень параметрів. Заключення нечітких правил з визначенням переможних термів параметрів направляються на кожен нейрон четвертого шару. Переможний лінгвістичний терм параметру визначається, як оптимальне значення переможних параметрів або максимальних переможних значень:

$$R_m = \text{opt}\left\{ \max \mu_{A_m}; x_m \right\}, \qquad (4)$$

– **четвертий шар** (класифікаційний) – складається з C_j нейронів, де j дорівнює 6 та має у своєму складі:

C_1, C_2, C_3, C_4 нейрони, які відповідають 4 категоріям вторгнень (DoS, U2R, R2L, Probe) вторгнень (атак) – f ;

C_5 нейрон нормальних видів поведінки (Norm) – l ;

C_6 нейрон нововиявлених вторгнень (N-V) – v .

Цей шар навчений виявленню вторгнень, він відіграє ключову роль в класифікації даних та здійсненні кластеризації вхідного простору образів. Кількість нейронів шару відзначатиметься:

$$C_K = f + l + v, \qquad (5)$$

У зв'язку з тим, що в шарі 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 чи декілька з f нейронів шару та v нейрон;

при подачі на вхід мережі параметрів нормального з'єднання переможцем буде l нейрон шару.

в інших випадках відбувається некоректна класифікація та визначається нововиявлена (N-V) поведінка v .

Для навчання шару використовується конкурентний метод навчання [12]. Суть даного методу полягає в тому, що в процесі навчання відбувається конкуренція між нейронними елементами, в результаті чого визначається нейронний елемент-переможець, який і характеризує параметри вторгнень. 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 C_j-го нейронного елемента шару. 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:

$$d_j = \left| X - \mu_j \right|, \qquad (6)$$

де μ_j – ваговий коефіцієнт параметру, якій відповідає значенню функції належності; $X = (x_1, ..., x_m)$ – вхідний образ.

При виявленні аномальних значень мережею, може виникати проблема так званих "мертвих нейронів". Одне з обмежень будь якого конкуруючого шару полягає в тому, що деякі нейрони можуть бути не задіяні. Тобто, нейрони, які мають початкові вагові вектори, значно віддалені від векторів входу та 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 $p_i(0) = \frac{1}{c}$,

де c – 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:

$$p_i(k) = \begin{cases} p_i(k-1) + \frac{1}{c}, & i \neq j \\ p_i(k-1) - p_{min}, & i = j \end{cases}, \quad (7)$$

де j – номер "нейрона-переможця".

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

$$d_k = \min_j d_j. \quad (8)$$

Нейрони цього шару являють собою нечіткі множини, які використовуються у наслідок нечітких правил. Вихідним значенням шару буде сукупна потужність визначених (переможних) параметрів на основі нечітких значень.

Нейрон шару обраховує переможні параметри шару $C_m = (C_1,...,C_6)$ тобто внесок нечітких правил у класифікування, що визначається:

$$C_m = 1 \Leftrightarrow \exists \text{opt} \left\{ \mu_{R_m} \right\} = 1, \quad (9)$$

або

$$C_m = 0 \Leftrightarrow \exists \text{opt} \left\{ \mu_{R_m} \right\} = 0, \quad (10)$$

При виявленні параметрів які характеризують вторгнення у C_j нейроні, нейрон який здійснив виявлення надає значенню параметра відповідну характеристичну терму, яка свідчить про характеристики атаки (параметри, види впливу на МР на рівнях мережевої моделі OSI). Надалі дане вихідне значення надсилається до наступного шару мережі.

– п'ятий шар – представлений одним елементом – суматором, який обраховує відповідність виявлених значень нейронами (категорій атак) нейрону (нормальної поведінки).

Вихідна змінна з суматора буде направлена до підсистеми реалізації рішень у вигляді:

якщо вихідне значення суматора, яке отримане з класифікаторів вторгнень C_1, C_2, C_3, C_4, C_6 рівне $Y_n = 1$, то встановлене з'єднання оцінюється як – "аномальне".

якщо вихідне значення суматора, яке отримане з класифікатора вторгнень C_1, C_2, C_3, C_4, C_6 рівне $Y_n = 0$, то встановлене з'єднання оцінюється як – "нормальне".

якщо вихідне значення суматора, яке отримане з класифікатора нормальної поведінки рівне $Y_n \neq 1$, або з класифікатора виявлення вторгнень рівне $Y_n \neq 0$, то з суматора надсилаються параметри нового виду вторгнень на нейрон (N-V) для їх фіксації. Таким чином відбувається навчання шару нейронної мережі, в наслідок чого на виході класифікатора нововиявлених аномалій буде отримане значення щодо виявлення нового вторгнення $Y_n = 1$.

Вихідне значення множин підраховується, як повне вихідне значення мережі Y, та являє собою окремий підрахунок значень множин C_1, C_2, C_3, C_4, C_6 класифікації вторгнень та виконання вищевказаної відповідності до значення C_5 – нормального виду поведінки, та має вигляд:

$$\Sigma = \begin{cases} 1, & \text{вторгнення} \\ 0, & \text{нормальна поведінка} \\ N-V, & \text{нововіявлене вторгнення} \end{cases} \quad (12)$$

Вихідне значення даної системи матиме вигляд:

$$Y = 1 \Leftrightarrow \exists C_м = 1, \quad (13)$$

або

$$Y = 0 \Leftrightarrow \neq \exists C_м = 1, \quad (14)$$

При виявлення вторгнення (атаки), на виході суматора 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) на підставі характеристичної терми.

Результати експериментальних досліджень.

В ході імітаційного моделювання побудови запропонованого методу було сформовано навчальну вибірку, яка має в собі 20% нормальних з'єднань та 80% аномальних, які містять зазначені типи вторгнень (атак). Результати досліджень щодо виявлення вторгнень 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 %;

виявлення вторгнень в класах DoS, Probe, R2L, U2R атак в порівнянні з методами розробленими [9,14,15] покращились.

Висновки й перспективи подальших досліджень

У статті представлено розроблений МВВ в МР класу MANET на основі гібридного нейро-нечіткого класифікатора. Суть розробки методу, яка визначає його новизну та відмінність від існуючих методів, полягає у: використанні гібридного нейро-нечіткого класифікатора, покращенні можливостей конкурування та навчання нейронів мережі завдяки проведенню підрахунку потенціалу нейронів мережі, що дозволило застосовувати розроблений метод у МР військового призначення.

Вказана розробка була застосована вперше, та на відміну від існуючих МВВ дозволила

покращити швидкість навчання нейронної мережі, підвищити точність та швидкість виявлення вторгнень у МР, що задовольняє меті даної роботи.

У ході подальших досліджень буде розроблено модель вторгненні в МР класу MANET та метод навчання нечітких баз правил, що дозволить проводити аудит, аналіз ситуацій та прогнозування вторгнень в МР, та підвищить ефективність запропонованого МВВ.

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 радіомереж / 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. Сова О. Я.**, Міночкін Д. А.,Сальник С. В. 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. **5. Борисов В. В.**, Круглов В. В., Федулов А. С. Нечеткие модели и сети. – М.: Горячая линия – Телеком, 2007. – 284 с. **6. Осовский С.** Нейронные сети для обработки информации / Пер. с польского И. Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.: ил. **7. KDD Cup 1999 Data** / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999. **8. 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. **9. 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. **10. Лукацкий А. В.** Обнаружение атак. 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2003. **11. Романюк В. А.** Інтелектуальні мобільні радіомережі: збірник матеріалів V науково-технічної конференції ["Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ", 2010. – С. 28–36. **12. Головко В. А.** Нейронные сети: обучение, организация, применение / Нейрокомпьютеры и их применение: учеб. пособие – М., 2001 - 256 с. **13. Вежневец А.** Популярные нейросетевые архитектуры/ Компьютерная Графика и Мультимедиа. Сетевой журнал – 2004. – №2 (1). **14. 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, 20-24. **15. 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

МЕТОД ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ КЛАССА MANET НА ОСНОВЕ ГИБРИДНОГО НЕЙРО-НЕЧЕТКОГО КЛАССИФИКАТОРА

[1]Сергей Васильевич Сальник
[1]Владимир Васильевич Сальник
***[1]Эдуард Николаевич Бовда** (канд. техн. наук)*
***[2]Дмитрий Анатольевич Миночкин** (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 представлен гибридный нейро-нечеткий классификатор обнаружения вторжений в мобильные радиосети класса MANET, с использованием нечетких сетей на основе нейронов, которые реализуют нечеткие операции. Разработка метода заключалась в построении алгоритма функционирования системы обнаружения вторжений в мобильной радиосети, улучшении возможностей конкурирования и обучение нейронов сети и разработке алгоритма обучения нейро-нечеткой подсистемы обнаружения вторжений в мобильную радиосеть. Это обеспечило работу метода обнаружения вторжений в режиме реального времени, при нечеткой сетевой активности, условиях мобильности, динамичной топологии и условиях, характеризующие мобильные радиосети военного назначения. Проведены экспериментальные исследования и выяснено уровень обнаружения вторжений разработанным методом. Определены задачи, для проведения дальнейших исследований, в которых будет разработана модель вторжений в мобильные радиосети класса MANET и метод обучения нечетких баз правил.

Ключевые слова: *мобильные радиосети; MANET; обеспечение безопасности мобильной радиосети; методы обнаружения вторжений; гибридный нейро-нечеткий классификатор.*

A METHOD OF INTRUSION DETECTION IN MOBILE RADIO CLASS MANET BASED ON A HYBRID NEURO-FUZZY CLASSIFIER

[1]Serhii V. Salnyk
[1]Volodymyr V. Salnyk
***[1]Eduard M. Bovda** (Candidate of Technical Sciences)*
***[2]Dmytro A. Minochkin** (Candidate of Technical Sciences, Senior Research Fellow)*

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

The article presents a hybrid neuro-fuzzy classifier of intrusion detection in mobile radio class MANET using fuzzy-based networks of neurons, which implement fuzzy operation. Development method was building the algorithm of functioning of intrusion detection system in the mobile radio network, improving the capabilities of competing and training a network of neurons and developing algorithm study of neuro-fuzzy intrusion detection subsystem in a mobile radio network. This ensured the work method of intrusion detection in real time, with fuzzy network activity, conditions, mobility, dynamic topologies and conditions that characterize mobile radio network for military purposes. Experimental study and determined the level of intrusion detection developed method. Defined tasks for further research, which will be the model of intrusion in mobile radio network class of MANET and method study of fuzzy rule bases.

Keywords: *mobile radio network; MANET; security of mobile radio network; methods of detection of intrusions; a hybrid neuro-fuzzy classifier.*

References

1. Romanyuk V.A. (2003), The mobile radio network - wireless technology prospects. [*Mobilnyie radioseti – perspektivyi bezprovodnyih tehnologiy*], Seti i telekommunikatsii, № 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", № 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. Sova O.Y.**, Minochkin D.A. Salnik S.V. (2015), 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" № 1 (22), Natsional'nyy universitet oborony Ukrainy, pp. 103-112. **5. Borisov V.V.**, Kruglov V.V., Fedulov A.S., (2007), Fuzzy models and networks [*Nechetkie modeli i seti*], Moscow, Goryachaya liniya, Telekom, 284 p. **6. Osovskiy S.** (2002), Neural network for processing information [*Neyronnyie seti dlya obrabotki informatsii*], Per. s polskogo I.D. Rudinskogo, Moscow, Finansyi i statistika, 344 p. **7. KDD Cup (**1999), Data**,** The UCI KDD Archive, Information and Computer Science.University of California, Irvine. **8. B. Sun**, K.Wu, and U. W. Pooch. (2003) "Alert Aggregation in Mobile Ad Hoc Networks". The ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78. **9. Komar M.P.**, Bodnar D.I., Sachenko A.O. (2010), Intelligent Information technology detect computer attacks [*Intelektualizovana informatsiyna tehnologiya viyavlennya komp'yuternih atak*], Vimiryuvalna ta obchislyuvalna tehnika v tehnologichnih protsesah, №2, pp. 133-137. **10. Lukatskiy A.V.** (2003) Detection of attacks [*Obnaruzhenie atak*], 2-e izd., pererab. i dop, SPb.: BHV-Peterburg. **11. Romanyuk V.A**. (2010) Intelligent mobile radio network [*Intelektualni mobilni radiomerezhi*], Zbirnik materialiv v naukovo-tehnichnoyi konferentsiyi [Prioritetni napryamki rozvitku telekomunikatsiynih sistem ta merezh spetsialnogo priznachennya], Kyiv: VITI NTUU „KPI", pp. 28–36. **12. Golovko V.A.** (2001) Neural network: Learning, organization, application [*Neyronnyie seti: obuchenie, organizatsiya, primenenie*], Neyrokompyuteryi i ih primenenie: ucheb. posobie, Moscow, 256 p. **13. Vezhnevets A.** (2004), Popular neural network architecture [*Populyarnyie neyrosetevyie arhitekturyi*] Kompyuternaya Grafika i Multimedia. Setevoy zhurnal, №2 (1). **14. 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. **15. 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, 2(1): 33.

Отримано: 14.02.2016 року.