УДК 621.396

С.В. Сальник, В.В. Сальник, Я.А. Стемпковська

Військовий інститут телекомунікацій та інформатизації, Київ

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ КЛАСУ MANET НА ОСНОВІ НЕЧІТКОЇ БАЗИ ЗНАНЬ

В статті представлено метод виявлення вторгнень в мобільних радіомережах класу MANET на основі нечіткої бази знань, який ґрунтується на нейро-нечіткій моделі ANFIS. Розробка методу полягала в: модифікації моделі ANFIS для застосування її в мобільних радіомережах класу MANET, проведенні самонавчання бази знань методів виявлення вторгнень, покращенні можливостей конкурування та навчання нейронів мережі, підрахунку потенціалу нейронів мережі, застосуванні нейро-нечіткого алгоритму. Вказана розробка дозволила покращити швидкість навчання нейро-нечіткої мережі, підвищити точність та швидкість виявлення вторгнень у мобільних радіомережах, а також застосовувати мережу при нечіткій мережевій активності. Визначені завдання, щодо подальших досліджень, в яких буде розроблено метод оцінки ефективності методів виявлення вторгнень в МР класу MANET.

Ключові слова: *мобільні радіомережі, MANET, забезпечення безпеки мобільної радіомережі, методи виявлення вторгнень, ANFIS.*

Вступ

Актуальність дослідження. Останнім часом спостерігається розвиток та поширення мобільних радіомереж (МР) класу MANET, які стають більш вживаними у повсякденному житті та у військовій галузі [1]. Основними особливостями побудови та застосування МР є: мобільність 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. Основною відмінністю МР від класичних радіомереж є відсутність фіксованої мережевої інфраструктури і, як наслідок, фіксованих маршрутів передачі інформації, що потребує використання нових підходів до управління МР та системами, які забезпечують її функціонування. Однією з основних систем МР є підсистема забезпечення безпеки, до склади якої входить система виявлення вторгнень (СВВ) [1].

З метою забезпечення інформаційної безпеки мережі застосовують СВВ, які ґрунтуються на роботі методів виявлення вторгнень (МВВ). Дані методи застосовуються для організації безпеки мережі, забезпечення безпеки даних та обмеження несанкціонованого входу в інформаційну систему або систему захисту. Робота методів вивчалася багатьма дослідниками та описана в [1 – 9].

Основними недоліками існуючих МВВ є обмежені можливості: самонавчання, застосування при непередбачуваній та нечіткій мережевій активності; нерозвиненість технології прийняття рішень; погана пристосованість до роботи в реальному режимі часу [2].

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. Тому одним із варіантів усунення вказаних недоліків є розробка методу для забезпечення роботи в умовах якими характеризується МР.

Метою статті є розробка методу виявлення вторгнень в мобільних радіомережах класу MANET на основі нечіткої бази знань, який ґрунтується на нейро-нечіткій моделі ANFIS.

Викладення основного матеріалу

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 нечіткої бази знань.

Аналіз предметної області. Через динамічну топологію МР класу MANET, її СУ відносяться до складних розподілених систем, які характеризуються слабкою формалізацією залежності вхідних та вихідних змінних. В даному випадку можуть бути застосовані інтелектуальні методи забезпечення безпеки, які дозволяють відобразити нечіткість в МР.

Функціонування інтелектуальних СВЗВ ґрунтується на збиранні та переробці вхідних параметрів в знання, завдяки яким будуть прийматися управлінські рішення. Ці знання являють собою інформацію щодо функціонування інформаційної, програмної та апаратної складової МР на рівнях мережевої моделі OSI та множину правил щодо використання даної інформації. На практиці будь які дії та перетворення з цими знаннями здійснюється базою знань (БЗ).

БЗ являє собою базу даних, яка містить структуровану, подану в певному вигляді інформацію про стан компонентів МР, що використовується ПВЗВ. Особливостями БЗ є здатність: пристосованість до нечіткої

© С.В. Сальник, В.В. Сальник, Я.А. Стемпковська, 2016

мережевої активності, знаходження розбіжностей; отримання нових знань та складання висновків [3; 4].

В цілому, за способом навчання методи отримання знань поділяються на:

1. Методи навчання з учителем, де кожного прецеденту примусово задається пара „ситуація – необхідне рішення”.

2. Методи навчання без вчителя, тобто спосіб машинного навчання, під час якого досліджувана система навчається виконувати завдання, без втручання з боку користувача.

Виходячи з вказаного, для СВЗВ в МР доцільно використовувати методи навчання з учителем на етапі побудови мережі, а далі для навчання мережі необхідно використовувати методи навчання БЗ без учителя, основною рисою яких є здатність до самоорганізації.

Таким чином, нечітке моделювання процесу функціонування вузлової СВЗВ передбачає опис причинно-наслідкових зв’язків між вхідними та вихідними змінними, які характеризують залежність на кожному з рівнів моделі OSI за допомогою нечітких БЗ. Процес функціонування в даному випадку описується лінгвістичними змінними, які оцінюються якісними термами [4]. Враховуючи нечітку мережеву активність та неповноту знань щодо стану МР, які викликані масштабованістю та динамічною топологією компонентів МР, пропонується метод виявлення вторгнень з урахуванням особливостей нечіткої БЗ в СВЗВ, при комплексному застосуванні нечіткої логіки та апарату нейронних мереж (НМ) з БЗ.

Обмеження та допущення: розглядається процес функціонування вузла в режимі реального часу, в складі якого є СВЗВ, в наслідок чого маємо множину вхідних параметрів МР – змінних x_n. В складі СВЗВ знаходиться БЗ, що будується на апараті НМ та НЛ. Допускається робота МВВ в умовах чіткої та нечіткої мережевої активності, децентралізованого управління; можливості взаємодії з іншими вузлами: {Bq ={B1, B2, B3, B4}.

Необхідно: Провести удосконалення нейронечіткої моделі ANFIS для застосування її в МР класу MANET з урахуванням особливостей навчання нечіткої бази знань.

Суть розробки МВВ полягає в модифікації нейро-нечіткої моделі ANFIS, яка ґрунтується на самонавчанні БЗ при комплексному використанні НЛ та апарата НМ, розподілі процесу навчання нечіткої бази знань СВЗВ, впровадженні класифікаційного шару та можливості роботи МВВ при нечіткій та чіткій мережевій активності.

Позначення вихідних даних: Вхідний трафік, який несе в собі (мову, відео, передачу даних тощо) складається з параметрів мережевого трафіка – 41, серед яких міститься три типи ознак: символьні, логічні та числові. В якості вхідних даних застосовується параметри бази даних (БД) KDD Cup 1999 Data, які характеризують вищевказані параметри [3; 5].

На основі вхідних параметрів з’єднання відбувається перевірка на наявність заборонених з’єднань та маркування їх, як „вторгнення” або „не вторгнення”. Так як кожен тип атак характеризує множину цілей при проведенні вторгнень у МР, 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 ставить у відповідність параметри мережевого трафіка, тобто 22 типи найбільш часто застосованих атак, які поділяються на 4 категорії. Виходячи з цього категоріям атак будуть відповідати нейрони (класифікатори), класифікатор для фіксації нових типів вторгнень та еталонний класифікатор, який визначає параметри „нормального” впливу на мережу [3].

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 розглядається модель нейро-нечіткої мережі ANFIS (Adaptive-Network-Based Fuzzy Inference System). 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 НМ. Це дозволяє застосовувати для налаштування нейронечітких мереж швидкі алгоритми навчання НМ, засновані на методі зворотного поширення помилки.

Мережа ANFIS являє собою НМ 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 [6].

Умови моделі: Припустимо, що модель ANFIS яка ґрунтується на мережі Тахакі-Сугено належить до типу MISO, має 41 вхідну змінну та по два лінгвістичних правила. В заключеннях правил є рівняння першого порядку:

$$R^1: \text{If } x_1 \text{is} A_1^1 \text{and } x_2 \text{ is } A_2^1, \text{then } y^1 = a_1^1 x_1 + a_2^1 x_2 + b^1,$$

$$R^2: \text{If } x_1 \text{is} A_1^2 \text{and } x_2 \text{ is } A_2^2, \text{then } y^2 = a_1^2 x_1 + a_2^2 x_2 + b^2,$$

$$R^n: \text{If } x_1 \text{is} A_1^n \text{and } x_2 \text{ is } A_2^n, \text{then } y^n = a_1^n x_1 + a_2^n x_2 + b^n, \quad (1)$$

де $l = 1, ..., L$ – число правил моделі; $x = \{x_1, ..., x_m\}$ – виходи; y^n – виходи правила R^l; A_i^l – нечіткі

множини передумов правил, $a^l = \left(a_1^l, ..., a_m^l\right)$; b^l – параметри лінійних рівнянь в заключеннях.

Вихід такої моделі визначається за виразом:

$$y = \sum_{l=1}^{n} \alpha^l \left(a_1^l x_1 + ... + a_n^l x_2 + b^l\right) / \sum_{l=n}^{n} \alpha^l, \qquad (2)$$

де α^l – рівень істинності передумов правила R^l, що розраховується з використанням t – норми, за виразом:

$$\alpha^l = \prod_{i=1}^{m} \mu_i^l(x_i). \qquad (3)$$

Навчаєма множина має вигляд $\left\{\left[x_1^k, ..., x_m^k\right], y^k\right\}$, $k = 1, ..., K$. Тоді її похибка на навчаємій множині визначається за виразом:

$$E = \frac{1}{2} \sum_{k=1}^{K} \left(y^k - \tilde{y}^k\right)^2, \qquad (4)$$

де $\tilde{y}^k$ – вихід навчаємої множини; y^k – вихід нейро-нечіткої моделі при вході з навчаємої множини $x^k = \left[x_1^k, ..., x_m^k\right]$, яка обраховується за виразом (2); K – навчаєма множина. Функція похибки мінімізується підбором параметрів заключень правил нейронной мережі a^l, b^l та параметрів нечіткої множини A_i^l.

Виходячи із вказаного, для рішення задачі класифікації та виявлення вторгнень, навчання БЗ запропонована модифікація моделі ANFIS. Структура модифікованої моделі типу ANFIS наведена на рис. 1, а модифікована модель нейро-нечіткої мережі складатиметься з наступних шарів:

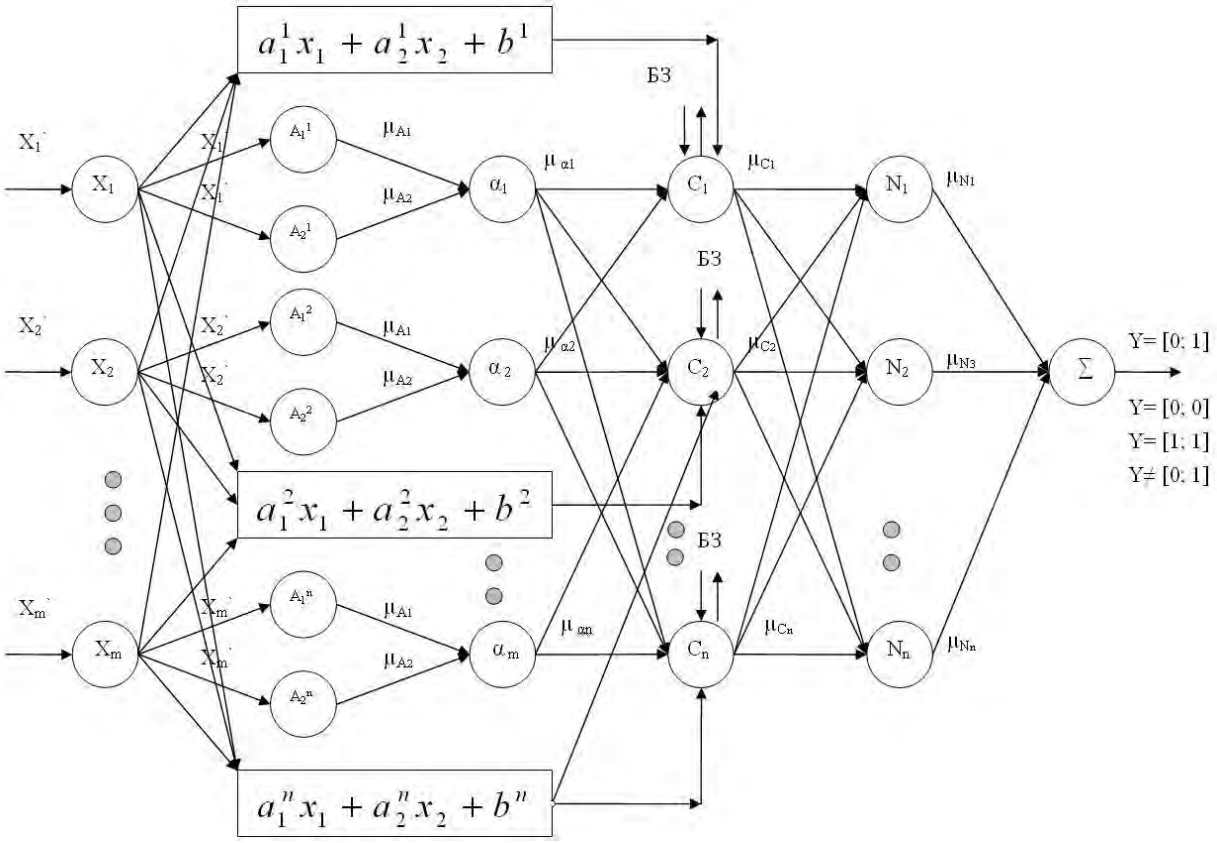

Рис. 1. Структура модифікованої моделі типу ANFIS

– перший шар – представляє собою вхідний шар (ідентифікатор), якій отримує вектор вхідних значень що характеризують 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 встановлює наявність нечіткої мережевої активності та розподіляє та надсилає вхідне значення або двома рівнозначними потоками на другий шар мережі(при нечіткій активності), або на четвертий шар (при чіткій активності).

– другий шар – виходи нейронів першого шару являють собою ступені належності вхідних значень передумовною нечіткою множиною з нейронами. Параметри нечітких множин налаштовуються в процесі навчання.

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

$$A_{im}(x_m) = \mu_{Ai}(x_m), \qquad (5)$$

де x_m – вхідний сигнал m-го елемента, A_i – лінг-

вістична 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:

$$R_m = \mu_{A1}(x_1) \times ... \times \mu_{Am}(x_m). \quad (6)$$

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

$$M = X_m = \sum_{i=1}^{m} A_{im}. \quad (7)$$

Далі етап здійснюється за кроками [7]:

– фазифікація вхідних змінних, встановлення відповідності між конкретним значенням окремої вхідної змінної системи нечіткого виводу і значенням S_n^{mk}, яке відображає ступінь істинності підумови правила на основі значення функції належності відповідного їй терма вхідної змінної:

$$S_n^{mk} = \mu_n^m(\overline{x_n}), \quad (8)$$

де $\overline{x_n}$ – вектор значень вхідних змінних системи нечіткого виводу; $\mu_n^m(\overline{x_n})$ – функція належності m-го терма;

– агрегування підумов в нечітких правилах, на якому відбувається визначення ступеню істинності умов S^{hk}, $h = \overline{1,H}$ за кожним з правил системи нечіткого виводу на основі відомих значень істинності підумов S_n^{mk}, які входять до нього. Якщо умову правила задано у формі нечіткого лінгвістичного виразу виду $x_1 = a_1^m$, $m = \overline{1,M}$, етап їх агрегування залишає ступінь істинності без зміни. Якщо ж умова правила складається з декількох підумов, степінь істинності для такого правила визначається:

$$S^{hk} = \min_n S_n^{mk}, \quad (9)$$

$$S^{hk} = \max_n S_n^{mk}, \quad (10)$$

де вираз (10) відображає логічну кон'юнкцію чи логічне „ТА" нечітких підумов, а вираз (12) – логічну диз'юнкцію чи логічне „АБО". Ті правила, ступінь істинності яких не нульова, вважаються активними і використовуються для подальших розрахунків.

У результаті виконання цієї процедури визначаються рівні „відсікання" для умов кожного з правил. Виходи вузлів цього шару позначаються:

$$\eta_h, \; h = \overline{1,H} \quad (11)$$

– активація проміжних висновків в нечітких правилах, передбачає визначення значень функції належності кожного з підвисновків для вихідних лінгвістичних змінних, які розглядаються;

$$\mu^{hk}(\overline{w_g}) = \min_h \left\{ Z_g^h, \mu_g^h(\overline{w_g}) \right\}, \quad (12)$$

де $\mu_g^h(\overline{w_g})$ – функція належності h-го терма вихідної змінної $\overline{w_g}$; Z_g^h – ступінь істинності кожного з підвисновків, що розраховується:

$$Z_g^h = S^{mk} \cdot F^k, \quad (13)$$

де F^k – ваговий коефіцієнт правила;

– акумулювання висновків нечітких правил – передбачає об'єднання і акумулювання з використанням операції max-диз'юнкції, всіх ступенів істинності підвисновків для отримання функції належності кожної із вихідних змінних:

$$\mu_g^*(\overline{w_g}) = \bigcup_{k=1}^{k_M} \bigcup_{h=1}^{H} \mu^{hk}(\overline{w_g}); \quad (14)$$

– дефазифікація вихідних змінних, полягає в тому, що на основі результатів акумуляції всіх вихідних лінгвістичних змінних отримуються чіткі значення кожної із вихідних змінних, які можуть бути використані підсистемами вузла в процесі функціонування. Відповідно до алгоритму Сугено, для дефазифікації використовується модифікований варіант в формі методу центру тяжіння для одноточкових множин:

$$w_g = \left(\sum_{h=1}^{H} Z_g^h \cdot d_g^h \right) \Big/ \left(\sum_{h=1}^{H} Z_g^h \right), \quad (15)$$

де w_g – результат дефазифікації у вигляді чіткого значення змінної; H – загальна кількість активних правил нечітких продукцій, в підвисновках яких є вихідна лінгвістична змінна d_g^h.

Після чого нейронний елемент розподіляє та надсилає вхідне значення на наступний шар.

– третій шар – являє собою збір ступенів належності вхідних параметрів відповідним нечітким правилам та визначення переможного значення рівня відповідності {висока, низька}. Рівень активізації правила підраховується за виразом:

$$\alpha^1 = \sum_{l=1}^{n} T\left(\mu_{A_1^l}(x_1), \mu_{A_n^l}(x_2) \right), \; l = 1,2. \quad (16)$$

В якості операції t – норми використовується добуток. Кількість нейронів шару R_m відповідає кількості вхідних значень параметрів. Заключення нечітких правил з визначенням переможних термів параметрів направляються на наступний шар. Переможний лінгвістичний терм параметру визначається, як оптимальне значення переможних параметрів або максимальних переможних значень:

$$R_m = \text{opt}\left\{ \max \mu_{A_m}; x_m \right\}; \quad (17)$$

– четверний шар – класифікаційний, який на основі власної БП, зв`язків з зовнішніми БЗ та у відповідності з алгоритмом навчання БЗ проводить встановлення типу поведінки на підставі чітких або нечітких параметрів даних. В даному шарі відбувається нормалізація рівнів істинності кожного правила за виразом:

$$\beta_1 = \alpha^1 / \left(\alpha^1 + \alpha^2 \right), \; l = 1,2. \quad (18)$$

Шар 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 – f ; C_5 нейрон нормальних видів поведінки – l; C_6 нейрон нововиявлених вторгнень – v.

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

$$C_K = f + l + v. \quad (19)$$

В даному шарі формується база правил (БП) вузлової СВЗВ, при виконанні наступних кроків:

– терм вхідних змінних, в якому відбувається форматування вхідних даних до нечіткого вигляду, а після цього результати проходять агрегування;

– формування початкової БП, який заснований на генерації множини правил, де максимальна кількість правил в базі визначається:

$$X = x_1 \times x_2 ... \times x_m, \quad (20)$$

де x_1, x_2, x_m – кількість функцій належності для визначення вхідних/вихідних змінних відповідно. Початкові БП ґрунтується на присвоєнні кожному з прикладів вибірки окремого правила. Кожному прикладу з навчальної вибірки ставляться у відповідність нечіткі множини з максимальними значеннями відповідності. Вони побудовані таким чином щоб множина правил становила початкову БП вузлової СВЗВ.

Особливістю підходу є формування початкової БП при невеликій кількості змінних і функцій належності, для завдання цих змінних.

– визначення рейтингу правил. БП може містити правила з однаковими передумовами і різними висновками, що призводить до надлишковості та суперечливості. З цього випливає необхідність оптимізації правил на основі емпіричних гіпотез, для уникнення надлишковості правил в БП.

В наслідок чого для кожного правила визначається його рейтинг за виразом:

$$r_i = \underset{k}{Agg}(r_i^k)(i = \overline{1, I}), \quad (21)$$

$$r_i^k = T(\mu_{a_{i1m}}(\delta_1^k), ..., \mu_{a_{inm}}(\delta_n^k), \mu_{d_{ih}}(w^k))(k = \overline{1, K}),$$

де Agg і T – оператор агрегування або норма;

– скорочення кількості правил, скорочення відбувається за групами правил, які мають однакові передумови і різні висновки. Таким чином, вирішується завдання суперечливості правил та зменшення їх кількість. Правила, що лишились, формують кінцеву базу правил вузлової СВЗВ.

Решта правила зберігають своє розміщення. Це пояснюється тим, що множина правил з більшим ступенем гранулярності не завжди дозволяє побудувати кращу модель функціонування того чи іншого об'єкту моделювання, ніж множина правил з меншим ступенем гранулярності [8];

– адаптація параметрів правил, у базі. Повністю сформованою БП можна вважати ту базу, яка пройшла адаптацію правил, які залишилися в ній після скорочення. Адаптація полягає у знаходженні, відповідно до наявних експериментальних даних і прийнятого критерію, оптимальних значень параметрів для правил з БП;

– формування груп правил шару дорівнює сумі потужностей терм-множин усіх вхідних змінних. Виходом вузлів шару є ступінь належності значення вхідної змінної відповідному нечіткому терму:

$$\mu^{a_{nm}}(X_n^*), m = \overline{1, M}, n = \overline{1, N}. \quad (22)$$

Далі відбувається підрахунок потенціалу p_i кожного нейрону в процесі виявлення вторгнення та навчання нейрона [9]. Перш за все нейронам другого шару надається потенціал:

$$p_i(0) = 1/c, \quad (23)$$

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:

$$p_i(k) = \begin{cases} p_i(k-1) + 1/c, & i \neq j; \\ p_i(k-1) - p_{min}, & i = j, \end{cases} \quad (24)$$

де j – номер „нейрона-переможця";

– п`ятий шар – виходи нейронів даного шару являють собою добуток, нормалізованих значень рівнів істинності на відповідні виходи правил:

$$y^l = \beta_1 \left(a_1^l x_1 + ... + a_n^l x_2 + b^l \right), l = 1, 2. \quad (25)$$

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;

– шостий шар – представлений одним елементом – суматором, який обраховує відповідність виявлених значень нейронами (категорій атак) нейрону (нормальної поведінки). Нейрон даного шару сумує виходи нейронів попереднього шару:

$$y^l = \beta_1 y^1 + ... + \beta_n y^n. \quad (26)$$

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.

При виявлення вторгнення, на виході суматора з`являється відповідне значення щодо виявлення впізнаного вторгнення, його класифікації та пропозицій для підсистеми реалізації рішень (на основі присвоєної терми), відносно варіантів реагування на виявлене вторгнення.

Висновок

У статті вперше представлено МВВ в МР класу MANET на основі нечіткої бази знань, який ґрунтується на нейро-нечіткій моделі ANFIS. Новизна методу, полягає у: модифікації моделі ANFIS для застосування її в МР класу MANET, проведенні самонавчання БЗ МВВ, покращенні можливостей конкурування та навчання нейронів мережі, підрахунку потенціалу нейронів мережі застосуванні нейро-нечіткого алгоритму. Вказана розробка дозволила покращити швидкість навчання нейро-нечіткої мережі, підвищити точність та швидкість виявлення вторгнень у МР, застосовувати мережу при нечіткій мережевій активності.

У ході подальших досліджень буде розроблено метод оцінки ефективності МВВ в МР класу MANET.

Список літератури

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

2. 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.

3. Сальник С.В. Метод виявлення вторгнень в мобільні радіомережі на основі нейронних мереж / С.В. Сальник, В.В. Сальник, О.А. Симоненко, О.Я. Сова. – СПб.: ВАС, 1998. – 404 с.

4. Гаврилова Т.А. Базы знаний интеллектуальных систем: учебник для вузов / Т.А. Гаврилова, В.Ф. Хорошевский. – СПб.: Питер, 2000. – 384 с.

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

6. Сальник С.В. Метод виявлення вторгнень в мобільні радіомережі класу MANET на основі гібридного нейро-нечіткого класифікатора / С.В. Сальник, В.В. Сальник, Е.М. Бовда, Д.А. Міночкін // Сучасні інформаційні технології у сфері безпеки та оборони. – 2016. – № 1. – С. 104-111.

7. Борисов В.В. Нечеткие модели и сети / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М.: Горячая линия – Телеком, 2007. – 284 с.: ил.

8. Ковтун М.В. Определение гранулярности данных таблиц фактов [Електронний ресурс] / М.В. Ковтун // Корпоративные хранилища данных. Интеграция систем. Проектная документация. – 2011. – Найменування з екрану. – Режим доступу до ресурсу: http://prj-exp.ru/dwh/granularity_of_data.php.

9. Вежневец А. Популярные нейросетевые архитектуры / А. Вежневец // Компьютерная графика и мультимедиа: сетевой журнал. – 2004. – №2 (1).

Надійшла до редколегії 22.09.2016

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

МЕТОД ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ КЛАССА MANET НА ОСНОВЕ НЕЧЕТКОЙ БАЗЫ ЗНАНИЙ

С.В. Сальник, В.В. Сальник, Я.А. Стемпковская

В статье представлен метод обнаружения вторжений в мобильных радиосетях класса MANET на основе нечеткой базы знаний, основанный на нейро-нечеткой модели ANFIS. Разработка метода заключалась в: модификации модели ANFIS для применения в мобильных радиосетях класса MANET, проведении самообучения базы знаний методов обнаружения вторжений, улучшении возможностей конкурирования и обучения нейронов сети, подсчета потенциала нейронов сети, применении нейро-нечеткого алгоритма. Указанная разработка позволила улучшить скорость обучения нейро-нечеткой сети, повысить точность и скорость обнаружения вторжений в мобильных радиосетях, а также применять сеть при нечеткой сетевой активности. Определены задачи дальнейших исследований, в которых будет разработан метод оценки эффективности методов обнаружения вторжений в МР класса MANET.

Ключевые слова: *мобильные радиосети, MANET, обеспечения безопасности мобильной радиосети, методы обнаружения вторжений, ANFIS.*

METHOD OF INTRUSION DETECTION IN MOBILE RADIO NETWORKS ON THE BASIS OF FUZZY KNOWLEDGE BASES

S.V. Salnyk, V.V. Salnyk, Y.O. Stempkovska

In article presents a method of intrusion detection in mobile radio networks class MANET based on fuzzy knowledge base based on neuro - fuzzy model ANFIS. Development method was in ANFIS model modified for use in its mobile radio networks class MANET, conduct self-knowledge base intrusion detection techniques, improved learning opportunities and compete neuronal network, calculating potential neuronal network, the use of neuro - fuzzy algorithm. The said development helped improve the speed of learning neuro-fuzzy network, improve the accuracy and speed of intrusion detection in mobile radio networks, and apply network with fuzzy network activity. Defined task for future studies that will assess effectiveness method of intrusion detection methods in the MR class MANET.

Keywords: *mobile network, MANET, mobile radio network security, intrusion detection methods, ANFIS.*