УДК 004.77.056.54 **doi: 10.32620/reks.2018.3.02**

В. В. МОСКАЛЕНКО, А. С. МОСКАЛЕНКО, М. О. ЗАРЕЦЬКИЙ

Сумський державний університет, Україна

МОДЕЛЬ І АЛГОРИТМ НАВЧАННЯ ДЕТЕКТОРА ШКІДЛИВОГО ТРАФІКУ НА ОСНОВІ МОДИФІКАЦІЇ ЗРОСТАЮЧОГО НЕЙРОННОГО ГАЗУ

Запропоновано модель ієрархічного згорткового екстрактора ознак шкідливого трафіка. На вхід моделі надходить 10-ти канальне зображення 28x28 пікселів, що сформоване на основі послідовних 10-ти потоків мережевих пакетів, що дозволяє описувати просторово-часові статистичні характеристики трафіка. Згортковий екстрактор містить два згорткові шари з тривимірними фільтрами, шари субдискретизації та шари обчислення активації на основі алгоритму ортогонального узгодженого переслідування і функції ReLU. Запропоновано модель вирішальних правил детектора шкідливого трафіка на основі інформаційно-екстремального класифікатора. Це дозволяє отримати обчислювально прості вирішальні правила і оцінити ефективність в інформаційному розумінні екстрактора ознак за умов обмеженого обсягу розміченого актуального набору навчальних даних. Класифікатор здійснює адаптивну дискретизацію ознакового опису і побудову оптимальних в інформаційному розумінні радіальнобазисних контейнерів класів в двійковому просторі Хеммінга. Як інформаційний критерій ефективності навчання розглядається модифікація міри С. Кульбака у вигляді функціоналу частоти помилок першого та другого роду. Удосконалено алгоритм зростаючого нейронного газу для попереднього навчання екстрактора ознак шляхом модифікації механізму вставки і оновлення нейронів, що дозволяє утилізувати нерозмічені навчальні зразки і отримати оптимальний розподіл нейронів для покриття навчальної вибірки. Модифікація механізму вставки нових нейронів полягає у формуванні нового нейрону за порогом досяжності, а не з заданою частотою, що дозволяє підвищити стабільність машинного навчання і регулювати ступінь узагальнення навчальної множини. Модифікація механізму оновлення вагових коефіцієнтів нейронів полягає у використанні правила Ойа замість правила Хебба, що дозволяє уникнути неконтрольованого росту вагових коефіцієнтів нейронів і адаптувати згорткові фільтри для розрідженого кодування спостережень. Для навчання вирішальних правил і тонкої настройки верхнього згорткового шару запропоновано використовувати метаевристичний пошуковий алгоритм симуляції відпалу. Результати імітаційного моделювання з використанням датасетів CTU-Mixed та CTU-13 підтверджують ефективність отриманих вирішальних правил при розпізнаванні шкідливості тестових зразків трафіку.

Ключові слова: *шкідливий мережевий трафік, зростаючий нейронний газ, згорткова нейронна мережа, розріджене кодування, інформаційний критерій*

Вступ

Існуючі системи виявлення шкідливого мережевого трафіку досі не забезпечують високої достовірності рішень, що обумовлено постійним зростанням кількості та різноманітності нових джерел шкідливого трафіку та малою кількістю актуальних розмічених даних [1, 2]. При цьому використання вручну сконструйованих ознак для опису спостережень призводить до зниження з плином часу інформативності ознакового опису та ефективності навчання вирішальних правил для детектування шкідливого трафіку [2, 3]. Тому найбільш перспективним підходом до синтезу екстрактора ознакового опису є використання ідей та методів машинного навчання ієрархічного представлення спостережень за нерозміченими даними [4, 5].

Згорткові багатошарові нейронні мережі дозволяють сформувати високорівневе інформативне ознакове подання спостережень [6]. При цьому вони вже показали високу ефективність у задачах машинного зору та аналізу часових рядів [6, 7]. Проте навчання згорткових мереж без вчителя, як правило, здійснюється на основі автоенкодера або обмеженої машини Больцмана, які потребують великий обсяг навчальних даних і тривалий час навчання для отримання прийнятного результату. У праці [8] пропонується використовувати кластер-аналіз на основі алгоритму k-середніх для навчання згорткових фільтрів. Проте k-середніх характеризується повільною збіжністю та субоптимальністю результатів внаслідок жорсткої конкурентної схеми навчання і чутливості до початкової ініціалізації кластерів.

У працях [9, 10] пропонується поєднання принципів нейронного газу та розрідженого кодування для навчання згорткових фільтрів за нерозмі-

ченими даними. Даний підхід характеризується м'якою конкурентною схемою навчання, що приводить до більш надійної збіжності алгоритму і оптимального розподілу згорткових фільтрів на вибірці фрагментів вхідних даних. При цьому вбудовування методів розрідженого кодування дозволяє підвищити завадозахищеність і узагальнюючу здатність ознакового подання. Однак кількість згорткових фільтрів задається на розсуд розробника і в загальному випадку є неоптимальною.

Необхідну кількість згорткових фільтрів в кожному згортковому шарі наперед оцінити важко, тому перспективним підходом до навчання згорткових фільтрів є використання принципів зростаючого нейронного газу, який дозволяє автоматично визначити необхідну кількість нейронів [10]. Присутність механізму додавання нових нейронів, а також видалення зайвих старих, робить алгоритм більш гнучким порівняно з класичним нейронним газом, однак він має і серйозні недоліки. Малі значення періоду між ітераціями породження нових нейронів λ призводять до нестабільності процесу навчання і викривлення утворених структур внаслідок надмірно частого додавання нових нейронів. Велике значення періоду λ забезпечує очікуваний ефект, але одночасно це призводить до значного уповільнення роботи алгоритму. Проте у працях [9, 10] було показано, що забезпечити стабільність навчання можна шляхом задавання «радіусу досяжності» нейронів, що передбачає заміну параметра λ на поріг максимального віддалення нейрону від кожної з віднесених до нього точок навчальної множини. Однак досі не було переглянуто механізми оновлення нейронів та оцінки віддаленості точок вхідного простору до нейронів з метою адаптації процесу навчання до процедури розрідженого кодування спостережень.

Крім екстрактора інформативного високорівневого ознакового опису спостережень в системі детектування шкідливого трафіку важливим компонентом є вирішальні правила, що, як правило, представляють із себе класифікатор. При цьому ефективність навчання класифікатора часто розглядається як міра ефективності навчання екстрактора ознак.

Найбільш популярним алгоритмом класифікаційного аналізу є метод опорних векторів, де тренування вирішальних правил відбувається в рамках геометричного підходу шляхом побудови у вторинному просторі ознак лінійної роздільної гіперповерхні. Проте цей алгоритм потребує багато ручних настройок для регуляризації моделі і його продуктивність залежить від складності ядерних функцій перетворення простору ознак і кількості опорних векторів [12]. У працях [13, 14] було запропоновано побудову вирішальних правил шляхом адаптивного двійкового квантування простору ознак і побудову радіально-базисних функцій в бінарному просторі Хеммінга. Такий класифікатор має високу оперативність функціонування, оскільки використовує обчислювально прості операції порівняння та "виключаючого АБО". При цьому використання популяційних алгоритмів пошуку оптимальних параметрів функціонування за інформаційним критерієм ефективності навчання дозволяє підвищити достовірність моделі даних та оперативність настройки її гіперпараметрів [14].

Таким чином, питання вибору оптимальних в інформаційному сенсі кількості та значень параметрів моделей розпізнавання вторгнень є актуальним. Його вирішення ускладнене неповною визначеністю даних, що обумовлена нестаціонарністю процесів формування шкідливого трафіку і обмеженим обсягом актуальних розмічених навчальних даних.

1. Постановка задачі

Мета статті – підвищити ефективність здатного навчатися детектора шкідливого мережевого трафіку за умов обмеженого обсягу актуальних розмічених навчальних даних.

Для досягнення поставленої мети пропонується розв'язання таких задач:

– розробити модель ієрархічного згорткового екстрактора ознак мережевого трафіку;

– розробити алгоритм попереднього навчання без вчителя моделі детектора шкідливого мережевого трафіку та алгоритм оптимізації в інформаційному розумінні його параметрів.

Дано два набори даних CTU-Mixed та CTU-13, які містять зразки нормального та шкідливого трафіку з реального мережевого середовища. Набори даних зібрані дослідниками Чешського технічного університету в період 2011-2015 рр. і записані в pcap-файли [2, 12]. Набір даних CTU-Mixed дано без метаданих розмітки, що може бути корисним для попереднього навчання екстрактора ознак без вчителя. Набір даних CTU-13 має розмітку і його можна використати для навчання вирішальних правил детектора з учителем.

Дано структурований вектор параметрів функціонування детектора шкідливого мережевого трафіку, який у загальному випадку має структуру

$$g = < e_1, ..., e_{\xi_1}, ..., e_{\Xi_1}, f_1, ..., f_{\xi_2}, ..., f_{\Xi_2} >, \qquad (1)$$

$$\Xi_1 + \Xi_2 = \Xi \ ,$$

де $< e_1, ..., e_{\xi_1}, ..., e_{\Xi_1} >$ – генотипні параметри функціонування системи інтелектуального аналізу спостережень, які впливають на параметри формування

ознакового опису спостережень;

$< f_1,...,f_{\xi_2},...,f_{\Xi_2} >$ – фенотипні параметри функціонування системи, які прямо впливають на точність детектування шкідливого трафіку.

При цьому відомі обмеження на відповідні параметри функціонування:

$$R_{\xi_1}(e_1,...,e_{\xi_1},...,e_{\Xi_1}) \le 0;\ R_{\xi_2}(f_1,...,f_{\xi_2},...,f_{\Xi_2}) \le 0.$$

Потрібно на етапі навчання детектора шкідливого трафіка отримати оптимальний вектор $\{g_\xi^* \mid \xi = \overline{1,\ \Xi_1 + \Xi_2}\}$ параметрів функціонування, який забезпечує максимум усередненого за алфавітом класів інформаційного критерію ефективності навчання

$$\overline{E}^* = \frac{1}{K}\sum_{k=1}^{K} \max_{\{s\}} E_k, \qquad (2)$$

де E_k – інформаційний критерій навчання вирішальних правил розпізнавати реалізації класу X_k^o; K – кількість класів розпізнавання; {s} – множина кроків машинного навчання.

2. Алгоритм навчання детектора шкідливого трафіку

Для розв'язання задачі розробки моделі ієрархічного згорткового екстрактора ознак в першу чергу необхідно розглянути спосіб кодування зразків трафіку в багатоканальне вхідне зображення для його аналізу згортковою нейронною мережею.

Внутрішні характеристики одиниці трафіку (потоку пакетів чи сесії) найкраще відображається у передній частині її байтів, де містяться дані про з'єднання і деякі дані контенту. Процес перетворення pcap файлу в навчальний набір даних включає три основні етапи: розділення трафіку на дискретні одиниці з урахуванням деякої гранулярності, очищення трафіку шляхом видалення пустих і дублюючих одиниць, формування навчальних зображень. При розділенні трафіку на дискретні одиниці можна розглядати такі гранулярності: TCP-з'єднання, потік, сесія, сервіс та хост. У цій роботі пропонується розділяти вхідний трафік на потоки, де ряд пакетів мають однаковий кортеж з п'яти елементів: IP-адреса джерела та отримувача, номер портів джерела і отримувача, номер протоколу. При цьому довжина потоку обмежена 784 байтами, тому довші потоки обрізаються, а коротші доповнюються нульовими байтами. Послідовні 10 потоків об'єднуються в канали вхідного зображення. В результаті маємо 10-ти канальне зображення 28x28 пікселів, що надходитиме на вхід згорткової мережі. Яскравість кожного пікселя нормалізується до діапазону [0, 1].

Як основу для побудови моделі згорткового екстрактора ознак використано відому мережу LeNet-5 [5], модифікація якої полягає в нефіксованій кількості згорткових фільтрів, кількість яких визначається під час пошарового навчання. Згорткові фільтри кожного рівня замінено на тривимірні, глибина яких рівна кількості каналів вхідного зображення для першого шару та кількості каналів карти активації – для решти. Активацію пікселя кожного каналу карти ознак пропонується обчислювати на основі алгоритму ортогонального узгодженого переслідування (Orthogonal Matching Pursuit) з функцією активації ReLU [9].

Для розв'язання задачі розробки алгоритму попереднього навчання екстрактора ознак без вчителя пропонується використання модифікації зростаючого нейронного газу. Перша модифікація полягає в заміні механізму вставки нових нейронів з заданою частотою на механізм вставки за порогом віддалення вхідного зразка до найближчого нейрону. Друга модифікація стосується механізму оновлення нейронів і полягає в реалізації правила Ойа замість правила Хебба для уникнення необмеженого росту вагових коефіцієнтів [8, 9]. При цьому навчальна вибірка для навчання фільтрів згорткової мережі формується шляхом розбиття вхідних зображень або карт активації на тривимірні патчі, що співпадають з розмірами фільтрів даного шару. Ці патчі перетворюють в одновимірні вектори і послідовно подають на вхід модифікованого алгоритму зростаючого нейронного газу, кроки якого наведено нижче:

1) ініціалізація лічильника навчальних векторів $t := 0$

2) задаються два початкові нефіксовані вузли (нейрони) w_a та w_b шляхом вибору випадковим шляхом з навчального набору і з'єднуються ребром, вік якого рівний нулю;

3) обирається з набору даних наступний вектор x, який приводиться до одиничної довжини (L2-нормалізація);

4) приведення кожного базисного вектору $w_k, k = \overline{1,M}$ до одиничної довжини (L2-нормалізація);

5) обчислення міри схожості вхідного вектору x до базисних векторів $w_{s_k} \in W$ для їх сортування

$$-(w_{s_0}^T x)^2 \le ... \le -(w_{s_k}^T x)^2 \le ... \le -(w_{s_{M-1}}^T x)^2;$$

6) обирається найближчий вузол w_{s_0} і другий за близькістю вузол w_{s_1};

7) вік усіх інцидентних w_{s_0} ребр збільшити на одиницю;

8) якщо w_{s_0} фіксований, то відбувається перехід до кроку 9, інакше до кроку 10;

9) якщо $(w_{s_0}^T x)^2 \geq v$, то переходимо до кроку 12, інакше додаємо новий нефіксований нейрон w_r в точку, що співпадає з вхідним вектором $w_r = x$, а також додається нове ребро, що з'єднує w_r та w_{s_0}, потім перехід до кроку 13;

10) вузол w_{s_0} і його топологічні сусіди (вузли, з'єднані з ним ребром) зміщуються в напрямку до вхідного вектора x згідно з правилом Ойа [9] за формулами

$$\triangle w_{s_0} = \varepsilon_b \eta_t y_0 (x - y_0 w_{s_0}),\ y_0 := w_{s_0}^T x,.$$
$$\triangle w_{s_n} = \varepsilon_n \eta_t y_n (x - y_n w_{s_n}),\ y_n := w_{s_n}^T x,.$$
$$0 < \varepsilon_b \ll 1,\ 0 < \varepsilon_n \ll \varepsilon_b,$$
$$\eta_t := \eta_0 (\eta_{final} / \eta_0)^{t/t_{max}},$$

де $\triangle w_{s_0}$, $\triangle w_{s_n}$ – вектор корекції вагових коефіцієнтів нейрона-переможця та його топологічних сусідів відповідно; ε_b, ε_n – константи сили оновлення вагових коефіцієнтів нейрона-переможця та його топологічних сусідів відповідно; $\eta_0, \eta_t, \eta_{final}$ – початкове, поточне і кінцеве значення коефіцієнту швидкості навчання відповідно.

11) якщо $(w_{s_0}^T x)^2 \geq v$, відмічаємо нейрон w_{s_0} як фіксований;

12) якщо w_{s_0} та w_{s_1} з'єднані ребром, то його вік обнуляється, в протилежному випадку між w_{s_0} та w_{s_1} формується нове ребро з нульовим віком;

13) всі ребра в графі з віком більше a_{max} видаляються і якщо деякі вузли не мають інцидентних ребр (стають ізольованими), ці вузли видаляються також;

14) якщо $t < t_{max}$ переходимо до кроку 15, інакше – інкремент лічильника кроків $t := t + 1$ і перехід до кроку 3;

15) якщо всі нейрони фіксовані, виконання алгоритму зупиняється, інакше перехід до кроку 3 і починається нова епоха навчання (повторення навчальної множини).

Навчання вирішальних правил детектора шкідливого трафіка полягає в пошуку глобального оптимуму інформаційного критерію в допустимій області його визначення. Для цього кожне вхідне спостереження кодується згортковою нейронною мережею і формується вибірка $\{x_{r,i}^{(j)} \mid i = \overline{1,N};\ j = \overline{1,n_r};\ r = \overline{1,R}\}$, де N – кількість високорівневих ознак розпізнавання; n_r – кількість навчальних зразків r-го класу; R – потужність алфавіту класів розпізнавання.

Інформаційно-екстремальний класифікатор, що оцінює належність мережевого трафіку до одного з R класів, здійснює дискретизацію ознакового опису в навчальній матриці $\{x_{r,i}^{(j)}\}$ шляхом порівняння значення i-ї ознаки з відповідними межами l-го, $l = \overline{1,L}$, одномірного рецептивного поля. Тобто формування бінарної навчальної матриці $\{b_{r,i}^{(j)} \mid i = \overline{1,N \cdot L};\ j = \overline{1,n_r};\ r = \overline{1,R}\}$ здійснюється за правилом

$$b_{r,l \cdot N+i}^{(j)} = \begin{cases} 1, & \text{if } x_{i,max}\left[1 - \delta_{i,l} / \delta_{max}\right] \leq x_{r,i}^{(j)} \leq x_{i,max}; \\ 0, & \text{otherwise.} \end{cases}$$

Обчислення значень координат двійкового еталонного вектору x_r, відносно якого відбувається побудова в радіальному базисі контейнерів класів, здійснюється за правилом

$$b_{r,l \cdot N+i} = \begin{cases} 1, & \text{if } \frac{1}{n_r}\sum_{j=1}^{n_r} b_{r,l \cdot N+i}^{(j)} > \frac{1}{R}\sum_{c=1}^{R}\frac{1}{n_c}\sum_{j=1}^{n_c} b_{c,l \cdot N+i}^{(j)}; \\ 0, & \text{otherwise.} \end{cases}$$

Як критерій ефективності машинного навчання класифікатора розглядається нормована модифікація інформаційної міри Кульбака [13] у вигляді функціоналу емпіричних частот помилок першого та другого роду

$$E_r = \frac{1 - (\alpha_r + \beta_r)}{\log_2(2 + \varsigma) - \log_2 \varsigma} \cdot \log_2 \left[\frac{2 - (\alpha_r + \beta_r) + \varsigma}{(\alpha_r + \beta_r) + \varsigma} \right], \quad (3)$$

де α_r, β_r – частота помилок першого та другого роду класифікаційних рішень щодо належності вхідних векторів до r-го класу; ς – будь-яке мале невід'ємне число, яке вводиться для уникнення невизначеності при діленні на нуль.

Допустима область визначання інформаційного критерію (3) обмежена нерівностями: $\alpha_r < 0,5$ і $\beta_r < 0,5$. При цьому, для уникнення проблеми незбалансованості класів, внаслідок переважання

зразків нормального (фонового) трафіку, альтернативним до r-го класу шкідливого трафіку є синтетичний клас. Синтетичний клас представлений з n_r зразків решти класів, найближчих до еталонного вектору b_r, де n_r є обсягом навчальної вибірки r-го класу.

Функція належності двійкового представлення b вхідного вектору x до r-го класу, оптимальний контейнер якого має еталонний вектор b_r^* та радіус d_r^*, обчислюється за формулою:

$$\mu_r(b) = \exp\left(-\sum_{i=1}^{N\cdot L} b_i \oplus b_{r,i}^* / d_r^*\right).$$

Для оптимізації вектору параметрів рецептивних полів класифікатора $\{\delta_{i,l} \mid i = \overline{1,N};\ l = \overline{1,L}\}$ та тонкої настройки екстрактора ознак пропонується використовувати метаевристичний алгоритм симуляції відпалу. Ефективність алгоритму симуляції відпалу залежить від реалізації процедури create_neighbor_solution, що здійснює формування нового рішення s_i на і-й ітерації алгоритму. На рис. 1 показано псевдокод алгоритму симуляції відпалу, що виконується epochs_max ітерацій, на кожній з яких обчислюється функція f() шляхом пропускання розміченої навчальної вибірки через модель детектора і обчислення критерію (2).

$s_{current} \leftarrow create\_initial\_solution()$
$s_{best} \leftarrow s_{current}$
$T \leftarrow T_0$
$c \leftarrow \varepsilon,\ 0 < \varepsilon < 1$
for($i = 1$ to $epochs\_max$)
  $s_i \leftarrow create\_neighbor\_solution(s_{current})$
  if $f(s_i) \geq f(s_{current})$
    $s_{current} \leftarrow s_i$
    if $f(s_i) \geq f(s_{best})$
      $s_{best} \leftarrow s_i$
    end if
  elseif $\exp\left(\frac{f(s_{current}) - f(s_i)}{T}\right) > uniform\_random(0,1)$
    $s_{current} \leftarrow s_i$
  end if
  $T \leftarrow c \times T$
end for
return(s_{best})

Рис. 1. Псевдокод метаевристичного алгоритму симуляції відпалу

Аналіз псевдокоду рис. 1 показує, що поточне рішення $s_{current}$, відносно якого шукають нові найкращі рішення s_{best}, оновлюється у випадку забезпечення новим рішенням зростання критерію (2), або випадковим шляхом із розподілу Гіббса [13]. При цьому початковою точкою пошуку, що формується за процедурою create_initial_solution, може бути або випадково згенеровано, або результатом попереднього навчання за іншим алгоритмом.

Для генерації нових рішень у процедурі create_neighbor_solution пропонується використовувати найпростіший неадаптивний алгоритм, який можна подати у вигляді формули:

$$s_{current} = s_{current} + uniform\_random(-1,1) \cdot step\_size,$$

де uniform_random – функція генерації випадкового числа з рівномірного розподілу із заданого діапазону; step_size – розмір околу пошуку нових рішень, сусідніх до $s_{current}$.

Під час навчання вирішальних правил пропонується до вектору параметрів додати і вагові коефіцієнти фільтрів останнього згорткового шару з метою врахування незбалансованості патчів, що відповідають різним класам.

Таким чином, оцінку ефективності навчання згорткового екстрактора ознак, фільтри якого навчаються на основі запропонованої модифікації зростаючого нейронного газу, буде здійснюватися за результатами інформаційно-екстремального машинного навчання.

3. Результати фізичного моделювання

Навчальна вибірка, сформована з CTU-Mixed, для навчання згорткового екстрактора ознак становить 10 000 екземплярів. Для навчання інформаційно-екстремального класифікатора сформовано по 1000 екземплярів на клас в навчальній та тестовій вибірках. В алгоритмі зростаючого розріджено кодуючого нейронного газу обрано наступні параметри $\varepsilon_b = 0,5$, $\varepsilon_b = 0,05$, $a_{max} = 100$, $\eta_0 = 1$ та $\eta_{final} = 0,01$. Параметр порогу фіксації нейронів ν та параметр кількості порогів на ознаку L системи рецептивних полів класифікатора налаштовуються шляхом перебору значень. У табл. 1 показано залежність кількості нейронів в першому M_1 і другому M_2 згорткових шарах мережі, усередненого за класами інформаційного критерію ефективності навчання $\bar{E}$ та точності за валідаційною вибіркою від параметрів ν та L.

Аналіз табл. 1 показує, що збільшення порогу ν призводить до збільшення кількості згорткових фільтрів в процесі навчання екстрактора ознак без вчителя. При цьому збільшення порогу з 0,8 до 0,9 практично не впливає на точність вирішальних правил. Тобто значення $\nu^* = 0,8$ є оптимальним і дозволяє сформувати більш компактне ознакове по-

дання (компресія), в той час як $\nu = 0,9$ дозволяє сформувати розріджене подання на основі надповного базису згорткових фільтрів.

Таблиця 1

Залежність результатів машинного навчання від параметрів моделі детектора шкідливого трафіка

ν	L	M_1	M_2	$\bar{E}$	Точність за тестовою вибіркою
0,6	1	27	41	0,36	90,0
0,7	1	45	52	0,39	91,0
0,8	1	49	300	0,42	92,0
0,9	1	320	1500	0,42	92,0
0,6	2	27	41	0,46	93,0
0,7	2	45	52	0,54	95,0
0,8	2	49	300	0,65	97,0
0,9	2	320	1500	0,65	97,0
0,6	3	27	41	0,46	93,0
0,7	3	45	52	0,55	95,2
0,8	3	49	300	0,81	98,9
0,9	3	320	1500	0,83	99,0
0,6	4	27	41	0,46	93,0
0,7	4	45	52	0,55	95,3
0,8	4	49	300	0,74	98,1
0,9	4	320	1500	0,83	99,0

Оптимальним значення гіперпараметра L рівне $L^* = 3$. Подальше збільшення параметра L не приводить до зростання точності вирішальних правил. При оптимальних параметрах екстрактора та класифікатора точність детектування шкідливого трафіку становить 98,9%.

На рис. 2 показано графік зміни максимумів усередненого за алфавітом класів інформаційного критерію (1) від кількості ітерацій пошуку за алгоритмом симуляції відпалу при $L^* = 3$ та $\nu^* = 0,8$. При цьому задано такі параметри алгоритму симуляції відпалу: c=0,998, T_0=10, epochs_max = 10000, step_size = 0,001.

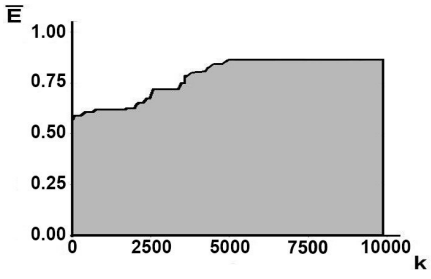
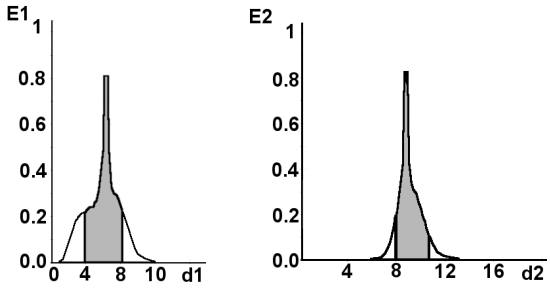


Рис. 2. Графік залежності максимального значення усередненого інформаційного критерію (2) від кількості ітерацій пошукового алгоритму

Аналіз рис. 2 показує, що алгоритму знадобилося лише 5000 ітерацій для досягнення глобального максимуму, що свідчить про інформативність ознакового опису спостережень. На рис. 3 показано залежність інформаційного критерію (2) від кодового радіусу контейнера кожного з класів.



а б

Рис. 3. Графіки залежності інформаційного критерію (2) від радіусу контейнерів класів: а – клас нормального трафіку; б – клас шкідливого трафіку

Аналіз рис. 3 показує, що максимальне значення інформаційного критерію ефективності навчання розпізнавати спостереження першого і другого класів рівні $E_1^* = 0,80$ і $E_2^* = 0,82$ відповідно. Оптимальні значення радіусів відповідних контейнерів класів розпізнавання рівні $d_1^* = 6$, $d_2^* = 10$ (в кодових одиницях). При цьому міжцентрова кодова відстань дорівнює 18, що свідчить про компактність розподілу векторів і чіткість розбиття в бінарному просторі Хемінга.

Таким чином, запропонований алгоритм навчання згорткової мережі дозволяє автоматично визначити оптимальну в інформаційному розумінні кількість нейронів на кожному згортковому рівні. При цьому результати моделювання на даних з наборів даних CTU-Mixed та CTU-13 показали придатність отриманих моделей для практичного використання.

Висновки

1. Наукова новизна одержаних результатів :

– вперше запропоновано модель ієрархічного екстрактор ознак шкідливого трафіка, на вхід якої надходить 10-ти канальне зображення 28x28 пікселів, сформоване на основі послідовних 10-ти потоків, і містить два згорткові шари з тривимірними фільтрами, шари субдискретизації та шари обчислення активації на основі алгоритму ортогонального узгодженого переслідування і функції ReLU, що дозволяє описувати просторово-часові характеристики трафіка;

– вперше запропоновано модель вирішальних правил детектора шкідливого трафіка на основі інформаційно-екстремального класифікатора, що дозволяє отримати обчислювально прості вирішальні правила і оцінити ефективність в інформаційному розумінні екстрактора ознак;

– удосконалено алгоритм зростаючого нейронного газу для попереднього навчання екстрактора ознак шляхом зміни механізму вставки і оновлення нейронів, що дозволяє утилізувати нерозмічені навчальні зразки і отримати оптимальний розподіл нейронів для покриття навчальної вибірки.

2. Практична цінність отриманих результатів для систем детектування шкідливого трафіку полягає у розробці нової моделі і методу її навчання, що дозволяє ефективно використовувати як нерозмічені так і розмічені зразки трафіку. При цьому результати імітаційного моделювання з використанням датасетів CTU-Mixed та CTU-13 підтверджують ефективність отриманих вирішальних правил при розпізнаванні шкідливості тестових зразків трафіку.

Наступні дослідження слід спрямувати на пошук оптимальних алгоритмів перетворення трафіку в багатоканальне зображення для врахування як короткострокових, так і довгострокових залежностей. Крім того в наступних дослідженнях варто розглянути підходи до налаштування параметрів алгоритму симуляції відпалу з метою підвищення оперативності машинного навчання.

Робота виконана на базі лабораторії інтелектуальних систем кафедри комп'ютерних наук Сумського державного університету при фінансовій підтримці МОН України в рамках держбюджетної науково-дослідної роботи ***ДР №0117U003934****.*

Література

1. Skrzewski, M. Flow Based Algorithm for Malware Traffic Detection [Text] / M. Skrzewski // Proceedings of the 18th Conference Computer Networks (Communications in Computer and Information Science). – Ustroń, Poland, 14–18 June, 2011. – Springer, 2011. – Vol. 160. – P. 271–280.
DOI: https://doi.org/10.1007/978-3-642-21771-5_29.

2. Malware traffic detection using tamper resistant features [Text] / Z. Berkay Celik, R. J. Walls, P. McDaniel, A. Swami // Proceedings of the IEEE MILCOM 2015 – 2015 IEEE Military Communications Conference. – Tampa, FL, 26–28 October 2015. – IEEE, 2015. – P. 330–335.
DOI: https://doi.org/10.1109/MILCOM.2015.7357464.

3. Iglesias, F. Analysis of network traffic features for anomaly detection [Text] / F. Iglesias, T. Zseby // Machine Learning. – 2015. – Vol. 101, I. 1–3. – P. 59–84. DOI: https://doi.org/10.1007/s10994-014-5473-9.

4. Autoencoder-based feature learning for cyber security applications [Text] / M. Yousefi-Azar, V. Varadharajan, L. Hamey, U. Tupakula // Proceedings of the 2017 International Joint Conference on Neural Networks (IJCNN). –Anchorage, Alaska, USA, 14–19 May 2017. – P. 3854–3861.
DOI: https://doi.org/10.1109/IJCNN.2017.7966342

5. Malware traffic classification using convolutional neural network for representation learning [Text] / W. Wang, M. Zhu, X. Zeng, X. Ye, Y. Sheng // Proceedings of the 31st International Conference on Information Networking (ICOIN 2017). – Da Nang, Vietnam, 5–8 August, 2017. – P. 712–717.
DOI: https://doi.org/10.1109/ICOIN.2017.7899588.

6. Convolutional neural networks for time series classification [Text] / B. Zhao, H. Lu, S. Chen, J. Liu, D. Wu // Journal of Systems Engineering and Electronics. – 2017. – Vol. 28, N. 1. – P. 162–169.
DOI: https://doi.org/10.21629/JSEE.2017.01.18.

7. Going deeper with convolutions [Text] / C. Szegedy, W. Liu, Y. Jia, P. Sermanet et al. // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – Boston, MA, 7–12 June, 2015. – P. 1–9.
DOI: https://doi.org/10.1109/CVPR.2015.7298594.

8. Feng, Q. Compressed auto-encoder building block for deep learning network [Text] / Q. Feng, C. L. P. Chen, L. Chen // Proceedings of the 3rd International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS). – Jinzhou, 26–29 Aug, 2016. – P. 131–136.
DOI: https://doi.org/10.1109/ICCSS.2016.7586437.

9. Labusch, K. Sparse coding neural gas: learning of overcomplete data representations [Text] / K. Labusch, E. Barth, T. Martinetz // Neurocomputing. – 2009. – Vol. 72, I. 7–9. – P. 1547–1555.
DOI: https://doi.org/10.1016/j.neucom.2008.11.027.

10. Mrazova, I. Image Classification with Growing Neural Networks [Text] / I. Mrazova, M. Kukacka // International Journal of Computer Theory and Engineering. – 2013 – Vol. 5, N. 3. – P. 422–427.
DOI: https://doi.org/10.7763/IJCTE.2013.V5.722.

11. Palomo, E. J. The Growing Hierarchical Neural Gas Self-Organizing Neural Network [Text] / E. J. Palomo, E. López-Rubio // IEEE Transactions on Neural Networks and Learning System. – 2017. –Vol. 28, N. 9. – P. 2000–2009.
DOI: https://doi.org/10.1109/TNNLS.2016.2570124.

12. Deep learning of support vector machines with class probability output networks [Text] / S. Kim, Z. Yu, R. Man Kil, M. Lee // Neural Networks. – 2015. – Vol. 64. – P. 19–28.
DOI: https://doi.org/10.1016/j.neunet.2014.09.007.

13. Dovbysh, A. S. Information-extreme learning algorithm for a system of recognition of morphological images in diagnosing oncological pathologies [Text] / A. S. Dovbysh, M. S. Rudenko // Cybernetics and Systems Analysis. – 2014. – Vol. 50, I. 1. – P. 157–162. DOI: https://doi.org/10.1007/s10559-014-9603-y.

14. Moskalenko, V. Optimizing the parameters of functioning of the system of management of data center IT infrastructure [Text] / V. Moskalenko, S. Pimonenko // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 5, I. 2 (83). – P. 21–29. DOI: https://doi.org/10.15587/1729-4061.2016.79231

References

1. Skrzewski, M. Flow Based Algorithm for Malware Traffic Detection. *Proc. of the 18th Conference Computer Networks (Communications in Computer and Information Science)*, Ustroń, Poland, 2011, vol. 160, pp. 271–280.
DOI: https://doi.org/10.1007/978-3-642-21771-5_29.

2. Berkay Celik, Z., Walls, R. J., McDaniel, P., Swami, A. Malware traffic detection using tamper resistant features. *Proc. of the IEEE MILCOM 2015 – 2015 IEEE Military Communications Conference*, Tampa, FL, 2015, pp. 330–335.
DOI: https://doi.org/10.1109/MILCOM.2015.7357464.

3. Iglesias, F., Zseby, T. Analysis of network traffic features for anomaly detection. *Machine Learning,* 2015, vol. 101, i. 1–3, pp. 59–84.
DOI: https://doi.org/10.1007/s10994-014-5473-9.

4. Yousefi-Azar, M., Varadharajan, V., Hamey, L., Tupakula, U. Autoencoder-based feature learning for cyber security applications. *Proc. of the 2017 International Joint Conference on Neural Networks (IJCNN).* Anchorage, Alaska, USA, 2017, pp. 3854–3861.
DOI: https://doi.org/10.1109/IJCNN.2017.7966342.

5. Wang, W. Zhu, M., Zeng, X., Ye, X., Sheng, Y. Malware traffic classification using convolutional neural network for representation learning. *Proc. of the 31st International Conference on Information Networking (ICOIN 2017).* Da Nang, Vietnam, 2017, pp. 712–717.
DOI: https://doi.org/10.1109/ICOIN.2017.7899588.

6. Zhao, B., Lu, H., Chen, S., Liu, J., Wu,D. Convolutional neural networks for time series classification. *Journal of Systems Engineering and Electronics*, 2017, vol. 28, no. 1, pp. 62–169.
DOI: https://doi.org/10.21629/JSEE.2017.01.18.

7. Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., Rabinovich, A. Going deeper with convolutions. *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, 2015, pp. 1–9.
DOI: https://doi.org/10.1109/CVPR.2015.7298594.

8. Feng, Q. Chen, C. L. P., Chen, L., Compressed auto-encoder building block for deep learning network. *Proc. of the 3rd International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS)*, Jinzhou, 2016, pp. 131–136.
DOI: https://doi.org/10.1109/ICCSS.2016.7586437.

9. Labusch, K., Barth, E., Martinetz, T. Sparse coding neural gas: learning of overcomplete data representations. *Neurocomputing*, 2009, vol. 72, i. 7–9, pp. 1547–1555.
DOI: https://doi.org/10.1016/j.neucom.2008.11.027.

10. Mrazova, I., Kukacka, M. Image Classification with Growing Neural Networks. *International Journal of Computer Theory and Engineering*, 2013, vol. 5, no. 3, pp. 422–427.
DOI: https://doi.org/10.7763/IJCTE.2013.V5.722.

11. Palomo, E. J., López-Rubio, E. The Growing Hierarchical Neural Gas Self-Organizing Neural Network. *IEEE Transactions on Neural Networks and Learning System*, 2017, vol. 28, no. 9, pp. 2000–2009.
DOI: https://doi.org/10.1109/TNNLS.2016.2570124.

12. Kim, S., Yu, Z., Man Kil, R., Lee, M. Deep learning of support vector machines with class probability output networks. *Neural Networks*, 2015, vol. 64, pp. 19–28.
DOI: https://doi.org/10.1016/j.neunet.2014.09.007.

13. Dovbysh, A. S., Rudenko, M. S. Information-extreme learning algorithm for a system of recognition of morphological images in diagnosing oncological pathologies. *Cybernetics and Systems Analysis*, 2014, vol. 50, i. 1, pp. 157–162.
DOI: https://doi.org/10.1007/s10559-014-9603-y.

14. Moskalenko, V., Pimonenko, S. Optimizing the parameters of functioning of the system of management of data center IT infrastructure. *Eastern-European Journal of Enterprise Technologies*, 2016, vol. 5, i. 2 (83), pp. 21–29.
DOI: https://doi.org/10.15587/1729-4061.2016.79231.

Поступила в редакцию 27.06.2018, рассмотрена на редколлегии 12.09.2018

МОДЕЛЬ И МЕТОД ОБУЧЕНИЯ ДЕТЕКТОРА ВРЕДОНОСНОГО ТРАФИКА НА ОСНОВЕ МОДИФИКАЦИИ РАСТУЩЕГО НЕЙРОННОГО ГАЗА

В. В. Москаленко, А. С. Москаленко, М. О. Зарецький

Предложена модель иерархического свёрточного экстрактора признаков вредоносного трафика. На вход модели поступает 10-ти канальное изображение 28x28 пикселей, сформированное на основе последовательных 10-ти потоков сетевых пакетов, что позволяет описывать пространственно-временные статистические характеристики трафика. Свёрточный экстрактор содержит два свёрточных слоя с трёхмерными фильтрами, слои субдискретизации и слои вычисления активации на основе алгоритма ортогонального согласованного преследования и функции ReLU. Предложена модель решающих правил детектора вредоносного трафика на основе информационно-экстремального классификатора. Это позволяет получить вычислительно простые решающие правила и оценить эффективность в информационном смысле экстрактора признаков в условиях ограниченного объёма размеченного актуального набора обучающих данных. Классифи-

катор осуществляет адаптивную дискретизацию признакового описания и построение оптимальных в информационном смысле радиально-базисных контейнеров классов в двоичном пространстве Хемминга. Как информационный критерий эффективности обучения рассматривается модификация меры С. Кульбака в виде функционала частоты ошибок первого и второго рода. Усовершенствован алгоритм растущего нейронного газа для предварительного обучения экстрактора признаков путем модификации механизма вставки и обновления нейронов, что позволяет утилизировать неразмеченные обучающие образцы и получить оптимальное распределение нейронов для покрытия обучающей выборки. Модификация механизма вставки новых нейронов заключается в формировании нового нейрона за порогом досягаемости, а не с заданной частотой, что позволяет повысить стабильность машинного обучения и регулировать степень обобщения обучающего множества. Модификация механизма обновления весовых коэффициентов нейронов заключается в использовании правила Ойа вместо правила Хебба, что позволяет избежать неконтролируемого роста весовых коэффициентов нейронов и адаптировать свёрточные фильтры для разреженного кодирования наблюдений. Для обучения решающих правил и тонкой настройки верхнего свёрточного слоя предложено использовать метаэвристический поисковый алгоритм симуляции отжига. Результаты имитационного моделирования с использованием датасета CTU-Mixed и CTU-13 подтверждают эффективность полученных решающих правил при распознавании вредоносности тестовых образцов трафика.

Ключевые слова: вредоносный сетевой трафик, растущий нейронный газ, свёрточная нейронная сеть, разреженное кодирование, информационный критерий.

MODEL AND TRAINING ALGORITHM OF MALWARE TRAFFIC DETECTOR BASED ON MODIFICATION OF GROWING NEURAL GAS

V. V. Moskalenko, A. S. Moskalenko, N. O. Zaretsky

It is proposed the model of the hierarchical convolutional extractor of malware traffic features. Image with resolution 28x28 pixels and 10-th channels formed on the basis of successive 10 network packet flows is considered as model input. It allows to describe the spatial-temporal statistical characteristics of the traffic. The feature extractor consists of two convolutional layers with three-dimensional filters, sub-sampling layers, and activation calculation layers based on the orthogonal matching pursuit algorithm and the ReLU function. It is proposed the model of decision rules of the malware traffic detector based on information-extreme classifier. It allows to receive computatially simple decision rules and evaluate the informational efficiency of the feature extractor in the condition of the limited volume of the relevant labeled training dataset. The classifier performs an adaptive feature discretization and construction of the optimal in the information sense of radial-basis containers of classes in binary Hamming space. An information criterion of learning efficiency is the modification of S. Kulbak's measure as a function of the frequency of errors of the first and second type. Growing neural gas algorithm for pretraining of the feature extractor is improved by modifying the mechanism of insertion and updating of neurons. It allows utilizing unlabeled training samples and obtaining the optimal distribution of neurons to cover the training sample. Modification of the mechanism of insertion of new neurons is to form a new neuron at the reach of the threshold, and not with a given frequency. It allows you to improve the stability of the learning process and regulate the generalization ability of the model. The modification of the mechanism for updating the weighting coefficients of the neurons is to use the of Oja's rule instead of the Hebb's rule, which allows to avoid uncontrolled growth of neuron weights and adapts convolutional filters for sparse coding of input observation. It is proposed meta-heuristic search algorithm of simulated annealing for the training of decision rules and fine-tuning high-level filters of feature extractor. Simulation results using CTU-Mixed and CTU-13 datasets confirm the effectiveness of the resulting decision rules for recognizing the malware traffic from test samples.

Keywords: malware network traffic, growing neural gas, convolutional neural network, sparse coding, information criterion

Москаленко В'ячеслав Васильович – канд. техн. наук, доцент каф. комп'ютерних наук, Сумський державний університет, Суми, e-mail: v.moskalenko@cs.sumdu.edu.ua.

Москаленко Альона Сергіївна – канд. техн. наук, асистент каф. комп'ютерних наук, Сумський державний університет, Суми, e-mail: a.moskalenko@cs.sumdu.edu.ua, alenarizhova@gmail.com.

Зарецький Микола Олександрович – аспірант каф. комп'ютерних наук, Сумський державний університет, e-mail: n.zaretskij@gmail.com.

Moskalenko Viacheslav Vasilyovich – PhD, associate professor of Computer Sciences Department of Sumy State University, Sumy, e-mail: v.moskalenko@cs.sumdu.edu.ua.

Moskalenko Alyona Sergiyvna – PhD, teaching assistant of Computer Sciences Department of Sumy State University, Sumy, e-mail: a.moskalenko@cs.sumdu.edu.ua, alenarizhova@gmail.com.

Zaretsky Nikolay Olexandrovich – PhD student of Computer Sciences Department of Sumy State University, e-mail: n.zaretskij@gmail.com.