УДК 004.89

Мирослав Комар
Тернопільський національний економічний університет, Україна

АЛГОРИТМИ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ

Myroslav Komar

ALGORITHMS OF ARTIFICIAL NEURAL NETWORKS FOR NETWORK INTRUSION DETECTION

В роботі представлені алгоритми функціонування системи виявлення мережевих вторгнень, де основним елементом виявлення атаки є нейромережевий детектор. В якості нейромережевого детектора вибрана багатошарова нейронна мережа з одним прихованим шаром, що складається з нейронів Кохонена. Для навчання шару Кохонена використовується конкурентний метод навчання. Алгоритм навчання шару Кохонена:

1. Випадкова ініціалізація вагових коефіцієнтів ω_{ci} нейронів Y_i шару Кохонена.

2. Розподіл вхідного образу з навчальної вибірки на нейронну мережу та обчислення наступних параметрів:

a) обчислюється Евклідова відстань між вхідним образом і ваговими векторами нейронних елементів шару Кохонена

$$D_i = |X - \omega_i| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + (X_n - \omega_{ni})^2}, \quad (1)$$

де $i = \overline{1, m}.$

b) визначається нейронний елемент переможець з номером k

$$D_k = \min_j D_j. \quad (2)$$

c) проводиться модифікація вагових коефіцієнтів нейрона-переможця у відповідності з наступними виразами:

$$\omega_{ck}(t+1) = \omega_{ck}(t) + \gamma (X_c - \omega_{ck}(t)), \quad (3)$$

якщо при подачі на вхід мережі легітимного з'єднання переможцем є один з перших f нейронів або при подачі на вхід мережі шкідливого фрагмента переможцем є один з l останніх нейронів мережі Кохонена. Інакше:

$$\omega_{ck}(t+1) = \omega_{ck}(t) - \gamma (X_c - \omega_{ck}(t)). \quad (4)$$

Процес повторюється для всіх вхідних образів, починаючи з пункту 2.

3. Навчання проводиться до бажаного ступеня узгодження між вхідними і ваговими векторами.

Розглянемо алгоритм функціонування системи:

1. Витягування атрибутів із встановленого мережевого з'єднання.

2. Подача атрибутів мережевого з'єднання на j-й нейромережевий детектор.

3. Якщо вихідне значення j-го нейромережевого детектора дорівнює $Y_j=1$, то мережеве з'єднання вважається забороненим і блокується. Користувачеві видається повідомлення про виявлення типу атаки. Якщо вихідне значення нейромережевого детектора дорівнює $Y_j=0$, то атрибути з'єднання подаються на наступний детектор.

4. Кроки 2 і 3 повторюються до тих пір, поки всі детектори системи не перевірять мережевий трафік. Якщо вихідні значення всіх детекторів дорівнюють нулю, то з'єднання вважається легітимним.

Для тестування розробленої системи проведений ряд експериментів, які доводять ефективність запропонованих алгоритмів.