ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

Методи виявлення вторгнень на основі алгоритмів нейронної мережі

Кваліфікаційна робота
Другий (магістерський) рівень

Автор:
Тимофєєв Д.І.,
студ. гр. КСМм-20-1

Керівник:
Горбачов В.О.,
проф. каф. ЕОМ

1

Мета роботи

Метою роботи:

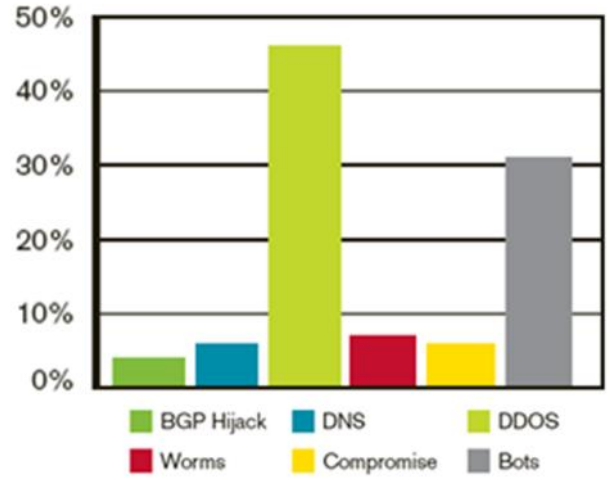
- розробка методу виявлення атак з підвищеною ефективністю;
- порівняння ефективності запропонованого методу з існуючими альтернативами.

2

Задачі роботи

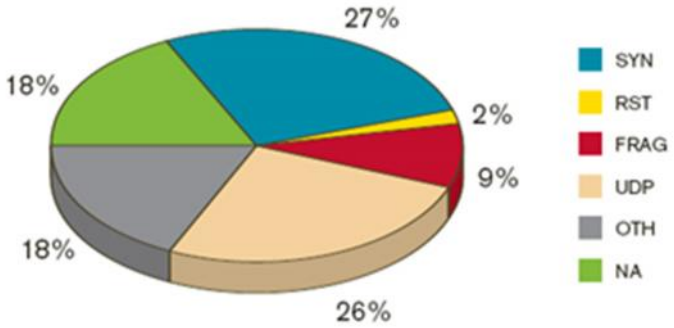
1. Розглянути існуючі методи протидії DoS-атакам в комп'ютерних мережах.
2. Оцінити ефективність методу протидії DoS-атакам на базі комбінації нейронних алгоритмів
3. Порівняти ефективності запропонованого методу з існуючими альтернативами

Найбільш істотні загрози



Source: Arbor Networks Inc.

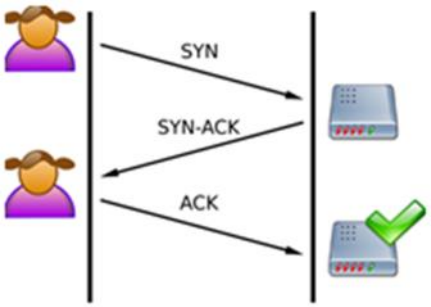
Типи атак відмови в обслуговуванні



Source: Arbor Networks Inc.

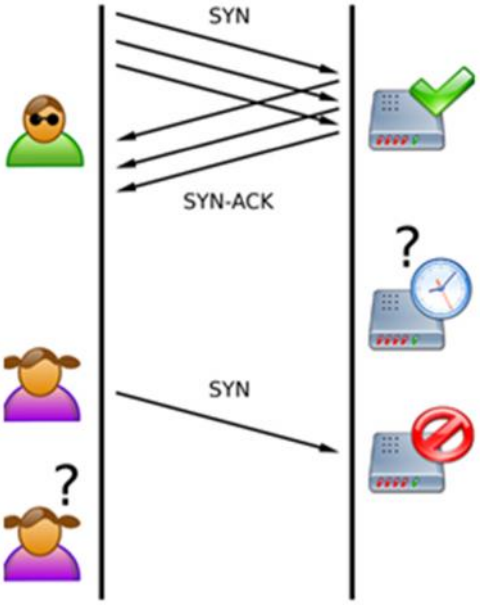
5

Що означає SYN атака?



Звичайне з'єднання між користувачем і сервером. Тристороннє рукостискання виконано правильно.

6



Зловмисник надсилає багато пакетів, але не надсилає «ACK» назад на сервер.

Таким чином, з'єднання напіввідкриті і споживають ресурси сервера.

Законний користувач намагається підключитися, але сервер відмовляється відкривати з'єднання, що призводить до відмови в обслуговуванні.

7

Переваги застосування нейронних мереж

Переваги НМ для IDS:

- НМ може тренуватися під час реальної роботи;
- можливість аналізувати дані з мережі, навіть якщо вони неповні та/або пошкоджені;
- можливість тренувати поведінку атак і розділення компонентів, які відрізняються від раніше відомих;
- висока швидкість обробки даних.

8

Метод що використовується

Запропонований метод базується на комбінації відомих і широко використовуваних алгоритмів нейронних мереж:

- самоорганізуючі карти (Self-Organizing Maps) (SOM) – основа цього алгоритму полягає в тому, що вхідні дані розподіляються на дві групи: «атаки» та «звичайні»;
- алгоритм навчання векторного квантування (Learning Vector Quantization) (LVQ), який використовується для більш точного налаштування результатів, отриманих шляхом застосування SOM алгоритму.

9

Самоорганізуючі карти (Self-Organizing Maps) (SOM)

- **Вектор вагових коефіцієнтів:**

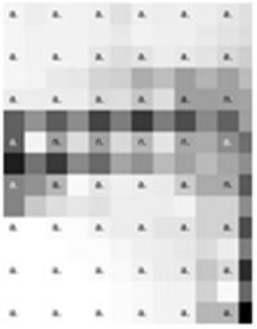
$$\omega_{ij} = [\omega_{ij1}, \omega_{ij2}, \ldots, \omega_{ijN}]$$

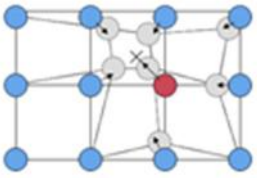
- **Визначення переможця:**

$$d(x, \omega_{ij}) = \|x - \omega_{ij}\| = \sqrt{\sum_{k=1}^{N} (x_k - \omega_{ijk})^2}$$

- **Правило адаптації вагових коефіцієнтів:**

$$\omega_{ij}(t+1) = \omega_{ij}(t) + \eta(t) G(i, \omega)(x - \omega_{ij}(t))$$





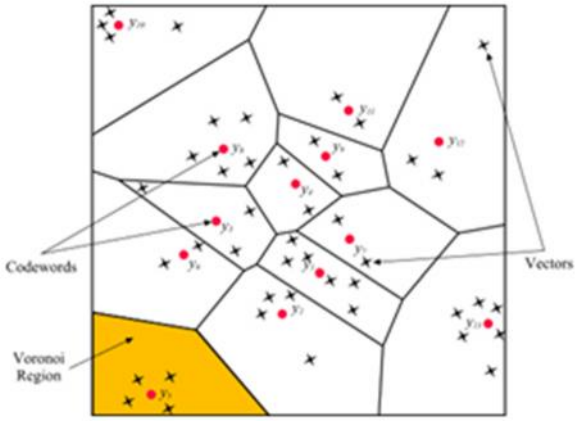
10

Навчання векторного квантування (Learning Vector Quantization) (LVQ)

Адаптація вагових коефіцієнтів:

$$\omega_{ij}(t+1) = \omega_{ij}(t) + \lambda(t)(x - \omega_{ij}(t))$$

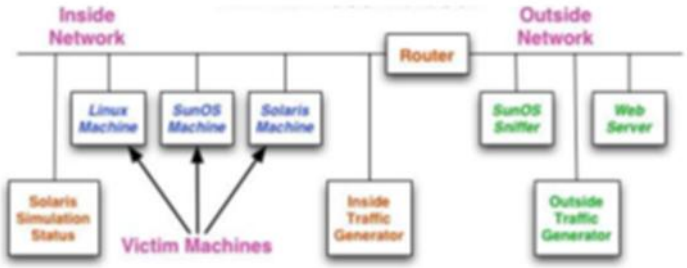
$$\omega_{ij}(t+1) = \omega_{ij}(t) - \lambda(t)(x - \omega_{ij}(t))$$



11

Набір даних KDD CUP'99

Мережа моделювання для набору даних DARPA (the Defense Advanced Research Projects Agency) 1998



Набір даних було компановано з TCP пакетів під час дослідження DARPA

12

Записи наборів даних KDD CUP'99

- Необроблений запис з'єднання:

  0,tcp,http,SF,181,5450,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,
  0.00,0.00,9,9,1.00,0.00,0.11,0.00,0.00,0.00,0.00,0.00, normal

- Попередньо оброблений запис з'єднання:

  19 20 0.00 0.00 0.00 0.00 1.00 0.00 0.10 255 255 1.00 0.00 0.00 0.00 0.00 0.00
  0.00 0.00 normal

13

Оціночні властивості

- результати оцінки порівнювалися з результатами, отриманими за допомогою чистого алгоритму SOM;
- для отримання систематичних оцінок була використана перехресна перевірка для чистого SOM та комбінації алгоритмів нейронних мереж.

14

Результати оцінки

Підсумковий результат класифікації показників успішності методів

	1	2	3	4	5	6	7	8	9	10	%
Комбінація алгоритмів	99.3	98.8	99.1	99.2	98.5	99.8	99.2	99	98.9	98.9	**99%**
SOM	97	97.8	96.2	96.7	97.5	97	97.2	96.7	96.8	96.9	**97%**

15

ВИСНОВКИ

- Запропонований метод добре справляється з проблемою виявлення атак «Відмова в обслуговуванні».
- У порівнянні з конкурентом і перевіреним алгоритмом чистих самоорганізуючих карт представлений метод має кращі характеристики.

16

ДОДАТОК Б

Спеціальні скрипти обробки даних

Лістинг 1.1 – Сценарій підготовки даних

```
     sed 's/,/ /g' $1 | awk '/normal|neptune|smurf/' |awk '{print
$23, $24, $25, $26, $27, $28, $29, $30, $31, $32, $33, $34, $35,
$36, $37, $38, $39, $40, $41, $42}' > $2
```

Лістинг 1.2 – Сценарій вилучення даних

```
     #!/bin/bash
     out_str_numbers=$1
     in_str_numbers=`sed -n '$=' $2`
     filename=$3

     touch $filename
     for i in `seq 1 $out_str_numbers`;
          do
               rand_str=`head -c4 /dev/urandom | od -N4 -tu4 |
sed -ne '1s/.* //p'`
               let "rand_str%=$in_str_numbers"
               sed ''$rand_str'q;d' $2 >> $filename
               echo $i
          done
```

Лістинг 1.3 – Навчальний сценарій нейронної мережі

```
     #!/bin/bash
     som_dat=$1
     lvq_dat=$2
     echo 'map initialization'
     randinit -xdim 10 -ydim 10 -din $som_dat -cout map.cod -
neigh gaussian -topol rect
     echo 'map training with SOM'
     vsom -din $som_dat -cin map.cod -cout map.som -rlen 20000 -
alpha 1 -radius 10
     rm -f map.cod
     echo 'map tuning with LVQ'
     setlabel -din $som_dat -cin map.som -cout map.knn -knn 1
     lvq1 -din $lvq_dat -cin map.knn -cout map.lvq -alpha 0.5 -
rlen 5000
     echo 'finished'
```

Лістинг 1.4 – Скрипт тестування нейронної мережі

```
#!/bin/bash
echo 'map trained with SOM algorithm'
qerror -din $1 -cin map.knn
accuracy -din $2 -cin map.knn
echo 'map trained with SOM algorithm plus LVQ tuning'
qerror -din $1 -cin map.lvq
accuracy -din $2 -cin map.lvq
```