УДК 621.391:007

Э. Д. Аведьян[1, 2, 3], д-р техн. наук, гл.-науч. сотр.[1], зам нач.[2], профессор[3], e-mail: avedian@mail.ru,
Т. Ч. Л. Ле[3], аспирант, e-mail: tranglinh2011@gmail.com
[1]Центр информационных технологий и систем органов исполнительной власти, Москва
[2]Международный центр по информатике и электронике, Москва
[3]Московский физико-технический институт, Москва

Двухуровневая система обнаружения DoS-атак и их компонентов на основе нейронных сетей CMAC

Приведены результаты применения системы нейронных сетей CMAC (НС CMAC) для обнаружения DoS-атак и их компонентов, выполненные на всех записях базы данных атак KDD Cup 99. Система состоит из двух уровней. Верхний уровень предназначен для обнаружения DoS-атак с помощью обученной НС CMAC, нижний уровень — для выделения из обнаруженных DoS-атак шести их компонентов: Back, Neptune, Land, Pod, Teardrop и Smurf с помощью шести обученных НС CMAC. Ошибка пропуска DoS-атаки и ложной тревоги не превышает 0,2 %.

Ключевые слова: *обнаружение DoS-атак, нейронная сеть CMAC, база данных атак KDD Cup 99, компоненты DoS-атак*

Введение

В работах Дж. Кеннеди [1] приведены результаты, которые показывают, что в качестве классификатора DoS-атак на информационные ресурсы может быть успешно использована нейронная сеть CMAC (НС CMAC). В этой же работе подчеркивается, что НС CMAC послужит аналитическим компонентом создаваемой полномасштабной интегрированной системы обнаружения атак. К сожалению, результаты создания подобной системы не опубликованы. Следует также отметить, что в работе [1] отсутствует важная информация об используемых автором признаках атак, параметрах НС CMAC, обучающей и тестовой последовательностях, которая позволила бы воспроизвести описанные результаты моделирования. В работе [2] была предпринята попытка подтвердить или опровергнуть утверждения Дж. Кеннеди [1] о возможности успешного применения НС CMAC в качестве классификатора DoS-атак, для чего была разработана и описана технология обнаружения DoS-атак на основе НС CMAC. С помощью этой технологии проведено обучение и тестирование нейронной сети по обнаружению DoS-атак на записях базы данных атак KDD Cup 99. Результаты тестирования системы продемонстрировали высокую вероятность обнаружения DoS-атак и подтвердили утверждение Дж. Кеннеди [1] о том, что НС CMAC может быть успешным классификатором DoS-атак.

В данной работе приведены новые результаты по применению системы нейронных сетей CMAC для обнаружения как DoS-атак, так и их компонентов, выполненные на всех данных базы атак KDD Cup 99 [3]. Система обнаружения состоит из двух уровней. Верхний уровень предназначен для обнаружения DoS-атак с помощью обученной НС CMAC так, как это реализовано в работе [2] с использованием уточненного набора из пяти признаков трафика. Нижний уровень предназначен для выделения из обнаруженных DoS-атак шести их компонентов: Back, Neptune, Land, Pod, Teardrop и Smurf [4]. Выделение указанных компонентов выполняется с помощью шести обученных НС CMAC, в каждой из которых используется свой набор, состоящий из двух признаков трафика. Высокая точность обнаружения как DoS-атак, так и их компонентов достигнута в результате оптимизации параметров нейронных сетей CMAC, входящих в систему обнаружения.

Цель настоящей статьи — описание важнейших моментов, которые следует учитывать при использовании НС CMAC при решении задачи обнаружения атак, и иллюстрация применения НС CMAC на примере обнаружения DoS-атак и их компонентов.

1. Постановка задачи и состав базы данных атак KDD Cup 99

Задача, которая рассматривается в настоящей работе, заключается в создании обучающейся системы обнаружения DoS-атак и их компонентов, основными аналитическими элементами которой являются нейронные сети CMAC.

Как отмечалось выше, обучение и тестирование системы выполнено на всем наборе записей о сетевых соединениях, которые имеются в общедоступной базе данных атак KDD Cup 99 [3], общее число которых равно 4 898 431. Поскольку, однако, данную базу данных характеризует избыточный характер [5], то в ней удалены повторы, в результате чего объем данных для обучения и тестирования в сжатой базе данных составил 1 074 992 записей, из которых 247 267 записей являются DoS-атаками. Каждая запись состоит из 41 признака сетевого трафика трех типов: символьные, логические и

числовые. Последний 42-й элемент записи содержит информацию о том, к какому одному из пяти классов относится соединение (нормальное соединение и четыре вида атак):

1. *Denial of Service* (DoS) — отказ в обслуживании, при котором происходит генерация большого объема трафика, в результате чего происходит перегрузка сервера и пользователи не могут получить доступ к предоставляемым вычислительной системой ресурсам.

2. *Remote to User* (R2L) — доступ незарегистрированного пользователя к компьютеру со стороны удаленной машины.

3. *User to Root* (U2R) — получение зарегистрированным пользователем привилегий администратора.

4. *Probing* — сканирование портов в целях получения конфиденциальной информации.

Отметим, что при этом каждый из перечисленных видов атак включает в себя несколько компонентов. Для DoS-атак, которые и являются в настоящей работе объектами обнаружения, такими компонентами в базе данных KDD Cup 99 являются атаки [4] Back, Neptune, Teardrop, Land, Pod и Smurf.

Back-атака. Нападающий отправляет запросы на Apache веб-сервер с URL, перед которым стоит большое число слешей. Сервер, пытаясь обработать эти запросы, замедляется и оказывается неспособным обработать другие запросы.

Neptune-атака (SYN Flood). Атакующий посылает на сервер жертвы запросы с открытым флагом SYN, игнорируя и не отвечая на ответные пакеты (режим полуоткрытого соединения). В результате на сервере происходит переполнение очереди на подключение, и он оказывается неспособным отвечать на запросы пользователей.

Teardrop-атака. Атака отказа в обслуживании, которая эксплуатирует недостаток в реализации старых стеков TCP/IP. Некоторые реализации кода повторной сборки фрагментированных IP-пакетов на этих платформах не обрабатывают должным образом пересекающиеся IP-фрагменты, в результате чего возникает необходимость в перезагрузке сервера.

Land-атака. Атакующий посылает сфальсифицированный пакет SYN, в котором адрес источника совпадает с адресом получателя. В результате сервер оказывается полностью заблокированным, и для восстановления требуется физически его выключить и вновь включить.

Pod-атака (Ping of death). Компьютер-жертва получает от атакующего подделанный эхо-запрос (*ping*), размер которого превышает допустимый. В результате компьютер-жертва вообще перестает отвечать на запросы. Современные операционные системы защищены от этого вида атак.

Smurf-атака. Атакующий посылает пакеты эхо-запроса ICMP по широковещательному адресу посредника, в котором адрес отправителя заменен на адрес жертвы. Большое число компьютеров посредника в ответ посылают пакеты по адресу жертвы, что приводит к выходу из строя сервера жертвы.

Таблица 1

Состав DoS-атак в сжатой БД KDDCup 99

№	Компоненты DoS-атак	Число записей компонентов
1	Back	968
2	Neptune	242 149
3	Teardrop	918
4	Land	19
5	Pod	206
6	Smurf	3007
Итого		247 267

Число неповторяющихся компонентов DoS-атак в базе данных KDD Cup 99 приведено в табл. 1.

2. Структура системы обнаружения DoS-атак и их компонентов

Система обнаружения DoS-атак и их компонентов имеет двухуровневую структуру, верхний уровень которой предназначен для обнаружения DoS-атак, нижний уровень — для отнесения обнаруженной DoS-атаки к тому или иному компоненту. Элементами обнаружения являются обученные нейронные сети CMAC. Структура системы обнаружения представлена на рис. 1.

Система функционирует следующим образом. Из базы данных KDD Cup 99 извлекается запись о сетевом соединении, содержащая значения 41 признака. Из записи выделяют пять признаков с номерами {3, 4, 5, 23, 30}, названия которых приведены в табл. 2.

Значения этих признаков квантуются, принимая целочисленные значения, и в таком виде поступают на вход обученной распознаванию DoS-атак НС CMAC. По реакции нейронной сети принимается решение о наличии или отсутствии DoS-атаки. Если система принимает решение о наличии DoS-атаки, то данная запись поступает на вход второго уровня системы, в котором находятся обученные распознаванию компонентов DoS-атак шесть НС CMAC. Из записи выделяются значения признаков компонентов DoS-атак с номерами:

Таблица 2

Названия признаков для обнаружения DoS-атак

Номер признака	Название признака	Описание признака
3	Service	Служба
4	Flag	Флаг состояния соединения
5	Source byte	Число байтов, переданных от источника к месту назначения
23	Count	Число соединений на одном хосте текущего соединения в течение последних 2 с
30	Diff srv rate	% подключений к различным услугам

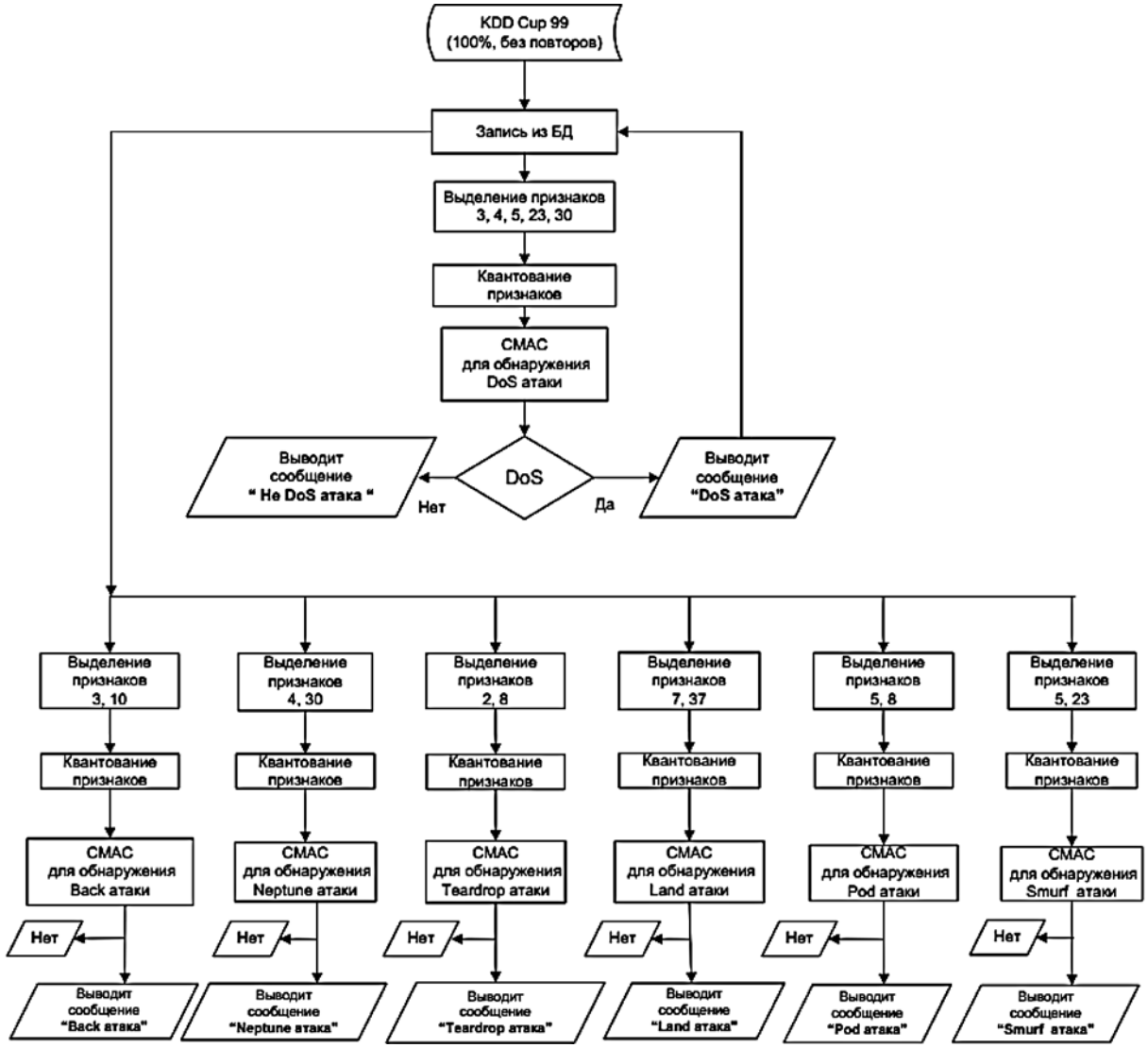

Рис. 1. Двухуровневая структура системы обнаружения DoS-атак и их компонентов

Таблица 3

Названия признаков для обнаружения компонентов DoS-атак

Номер признака	Название признака	Описание признака
2	Protocoltype	Протокол связи
3	Service	Служба
4	Flag	Флаг состояния соединения
5	Source byte	Число байтов, переданных от источника к месту назначения
7	Land	1, если соединение с/на тот же хост/порт; 0, в противном случае
8	Wrong fragment	Число неправильных фрагментов
10	Hot	Число "hot" показателей
23	Count	Число соединений на одном хосте текущего соединения в течение последних 2 с
30	Diff srv rate	% подключений к различным услугам
37	Dst host srv diff host rate	% подключений к одной и той же услуге хоста назначения, поступающих от разных хостов

Back — {3,10}, Neptune — {4,30}, Teardrop — {2,8}, Land — {7,37}, Pod — {5,8} и Smurf — {5,23}, признаки квантуются и поступают на входы обученных выделению компонентов DoS-атак соответствующих НС CMAC. Названия и описания признаков, используемых во втором слое системы, приведены в табл. 3.

3. Нейронная сеть CMAC: структура, алгоритмы обучения

Основным аналитическим элементом описываемой системы обнаружения атак является нейронная сеть CMAC, предложенная в работах Дж. Альбуса [6, 7]. Подробное описание нейронной сети CMAC на русском языке можно найти в работах [8, 9]. Далее приводится краткая информация об этом виде нейронных сетей, которая необходима для понимания особенностей применения НС CMAC в задаче обнаружения атак, см. также [2].

Наиболее существенным отличием НС СМАС от других нейронных сетей является следующее:

- аргументы запоминаемой и воспроизводимой функции (входной N-мерный вектор нейронной сети, или вектор признаков) принимают только дискретные значения:

$$X = \{x^{(1)} = \overline{1, x_{\max}^{(1)}};\ x^{(2)} = \overline{1, x_{\max}^{(2)}},\ ...;$$
$$x^{(N)} = \overline{1, x_{\max}^{(N)}}\}; \qquad (1)$$

- нелинейное преобразование аргументов функции происходит неявно с помощью алгоритма вычисления адресов ячеек ассоциативной памяти [8], в которых хранятся числа, определяющие значение запоминаемой функции.

В НС СМАС каждый входной N-мерный вектор x (вектор признаков) делает активными ровно ρ ячеек памяти, суммарное содержимое которых равно значению запоминаемой функции. Каждому входному N-мерному вектору x однозначно соответствует ρ-мерный вектор активных номеров ячеек памяти m. Параметр ρ (обобщающий параметр) играет очень важную роль, его значение определяет разрешающую способность НС СМАС и требуемый объем памяти нейронной сети.

Структура НС СМАС показана на рис. 2.

Важными характеристиками НС СМАС являются объем памяти

$$M = \rho^{-N+1} \prod_{i=1}^{N} (x_{\max}^{(i)} + \rho - 1) \qquad (2)$$

и значение обобщающего параметра ρ, которое характеризует аппроксимационные свойства: с увеличением ρ увеличиваются аппроксимационные свойства сети, но при этом теряется детализация запоминаемой функции. Поэтому для параметра ρ имеется оптимальное значение, при котором запоминаемая функция воспроизводится наилучшим образом. Для полного использования памяти НС СМАС и нахождения оптимального значения параметра ρ далее полагается

$$x_{\max}^{(i)} = 2^{l^{(i)}} + 1,\ i = \overline{1, N},\ \rho = 2^k, \qquad (3)$$

где $l^{(i)}$ и k — целые.

Если компоненты входного вектора запоминаемой функции непрерывны, то их следует преобразовать в цифровые значения. На примере одной переменной z это преобразование выполняется следующим образом. Задаются минимальное и максимальное значения $z_{\min}$, $z_{\max}$ переменной z и число уровней ее квантования $x_{\max}$. Вычисляется шаг квантования $\Delta = (z_{\max} - z_{\min})/x_{\max}$, и каждому элементу квантования каждой компоненты присваиваются целочисленные номера $x^{(i)} = 1, 2, ..., x_{\max}$ по формуле

$$x^{(i)} = Round((z - z_{\min})/\Delta + 0{,}5), \qquad (4)$$

где *Round* — функция округления до ближайшего целого.

Структура НС СМАС, представленная на рис. 2, предназначена для запоминания произвольных функций многих переменных. Для применения НС СМАС в задачах классификации эта структура дополняется пороговым элементом, выходом которого служат номера классов входной информации. В рассматриваемой задаче верхнего уровня число классов равно двум: класс DoS-атак и класс не DoS-атак. В этом случае выход v порогового элемента имеет вид:

$$v = 1, \text{ если } (y_{out} - \Delta) \geqslant 0$$
$$\text{и } v = 0, \text{ если } (y_{out} - \Delta) < 0, \qquad (5)$$

при этом значение $v = 1$ соответствует DoS-атаке, $v = 0$ — ее отсутствию. В (5) y_{out} — выход обученной НС СМАС; Δ — порог, значение которого выбирается экспериментально.

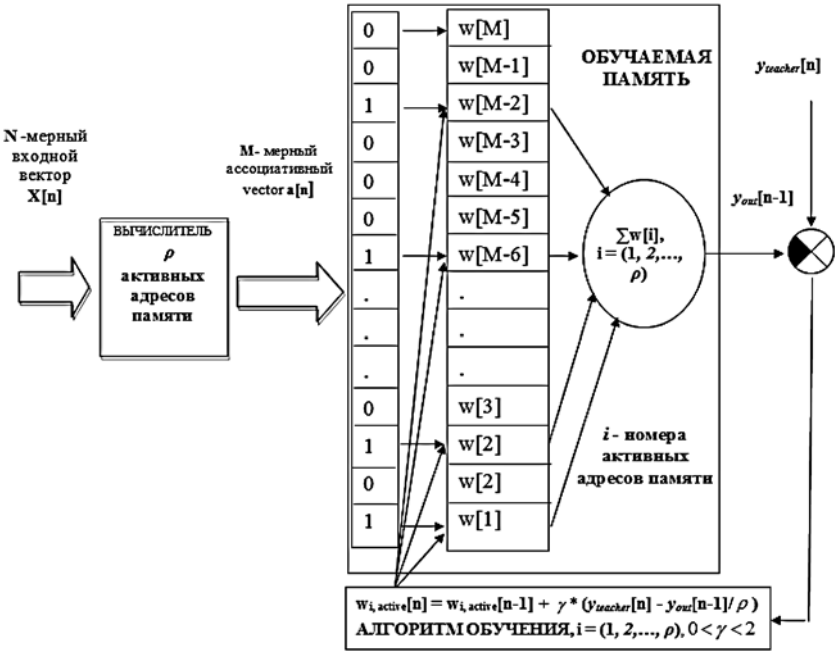

Рис. 2. Структура НС СМАС

4. Обучающие и тестирующие последовательности системы обнаружения атак

Обучение системы обнаружения атак заключается в обучении 7 НС СМАС по информации из базы данных атак KDD Cup 99.

Для обучения НС СМАС верхнего уровня, предназначенной для обнаружения DoS-атак, из имеющихся 247 267 записей DoS-атак случайным образом выделяется 75 % записей (185 448 записей), состав которых представлен в табл. 4.

Таблица 4

Состав обучающих записей нижнего уровня

Номер	Компоненты DoS-атак	Число обучающих записей компонентов
1	Back	726
2	Neptune	181 611
3	Teardrop	688
4	Land	14
5	Pod	154
6	Smurf	2255
Итого		185 448

Тестирование обученной системы проводится по всем 889 544 записям из базы данных атак KDD Cup 99, за исключением 75 % записей DoS-атак, которые были использованы для обучения системы. Тестовые данные состоят из $N_{DoS} = 61\,819$ записей DoS-атак и $N_{NotDoS} = 827\,725$ записей, которые содержат три класса атак: Probe, R2L и U2R и нормальные соединения.

5. Экспериментальные результаты

5.1. Обучение и тестирование НС СМАС верхнего уровня обнаружению DoS-атак

Обучение. Обучение НС СМАС верхнего уровня обнаружению DoS-атак выполняется с помощью 185 448 записей о DoS-атаках (75 % от общего числа DoS-атак). Из этих записей выделяют значения пяти признаков с номерами {3, 4, 5, 23, 30}. Максимальные значения признаков 3 и 4 согласно выражениям (3) принимают равными $x_{\max}^{(1)} = 129$ и $x_{\max}^{(2)} = 17$, соответственно. Максимальные значения признаков 5, 23, 30 принимают несколько значений. Для признака 5 максимальные значения $x_{\max}^{(3)}$ равны 129, 257, 513, 1025 и 2049, для признака 23 $x_{\max}^{(4)}$ равны 33, 65, 129, 257 и 513, а для признака 30 $x_{\max}^{(5)}$ равны 33, 65 и 129. Признаки квантуются с различными шагами квантования согласно выражениям (3) и (4). После квантования в полученных выборках возникают повторы квантованных записей, которые удаляются. При этом число записей для обучения, которое зависит от введенных шагов квантования по соответствующим переменным, существенно уменьшается, более чем на порядок.

Как отмечалось в разд. 3, на точность обучения оказывает существенное влияние значение обобщающего параметра ρ, которое в экспериментах согласно выражению (3) принимает значения $\rho = 2$, 4, 8, 16. Кроме того, точность обнаружения атак также зависит от значения порога обнаружения Δ (5), который принимает значения 0,2, 0,3, 0,4 и 0,5.

Обучение НС СМАС обнаружению DoS-атак проводится для каждого отдельного набора записей при фиксированных значениях параметров ρ и Δ. Перед процессом обучения память НС СМАС обнуляется, на ее вход подается 5-мерный вектор дискретных признаков, который случайным образом извлекается из обучающего набора данных. Число шагов обучения N принято заведомо завышенным и равняется $N = 500\,000$. Значение указаний учителя для DoS-атаки принимается равным 1. После завершения процесса обучения НС СМАС подвергается тестированию. Поскольку в результате тестирования выясняется область возможных оптимальных значений шагов квантования и значений обобщающего параметра, то для нахождения оптимальных параметров НС СМАС используется только часть из 75 наборов выборок с различными шагами квантования при различных значениях обобщающего параметра и порога.

Тестирование. Тестирование обученной НС СМАС верхнего уровня выполняется подачей на ее вход квантованных значений пяти признаков с номерами {3, 4, 5, 23, 30} 889 544 записей из сжатой базы данных атак KDD Cup 99, в которых отсутствуют 75 % использованных для обучения записей DoS-атак. Признаки записей квантуются с теми же шагами квантования, которые использовались для обучения нейронной сети. О каждой записи известно, к какому она относится классу: 0 — отсутствует DoS-атака, 1 — присутствует DoS-атака. Выход нейронной сети позволяет определить оценки вероятностей ошибок первого и второго рода системы обнаружения DoS-атак. При этом ошибка первого рода возникает, когда входная запись не является DoS-атакой, а система относит ее к DoS-атаке (ложная тревога), а ошибка второго рода возникает тогда, когда на вход системы поступает DoS-атака, а система ее не обнаруживает (пропуск атаки). Оценки вероятностей ошибок первого $\hat{\alpha}$ и второго $\hat{\beta}$ рода определяются следующими соотношениями:

$$\hat{\alpha} = \Delta N_{NotDoS}/N_{NotDoS},\ \hat{\beta} = \Delta N_{DoS}/N_{DoS}, \qquad (6)$$

где $N_{NotDoS} = 827\,725$ — число не DoS-атак, $N_{DoS} = 61\,819$ — число DoS-атак для всех случаев тестирования. Величины ΔN_{NotDoS} — число ложных тревог, ΔN_{DoS} — число пропущенных DoS-атак в (6) зависят от выбранных параметров системы обучения, определяют ее точностные характеристики и их вычисляют в результате каждого эксперимента. Кроме значений параметров (6) вычисляется значение однопараметрической характеристики системы

$$\hat{\gamma} = (\hat{\alpha}^2 + \hat{\beta}^2)^{1/2}, \qquad (7)$$

в которой ошибки первого и второго рода сворачиваются с одинаковыми весами.

5.2. Результаты обучения и тестирования НС СМАС верхнего уровня

В результате обучения и тестирования 216 вариантов нейронной сети СМАС верхнего уровня, для

которой шаги квантования, значения обобщающего параметра и значение порога принимали различные значения, были получены значения параметров $\hat{\alpha}$, $\hat{\beta}$ и $\hat{\gamma}$, характеризующие точность системы обнаружения DoS-атак.

В наилучшей системе обнаружения DoS-атак по критерию наименьшего значения параметра $\hat{\gamma}$ значения $\rho = 4$ и $\Delta = 0{,}5$, а максимальные значения компонент входного вектора признаков (1) принимают значения

$$X_{opt} = \{x^{(1)} = \overline{1{,}129}\,;\ x^{(2)} = \overline{1{,}17}\,;\ x^{(3)} = \overline{1{,}513}\,;$$
$$x^{(4)} = \overline{1{,}65}\,;\ x^{(5)} = \overline{1{,}33}\,\}. \qquad (8)$$

В этой близкой к оптимальной системе число ложных тревог $\Delta N_{NotDoS} = 1336$, число пропусков DoS-атак $\Delta N_{DoS} = 39$. С учетом выражений (6) и (7) оценки вероятностей ошибок первого $\hat{\alpha}$ и второго рода $\hat{\beta}$ будут $\hat{\alpha} = 0{,}0016$, $\hat{\beta} = 0{,}0006$. Значение параметра $\hat{\gamma} = 0{,}0017$. Из этих результатов следует, что оценка вероятности обнаружения DoS-атак для такой оптимальной системы равна $\hat{P}_{DoS} = 0{,}9994$. Доля ложных тревог составляет 0,02 от общего числа DoS-атак.

Для другой системы обнаружения DoS-атак, близкой по оптимальности к описанной выше, в которой обобщающий параметр и порог приняли новые значения: $\rho = 8$ и $\Delta = 0{,}2$, а максимальные значения компонент входного вектора признаков (8) остались без изменения, все атаки были обнаружены: $\Delta N_{DoS} = 0$, однако возросло число ложных тревог $\Delta N_{NotDoS} = 2549$. Для такой системы $\hat{\alpha} = 0{,}0031$, $\hat{\beta} = 0{,}0$. Значение параметра $\hat{\gamma} = 0{,}0031$.

5.3. Результаты обучения и тестирования НС СМАС нижнего уровня обнаружения компонентов DoS-атак

Обучение всех шести НС СМАС нижнего уровня проводится в полной аналогии с описанными выше процессами обучения НС СМАС верхнего уровня.

Из записей DoS-атак для обучения выделяются значения признаков компонентов DoS-атак: Back — {3,10}, Neptune — {4,30}, Teardrop — {2,8}, Land — {7,37}, Pod — {5,8} и Smurf — {5,23}, признаки квантуются и из них удаляются повторы. В результате этих процедур для обучения обнаружению компонентов DoS-атак число записей для компонентов Back, Neptune, Teardrop, Land, Pod и Smurf существенно уменьшается, в том числе вследствие наличия только двух признаков для каждого компонента, и оказывается равным 3, 87, 3, 3, 7 и 850, соответственно. В силу небольшого числа обучающих записей для нижнего уровня число шагов обучения, которое зависит от номеров компонентов DoS-атак, существенно ниже, чем для верхнего уровня. Проведенный предварительный анализ возможных значений параметров нижнего уровня обнаружения компонентов DoS-атак определил

Таблица 5

Параметры обучения НС СМАС обнаружению компонентов DoS-атак

Компоненты DoS-атак	Номера признаков	Минимальное значение квантованного признака	Максимальное значение квантованного признака	Число записей для обучения	Порог Δ	ρ
Back	3 10	1 1	129 9	4	0,5	2
Neptune	4 30	1 1	33 129	87	0,5	2
Teardrop	2 8	1 1	5 5	3	0,5	2
Land	7 37	1 1	3 129	7	0,5	2
Pod	5 8	1 1	2049 5	3	0,5	2
Smurf	5 23	1 1	2049 513	850	0,5	2

максимальные значения признаков, значения обобщающего параметра и порога, значения которых приведены в табл. 5. Указание учителя в режиме обучения принимается равным единице. Отметим, что параметры нижнего уровня не оптимизированы, оптимизация последних является предметом последующих исследований. Следует также учесть, что в базе данных атак KDD Cup 99 число некоторых компонентов DoS-атак незначительно, например для компонентов Land и Pod (см. табл. 4).

Тестирование несколько отличается от тестирования верхнего уровня: в роли тестовых данных выступают те записи, которые НС СМАС верхнего уровня приняла за DoS-атаку. Из этих записей выделяются соответствующие каждому компоненту DoS-атак признаки, они квантуются с теми же шагами квантования, которые были использованы при обучении каждой из шести НС СМАС, и эти данные подаются на входы каждой нейронной сети. Если несколько НС дают сообщение относительно обнаружения компонента DoS-атаки, то предпочтение отдается той сети, у которой выше аналоговый выход.

В табл. 6 приведены результаты тестирования нижнего уровня системы обнаружения DoS-атак для случая, когда параметры верхнего уровня оптимальны и соответствуют описанным в разделе 5.2 значениям, для которых $\hat{\gamma} = 0{,}0017$. Число записей для тестирования равно 63 116, из которых 61780 представляют записи DoS-атак.

Из табл. 6 следует, что значения параметров нижнего уровня системы обнаружения DoS-атак и их компонентов близки к оптимальным. Вероятность обнаружения большинства компонентов DoS-атак (Teardrop, Land, Pod, Smurf) для такой системы практически равна единице. Несколько хуже ре-

Таблица 6

Результаты тестирования нижнего уровня системы обнаружения компонентов DoS-атак

Компоненты DoS-атак	Точное число компонентов в выборке	Точное число некомпонентов в выборке	Число принятых за компонент	Число пропущенных компонентов	$\hat{\alpha}$	$\hat{\beta}$	$\hat{\gamma}$
Back	242	62 874	5	3	0,0001	0,0124	0,0124
Neptune	60 499	2617	461	61	0,1762	0,0010	0,1762
Teardrop	230	62 886	0	0	0	0	0
Land	5	63 111	6	0	0,0001	0	0,0001
Pod	52	63 064	0	0	0	0	0
Smurf	752	62 364	129	0	0,0021	0	0,0021

зультаты для компонента Back, для которого эта оценка равна $\hat{P}_{Back} = 0{,}9876$. Отметим также несколько высокую вероятность ложной тревоги для компонента Neptune, которая равна $\hat{\alpha} = 0{,}1762$.

6. Заключение

Приведенные выше результаты обучения и тестирования системы обнаружения DoS-атак и их компонентов на базе нейронных сетей CMAC расширяют результаты, приведенные в работе [2], и подтверждают утверждения Дж. Кеннеди [1] о большой перспективности НС CMAC как аналитического инструмента обнаружения атак на информационные ресурсы. Для развития полученных в работе результатов следует провести исследования, используя информацию из других баз данных и другие наборы признаков применительно не только к DoS-атакам, но и к другим видам атак.

Список литературы

1. **Cannady J.** Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks // Proc. of the 23-rd National Information Systems Security Conference, October 16—19, 2000, Baltimore, MD, USA, 2000. (http://csrc.nist.gov/nissc/2000/proceedings/toc.html).

2. **Аведьян Э. Д., Ле Т. Ч. Л.** Нейронная сеть CMAC в задаче обнаружения атак на информационные ресурсы // Информатизация и связь. 2015. № 4. С. 93—98.

3. **KDD Cup** 1999 Data: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

4. **Bhoria P., Garg K.** Determining feature set of DoS-attacks // International Journal of Advanced Research in Computer Science and Software Engineering. 2013. Vol. 3. N. 5. P. 875—878.

5. **Tavallaee M., Bagheri E., Lu W., Ghorbani A. A.** A Detailed analysis of the KDD Cup 99 data set // Proc. of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications 2009, Ottawa, 2009. P. 53—58.

6. **Albus J. S.** A new approach to manipulator control: the cerebellar model articulation controller // ASME Trans., J. Dynamic Systems, Measurement and Control. 1975. Vol. 97. N. 3. P. 220—227.

7. **Albus J. S.** Data storage in the cerebellar model articulation controller (CMAC) // ASME Trans., J. Dynamic Systems, Measurement and Control. 1975. Vol. 97. N. 3. P. 228—233.

8. **Аведьян Э. Д.** Ассоциативная нейронная сеть CMAC. Часть I. Структура, объем памяти, обучение и базисные функции // Информационные технологии. 1997. № 5. С. 6—14.

9. **Аведьян Э. Д.** Ассоциативная нейронная сеть CMAC. Часть II. Процессы обучения, ускоренное обучение, влияние помех, устранение влияния помех в двухслойной сети // Информационные технологии. 1997. № 6. С. 16—27.

E. D. Aved'yan[1, 2, 3], Senior research Fellow[1], Deputy Head[2], Professor[3], **T. T. L. Le**[3], Postgraduate Student

[1]Department of Advanced Research and special Projects of the Federal State Autonomous Research Institution CIT&S, Moscow, Russia

[2]The Neural Network Technology Centre of the International Centre of Informatics and Electronics, Moscow, Russia

[3]Department of Radio Engineering and Cybernetics of the Moscow Institute of Physics & Technology (State University), Moscow, Russia

A Two-Level System for DoS attacks and their Components Detection based on the Neural Networks CMAC

The results of the application of the system of neural networks CMAC (NN CMAC) to detect DoS attacks and their components are given. The system used all the data in the database KDD Cup 99. The system consists of two levels. The first level is designed to detect DoS attacks using trained NN CMAC. The second level is designed to separate from the detected DoS attacks all the 6 components: Back, Neptune, Land, Pod, Teardrop and Smurf using 6 trained NN CMAC. Miss rate of DoS attacks and false alarm in the first level does not exceed 0,2 %.

Keywords: *Detection of DoS attacks, the neural network CMAC, attacks, database KDD Cup 99, the components of DoS attacks*

References

1. **Cannady J.,** Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks, *Proceedings of the 23-rd National Information Systems Security Conference, October 16—19, 2000, Baltimore, MD, USA, 2000* (http://csrc.nist.gov/nissc/2000/proceedings/toc.html).

2. **Aved'yan E. D., Le T. Ch. L.,** Nejronnaja set' SMAS v zadache obnaruzhenija atak na informacionnye resursy (The Neural network CMAC in the Problem of Intrusion Detection on the Information Resources), *Informatizacija i svjaz'*, 2015, no. 4, pp. 93—98.

3. **KDD Cup** 1999 Data: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

4. **Bhoria P, Garg K.**, Determining feature set of DoS attacks, *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013, vol. 3, no. 5, pp. 875—878.

5. **Tavallaee M., Bagheri E., Lu W., Ghorbani A. A.** A Detailed analysis of the KDD Cup 99 data set, *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications 2009, Ottawa*, 2009, pp. 53—58.

6. **Albus J. S.,** A new approach to manipulator control: the cerebellar model articulation controller, *ASME Trans., J. Dynamic Systems, Measurement and Control*, 1975, vol. 97, no. 3, pp. 220—227.

7. **Albus J. S.,** Data storage in the cerebellar model articulation controller (CMAC), *ASME Trans., J. Dynamic Systems, Measurement and Control*, 1975, vol. 97, no. 3, pp. 228—233.

8. **Aved'yan E. D.,** Associativnaja nejronnaja set' SMAS. Chast' I Struktura, ob#em pamjati, obuchenie i bazisnye funkcii (The Associative CMAC Neural Network. Part I. The Structure, Memory, Learning and Basis functions), *Informacionnye tehnologii*, 1997, no. 5, pp. 6—14.

9. **Aved'yan E. D.**, Associativnaja nejronnaja set' SMAS. Chast' II. Processy obuchenija, uskorennoe obuchenie, vlijanie pomeh, ustranenie vlijanija pomeh v dvuhslojnoj seti (The Associative CMAC Neural Network. Part II. The Learning Processes, Accelerated Learning, Noise Influences, Noise Elimination in the Two-Layer CMAC Network). *Informacionnye tehnologii*, 1997, no. 6, pp. 16—27.

Адрес редакции:

107076, Москва, Стромынский пер., 4

Телефон редакции журнала **(499) 269-5510**

E-mail: it@novtex.ru

Технический редактор *Е. В. Конова*.

Корректор *Е. В. Комиссарова*.

Сдано в набор 08.07.2016. Подписано в печать 23.08.2016. Формат 60×88 1/8. Бумага офсетная.

Усл. печ. л. 8,86. Заказ IT916. Цена договорная.

Журнал зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций.

Свидетельство о регистрации ПИ № 77-15565 от 02 июня 2003 г.

Оригинал-макет ООО "Адвансед солюшнз". Отпечатано в ООО "Адвансед солюшнз".

119071, г. Москва, Ленинский пр-т, д. 19, стр. 1.