УДК 004.056.5
DOI: 10.17586/0021-3454- 2021-64-5-357-363

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Т. В. Тимочкина, Т. М. Татарникова, Е. Д. Пойманова

Российский государственный гидрометеорологический университет,
192007, Санкт-Петербург, Россия
E-mail: e.d.poymanova@gmail.com

Предложен метод обнаружения сетевых атак, основанный на выборе полезных параметров нейронной сети, которые характеризуют аномальный трафик. Полезные параметры получены в результате ранжирования всех параметров нейронной сети по степени значимости для обнаружения каждой атаки. Ранжирование выполнено по системе правил, учитывающих три критерия эффективности нейронной сети: общую точность классификации параметров, время обучения сети и время ее тестирования. Для обучения нейронной сети использована известная база данных атак NSL—KDD, характеризующая каждую атаку по 41 информационному признаку. Ранжирование позволило сократить количество признаков до 10. Обученная на полезных параметрах нейронная сеть показала высокую скорость обнаружения и точность классификации большинства рассматриваемых атак.

Ключевые слова: *нейронные сети, информационная безопасность, обнаружение вторжений, сетевые атаки, система защиты информации, база данных*

Введение. Для обнаружения сетевых атак, наряду с общепризнанными сигнатурными подходами, используются нейронные сети [1], сложность применения которых при решении любых задач заключается в выборе структуры нейронной сети, необходимости наличия обучающей выборки и алгоритма обучения.

Основная идея искусственных нейронных сетей — копирование сложных взаимных связей между клетками искусственного мозга, при этом компьютер должен иметь возможность обучаться, распознавать образы и принимать решения, как это делает человек [2].

Возможность обучения — одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. Суть обучения заключается в нахождении коэффициентов связей между нейронами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять их обобщение. Для инициализации нейрона используется дополнительный вход x_0 и соответствующий ему вес w_0. Под инициализацией понимается формирование порога чувствительности, т.е. смещение активной функции по горизонтальной оси. Для разных типов искусственных нейронов используются разные функции активации. Передаточная функция, которая может быть ступенчатой, линейной или нелинейной, должна моделировать резкий переход в состояние активации. При обучении сети по алгоритму обратного распространения часто используется сигмоидальная функция [3, 4]

$$\sigma(x) = \frac{1}{1+\exp(-tx)}, \qquad (1)$$

что объясняется непрерывностью этой функции и простотой ее производной:

$$\frac{d\sigma(x)}{dx} = t\sigma(x)(1-\sigma(x)), \qquad (2)$$

где t — коэффициент крутизны функции активации; если $t \to \infty$, сигмоидальная функция становится похожей на пороговую, если t=0, похожа на линейную.

На рис. 1 приведен скриншот среды Deductor, где задана структура нейронной сети и построена сигмоидальная функция активации.

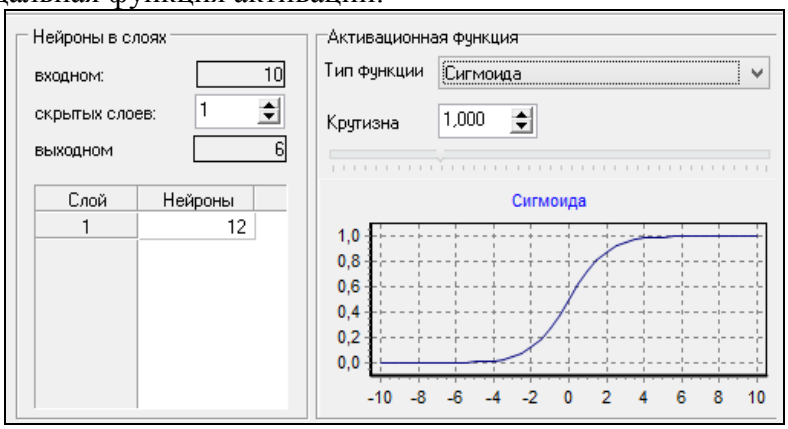

Рис. 1

Постановка задачи. Обнаружение сетевых атак связано с выделением определенных параметров, которые могут быть задействованы для выявления аномального трафика, но не все параметры одинаково важны. Поэтому актуальной становится задача классификации параметров, а также сокращение их числа для более быстрой работы системы обнаружения атак.

В процессе обучения нейронной сети использована база данных атак NSL—KDD. Данные об атаках представляют собой текстовый файл, который содержит аномально активные векторы, отмеченные типом атаки, и векторы нормального поведения. Каждая запись представляет собой образ сетевого соединения и включает 43 информационных признака — характеристику наблюдаемого явления, причем 41 параметр (табл. 1) относится к входному трафику, последние два параметра являются меткой класса „атака“/„не атака“ и меткой входа трафика „да/нет“ [5, 6].

Таблица 1

Номер параметра	Параметр	Описание
Данные TCP-соединения		
1	duration	Продолжительность сессии, с
2	protocol_type	Тип протокола (TCP, UDP и т.д.)
3	service	Удаленный сервис (http, telnet и т.д.)
4	flag	Статус соединения (normal или error)
5	src_bytes	Количество исходящих байтов (источник –> назначение)
6	dst_bytes	Количество входящих байтов (назначение –> источник)
7	land	1, если подключен с того же хоста/порта, по умолчанию — 0
8	wrong_flagment	Количество „неправильных“ пакетов
9	urgent	Количество срочных пакетов
Данные домена		
10	hot	Количество „hot“ индикаторов
11	num_failed_logins	Количество неудачных авторизаций
12	logged_in	1 при успешной авторизации, 0 — по умолчанию
13	num_compromised	Количество „скомпрометированных“ условий
14	root_shell	1, если вход выполнен под „root“, 0 — по умолчанию
15	su_attempted	1, если была попытка входа под „root“, 0 — по умолчанию
16	num_root	Количество доступов суперпользователя
17	num_file_creations	Количество операций по созданию файла
18	num_shells	Количество сессий терминала
19	num_access_files	Количество операций по доступу к файлам
20	num_outbound_cmds	Количество исходящих команд в ftp-сессии
21	is_host_login	1, если логин в списке „hosts“, 0 — по умолчанию
22	is_guest_login	1, если логин гостевой, 0 — по умолчанию

Продолжение табл. 1

Номер параметра	Параметр	Описание
Данные, посчитанные в 2-секундном окне		
23	count	Количество подключений на один хост в рамках текущей сессии за последние 2 с
24	srv_count	Количество подключений к одному сервису в рамках текущей сессии за последние 2 с
25	serror_rate	Доля, %, от подключений с SYN-ошибкой
26	srv_serror_rate	Доля, %, от подключений с SYN-ошибкой при подключении на один сервис
27	rerror_rate	Доля, %, от подключений с REJ-ошибкой
28	srv_rerror_rate	Доля, %, от подключений с REJ-ошибкой при подключении на один сервис
29	same_srv_rate	Доля, %, от подключения к одному и тому же сервису
30	diff_srv_rate	Доля, %, от подключения к разным сервисам
31	srv_diff_host_rate	Доля, %, от подключения к разным хостам
Данные, посчитанные в 100-секундном окне		
32	dst_host_count	Количество подключений на один хост в рамках текущей сессии за последние 100 с
33	dst_host_srv_count	Количество подключений на один сервис в рамках текущей сессии за последние 100 с
34	dst_host_same_srv_rate	Доля, %, от подключения к одному и тому же сервису
35	dst_host_diff_srv_rate	Доля, %, от подключения к разным сервисам
36	dst_host_same_src_port_rate	Доля, %, от подключения с одного и того же порта источника
37	dst_host_srv_diff_host_rate	Доля, %, от подключения к одному и тому же хосту
38	dst_host_serror_rate	Доля, %, от подключений с SYN-ошибкой
39	dst_host_srv_serror_rate	Доля, %, от подключений с SYN-ошибкой при подключении на один сервис
40	dst_host_rerror_rate	Доля, %, от подключений с REJ-ошибкой
41	dst_host_srv_rerror_rate	Доля, %, от подключений с REJ-ошибкой при подключении на один сервис

Задача сокращения числа параметров решается сначала их ранжированием по значимости: полезные, малозначимые (второстепенные) и бесполезные параметры, далее неинформативные параметры трафика исключаются или используются множества только полезных параметров при обнаружении конкретной атаки.

С математической точки зрения задачу сокращения размерности можно представить в следующем виде: дана p-мерная переменная $\mathbf{X} = (x_1, x_2, ..., x_p)^{\mathrm{T}}$, необходимо найти пространство меньшей размерности, в котором переменная $\mathbf{S} = (s_1, s_2, ..., s_k)^{\mathrm{T}}$, $k \le p$, отражает содержание исходных данных в соответствии с некоторым критерием.

В ходе исследования использован линейный метод сокращения размерности, когда результат вычисления каждого k-го, $k \le p$, компонента есть линейная комбинация исходных переменных [7, 8]:

$$s_i = w_{i,1}x_1 + ... + w_{i,p}x_p, \; i = \overline{1,k};$$

$$\mathbf{S}=\mathbf{WX},$$

где **W** — матрица весов линейных преобразований.

Сокращение контрольной выборки за счет устранения бесполезных параметров позволяет повысить точность обнаружения атак и ускорить вычисления, тем самым увеличивая общую производительность системы обнаружения атак.

В настоящей статье предложен подход к решению задачи обнаружения какого-либо класса атак или отдельной атаки. Задача решается в два этапа: 1) выбор полезных параметров, 2) построение нейронной сети, автоматизирующей обнаружение атаки на основе выбранных параметров [9].

Оценка значимости параметров. Построение нейронной сети. Значимость параметров определялась эмпирическим путем: сначала единожды исключается один параметр, чтобы ранжировать входные параметры и идентифицировать наиболее значимые для обнаружения атаки с использованием метода опорных векторов, затем полученный набор используется для обучения и тестирования нейронной сети. Таким образом, оценка значимости параметров включает следующие этапы:

1) формирование обучающего и тестового наборов параметров для каждой атаки;

2) исключение параметра из обучающего и тестового наборов;

3) использование полученного набора для обучения сети;

4) анализ производительности нейронной сети с помощью тестового набора с учетом выбранных критериев эффективности;

5) оценка значимости параметра в соответствии с правилами.

Для оценки значимости каждого параметра используются три основных критерия эффективности нейронной сети: общая точность классификации параметров P, время обучения сети t и время тестирования сети τ. Каждый параметр классифицирован как „полезный“, „второстепенный“ и „бесполезный“ в соответствии со следующими правилами:

— если значение P уменьшается, время обучения t увеличивается, а время тестирования τ уменьшается, то параметр полезный;

— если значение P уменьшается, а время t и время τ увеличиваются, то параметр полезный;

— если значение P и время t уменьшаются, а время τ увеличивается, то параметр полезный;

— если значение P не изменяется, а время t и время τ увеличиваются, то параметр полезный;

— если значение P не изменяется, время t уменьшается, а время τ увеличивается, то параметр второстепенный;

— если значение P не изменяется, время t увеличивается, а время τ уменьшается, то параметр второстепенный;

— если значение P не изменяется, а время t и время τ уменьшаются, то параметр бесполезный;

— если значение P и время t увеличиваются, а время τ уменьшается, то параметр второстепенный;

— если значение P увеличивается, время t уменьшается, а время τ увеличивается, то параметр второстепенный;

— если значение P увеличивается, а время t и время τ уменьшаются, то параметр бесполезный.

Процесс оценивания значимости выполнен для 41 параметра каждого класса атак (см. табл. 1), в результате чего для обучения нейронной сети использовались параметры только класса „полезный“.

Путем проведенного ранжирования удалось сократить количество входных параметров в 4 раза, что естественно обеспечило преимущество по времени анализа поступающего сетевого трафика. Анализ проводился для трех классов атак: DoS, Probe и R2L, полученные параметры приведены в табл. 2. На основе этих параметров построены нейронные сети, способные выявлять атаки (рис. 2).

Таблица 2

Класс атаки	Количество параметров	Номер параметра*
DoS:	10	23, 24, 25, 26, 32, 33, 35, 36, 38,39
Probe	10	23, 24, 27, 28, 29, 30, 32, 33, 40, 41
R2L	10	6, 10, 12, 22, 23, 32, 33, 34, 36, 37, 40
* Соответствует номеру параметра в табл. 1		

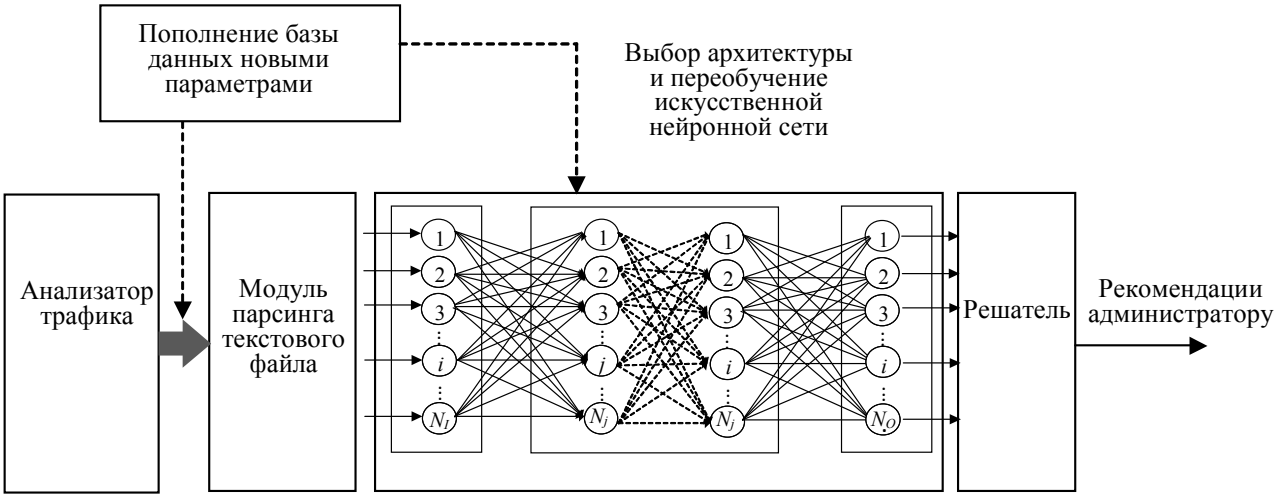

Рис. 2

Оценка эффективности системы обнаружения атак выполнена по следующим критериям:

— точность классификации P (*precission*)*:*

$$P = \frac{\mathrm{TP}}{\mathrm{TP+FP}},$$

где TP — количество истинно-положительных записей, FP — количество ложноположительных записей;

— скорость обнаружения DR (*detection rate*)*:*

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP+FN}},$$

где FN — количество ложноотрицательных записей.

Полученные показатели эффективности обнаружения атак канального уровня и сетевых атак представлены в табл. 3 и 4 соответственно.

Таблица 3

Атака	Скорость обнаружения, %	Точность классификации, %
normal	94,37	99,38
auth_flood	100,00	92,50
deauth_flood	100,00	84,39
caffe_latte	100,00	70,97
client_fragment	100,00	96,98
AP_fragment	100,00	98,26
data_replay	99,96	99,53
evil_twin_AP	100,00	94,30
EAP_replay	100,00	100,00
beacon_flood	99,91	100,00
RTS/CTS_flood	100,00	91,49

Таблица 4

Класс атаки	Атака	Скорость обнаружения, %	Точность классификации, %
—	normal	97,07	87,25
DoS	neptune	99,36	99,98
R2L	guess_passwd	66,37	97,03
DoS	smurf	95,19	99,53
Probe	satan	90,75	81,84
DoS	back	96,10	97,73
R2L	warezmaster	16,10	98,06
DoS	pod	82,93	70,83
Probe	nmap	79,45	90,62
Probe	ipsweep	97,87	79,31
Probe	portsweep	89,17	61,67
DoS	teardrop	75,00	18,75

Удовлетворительной считается такая система обнаружения атак, которая имеет общую точность обнаружения выше 70 % и скорость обнаружения выше 80 % [10].

Заключение. Согласно результатам исследования, сокращение количества параметров, характеризующих аномальный трафик, играет важную роль при построении нейронных сетей для выявления атак, так как большое число входных параметров сети порождает большое количество ошибок первого и второго рода. Также сокращение числа параметров обеспечивает выигрыш по времени работы нейронной сети.

СПИСОК ЛИТЕРАТУРЫ

1. *Сафронова Е. О., Жук Г. А.* Применение искусственных нейронных сетей для прогнозирования DoS атак // Молодой ученый. 2019. № 23. С. 27—30.
2. *Татарникова Т. М., Журавлев А. М.* Нейросетевой метод обнаружения вредоносных программ на платформе Android // Программные продукты и системы. 2018. № 3. С. 543—547.
3. Краткий анализ решений в сфере СОВ и разработка нейросетевого детектора аномалий в сетях передачи данных / Хабр [Электронный ресурс]: <https://m.habr.com/ru/post/358200/>, 27.01.2021.
4. Нейронные сети — математический аппарат [Электронный ресурс]: <http://www.basegroup.ru/library/analysis/neural/math/>, 26.01.2021.
5. A Deeper Dive into the NSL-KDD Data Set – Towards Data Science [Электронный ресурс]: <https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657>, 28.01.2021.
6. *Ingre B., Yadav A., Soni A. K.* Decision tree based intrusion detection system for NSL-KDD dataset // Proc. of the Intern. Conf. on Information and Communication Technology for Intelligent Systems (ICTIS), Ahmedabad, India, 25—26 March 2017. Cham: Springer, 2017. Vol. 2. P. 207—218.
7. Главные компоненты и факторный анализ [Электронный ресурс]: <http://www.statsoft.ru/home/textbook/modules/stfacan.html>, 28.01.2021.
8. *Jyothsna V., Prasad V. V. R.* A review of anomaly based intrusion detection systems // Intern. Journal of Computer Applications. 2011. Vol. 28, N 7. P. 26—35.
9. *Sadek R. A., Soliman M. S., Elsayed H. S.* Effective anomaly intrus ion detection system based on neural network with indicator variable and rough set reduction // Intern. Journal of Computer Science Issues (IJCSI). 2013. Vol. 10, iss. 6, N 2. P. 227—233.
10. *Татарникова Т. М., Степанов С. Ю., Петров Я. А., Сидоренко А. Ю.* Разработка метода защиты геоинформационных систем и пространственных данных на основе нейронной сети // Программные продукты и системы. 2020. № 2. С. 229—235.

Сведения об авторах

Татьяна Владимировна Тимочкина — аспирант; РГГМУ; E-mail: timo4kina.tanya@ya.ru

Татьяна Михайловна Татарникова — д-р техн. наук, профессор; РГГМУ, Институт информационных систем и технологий; директор; E-mail: tm-tatarn@yandex.ru

Екатерина Дмитриевна Пойманова — канд. техн. наук; РГГМУ, кафедра информационных технологий и систем безопасности; доцент; E-mail: e.d.poymanova@gmail.com

Поступила в редакцию
23.01.2021 г.

Ссылка для цитирования: *Тимочкина Т. В., Татарникова Т. М., Пойманова Е. Д.* Применение нейронных сетей для обнаружения сетевых атак // Изв. вузов. Приборостроение. 2021. Т. 64, № 5. С. 357—363.

NEURAL NETWORKS APPLICATION TO NETWORK ATTACK DISCOVERY

T. V. Timochkina, T. M. Tatarnikova, E. D. Poymanova

Russian State Hydrometeorological University,
192007, St. Petersburg, Russia
E-mail: e.d.poymanova@gmail.com

A method for network attacks discovery based on the choice of useful neural network parameters that characterize abnormal traffic, is proposed. Useful parameters are obtained with ranking all parameters of the neural network according to the degree of significance for detecting each attack. The ranking is carried out according to a system of rules that account for three criteria of a neural network efficiency: the general accuracy of the parameters classification, the training time of the network, and the time of its testing. To train the neural network, the well-known NSL – KDD attack database is used, which characterizes each attack by 41 information signs. The ranking makes it possible to reduce the number of features to 10. The neural network trained on useful parameters showed a high detection rate and classification accuracy for most of the attacks under consideration.

Keywords: neural networks, information security, intrusion detection, network attacks, information security system, database

REFERENCES

1. Safronova E.O., Zhuk G.A. *Young scientist*, 2019, no. 23, pp. 27–30. (in Russ.)
2. Tatarnikova T.M., Zhuravlev A.M. *Software & Systems,* 2018, no. 3, pp. 543–547. (in Russ.)
3. https://m.habr.com/ru/post/358200/. (in Russ.)
4. http://www.basegroup.ru/library/analysis/neural/math/. (in Russ.)
5. *A Deeper Dive into the NSL-KDD Data Set – Towards Data Science*, https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657.
6. Ingre B., Yadav A., Soni A.K. *Proceedings of the International Conference on Information and Communication Technology for Intelligent Systems,* ICTIS, Ahmedabad, India, March 25–26, 2017, Cham, Springer, 2017, vol. 2, pp. 207–218.
7. http://www.statsoft.ru/home/textbook/modules/stfacan.html.
8. Jyothsna V., Prasad V.V.R. *International Journal of Computer Applications*, 2011, no. 7(28), pp. 26–35.
9. Sadek R.A., Soliman M.S., and Elsayed H.S. *International Journal of Computer Science Issues (IJCSI)*, 2013, no. 6(10), pp. 227–233.
10. Tatarnikova T.M., Stepanov S.Yu., Petrov Ya.A., Sidorenko A.Yu. *Software & Systems*, 2020, no. 2, pp. 229–235. (in Russ.)

Data on authors

Tatiana V. Timochkina — Post-Graduate Student; Russian State Hydrometeorological University; E-mail: timo4kina.tanya@ya.ru

Tatiana M. Tatarnikova — Dr. Sci., Professor; Russian State Hydrometeorological University, Institute of Information Systems and Geotechnologies; Head of the Institute; E-mail: tm-tatarn@yandex.ru

Ekaterina D. Poymanova — PhD; Russian State Hydrometeorological University, Department of Information Technology and Security Systems; Associate Professor; E-mail: e.d.poymanova@gmail.com

For citation: Timochkina T. V., Tatarnikova T. M., Poymanova E. D. Neural networks application to network attack discovery. *Journal of Instrument Engineering*. 2021. Vol. 64, N 5. P. 357—363 (in Russian).

DOI: 10.17586/0021-3454- 2021-64-5-357-363