УДК 004.89

НЕЙРОСЕТЕВОЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ ОТ DDOS-АТАК

Частикова В.А., Картамышев Д.А., Власов К.А.

ФГБОУ ВПО «Кубанский государственный технологический университет», Краснодар, e-mail: chastikova_va@mail.ru

Разработана методика защиты от сетевых атак типа DDoS на основе механизма работы нейронных сетей. Выполнен анализ существующих методик и механизмов защиты от сетевых атак; изучена эффективность работы нейронных сетей различных структур. Для поиска наиболее эффективной архитектуры нейронной сети проведен ряд исследований. Архитектура, показавшая наилучший результат – нейронная сеть вида многослойный персептрон, обучающаяся методом обратного распространения ошибки, была реализована в виде программного комплекса в среде Microsoft Visual Studio. На его основе осуществлялось тестирование реализованной методики защиты. В процессе изучения работы алгоритма была выполнена оптимизация параметров обучения нейронной сети. Проведенные исследования показали, что применение предложенной методики существенно повысило эффективность работы и снизило количество ошибок распознавания нейронной сети.

Ключевые слова: сетевая атака, DDoS-атака, нейронная сеть, персептрон.

NEURAL NETWORK METHOD FOR INFORMATION PROTECTION FROM DDOS-ATTACKS

Chastikova V.A., Kartamyshev D.A., Vlasov K.A.

Kuban State Technological University, Krasnodar, Russia, e-mail: chastikova_va@mail.ru

In this article was analyzed some of existing methods and mechanisms of protection from network attacks; been studied the effectiveness of the neural networks of different structures. To search for the most effective architecture of the neural network conducted a number of studies. The best architecture on the results of research – is a neural network type of multilayer perceptron. Learning of neural network performed by using the error back-propagation algorithm. For learning was used signature database of network attacks, including more than 4 million records. This network has been implemented as a software package using the Microsoft Visual Studio. The computer program includes a training mode, benchmarking and diagnostic records. On the basis of the developed software carried out testing of implemented protection methods. During the study of the algorithm been performed optimization the parameters of neural network training. Researches have shown that the application of the proposed method significantly increased the work efficiency and reduced number of errors in detection neural network.

Keywords: network attack, DDoS-attack, neural network, perceptron.

Быстрое и повсеместное распространение Интернета привело к бурному развитию компьютерных сетей, что позволило существенно расширить возможности для компаний, предоставляющих свои услуги через глобальную сеть. К глобальной сети подключены миллионы устройств и пользователей, благодаря чему множество фирм и потребителей взаимодействуют между собой. Для реализации своих услуг компании используют информационные ресурсы, которые позволяют выполнять обработку информации, относящуюся к их клиентам. Некорректная работа или недоступность сервисов может повлечь значительные потери, как финансовые, так и клиентские.

Именно по этим причинам в последние годы информационные ресурсы и сервисы все чаще сталкиваются с вредоносным воздействием, осуществляемым с использованием протоколов межсетевого взаимодействия – удаленной сетевой атакой.

Среди множества видов сетевых атак наибольшее распространение получила атака типа DDoS. По данным статистики [2-3,7] данный вид угрозы занимает одно из лидирующих мест ежегодно. Причинами распространения подобного вредоносного сетевого воздействия является простота реализации, исчерпывающие сведения о механизме исполнения и малые требования к знаниям и вычислительным ресурсам злоумышленника.

DDoS-атака (Distributed Denial of Service) – вид злонамеренной деятельности, ставящей своей целью довести компьютерную систему до состояния, когда обслуживание правомерных пользователей и корректное выполнение возложенных на нее функций невозможно. DDoS-атака осуществляется одновременно с большого числа компьютеров, совокупность которых представляет собой ботнет [11].

Материалы и методы исследования

Для успешного противодействия сетевым атакам разрабатываются методы и механизмы защиты; практически все современные программные и программно-аппаратные средства защиты используют целый набор методов. Из-за высокой стоимости средств защиты многие компании отказываются от их приобретения и эксплуатации, что приводит к существенному росту финансовых и клиентских потерь при осуществлении сетевых атак. Основные механизмы, применяемые в современных средствах противодействия DDoS-атакам, представлены в таблице 1 [1].

Таблица 1

Основные механизмы защиты. Сравнительный анализ

	Метод				
Критерий	Анализ состояний	Нейронные сети	Экспертные системы	Сигнатурные методы	Статистические методы
Уровень наблюдения	Сеть, ОС, приложение	Сеть, ОС	Сеть, ОС	Сеть, ОС, приложение	Сеть, ОС
Аномалии/ Злоупотребления	-/+	+/+	+/+	-/+	+/-
Верифицируемость	+	-	+	+	-
Адаптивность	-	+	+	-	+
Устойчивость	+	-	+	+	-
Вычислительная сложность	Низкая	Средняя	Высокая	Низкая	Средняя

Одним из наиболее эффективных и перспективных методов обнаружения DDoS-атак является механизм работы нейронных сетей, широко применяющийся в современных средствах защиты.

Искусственная нейронная сеть – математическая модель, а также её программная или аппаратная реализация, построенная по принципу организации и функционирования

биологических нейронных сетей [9-10]. Производительность нейронной сети напрямую зависит от выбранной архитектуры, параметров и метода обучения.

Каждый нейрон представляет собой единицу обработки информации в нейронной сети. В модели нейрона можно выделить три основных элемента [5-6,8]:

1. Набор синапсов – входные значения, предаваемые в нейрон. Каждый синапс характеризуется своим весом.
2. Сумматор – складывает значения входных сигналов, взвешенных относительно соответствующих синапсов нейрона.
3. Функция активации – ограничивает амплитуду выходного значения сигнала нейрона.

В модели нейрона также реализован пороговый элемент, который отражает увеличение или уменьшение входного сигнала, подаваемого на функцию активации.

В математическом представлении функционирование нейрона можно описать следующими уравнениями:

$$u_k = \sum_{j=1}^{m} w_j x_j, \quad (1)$$

$$y_k = \varphi(u_k + b_k), \quad (2)$$

где $x_1 \dots x_m$ – входные сигналы; $w_{k1} \dots w_{km}$ – синаптические веса нейрона k; b_k – порог; $\varphi(u_k + b_k)$ – функция активации; y_k – выходной сигнал нейрона.

В качестве функции активации была выбрана сигмоидальная функция, график которой напоминает букву S. Данная функция задается следующим выражением:

$$\varphi(u_k + b_k) = \frac{1}{1 + \exp(-a(u_k + b_k))}, \quad (3)$$

где a – параметр наклона сигмоиды.

Следующим важным этапом в процессе создания нейронной сети является реализация обучения. Эффективность работы нейронной сети напрямую зависит от качественной настройки синаптических весов.

Обучение – это процесс, в котором свободные параметры нейронной сети настраиваются посредством моделирования среды, в которую эта сеть встроена. Тип обучения определяется способом настройки этих параметров.

Процесс обучения предполагает следующую последовательность событий:

1. В нейронную сеть поступают стимулы из внешней среды – входные значения.
2. В результате изменяются свободные параметры нейронной сети – синаптические веса.
3. После изменения внутренней структуры нейронная сеть отвечает на возбуждения уже иным образом.

В качестве алгоритма обучения был выбран один из наиболее известных [8] методов – метод обратного распространения ошибки. Обучение предполагает два вычислительных прохода по всем слоям сети: прямого и обратного. При прямом проходе входной вектор подается на входные узлы сети, после чего распространяется от слоя к слою. В результате генерируется набор выходных сигналов, который и является фактической реакцией сети. Во время прямого прохода все синаптические веса сети фиксированы; во время обратного прохода синаптические веса настраиваются в соответствии с правилом коррекции ошибок, а именно: фактический выход сети вычитается из желаемого отклика, в результате формируется сигнал ошибки. Этот сигнал впоследствии распространяется по сети в направлении, обратном направлению синаптических связей. Синаптические веса настраиваются с целью максимального приближения выходного сигнала сети к желаемому.

Вычисление сигнала ошибки сети задается следующей формулой:

$$e_j(n) = d_j(n) - y_j(n), \tag{4}$$

где $e_j(n)$ – сигнал ошибки нейрона j на итерации n, $d_j(n)$ – желаемый отклик нейрона j, $y_j(n)$ – сигнал, генерируемый на выходе нейрона j.

Обучение нейронной сети происходит путем расчета необходимой величины корректировки каждого из синаптических весов по следующей формуле:

$$\Delta w_{ji}(n) = a\Delta w_{ji}(n-1) + \eta\delta_j(n)y_i(n), \tag{5}$$

где a – положительное значение, называемое постоянной момента, η – параметр скорости обучения, i – синаптическая связь нейрона j с нейроном i, $\delta_j(n)$ – локальный градиент нейрона j, $y_i(n)$ – поступивший сигнал от нейрона i в нейрон j. Правая часть выражения (5) необходима для повышения скорости обучения без потери устойчивости, левая часть является классическим дельта-правилом изменения синаптических весов.

Локальный градиент определяется в соответствии с положением слоя, где находится нейрон:

$$\delta_j(n) = \begin{cases} e_j^{(L)}(n)\varphi_j'(u_k + b_k) & \text{для нейрона } j \text{ выходного слоя } L \\ \varphi_j'(u_k + b_k)\sum_k \delta_k^{(l+1)}(n)w_{kj}^{(l+1)}(n) & \text{для нейрона } j \text{ скрытого слоя } l. \end{cases} \tag{6}$$

Осуществив вычисление локального градиента нейронов, необходимо произвести постепенный расчет их новых весовых коэффициентов по формуле (5), начиная с выходного слоя. Новые весовые коэффициенты вычисляются после каждого обучающего примера.

В качестве обучающей выборки использована база сетевых атак одного из ведущих университетов [12]. В данную базу включены основные виды сетевых атак, в том числе атаки типа DDoS. База данных состоит из текстовых файлов, в каждой строке которых содержится

образ соединения, включающий 41 параметр сетевого трафика; образ соединения отмечен как «атака» или «не атака».

В связи с тем, что обучение нейронной сети будет осуществляться на примере DDoS-атак, исходная база данных была оптимизирована: выделены основные параметры соединения, достаточные для идентификации DDoS-атак и убраны записи сетевых образов, не относившихся к выбранному типу вредоносного воздействия.

В результате была составлена новая база данных, включающая записи 6 видов DDoS-атак: back, land, neptune, pod, smurf, teardrop. Каждая запись содержит 28 переменных; наиболее важные параметры представлены в таблице 2 [12].

Таблица 2

Основные параметры сетевого трафика

№	Параметр	Описание
1	duration	Продолжительность соединения
2	service	Служба
3	flag	Флаг терминального состояния IP-соединения
4	src_byte	Количество байт, передаваемых от источника к приемнику
5	dst_byte	Количество байт, переданных от приемника к источнику
6	land	Равенство порта отправителя порту получателя
7	wrong_fragment	Количество отброшенных пакетов
8	urgent	Число пакетов с флагом URG

При обучении нейронной сети и её дальнейшем использовании необходимо произвести предварительное нормирование параметров поступающих примеров, поскольку значения параметров могут отличаться друг от друга на несколько порядков. После нормализации значения элементов находятся в промежутке от 0 до 1 [4].

Нормализация каждого элемента происходит по формуле:

$$\widetilde{x_i} = \frac{x_i - x_{i(\min)}}{x_{i(max)} - x_{i(min)}}, \quad (7)$$

где $x_i -$ значение элемента до нормализации, $x_{i(min)}$ и $x_{i(max)} -$ минимальное и максимальное значения элементов, $\widetilde{x_i} -$ нормализованный параметр.

Результаты исследования

Для практической реализации нейронной сети была выбрана архитектура многослойного персептрона – многослойная нейронная сеть прямого распространения. Сеть состоит из множества входных узлов, образующих первый слой, нескольких скрытых слоев вычислительных нейронов и одного выходного слоя нейронов. Входной сигнал распространяется по сети в прямом направлении, от слоя к слою.

Для определения количества скрытых слоев и числа нейронов в каждом скрытом слое были проведены исследования эффективности работы нейронных сетей различных структур по ключевым параметрам.

Вначале оценивалась эффективность работы нейронной сети с разным количеством нейронов в единственном скрытом слое. Размер обучающей выборки во всех экспериментах составил 70 % от составленной базы данных. Далее изучалось влияние количества слоев нейронной сети на успешность вычислений, в каждом скрытом слое нейронной сети находилось 28 нейронов. После этого производился поиск оптимального количества нейронов второго скрытого слоя. Эффективность работы нейронной сети оценивалась по следующим критериям: скорость обучения, количество ошибок и вычислительная сложность.

Оптимальный результат показала нейронная сеть со следующей архитектурой:

- входной слой;
- первый скрытый слой из 28 нейронов;
- второй скрытый слой из 14 нейронов;
- выходной слой.

Используя полученные данные, в среде Microsoft Visual Studio был разработан программный комплекс на языке C#, который включает несколько режимов работы: обучение, тестирование и диагностику. В режиме обучения происходит изменение синаптических весов согласно выбранному алгоритму обучения. Реализованные опции, такие как скорость обучения, диапазон угла наклона сигмоиды, параметр порога и величина момента градиентного спуска, позволяют настраивать режим обучения. В режиме тестирования осуществляется анализ корректности подобранных синаптических весов нейронной сети; в режиме диагностики нейронная сеть выполняет проверку лог-файлов на наличие аномалий, свидетельствующих о DDoS-атаке.

На основе разработанного программного комплекса были проведены исследования влияния параметров обучения на эффективность работы нейронной сети: начальные значения параметров были заданы случайным образом, их коррекция осуществлялась вручную в процессе обучения. Сравнительный анализ начальных и предложенных значений параметров проводился путем подсчета ошибок первого и второго рода в режиме тестирования нейронной сети с использованием тестовой выборки. Ошибки первого рода представляют собой ситуацию, когда авторизованные пользователи классифицируются как нарушители; ошибки второго рода – когда нарушители классифицируются как авторизованные пользователи.

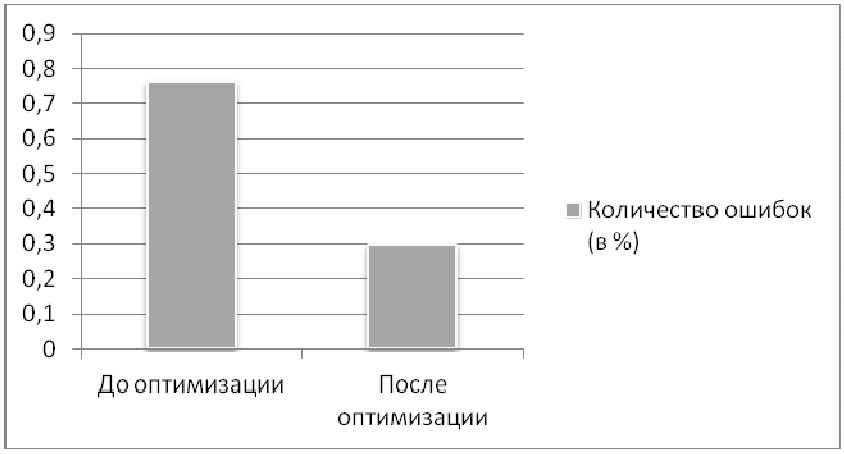

Рисунок 1. Сравнительный анализ работы нейронной сети

Выводы

При обработке обучающей выборки общее число ошибок из 200 000 примеров при начальных параметрах достигало 0,762 %. После оптимизации параметров обучения общее число ошибок снизилось до 0,298 %. Для обучения нейронной сети были выбраны следующие значения параметров:

- скорость обучения: 0,300;
- угол наклона сигмоиды: 2,0;
- параметр порога: 0,250;
- величина момента: 0,200.

Список литературы

1. Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: дисс. … канд. физико-математических наук / Моск. гос. ун-т им. М.В. Ломоносова. – М., 2007.

2. Гостев А. Kaspersky. Основная статистика за 2009 год // Securelist.com URL: http://www.securelist.com/ru/analysis/208050606/Kaspersky_Security_Bulletin_2009_Osnovnaya_statistika_za_2009_god (дата обращения: 17.04.2014).

3. Гостев А. Kaspersky. Основная статистика за 2010 год // Securelist.com URL: http://www.securelist.com/ru/analysis/208050678/Kaspersky_Security_Bulletin_2010_Osnovnaya_statistika_za_2010_god (дата обращения: 17.04.2014).

4. Жульков Е. В. Построение модульных нейронных сетей для обнаружения классов сетевых атак: дисс. … канд. техн. наук / Политехн. ун-т. – Санкт-Петербург, 2007.

5. Малыхина М.П., Бегман Ю.В. Гибридные нейроэкспертные системы в образовании // Материалы XIV Всероссийской научно-практической конференции «Инновационные процессы в высшей школе», 2008. – С. 193-194.

6. Малыхина М.П. Оценка эффективности гибридизации интеллектуальных методов на примере нейросетевой экспертной системы на основе прецедентов // Малыхина М.П., Бегман Ю.В. // Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2013. – № 86(02). – С. 253-262.

7. Наместников Ю. Kaspersky. Основная статистика за 2010 год // Securelist.com URL: http://www.securelist.com/ru/analysis/208050741/Kaspersky_Security_Bulletin_Osnovnaya_statistika_za_2011_god (дата обращения: 17.04.2014).

8. Хайкин С. Нейронные сети: полный курс, 2-е издание: пер. с англ. – М.: Издательский дом "Вильямс", 2006.

9. Частиков А.П., Дедкова Т.Г., Алешин А.В. Системы искусственного интеллекта. От теории к практике. – Краснодар, 1998. – 166 с.

9. Частиков А.П., Тотухов К.Е., Урвачев П.М. Интеллектуальная диагностика состояния виртуального робота с программным управлением // Современные проблемы науки и образования. – 2012. – № 6.

10. Peng Liu. Denial of Service Attacks. School of Information Sciences and Technology. University Park, 2004.

11. UCI KDD Archive // kdd.ics.uci.edu URL: http://kdd.ics.uci.edu/databases/kddcup99/ (дата обращения 20.04.2014).

Рецензенты:

Ключко В.И., д.т.н., профессор, профессор кафедры ИСП Кубанского государственного технологического университета, г. Краснодар;

Пиотровский Д.Л., д.т.н., профессор, зав. кафедрой АПП Кубанского государственного технологического университета, г. Краснодар.