004.94

К ВОПРОСУ ЗАЩИТЫ ИНФОРМАЦИИ ОТ СЕТЕВЫХ АТАК НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

В.А. ЧАСТИКОВА, Д.А. КАРТАМЫШЕВ

Кубанский государственный технологический университет
350072, Российская Федерация, г. Краснодар, ул. Московская, 2
электронная почта: chastikova_va@mail.ru

В статье рассматривается разработка и исследование методики защиты от сетевых атак типа DDoS на основе механизма работы нейронных сетей. Для этого был проведен анализ эффективности работоспособности нейронных сетей различных структур. Архитектура, показавшая наилучший результат, была реализована в виде программного комплекса в среде Microsoft Visual Studio на языке C#. На основе разработанного комплекса осуществлялось тестирование реализованного алгоритма защиты. В процессе исследований была произведена оптимизация параметров обучения нейронной сети, что существенно повысило эффективность работы сети и снизило количество ошибок распознавания нейронной сети.
Ключевые слова: сетевые атаки, DDoS-атаки, нейронная сеть, персептрон.

Среди множества видов сетевых атак наибольшее распространение получила атака типа DDoS. По данным статистики [1] подобный вид угрозы занимает одно из лидирующих мест ежегодно.

DDoS-атака – вид злонамеренной деятельности, ставящей своей целью довести компьютерную систему до состояния, когда обслуживание правомерных пользователей и корректное выполнение возложенных на нее функций невозможно[2].

Для успешного противодействия сетевым атакам разрабатываются различные методы и механизмы защиты. Практически все современные программные и программно-аппаратные средства защиты используют как один механизм противодействия, так и целый набор методов. Одним из наиболее эффективных и перспективных алгоритмов обнаружения DDoS-атак является механизм работы нейронных сетей [3].

Искусственная нейронная сеть — математическая модель, а также её программная или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей. В модели

нейрона можно выделить три основных элемента [4]: набор синапсов, сумматор и функцию активации.

В математическом представлении функционирование нейрона можно описать следующим уравнением:

$$y_k = \varphi\left(\sum_{j=1}^{m} w_j x_j + b_k\right),$$

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

В качестве алгоритма обучения был выбран один из наиболее распространенных и эффективных [3] – метод обратного распространения ошибки. Во время процесса обучения все синаптические веса настраиваются в соответствии с правилом коррекции ошибок, а именно: фактический результат работы сети вычитается из желаемого ответа, 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.

Корректировка каждого синаптического веса осуществляется по формуле:

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

где a – постоянная 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 к нейрону j. Правая часть выражения необходима для повышения скорости обучения без потери устойчивости, левая часть является классическим дельта-правилом изменения синаптических весов.

Для практической реализации нейронной сети, была выбрана архитектура многослойного персептрона – многослойной нейронной сети прямого распространения. Сеть состоит из нескольких скрытых слоев вычислительных нейронов. Входной сигнал распространяется по сети в прямом направлении от слоя к слою.

В ходе исследований осуществлялся анализ эффективности работы нейронной сети различных структур. Наилучший результат показала нейронная сеть, обладающая следующей структурой: первый скрытый слой из 28 нейронов, второй скрытый слой из 14 нейронов.

Используя полученные результаты, в среде Microsoft Visual Studio на языке C# был разработан программный комплекс. На его основе были проведены исследования влияния параметров обучения на работу нейронной сети: начальные значения параметров были заданы случайным образом, их коррекция осуществлялась вручную в процессе обучения.

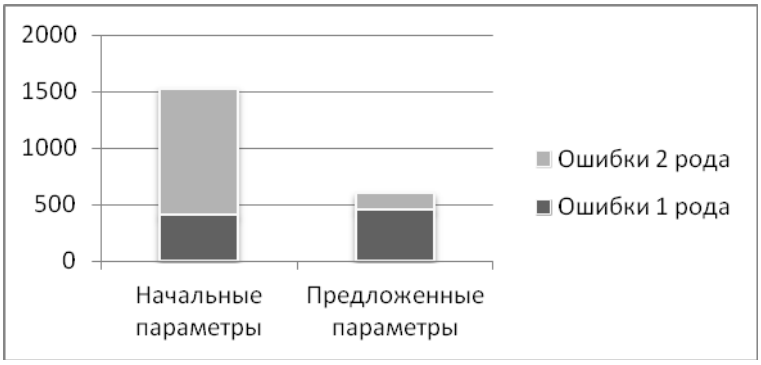

Рисунок 1 - Сравнительный анализ работы нейронной сети

Сравнительный анализ начальных и предложенных значений параметров производился путем подсчета ошибок первого и второго рода. Ошибки первого рода - когда авторизованные пользователи классифицируются как нарушители. Ошибки второго рода - когда нарушители классифицируются как авторизованные пользователи.

ЛИТЕРАТУРА

1. 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).

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

3. Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: диссертация … кандидата физико-математических наук. Моск. Гос. ун-т им. М.В. Ломоносова, Москва, 2007.

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

REFERENCES

1. Namestnikov Y. Summary statistics for the year 2010 // Securelist.com URL: http://www.securelist.com/ru/analysis/208050741/Kaspersky_Security_Bulletin_Osnovnaya_statistika_za_2011_god (date accessed: 17.04.2014).

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

3. Gamayunov D. Y. Detection of network attack based on the analysis of the behavior of network entities: dissertation of the candidate of physical and mathematical sciences. Lomonosov Moscow State University, 2007.

4. Haykin S. Neural Networks and Learning Machines, 2006.

TO THE QUESTION OF INFORMATION PROTECTION FROM NETWORK ATTACKS BASED ON NEURAL NETWORKS

V.A. CHASTIKOVA, D.A. KARTAMYSHEV

Kuban State Technological University
2, Moskovskaya st., Krasnodar, Russian Federation, 350072,
e-mail: chastikova_va@mail.ru

The article contains the development and research methods to protect from network attacks type DDoS on the basis of neural networks mechanism. Efficiency analysis the operability of neural networks different structure was executed on first stage of work. The best architecture with high result was implemented as bundled software in programming environment Microsoft Visual Studio on C#. With the help of designed program was implemented testing of protection algorithms. In process of research an algorithm the parameters for training neural network was optimized, what increased the operational efficiency and reduced the amount of identification errors in neural network.

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