УДК 004.02

ОБНАРУЖЕНИЕ DDOS-АТАК НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ С ПРИМЕНЕНИЕМ МЕТОДА РОЯ ЧАСТИЦ В КАЧЕСТВЕ АЛГОРИТМА ОБУЧЕНИЯ

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

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

Для разработки методики обнаружения DDoS-атак на основе нейронных сетей проведены исследования эффективности работы ряда методов роевого интеллекта. По результатам исследований для настройки параметров нейронной сети выбран метод роя частиц, который показал высокую скорость и точность вычислений. Разработан программный комплекс, в котором реализована нейронная сеть вида многослойный персептрон, обучающаяся методом обратного распространения ошибки. На ее основе проводилась настройка параметров метода роя частиц, который был использован как алгоритм обучения нейронной сети совместно с методом обратного распространения ошибки для повышения эффективности процесса обучения. Коррекция синаптических весов с применением данного подхода существенно снижает значение среднеквадратичной ошибки с каждым пройденным примером. Также уменьшается количество ложных срабатываний в уже обученной сети, настроенной на обнаружение DDoS-атак.

Ключевые слова: DDoS-атака, метод роя частиц, искусственная нейронная сеть, роевой интеллект

DDOS ATTACKS DETECTION ON THE BASIS OF NEURAL NETWORKS USING THE PARTICLE SWARM OPTIMIZATION AS A LEARNING ALGORITHM

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

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

For developing methods of DDoS attacks detection based on neural networks were conducted researches on the work efficiency of a number of swarm intelligence methods. By results of researches for setting the parameters of the neural network was chosen particle swarm optimization, which showed a high speed and accuracy of computations. The developed program complex, which is implemented in the neural network of a multilayer perceptron, learning error back-propagation algorithm. On its basis were held settings particle swarm optimization, which was used as a neural network learning algorithm together with error back-propagation algorithm to increase the efficiency of the learning process. Correction of synaptic weights using this approach significantly reduces the value of root mean square error with each passed example. It also reduces the number of false alarms in the already trained network configured on the DDoS attacks detection.

Keywords: DDoS attack, particle swarm optimization, artificial neural network, swarm intelligence

С развитием сетевых технологий развиваются и сетевые угрозы. В последнее время все большую актуальность приобретают DDoS-атаки. DoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) – атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ значительно затруднён. Распределенная атака DoS (distributed DoS, DDoS) проводится одновременно через множество устройств [7].

Для противодействия DDoS-атакам применяется целый ряд механизмов, особой значимостью обладают средства обнаружения вторжений. Ведь своевременное обнаружение DDoS-атаки позволит сохранить работоспособность сети, так как если не остановить у провайдера трафик, предназначенный для переполнения атакуемой сети, то сделать это на входе окажется невозможным, поскольку вся полоса пропускания будет уже занята. Стандартные методы анализа статистики не позволяют выявлять неизвестные ранее атаки, поэтому в качестве механизма решения данной проблемы активно выступают нейронные сети.

Искусственная нейронная сеть (ИНС) – математическая модель, а также её программная или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма [2, 3]. ИНС используются практически во всех средствах обнаружения вторжений как отдельно, так и в комплексе с другими механизмами защиты.

Целью исследования является анализ мер противодействия и совершенствование механизма защиты от DDoS-атак в виде средства обнаружения вторжений на основе искусственных нейронных сетей, результаты которой возможно применить в уже существующих системах защиты. В данной работе отражены результаты исследований, настройки и применения метода роя частиц при оптимизации параметров нейронной сети для эффективного обнаружения DDoS-атак.

Материалы и методы исследования

В работе использовалась модель многослойного персептрона с двумя скрытыми слоями, построенная на сигмоидальной логистической функции активации. Количество входных сигналов – 28. В скрытых слоях количество нейронов составляет 28 и 14, в выходном слое содержится 2 нейрона. Представленная модель выдает ответы (1, 0) и (0, 1), характеризующие наличие или отсутствие атаки.

Для анализа эффективности обучения сети была выбрана база данных, составленная одним из ведущих университетов [9], содержащая в себе сведения об атаках различных типов, однако в рассматриваемой работе использовались лишь те параметры, которые отвечают за атаки типа DoS.

В настоящее время при оптимизации параметров сложных систем [5] все чаще применяются природные механизмы поиска; в последние годы интенсивно разрабатывается научное направление «Роевой интеллект» (Swarm intelligence), включающее в себя целый ряд эвристических алгоритмов. Для исследования эффективности работы указанных алгоритмов был разработан программный комплекс, на основе которого проведен сравнительный анализ [4]. Так как достаточно высокую скорость и точность вычислений показал метод роя частиц, для оптимизации параметров нейронной сети был выбран именно он.

Метод роя частиц (МРЧ), particle swarm optimization (PSO) – эвристический метод оптимизации, использующий имитацию социального поведения роя некоторых элементов (птиц, рыб, светлячков, пчел и т.д.), применение которого не требует знания точного градиента оптимизируемой функции.

В алгоритме агентами являются частицы, которые в каждый момент времени имеют в пространстве параметров задачи некоторое положение и скорость. Правила, по которым частица меняет свое положение и скорость, определяются на основе вычисления целевой функции частицы. Канонический метод роя частиц был предложен в 1995 г. в работе J. Kennedy, R. Eberhart [6], в основе которого лежит следующий принцип: на каждой итерации для определения следующего положения частицы учитывается информация о наилучшей единице от «соседей» и информация о данной частице на том шаге, когда ей соответствовало оптимальное значение целевой функции. Существуют модификации канонической модели, учитывающие значения целевых функций всех частиц роя, в некоторых моделях частицы группируются в несколько роев и т.д. [1].

В классическом варианте алгоритма скорость каждой частицы в рое изменяется по следующей формуле:

$$v_{i+1} = o \cdot v_i + a_1 \cdot rnd \cdot \left(pbest_i - x_i\right) + a_2 \cdot rnd \cdot \left(gbest_i - x_i\right), \quad (1)$$

где v_i – скорость частицы в момент времени i; x_i – координата частицы в момент времени i; o – весовая доля инерции; a_1, a_2 – некоторые константы; rnd – случайное значение в промежутке (0; 1]; $pbes_i$, $gbest_i$ – локальное и глобальное лучшее положение частицы в момент времени i.

Затем происходит изменение положения каждой из частиц:

$$x_{i+1} = v_{i+1} + x_i. \quad (2)$$

Следует отметить, что значения скорости и координаты представлены в виде векторных значений и содержат множество компонент, а не просто одно скалярное значение. Количество итераций и частиц в рое указывают на продолжительность работы алгоритма, а следовательно, и на качество получаемых результатов; значения констант определяются экспериментально исходя из поставленной задачи.

Процесс обучения нейронной сети представляет собой стандартный метод обратного распространения ошибки, после работы которого синаптические веса дополнительно корректируются. Схема обучения представлена на рисунке.

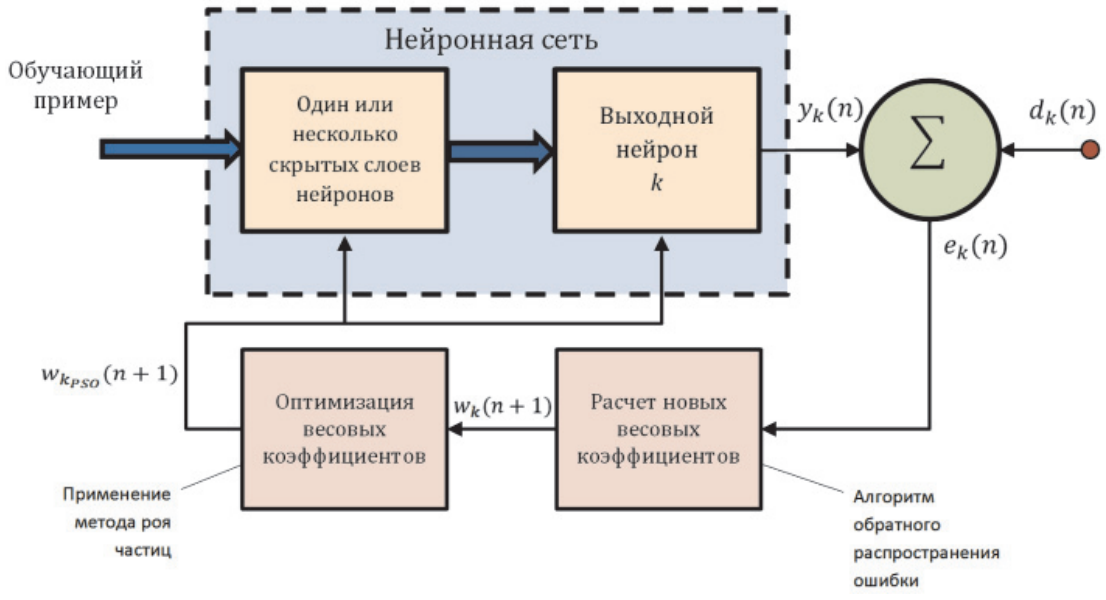

Схема обучения нейронной сети

Синаптические веса каждого нейрона k с помощью метода обратного распространения ошибки рассчитываются по следующей формуле:

$$\Delta w_{kj}(n) = m \cdot \Delta w_{kj}(n-1) + \mu e_k(n) \cdot \varphi_k(v_k) y_j(n). \quad (3)$$

Затем синаптические веса дополнительно корректируются методом роя частиц:

$$gbest = w_k(n) + \Delta w_k(n); \quad (4)$$

$$pbest_i = \min_{0 \le q \le N} E(x_{i,q}); \quad (5)$$

$$w_k(n) = \min_{0 \le i \le L} E(pbest_i). \quad (6)$$

Полученный результат метода обратного распространения ошибки записывается в вектор *gbest*, затем создается рой с количеством частиц L, где L – количество синаптических связей каждого нейрона в слое, а переменная N отображает количество нейронов в рассматриваемом слое. Далее случайно генерируются начальные координаты каждой из частиц и их скорости. После каждой итерации алгоритма в переменную $pbest_i$ заносится лучший текущий результат, при котором значение среднеквадратичной ошибки минимально. После N итераций алгоритма оптимальное значение $pbest_i$ записывается в вектор синаптических весов $w_k(n)$, где n – номер обучающего примера.

Одной из основных задач является правильная настройка параметров метода роя частиц, так как при неправильной настройке метода процесс обучения может вовсе остановиться на хаотичных и слишком больших значениях синаптических весов, при которых, вне зависимости от входных параметров, на выходе получается один и тот же результат. Или же метод роя частиц совсем не окажет никакого воздействия на процесс обучения.

В задаче разработки средства обнаружения вторжений оптимальные начальные значения синаптических весов лежат в промежутке [–0,5; 0,5], поэтому исходные положения частиц целесообразно генерировать в том же диапазоне значений [–0,5; 0,5]. Чтобы частицы не разлетались далеко за пределы установленного промежутка и кардинально не нарушили процесс обучения, необходимо задать им начальные скорости движения в диапазоне [–0,03; 0,03]. Далее в ходе проведенных исследований были экспериментально установлены оптимальные значения констант: $a_1 = 0{,}4$; $a_2 = 0{,}5$, а также значение весовой доли инерции: $o = 0{,}5$.

Использование корректора необходимо применять только в том случае, если нейронная сеть дает ответ, близкий к желаемому, ведь в противном случае синаптические веса резко изменяются, вызывая еще большую неточность в работе алгоритма обучения. Во избежание смещения синаптических весов в сторону одной из возможных комбинаций значений выходного слоя нейронной сети необходимо подавать обучающие примеры с равновероятным желаемым ответом. В целях повышения эффективности работы алгоритма обучения рекомендуется подавать одновременно несколько примеров со всевозможными комбинациями выходных значений сети.

Результаты исследования и их обсуждение

Таким образом, была достигнута оптимальная настройка параметров метода роя частиц, которая оказывает существенное влияние на ход процесса обучения методом обратного распространения ошибки, постепенно снижая значение среднеквадратичной ошибки всей сети и уменьшая количество ложных срабатываний.

Для исследования эффективности работы предложенной методики был разработан программный модуль, в котором реализована вышеописанная модель нейронной сети, обучающейся по одному из выбранных пользователем методов. Используется одна и та же база для обучения, состоящая из 283891 примеров, а для проверки правильности полученного решения создана вторая база такого же размера, но с совершенно иными примерами входных данных, чтобы иметь возможность проанализировать вероятность обнаружения неизвестных атак. Для анализа точности полученного ответа рассчитывалось значение среднеквадратичной ошибки:

$$E = \frac{1}{2} \cdot \sum (d_k(n) - y_k(n))^2, \quad (7)$$

где $d_k(n)$ – желаемый ответ; $y_k(n)$ – полученный ответ.

В ходе сравнительного анализа исследуемых методов обучения (стандартный метод обратного распространения ошибки и метод роя частиц) проведено несколько повторяющихся этапов процесса обучения вновь сгенерированной нейронной сети во избежание ошибок полученных результатов. Усредненные значения среднеквадратичных ошибок занесены в таблицу.

Сравнительный анализ среднеквадратичной ошибки

Количество пройденных примеров	Среднеквадратичная ошибка метода обратного распространения ошибки	Среднеквадратичная ошибка метода роя частиц
100	0,004	0,00016
1000	2,65E-05	2,79E-05
5000	2,37E-05	1,08E-08
10000	8,54E-06	2,58E-09
30000	4,98E-06	1,11E-13
60000	3,19E-06	3,97E-16
100000	1,79E-06	6,45E-17
150000	9,61E-07	4,02E-20
250000	1,19E-06	3,88E-22

Из таблицы видно, что при использовании метода роя частиц для коррекции алгоритма обучения значение среднеквадратичной ошибки резко стремится к нулю в отличие от метода обратного распространения ошибки.

Выводы

Разработанная методика применения метода роя частиц в качестве алгоритма обучения нейронной сети не только повышает точность получаемых результатов, но и снижает количество ложных срабатываний. Так, например, сеть, обученная всей базой из 283891 примеров стандартным методом обратного распространения ошибки, выдает 670 ошибок (0,670%) из 100000 тестовых примеров, тогда как методом роя частиц – 439 ошибок (0,439%).

Такое незначительное количество ошибок в обоих случаях обусловлено большим размером нейронной сети для задачи обнаружения факта атаки, то есть для вывода результата «да» или «нет». Но для более сложных задач (например, для распознавания вида атаки) с помощью данной методики можно заметно уменьшить количество ложных срабатываний (ошибок), а резкое повышение точности вычислений позволит значительно сократить время обучения.

Список литературы

1. Карпенко А.П., Селиверстов Е.Ю. Обзор методов роя частиц для задачи глобальной оптимизации (Particle Swarm Optimization // Наука и образование: электронное научно-техническое издание. – 2009. – № 3. – URL: http://technomag.edu.ru/doc/116072.html (дата обращения 28.04.2014).

2. Малыхина М.П., Бегман Ю.В. Нейросетевая экспертная система на основе прецедентов для решения проблем абонентов сотовой связи: монография. – Краснодар, 2011.

3. Хайкин С. Нейронные сети. Полный курс. –2-е изд. – М.: Издательский дом «Вильямс», 2006. – 1104 с.

4. Частикова В.А., Власов К.А. Разработка и сравнительный анализ эвристических алгоритмов для поиска наименьшего гамильтонова цикла в полном графе // Фундаментальные исследования. – 2013. – № 10. – С. 63–67.

5. Частиков А.П., Тотухов К.Е., Урвачев П.М. Теоретические основы интеллектуальной диагностики виртуального робота // Современные проблемы науки и образования. – 2013. – № 1. – С. 153. (дата обращения 18.04.2014).

6. Kennedy J., Eberhart R. Particle swarm optimization // Proceedings of IEEE International conference on Neural Networks. – 1995. – P. 1942–1948.

7. Denial of service attack. – URL: http://en.wikipedia.org/wiki/Denial-of-service_attack (дата обращения 18.04.2014).

8. Swarm intelligence. – URL: http://en.wikipedia.org/wiki/Swarm_intelligence(дата обращения 18.04.2014).

9. KDD Cup 1999 Data. – URL: http://kdd.ics.uci.edu/databases/kddcup99/(дата обращения 18.04.2014).

References

1. Karpenko A.P., Seliverstov E.Ju. Obzor metodov roya chastits dlya zadachi globalnoy optimizatsii (Particle Swarm Optimization // Nauka i obrazovanie: elektronnoe nauchno- tekhnicheskoe izdanie, 2009, no. 3. URL: http://technomag.edu.ru/doc/116072.html (data obrashheniya 28.04.2014).

2. Malykhina M.P., BegmanYu.V. Neyrosetevaya ekspertnaya sistema na osnove pretsedentov dlya resheniya problem abonentov sotovoy svyazi. Monografiya. Krasnodar, 2011.

3. Hajkin S. Neyronnye seti. Polnyy kurs.Vtoroe izdanie. Izdatelskiy dom «Vilyams», 2006. 1104 p.

4. Chastikova V.A., Vlasov K.A. Razrabotka i sravnitelnyy analiz evristicheskikh algoritmov dlya poiska naimenshego gamiltonova tsikla v polnom grafe. Fundamentalnye issledovaniya, no. 10, 2013. pp. 63–67.

5. Chastikov A.P., Totukhov K.E., Urvachev P.M. Teoreticheskie osnovy intellektualnoy diagnostiki virtualnogo robota. Sovremennye problem nauki i obrazovaniya, 2013, no. 1. pp. 153. (data obrascheniya 18.04.2014)

6. Kennedy J, Eberhart R. Particle swarm optimization // Proceedings of IEEE International conference on Neural Networks. 1995. pp. 1942–1948.

7. Denial of service attack. URL: http://en.wikipedia.org/wiki/Denial-of-service_attack (data obrascheniya 18.04.2014).

8. Swarm intelligence. URL: http://en.wikipedia.org/wiki/Swarm_intelligence(data obrascheniya 18.04.2014).

9. KDD Cup 1999 Data. URL: http://kdd.ics.uci.edu/databases/kddcup99/(data obrascheniya 18.04.2014).

Рецензенты:

Видовский Л.А., д.т.н., доцент, зав. кафедрой информационных систем и программирования, ФГБОУ ВПО «Кубанский государственный технологический университет», г. Краснодар;

Ключко В.И., д.т.н., профессор кафедры информационных систем и программирования, ФГБОУ ВПО «Кубанский государственный технологический университет», г. Краснодар.

Работа поступила в редакцию 04.06.2014.