СПИСОК ЛИТЕРАТУРЫ

1. Режущий инструмент. Курсовое и дипломное проектирование [Текст]: учеб. пособие / Под ред. Е.Э. Фельдштейна. Мн.: Дизайн ПРО, 2002, - 320 с.
2. Проектирование зубчатых передач и планетарных механизмов с использованием ЭВМ [Текст]: учеб. пособие / Под ред. Г.А. Тимофеева. М.: Изд-во МГТУ им. Н.И. Баумана, 2000, - 60 с.
3. Желтобрюхов Е.М. Автоматизированное проектирование червячных шлицевых фрез [Текст]: / Е.М. Желтобрюхов, М.С. Кузнецов // Ползуновский вестник, 2011, № 3/1, - С.22-25

*Зав. кафедрой, **Е.М. Желтобрюхов**, к.т.н., доцент, (3902)225355, tms_hti@list.ru; инженер кафедры, **М.С. Кузнецов**, e-mail: mikha20@yandex.ru; студент, **А.В. Неклюдов**, e-mail: vxfw@mail.ru - Хакасский технический институт – филиал СФУ, кафедра машиностроительных и металлургических технологий, tms_hti@list.ru, (3902)225355.*

УДК 004.891.3

МЕТОД ФИЛЬТРАЦИИ ВХОДЯЩЕГО ТРАФИКА НА ОСНОВЕ ДВУХСЛОЙНОЙ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

М. Е. Бурлаков

В статье рассматривается принцип фильтрации входящего в вычислительную (далее компьютерную) систему трафика с использованием алгоритма на основе двухслойной рекуррентной нейронной сети. Предложена вероятностная схема самообучающегося механизма фильтрации трафика в компьютерных сетях. Рассмотрена применимость анализируемых нейронных сетей против угроз отказа в обслуживании. Разработанная система фильтрации входящего трафика апробирована на реальном примере.

Ключевые слова: вычислительные сети, фильтрация трафика, нейронная сеть, рекуррентные нейронные сети, защита вычислительных сетей.

Введение

В ходе развития компьютерных сетей (КС), вопрос защиты является наиболее актуальным. Существует множество внешних и внутренних факторов, влияющих на формирование угроз доступности информации. Наиболее опасной угрозой, в этом плане, является угроза отказа компьютерной сети в обслуживании (*DDos*). Данная угроза реализуются путем непропорционального увеличения трафика в сторону КС и неспособности ее узлов (серверы, маршрутизаторы) данный трафик обслужить.

Основными требованиями, которые предъявляются к системам противодействия отказам в обслуживании, являются:

1. Скорость реакции на нелегитимный трафик;
2. Способность с высокой вероятностью определить ложный и легитимный запрос;
3. Масштабируемость и совместимость с системами безопасности КС.

Существует множество комплексных решений, которые обладают своими преимуществами и недостатками [1]. Многие из существующих основаны на классических статистических методах. В данной статье рассматривается метод противодействия угрозам отказа в обслуживании на основе двухслойной рекуррентной нейронной сети.

Определение параметров

Для построения алгоритма определим ряд наиболее существенных параметров, анализ которых позволит построить механизм фильтрации трафика. Все параметры берутся из стандартного TCP/IP пакета, вид которого представлен в Таблице1 Ниже приведены наиболее значимые из них:

Таблица 1 - Стандартный вид записи TCP-IP пакета в журнале отчета сервера

1.1.1.1 - - [06/*May*/2012:00:08:19 +0400] "*GET http://example.ru/map6095*" 200 2156 "-" "*Mozilla*/5.0 (*compatible*; *Googlebot*/2.1; *+http://www.google.com/bot.html*)" 1

1. Статус (*status*) ответа сервера (200,404, 500, 503 и другие коды);
2. Тип (*type*) запроса к серверу (*GET, POST, HEAD*);
3. Тип клиента (User-Agent), инициировавшего запрос;
4. Источник (Referer) (откуда запрос пришел);
5. *URL* и http_version.

От URL берутся: протокол, имя хоста и все дополнительные параметры строки запроса (query_string). Данные категории будут

определять множество признаков для дальнейшего обучения нейронной сети.

Подготовительный этап

Для проведения подготовительного этапа необходимо наличие легитимных и нелегитимных запросов к КС (к таковым можно, например, отнести данные о запросах к серверу в журнале отчетов до и после момента начала фильтрации). Эти условия позволят в ходе дальнейшего обучения системы качественнее определить фильтруемое содержимое.

К нелегитимным запросам отнесем запросы, имеющие следующие параметры:

1. Статус (*status*) ответа запросу не будет равен 200 или 404;
2. Тип клиента не соответствует стандарту *RFC2616;*
3. Протокол URL не ровняется 1.0 или 1.1.

Отметим ряд косвенных параметров пакета, наличие или отсутствие которых, при определенных условиях, позволяет определить его легитимность:

1. Referer является прямым (т.е. обращение идет напрямую к самому источнику(серверу), например, сразу к сайту или инфраструктуре КС);
2. URL содержит нехарактерные элементы (например, наличие символа “?” при полностью включенном механизме ЧПУ на сайте).

Причина косвенности, выше описанных параметров в том, что первый параметр (*Referer*) нивелируется при постоянном, большом обращении («популярности») к ресурсу КС, второй параметр (*URL*) стоит учитывать только тогда, когда структура ресурса КС жестко детерминирована и полностью отвечает поставленным выше условиям, в противном случае данный параметр не имеет смысл использовать.

Определим шаблон записи как множество параметров, которые формируют векторы признаков для дальнейшей идентификации каждого запроса. Другими словами, шаблон записи это калька, по которой вектор признаков принимает то или иное значение в зависимости от выбранной записи.

Под вектором признаков будем понимать бинарную матрицу размера d×1, где d – нечетное количество признаков, соответствующих всем записям из журнала отчетов. Другими словами, d определяет размерность вектора шаблона. Значение «0» в данной матрице будет говорить о наличии параметра у данного пакета, «1» - об отсутствии. Нечетное количество признаков выбиралось из соображения получения явного результирующего значения, равного бинарной сумме (исключающее ИЛИ) всех значений данного вектора признаков. Результирующее значение определяется следующим выражением.

$$q = \sum v_j, \qquad (1)$$

где v_j – j-ое значение бинарного вектора признака.

Соответствие того или иного запроса вектору признаков будет определять его принадлежность к легитимному или нелегитимному множеству.

Обучение и тестирование системы

Под обучением системы понимается процесс построения оптимального шаблона записи, применение которого даст минимальную ошибку при тестировании алгоритма.

Для обучения необходимо иметь некоторое множество записей запросов из журнала запросов (как легитимных, так и нелегитимных). Множество записей разделим на три подмножества: для обучения, для тестирования и для подбора наиболее оптимального состояния системы. Отношение количества между элементами данного множества рассчитывается эмпирически. Отметим, что увеличенный процент обучающих записей может привести к процессу «переобучения» системы, это происходит тогда, когда процент высок при распознавании обучающих записей, но низок при использовании на тестовых записях. Увеличенное значение процентов в сторону тестовых записей может привести к «недообучению» системы, также негативно влияющему на дальнейшую эффективность в целом.

Для формирования процесса обучения введем бинарную матрицу A. Размерность матрицы A должна ровняться m×n. Данная матрица получена умножением вектора шаблона записи размерности m=d+1 (1 - результирующее значение вектора признаков q) на n бинарных векторов признаков (где значение 0 – когда данный параметр данного вектора определяет легитимный источник, 1 – нелегитимный).

Для формирования процесса тестирования введем результирующее значение w, определяемое обучающей матрицей A и результирующим значением бинарной суммы векторов признаков q, которое имеет следующий вид:

$$w = \sum v_j \times A_i, \qquad (2)$$

где A_i – i-ый столбец матрицы A.

Под корректным значением w будем понимать значение 0 – если запись является легитимной и 1 - если нет.

В результате тестирования и обучения из матрицы *A* исключаются вектора, вносящие искажения в результирующее значение *w*. Таким образом, образуется новая бинарная матрица *A'*, которая используется при дальнейшем подборе оптимального состояния системы на нейронной сети.

Построение и работа нейронной сети

Определим рекуррентную нейронную сеть как сеть с обратной связью, состоящую из искусственных нейронов. Характеристика двуслойности означает наличие двух слоев нейронов в данной сети. Искусственный нейрон, с математической точки, это нелинейная функция от единственного аргумента, которая является линейной комбинацией всех входных сигналов нейрона. Данная функция называется функцией активации или функцией срабатывания.

Существует множество видов функций активации. В конкретном случае можно выделить два типа: бинарные и аналоговые. Под бинарными понимают функции, выходы которых равны либо нулю, либо единице (например, пороговая передаточная функция). Под аналоговыми функциями понимают функции область, значений которых лежит в заданном диапазоне (логистическая функция, сигмоида). Так как в самом начале исследования ставилась цель не просто определить легитимность пакета, но и расширить классифицирующую составляющую, для дальнейшего построения функции активации используется сигмоида, определяемая следующей формулой:

$$\sigma(x) = \frac{1}{1+e^{-x}}, \qquad (3)$$

Область значений данной функции лежит в диапазоне [0,1], где крайнее значение 0 показывает полную принадлежность запроса к легитимному множеству запросов, а 1 – принадлежность к нелегитимному множеству.

В качестве функции активации второго слоя возьмем *k-Binary* классифицирующую функцию. Выбор именно такой функции был определен благодаря ее способности к расширению классифицирующей структуры ответа первого слоя нейронной сети. Это, в свою очередь, позволит более ранжировано дать характеристику тому или иному запросу.

Схематически, нейронная сеть представлена на рисунке 1.

Любая рекуррентная нейронная сеть обладает свойством ухода в локальный минимум при каждой итерации своей работы.

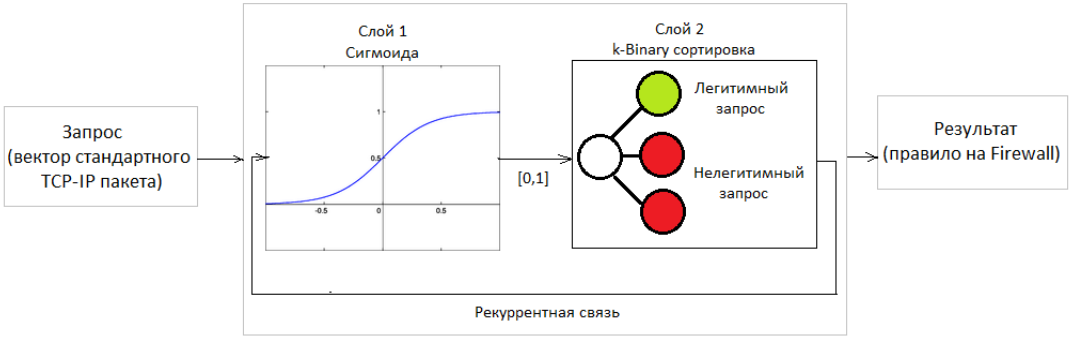

Рисунок 1 – Схема нейронной сети

Для преодоления данной проблемы была выбрана стратегия построения нескольких сетей с дальнейшей выборкой той, которая для данного значения давала бы минимальную ошибку в процессе.

Определим метод фильтрации входящего трафика на основе двухслойной нейронной рекуррентной сети. Стандартный *TCP-IP* пакет поступает на узел КС, отвечающий за фильтрацию трафика. Из данного пакета формируется запрос (вектор пакета), который передается в первый слой нейронной сети. После применения функции активации первого слоя, запрос получает значение в диапазоне [0,1]. Чем ближе значение к 0 тем он «легитимнее». Далее, полученное значение попадает во второй слой сети, где пройдя *k-Binary* классификацию, он будет определен в соответствующее множество легитимных или нелегитимных запросов. В случае, если запрос нелегитимен, на него создается правило в файерволе (*Firewall*) фильтрующего узла.

Результаты работы

Выше описанный метод был применен на практике в хостинговой компании. Возможность практического применения появилась в ходе атаки (*DDoS*) одного из узлов КС.

Для построения обучающей и тестовой базы выбранного метода фильтрации трафика на основе двухслойной рекуррентной

нейронной сети, было определено следующее соотношение - 60/25/15, где 65% записей использовалось для обучения системы, 25% - тестирование, а 15% - для подбора наиболее оптимального состояния системы.

Данное соотношение было получено эмпирически и не претендует на универсальность. Для каждого случая реализации соотношение может быть свое.

На рисунке 2 представлена динамика развития угрозы, когда количество запросов начало превышать физические возможности узла (сервера).

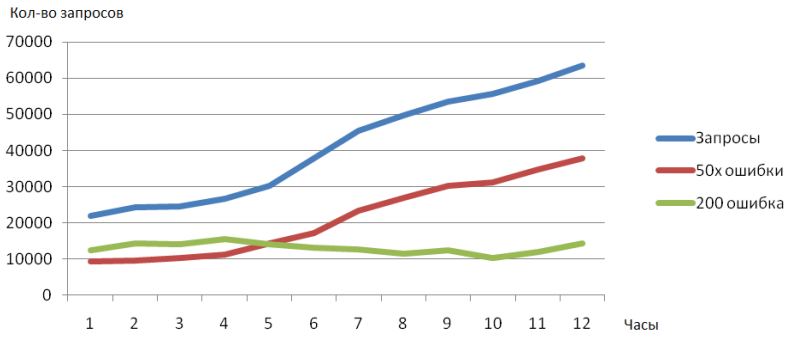

Рисунок 2 - График роста количества запросов за 12 часов работы сервер (классическая DDos атака)

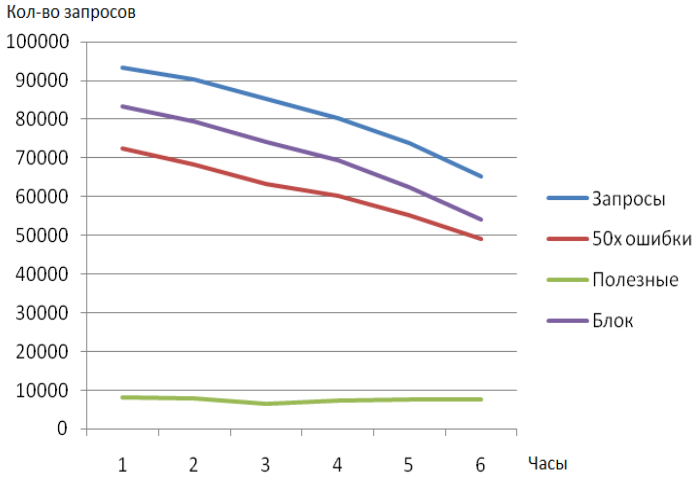

Рисунок 3 - Применение механизма фильтрации на базе нейронной сети за час работы после внедрения

После внедрения метода фильтрации на основе двухслойной рекуррентной нейронной

сети, скорость создания ограничений на файерволе узла резко выросла. Это позволило снизить количество нелегитимных запросов к данному узлу (рисунок 3).

200-ый тип ошибок - полезные запросы на рисунка 3 не сильно отличаются от аналогичного параметра на рисунке 2. Именно этот параметр позволяет показать физические данные сервера по количеству одновременно обрабатываемых запросов. Таким образом, внедренный метод фильтрации позволил повысить защищенность КС.

Выводы

Предложен и разработан метод фильтрации входящего трафика на основе двухслойной рекуррентной нейронной сети. Данный метод практически апробирован в составе системы защиты КС хостинговой компании. Практическая применимость нейронных сетей в процессе фильтрации трафика была доказана при использовании построенной модели против угроз отказа в обслуживании. Количество нелегитимного трафика после внедрения механизма уменьшалось пропорционально времени работы системы.

СПИСОК ЛИТЕРАТУРЫ

1. Комарцова Л.Г. "Нейрокомпьютеры" [Текст] / Л.Г. Комарцова – М.: МГТУ им. Н. Э. Баумана, 2004 г. – 195 с.
2. Савельев А.В. Нейрокомпьютеры в изобретениях [Текст] / А.В. Савельев // Нейрокомпьютеры: разработка, применение. – М.: Радиотехника, 2004 г. № 2-3. С. 33-49.
3. Сигеру О., Марзуки Х., Рубия Ю. Нейроуправление и его приложения [Текст] / О. Сигеру, Х. Марзуки, Ю. Рубия — М.: ИПРЖР, 2005.С. 272.

4. Хайкин С. Нейронные сети: полный курс [Текст] / С. Хайкин – М.: Вильямс, 2006 г. — 1104 с.
5. Ясницкий Л.Н., Введение в искусственный интеллект [Текст] / Л.Н. Ясницкий – М.: Издательский центр Академия, 2005 г. – 176 с.

*Аспирант **Бурлаков М.Е.**. тел. 8-929-703-33-38, vlast@ssu.samara.ru - кафедра Безопасности информационных систем Самарского государственного университета*

УДК 544.46; 620.179.14.05:1.082.5.05

НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО МОДЕЛИРОВАНИЮ СОВМЕСТНОЙ ДЕЯТЕЛЬНОСТИ ПЕДАГОГА И ОБУЧАЕМОГО, ОПОСРЕДОВАННОЙ ПРИМЕНЕНИЕМ ИКТ, СРЕДСТВАМИ МПЦУ

А.И. Горячих

В статье рассматриваются аспекты моделирования совместной деятельности педагога и студента, опосредованной применением ИКТ средствами мотивационного программно-целевого управления (МПЦУ). В результате была сконструирована структурно-функциональная модель совместной деятельности педагога и обучаемого, позволяющая проектировать учебную деятельность на концептуальном, технологическом и практическом уровнях. Также в статье приведены научно-методические рекомендации по моделированию совместной деятельности педагога и обучаемого, опосредованной применением ИКТ средствами МПЦУ.

Ключевые слова: средства ИКТ, мотивационное программно-целевое управление, учебная деятельность.

Введение

Моделирование совместной деятельности педагога и обучаемого, опосредованной применением ИКТ, представляет собой сложную динамическую систему со многими тесно связанными элементами и не может эффективно функционировать без современных технологий управления. Управление обучением в такой системе должно реализовывать четыре его функции: мотивационную, познавательную, контрольно-корректировочную, адаптивную, что обеспечит перевод этой системы в новое, более качественное, состояние.

Технические возможности любых ИКТ сами по себе не могут оказывать воздействие на совместную деятельность педагога и обучаемого, так как субъекты педагогического процесса зачастую не подготовлены к их использованию в своей деятельности, или используют недостаточно эффективно. Эффективность ИКТ зависит от степени их гибкости, то есть способности соответствовать потребностям и характеристикам различных групп студентов, а также различным образовательным контекстам.

Комплексная реализация необходимых для эффективного обучения функций управления возможна в интеграции идей совершенствования образовательного процесса с использованием компьютерных технологий с технологией управления. В качестве такой технологии было использовано мотивационное программно-целевое управление (МПЦУ), разработанное И.К.Шалаевым [1].

В результате проведенной нами работы по моделированию совместной деятельности педагога и студента , средствами МПЦУ были созданы:

- модель объекта управления;
- модель субъекта управления;
- модель совместной деятельности педагога и обучаемого, опосредованной применением компьютерных обучающих программ (средств ИКТ) [2].

Структурно-функциональные модели объекта и субъекта управления были построены в виде дерева целей. Поскольку именно цели выступают в качестве важнейшего звена в моделировании проблем оптимального управления обучением и определяют то содержание, которое должно быть достигнуто как конечный результат процесса управления. Система этих целей составляет сложную иерархию от формирования мотивов обучения до четкого определения качества знаний и навыков, которыми должен обладать студент в результате обучения.

Рассмотрим исполняющую программу для управляющей и управляемой подсистем.