4. *Tzermias Z. et al.* Combining static and dynamic analysis for the detection of malicious documents, Proceedings of the Fourth European Workshop on System Security. ACM, 2011, pp. 4.
5. MITRE Corporation, Common Weakness Enumeration, 2014. Available at: http://cwe.mitre.org/.
6. SecurityLab, Microsoft ne budet ispravlyat' uyazvimost' v Internet Explorer 8 semimesyachnoy davnosti, 2014 [SecurityLab, Microsoft will not fix the vulnerability in Internet Explorer 8 seven-month-old]. Available at: http://www.securitylab.ru/news/453198.php.
7. MITRE Corporation, Common Weakness Enumeration. Available at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2389.
8. Microsoft, KB-917150, 2014. Available at: http://support.microsoft.com/kb/917150/ru, свободный.
9. MITRE Corporation, Common Weakness Enumeration. Available at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3431.
10. *Arora A. et al.* An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure, *Information Systems Research,* 2010, Vol. 21, No. 1, pp. 115-132.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Катаргин Дмитрий Андреевич – Южный федеральный университет; e-mail: dakatargin@sfedu.ru; 346880, Ростовская обл., г. Батайск, Северный Массив, 15, кв. 51; тел.: +79286211661; аспирант.

Katargin Dmitry Andreevich – Southern Federal University; e-mail: dakatargin@sfedu.ru; 15, Severniy Massiv, kv. 51 Bataysk, Rostovskaya obl, 346880; phone: +79286211661; postgraduate student.

УДК 004.056

Я.В. Тарасов

МЕТОД ОБНАРУЖЕНИЯ НИЗКОИНТЕНСИВНЫХ DDOS-АТАК НА ОСНОВЕ ГИБРИДНОЙ НЕЙРОННОЙ СЕТИ

Представлены результаты разработки метода обнаружения сетевых атак типа «отказ в обслуживании» на различные сервисы хранения, обработки и передачи данных в сети Интернет. Основное внимание уделено обнаружению низкоинтенсивных атак типа «отказ в обслуживании». Опровергается мнение, что специальные средства для обнаружения атак «отказ в обслуживании» (denial of service, DoS) не требуются, поскольку факт DoS-атаки невозможно не заметить. Показано, что для эффективного противодействия необходимо знать тип, характер и другие показатели атаки «отказ в обслуживании», а системы обнаружения распределённых атак позволяют оперативно получить эти сведения. Кроме того, использование такого рода систем обнаружения атак позволяет существенно уменьшить время определения факта проведения атаки – с 2–3 суток до нескольких десятков минут, что снижает затраты на трафик и время простоя атакуемого ресурса. В качестве модуля обнаружения используется гибридная нейронная сеть на основе сети Кохонена и многослойного персептрона. Описана работа созданного прототипа системы обнаружения атак, методика формирования обучающей выборки, ход экспериментов и топология экспериментального стенда. Представлены результаты экспериментального исследования прототипа, в ходе которых ошибки первого и второго рода составили соответственно 3,16 и 1,23 %.

Обнаружение атак; низкоинтенсивные DDoS-атаки; гибридная нейронная сеть; безопасность вычислительных сетей.

Y.V. Tarasov

MODELING AND STUDY OF LOW-INTENSITY DDOS-ATTACKS ON BGP-INFRASTRUCTURE

The article presents the development of the method of detection of network attacks such as "denial of service" for various services of storage, processing and transmission of data over the Internet. Emphasis is placed on the detection of low-rate DoS-attacks. Refuted the view that the special tools for intrusion detection, "denial of service" are not required, since the fact of DoS-attacks can not be ignored. It is shown that for an effective response is necessary to know the type, nature, and other indicators of the attack, "denial of service", and the detection system of distributed attacks allow to quickly get the information. Furthermore, the use of such intrusion detection systems can significantly reduce the time of determining the attack – 2–3 days to a few tens of minutes, which reduces costs and downtime traffic attacked resource. As a detection module a hybrid neural network based on Kohonen network and multilayer perceptron is used. The operation of the intrusion detection system prototype, the method of formation of the training sample, all experiments and the topology of the experimental stand are presented. Experimental results of a prototype, in which the type I and type II errors were respectively 1 and 1.5 %, also presented.

Attack detection; low-rate DDoS-attacks; hybrid neural network; security of computer networks.

Введение. Одной из основных тенденций последних лет в сфере компьютерных преступлений является рост количества и сложности атак на доступность информации (ресурсов автоматизированной системы), как один из трех основных критериев, наряду с конфиденциальностью и целостностью информационной безопасности объекта. Данные атаки образуют класс атак типа «отказ в обслуживании» (DDoS-атаки). Если атака выполняется одновременно с большого числа компьютеров, имеет место DDoS-атака (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»).

В целом, DoS-атаки нацелены как на сети в целом и серверные кластеры, так и на конечные хосты, их задачей является максимальное потребление предоставляемых ресурсов с целью значительного ухудшения или прекращения предоставления сервиса нормальным пользователям. Обычно атакуемыми ресурсами являются: ширина канала, процессорное время серверов и роутеров и конкретные реализации протоколов. В качестве примеров можно привести SYN-атаку, нацеленную на переполнение стека TCP операционной системы; направленные широковещательные ICMP – атакуемому отправляются подобные пакеты, ответы от него снижают пропускную способность сети; DNS–флуд-атаки, использующие определенную слабость протокола DNS и направленные на существенное увеличение трафика к атакуемому.

В целях минимизации последствий DDoS-атак, их обнаружение и классификация является крайне важной и вместе с тем сложной задачей. Основной способ распознавания DDoS-атаки заключается в обнаружении аномалий в структуре трафика. Традиционные механизмы обеспечения безопасности – межсетевые экраны и системы обнаружения вторжений – не являются эффективными средствами для обнаружения DDoS-атак и защиты от них, особенно атак трафиком большого объема [1]. Фундаментальной предпосылкой для обнаружения атак является построение контрольных характеристик трафика при работе сети в штатных условиях с последующим поиском аномалий в структуре трафика (отклонения от контрольных характеристик) [2]. Аномалия сетевого трафика – это событие или условие в сети, характеризуемое статистическим отклонением от стандартной структуры трафика, полученной на основе ранее собранных профилей и контрольных характеристик. Любое отличие в структуре трафика, превышающее определенное пороговое значение, вызывает срабатывание сигнала тревоги.

Вместе с тем существующие методы обнаружения DDoS-атак, позволяющие эффективно распознавать DDoS-атаки транспортного уровня (SYN-флуд, UDP-флуд и другие), малоэффективны для обнаружения низкоинтенсивных DDoS-атак (Low-Rate DDoS) прикладного уровня («медленный» HTTP GET-флуд и «медленный» HTTP POST-флуд) [3]. Данный класс DDoS-атак возник сравнительно недавно и на сегодняшний день представляет основную угрозу доступности информации в распределенных компьютерных сетях [4]. Отличить трафик, генерируемый в ходе данных атак, от легального HTTP-трафика достаточно сложно, кроме того, каналы передачи данных практически не перегружаются. Данные атаки приводят к потерям запросов и ответов, т.е. фактическому отказу веб-серверов на основе Microsoft IIS, Apache и других систем. Кроме того, атака может быть адаптирована для воздействия на SMTP и даже на DNS-серверы. В варианте DDoS особую опасность представляет участившееся использования техники DNS-amplification для лавинообразного усиления мощности сетевого ботнета. Данные факты обуславливают актуальность разработки новых механизмов обнаружения низкоинтенсивных распределенных атак прикладного уровня типа «отказ в обслуживании» в компьютерных сетях при помощи методов искусственного интеллекта.

1. Анализ механизма Low-Rate DDoS. Общим фактором, необходимым для осуществления Low-Rate DDoS-атак, является наличие большого количества компрометированных или добровольно участвующих хостов и грубое "заваливание" пакетами атакуемый узел. Именно «грубость» в реализации данных атак может свести на нет весь эффект в случае обнаружения больших объемов аномального трафика сетевыми мониторами [1, 5].

Low-Rate DDoS-атаки представляют собой периодический трафик малого объема, т.е. всплески. В момент, когда открытая сессия подключения должна закрыться по тайм-ауту, посылается новый всплеск для поддержания данной сессии в открытом состоянии. Постепенно буфер маршрутизатора или сервера будет переполняться, что приведет к отказу обработки легитимного трафика. При таком подходе не требуется большой пропускной способности и вычислительной мощности у атакующей стороны.

Показательным примером являются DDoS-атаки, направленные на снижение полосы пропускания TCP потоков трафика, осуществляемые с низкой интенсивностью во избежание обнаружения. Используя уязвимость в механизме тайм-аута повторной передачи TCP-стека, можно добиться нулевой пропускной способности, путем смешивания с основным трафиком специально подобранных шаблонов DDoS-трафика.

Управление полосой пропускания в TCP осуществляется на 2-х временных шкалах. На малой временной шкале отметки времени прохождения пакетов по каналу связи до адресата и обратно (RTT), обычно от 10 до 100 миллисекунд, TCP-стек использует аддитивно-мультипликативное (additive-increase multiplicative-decrease) управление (AIMD) для передачи каждого потока трафика на одинаковых скоростях через самое узкое место, так называемое бутылочное горлышко. Когда канал связи начинает «забиваться» и возникает большое количество потерь, TCP-стек начинает работать по 2-й, большей временной шкале с отметками тайм-аутов повторной передачи пакетов (RTO, рекомендованное минимальное значение 1 секунда). Что бы избежать «забития» канала, поток трафика уменьшается до одного пакета, и по прошествии времени RTO пакет пересылается заново. При последующих потерях время RTO удваивается с каждым следующим тайм-аутом. В случае удачного получения пакета, TCP-стек начинает использовать AIMD-управление [6].

Для проведения Low-Rate DDoS-атаки необходимо взять потоки трафика в виде импульсов и рассмотреть периодические импульсные атаки, состоящие из коротких пиков со специально подобранной длительностью, повторяющихся с

определенной, специально выбранной, частотой по медленной временной шкале. Если для первого потока TCP-трафика общий трафик (DDoS-атаки и обычный) в течение пика достаточен, чтобы произошли потери пакетов, то этот поток "отвалится" по тайм-ауту и будет произведена попытка отправить новый пакет по прошествии времени RTO. В случае, если периодичность посылки DDoS-трафика совпадает (даже примерно) с RTO нормального трафика, обычный трафик будет постоянно получать тайм-аут, как следствие, потери будут приближаться к 100 % и пропускная способность приблизится к нулю. Кроме того, если период DDoS-посылок примерно равен, но лежит вне диапазона RTO, то будет наблюдаться существенное (но не полное) снижение полосы пропускания. Более подробно данный механизм рассмотрен в работе [5], а механизм тайм-аута TCP-стека в [6].

На рис. 1 видна зависимость доступности web-сервиса от периодичности атаки. В идеальной модели без погрешностей на задержки в сети и производительность атакующих машин, а также на потери в сети Интернет, можно с уверенностью сказать, что такая атака проводится без серьезных затрат на пропускную способность канала связи атакующих машин.

Рис. 1. График сравнения доступности атакуемой системы и потерь во время атаки

Проведение низкоинтенсивной атаки на web-сервер сильно повлияло на общую пропускную способность. После начала атаки наблюдалось снижение пропускной способности канала связи (рис. 2), что приводило к снижению качества обслуживания клиентов http-сервером. Для сравнения, на рис. 3 отображается график пропускной способности во время покоя.

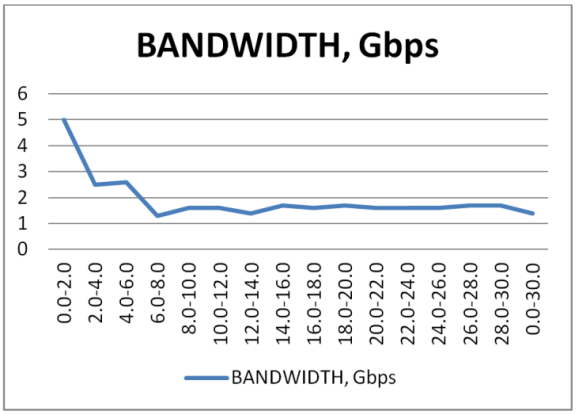

Рис. 2. График пропускной способности канала связи во время атаки

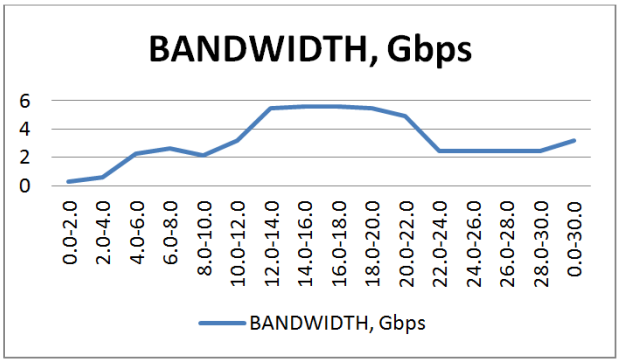

Рис. 3. График пропускной способности канала связи в состоянии покоя

2. Описание системы исследования атак типа «отказ в обслуживании». Кратко опишем программно-аппаратное обеспечение экспериментального стенда. Во время моделирования сетевого взаимодействия использовались технологии виртуализации, для обеспечения чистоты экспериментальных данных. Так как системы виртуализации позволяют создавать изолированные виртуальные машины с набором выделенных ресурсов. Для каждой виртуальной машины выделяется процессорное время и оперативная память, при исчерпании которых не будет происходить вмешательства в ресурсы других виртуальных машин. Также системы виртуализации позволяют изменять пропускную способность виртуальных сетей и регулировать потери при передаче данных в этих сетях, тем самым можно создать модель, максимально близко приближенную к реальным условиям в глобальных сетях.

В качестве аппаратной площадки использовался персональный компьютер на базе процессора Intel Core i7-3770 с тактовой частотой 3.4 ГГц, объемом оперативной памяти в размере 16 Гб и высокоскоростной твердотельный жесткий диск объемом 120 Гб.

На компьютер был установлен «Citrix XenServer 6.1» (является бесплатно распространяемым продуктом компании Citrix) с активированным параметром в BIOS – аппаратная виртуализация.

Для проведения экспериментов использовался стенд в составе:

1. Атакуемый сервер – Debian Wheezy, web-сервер Apache, Php5(libapache2-mod-php5), MySQL-server.
2. Атакующий сервер – Debian Wheezy, Perl, Slowloris ddos script.
3. Сервер сбора данных поведения трафика в сети – Windows 7 Pro x64, WinPcap, прототип системы обнаружения атак.

Моделирование низкоинтенсивной DDoS-атаки. Для исследования различных видов атак типа «отказ в обслуживании» была создана среда, в которой для передачи, хранения и обработки информации используются сетевые протоколы различных уровней модели OSI.

В рамках исследования была смоделирована атака slowloris. Атака базируется на уязвимости в протоколе HTTP. Slow HTTP POST атака работает следующим образом: злоумышленник отправляет POST заголовок с легитимным полем «Content-Length», которое позволяет web-серверу понять, какой объём данных к нему поступает. Как только заголовок отправлен, тело POST-сообщения начинает передаваться с очень медленной скоростью, что позволяет использовать ресурсы сервера намного дольше, чем это необходимо, и, как следствие, помешать обработке других запросов. Несколько тысяч таких соединений могут вывести web-сервер из строя на несколько минут.

Для рекрутинга ботов использовались онлайн-игры – компьютеры незадачливых игроков использовались для отправки специально сформированных HTTP-запросов целевой системе.

Простота реализации атаки позволяет эффективно использовать для этого простой Java-аплет, который запускается во время онлайн-игры. Как только жертва принимает self-signed-аплет, он начинает выполнять атаку в то время, пока пользователь играет в игру. После выхода из игры и закрытия браузера атака прекращается, а аплет удаляется. Обнаружить, что компьютер стал источником атаки, довольно проблематично, поскольку компьютер не заражается в классическом понимании этого слова, а отличить атакующий трафик от легального HTTP-трафика сложно. Кроме того, интернет-канал почти не перегружается.

Атака приводит к обрушению web-серверов с Microsoft IIS и Apache (однако список уязвимых web-серверов ими не ограничивается) в рамках протоколов HTTP или HTTPS и любых «безопасных» подключений вроде SSL, VPN и других. Также атака может быть адаптирована для работы с SMTP и даже DNS-серверами. Программное обеспечение, балансирующее нагрузку, ныне используемое для предотвращения DDOS-атак, схожих по типу, неэффективно против новой методики.

3. Обнаружение атак с использованием гибридной нейронной сети. Опишем метод и архитектуру прототипа СОА. Существует мнение, что специальные средства для обнаружения DDoS-атак не требуются, поскольку факт DDoS-атаки невозможно не заметить. Во многих случаях это действительно так. Однако достаточно часто отмечались успешные атаки, которые были замечены жертвами лишь через 2–3 суток. Бывало, что негативные последствия атаки (типа флуд) заключались в излишних расходах по оплате трафика, что выяснялось лишь при получении счёта.

Большинство современных систем обнаружения атак (СОА) осуществляют обнаружение атак путём контроля профилей поведения либо поиска специфических строковых сигнатур. Используя эти методы, практически невозможно создать полную базу данных, содержащую сигнатуры большинства атак. Существует три главные причины этого:

1. Новые сигнатуры необходимо создавать вручную. Сигнатуры известных атак, которые уже включены в БД, не могут гарантировать надёжной защиты без постоянных обновлений.
2. Теоретически существует бесконечное число методов и вариантов атак, и для их обнаружения понадобится БД бесконечного размера. Таким образом, имеется возможность того, что некая атака, не включённая в базу данных, может быть успешно осуществлена.
3. Современные методы обнаружения вызывают большое число ложных тревог. Таким образом, могут быть скомпрометированы легальные сетевые события.

В работах [8, 9] показана возможность использования многослойного персептрона в качестве решающего блока в СОА, анализирующей последовательно приходящие сетевые пакеты. Предлагаемый в статье подход предполагает использование нейросети для выявления злоупотреблений, распределённых во времени и основанных на совместном создании искусственного (аномального) потока данных несколькими источниками.

Распределенными по времени называются атаки, проводимые в течение одного продолжительного периода времени. При совместном нападении существует несколько злоумышленников, работающих параллельно с разных источников, распределённых в пространстве. Каждый из них по отдельности может предпринимать действия, которые могут показаться безвредными. Атаки становятся очевидными только тогда, когда все события рассматриваются вместе.

Основное преимущество СОА, использующих нейронные сети, в том, что нейросеть не ограничена знаниями, которые заложил в неё программист. Они имеют возможность учиться на предшествующих событиях – как на аномальном, так и на нормальном трафике. За счёт этого достигается высокая эффективность и адаптивность СОА.

Существуют различные варианты применения нейросетевых систем обнаружения атак (НСОА) – анализ всего сетевого трафика в защищаемом сегменте сети, анализ команд, вводимых пользователем, анализ переходов состояний и др. В настоящей статье предлагается метод обнаружения и архитектура СОА, основанная на использовании гибридной нейронной сети в качестве анализатора трафика.

Пример сильно распределённой по времени и адресам атаки приведён ранее в п. 2.2. Другим, более простым примером распределённой по времени атаки может служить взлом пароля методом перебора [11].

Потоки данных были разделены на наборы из 150 пакетов, причём кроме данных из заголовков пакетов сетевого и транспортного уровней, как предлагается в работе [10], учитывались также и первые 50 символов полезной нагрузки прикладного уровня (в ASCII-коде). Кроме того, проводится нормализация представления значений порт назначения для уточнения используемого прикладного протокола (telnet, ftp и т.д.). Схожий метод анализа исходных данных был описан в [11].

Как правило, ни одно событие, составляющее трафик DDoS-атаки, по отдельности не выглядит подозрительно. Кроме того, даже два или три события не являются чем-то необычным. Тем не менее, взятые вместе, в определенной последовательности, повторяемые в определённое время, эти события являются указанием на то, что осуществляется атака. Дальнейшее осложнение обнаружения состоит в том, что эти события, хотя и в определенной последовательности, могут поступать из различных источников и чередоваться с другими, нормальными событиями.

Для обработки аномального трафика предлагается применять гибридную нейронную сеть, состоящую из самоорганизующейся сети Коханена (self-organizing map, SOM) и многослойного персептрона. Архитектура прототипа предлагаемой системы обнаружения атак представлена на рис. 4.

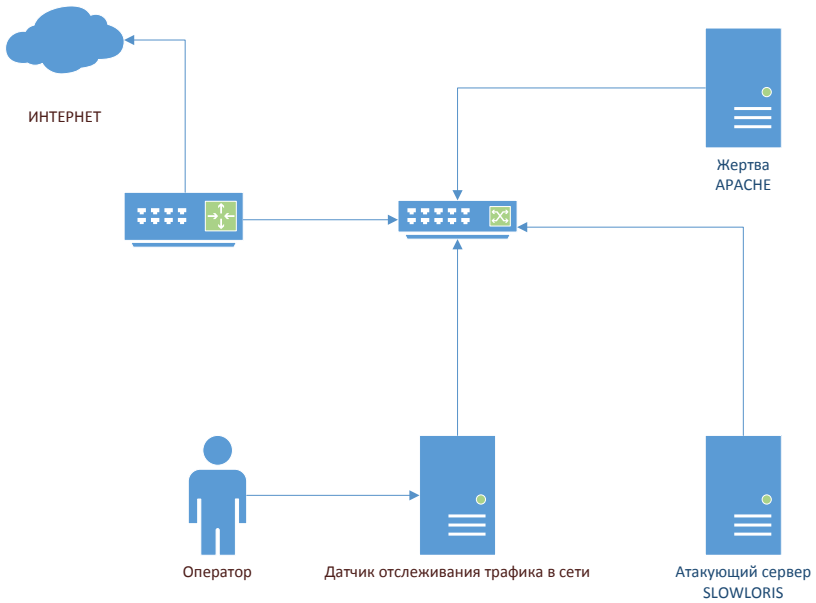

Рис. 4. Общая схема экспериментального стенда

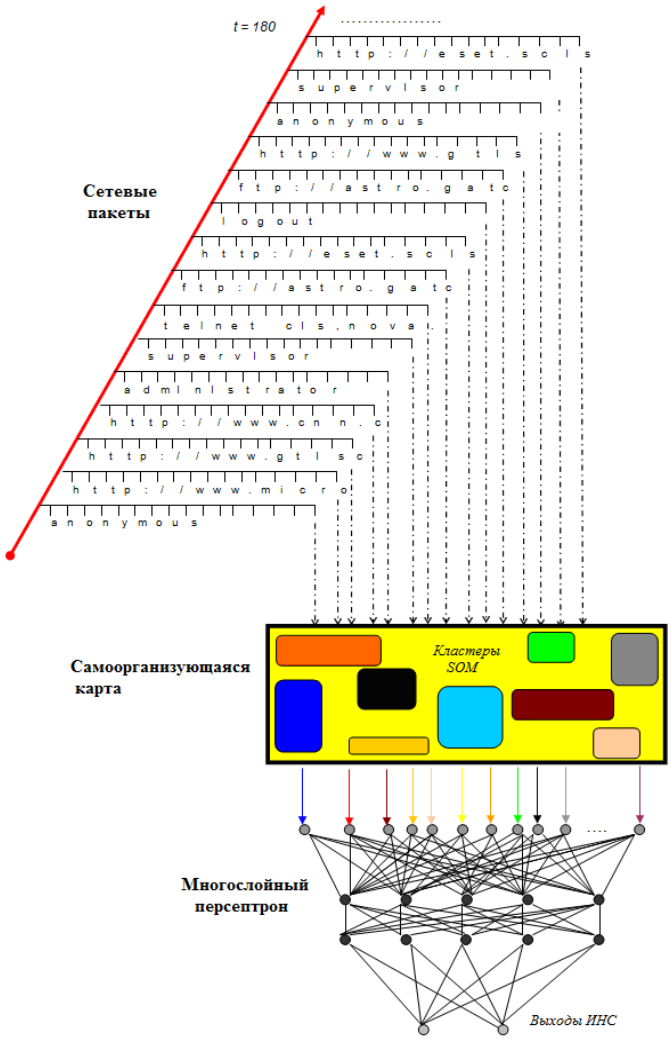

Рис. 4. Архитектура предлагаемой системы обнаружения атак

При помощи применения карты Коханена происходит кластеризация 50-символьных событий в узлы матрицы, в которых будут сгруппированы события аналогичных числовых символов. Фактически, отдельные узлы будут представлять собой определённые сценарии атак.

Входной вектор для SOM содержит следующие компоненты:

- 1–4 – байты, составляющие адрес пакета (для протокола IPv4), приведённые в диапазон 0-1;
- 5 – порт пакета, приведённый в диапазоне 0–1;
- 6–55 – первые 50 байтов данных пакета, приведённые в диапазоне 0–1.

После этого данные заголовков пакетов и информация о группировке подаются на вход многослойного персептрона, обученного распознавать аномальный трафик, но уже с учётом информации о событии, т.е. принадлежности пакета той или иной группе-сценарию. Это позволяет не только обнаруживать аномалии в единичных пакетах, но и выявлять принадлежность пакета к распределённой по времени атаке.

Формат входного вектора для FF-сети (персептрона) следующий. Входная выборка разбивается на непересекающиеся части длиной 150 пакетов. Все пакеты проходят через сеть Кохонена. Пакету ставится в соответствие номер кластера (номер нейрона-победителя).

Кластеры укрупняются – 5 соседних объединяются воедино. Получается 100 укрупнённых кластеров.

По укрупнённым кластерам считается гистограмма для представления трафика. То есть, первый компонент вектора – это число пакетов, попавших в первый укрупнённый кластер (кластеры 1–5), и так далее. Гистограмма нормируется, компоненты приводятся к диапазону 0–1. После этого вычисляется дельта между соседними векторами.

В предлагаемом методе учитывается два типа активности трафика. При анализе отдельных узлов кластера выявляются отдельные сценарии атак. Кроме того, анализируются резкие перепады мощности сетевого потока для выявления всплесков нагрузки. Совместный анализ этих двух типов событий позволяет более точно реагировать на появление DDoS-трафика, при этом снижая число ложных срабатываний, связанных с легальным возрастанием использования полосы пропускания.

Для обучения искусственной нейронной сети моделировались два типа сетевого трафика – нормальный и аномальный. Первый содержал пакеты, появляющиеся в сети при обычной работе, а второй имитировал распределённую атаку.

Сбор данных проводилось в 2 этапа.

1. Этап сбора нормального поведения. На атакуемом сервере создан php-скрипт, который выполняет «тяжелый» sql-запрос (Цикл в N итераций). С атакующего сервера запускался Apache BanchMark для создания легитимных подключений к серверу. 10 потоков по 100 запросов.
2. Этап сбора аномального поведения. Для имитации трафика, возникающего во время атаки, на атакующем сервере запускается 3 копии скрипта slowloris с разницей в параметре, отвечающем за задержку между повторными подключениями. Пример запуска:

./slowloris.pl -dns google.com -port 80 -timeout 500 -num 100500.

Обучение и тестирование ИНС проводилось на непересекающихся окнах, поскольку при использовании скользящих окон при тестировании ухудшается возможность контроля за степенью использования полосы пропускания сетевого канала.

Анализ результатов экспериментов. В результате тестирования прототипа были получены следующие результаты:

- величина ошибки первого рода (ложное срабатывание) составила 3,16 %;
- величина ошибки второго рода (пропуск атаки) составила 1,23 %.

Графически результаты распознавания нормального трафика представлены на рис. 5, результаты распознавания атакующего трафика – на рис. 6.

Выводы. Анализ механизма реализации Low-rate DDoS-атак на примере атаки slowrolis показал, что этот тип атак может быть организован с минимальным соотношением необходимой мощности/канала атакующего компьютера (компьютеров) и атакуемого сервера, недостижимым раньше. Также анализ статистики уязвимостей свидетельствует о том, что большое количество сайтов подвержены этой атаке, однако со стороны сервера зачастую сложно даже диагностировать, что сайт атакуют, поскольку трафик не превышает нормальных значений.

Предлагаемый метод обнаружения низкоинтенсивных атак позволяет эффективно выявлять принадлежность трафика к распределённой по времени атаке.

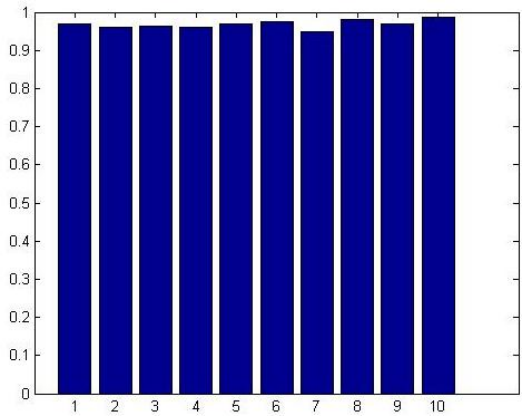

Рис. 5. Визуализация результатов распознавания нормального трафика

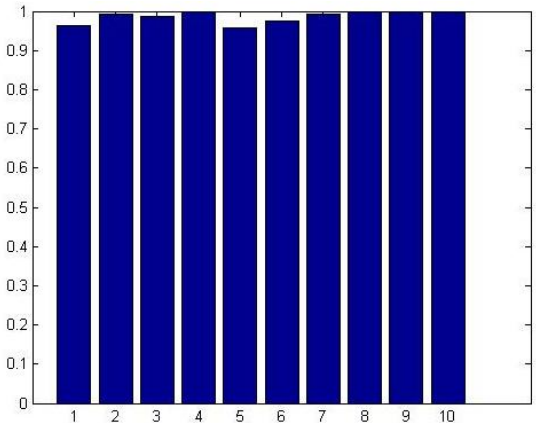

Рис. 6. Визуализация результатов распознавания атакующего трафика

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Решение Cisco Systems «Clean Pipes» по защите от распределенных DDOS-атак для операторов связи и их клиентов. [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/RU/downloads/CleanPipes_rus.pdf, свободный (дата обращения: 01.09.2014).
2. *Лобанов В.Е., Оныкий Б.Н., Станкевичус А.А.* Архитектура системы защиты Грид от атак типа «отказ в обслуживании» и «распределенный отказ в обслуживании» // Безопасность информационных технологий. – 2010. – № 3. – С. 136-139.
3. Отчет «Лаборатории Касперского» о DDoS-атаках за первое полугодие 2013 года. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/444464.php (дата обращения: 01.09.2014).
4. *Chee W.O. Brennan T.* OWASP AppSec DC 2010. HTTP POST DDoS. [Электронный ресурс]. – Режим доступа: https://www.owasp.org/images/4/43/ Layer_7_DDOS.pdf (дата обращения: 01.08.2014).
5. *Aleksandar Kuzmanovic, Edward W. Knightly*: Low-rate TCP-targeted denial of service attacks and counter strategies // IEEE/ACM Trans. Netw. – 2006. – № 14 (4). – P. 683-696.
6. *Paxson V., Allman M., Chu H.K. and M. Sargent.* Computing TCP's Retransmission Timer, RFC 6298, Proposed Standard, June 2011.
7. Сайт «RFC 2.0 – Русские Переводы RFC». [Электронный ресурс]. Режим доступа: http://rfc2.ru/4272.rfc – свободный (дата обращения 22.08.2014).
8. *Абрамов Е.С., Аникеев М.В., Макаревич О.Б.* Использование аппарата нейросетей при обнаружении сетевых атак // Известия ТРТУ. – 2004. – № 1 (36). – С. 130.

9. *Абрамов Е.С., Аникеев М.В., Макаревич О.Б.* Подготовка данных для использования в обучении и тестировании нейросетей при обнаружении сетевых атак // Известия ТРТУ. – 2003. – № 4 (33). – С. 204-206.
10. *James Cannady.* The Application of Artificial Neural Networks to Misuse Detection. 2001.
11. *Абрамов Е.С., Сидоров И.Д.* Метод обнаружения распределенных информационных воздействий на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 154-164.

REFERENCES

1. Reshenie Cisco Systems «Clean Pipes» po zashchite ot raspredelennykh DDOS-atak dlya opera-torov svyazi i ikh klientov [Cisco Systems "Clean Pipes" for protection against distributed DDOS attacks for Opera-tors of communication and their clients]. Available at: http://www.cisco.com/ web/RU/downloads/CleanPipes_rus.pdf. (Accessed 01 September 2014).
2. *Lobanov V.E., Onykiy B.N., Stankevichus A.A.* Arkhitektura sistemy zashchity Grid ot atak tipa «otkaz v obsluzhivanii» i «raspredelennyy otkaz v obsluzhivanii» [The system architecture protect the Grid from attacks such as denial of service and distributed denial of service"], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2010, No. 3, pp. 136-139.
3. Otchet «Laboratorii Kasperskogo» o DDoS-atakakh za pervoe polugode 2013 goda [The report "Kaspersky Lab" about DDoS attacks for the first six months of 2013]. Available at: http://www.securitylab.ru/news/444464.php. (Accessed 01 September 2014).
4. *Chee W.O. Brennan T.* OWASP AppSec DC 2010. HTTP POST DDoS. Available at: https://www.owasp.org/images/4/43/ Layer_7_DDOS.pdf (Accessed 01 August 2014).
5. *Aleksandar Kuzmanovic, Edward W. Knightly*: Low-rate TCP-targeted denial of service attacks and counter strategies, *IEEE/ACM Trans. Netw*, 2006, No. 14 (4), pp. 683-696.
6. *Paxson V., Allman M., Chu H.K. and M. Sargent.* Computing TCP's Retransmission Timer, RFC 6298, Proposed Standard, June 2011.
7. Sayt «RFC 2.0 – Russkie Perevody RFC» [The website "RFC 2.0 - Russian Translations RFC"]. Available at: http://rfc2.ru/4272.rfc - svobodnyy (Accessed 01 September 2014).
8. *Abramov E.S., Anikeev M.V., Makarevich O.B.* Ispol'zovanie apparata neyrosetey pri obnaruzhenii setevykh atak [The use of the apparatus of neural networks in the detection of network attacks], *Izvestiya TRTU* [Izvestiya TSURE], 2004, No. 1 (36), pp. 130.
9. *Abramov E.S., Anikeev M.V., Makarevich O.B.* Podgotovka dannykh dlya ispol'zovaniya v obuchenii i testirovanii neyrosetey pri obnaruzhenii setevykh atak [Preparing data for use in training and testing of neural networks in the detection of network attacks], *Izvestiya TRTU* [Izvestiya TSURE], 2003, No. 4 (33), pp. 204-206.
10. *James Cannady.* The Application of Artificial Neural Networks to Misuse Detection. 2001.
11. *Abramov E.S., Sidorov I.D.* Metod obnaruzheniya raspredelennykh informatsionnykh vozdeystviy na osnove gibridnoy neyronnoy seti [iscovery of distributed information impacts based on hybrid neural network*], Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11 (100), pp. 154-164.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Тарасов Ярослав Викторович – ЗАО «Инфосистемы Джет»; e-mail: info@jet.msk.su; 125252, г. Москва, ул. 2-я Песчаная, 2/1, корп. 50; тел.: 84954117601, факс: 84954117602; директор по развитию бизнеса компании «Инфосистемы Джет».

Tarasov Yaroslav Viktorovich – Jet Infosystems; e-mail: info@jet.msk.su; 2/1, 2nd Peschanaya street, build. 50, Moscow, 125252, Russia; phone: +74954117601, fax: +74954117602; director of Business Development in Jet Infosystems.