УДК 004.032.26

ВЫЯВЛЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА НА ПРИМЕРЕ НЕЙРОННЫХ СЕТЕЙ

Голованов Алексей Александрович[1], Мельникова Ольга Игоревна[2], Деменко Кирилл Андреевич[3]

[1]Инженер отдела Информационных технологий;
ООО «Телеком МПК»;
141981, Московская обл., г. Дубна, ул. Болшеволжская,1;
e-mail: golovanov@tmpk.net.

[2]Кандидат технических наук, доцент;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: oimelnik@mail.ru.

[3]Студент;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: kyrilloausdubna@gmail.com.

В представленной статье описываются актуальные сетевые атаки, а также различные способы обнаружения аномальной активности в сетевом трафике. Применение нейронных сетей для анализа сетевого трафика позволит моментально обнаруживать известные системе сетевые атаки и приспосабливаться к новым ранее неизвестным аномалиям сетевого трафика.

Ключевые слова: аномалии сетевого трафика, нейронная сеть, DDoS-атака, системы обнаружения аномалий.

DETECTION OF NETWORK TRAFFIC ANOMALIES ON THE EXAMPLE OF NEURAL NETWORKS

Golovanov Aleksey[1], Mel'nikova Olga[2], Demenko Kirill[3]

[1]Engineer of Information technology;
OOO «Telecom MPK»;
141981, Dubna, Moscow reg., Bolshevolzhskay str., 1;
e-mail: golovanov@tmpk.net.

[2]Candidate of Science in Engineering, associate professor;
Dubna State University,
Institute of the system analysis and management;
141980, Moscow region, Dubna, Universitetskaya str.,19;
e-mail: oimelnik@mail.ru.

[3]Student;
Dubna State University,
Institute of the system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: kyrilloausdubna@gmail.com.

The article contains current network attacks and different ways of detecting abnormal activity in a network traffic. The use of neural networks for the analyzing of neutral traffic will instantly let the network attacks to be discovered and to be adapted to a new previously unknown network traffic anomaly.

Keywords: network traffic anomalies, neural network, DDoS-attack, anomaly detection systems.

Введение

Современный мир страдает из-за огромного числа уязвимостей и угроз, существующих в информационных системах, что обуславливает актуальность задачи поиска и внедрения новых методов обеспечения безопасности систем и информации в существующих вычислительных сетях. Для выявления атак и различных незаконных действий в компьютерных сетях используют *IDS* (*Intrusion Detection System*). *IDS* представляет собой специальный инструмент, который позволяет захватывать сетевой трафик и представлять его в виде потока данных, и применяя к нему определенные правила выявлять аномалии в потоке.

В настоящее время систем обнаружения аномалий как самостоятельных продуктов практически не существует, но распространены системы обнаружения вторжений, основанные на анализе сигнатур [1]. Однако сигнатурный метод обладает следующими недостатками:

1. невозможность обнаруживать новые, не встречавшиеся ранее несанкционированные воздействия;

2. неустойчивость к модификациям уже известных атак;

3. неспособность определять распределенные во времени атаки и аномалии.

Для построения систем обнаружения аномалий можно использовать различные технологии, но наиболее перспективным направлением является искусственные нейронные сети

В представленной работе проводится анализ наиболее актуальных сетевых атак, а также представлена возможность обнаружения аномалий с помощью нейронной сети, в качестве которой использовался многослойный персептрон.

Системы обнаружения аномалий сетевого трафика

Все атаки делятся на две группы: узловые атаки и сетевые атаки, в первом случае атаки на основе узлов направлены на получения доступа к некоторым функциям или данным вычислительной машины, на которую выполняется атака, например, к учетным записям и паролям, файлам, доступу к процессам. Сетевые атаки направлены на некоторый отказ в обслуживании и функционировании атакуемого устройства, ограничивая нормальный доступ к службам и замедляя сетевое подключение. Методы обнаружения атак на уровне хоста предназначены для мониторинга, детектирования и реагирования на действия злоумышленников на определенном хосте. При этом используются данные системных вызовов и анализ журналов регистрации. Методы обнаружения сетевых атак использует данные сетевого трафика и анализаторы сетевых пакетов, при этом такие системы используют сигнатуры атак и анализ трафика, близкого к реальному времени.

Под системами обнаружения аномалий понимаются системы, которые используют модели предполагаемого поведения исследуемой системы и регистрируют любые отклонения от нормального состояния [2]. Для работы систем обнаружения аномалий необходимо создать базу знаний, в которой будет накапливаться информация и строиться концепция нормальной активности системы. Под нормальным состоянием системы понимается такое состояние, при котором она выполняет все возложенные на нее задачи. Аномалии бывают разного вида и характера. Применительно к сетям передачи данных они могут быть:

1. Связаны с неисправностью оборудования.

2. Случайные или преднамеренные действия со стороны легитимных пользователей.

3. Ошибка в работе ПО.

4. Преднамеренные действия злоумышленников.

Наиболее опасными и наносящими значительный ущерб являются преднамеренные атаки злоумышленников.

Для сетевых атак самой опасной является *DoS* (отказ в обслуживании) и *DDoS* (распределенный отказ в обслуживании). По данным отчетов компании *Kaspersky Lab* за 2018 год количество *DDoS*-атак по сравнению с 2017 годом уменьшилось на 13%, однако увеличилась продолжительность и мощность

атак [3]. Самая мощная атака насчитывала 1,35 терабита в секунду, она была направлена на сервис *Git Hub*. За 2018 год так же произошло изменение разновидностей *DDoS* атак. Лидирующее положение занимает *SYN*-флуд, а менее популярным остается *ICMP*-флуд. С 1 по 4 квартал увеличилось количество *UDP*-флуд, это обусловлено простотой и разносторонностью атаки (рис. 1).

DDoS-атаки с каждом годом увеличиваются по времени продолжительности, в мощности и сложности и главное задачей провайдеров состоит в быстром реагировании на изменения в трафике и моментальном прекращении атаки.

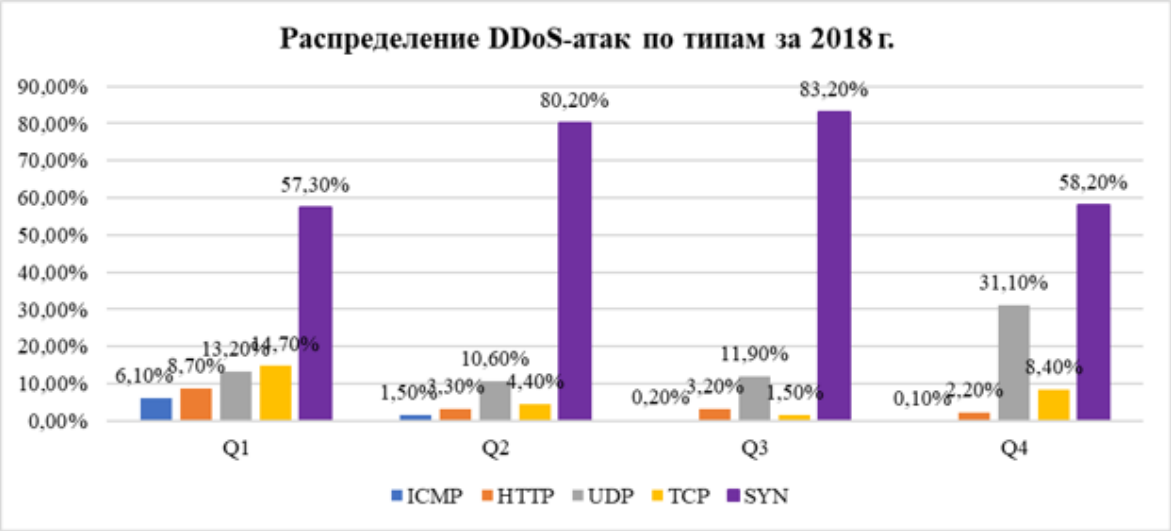

Рис. 1. Динамика изменения DDoS-атак по типам за 2018 г.

С увеличением размера сети, увеличивается и количество поддерживаемого оборудования, в связи с чем сетевое оборудование может подвергаться не менее опасным атакам, как брутфорс, разнообразные *IP-spoofing*, сканирования портов и т.п. Чаще в общем объеме трафика невозможно зафиксировать данные атаки, так как доля трафика для них будет минимальна, но для системного администратора они являются аномальной активностью в сети, в связи с чем стоит задачи в обнаружении данных угроз.

Искусственные нейронные сети в задаче обнаружения аномалий

Методы обнаружения атак можно разделить на основные 2 группы:

1. Сигнатурные.

2. Поведенческие.

Одним из перспективных направлений, относящихся к поведенческому методу, являются интеллектуальные системы. Нейросеть представляет собой математическую модель обработки информации, основанную на имитации работы человеческого мозга. Характерной особенностью данной модели является то, что она состоит из множества взаимосвязанных узлов обработки (нейронов), которые работают одновременно для решения указанной задачи. Нейронная сеть настраивается для конкретной задачи, например, может использоваться для распознавания паттернов, которые сложны для наблюдения или обнаружения человеком, или даже другими компьютерными методами. Для искусственных нейронных сетей, как и для человека, характерен процесс обучения на примерах.

Нейронная сеть в основном состоит из трех категорий слоев, которые включают в себя входной слой, скрытый слой и выходной слой. Любые действия нейронной сети определяются «весом», который накладывается на узлы скрытого слоя. Задача входного слоя представлять исходную информацию, получаемую сетью. Соединения и веса между скрытым слоем и входным слоем определяют действия скрытого слоя. Действия скрытого слоя и веса между выходным слоем определяют производительность и поведение выходного слоя [4].

Для создания собственной модели нейронной сети были проанализированы уже имеющиеся статьи с описанием собственных методов и моделей определения аномалий сетевого трафика на основе нейронный сетей. Наиболее подходящими к нашей задаче являются следующие работы.

В статье [5] описываются три отдельные модели нейронной сети, предназначенные для определения отдельных видов *DDoS*-атак:

– нейронные сети состоят из 3 слоев: входного, внутреннего и выходного, для обучения использовался алгоритм обратного распространения ошибки;

– входные параметры для *TCP-flood*: *IP*-адрес источника, порт источника, порт назначения, номер пакета;

– входные параметры для *ICMP-flood*: *IP*-адрес источника, номер пакета;

– входные параметры для *UDP-flood*: *IP*-адрес источника, порт источника, порт назначения, размер пакета.

Недостатком такой модели является создание и обучение трех отдельных нейронных сетей для обнаружения *TCP, ICMP, UDP-flood*, что снижает общую производительность обнаружения атак.

В работе [6] описана архитектура созданной системы обнаружения *DDoS*-атак, состоящая из 4 модулей:

– Фильтрующий модуль.

– Модуль захвата пакетов.

– Модуль обнаружения *DDoS*-атак.

– Модуль оповещения.

В данной системе используется нелинейная *RBF* нейронная сеть с 2 скрытыми слоями, в качестве выходных данных система имеет возможность сортировать трафик на обычный и аномальный. В ходе эксперимента система показала возможность обнаружения *DDoS*-атаки с точностью около 98,2%.

В работе [7] описана модель нейронной сети с сигмоидной функцией активации, для обучения использовался алгоритм обратного распространения ошибки. Входными параметрами нейронной сети являются: количество входящего/исходящего трафика для протокола, использование портов, размер пакета, количество открытых соединений, среднее значение трафика к хосту.

В ходе обучения нейронная сети показала отличные результаты обнаружения следующих видов атак:

– *UDP-flood* – 91%.

– *TCP-flood* – 85%.

– Сканирование портов – 96%.

– Сканирование портов в режиме ожидания – 78%.

– *ARP-spoofing* – 83%.

Анализ представленных выше работ дает понять, что на текущий момент не существует полноценной системы обнаружения аномалий сетевого трафика, способной захватывать разнообразные сетевые атаки. Несомненным преимуществом можно отметить факт распознавания нейронными сетями *DDoS*-атак, доходящий до 98%. Использование уже ранее проверенных алгоритмов позволит сэкономить время для создания и обучения системы.

Исходя из имеющихся работ, нами была разработана собственная модель нейронной сети, в которой отсутствуют недостатки присущие уже имеющимся системам определения аномалий. Нами был использован многослойный персептрон, так как он лучше всего решает задачу классификации. Многослойный персептрон представляет из себя полносвязную многослойную нейронную сеть, в которой каждый нейрон следующего слоя связан со всеми нейронами предыдущего слоя. Предполагаемый персептрон будет состоять из 4-х слоев и в каждом нейроны имеют определенную нелинейную функцию активации. Входной слой будет состоять из 8 нейронов, скрытый слой будет состоять из 3 нейронов. Для обучения нейросети нами были определены наиболее популярные сетевые атаки: *SYN-flood, UDP-flood, brute force, IP-spoofing, ARP-spoofing*, сканирование портов.

Массив входных данных может быть разбит на 3 группы:

– обучения,

– тестирования,

– подбор оптимального состояния.

Для обучения системы может использоваться алгоритм обратного распространения ошибки (*backpropagation neural network, BPNN*), благодаря которому имеется возможность производить коррекцию весов нейронов сети. Начальные веса нейронных связей определяются как 0 (нормальные параметры в сети) или 1 (аномальные параметры сети).

В качестве параметров могут использоваться: время, протокол, *IP*-адрес источника/назначения, порт источника/назначения, размер, номер пакета. На рис. 2 представлена модель нейронной сети для обнаружения сетевых атак.

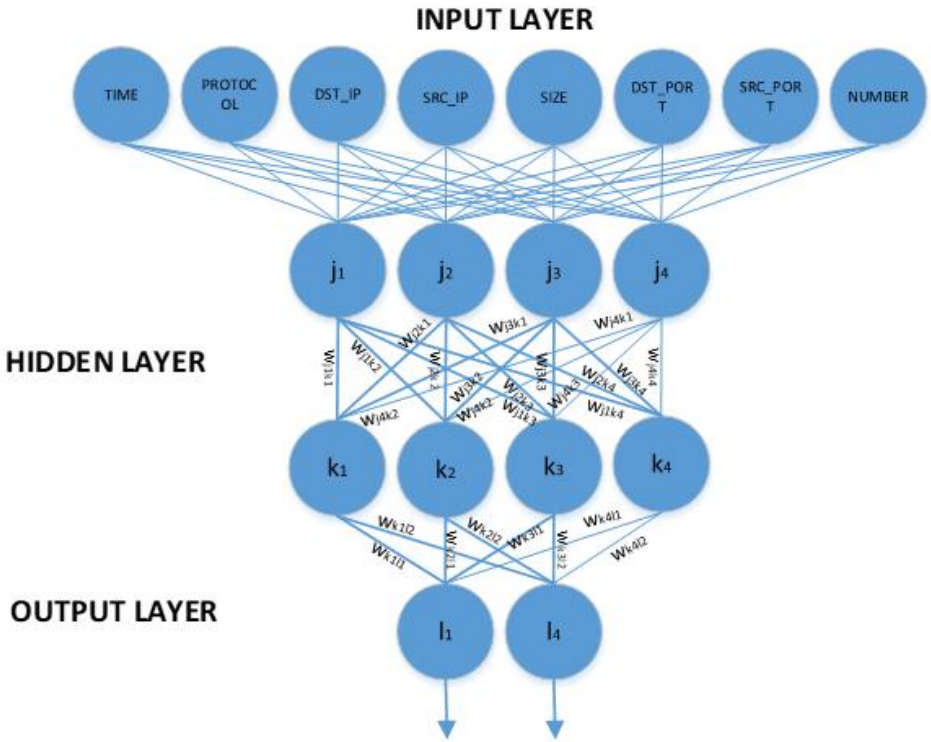

Рис. 2. Структура нейросети для обнаружения сетевых атак

Контролируемое обратное распространение использует вес для калибровки и обучения по шаблонам. Алгоритм изменяет веса между узлами, пока не будет получен желаемый результат (имеющий флаг 1 или 0). Добавляя входные параметры *PROTOCOL* и *TIME*, предполагаемая нейросеть способна обнаружить *brute force* по протоколам: *telnet*, *ssh*, *http*, а также эти параметры помогут обучать нейросеть новым видам атак по всем известным сетевым протоколам.

Заключение

Предполагаемая система сможет самообучаться, и улучшать способность распознавания нормальной и аномальной активности в сетевом трафике, что в свою очередь позволяет уменьшить время реагирования на сетевую атаку и со временем увеличивать объемы пропускаемого трафика через систему. Однако более перспективным направлением в данной области является возможность обучения нейросети не только конкретной сетевой атаке, а множеству существующих атак и возможность ее адаптации к проходящему трафику и анализу неизвестных или видоизмененных сетевых атак. В будущем стоит задача разработать алгоритм, который позволит нейронной сети помимо сетевых атак определять аномалии от ошибок ПО, случайных действий в конфигурации оборудования способных отразить на работе локальной сети. Возможность использовать нейронную сеть для определения и классификации аномалий в сетевом трафик до сих пор является актуальной задачей в сетевой безопасности.

Список литературы

1. Сухов В.К Системы обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов // Вестник РГРТУ. – 2015. – № 54. – С.84-90.
2. Tariq Ahamed Ahanger An Effective Approach of Detecting DDoS Using Artificial Neural Networks // IEEE international Conference on Wireless Communications, Signal Processing and Networking. – 2017.
3. DDoS-атаки в четвертом квартале 2018 года. – [Электронный ресурс]. URL: https://securelist.ru/ddos-attacks-in-q4-2018/93384/ (Дата обращения 25.03.2019).
4. Осовский С.О. Нейронные сети для обработки информации. – М. : Финансы и статистика, 2002. С. 304.
5. Abdullah Aljumah. Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks // International Journal of Advanced Computer Science and Applications. – 2017. – Vol. 8. – No. 8.
6. Reyhaneh Karimazad, Ahmad Faraahi Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks // International Conference on Network and Electronics Engineering IACSIT Press, Singapore. – 2011.
7. Sergey Andropov, Alexei Guirik, Mikhail Budko, Marina Budko. Network Anomaly Detection Using Artificial Neural Networks // PROCEEDING OF THE 20TH CONFERENCE OF FRUCT ASSOCIATION.