Министерство образования Республики Беларусь

Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.021

Бубнов
Яков, Васильевич

АНАЛИЗ ТОПОЛОГИИ ТРАФИКА В КОМПЬЮТЕРНЫХ СЕТЯХ

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-40 80 03 «Вычислительные машины и системы»

_____

Научный руководитель
Иванов Николай Николаевич
кандидат физико-математических наук, доцент

_____

Минск 2017

Нормоконтроль
Сидорович Александра Сергеевна

_____

КРАТКОЕ ВВЕДЕНИЕ

Безопасность функционирования компьютерных систем не возможна без обеспечения надлежащего уровня защищенности сетевой инфраструктуры. Использование межсетевых экранов с целью как предотвращения атак извне, так и блокировки потенциально небезопасных исходящих соединений при подключении компьютерной сети к внешним сетям является распространенной практикой. Одним из многочисленных способов вторжения в частные сети, помимо непосредственного подключения через прослушиваемые атакуемым узлом порты сервисов, может служить создание туннелей через протоколы прикладного уровня.

Одним из протоколов, широко игнорируемых межсетевыми экранами, в основном по причине предполагаемой безопасности, является протокол DNS. Таким образом, представляет интерес исследование более интеллектуальных механизмов обнаружения сетевых туннелей.

Основным направлением исследований в данной области является использование аппарата статистического анализа для классификация трафика протоколов прикладных уровней. Однако, алгоритмы, использующие аппарат математической статистики для разбиения пространства входных образов, чувствительны к выбору порога.

Топологический анализ является альтернативным способом извлечения знаний из данных, в частности, использование аппарата линейной алгебры в рамках теории устойчивых гомологий. Устойчивые гомологии в данном случае позволят судить о разделимости топологии сформированной из входных образов, что позволяет использовать данный инструмент для решения задачи кластеризации образов DNS трафика.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью данной работы является исследование целесообразности и эффективности использования алгоритмов устойчивых гомологий при анализе компьютерных сетей, а именно обнаружении DNS туннелей.

В рамках настоящей работы для достижения поставленной цели решались следующие задачи:

1. Разработка и реализация параллельного алгоритма построения симплициальных комплексов, а также вычисления устойчивых гомологий с учетом их использования на кластерах с большим количеством вычислительных узлов.

2. Исследование структуры разработанных алгоритмов с целью дальнейшей их оптимизации.

3. Использование разработанных алгоритмов для кластеризации DNS трафика с целью обнаружения DNS туннелей.

Объект исследования: устойчивые гомологии

Предмет исследования: алгоритм вычисления устойчивых гомологий для детектирования DNS туннелей.

В работе предложен эффективный распределенный алгоритм обнаружения DNS туннелей, а также произведен анализ разработанных алгоритмов. Представлены результаты проведенных экспериментов по обнаружению DNS туннелей. Итогом работы является разработанная система интеллектуального анализа данных.

Основные положения и результаты работы нашли отражение в 3 публикациях автора.

Цели и задачи работы обуславливают ее структуру, которая состоит из введения, пяти глав основной части, заключения, списка использованных источников и приложения. В первой главе осуществляется краткий обзор проблемы, а также методики ее решения. В последующих главах описываются предложенные методы и их анализ, а также результаты их применения. В конце каждой главы представлены соответствующие выводы.

Диссертация выполнена на 72 страницах, включая 1 приложение информационного характера. Работа включает в себя 5 глав, 29 иллюстраций, 2 таблицы, 72 формулы, 43 библиографических источника.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Основные результаты по каждой из глав:

- В главе 1 приведен обзор литературы по системе DNS, инструментам создания DNS туннелей, а также по способам их обнаружения. Помимо этого, рассмотрен математический аппарат для построения устойчивых гомологий, а также алгоритмы для вычисления устойчивых гомологий.
- В главе 2 сформулирована математическая модель для обнаружения DNS туннелей. Определены атрибуты DNS трафика, которые будут использоваться для детектирования туннелей, описан подход к использованию устойчивых гомологий с целью кластеризации трафика.
- В главе 3 проводится асимптотический анализ алгоритмов построения симплициальных комплексов, а также ставятся эксперименты с целью определения наиболее эффективного алгоритма с точки зрения требуемой памяти и времени для вычисления.
- В главе 4 описывается распределенный алгоритм вычисления интервалов гомологической устойчивости, основанный на классическом алгоритме Эдельсбруннера.
- В главе 5 рассматривается система интеллектуального анализа для решения задачи обнаружения DNS туннелей, описываются её компоненты и принцип работы. Вычисляются параметры качества кластеризации, а также значения чувствительности и специфичности разработанного алгоритма в сравнении с алгоритмом k-means.

ЗАКЛЮЧЕНИЕ

В работе рассмотрен подход к решению проблемы обнаружения DNS туннелей с помощью распределенного алгоритма кластеризации методом устойчивых гомологий. Для анализа DNS трафика использовались величины энтропии доменных имен, средних размеров запросов и ответов, процентов записей типа TXT от общего числа запросов, а также проценов неподтвержденных запросов, относительно рассматриваемого сетевого узла. Данная совокупность признаков использовалась в качестве векторов информационных признаков или образов трафика. Совокупность полученных образов анализировалась с помощью метода устойчивых гомологий, детально описанного в главах 3-4.

Рассмотренный метод кластеризации с помощью устойчивых гомологий позволил обнаружить некоторые установленные DNS туннели.

Существенный вывод из проведенных экспериментов по кластеризации заключается в осутствии необходимости анализа гомологических групп наивысших размерностей. Результаты экспериментов показали, что достаточно вычислить 0-мерные гомологические группы или связные компоненты. Это связано в первую очередь с формой анализируемых данных, а именно – образы DNS трафика образуют сферические кластеры.

Оценки, полученные при анализе качества кластеризации, показывают, что данный метод уступает методу k-means по величине отношения среднего внутрикластерного расстояния к среднему межкластерному расстоянию. Поэтому, представляет интерес сравнение методов кластеризации по другим критериям.

Исходя из результатов кластеризации, требуется проведение детального анализа инструментов и подходов создания DNS туннелей с целью поиска атрибутов, позволяющих получать более качественные результаты в решении задачи обнаружения DNS туннелей.

Разработанная методика поиска DNS туннелей в корпоративных сетях предоставляет решение для задачи обнаружиния только установленных DNS туннелей, что не позволяет предотвратить угрозу безопасности сети. Таким образом, основным направлением в исследовании проблемы угроз безопасности корпоративных сетей заключается в разработке методов предотвращения создания DNS туннелей.

Решение задачи из данной работы планируется использовать в дальнейшем исследовании для анализа истории DNS трафика, на основе которой будет производиться формирование предсказаний о потенциальных угрозах.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Бубнов, Я.В. Кластеризация данных методом устойчивых гомологий / Я.В. Бубнов // Компьютерные системы и сети: 52-я научная конференция аспирантов, магистрантов и студентов – Минск : БГУИР, 2016. – С. 11-13.

Bubnov, Y. DNS Tunneling Detection / Y. Bubnov // International journal of recent trends in engineering & research – Bhavnagar: Nandkunvarba Mahila College, 2016. – P. 241-245.

Бубнов Я.В. Детектирование DNS туннелей / Я.В. Бубнов // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT-2016): сб. статей VI международной заочной научно-технической конференции – Тольятти: ПВГУС, 2016. – С. 85-91.

Магистрант
Бубнов Яков Васильевич

_____

Научный руководитель
Иванов Николай Николаевич
кандидат физико-математических наук, доцент

_____