ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
Т. 63, № 4 ФИЗИКА 2020

МАТЕМАТИЧЕСКАЯ ОБРАБОТКА ДАННЫХ ФИЗИЧЕСКОГО ЭКСПЕРИМЕНТА

УДК 51-74, 004.048, 004.93 DOI: 10.17223/00213411/63/4/30

А.Е. КРАСНОВ, Д.Н. НИКОЛЬСКИЙ

ФОРМИРОВАНИЕ ОДНОМЕРНЫХ РАСПРЕДЕЛЕНИЙ ЗНАЧЕНИЙ КОРРЕЛЯТОРОВ АГРЕГАТОВ СЕТЕВОГО ТРАФИКА [*]

Предложена математическая модель потока агрегированных нагрузочных характеристик пакетов данных сетевого трафика в виде совокупности аналитических сигналов. При этом реальные части аналитических сигналов определены как функции числа пакетов в каждом агрегате, а каждый аналитический сигнал соответствует одному из флаговых индексов агрегата. Проведена условная аналогия между потоком агрегатов сетевого трафика и огибающей потока волновых пакетов когерентного электромагнитного поля, на основе которой рассмотрены фазовые портреты и корреляторы агрегатов сетевого трафика, подобные фазовым портретам и корреляторам огибающих когерентного электромагнитного поля. Показано, что фазовые портреты и одномерные распределения значений корреляторов возможно использовать для описания различных нормальных и аномальных состояний сетевого трафика, обусловленных сложными DDoS-атаками.

Ключевые слова: *сетевой трафик, поток агрегатов, аналитический сигнал, аналогия, огибающая потока волновых пакетов, электромагнитное поле, фазовый портрет, парциальный коррелятор.*

Введение

Для анализа сетевого трафика с целью обнаружения и классификации его аномальных состояний, вызванных, например, DDoS-атаками, было построено множество статистик, основанных на методах корреляционного, спектрального, фрактального и динамического анализа [1, 2]. Однако результаты применения данных статистик для обнаружения сложных атак [2] в литературе не приведены, а были лишь высказаны предположения о возможной применимости рассмотренных методов. В [3] был предложен и исследован новый метод корреляционного анализа связанных с сетевым трафиком сигналов, основанный на введении оператора их эволюции, а также экспериментально показана его применимость для обнаружения сложных атак на основе байесовской классификации. В данной работе оператор эволюции реконструировался по вещественным сигналам, связанным с нагрузочными характеристиками заголовков пакетов данных сетевого трафика.

Цель настоящей работы – развитие метода оператора эволюции, но применительно к аналитическим сигналам трафика, позволяющим рассматривать сетевой канал передачи телеметрических данных как динамическую систему, описываемую обобщенными координатами и скоростями. Для этого вводятся поток агрегатов или агрегированных нагрузочных характеристик пакетов данных сетевого трафика, каждый аналитический сигнал связывается с одним из флаговых индексов агрегата, а значение его реальной части определяется как функция числа агрегированных пакетов. Для формирования статистик и их распределений, характеризующих различные нормальные и аномальные состояния трафика, в работе проводится условная аналогия между потоком агрегатов сетевого трафика и огибающей потока волновых пакетов когерентного электромагнитного поля. Важной задачей исследования является проведение численного эксперимента по использованию данных распределений для различения состояний сетевого трафика при сложных DDoS-атаках.

1. Постановка задачи

В численном эксперименте использовались 10-минутные записи сетевого трафика, снятые с одного из Frontend-серверов к некоторому Web-сервису. Frontend-сервер работал под управлением сервера Nginx [4]. В качестве аппаратной поддержки применялась сетевая карта Qlogic с производительностью 10 Гбит/с.

[*] Статья подготовлена в рамках научно-исследовательской работы по теме «Автоматизированная интеллектуальная информационная система управления (АИИСУ) цифровым университетом. I. Цифровой факультет», выполненной при финансовой поддержке Российского государственного социального университета.

Уважаемые читатели!

Доступ к полнотекстовой версии журнала
«Известия высших учебных заведений. Физика»
осуществляется на платформе
Научной электронной библиотеки eLIBRARY.RU
на платной основе:

https://www.elibrary.ru/contents.asp?titleid=7725