МЕТОД ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ ВТОРЖЕНИЙ В КОМПЬЮТЕРНОЙ СЕТИ, ИСПОЛЬЗУЮЩИЙ КРИТЕРИЙ ФИШЕРА

A METHOD FOR DETECTING ABNORMAL INTRUSIONS IN A COMPUTER NETWORK THAT USES THE FISHER CRITERION

УДК 004

Силаков Николай Владимирович, студент ИУ7-43м, МГТУ им. Н.Э. Баумана, Россия г. Москва, silakov.nikolay@gmail.com

Silakov Nikolay Vladimirovich, student of IU7-43m, Bauman Moscow state technical University, Russia Moscow, silakov.nikolay@gmail.com

АННОТАЦИЯ

На сегодняшний день в области информационной безопасности вопрос, связанный с обнаружением и предотвращением атак злоумышленника в компьютерные сети, является одним из наиболее актуальных для современного общества. Всё чаще ресурсы, где важен фактор доступность информации, подвергаются DoS атакам. Поэтому большую популярность стали получать системы обнаружения вторжений. Для написания работы было проведено имитационное моделирование DoS атак: UDP-flood, Slowloris с целью определения статистических характеристик для их выявления. метод обнаружения DDoS атак на примере Slowloris и UDP-flood атак, использующий критерий Фишера для дисперсий.

ANNOTATION

Today, in the field of information security, the issue of detecting and preventing malicious attacks on computer networks is one of the most relevant for

modern society. Increasingly, resources where the availability of information is important are subject to DoS attacks. Therefore, intrusion detection systems have become very popular. To write this paper, we conducted a simulation of DoS attacks: UDP-flood, Slowloris in order to determine statistical characteristics for their detection. a method for detecting DDoS attacks based on Slowloris and UDP-flood attacks that uses the Fisher criterion for variance.

Ключевые слова: аномальные вторжения, DoS атаки, статистические характеристики, статистические методы, временная последовательность пакетов.

Keywords: abnormal intrusions, DoS attacks, statistical characteristics, statistical methods, time sequence of packets.

Введение

Для предотвращения противоправных действий злоумышленников анализируют весь трафик, проходящий в компьютерной сети на предмет аномалий. Аномалия – это отклонение от правил (в нашем случае от «нормального» поведения сетевого трафика). Эти правила регулируют поведение пользователей, которые не противоречат политике безопасности.

К сожалению, в последнее время все большее распространение получил целый класс атак (DoS/DDoS), направленных на отказ в обслуживании. Одним из способов реализации атаки типа отказа в обслуживании является загрузка всех ресурсов сервера обработкой огромного количества ложных запросов. В большинстве случаев, для организации таких атак используются компьютеры "мирных" пользователей без их ведома и согласия.

Для составления профиля «нормального» трафика исследуются статистические характеристики обучающей выборки. В современных системах обнаружения вторжений (СОВ) статистические методы довольно эффективно обнаруживают атаки, а так же, благодаря тому, что они не анализируют каждый пакет, в следствии чего экономят ресурсы обнаружения атак.

Преимущества данного подхода в следующем:

- не требует полного анализа каждого пакета;
- не требуют больших вычислительных ресурсов, в отличии от других методов;
- способность обнаруживать ранее неизвестные атаки;
- применяются хорошо известные статистические характеристики.

Недостатки данного подхода:

- может пропустить вторжение, которое проявляется в виде последовательности сходных событий;
- система может быть последовательно обучена таим образом, что аномальное поведение будет считаться нормальным;
- сложность определения порога, выше которого аномалии можно рассматривать как вторжение.

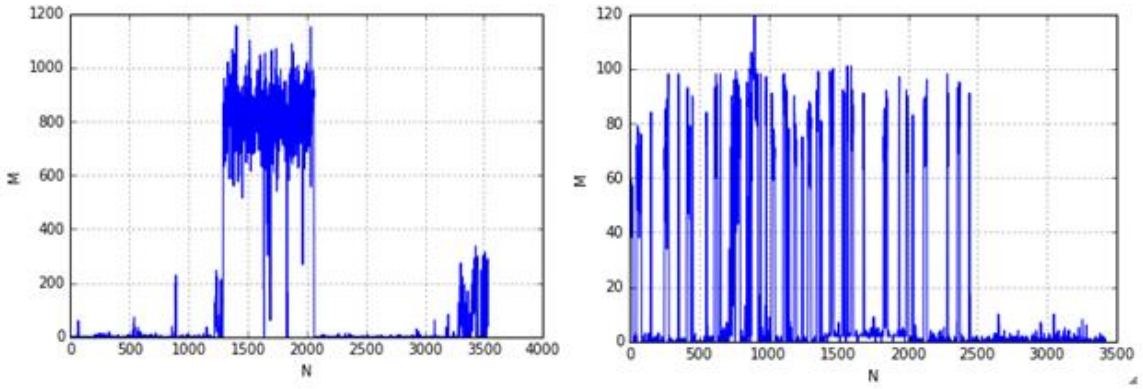
Имитационное моделирование DDoS атак и определение их статистических характеристик.

Для примера рассмотрены наиболее популярные DDoS атаки, такие как UDP-flood и Slowloris. UDP-flood относится к атакам, которые направлены на насыщение полосы пропускания. Этот тип атак легко блокируется на маршрутизаторах обычными access листами, чаще всего пакеты имеют один и тот же размер, содержимое или время жизни (ttl). Атака типа Slowloris относится к атакам на уровне приложений, часто говорят о таких атаках, как атаки l7 (так как уровень приложения по модели OSI находится на 7 уровне). Идея этой атаки очень проста: злоумышленник пытается открыть как можно больше HTTP соединений и держать их как можно дольше, досылая с заданной периодичностью заголовки – отчего лимит одновременных подключений на атакуемом сервере весьма быстро заканчивается, и он перестаёт принимать полезные запросы.

При проведении имитационного моделирования атаки UDP-flood длительность эксперимента составила 354 секунды: от 0 до 137 секунды –

участок штатного функционирования сети (не было атак), от 137 до 205 секунды – участок, на котором проводились атаки, от 205 до 354 секунды – участок после атаки. А при проведении имитационного моделирования атаки Slowloris длительность эксперимента составила 341 секунды: от 0 до 141 секунды – участок штатного функционирования сети (не было атак), от 141 до 201 секунды – участок, на котором проводились атаки, от 201 до 341 секунды – участок после атаки.

На рисунке 1 представлен сетевой трафик на всем интервале наблюдения при имитации атак. На рисунке 3 (а) при атаке UDP-flood, на рисунке 3 (б) при атаке Slowloris.



а) б)

Рисунок 1. График сетевого трафика на всём интервале наблюдения.

После имитационного моделирования были получены следующие графики и вероятностные характеристики:

1. Гистограммы распределения пакетов:

На рисунке 2 (а, б, в) представлены гистограммы распределения пакетов на разных участках наблюдения для атаки UDP-flood, а на рисунке 2 (г, д, е) - для атаки Slowloris.

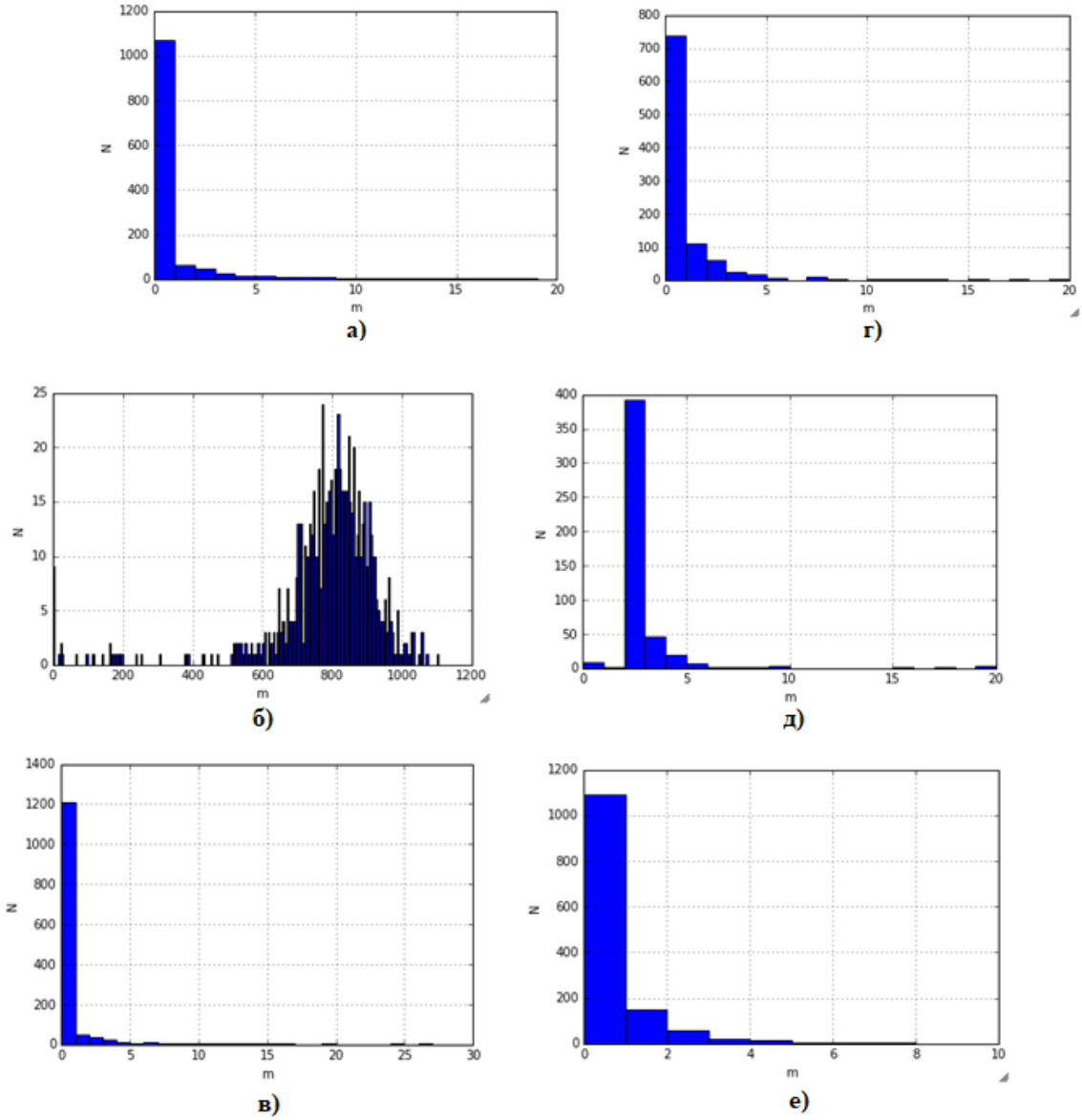


Рисунок 2. Гистограмма распределения пакетов на разных интервалах наблюдения.

а, г – до атаки; б, д – во время атаки; в, е – после атаки; высота уровней квантования - 1 пакет.

2. Автокорреляционная функция:

На рисунке 3 (а, б, в) представлены автокорреляционные функции на разных участках наблюдения для атаки UDP-flood, а на рисунке 3 (г, д, е) - для

атаки Slowloris.

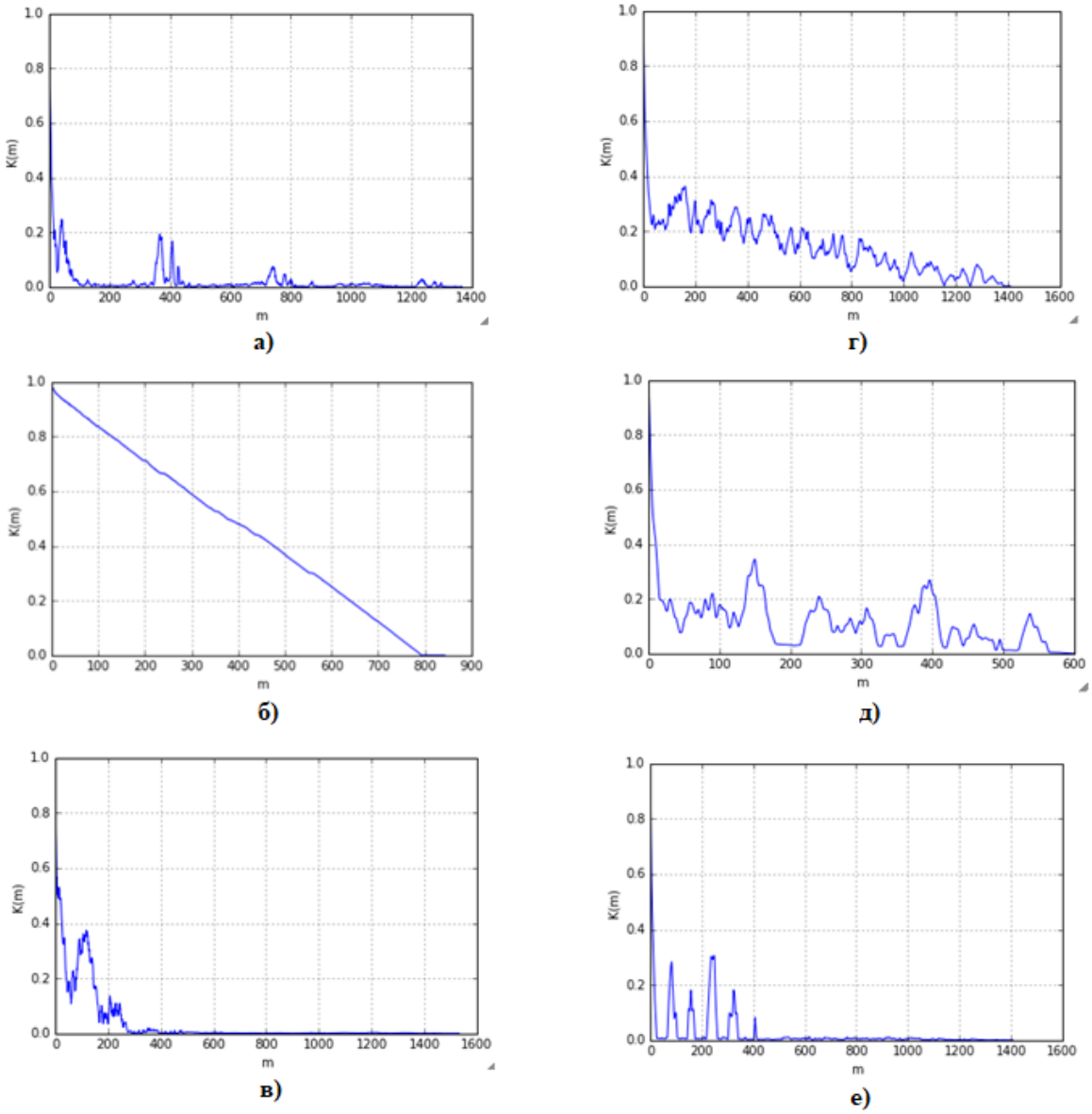


Рисунок 3. Автокорреляционная функция трафика на разных интервалах наблюдения.

а, г – до атаки; б, д – во время атаки; в, е – после атаки.

3. Статистические характеристики:

В таблице №1 и №2 представлены значения статистических характеристик при имитации UDP-flood и Slowloris соответственно. В качестве статистических характеристик используются: математическое ожидание, дисперсия и интервал корреляции.

Таблица 1. Статистические характеристики при реализации UDP-flood.

Характеристики	До атаки	Во время атаки	После атаки
M_x	5,2	788,7	13,9
D_x	576,5	21890,9	2376,1
τ_k , с	39,8	79,3	23,6

Таблица 2. Статистические характеристики при реализации Slowloris.

Характеристики	До атаки	Во время атаки	После атаки
M_x	22,9	16,7	3,7
D_x	1248,9	936,1	255,1
τ_k , (с)	115,7	55,7	40,4

Проведенные имитационные моделирования показали, что статистические характеристики сетевого трафика во время атаки отличаются от характеристик легитимного трафика и они могут быть положены в основу разрабатываемых алгоритмов обнаружения аномальных вторжений в компьютерные сети.

Реализация алгоритма критерия Фишера для дисперсий на исследуемых данных

Для анализа временной последовательности пакетов (ВПП) исследуемых трафиков (рисунок 2) с помощью алгоритма критерия Фишера для дисперсий используется модифицированная формула (1).

$$\boldsymbol{F(k) = T}\left(\frac{\frac{1}{N_1}\sum_{i=0}^{N_1-1}(x_k(i)-x_k^*(i))^2}{\frac{1}{N_2}\sum_{i=0}^{N_2-1}(y_k(i)-y_k^*(i))^2}\right), \quad (1)$$

где k — номер шага,

$x_k(i) = x[k \cdot s, k \cdot s + N1]$ — значения окна наблюдения,

$y_k(i) = y[k \cdot s, k \cdot s + N2]$ — значения окна обнаружения,

s — шаг,

N_1 и N_2 — размеры окон,

$x_k{}^*(i)$ и $y_k{}^*(i)$ — математические ожидания для k—го окна,

T — функция (введена для того, чтобы вместо двух уровней h1 и h2 использовать один h), определяемая как

$$\boldsymbol{T(x)} = \begin{cases} \boldsymbol{\frac{1}{x}}, & \boldsymbol{x < 1} \\ \boldsymbol{x}, & \boldsymbol{x \geq 1} \end{cases}, \quad (2)$$

Решение о наличии или отсутствии аномалии принимается на основании заданных уровней h1 и h2. Если значение функции Фишера находится между заданными уровнями h1 и h2, то принимается решение, что аномалии нет. Если же значение функции Фишера выходит за заданные уровни h1 и h2, то принимается решение, что аномалия есть.

На рисунке 6 изображены окно наблюдения и окно обнаружения на графике ВПП трафика UDP-flood. При этом N_1 и N_2 равны 500 дс. Окно наблюдения и окно обнаружения следуют друг за другом с определенным шагом s.

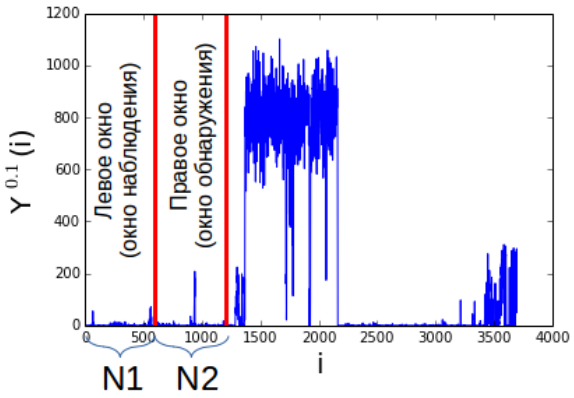
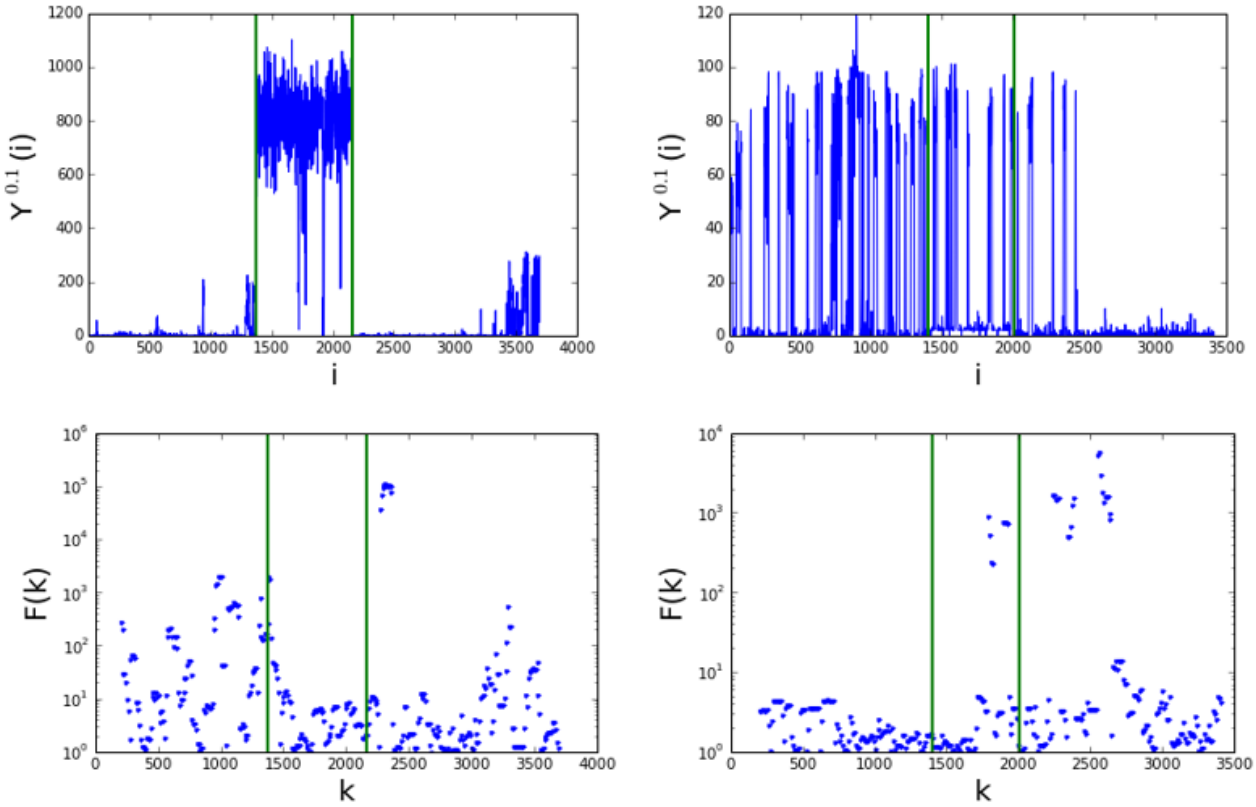


Рисунок 4. Поясняющий рисунок к формуле (1).

На рисунке 5 представлены графики сетевого трафика на всём интервале наблюдения для данных атак, а под ними функции Фишера для дисперсий (ФФД)**Ошибка! Источник ссылки не найден.**. Установлена параметры построения графиков $\boldsymbol{N_1}$=100 дс, $\boldsymbol{N_2}$=100 дс, s=10 дс. Для наглядности графики ВПП трафиков и ФФД были синхронизированы, а также на них отображены границы начала и конца атак.



а) б)

Рисунок 5. Графики ВПП исследуемых трафиков и графики ФФД для этих ВПП.

Как видно по рисунку 5 а), на границах периода действия атаки типа UDP-flood ФФД достигает наибольших значений, а во время атаки достигает минимума. Это означает, что если критерием наличия аномалии считать превышение порога, то алгоритм пропустит всю атаку. Поэтому необходимо поменять алгоритм обнаружения с помощью порога.

Для правильного детектирования атаки необходимо ввести порог. На рисунке 6 построена примерная модель поведения ФФД.

В тот момент, когда окно обнаружения заходит в зону атаки, значения ФФД начинают возрастать и в какой-то момент превысят порог (начало участка А). После превышения порога, значения ФФД продолжат возрастать некоторое время, пока окно наблюдения не войдет в зону атаки. В момент входа окна наблюдения в зону атаки значения ФФД начнут убывать и вскоре опустятся ниже порога (конец участка А).

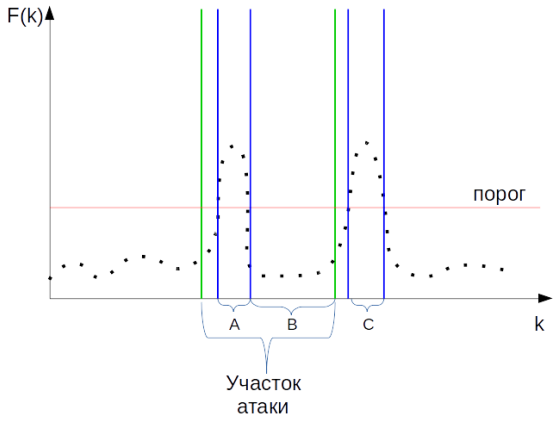


Рисунок 6. Модель поведения ФФД.

В участке В окно обнаружения и окно наблюдения находятся в зоне атаки, поэтому значения ФФД будут находиться ниже порога. В момент выхода окна обнаружения из зоны атаки значения ФФД начнут вновь увеличиваться, и в определенный момент снова превысят порог (начало участка С). Увеличение значений ФФД будет продолжаться до тех пор, пока окно наблюдения не начнет выходить из зоны атаки. В момент выхода окна наблюдения из зоны атаки значения ФФД начнут падать, пока не опустятся ниже порога (конец участка С).

Алгоритм для обнаружения аномалий начинает сигнализировать об атаке, как только значения ФФД превысят порог (начало участка А). Сигнализация об атаке будет продолжаться до тех пор, пока значения ФФД не опустятся ниже порога, а потом снова его превысят (начало участка С). После окончания участка С алгоритм начинает заново анализировать трафик.

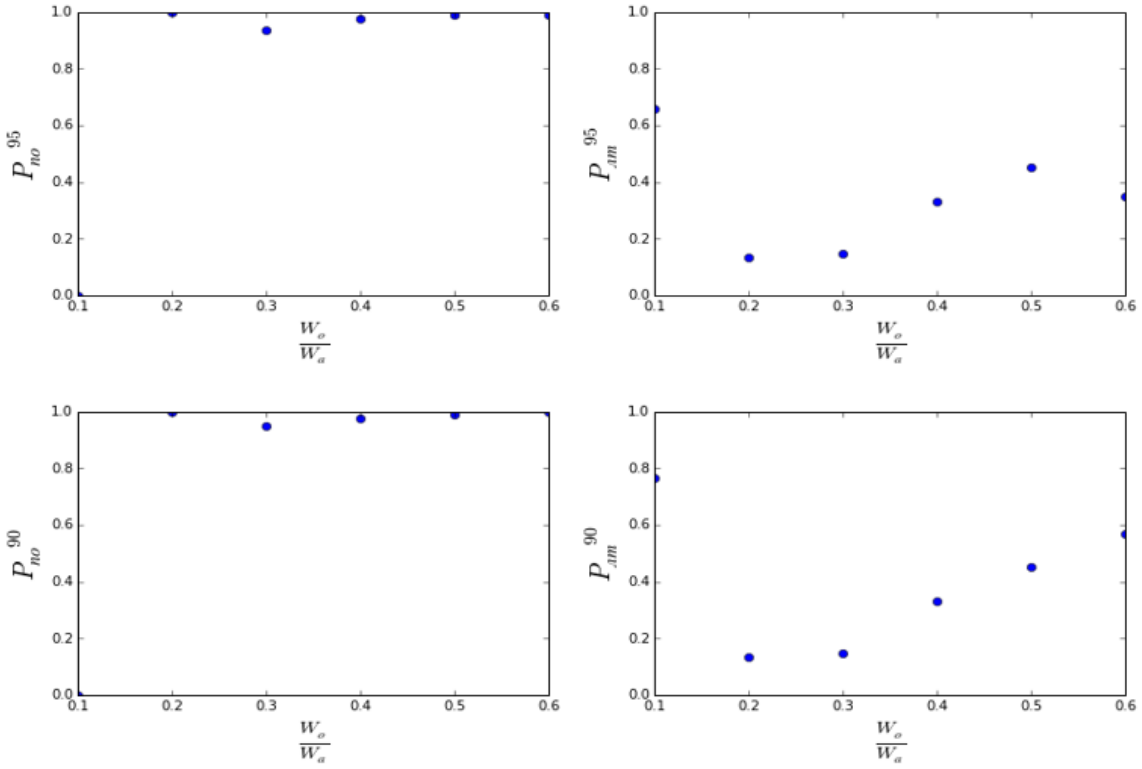
Оценка алгоритма критерия Фишера для дисперсий

Вероятность правильной работы и вероятность ложной тревоги вычисляются по формулам **Ошибка! Источник ссылки не найден.** и (4):

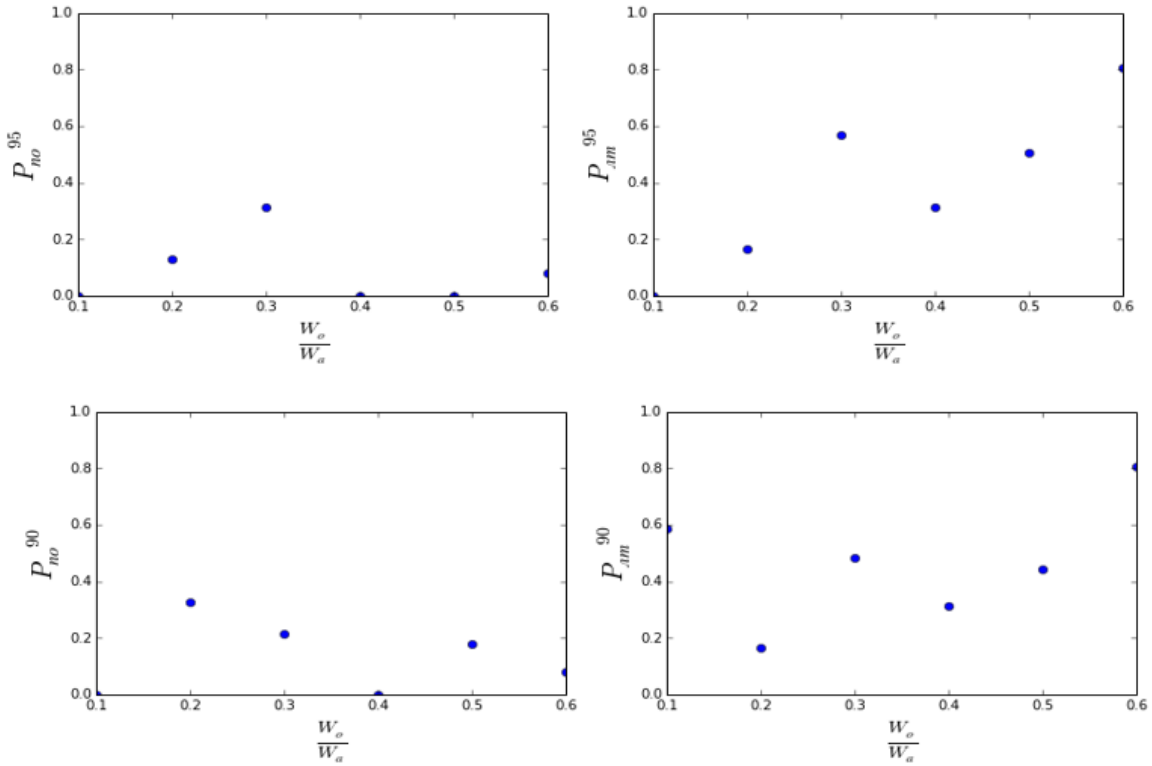
$$\boldsymbol{P_{по}} = \frac{\boldsymbol{T_1}}{\boldsymbol{T_A}}, \quad (3)$$

$$\boldsymbol{P_{лт}} = \frac{\boldsymbol{T_2}}{\boldsymbol{T_o}},, \quad (4)$$

Рассчитана вероятность $P_{по}$ и $P_{лт}$ при различных отношениях $\frac{W_o}{W_a}$, где W_o — ширина окна обнаружения, W_a — ширина атаки (рисунок 7). При этом верхний индекс в $P_{по}$ и $P_{лт}$ обозначает процент данных, отсеченных уровнем h.



а)



б)

Рисунок 7. Зависимости P_по и P_лт от отношения W_o/W_a при разных порогах h

а) UDP-flood, б) Slowloris.

Данные результаты говорят о том, что алгоритм Фишера для дисперсий эффективен для атаки UDP-flood и не эффективен для атаки Slowloris.

Заключение

В настоящий момент от действий DDoS атак страдают многие сервисы, особенно это касается игровых серверов и веб-приложений, так как для них важен фактор доступности, а такие атаки не требуют особых усилий и навыков у злоумышленников.

Несмотря на то, что со временем растут скорости и расширяются каналы передачи данных, атаки на l7 уровнемогут вызвать отказ в обслуживании сервиса и при этом не забить канал. Становится очевидным, что анализировать каждый пакет из сетевого трафика усиливает потребность в вычислительных ресурсах, а это, в свою очередь, ведёт к росту нагрузки системы. Поэтому всё чаще используются статистические подходы к обнаружению DDoS атак.

Для улучшения обнаружения атак необходимо добавлять критерии отличающие легитимный трафик для своего сервиса. Также важен выбор порога, поскольку от правильности его настройки будет зависеть количество ложных срабатываний и пропусков событий.

ЛИТЕРАТУРА:

1. Дарховский Б.С., Бродский Б.Е. Апостериорное обнаружение момента «разладки» случайной последовательности — Теория вероятности и её применение., 1980, т. XXV, в. 3 — С.635-639
2. Дисперсионный анализ сетевого трафика для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А. А. Кузнецов, А. А. Смирнов, Д. А. Даниленко // Системи обробки інформації. - 2014. - Вип. 2. - С. 124-133.
3. Системы обнаружения вторжений.Intrusion Detection System - IDS., 2016 // WEB: https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids
4. Шелухин О.И., Д.Ж.Сакалема, Филинова А.С. Обнаружение вторжений в компьютерные сети. Сетевые аномалии // Горячая линия – телеком, 2013г. –С 220.

LITERATURE:

1. Darkhovsky B. S., Brodsky B. E. a posteriori detection of the moment of" breaking " of a random sequence-probability Theory and its application., 1980, vol. XXV, V. 3-P. 635-639
2. Dispersion analysis of network traffic for detecting and preventing intrusions in telecommunications systems and networks / A. A. Kuznetsov, A. A. Smirnov, D. A. Danilenko / / Sistemi obrobki informatsii. - 2014. - VIP. 2. - Pp. 124-133.
3. intrusion detection Systems.Intrusion Detection System - IDS., 2016 // WEB: https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids
4. Shelukhin O. I., D. Zh. Sakalema, Filinova A. S. Detection of intrusions into computer networks. Network anomalies / / Hotline-Telecom, 2013-C 220.