УДК 004.7

И.В. Рубан, Д.В. Прибыльнов, Е.С. Лошаков

Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков

МЕТОД ВЫЯВЛЕНИЯ НИЗКОСКОРОСТНОЙ АТАКИ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

В статье затронуты принципы и особенности реализации низкоскоростной DOS – атаки. Предложен алгоритм реализации метода обнаружения данного типа атаки. Рассмотрены особенности выявления шаблонов трафика в зависимости от состояния загруженности сервера. Рассмотрены аспекты связанные с задержками в канале связи, а также возможными маскирующими воздействия со стороны атакующего.

Ключевые слова: *информационная безопасность, моделирование обнаружения сетевых атак, модель DOS-атаки, модель выявления DOS-атаки, медленные DOS-атаки, отказ в обслуживании, модель выявления атаки типа отказ в обслуживании.*

Введение

DDoS-атаки получили широкое распространение в связи с простотой реализации и доступностью инструментов для поиска уязвимостей и анализа на этапе подготовки атаки как один из надежных способов гарантированного достижения целей.

С развитием интернет – технологий и развитием на их базе сетей специального назначения, возникают особенности связанные с информационной безопасностью, а также с вопросами непосредственно связанными с непрерывностью предоставляемых вычислительных мощностей. Так на первый план необходимо вынести атаки на непрерывность предоставляемых услуг или другими словами отказ в обслуживании сетью. При всей простоте выполнения атаки, попытки противостоять атакам стандартными методами обычно оказываются безрезультатными. Так, прежде, чем искать средства противодействия DDoS-атакам, необходимо разобраться с механизмом реализации атак типа отказ в обслуживании. Стоит заметить, что изначально технология DDoS применялась исключительно для проверок пропускной способности сетей. Однако в дальнейшем получили широкую реализацию, как инструментарий для достижения максимального вредоносного эффекта наиболее простыми методами [1].

DDoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) — атака на вычислительную систему с целью довести её до отказа, то есть, создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.). Но чаще это мера, которая приводит к простою сложнейших сбалансированных систем достаточно простым способом без учёта каких-либо особенностей атакуемой информационной сети [2].

Применительно к системам специального назначения, атаки типа «отказ в обслуживании» представляют собой непосредственную угрозу для систем управления.

Простота реализации DDoS-атак делает их распространёнными, а широкое разнообразие используемых инструментов затрудняет поиск и применение механизмов противодействия.

Основная часть

Для противодействия распределенным атакам, направленным на отказ в обслуживании, требуется выполнение двух основных задач [4].

1. Диагностировать DDOS-атаку на самых ранних стадиях. Чем раньше будет обнаружена

DDOS-атака, тем раньше сможет включиться в игру сетевой администратор и тем раньше можно будет начать проводить антиDDOS-мероприятия. Кроме того, при обнаружении DDOS-атаки можно будет, не дожидаясь реагирования администратора, автоматически запустить мероприятия по противодействию: задействовать резервные каналы связи, включить фильтры и т.д.

2. Вторая задача связана с разделением общего потока трафика на вредоносный и обычный.

Поняв, какие из клиентских запросов являются результатом DDOS-атаки, можно будет создать соответствующие правила для межсетевого экрана, правила для маршрутизатора или же, в случае масштабной атаки, передать эти данные на вышестоящие маршрутизаторы[4].

Одним видов DDOS-атак являются медленные атаки типа отказ в обслуживании. Их особенностью является использование недостатка в механизме рестарта протокола TCP. Исходя из особенностей атаки, а также построенной модели атаки на указан-

© И.В. Рубан, Д.В. Прибыльнов, Е.С. Лошаков

ный механизм, необходимо строить средства обнаружения и противодействия.

Рассмотрим более детально механизм медленной DOS-атаки. Создавая периодические перебои, искусственно вызывается простой канала связи. Перебои создаются в определённые временные интервалы с использованием импульсов высокоинтенсивного трафика. Искажение временных интервалов может быть вызвано, как умышленно с целью маскировки вредоносного воздействия, так и неумышленно, в результате задержек в канале связи.

Исходя из специфики медленных DOS – атак, можно сформулировать основное их отличие от распределённых атак типа отказ в обслуживании. Данное отличие заключается в отсутствии резкого прироста трафика, чем в дальнейшем может быть вызван отказ в обслуживании сервером. Если рассматривать график зависимости интенсивности трафика от времени (рис. 1), то видно, что интенсивность трафика при распределённой DOS – атаке постоянно возрастает. А в случае медленной DOS – атаки, возможно наблюдать пики трафика на определённых временных интервалах. Если рассматривать указанный вид атаки, то зависимость суммарного количества трафика от времени экспоненциально уменьшается, точно так же как и в результате распределённой DOS – атаки.

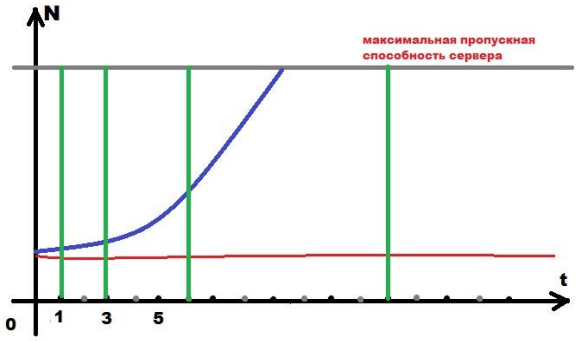

Рис. 1. Зависимость интенсивности потока трафика от времени при медленной и распределённой атаках

Из выше изложенного следует, что структурная модель, распределённой и медленной DOS – атаки, также как и графовая не имеют принципиальных отличий, что делает обнаружение низкоскоростных атак и отнесение их к отдельному классу для дальнейшего противодействия затруднительным.

Необходимо разработать новый подход к выявлению и распознанию медленных DOS – атак. Таким подходом является распознавание шаблонов трафика. Основываясь на специфике медленной DOS – атаки, а именно: необходимости создания периодических перебоев в канале связи, создаётся система распознавания, в основе которой заложен принцип сравнения полученных сервером шаблонов трафика с эталонными, заранее рассчитанными шаблонами.

Эталонные расчётные времена получения пиковых нагрузок представлены в табл. 1 в результате расчёта согласно стандарта RFC 793 по соотношению:

$$RTO_{i+1} = RTO_i + 2 * RTO_i ; \quad (1)$$
$$RTO_0 = 1 \text{ секунда.}$$

Таблица 1

Значение между интервалами получения пиков загрузки атакуемым сервером

	Значение времени в соответствии с номером интервала					
Номер интервала	0	1	2	3	4	5
Предельные значения окончания интервала	1	3	9	27	81	243
Длительность интервала	2	6	18	54	162	

В основу выявления факта атаки ложится сопоставление полученных пиковых нагрузок на временных интервалах с полученными эталонными интервалами времени и учётом возможности изменения времени прихода очередного пика атаки.

Предложенный метод включает в себя четыре основных этапа, на основе которых построен алгоритм, представленный на рис. 2.

1. Выявление факта перегрузки канала связи, достаточного для выдачи сервером таймаута некоторому количеству обрабатываемых потоков.

2. Создание эталонных шаблонов трафика в зависимости от времени получения первого пика;

3. Выявление последовательности полученных пиков трафика, сопоставление с шаблоном.

4. Принятие решения об отнесении выявленной последовательности перегрузок к наличию или отсутствию атаки.

Перед началом старта выявления факта атаки на защищаемый сервер, необходимо однозначно выявить «бутылочное горлышко» канала связи и определить его пропускную способность. Также необходимо выполнять нормализацию всех показателей загрузки сервера, в том числе и пропускной способности канала связи. Под нормализацией понимается деление на максимальное значение данного показателя для заданного сервера. Для дальнейшего удобства можно помножить полученные показатели на 100%, и выполнять операции сравнения в процентных соотношениях.

Начальное состояние системы перед началом активного внутреннего мониторинга: от системы внешнего мониторинга поступил сигнал о сбое в канале связи или превышении заданного порогового уровня загрузки канала связи ($C_з \geq 90\%$).

Пороговый уровень, равный 90% от максимальной загрузки канала связи, для задачи выявления медленной DOS атаки является приемлемым. При достижении данного уровня загрузки с вероят-

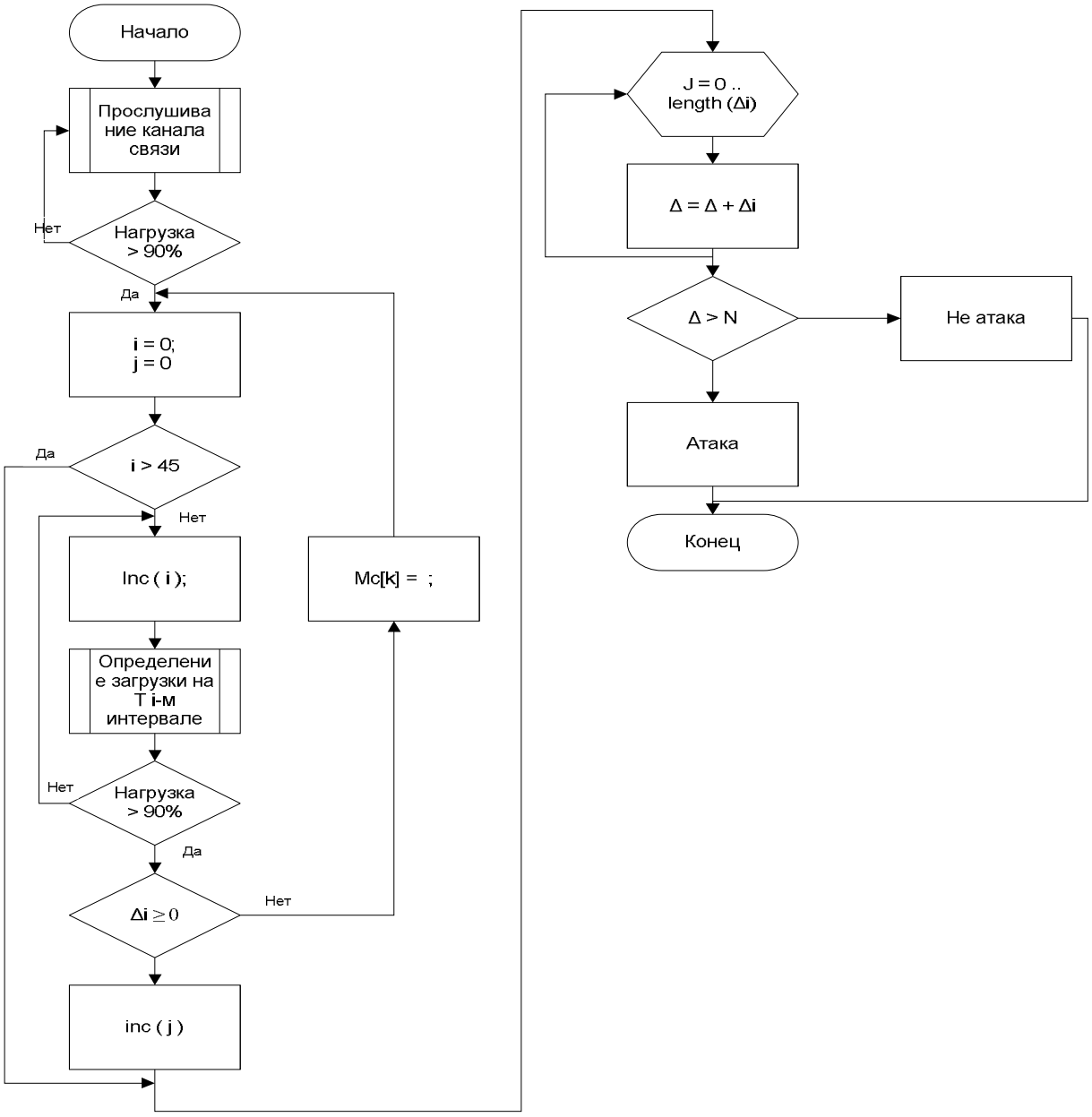

Рис. 2. Алгоритм обнаружения медленной DOS атаки

ностью равной 0.98 протокол TCP не получает квитанций о доставке пакетов, соответственно, для данного потока начинается переход на работу по шкале времени RTO или, если данный переход уже был выполнен, то время RTO удваивается. Данный факт, в свою очередь, является предпосылкой к возникновению медленной DOS атаки.

После того, как был зафиксирован первый пик трафика, включается прослушивание канала связи специализированным программным обеспечением, установленным на сервер с дискретностью в 1 секунду на интервале времени в 45 секунд и, полученные значения загрузки канала связи, сохраняются в базе данных в виде таблицы или массива. Первый пик трафика становится началом отсчёта, присваивается порядковый номер 0.

Эталонные времена прихода пиков атаки представлены в (табл. 1) и также сохраняются в базе данных.

Каждую последующую секунду снимается показатель загруженности. Если получен пик трафика, то фиксируется время получения относительно начала отсчёта, то есть прихода первого пика трафика, время прихода очередного пика T_i, сохраняется в отдельном массиве (таблице) базы данных. Рассчитывается дисперсия между эталонным и полученным временем

$$\Delta_i = T_{эi} - T_i \qquad (2)$$

В случае, если $\Delta_i << 0$, то полученный пик считается случайным перебоем в канале связи. В результате этого необходимо обнулить счётчик на-

чала отсчётов и ожидать следующего пика трафика, приняв его за начало отсчёта. Также необходимо внести запись о сбое в канале связи в базу данных для дальнейшего проведения анализа.

В случае, когда $\Delta_i \le 0$, то необходимо продолжить расчёты.

На интервале 45 секунд, получен массив времён T_i и рассчитаны отклонения приходов пиков Δ_i – дисперсии времён T_i с эталонами, задача выявления факта медленной DOS атаки вырождается в оценку суммарной дисперсии Δ.

$$\Delta = \sum_{i=1}^{n} \Delta_i \qquad (3)$$

В результате получаем три случая:

$\Delta \to +\infty$, проходит DDOS атака или возникновение сбоя в канале связи в результате выхода из строя какого-либо устройства сети.

$\Delta \to -\infty$, происходят спонтанные перебои в канале связи, вызванные временной загрузкой данного канала связи.

$\Delta \to 0$, сервер подвергся вредоносному воздействию по средства медленной DOS атаки.

В общем виде алгоритм обнаружения медленной DOS - атаки представлен на (рис. 1).

Этапы выполнения представляют собой целостную последовательность взаимосвязанных процедур. Необходимо акцентировать внимание на уточнении процедур получения эталонных значений, которые будут использоваться для вычисления промежуточных отклонений, а также на процедуре вычисления граничного значения разброса времён получения пиков трафика. Данные процедуры несут основную вычислительную нагрузку в ходе выполнения этапа обнаружения низкоскоростной DOS – атаки.

Конечный результат, а именно выявление факта воздействия на ИТКС по средствам медленной DOS – атаки непосредственно зависит от выбранных пороговых уровней Δ, то есть минимального порогового уровня достаточного для отнесения $\Delta \to 0$.

Вывод

Предложенная структурная модель обнаружения медленных атак типа отказ в обслуживании позволяет выявить и отнести обнаруженную атаку к известному классу атак, что в свою очередь даст возможность применить методы противодействия без вреда для системы, которая предоставляет сервисы обслуживания.

Список литературы

1. Платов А. DDoS-атака и защита от нее [Электронный ресурс] / Антон Платов – Режим доступа к стате:. http://www.nestor.minsk.by/sr/2008/10/sr81004.html.

2. DoS-атака. Материал из русскоязычной Википедии [Электронный ресурс]. – Режим доступа к материалу: http://ru.wikipedia.org/wiki/DoS-атака

3. Предотвращение атак с распределенным отказом в обслуживании (DDoS). Официальный сайт компании Cisco [Электронный ресурс]. – Режим доступа к материалам сайта: http://www.cisco.com/web/RU/pro-ducts/ps5887/products_white_paper0900aecd8011e927_.html.

4. Методы защиты от DDOS нападений [Электронный ресурс]. – Режим доступа к материалам: http://www.securitylab.ru/analytics/216251.php.

5. RFC 793. Протокол управления передачей (Transmission Control Protocol) [Электронный ресурс]. – Режим доступа к переводу описанию протокола http://www.ipv6.ru/russian/documents/theory/rfc/793.php.

Поступила в редколлегию 9.08.2013

Рецензент: д-р техн. наук проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ВИЯВЛЕННЯ НИЗЬКОШВИДКІСНОЇ АТАКИ ТИПУ «ВІДМОВА У ОБСЛУГОВУВАННІ»

І.В. Рубан, Д.В. Прибильнов, Є.С. Лошаков

У статті розглянуті особливості реалізації низько швидкісної DOS-атаки. Запропоновано алгоритм виявлення даного типу атаки. Розглянуті особливості виявлення шаблонів трафіка у залежності від стану завантаження серверу. Розглянуті аспекти пов'язані із затримками у каналі зв'язку а також можливими маскуючими впливами зі сторони атакуючого.

Ключові слова: *інформаційна безпека, моделювання виявлення мережевих атак, модель DOS-атаки, модель виявлення DOS-атаки, повільні DOS-атаки, відмова в обслуговуванні, модель виявлення атаки типа відмова в обслуговуванні.*

A METHOD OF EXPOSURE OF LOW-SPEED ATTACK OF TYPE «DANIED OF SERVICE»

I.V. Ruban, D.V. Pribylnov, E.S. Loshakov

The article considers features low speed DOS attacks realization. The algorithm of exposure of this type of attacks is offered. The features of traffic templates exposure depending on the server load status are examined. The aspects related to the delays in a communication channel as well as possible masking impact from attacker are viewed.

Keywords: *informative safety, design of exposure of network attacks, model of DDOS attacks, DDOS attacks, a model of exposure of DOS attacks, slow DOS attacks, denied of service.*