Математические структуры и моделирование
2013. № 1(27). С. 42–45

УДК 517.925:004.052.3

ОПИСАНИЕ DDOS-АТАКИ С ПОМОЩЬЮ КАТАСТРОФЫ «СБОРКА»

А.К. Гуц, Д.Н. Лавров

Показано, что DDoS-атаки на компьютерные системы можно описать с помощью катастрофы «сборка».

$DDoS$-атаки — наиболее распространённая атака злоумышленников на компьютерный информационный ресурс. Существуют два способа добиться от сервера отказа в обслуживании ($Denial\ of\ Service$).

Первый способ позволяет остановить работу *всей* атакуемой компьютерной системы. Для этого злоумышленник посылает серверу-жертве данные или пакеты, которые она не ожидает, и это приводит либо к остановке системы, либо к её перезагрузке. В результате никто не сможет получить доступ к ресурсам. Атака хороша тем, что с помощью нескольких пакетов можно сделать систему неработоспособной.

Второй способ ($Flood$-атаки) состоит в том, чтобы добиться переполнения системы с помощью такого большого количества пакетов, которое невозможно обработать. Например, если система может обрабатывать только 10 пакетов в секунду, а злоумышленник отправляет к ней 20 пакетов в секунду, то остальные пользователи при попытке подключиться к системе получают отказ в обслуживании, поскольку все ресурсы заняты. При таких атаках значительно снижается производительность компьютерной системы или приложений. Очевидно, что при этом способе атаки наблюдается резкое возрастание входящего трафика.

Есть и третий способ атаки, при которой стараются добиться переполнения канала, т.е. резко снизить пропускную способность канала.

Целью нашей заметки является математическое описание второго способа $DDoS$-атаки.

Мы видим, что для этого способа, во-первых, важную роль играет *входящий трафик*. Трафик — это параметр τ, характеризующий типичную ситуацию для функционирующей компьютерной системы, которая говорит, что, как правило, ежедневный трафик именно таков, и система способна с ним справляться с определённым запасом надёжности системы.

Увеличение трафика требует для его обработки увеличения свободных ресурсов системы.

Омский государственный университет им. Ф.М. Достоевского
E-mail: guts@omsu.ru, lavrov@omsu.ru

Во-вторых, мы видим, что важным параметром стойкости, надёжности компьютерной системы является ее *производительность* p, выражающаяся как в скорости обработки входящих пакетов, так и количестве устанавливаемых соединений.

При получении сервером пакета данных происходит его обработка. Это требует времени и определённых ресурсов компьютерной системы. Если приходит новый пакет, а сервер занят приёмом или обработкой предыдущего или другого пакета, то вновь приходящий запрос-пакет *ставится в очередь*, занимая при этом часть ресурсов системы.

При $Flood$-атаках происходит исчерпание ресурсов, а точнее ресурсов процессора, памяти или каналов связи, сводящееся к следующим моментам:

– ограниченное количество соединений, находящихся в состоянии установки (соединения), которыми располагает система (при TCP SYN $Flood$- и TCP $Flood$-атаках направляется большое количество запросов на инициализацию TCP-соединения с потенциальной системой-жертвой). Добиваются того, что система не может устанавливать новые соединения,

– способность системы автоматически отвечать на отправленные ping-запросы ($ICMP$ $Flood$-атаки, $Smurf$-атаки). Если запрос использует большие (64 кБ) ICMP-пакеты, то они подвергаются фрагментации. Большое количество фрагментированных пакетов, могут привести к зависанию атакуемой системы, расходующей свои ресурсы на сборку.

– снижение пропускной способности канала связи за счёт потока большого количества UDP-пакетов разного размера (UDP $Flood$-атаки). Происходит перегрузка канала связи, и сервер, работающий по протоколу TCP, перестаёт отвечать.

Таким образом, способность к нормальному функционированию определяется числом откликов на запросы.

Обозначим через $x(t)$ число откликов на запросы в момент времени t.

Тогда

$$x(t+1) = x(t) + f[x(t)] + \tau, \tag{1}$$

где $f[x(t)]$ — результат работы системы по обработке запросов на момент t. В уравнении отражено требование, что больший трафик требует нарастания числа откликов на запросы.

Примем для простоты, что $f[x(t)] = kx(t)$, где k — величина, определяющая производительность системы

$$k = \{p - g[x(t)]\}, \tag{2}$$

сводящаяся к средней скорости обработки входящих пакетов p с учётом её падения или увеличения в зависимости от объёма занятых ресурсов: чем больше загружены ресурсы, тем меньше скорость обработки входящих пакетов.

Пакет x, стоящий в очереди, должен пройти через соединение (либо просто пройти по забитому каналу, как UDP-пакет) и после обработки, возможно, породить отклик для пославшего его компьютера. Иначе говоря, пакет участвует в процессе его обработки как минимум дважды. Поэтому мы это отразим путём принятия предположения, что $g[x] = x^2$.

Таким образом, $g[x(t)] = [x(t)]^2$ и тогда

$$x(t+1) = x(t) + [(p - p_0) - x^2(t)]x(t) + (\tau - \tau_0), \tag{3}$$

где введены некоторые «типичные» характерные для данного сервера величины производительности p_0 и трафика τ_0. При переходе к непрерывному времени уравнение (3) сводится к уравнению

$$\frac{dx}{dt} = [(p - p_0) - x^2(t)]x(t) + (\tau - \tau_0)$$

или

$$\frac{dx}{dt} = -\frac{\partial}{\partial x}V(x, p, \tau), \tag{4}$$

где

$$V(x, p, \tau) = \frac{1}{4}x^4 - \frac{1}{2}(p - p_0)x^2 - (\tau - \tau_0)x. \tag{5}$$

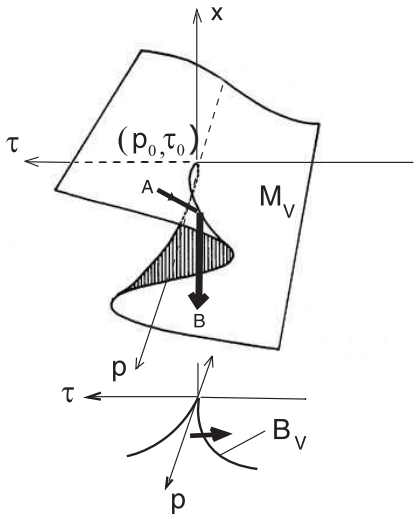

Рис. 1. Катастрофа сборки

Из вида выражения (5) видим, что сервер — это потенциальная динамическая система, потенциал которой описывается катастрофой «сборка» [1].

Естественно предположить, что в повседневных рутинных условиях сервер имеет в среднем одни и те же производительность p и трафик τ. При этом число откликов в среднем является более или менее постоянным, т.е. $x(t) = x_0 = const$. В таком случае

$$\frac{dx}{dt} = 0$$

и, следовательно, $x_0 = x_0(p, \tau)$ — это решение уравнения

$$\frac{\partial}{\partial x}V(x_0, p, \tau) = 0.$$

Такие решения называются состояниями *стационарного равновесия* системы. Сервер, таким образом, пребывает, как правило, в состоянии стационарного равновесия. Точки-равновесия (x_0, p, τ) находятся в пространстве с осями x, p, τ и началом $(0, p_0, \tau_0)$ на поверхности M_V (рис.1). Из рисунка видно, что если

компьютерная система имела производительность $p < p_0$, т.е. не очень высокую, и трафик $\tau > \tau_0$ и находилась в равновесии A, то при нарастании трафика (жирная стрелка на рисунке от A к B) происходит скачкообразное обрушение такой характеристики, как количество откликов на запросы. Другими словами, происходит переход к равновесию «упавшего» сервера B.

Литература

1. Брёкер Т., Ландер Л. Дифференцируемые ростки и катастрофы. М.: Мир, 1977.