Математические структуры и моделирование
2016. № 3(39). С. 184–188

УДК 519.83+681.3.067

DDOS-АТАКИ КАК ДИФФЕРЕНЦИАЛЬНАЯ ИГРА

Т.В. Вахний
к.ф.-м.н., доцент, e-mail: vahniytv@mail.ru
А.К. Гуц
д.ф.-м.н., профессор, e-mail: guts@omsu.ru

Омский государственный университет им. Ф.М. Достоевского

Аннотация. Для нахождения возможных равновесных ситуаций при DDoS-атаках на компьютерные системы предлагается использовать теорию дифференциальных игр.

Ключевые слова: DDoS-атаки, защита компьютерной системы, дифференциальная игра, равновесие Нэша.

Введение

DDoS-атаки являются распространённым способом нанесения ущерба компьютерным системам. Как известно, DDoS-атака предполагает истощение злоумышленниками ресурсов, например, Web-сервера или канала связи путём коллективной отправки со своих компьютеров бессмысленных вредоносных запросов. При этом легитимные пользователи не могут получить доступ к предоставляемым системой ресурсам (серверам), либо такой доступ затруднён. Целью такой атаки является доведение компьютерной системы до отказа в обслуживании.

Полностью защититься от DDoS-атак невозможно, так как совершенно надёжных систем в настоящее время не существует. Здесь также большую роль играет человеческий фактор, потому что любая ошибка системного администратора, неправильно настроившего маршрутизатор, может привести к весьма плачевным последствиям. Однако, несмотря на все это, на настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния [1,2].

В данной работе DDoS-атаки рассматриваются как дифференциальная игра двух игроков — хакера и администратора, первый из которых управляет трафиком τ, а второй — производительностью p компьютерной системы. Устанавливается наличие особого типа оптимального управления (τ^*, p^*), известного в теории игр под названием равновесие Нэша.

1. DDoS-атака как дифференциальная игра

В работе [3] DDoS-атаки описаны с помощью дифференциального уравнения

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

где:
$x(t)$ — число откликов в момент времени t компьютерной системы на внешние запросы, востребованные при обработке получаемых системой пакетов.
p — средняя скорости обработки входящих пакетов с учётом её падения или увеличения в зависимости от объёма занятых ресурсов: чем больше загружены ресурсы, тем меньше скорость обработки входящих пакетов. Другими словами, это производительность компьютерной системы, а p_0 — «типичная» характерная для данной системы величина производительности;
τ — величина входящего трафика; τ_0 – «типичная» характерная для системы «нормальная» величина трафика.

В уравнении (1) отражено требование, что увеличение трафика требует нарастания числа откликов на запросы.

Функционирующая компьютерная система способна справляться с ежедневным характерным трафиком τ_0 с определённым запасом надёжности системы. Один из способов DDOS-атаки состоит в том, чтобы добиться переполнения компьютерной системы с помощью такого большого количества пакетов, которое невозможно обработать. Очевидно, что при таком способе атаки наблюдается резкое возрастание входящего трафика. Увеличение трафика требует для его обработки увеличения свободных ресурсов системы.

Естественно поискать некоторое равновесие, которое может установиться при DDoS-атаках, если ресурсы хакера наращивать трафик не беспредельны, а компьютерная система имеет достаточно высокий уровень производительности.

Для отыскания такого равновесия (τ^*, p^*) воспользуемся теорией дифференциальных игр [2, 4], имея ввиду под равновесием равновесия Нэша.

2. Алгоритм нахождения равновесий Нэша

Естественно рассматривать игру с ненулевой суммой, поскольку выигрыши хакера и администратора слабо связаны.

Если игрок формирует «своё» управляющее воздействие в виде только функции времени $u(t)$ на всю продолжительность игры, то $u(t)$ — это *программное управление* игрока. Ранее мы называли его, используя термин «управление». Однако игрок может выбирать своё управление в зависимости от того, в каком положении x в момент времени t находится система. В таком случае игрок конструирует управляющее воздействие в виде функции $u(t, x)$, зависящей уже от позиции $\{t, x\}$, и для $u(t, x)$ используется термин *позиционное управление* игрока [5]. Часто пишут просто $u(x)$.

Мы будем искать позиционное управление, позиционное равновесие Нэша, когда хакер и администратор выбирают оптимально возможные доступные им управляющие параметры в каждой позиции $\{t, x\}$ в каждый момент времени.

Для дифференциальной игры N-игроков

$$\frac{dx}{dt} = f(x) + \sum_{j=1}^{N} g_j(x)u_j, \quad f(0) = 0,$$

$$x \in \mathbb{R}, \quad u_j \in \mathbb{R},$$

$$J_i(x, u_1, ..., u_N) = \int_0^{+\infty} [Q_i(x) + \sum_{j=1}^{N} R_{ij}(u_j)^2]dt, \quad (i = 1, ..., N),$$

$$Q_i > 0, \quad R_{ii} > 0, \quad R_{ij} \geqslant 0,$$

существование равновесий Нэша

$$J_i(u_1^*, u_2^*, u_i^*, ..., u_N^*) \leqslant J_i(u_1^*, u_2^*, ..., u_{i-1}^*, u_i, u_{i+1}^*..., u_N^*), \quad \forall u_i, \quad i \in N, \tag{2}$$

сводится к крайне сложной задаче отыскания положительно определённого решения $V_i(x) > 0$ нелинейного уравнения Гамильтона-Якоби

$$(V_i)'_x(x)f(x) + Q_i(x) - \frac{1}{2}(V_i)'_x \sum_{j=1}^{N} [g_j(x)]^2 (R_{jj})^{-1} (V_j)'_x +$$

$$+ \frac{1}{4} \sum_{j=1}^{N} R_{ij}[g_j(x)]^2 (R_{jj})^{-1} [(V_j)'_x]^2 = 0, \tag{3}$$

по которому строится равновесие Нэша [4, Theorem 10.4-2]:

$$u_i^*(x) = u_i(V_i(x)) = -\frac{1}{2} R_{ii} g_i(x) (V_i)'_x, \quad i \in N. \tag{4}$$

Равновесие Нэша в данном случае означает, что если каждый игрок пытается в одностороннем порядке изменить свою стратегию управления, в то время как политика остальных игроков остаётся неизменной, то он имеет худший результат (больший проигрыш).

В нашем случае $N = 2$, игрок 1 — это администратор, игрок 2 — это хакер и

$$f(x) = -x^3, \quad g_1(x) = x, \quad g_2(x) = 1,$$

и при $R_{11} = R_{22} = 1, R_{12} = R_{21} = 0$ уравнения Гамильтона-Якоби имеют вид:

$$\begin{aligned} Q_1 + (V_1)'_x f(x) - \frac{1}{4}[g_1(x)]^2 [(V_1)'_x]^2 - \frac{1}{2}[g_2(x)]^2 (V_1)'_x (V_2)'_x = 0, \\ Q_2 + (V_2)'_x f(x) - \frac{1}{4}[g_2(x)]^2 [(V_2)'_x]^2 - \frac{1}{2}[g_1(x)]^2 (V_1)'_x (V_2)'_x = 0. \end{aligned} \tag{5}$$

Полагая, что

$$V_1(x) = V_2(x) = \frac{1}{2}x^2,$$

получаем уравнения Гамильтона-Якоби в виде

$$\begin{aligned} Q_1 - x^4 - \frac{1}{4}x^4 - \frac{1}{2}x^2 = 0, \\ Q_2 - x^4 - \frac{1}{4}x^2 - \frac{1}{2}x^4 = 0. \end{aligned} \tag{6}$$

Следовательно,

$$\begin{aligned} Q_1 = \frac{5}{4}x^4 + \frac{1}{2}x^2 > 0, \\ Q_2 = \frac{3}{2}x^4 + \frac{1}{4}x^2 > 0. \end{aligned} \tag{7}$$

(Эти функции положительно определённые). Поэтому по теореме 10.4-2 из [4] имеем равновесие Нэша

$$p^* = p_0 - \frac{1}{2}x^2, \qquad \tau^* = \tau_0 - \frac{1}{2}x, \tag{8}$$

найденное по формулам (4). Выигрышные/проигрышные функции приобретают следующий вид:

$$\begin{aligned} J_1(x,p,\tau) = \int\limits_0^{+\infty} [Q_1(x) + (p-p_0)^2]dt, \\ J_2(x,p,\tau) = \int\limits_0^{+\infty} [Q_2(x) + (\tau-\tau_0)^2]dt. \end{aligned} \tag{9}$$

Если подставить (8) в (1) и проинтегрировать получаемое дифференциальное уравнение, то найдём оптимальное число откликов в момент времени t компьютерной системы на внешние запросы, востребованные при обработке получаемых системой пакетов:

$$x^2 = \frac{1}{Ce^t - 3},$$

где C — константа интегрирования.

3. Заключение

Мы показали, что между хакером и администратором возможно установление равновесия Нэша, идеология которого состоит в том, что каждая сторона считается с другой. Конечно, трудно надеяться, что хакер придерживается столь гуманной психологии, но учитывать, что его атаки, если они длительны или в значительной мере разрушительны, способствуют успешному проведению ответных мер со стороны жертвы, ему приходится.

Проведение дифференциальных игр и вычисление равновесий полезно с точки зрения определения степени надёжности компьютерной системы. Равновесия устанавливаются, если система способна сопротивляться. Если равновесий много, то в распоряжении администратора оказывается спектр порогов сопротивления, состоящих из пар (τ^*, p^*), дающих критические значения трафика и соответствующих значений производительности системы.

Литература

1. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: Учебное пособие. Омск : Изд-во ОмГУ, 2013. 160 с.
2. Гуц А.К., Володченкова Л.А. Дифференциальные игры в экологии человека и в социологии // Математические структуры и моделирование. 2016. № 3(39). С. 109–117.
3. Гуц А.К., Лавров Д.Н. Описание DDoS-атаки с помощью катастрофы «сборка» // Математические структуры и моделирование. 2013. № 1(27). С. 42–45.
4. Lewis F.L., Vrabie D.L., Syrmos V.L. Optimal Control. John Wiley & Sons, Inc., 2012. URL: `http://www.uta.edu/utari/acs/FL\%20talks/CDC\%20Orlando\%202011-\%20online\%20synch\%20PI.pdf`
5. Тынянский Н.Т., Жуковский В.И. Дифференциальные игры с ненулевой суммой (кооперативный вариант) // Итоги науки и техн. Сер. Мат. анал. 1979. Т. 17. С. 3—112.

DDOS-ATTACKS AS A DIFFERENTIAL GAME

T.V. Vahniy
Candidate of Mathematics, docent, e-mail: vahniytv@mail.ru
A.K. Guts
Doctor of Mathematics, Professor, e-mail: guts@omsu.ru

Dostoevsky Omsk State University

Abstract. Method of finding of the most optimal strategies for computer protection from DDoS-attacks is given based on differential game theory.

Keywords: DDoS-attacks, protection of computer system, differential game, Nash's blalance.