Министерство образования Республики Беларусь
Учреждение образования «Витебский государственный
университет имени П.М. Машерова»

Н А У К А – ОБРАЗОВАНИЮ, ПРОИЗВОДСТВУ, ЭКОНОМИКЕ

Материалы 73-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов

Витебск, 11 марта 2021 г.

Витебск
ВГУ имени П.М. Машерова
2021

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ СИСТЕМАМИ, ПОДВЕРГАЮЩИМИСЯ DDoS-АТАКАМ

А.К. Гуц[1], М.Н. Подоксёнов[2]
[1]Омск, ОмГУ им. Ф.М. Достоевского
[2]Витебск, ВГУ имени П.М. Машерова

DDoS-атака (от англ. Distributed Denial of Service) – это хакерская атака на сервер типа «отказ в обслуживании». При ее исполнении создается ситуация, при которых пользователи не смогут получить доступ к сайту или веб-сервису из-за его перегрузки. Для обслуживания запросов у сервера не хватает необходимой производительности. В результате атаки владельцы проектов, размещенных на сервере, несут серьёзные убытки.

Материал и методы. Рассматриваются равновесные ситуации, в которых могут пребывать компьютерные системы, подвергаемые DDoS-атакам. Используются методы теории оптимального управления и теории дифференциальных игр.

Результаты и их обсуждение. Мы обращаем внимание на то, что DDoS-атак совершаются *на четырех уровнях* OSI [1].

«Прежде всего возможны «низкоуровневые атаки»:

1. Атаки на сетевом уровне OSI представляют из себя «забивание» канала. Примером может быть CMP-флуд – атака, которая использует ICMP-сообщения, которые снижают пропускную способность атакуемой сети и перегружают брандмауэр. Хост постоянно «пингуется» нарушителями, вынуждая его отвечать на ping-запросы. Когда их приходит значительное количество, пропускной способности сети не хватает и ответы на запросы приходят со значительной задержкой. Для предотвращения таких DDoS-атак можно отключить обработку ICMP-запросов посредством Firewall или ограничить их количество, пропускаемое на сервер.

2. Атаки транспортного уровня выглядят как нарушение функционирования и перехват трафика. Например, SYN-флуд или Smurf-атака (атака ICMP-запросами с изменёнными адресами). Последствия такой DDoS-атаки – превышение количества доступных подключений и перебои в работе сетевого оборудования.

А также имеем высокоуровневые атаки:

3. На сеансовом уровне атакам подвергается сетевое оборудование. Используя уязвимости программного обеспечения Telnet-сервера на свитче, злоумышленники могут заблокировать возможность управления свитчем для администратора. Чтоб избежать подобных видов атак, рекомендуется поддерживать прошивки оборудования в актуальном состоянии.

4. Высокоуровневые **атаки прикладного уровня** ориентированы на стирание памяти или информации с диска, «воровство» ресурсов у сервера, извлечение и использование данных из БД. Это может привести к тотальной нехватке ресурсов для выполнения простейших операций на оборудовании. Наиболее эффективный способ предупреждения атак – своевременный мониторинг состояния системы и программного обеспечения» [1].

С учетом сказанного о каналах OSI, подвергаемых DDoS-атаках, и принципа построения модели работы компьютера в непрерывном времени [2], рассмотрим следующую модель компьютерной системы, подвергаемой DDoS-атакам, в виде дифференциального уравнения

$$\frac{dx}{dt} = [(p - p_o) - x^4(t)]x(t) + (\tau - \tau_o) \quad (1)$$

где $x(t)$ – число откликов на запросы в момент времени t, с управляющими факторами (τ, p), где τ – трафик и p – производительность сервера, p_o и τ_o – «типичные» характерные для данного сервера величины.

Для анализа управления компьютерной системой, подвергнутой DDos-атаке, используем теорию дифференциальных игр [4]. Мы посмотрим на управляющие факторы (τ, p), как на двух игроков, один их которых злоумышленник (управляет трафиком), а второй – системный администратор (управляет производительностью системы).

Игроки пытаются оптимизировать свой выигрыш, меняя стратегии управления. Очевидно, в практике работы системных администраторов может реализоваться некоторое равновесие, которое возникает в том случае, когда один игрок каким-то образом соотносит

свои действия, свою стратегию управления с действиями другого игрока. В теории игр одним из самых известных равновесий является *равновесие Нэша*.

Наша задача: уставить наличие равновесий Нэша в случае игры с ненулевой суммой. Рассматривать игру с ненулевой суммой вполне разумно, поскольку «выигрыши» наших игроков слабо связаны.

Если игрок формирует «свое» управляющее действие в виде только функция времени $u(t)$ на протяжении всей игры, то $u(t)$ – это программное управление игрока. Однако игрок может выбрать свое собственное управление в зависимости от положения x системы в момент времени t. В этом случае игрок конструирует управляющее действие в виде функции $u(t, x)$, которая уже зависит от позиции x. Поэтому для $u(t, x)$ используется термин *позиционное управление.* Часто пишут просто $u(x)$.

Будем искать позиционное управление или позиционное равновесие по Нэшу, применяя теорию, изложенную в [3].

Вводя для (1) обозначения

$$f(x) = -x^5,\ g_1(x) = -x^5,\ g_2(x) = 1\ ,\ u_1 = p - p_o,\ u_2 = \tau - \tau_o,$$

и полагая

$$V_1(x) = V_2(x) = \frac{1}{2}x^2,\ Q_1(x) = x^6 + \frac{1}{4}x^4 + \frac{1}{2}x^2 > 0\ ,\ Q_2(x) = x^6 + \frac{1}{4}x^2 + \frac{1}{2}x^4 > 0\ ,$$

мы легко убеждаемся, что справедливы уравнения Гамильтона-Якоби:

$$Q_1 + V_1' f(x) - \frac{1}{4}[g_1(x)]^2[V_1']^2 - \frac{1}{2}[g_2(x)]^2 V_1' V_2' = 0\ ,$$

$$Q_2 + V_2' f(x) - \frac{1}{4}[g_2(x)]^2[V_2']^2 - \frac{1}{2}[g_1(x)]^2 V_1' V_2' = 0\ ,$$

и выполнены условия теоремы 10.4-2 из [3].

Тем самым гарантируется существование равновесного управления Нэша:

$$J_1(u_1^*, u_2^*) \le J_1(u_1, u_1^*),$$
$$J_2(u_1^*, u_2^*) \le J_2(u_1^*, u_2)$$

для любых u_1, u_2, задаваемого формулами

$$u_1^* = p^* = p_o - \frac{1}{2}x^2,\ u_2^* = \tau^* = \tau_o - \frac{1}{2}x$$

с выигрышными функциями

$$J_i(x, p, \tau) = \int_0^{+\infty} [Q_i + u_i]dt,\ i = 1, 2.$$

Заключение. В данной работе мы нашли стратегию управления, которая гарантирует наличие равновесного состояния, в котором могут пребывать компьютерные системы, подвергаемые DDoS-атакам.

1. DDoS-атаки: виды атак и уровни модели OSI [Электронный ресурс]. URL: https://www.reg.ru/support/hosting-i-servery/bezopasnost-hostinga/ddos-ataki-vidy-atak-i-urovney-modeli-OSI [Дата обращения 15.11.2020].

2. Гуц, А.К. Описание DDoS-атаки с помощью катастрофы «сборка» / Гуц А.К., Лавров Д.Н. // Математические структуры и моделирование. –2013. - Вып.27. - С.42-45.

3. Lewis, F. Optimal Control / LewisF., VrabieD.,Syrmos V.– New Jersey: JohnWiley & Sons, Inc., 2012.–540 p.

МАШИННОЕ ЗРЕНИЕ В КОНЦЕПЦИИ ИНТЕРНЕТА ВЕЩЕЙ

Д.А. Довгулевич
Витебск, ВГУ имени П.М. Машерова

В современном мире, благодаря развитию технологий появилась концепция, суть которой объединения различных бытовых и промышленных устройств в единую сеть для взаимодействия между собой и внешним миром. Эта концепция получила название Интернет Вещей (Internet of Things) или сокращенно IoT.

По мимо непосредственно межмашинному взаимодействию, основным вопросом стоит взаимодействие устройств и окружающего мира. По аналогии с человеком, для этого им необ-