МОДЕЛИРОВАНИЕ DDOS-АТАКИ В СРЕДЕ NETLOGO

И.В. Ковалева
Р.И. Баженов, к.п.н., доцент
Приамурский государственный университет имени Шолом-Алейхема, г. Биробиджан, ЕАО
irinakovaleva97@mail.ru

Во времена информационных технологий более популярными становятся распределенные атаки на глобальные компьютерные сети. Большая часть таких атак направлена на нарушение доступности или «Распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS) и выведение из строя сервера путем наполнения системы большим количеством сетевых пакетов. Реализация таких атак может привести не только к выходу из строя отдельных хостов, но и остановить работу корневых DNS-серверов и вызвать частичное или полное прекращение работы Интернета [1].

DDoS-атака выполняется одновременно с большого числа компьютеров. Коммерческие и информационные сайты чаще становятся жертвами таких атак.

Например, в Альфа-банке был совершен факт хакерской атаки. Но атака была достаточно слабая и краткосрочная и не повлияла на работу бизнес-систем банка. Последняя серия DDoS-атак произошла в октябре 2015 года, когда были атакованы восемь крупных российских банков. Всего с октября 2015 года по март 2016 года Центробанк зафиксировал 21 кибератаку на платежные системы российских финансовых организаций. Мошенники пытались похитить со счетов достаточную сумму миллиардов рублей, но ЦБ и банкам удалось предотвратить хищения на 56% [2].

В 2014 году в результате масштабной DDoS-атаки были выведены из строя сразу несколько популярных, таких как PlayStation, Network, Xbox Live. Позже после удара атаки компания Sony сообщила и успокоила пользователей тем, что все данные остались целыми и невредимыми [3].

Для того чтобы исследовать поведение таких атак, была создана модель DDoS-атаки. Модель реализована в среде мультиагентного моделирования NetLogo. Среда программирования NetLogo предназначена для моделирования ситуаций и феноменов, которые происходят в природе и обществе. В данной программе можно давать указания и управлять тысячами независимых «агентов» действующих параллельно. NetLogo отлично подходит для проведения исследовательских работ, а библиотека моделей программы содержит множество моделей по математике, биологии, химии и других наук. Программа открывает возможность для понимания и объяснения связей между поведением отдельных индивидуумов, природными явлениями и т.д. [4, 5].

В библиотеке примеров программы находится модель популяции волков и овец. С помощью данной модели можно исследовать популяцию животных. Волки пытаются съесть овец, а овцы могут перемещаться и отбиваться от волков [6, 7].

В библиотеке моделей находится модель «Rabbits grass weeds», в которой показана популяция зайцев, которые питаются травой и сорняками. С помощью данной модели существует возможность исследовать поведение сервера и поведение атаки, которая пытается пробить данный сервер. Также можно посмотреть через какое время сервер будет выведен из строя.

В качестве сервера берется трава, а в качестве атаки – заяц. Тем самым заяц двигается по полю и ест траву до тех пор, пока вся трава не исчезнет. Так же как атака пробивает сервер до тех пор, пока сервер не будет выведен из строя.

На рисунке 1 показан интерфейс программы, на котором изображены кнопки запуска и обновления модели, рычаги изменения параметров агентов, поле графика, изображающее изменения модели во время запуска и также на поле интерфейса находится окно, где показана сама модель. В окне модели присутствует трава, которая заполняет все пространство и один заяц, являющийся атакой.

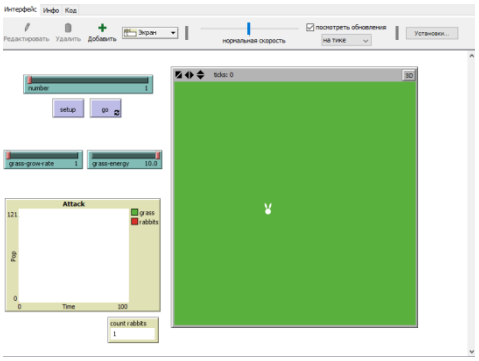

Рис. 1. Интерфейс модели Ddos-атаки.

После запуска модели заяц начинает двигаться по полю и есть траву. Клетка, на которой травы нет, становится черной и трава на ней уже не растет (рис. 2).

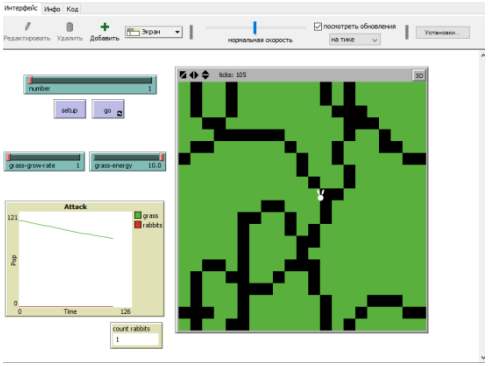

Рис. 2. Интерфейс модели после запуска.

Было проведено исследование и в ходе было определено, за сколько тиков атака выведет сервер из строя. В NetLogo существует свой встроенный счетчик тиков. С каждым разом первоначальное количество атак становится больше. После запуска модели в графике можно увидеть то, как линия сервера падает. В коде изначально прописаны энергия сервера и энергия атаки. Сервер будет выведен из строя тогда, когда на поле не останется ни одной зеленой клетки. В таблице представлены результаты исследования при разном количестве атак (см. таблица 1).

Таблица 1. Данные исследования

№	Первоначальное количество атак	Количество тиков
1.	1	2739
2.	5	582
3.	10	307

Таким образом, можно сделать вывод, чем выше количество первоначальных атак, тем меньше времени занимает выведение сервера из строя.

Дополнительно в коде можно прописать небольшую защиту для сервера. Тем самым увеличится количество тиков и для того, чтобы вывести сервер из строя.

Исходя из данного исследования, можно сказать, что если добавить серверу дополнительную защиту, то количество тиков немного увеличивается. Тем самым, сервер сможет продержаться дольше, нежели как в предыдущем исследовании, когда у сервера отсутствовала защита.

Таблица 2. Данные исследования с защитой для сервера

№	Первоначальное количество атак	Количество тиков
1.	1	3456
2.	5	789
3.	10	346

В ходе проведенного исследования была разработана простая модель DDoS-атаки, которая реализована в мультиагентной среде NetLogo. Данную систему можно использовать в курсах «Интеллектуальные системы и технологии» и «Защита информации».

Список использованных источников

1. NetLogo: И взрослым, и детям tu URL: https://habrahabr.ru/post/220589/ (дата обращения: 15.04.2017).
2. Хакеры провели DDoS-атаку на Сбербанк и Альфа-банк URL: http://www.rbc.ru/economics/09/11/2016/582372be9a79476357a4a62d (дата обращения: 14.04.2017).
3. Синхронная атака вывела из строя PlayStation Network, Xbox Live и Battle.net URL: https://tjournal.ru/p/hackers-psn-xbl-outage (дата обращения: 14.09.2017).
4. Мезенцев К.Н. Мультиагентное моделирование в среде netlogo/ К.Н. Мезенцев / Автоматизация и управление в технических системах. - 2015.- № 1 (13).- С. 10-20.
5. Векслер В.А. Агентное моделирование в среде netlogo на уроках информатики / В.А. Векслер / NovaInfo.Ru.- 2016.- Т. 3.- № 44.- С. 314-326.
6. Векслер, В.А. Моделирование экологических систем в среде netlogo на уроках информатики в средней школе / В.А. Векслер // NovaInfo.Ru.- 2017.- Т. 3.- № 62.- С. 327-335
7. NetLogo. URL: http://letopisi.org/index.php/NetLogo (дата обращения: 14.09.2017).