УДК 543.42:004.056

АНАЛИТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА РЕАЛИЗАЦИИ DDoS-АТАКИ ТИПА HTTP-flood

Г.А. Остапенко, М.В. Бурса, Е.Ф. Иванкин

В работе на основе использования аппарата теории сетей Петри-Маркова производится моделирование процесса реализации DDoS-атаки типа HTTP-flood, в результате которого получена зависимость вероятности реализации атаки от времени

Ключевые слова: DDoS-атака типа HTTP-flood, сети Петри-Маркова

Среди всего множества сетевых атак DDoS-атаки занимают немаловажное место, при помощи них пали крупнейшие и известнейшие компании такие, как Yahoo!, eBay, Amazon.com, CNN.com и целый ряд менее известных. Последствием таких атак является невозможность соединения пользователя с сервером, а следовательно, и невозможность получения пользователем необходимой ему информации. Особенностью DDoS-атак является то, что атаке подвергаются очень мощные сервера. Злоумышленник посредством метода грубой силы тем или иным способом, зачастую с помощью крупной сети, находящейся под его контролем, пытается «забить» канал атакуемого сервера [1-4].

Наиболее распространенной DDoS-атакой является атака типа HTTP-flood. В ее основе лежит отправка HTTP-запросов GET. Данная flood-атака также может быть направлена на уязвимые места сервера, занятые выполнением ресурсоемких задач. В результате, как и при DDoS-атаках другого типа, сервер становится неспособным к обработке запросов, т.к. не успевает обрабатывать запросы, посредством которых его атакуют.

Смоделируем [1-2] данную атаку с помощью сети Петри-Маркова. Граф данной сети для данной атаки представлен на рис. 1.

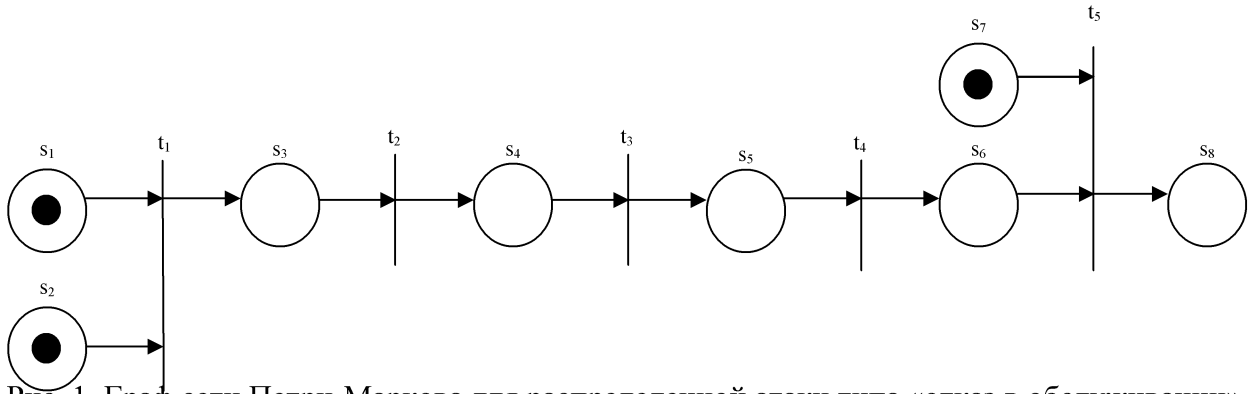

Рис. 1. Граф сети Петри-Маркова для распределенной атаки типа «отказ в обслуживании»

Остапенко Григорий Александрович – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru
Бурса Максим Васильевич – ВГТУ, аспирант, e-mail: tavduk@gmail.com
Иванкин Евгений Филиппович – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru

Обозначения элементов этой сети приведены ниже, s_i – позиции, t_i – переходы:

s_1 – атакующий A готов;

s_2 – R (атакуемый ресурс) готов;

t_1 – A сканирует сеть для поиска управляющих хостов;

s_3 – хосты-зомби найдены;

t_2 – A отправляет хостам вредоносное ПО и управляющие запросы;

s_4 – захваченные хосты становятся управляющими хостами;

t_3 – управляющие хосты сканируют сеть для поиска хостов, которые будут осуществлять атаку;

s_5 – хосты, которые будут осуществлять атаку, найдены;

t_4 – A посредством управляющих хостов направляет вредоносное ПО и управляющие запросы найденным хостам;

s_6 – вновь захваченные хосты становятся атакующими хостами;

s_7 – L (легитимный пользователь) готов;

t_5 – атакующие хосты начинают по команде A отправлять запросы R, ресурсы R начинают истощаться, легитимный пользователь получает сбои в подключении к атакуемому ресурсу R;

s_8 – результат – ресурсы R истощены, ресурс недоступен, пользователь не может получить необходимую информацию.

Так как в данной сети достаточно рассмотреть процесс перехода из начального состояния s_1 в конечный переход t_6, то элементы матрицы, определяющие логические функции срабатывания сети, без учета направленности дуг графа, могут быть записаны следующим образом:

$$v_{s_1 t_5} =$$

	t_1	t_2	t_3	t_4	t_5
s_1	1	0	0	0	0
s_2	1	0	0	0	0
s_3	$s_1t_1 \cup s_2t_1$	1	0	0	0
s_4	0	1	1	0	0
s_5	0	0	1	1	0
s_6	0	0	0	1	1
s_7	0	0	0	0	1
s_8	0	0	0	0	$s_6t_5 \cap s_6t_5$

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений:

$$\Phi_{s_1t_1}(t) = \pi_{11} \int_0^t f_{s_1t_1}(\tau)d\tau,$$

$$\Phi_{s_2t_1}(t) = \pi_{21} \int_0^t f_{s_2t_1}(\tau)d\tau,$$

$$\Phi_1(t) = \int_0^t f_{s_1t_1}(\tau)\left(1 - \Phi_{s_2t_1}(\tau)\right) + f_{s_2t_1}(\tau)\left(1 - \Phi_{s_1t_1}(\tau)\right)d\tau,$$

$$\Phi_{s_3t_2}(t) = \pi_{32} \int_0^t f_{s_3t_2}(\tau)\Phi_1(t-\tau)d\tau,$$

$$\Phi_{s_4t_3}(t) = \pi_{43} \int_0^t f_{s_4t_3}(\tau)\Phi_{s_3t_2}(t-\tau)d\tau,$$

$$\Phi_{s_5t_4}(t) = \pi_{54} \int_0^t f_{s_5t_4}(\tau)\Phi_{s_4t_3}(t-\tau)d\tau,$$

$$\Phi_{s_5t_4}(t) = \pi_{54} \int_0^t f_{s_5t_4}(\tau)\Phi_{s_4t_3}(t-\tau)d\tau,$$

$$\Phi_{s_6t_5}(t) = \pi_{65} \int_0^t f_{s_6t_5}(\tau)\Phi_{s_5t_4}(t-\tau)d\tau,$$

$$\Phi_{s_7t_5}(t) = \pi_{75} \int_0^t f_{s_7t_5}(\tau)d\tau,$$

$$\Phi_2(t) = \int_0^t f_{s_6t_5}(\tau)\left(1-\Phi_{s_7t_5}(\tau)\right) + f_{s_7t_5}(\tau)\left(1-\Phi_{s_6t_5}(\tau)\right)d\tau.$$

Полагаем, что плотности распределения вероятностей являются гамма-зависимостями и имеют вид:

$$f_{s_it_j} = t^{k_{ij}-1}\frac{e^{-\frac{t}{\theta_{ij}}}}{\Gamma(k_{ij})\theta_{ij}^{k_{ij}}}.$$

Так как расчет посредством применения прямого и обратного преобразования Лапласа является весьма громоздким, имеет смысл применить пуассоновское приближение для плотностей распределения вероятностей времени перемещения в переходы сети Петри-Маркова. В результате будет получено среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения:

$$\tau_1 = \frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}},$$

$$\tau_{65} = \frac{nT}{k},$$

$$\tau_2 = \tau_1 + \tau_{32} + \tau_{43} + \tau_{54} + \tau_{65},$$

$$\tau = \frac{\tau_2^2 + \tau_2\tau_{75} + \tau_{75}^2}{\tau_2 + \tau_{75}},$$

$$\tau = \frac{\left(\frac{\tau_{11}^2 + \tau_{11}\tau_{12} + \tau_{12}^2}{\tau_{11} + \tau_{12}} + \tau_{32} + \tau_{43} + \tau_{54} + \tau_{65}\right)^2 + \left(\frac{\tau_{11}^2 + \tau_{11}\tau_{12} + \tau_{12}^2}{\tau_{11} + \tau_{12}} + \tau_{32} + \tau_{43} + \tau_{54} + \tau_{65}\right)\tau_{75} + \tau_{75}^2}{\frac{\tau_{11}^2 + \tau_{11}\tau_{12} + \tau_{12}^2}{\tau_{11} + \tau_{12}} + \tau_{32} + \tau_{43} + \tau_{54} + \tau_{65} + \tau_{75}}.$$

$$P(t) = 1 - e^{-\frac{1}{\tau}t}.$$

Описание временных характеристик распределенной атаки типа «отказ в обслуживании» зависит от конфигурации системы и сети. Среднее время запуска и настройки программы-сканера сети $\tau_{11} = \tau_{43} = 10{,}5$ с. Среднее время пересылки и обработки пакетов $\tau_{32} = \tau_{54} = 0{,}1$ с. Среднее время приведения атакуемого ресурса в состояние недоступности равно среднему времени отправления подготовки и отправки одного пакета, т.е. $\tau_{65} = 0{,}01$, так как для реализации атаки посредством атакующих хостов необходимо одновременно отправить как минимум максимальное количество запросов, которые заполнят сетевой канал атакуемого ресурса.

Без применения мер защиты от данной атаки время перехода атакуемого ресурса в недоступное состояние стремится к нулю, тогда среднее время перехода по всей сети $\tau = 21{,}3$ с. Зависимость вероятности реализации атаки от времени представлена на рис. 2.

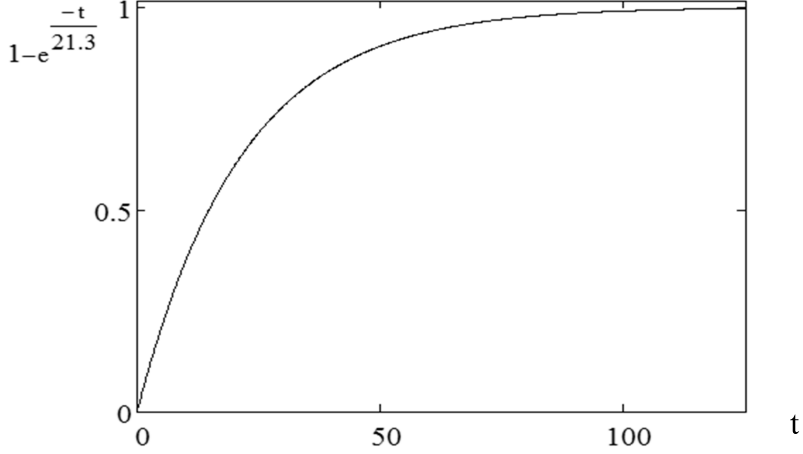

Рис. 2. Зависимость вероятности реализации DDoS-атаки типа HTTP-flood от времени

Таким образом, полученные данные демонстрируют, что среднее время реализации распределенной атаки типа «отказ в обслуживании» занимает незначительное время. Следовательно, для уменьшения опасности реализации атак данного типа необходимо использовать программные средства контроля входящего потока информации и средства защиты от DDoS-атак.

Литература

1. Игнатьев В.М., Ларкин Е.В. Сети Петри-Маркова. – Тула: Тул. Гос. ун-т, 1997, -163 с.

2. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М.: РадиоСофт, 2010, -230 с.

3. Бурковский В.Л., Дорофеев А.Н. Организация управления глобальными транзакциями в гетерогенной информационной среде // Системы управления и информационные технологии. 2004. №1(13). С. 92-98.

4. Шмельков Е.А., Юрасов В.Г., Попова Л.Г. Исследование возможности прогнозирования загруженности портала с целью повышения информационной безопасности и доступности портала // Информация и безопасность. 2012. Т. 15. №2. С. 285 – 286.

Воронежский государственный технический университет
Voronezh state technical university

ANALYTICAL MODELLING OF IMPLEMENTATION PROCESS OF DDoS-ATTACK SUCH AS HTTP-flood

G.A. Ostapenko, M.V. Bursa, E.F. Ivankin

In this paper is simulating the process of implementation of DDoS-attack such as HTTP-flood which resulted in the dependence of the probability of an attack on the time

Key words: DDoS-attack such as HTTP-flood, Petri nets and Markov chains