УДК 004.75: 004.492.3

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ РАСПРЕДЕЛЁННЫХ СЕТЕВЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

Е. В. Щерба, Д. А. Волков

Предложена методика, разработана архитектура и построена реализация системы обнаружения сетевых атак типа «отказ в обслуживании». Методика основана на моделировании исследуемой сети сетями массового обслуживания с последующей оценкой вероятности потерь заявок в сети.

Ключевые слова: *обнаружение сетевых атак, отказ в обслуживании.*

Традиционные механизмы обеспечения безопасности — межсетевые экраны и сигнатурные системы обнаружения вторжений — не являются эффективными средствами для обнаружения низкоактивных сетевых атак типа «отказ в обслуживании» (DDoS-атак) прикладного уровня и защиты от них [1].

Фундаментальной предпосылкой для обнаружения атак является построение контрольных характеристик трафика при работе сети в штатных условиях с последующим поиском аномалий в структуре трафика (отклонения от контрольных характеристик). Для обнаружения аномалий могут применяться статистические критерии (среднеквадратичное отклонение, хи-квадрат, отклонение от стандартного нормального распределения, значительное увеличение энтропии и т. д.), кластеризация, метод обнаружения точки перехода, спектральный анализ и др. [2 – 4]. Каждый из указанных методов имеет определённые достоинства и недостатки и не является универсальным для обнаружения всех типов сетевых атак. Достаточно часто для расчёта параметров потоков данных в вычислительных сетях применяют математические модели в виде сетей массового обслуживания (СеМО). В данной работе для обнаружения DDoS-атак предложен метод оценки вероятности потери произвольной заявки при её прохождении по СеМО. Поскольку атаки прикладного уровня на различные сетевые службы происходят независимо, в рамках каждой службы для моделирования узлов можно использовать одноканальную систему массового обслуживания с очередью длины m.

Рассматривая отдельный узел СеМО, можно предположить, что вся сеть в целом и выбранный узел в частности функционируют в стационарном режиме. Извне поступает пуассоновский поток заявок с параметром λ. Узел содержит одно устройство обслуживания заявок, для которого задана интенсивность μ их обработки. После обработки заявка покидает узел. Если во время поступления заявки обслуживающее устройство занято обработкой другой заявки, то входящая заявка становится в очередь. Если заявка поступает и очередь полностью заполнена, заявка теряется.

Пусть для узлов сети задан вектор интенсивностей входящих потоков заявок извне $\overrightarrow{\lambda}$, вектор интенсивностей обработки заявок $\overrightarrow{\mu}$ и субстохастическая матрица вероятностей переходов заявок P. В работе [5] предложена итерационная процедура расчёта вектора интенсивностей $\overrightarrow{\rho}$ входящих в узлы исходной сети потоков (суммарных потоков извне и из других узлов) и скорректированной субстохастической матрицы вероятностей переходов заявок $\widetilde{P}$. Исходя из потребности оценки вероятности потерь заявок в сети, предложена методика построения цепи Маркова с дискретным временем, соответствующей пути произвольной заявки по узлам. Для этого вводятся расщеплённые состояния этой цепи, т. е. состоянием называется упорядоченная пара чисел (i, d), где i соответствует номеру узла, в котором находится заявка (меняется в пределах от 1 до J), а d — количеству занятых мест в очереди узла (меняется

в пределах от 1 до $m_i + 1$). Состояние $(i, m_i + 1)$ соответствует переполненной очереди в узле i. Начальное распределение данной цепи $\widehat{p}$ можно рассчитать как

$$\widehat{p}\{(i,d)\} = \frac{\lambda_i}{\sum\limits_{j=1}^{J}\lambda_j}\frac{\frac{\rho_i^{d-1}}{\mu_i^{d-1}}\left(1-\frac{\rho_i}{\mu_i}\right)}{1-\frac{\rho_i^{m_i}}{\mu_i^{m_i}}}.$$

Кроме того, вводятся два дополнительных состояния (S) и (F). Первое соответствует успешной обработке заявки, а второе — потере заявки. Начальные вероятности этих состояний равны нулю. Далее определяется матрица вероятностей переходов $\widehat{P}$ заданной цепи Маркова, соответствующей пути произвольной заявки по узлам. Состояния (S) и (F) не сообщаются. Цепь, попав в одно из этих состояний, уже из него не выходит. Вероятность перехода из состояния (i, d) в состояние (j, w) можно рассчитать по формуле

$$p\{(i,d) \rightarrow j,w)\} = \widetilde{p_{ij}}\frac{\frac{\rho_j^{w-1}}{\mu_j^{w-1}}\left(1-\frac{\rho_j}{\mu_j}\right)}{1-\frac{\rho_j^{m_j}}{\mu_j^{m_j}}},$$

где $\widetilde{p_{ij}}$ — элементы скорректированной субстохастической матрицы вероятностей переходов заявок $\widetilde{P}$ (коррекция необходима, поскольку матрица P устаналивается для СеМО без потерь заявок). Вероятность успешной обработки заявки в узле равна

$$p\{(i,d) \rightarrow S)\} = \widetilde{p}_i^{\,*},$$

где $\widetilde{p}_i^{\,*}$ — вероятность успешной обработки заявки в узле i (после чего заявка покидает сеть); она вычисляется в ходе итерационной процедуры на основе матрицы P и $p_i^* = 1 - \sum\limits_{k=1}^{J} p_{ik}$. Если заявка находится в переполненной очереди, вероятность её потери (перехода цепи в состояние (F)) равна

$$p\{(i, m_i + 1) \rightarrow F)\} = 1.$$

Все остальные вероятности равны нулю.

Для оценки вероятности потери заявки при стационарном режиме работы сети необходимо рассчитать член вектора $\widehat{p}^{(k)}\{(F)\}$, соответствующий состоянию (F) на k-м шаге заданной цепи Маркова, где $\widehat{p}^{(k)} = \widehat{p} \cdot (\widehat{P})^k$.

Установка параметра k происходит с помощью дополнительной итерационной процедуры. По результатам расчёта вычисляется $\widehat{p}_N^{(k)}$ — вероятность того, что на k-м шаге заданной цепи Маркова заявка всё еще находится в сети, т. е. не потеряна и не обработана полностью:

$$\widehat{p}_N^{(k)} = 1 - \widehat{p}^{(k)}\{(F)\} - \widehat{p}^{(k)}\{(S)\}.$$

Если в результате вычислений $\widehat{p}_N^{(k)}$ превышает некоторую наперёд заданную точность, то k увеличивается и расчёт повторяется до тех пор, пока не будет достигнута заданная точность указанной вероятности.

На основе представленной методики разработана архитектура и построена программная реализация системы обнаружения DDoS-атак (рис. 1). Разработанная методика позволяет получать адекватную оценку частоты потери заявок в сети в случае,

если СеМО находится в стационарном режиме. При возникновении DDoS-атаки узлы СеМО выходят из стационарного режима на некоторое время, после чего устанавливается стационарный режим с другими параметрами. На время перехода между режимами методика неприменима. Так как время перехода между режимами зависит от топологии сети и параметров узлов, оценка эффективности разработанной методики и её сравнительный анализ с другими подходами представляет отдельную задачу.

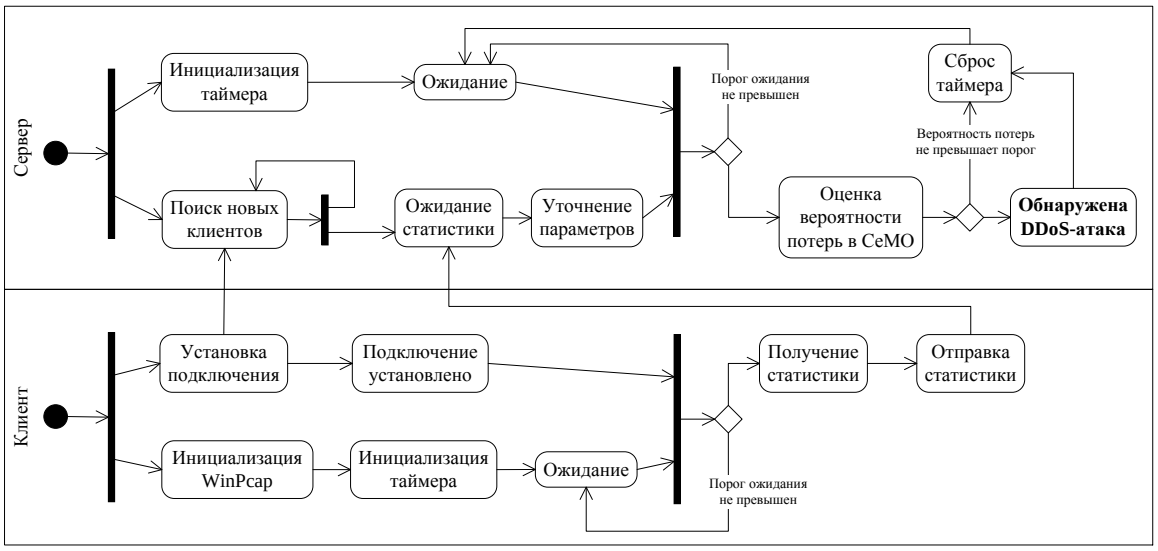

Рис. 1. UML-диаграмма деятельности системы обнаружения

ЛИТЕРАТУРА

1. `http://www.cisco.com/web/RU/netsol/ns480/whitepapers.html` — Предотвращение атак с распределенным отказом в обслуживании (DDoS). Дата обращения: 30.03.2013.
2. *Li Muh., Li Min., and Jiang X.* DDoS attacks detection model and its application // WSEAS Trans. Computers. 2008. V. 7. No. 8. P. 1159–1168.
3. *Wang H., Zhang D., and Shin K. G.* Detecting SYN flooding attacks // Proc. IEEE INFOCOM'2002. New York City, 2002. P. 1530–1539.
4. *Hussain A., Heidemann J., and Papadopoulos C.* A framework for classifying denial of service attacks // Proc. ACM SIGCOMM. Karlsruhe, Germany, 2003. P. 99–110.
5. *Щерба Е. В., Щерба М. В.* Разработка архитектуры системы обнаружения распределенных сетевых атак типа «отказ в обслуживании» // Омский научный вестник. Сер. Приборы, машины и технологии. 2012. № 3 (113). С. 280–283.