ПРИМЕНЕНИЕ G-СЕТЕЙ ПРИ МОДЕЛИРОВАНИИ ПОВЕДЕНИЯ ВИРУСОВ И КОМПЬЮТЕРНЫХ АТАК В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

В.В. Науменко
Кафедра стохастического анализа и эконометрического моделирования,
Гродненский государственный университет им. Я. Купалы
Гродно, Республика Беларусь
E-mail: victornn86@gmail.com

Объектом исследования являются открытая сеть массового обслуживания с положительными и отрицательными заявками (G-сеть). Исследования такой сети проводятся в нестационарном режиме с учетом сигналов, сигналов со случайной задержкой сигналов, а также с учетом изменения доходов в системах сети. Описывается применение таких сетей при моделировании поведения вирусов в информационно-телекоммуникационных системах и сетях, а также при атаках на компьютерные сети (DDoS-атаки).

Введение

Довольно часто в последнее время наблюдается бурное развитие информационно-телекоммуникационных систем и сетей (ИТСС). ИТСС становятся все более сложными, что обусловлено необходимостью повышения надежности передачи и обработки информации. Функционирование таких объектов связано с бесперебойной передачей и обработкой огромного числа информационных потоков. Поскольку вероятностная природа этих потоков приводит к появлению целого ряда проблем, которые возникают на этапе проектирования сетевых систем и при их эксплуатации, то это стимулирует математические исследования, направленные на разработку адекватных стохастических моделей. Построение и исследование этих моделей для оценки качества их функционирования является важной задачей. А анализ таких моделей необходим для получения количественных оценок показателей производительности сетевых систем. Мощный инструментарий для аналитического моделирования ИТСС создан на основе теории сетей массового обслуживания (МО).

I. Концепции отрицательных заявок

Применение классических моделей теории МО, которые учитывали бы как характерные особенности систем, так и возможное влияние различных дестабилизирующих факторов, как например, внезапные сбои, попадание вирусов, потеря передаваемых или обрабатываемых данных, не всегда дает адекватные результаты. Чтобы учесть подобные факторы предложена концепция G-сетей, в которых помимо потоков обычных заявок рассматриваются также дополнительные пуассоновские потоки отрицательных заявок [1; 2]. В таких сетях, когда в систему поступает отрицательная заявка (при этом сама не получает никакого обслуживания), она уничтожает одну положительную заявку, если таковая имеется в данной системе, тем самым уменьшая число положительных заявок в системе на единицу (эффект проникновения вируса в компьютерную сеть). Например, в компьютерных сетях “положительными” заявками являются задания (программы), а “отрицательными” заявками – компьютерные вирусы. При поступлении в компьютерную сеть вирус уничтожает или наносит вред, заражает одну из исполняемых программ, уменьшая количество действующих программ или запросов в системе на единицу. Это соответствует тому, что при поступлении в компьютерную сеть вирус уничтожает или наносит вред, заражает одну из исполняемых программ, уменьшая количество действующих программ или запросов в системе на единицу. Затем вирус исчезает из сети, не получая для себя никакого обслуживания. Исследование такой модели сети в переходном режиме проведено в [3; 4].

II. G-сеть с учетом сигналов

Воздействие внешней среды на процесс очереди положительных заявок может оказываться не только отрицательными заявками, которые просто уничтожают одну или более положительных заявок в данной системе МО (СМО), но и поступающими извне сигналами-триггерами, действие которых заключается в мгновенном перемещении положительной заявки из данной системы в некоторую другую систему сети [5]. Таким образом, триггер, в отличие от отрицательной заявки, не уничтожает положительную заявку, а лишь мгновенно перемещает ее с заданной вероятностью из данной системы в некоторую другую систему сети. G-сеть с триггерами в переходном режиме была изучена в работах [6].

Сети МО с сигналами (отрицательными заявками и/или триггерами) используются при аналитическом моделировании ИТСС, при этом отрицательные заявки могут возникать, например, при моделировании компьютерных вирусов,

а введение триггеров позволяет управлять нагрузкой в сети. G-сети также широко используются для моделирования нейронных сетей, при этом сигналы возбуждения моделируются положительными заявками, а сигналы торможения – отрицательными заявками.

III. Модель DDoS-атаки

G-сети с сигналами применяются при моделировании различного рода компьютерных вирусов, в зависимости от типа их функционирования, а также для управления нагрузкой в сети. Однако время активизации любого сигнала равнялось нулю и проявлялось мгновенно и поэтому не принималось в расчет при анализе таких сетей. Будем предполагать, что поступающий в систему обслуживания сети сигнал активизируется не сразу, а лишь по истечении случайного времени (некоторого тайм-аута) [7].

Отрицательные заявки и сигналы в рассматриваемой модели могут описывать вирусы в системе, которые начинают действовать через случайное время, при этом сигнал либо «исправляется» – становится положительной заявкой, либо «несет разрушение», т.е. став отрицательной заявкой, уничтожает положительную заявку в системе, либо «отражается» или «уничтожается» – не оказывает воздействия на систему. В таком случае под положительными заявками или просто заявками, будем подразумевать запросы с различных компьютеров. Под отрицательными заявками будем понимать данные или пакеты, которые система не ожидает (вирус-программы), что и приводит к ее остановке или к ее перезагрузке. Другими словами, такие запросы уничтожают другие заявки в системе.

Выбранные узлы сети подвергаются нападению, и злоумышленник получает на них права администратора. На каждый из захваченных узлов устанавливаются троянские программы, которые работают в фоновом режиме. Под сигналами в сети будем подразумевать такие программы, которые затем активируются через некоторое случайное время по команде злоумышленника. Они называются компьютерами-зомби, их пользователи даже не подозревают, что являются потенциальными участниками DDoS-атаки. Это означает, что в любой момент времени в этих узлах находится хотя бы один неактивизированный сигнал. Далее злоумышленник отправляет определенные команды захваченным компьютерам и те, в свою очередь осуществляют мощную DoS-атаку на целевой компьютер. Модель такой сети исследована в нестационарном режиме в [8].

IV. Прогнозирование изменения доходов

Компьютерные вирусы проникают в сеть вместе с файлами и из-за потери информации или ее искажения ИТСС несет некоторые расходы или убытки. После обслуживания положительная заявка переходит из одной СМО в другую, которая в свою очередь получает некоторый доход, а доход первой СМО уменьшается соответственно на эту величину. Отрицательные заявки и сигналы в рассматриваемой модели могут описывать вирусы в системе, которые начинают действовать через случайное время. При этом сигнал либо становится положительной заявкой (исправляется) и приносит доход системе после обслуживания в ней, либо несет разрушение, (став отрицательной заявкой, уничтожает положительную заявку в системе) и, соответственно, приносит убыток этой системе, либо отражается или уничтожается, не оказывая воздействия на систему, – в этом случае изменения дохода системы не происходит.

Учет этого можно осуществить, применив в качестве модели НМ-сеть с доходами, положительными и отрицательными заявками [9]. Также, если есть необходимость, в такую модель можно ввести триггеры (сигналы), учитывая или не учитывая при этом их случайную задержку [8]. Предложенная модель может быть применена при моделировании изменения доходов в ИТСС, к примеру, в компьютерной сети предприятия при DDoS-атаке на эту сеть, а также при проникновении вирусов [9].

1. Gelenbe, E. Product form queueing networks with negative and positive customers / E. Gelenbe // Journal of Applied Probability. – 1991. – Vol. 28. – P. 656–663.
2. Gelenbe, E. Stability of product-form G-networks / E. Gelenbe, R. Schassberger // Probability Statistics for Engineers Scientists. – 1992. – Vol. 6. – P. 271–276.
3. Науменко, В. В. Анализ сети с положительными и отрицательными заявками в переходном режиме / В. В. Науменко, М. А. Маталыцкий // Вестник ГрГУ. –Сер. 2 –2013. – № 3. – С. 135–142.
4. Matalytski, M. Nonstationary analysis of queueing network with positive and negative messages / M. Matalytski, V. Naumenko // Journal of Applied Mathematics and Computational Mechanics. –Vol. 2 – 2013. – № 12. – С. 61–71.
5. Gelenbe, E. G-networks with triggered customer movement / E. Gelenbe // Journal of Applied Probability. – 1993. – Vol. 30. – P. 742–748.
6. Matalytski, M. Investigation of G-network with signals at transient behavior / M. Matalytski, V. Naumenko // Journal of Applied Mathematics and Computational Mechanics. –Vol. 13 –2014. – № 1. – С. 75–86.
7. Бочаров, П. П. Сеть массового обслуживания с сигналами со случайной задержкой / П. П. Бочаров // Автоматика и телемеханика. – 2002. – № 9. – С. 90–101.
8. Маталыцкий, М. А. Анализ G-сети со случайной задержкой сигналов в переходном режиме и ее применение / М. А. Маталыцкий, В. В. Науменко // Вестник ГрГУ. –Сер. 2 –2014. – № 1. – С. 135–147.
9. Науменко, В. В. Анализ марковских сетей с доходами, положительными и отрицательными заявками / В. В. Науменко, М. А. Маталыцкий // Информатика. –2014. – № 1. – С. 5–14.