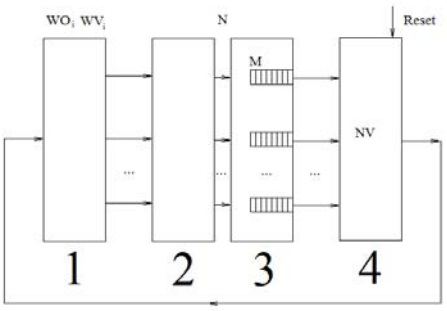
МОДЕЛИРОВАНИЕ СИТУАЦИИ ПИКОВОЙ НАГРУЗКИ В ИНФОРМАЦИОННОЙ СЕТИ

Н.Г. Булахов Аспирант
ТГУ, г. Томск, т.923-402-72-32, nboolahov@yandex.ru

Сегодня вирусные атаки являются одной из первостепенных угроз информационной безопасности. Такие действия наносят финансовый ущерб, а также позволяют реализовать многих других опасных угроз. И это – несмотря на то, что для борьбы с такими вредителями уже разработано много сигнатурных, статистических и эвристических методов. В их основе лежат модели функционирования сети, по которой передаётся зловредный трафик в различных ситуациях (например, эпидемиологическая модель и её модификации). Применение этих методов ограничивает приближённость описания функционирования сетей либо малое число релевантных параметров.

Поэтому актуальна разработка модели, устраняющей вышеперечисленные недостатки. Основу предлагаемой модели составляет устройство пересылки пакетных данных, имеющее *N* входов и *N* выходов (рис. 1). Входы и выходы не равноправны между собой, что позволяет отразить наличие в реальной сети магистральных каналов и присоединение оконечных станций. Для учёта различия между ними каждому каналу присваивается свой весовой коэффициент *W=WO+WV*, который показывает, насколько вероятнее появление пакета на данном входе, относительно всех остальных. Вес *WO* соответствует нагрузке канала за счёт полезных пакетов, вес *WV* за счёт саморазмножающихся пакетов. Входящие пакеты имеют адрес назначения, указывающий выходной порт. Каждый выходной порт рассчитан на очередь длиной *M* пакетов.



1 и 2 – блоки распределения пакетов на входе и по выходам, соответственно, 3 – блок очередей, 4 – блок обработки информации о выходных пакетах.

Рис. 1. Структура устройства пересылки пакетов с *N* входами и *N* выходами:

В заданный такт времени условие того, что на входе n есть пакет, определяется формулой

$$f(n)=\begin{cases}1, rnd \le \dfrac{WO_i + WV_i}{WO_{\max} + WV_{\max}},\\ 0, rnd > \dfrac{WO_i + WV_i}{WO_{\max} + WV_{\max}}.\end{cases} \quad (1)$$

Если на входе *n* имеется пакет, то условие того, что он – саморазмножающийся либо полезный, есть

$$f_1(n)=\begin{cases}1, rnd \le \dfrac{WV_i}{WO_i + WV_i},\\ 2, rnd > \dfrac{WV_i}{WO_i + WV_i}.\end{cases} \quad (2)$$

В зависимости от порта назначения *k* каждый пакет помещается в выходную очередь согласно условию.

$$\sum_{i=1}^{k}(WO_i + WV_i) \le random(\sum_{i=1}^{N}(WO_i + WV_i)) < \sum_{i=1}^{k+1}(WO_i + WV_i) \quad (3)$$

А если число пакетов в очереди достигает *M*, то *M*+1-й пакет отбрасывается. Между входом и выходом устройства есть положительная обратная связь. Если число пакетов на выходе каждого типа NO_t и NV_t., то обратная связь задаётся формулой

$$WV_{i,t} = WV_{i,t-1} \bullet \frac{NV_t + 1}{NV_{t-1} + 1}. \quad (4)$$

Предложенное обобщённое устройство пересылки пакетных данных и статистическая модель его функционирования позволяет корректно описать работу реальной сети в различных ситуациях, включая случай пиковой нагрузки. Проведённая верификация модели показала её корректность. Достоинством предложенной модели оказывается возможность учёта различных сетевых топологий с целью выяснения их влияния на распространение саморазмножающихся пакетов. При этом принципы построения исходной модели и соотношения (1)–(4) сохраняются.

ЛИТЕРАТУРА

1. Zou C.C., Gong W, Towsley D. Code Red Worm Propagation Modeling and Analysis // Доступно в сети Internet: http://tennis.ecs.umass.edu/~czou/research/codered.pdf

2. Kim J., Radhakrishnan S., Dhall S.K. Measurement and Analysis of Worm Propagation on Internet Network Topology // Доступно в сети Internet: http://www.computer.org.ru/ieee_lib/Catalog/catalog_14_.html