Возможность использования статистической модели цифровой информационной сети для обнаружения компьютерных червей

Булахов Николай Георгиевич

Томский государственный университет

Калайда Владимир Тимофеевич, д.т.н., Пойзнер Борис Николаевич, к.ф.-м.н.

E-mail: nboolahov@yandex.ru

Проблема математического описания функционирования цифровых информационных сетей, ориентированного на выработку принципов регулирования режимами в сети – одна из первоочередных. Существующие методы описания, как правило, ограничиваются статистическими характеристиками конкретных типичных ситуаций либо реальных событий, имевших ранее место. Но они не дают общих подходов, позволяющих строить систему анализа поведения сетей и управления ими. Подтверждение отсутствия общего подхода – многочисленные случаи неконтролируемого распространения вирусных пакетов. Поэтому необходимы новые подходы, позволяющие разрешить эти проблемы.

Автором ранее было предложено рассматривать всю сеть как некое устройство, содержащее в себе коммутаторы, маршрутизаторы и оконечные станции. Тогда достаточно простой моделью, которая учитывает особенности функционирования всей реальной сети (в том числе при пиковых нагрузках), способно служить сетевое устройство с обратной связью. Оно объединяет в себе функции маршрутизирующего оборудования и оконечных станций, являясь в этом смысле универсальным.

Указанное устройство имеет N входов и N выходов. Пара вход-выход образует подключение. Каждому подключению ставятся в соответствие два веса WO_i и WV_i, позволяющие дифференцировать загруженность выбранного канала, что отражает реальное разделение на магистральные и оконечные подключения сети. Внутри предлагаемого устройства каждому выходу соответствует очередь пакетов длиной M. Вес WO соответствует нагрузке канала за счёт обычных информационных пакетов, вес WV – за счёт саморазмножающихся пакетов, представляющих в данной модели компьютерных «червей». Чтобы учесть динамику распространения саморазмножающихся пакетов, вводится обратная связь. Она осуществляется за счёт изменения веса WV при изменении числа саморазмножающихся пакетов на выходе устройства.

Найдены условия того, что в заданный такт времени на входе с номером n присутствует пакет, а если присутствует, то является либо саморазмножающимся, либо нет. В зависимости от весов WO_i и WV_i, соответствующих порту назначения с номером k, каждый пакет помещается в некоторую выходную очередь – согласно заданному критерию. Если же очередь переполнена, то пакет отбрасывается. Далее подсчитывается число пакетов каждого типа (NO_t и NV_t) на каждом выходе. Действие обратной связи (о которой говорилось выше) проявляется в коррекции весов WO_i и WV_i, согласно разработанному соотношению [1]. Очевидно, что предлагаемое устройство и его модель работают дискретно. Тога логично использовать модель расширенного автомата, известную в теории автоматов.

Для проверки корректности предложенной модели выполнено компьютерное моделирование, результаты которого показывают, что модель отражает характер поведения разнородного трафика в проблемных сетях, согласуясь с экспериментальными данными [2], полученными в ходе анализа распространения реальных сетевых червей.

Модель [1] позволяет оценить влияние распространения саморазмножающихся пакетов на качество передачи информации по сети. Однако практический интерес представляет обнаружение факта вторжения зловредного программного кода на сетевые компьютеры и предотвращение его дальнейшего распространения. Большинство предлагаемых на сегодняшний день способов обнаружения сетевых атак основаны на анализе передаваемого по сети трафика, а также установки «приманки» – специально выделенного компьютера с программным обеспечением, эмулирующим уязвимости операционных систем и отслеживающих обращения к ним с целью проникновения.

Характеристиками передаваемого по сети трафика, пригодными для выявления потенциально опасной активности являются: интенсивность пересылки отдельных пактов, интенсивность пересылки небольших очередей пакетов и интенсивность попыток установить соединение отдельными хостами, распределение IP- и MAC-адресов источника и назначения в передаваемых пакетах, размеры передаваемых пакетов, типы пакетов (принадлежность к определённым протоколам). Однако для достаточно надёжного детектирования вредоносной активности и сведения риска ложного срабатывания к минимуму в данном случае часто требуется некоторая «калибровка», составление сигнатур распространения известных червей, что сужает область применения данных алгоритмов обнаружения сетевых атак и делает уязвимыми сети для новых (не внесённых в базу) червей. Автор предлагает исключить параметры, варьирующиеся для конкретных реализаций червя, и добавить характеристики пересылки информационных пакетов внутри маршрутизаторов и коммутаторов:

количество отбрасываемых пакетов в единицу времени, заполненность буферов пересылки, нагрузка оборудования.

Дело в том, что основная причина отказа маршрутизационного оборудования – это переполнение буферов сетевых интерфейсов пакетами с отсутствующей возможность дальнейшей моментальной пересылки. Эти пакеты хранятся в буфере интерфейса в надежде появления таковой возможности до истечения достаточно длительного временного интервала ожидания. Однако часто такие пакеты генерируются в больших количествах зловредным программным обеспечением заведомо без возможности нормальной пересылки маршрутизатором, что вызывает переполнение буфера и отбрасыванием остальных поступающих пакетов.

Таким образом, можно увеличить количество параметров, идентифицирующих сетевую атаку и в случае идентификации пакетов с отсутствующей возможность дальнейшей пересылки игнорировать их, освобождая мощности оборудования для пересылки нормального трафика. После идентификации источника распространения вредоносного трафика возможна его локализация и изоляция. Практическая проверка возможности использования статистической модели цифровой информационной сети для обнаружения компьютерных червей планируется в ближайшем будущем.

Список публикаций:

[1] Булахов Н.Г., Пойзнер Б.Н., Турицин А.Л., Хасанов В.Я. Статистическая модель цифровой информационной сети, учитывающая возможность пиковых нагрузок // Материалы международной научной конф. "Статистические методы в естественных, гуманитарных и технических науках" (апрель 2006 г., г. Таганрог). Ч. 3. Таганрог: «Антон», ТРТУ, 2006. С. 7–11.

[2] Kim J., Radhakrishnan S., Dhall S.K. Measurement and Analysis of Worm Propagation on Internet Network Topology // Доступно в сети Internet: http://ieeexplore.ieee.org/iel5/9617/30391/01401716.pdf