2. Системы, построенные на основе технологии клиент-серверных СУБД, обладают более простой реализацией, чем системы, построенные с использованием MPI, сложность которых связана с самой парадигмой передачи сообщений.

3. При построении приложений на основе технологии клиент-серверных СУБД необходимо вручную реализовывать сервисные возможности, уже реализованные в MPI.

НЕКОТОРЫЕ АСПЕКТЫ ОБНАРУЖЕНИЯ АНОМАЛЬНОЙ СЕТЕВОЙ АКТИВНОСТИ

П. А. Кочурко, С. В. Безобразова

Брестский государственный технический университет, Беларусь

Научный руководитель В. А. Головко

При построении программно-аппаратных комплексов информационной безопасности корпоративной сети среди основных функций выделяется обнаружение злоумышленного трафика: удаленных сетевых атак, вирусов, сетевых червей, троянских программ и другого вредоносного кода.

В нашем исследовании мы концентрируем внимание на сетевых атаках различных типов – отказ в обслуживании, сканирование, удаленное проникновение, локальное проникновение. Выделяют два основных подхода к обнаружению атак: обнаружение аномалий и обнаружение злоупотреблений.

В процессе обнаружения аномалии система обнаружения атак (СОА) производит анализ входного образа, которым может являться информация о TCP-соединении или строка журнала регистрации сетевых событий на предмет принадлежности его к одному единственному классу, который известен системе – классу нормальной активности. В случае, если делается вывод о его непринадлежности к данному классу, то данный образ считается атакой, то есть относится ко второму классу. В процессе определения злоупотреблений СОА наоборот реализует поиск того класса атак из известных классов, к которому данный входной образ может относиться. Если такой класс не найден, то данный образ объявляется нормальным.

Специфика первого подхода заключается в том, что, рассматривая сетевую активность, подозрительно отклоняющуюся от некоторой нормы, могут быть обнаружены не только попытки осуществления удаленной сетевой атаки, но и следы функционирования, например, сетевых червей или троянских программ. Тем самым анализ сетевой активности позволяет опосредованно сделать вывод о возможном наличии вредоносных программ в защищаемом субъекте. Конечно, для точного установления этих программ необходимы специфические антивирусные алгоритмы, тем не менее некоторый уровень тревоги может быть дан.

В современных системах обнаружения атак с разной степенью эффективности применяются различные технологии: статистический анализ, сигнатурный поиск, нечеткая логика и другие. Подходы с использованием искусственных нейронных сетей показали высокое качество обнаружения и распознавания атак, базируясь главным образом на анализе параметров TCP-соединений. Для обнаружения аномальной сетевой активности авторами были предложены нелинейные рециркуляционные нейронные сети, а также их ансамбли для распознавания класса сетевых атак [1]. Высокое качество работы данного алгоритма, впрочем, несколько снижается в отсутствие подходящей базы для обучения сетей.

Хорошие результаты показывает подход с использованием энтропии [2]. Система обнаружения атак собирает информацию о сетевом трафике в нескольких клю-

чевых местах сети. Собирается информация о запрашиваемых сетевых сервисах, количествах переданных байт, времени поступления запросов, адресах источника и приемника соединения. Кроме того, могут использоваться и дополнительные параметры, напрямую не связанные с сетевым трафиком, а именно загрузка ЦПУ или использование оперативной памяти.

Во время совершения атак сетевая активность приобретает новые черты – по некоторым параметрам становясь более упорядоченной, по некоторым более хаотичной. Так, например, при распределенной атаке типа «отказ в обслуживании» (DDoS-атаке) намного разнообразней стандартного становятся адреса источников соединений во внешней сети и, наоборот, намного менее разнообразны приемники этих соединений во внутренней сети потому как являются целью этой атаки. Подход с применением энтропии позволяет отслеживать одновременное изменение энтропии в нескольких характеристиках сетевой активности (рис. 1), тем самым делая вывод о наличии аномальной сетевой активности.

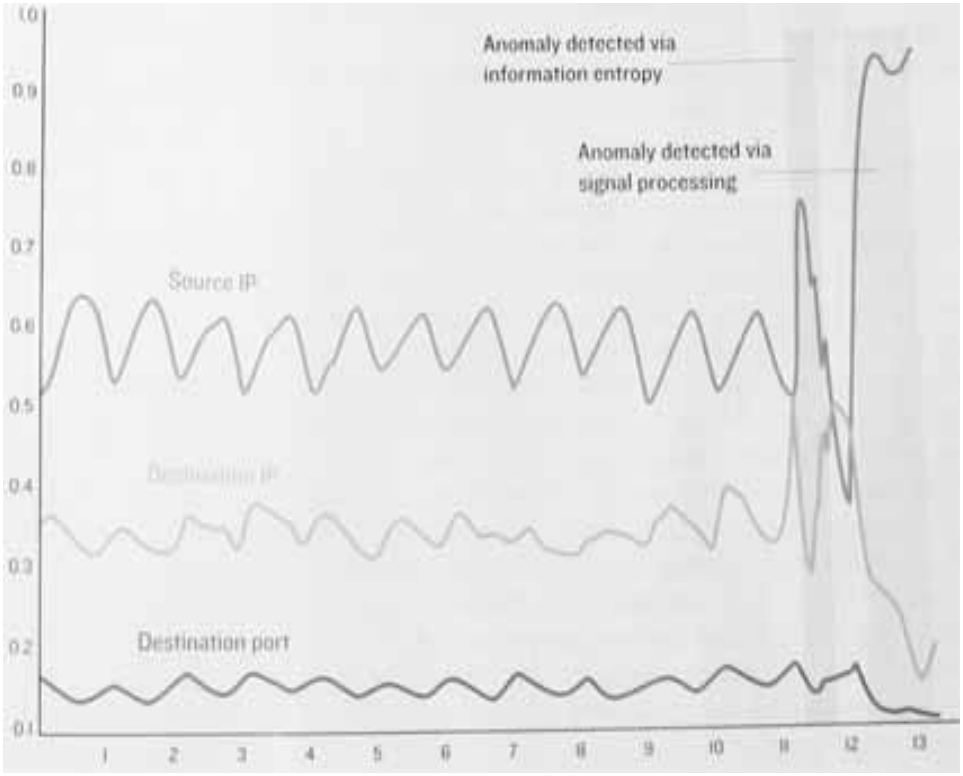

Рис. 1. Энтропия трех параметров сетевого трафика на протяжении нескольких дней наблюдений и обнаружение активности сетевого червя Sasser [2, с. 39]

В обычно хаотической активности наличие участка, в котором хаос уступает место упорядоченности, означает наличие серьезной аномалии. Анализ хаотического временного ряда на предмет наличия в нем упорядоченных участков предлагался для обнаружения эпилептиморфной активности в сигнале электроэнцефалограмм [3]. Для определения степени хаотичности сигнала в данный момент времени рассчитывается значение старшего показателя Ляпунова. Если он больше нуля – активность хаотическая, а значит нормальная. Если меньше – активность не хаотическая, имеет место аномалия.

Расчет старшего показателя Ляпунова является обычно достаточно ресурсоемким процессом. Однако использование искусственных нейронных сетей [3] позволяет не только ускорить, но и перевести практически в реальный режим времени. Нейронная сеть выполняет прогнозирование хаотического временного ряда и ряда с отклонением, после чего на основании отличия рассчитывается показатель Ляпунова.

Используя данную теорию, можно анализировать сетевую активность на предмет наличия аномалий. Если во время атаки некоторые характеристики приобретают черты более упорядоченного ряда, некоторые, наоборот, менее упорядоченного, то анализ хаотичности сетевой активности и будет являться тем самым обнаружением аномальной сетевой активности.

Анализ параметров сетевого трафика (например, времени появления пакетов, (рис. 2), позволил сделать вывод о действительной хаотичности данного временного ряда. Прогнозирующая нейронная сеть (рис. 3), являющаяся многослойным персептроном с одним скрытым слоем выдала следующие результаты анализа рядов.

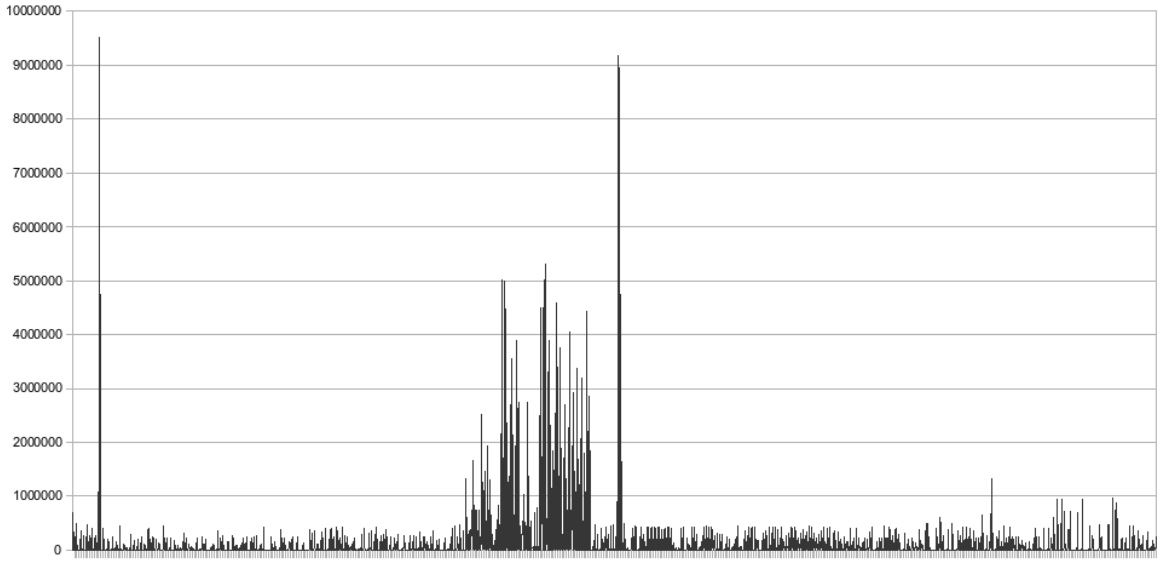

Рис. 2. Сетевая активность: значение задержек между каждыми двумя пакетами

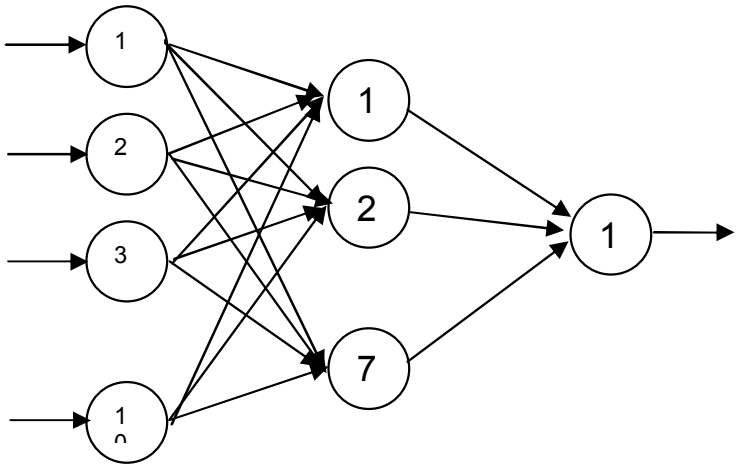

Рис. 3. Прогнозирующая нейронная сеть

Значение старшего показателя Ляпунова колеблется для нормальной сетевой активности от 0,1 до 0,3, тем самым доказывая, что данный временной ряд представляет собой хаотический ряд. Анализ изменений в хаотичности параметров сетевого трафика позволит обнаружить в реальном времени аномальную сетевую активность.

Литература

1. Кочурко, П. А. Нейросетевой детектор аномалий / П. А. Кочурко // Изв. Белор. инженер. акад. – 2005. – № 1 (19)/2. – С. 78–81.
2. Nucci, A. Controlled chaos / A. Nucci, S. Bannerman // IEEE Spectrum. – 2007. – № 12 (44). – P. 37–42.
3. Neural Networks for Chaotic Signal Processing: Application to the Electroencephalogram Analysis for Epilepsy Detection / V. Golovko, S. Bezobrazova // International Conference on Neural Networks and Artificial Intelligence (ICNNAI'2006): Proceedings, Brest, 31 May – 2 June, 2006 / Brest State Technical University; eds. : V. A. Golovko [et al.]. – Brest, 2006. – P. 136–139.

ПРИМЕНЕНИЕ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ ДЛЯ ИССЛЕДОВАНИЯ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ИЗНОСА ЖЕЛЕЗНОДОРОЖНОЙ СЕТИ

Д. П. Парфиевич, В. А. Сковпнев

Гомельский государственный университет имени Ф. Скорины, Беларусь

Научный руководитель Е. И. Сукач

В настоящее время большое внимание уделяется разработке математических моделей, позволяющих исследовать реальные процессы, происходящие в сложных системах, для своевременного принятия решений с целью исключения нежелательных ситуаций, возникающих при функционировании этих систем. К таким системам можно отнести и транспортные сети. Транспортный поток значительно увеличивается год за годом. Это приводит к быстрому износу дорог, как автомобильных, так и железнодорожных, что приводит к снижению эффективности функционирования транспортных сетей и увеличивает возможность возникновения аварий.

В докладе рассматривается задача исследования вероятностных характеристик износа железнодорожной сети, которая включает две составляющие ее задачи: исследование износа участка железнодорожной сети и исследование вероятностного изменения состояния железнодорожной сети. При решении поставленных задач предлагается использовать компьютерное моделирование, которое реализуется на основе комплекса взаимосвязанных моделей разного уровня. Модели первого уровня позволяют исследовать процессы износа отдельных участков дорог, которые описываются стационарными поглощающими цепями Маркова. Вершины цепи Маркова определяют состояния участков дорог. Они носят вероятностный характер и влияют на пропускные способности этих участков, которые уменьшаются по мере износа. Логико-вероятностная модель второго уровня, используя информацию первого уровня о текущем состоянии участков, позволяет в динамике проследить изменение вероятностных характеристик износа всей сети.

В процессе эксплуатации участок железнодорожной сети, описываемой графом, подвергается износу. Процесс эксплуатации участка дороги состоит из повторяющихся циклов постоянной жесткости, связанных с передвижением по участку транспортных единиц. Процесс износа является непрерывным физическим процессом, который происходит в результате функционирования комбинированной силовой системы, образованной верхним строением железнодорожного пути и колесом [1]. В этом процессе выделяется ряд состояний, которые характеризуются множеством сочета-