ВОЗМОЖНОСТИ СИСТЕМ ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Ручкин В.Н.

Рязанский институт Московского государственного открытого университета
390046, Рязань, ул. Колхозная, д. 2, тел. (0912) 77-41-48

Безопасность данных является одной из главных проблем в Internet, т.к. у конкурентов появляется возможность доступа к архивам коммерческих данных. Это заставляет руководство корпораций отказываться от использования открытых информационных систем. Возрастающее преобладание распределенных сетевых систем и незащищенных сетей, таких как Internet, значительно увеличили потребность в своевременном и точном обнаружении атак на компьютер или вычислительные системы.

Большинство современных подходов к процессу обнаружения атак используют некоторую форму анализа на основе правил. Набор правил входит в экспертную систему. К сожалению, экспертные системы требуют постоянного обновления для того, чтобы оставаться актуальными. Кроме того, экспертные системы на основе правил не обладают достаточной гибкостью в представлении структуры типа "правило-проверка".

За прошедшие несколько лет разработано большое количество подходов к обнаружению атак, опирающихся на неэкспертные системы.

Искусственная нейросеть (artificial neural network) состоит из набора элементарных элементов, которые взаимосвязаны друг с другом и трансформируют набор входных данных к набору желаемых выходных данных. Результат преобразования определяется характеристиками элементов и весами, соответствующими взаимосвязям между ними. Путем видоизменения соединений между узлами сети можно адаптироваться к желательным выходным результатам. В отличие от экспертных систем, которые могут дать пользователю определенный ответ, соответствуют или нет рассматриваемым характеристикам, заложенным в базе данных правил, нейросеть проводит анализ информации и предоставляет возможность оценить, что данные согласуются с характеристиками, которые она научена распознавать. В то время как степень соответствия нейросетевого представления может достигать 100%, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи так называемые обучение.

По вопросу применения нейросетей для обнаружения компьютерных атак было проведено небольшое количество исследований. Искусственные нейросети предлагают потенциал для решения большого количества проблем, охватываемых другими современными подходами к обнаружению атак.

Первым преимуществом в использовании нейросетей при обнаружении злоупотреблений является гибкость, которую эти сети предоставляют.

Второе наиболее важное преимущество нейросетей при обнаружении злоупотреблений заключается в способности нейросетей "изучать" характеристики умышленных атак и идентифицировать элементы (*например, трафик*), которые не похожи на те, что наблюдались в сети прежде.

Есть две основных причины, почему нейросети не применялись ранее в задачах обнаружения злоупотреблений. Первая причина связана с требованиями к обучению нейросети. Поскольку способность искусственной нейросети идентифицировать указания на атаку полностью зависит от точности обучения системы, обучающие данные и используемые методы обучения являются наиболее важными. Однако, основное неудобство применения нейросетей для детектирования вторжения - это природа "черного ящика" нейросети.

Есть два общих варианта реализации нейросетей в системах обнаружения злоупотреблений. Первый включает объединение их в существующих или видоизмененных экспертных системах. Второй подход заключается в реализации нейросети, как отдельно стоящей системы обнаружения злоупотреблений.

Для построения нейросетей использовать отечественные нейропроцессоры NeuroMatrix NM6 403 и NM6404, которые представляют собой высокопроизводительные DSP ориентированные RISC процессоры. В состав нейропроцессоров входят два основных блока: 32-бит RISC ядро и запатентованный 64-бит VECTOR сопроцессор для поддержки операций над векторами с элементами переменной разрядности. Причем, последний процессор NM6404 совместим по системе команд с предыдущей версией NM6403. Внутри кристалла имеются два идентичных программируемых интерфейса для работы с внейшей памятью различного типа и два коммуникационных порта, аппаратно совместимых с портами ЦПС TM320C4x, для возможности построения мультипроцессорных систем. Нейропроцессор NM6403 работает с частотой 40 Мгц, а NM6404– 133 Мгц. Основу обоих нейропроцессоров составляет RISC – ядро с 5-ти ступенчатым 32-бит конвейером с использованием 32- и 64-бит команды(обычно выполняется две операции в одной команде).

Процессор имеет 2Мбит внутреннее ОЗУ с доступом к внутренней памяти соседа и два адресных генератора с адресным пространством 16 GB. Схема имеет два 64-бит программируемых интерфейса с SDRAM/SRAM/ DRAM /Flash ROM разделяемой памятью. При этом обеспечивается 4 одновременных доступа к внутренней памяти. Имеющиеся два коммуникационных порта осуществляют аппаратную совместимость с TMS320Cx . Кроме того, имеется JTAG – совместимый отладочный интерфейс. Система управления потребляемой мощностью стабилизирует работы всей схемы в целом. Одним из достоинств нейропроцессоров NM6403 и NM6404 является наличие встроенного VECTOR сопроцессора, который обеспечивает работу с длиной векторных операндов и результатов от 1- до 64-бит.

Для создания нейросетей в вышеперечисленных нейропроцессорах имеется три варианта реализации многопроцессорного режима по любой из двух внешних шин. При этом арбитраж для доступа к общей памяти подключенных двух процессоров осуществляется без использования внешнего контролера. Конфигурация 1-го типа характеризуется тем, что доступ в память (MEMORY BANK1, MEMORY BANK2) осуществляется только одним процессором NP1или NP2 в данный момент времени.

Конфигурация 2-го типа отличается тем, что каждый процессор имеет свой банк памяти, к которому другой не имеет доступа. Имеется также банк MEMORY BANK3, который является общим для NP1 и NP2 и подключается к ним поочередно через буфер BUFFER1 и BUFFER2.

Конфигурация 3-го типа характеризуется тем, что каждый процессор имеет свой банк памяти и существует возможность каждому процессору обратиться к чужому банку через буфер BUFFER.

Достоинствами предложенных аппаратных реализаций систем обнаружения атак на основе нейронных сетей являются: а) использование ее для широкого класса задач от систем ЦОС до обработки видеоизображений, б) возможность эмуляции нейронных сетей и осуществление векторно-матричных вычислений для реализации сложных мультимикропроцессорных систем [3] в качестве элементной базы мультипроцессорных супер-ЭВМ.

Литература

1. Ручкин В.Н. Концептуальная модель и реализация системы цифровой обработки сигналов // Труды 3-ей Международной конференции и выставки “ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ И ЕЕ ПРИМЕНЕНИЕ ” Москва,-2000 - т.□С.70-73

2. Ручкин В.Н. Проектирование и выбор специализированных средств обработки информации. М.: Московский государственный открытый университет, 1997.120 с.126: ил.

3. П.Е. Виксне, Д.В. Фомин, В.М. Черников Однокристальный цифровой нейропроцессор с переменной разрядностью операторов // ИЗВЕСТИЯ ВУЗОВ, Приборостроение, 1996, т.39, № 7, С.13-21.л