УДК 681.3

КАМЕНДА Д. В.

Научный руководитель: Головко В. А. (к.т.н., профессор)

АНАЛИЗ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Интенсивное развитие компьютерных систем и их объединение в сети привело к росту зависимости, как отдельных лиц, так и организаций от хранящейся в компьютерах информации, а также от средств связи между компьютерными системами. Это, в свою очередь, привело к пониманию того, что данные и ресурсы необходимо защищать от постороннего доступа, чтобы гарантировать аутентичность данных и сообщений, а также оградить системы от атак по сети.

В связи с определёнными трудностями, возникшими при реализации систем обнаружения атак, приходится искать новые пути для решения задач по обнаружению атак. Одно из таких решений найдено в области нейронных сетей и нечеткой логики. Именно с помощью этих математических теорий системы обнаружения аномального поведения (истоки технологии обнаружения злоупотреблений) получили второе рождение.

Идея использования нейросетей при обнаружении атак заключается в "обучении" сети таким образом, чтобы она могла прогнозировать действия или операции пользователя, основанные на его предыдущих действиях или операциях. Обучение - это главная характеристика нейронных сетей. Она позволяет системе обнаружения атак или аномалий, построенной с учетом нейротехнологии, изучить правила поведения пользователя. Обучающий алгоритм позволяет системе следить за поведением пользователя и самостоятельно адаптироваться к постоянному изменению его поведения. После периода обучения сеть пытается согласовывать осуществляемые операции и действия с существующим профилем активного пользователя. Любое неправильно предсказанное событие фактически означает отклонение действий пользователя от установленного для него профиля.

К преимуществам нейронных сетей можно отнести следующее:

- они хорошо справляются с "шумовыми" данными;
- их успех не зависит от статистического предположения относительно характера обрабатываемых данных;
- они просты для модификации при добавлении новых данных;
- на них не влияют утомление и потеря внимательности, присущие человеку.

Существуют две обобщённые категории атак, которые пытаются идентифицировать системы обнаружений вторжений (атак) - аномалии и неправильное использование (злоупотребление). Рассмотрим нейронные сети для решения задачи обнаружения атак. В отличие от экспертных систем, которые предоставляют пользователю чёткий ответ о том, принадлежит ли данный набор характеристик некоторому набору базе правил, нейронная сеть производит анализ информации и способна сообщить о степени соответствия поданных на её вход данных тому набору, которому она была обучена. Совпадение может быть стопроцентным, однако точность зависит только от результатов обучения образцов конкретной проблемы. Но несомненным преимуществом ИНС является ей способность адекватно реагировать на данные, не нахо-

дившиеся в тренировочном наборе - то есть фактически сеть может идентифицировать относительно новый тип атаки, так как часть процесса её проведения применялась ранее в других типах атак.

Рассмотрим нейронные сети для решения задачи обнаружения атак. В отличие от экспертных систем, которые предоставляют пользователю чёткий ответ о том, принадлежит ли данный набор характеристик некоторому набору в базе правил, нейронная сеть производит анализ информации и способна сообщить о степени соответствия поданных на её вход данных тому набору, которому она была обучена. Совпадение может быть стопроцентным, однако точность зависит только от результатов обучения образцов конкретной проблемы. Но несомненным преимуществом ИНС является её способность адекватно реагировать на данные, не находившиеся в тренировочном наборе - то есть фактически сеть может идентифицировать относительно новый тип атаки, так как часть процесса её проведения применялась ранее в других типах атак.

В качестве задачи возьмём идентификацию неправильного использования сети, что выражается в сетевом графике какими-либо признаками. Для начала необходимо определить, какие показатели работы сети позволяют сделать вывод о предполагаемой атаке. Сеть Интернет - это сеть сетей, объединяющая как локальные сети, так и глобальные сети типа NSFNET. Поэтому центральным местом при обсуждении принципов построения сети является семейство протоколов межсетевого обмена TCP/IP. Под термином "TCP/IP" обычно понимают все, что связано с протоколами TCP и IP. Это не только собственно сами протоколы с указанными именами, но и протоколы, построенные на использовании TCP и IP, а также прикладные программы.

Один из вариантов использования ИНС для обнаружения атак построен на принципе выявления посторонних активностей. Иногда постороннее вызывает куда больший интерес, чем привычное, классический пример - системы обнаружения мошенничества (Fraud Detection Systems).

Для реализации этого метода обнаружения атак (посторонних активностей) используется многослойный персептрон с одинаковым числом входных и выходных нейронов. Такие сети известны как рециркуляционные нейронные сети (РНС). В РНС входной набор должен отобразиться в такой же выходной набор. Таким образом, мерой посторонней активности может служить ошибка реконструкции входного образа. Тогда мера посторонней активности i-го входного образа может быть определена как:

$$OF_i = \frac{1}{n}\sum_{j=1}^{n}(x_{ij} - o_{ij})^2, \qquad (1)$$

где n - размерность входного и выходного образов.

Мера посторонней активности вычисляется для всех записей данных, используя обученную нейронную сеть.

В качестве данных для обучения необходимо выбрать параметры сетевого трафика, которые позволяют идентифицировать данные TCP/IP-пакета, TCP/IP-соединения и т.п. Важной особенностью процесса обучения является то, что в обучающей выборке должно число записей, которые характеризуют атаки (аномальное поведение), должно быть гораздо меньше чем число записей о нормальном состоянии системы.

РНС часто применяются благодаря своей способности сжимать данные в процессе своей работы внутри сети. Этот фактор можно использо-

вать и при обнаружении посторонних активностей. Например, в одном из внутренних слоёв сети можно оставить небольшое количество нейронных элементов, в зависимости от значений которых образы можно причислить к определённым кластерам. Например, при наличии K нейронных элементов в скрытом слое, которые могут принимать дискретные значения 0, 1, 2, ..., N-1 возможно закодировать M кластеров, что выражается формулой (2).

$$M = N^K \quad (2)$$

В результате удалось разработать программные модули для обучения, тестирования и применения описанного метода обнаружения атак на практике. Следует отметить, что обучение производилось на условии разумного компромисса между временем обучения и точностью работы.

Литература

1. S.J. Stolfo, et al., "KDD cup 1999 dataset", UCI KDD repository, http://kdd.ics.uci.edu
2. University of New Mexico. Computer Immune Systems. http://www.cs.unm.edu/~immsec/data/
3. K. Jain, and R. Sekar, "User level Infrastructure for System Call Interposition: A Platform for Intrusion Detection and Confinement", 1999 http://citeseer.nj.nec.com/jain00userlevel.html
4. Головко В.А. Нейроинтеллект: теория и применение. Книга 1.: Организация и обучение нейронных сетей с прямыми связями. Брест Изд. БПИ, 1999 - 264 с.

УДК 621.9.044

КРАВЧУК А.В.

Научный руководитель: доцент Григорьев В.Ф.

СОСТАВЛЕНИЕ ОПТИМАЛЬНОЙ ЧПУ-ПРОГРАММЫ ДЛЯ ВЫСОКОСКОРОСТНОГО ФРЕЗЕРОВАНИЯ (ВСФ)

Для оптимальной обработки пространственно-сложных поверхностей современного технологического оборудования не достаточно - необходима оптимальная технология. При составлении подобной технологии важным условием является рассмотрение всей цепи процесса создания продукта.

Возникающие проблемы [1]:

- обмен данными между CAD- и CAM-системами. Опыт показывает, что при экспортировании данных часть из них теряется, в результате чего на 3D модели появляются незамкнутые контуры детали;
- программист при составлении ЧПУ-программы имеет неполную информацию об оптимальном планировании ВСФ. Связано это с тем, что существующие CAD/CAM-системы имеют многочисленные функции для обработки сложных поверхностей базирующиеся на геометрии, но не несущие технологической информации;
- практически отсутствуют рекомендации для программиста по составлению ЧПУ-программ при ВСФ на уровне технологических модулей.

Классическое проектирование процесса фрезерования проводится в три этапа. Сначала на основе конструктивных данных составляется последовательность обработки: черновое, получистовое, чистовое фрезерование. Затем проектируются операции фрезерования на отдельных