В.А. ГОЛОВКО, Л.Ю. ВОЙЦЕХОВИЧ
Брестский государственный технический университет

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

Важным этапом обеспечения безопасности компьютерных систем является проектирование систем обнаружения атак (Intrusion Detection System – IDS). Такие системы способны на основе анализа сетевого трафика автоматически обнаруживать атаки TCP/IP, что позволяет предпринять необходимые меры для нейтрализации угрозы.

В данной работе рассматриваются нейросетевые подходы для построения систем обнаружения атак. В качестве базы данных для тестирования системы используется KDD-99 [1], которая содержит почти 5 миллионов записей соединений и 41 параметр сетевого трафика. При этом атаки делятся на четыре основных класса: DoS, U2R, R2L и Probe.

Атака DoS – отказ в обслуживании – характеризуется генерацией большого объема трафика, что приводит к перегрузке и блокированию сервера.

Атака U2R предполагает получение зарегистрированным пользователем привилегий локального суперпользователя (администратора).

Атака R2L характеризуется получением доступа незарегистрированного пользователя к компьютеру со стороны удаленной машины.

Атака Probe заключается в сканировании портов с целью получения конфиденциальной информации.

В работе предлагаются различные варианты построения систем обнаружения атак, которые базируются на использовании рециркуляционных и многослойных нейронных сетей. Результаты экспериментов обсуждаются.

Рассмотрим различные архитектурные решения для построения систем обнаружения атак. В качестве входных данных применяется 41-размерный вектор, который характеризует параметры соединения сети. Задачей IDS является обнаружение и распознавание атак. Поэтому в качестве выходных данных используется m-мерный вектор, где m равняется количеству атак плюс нормальное состояние.

На рис. 1 приведена система обнаружения атак, которая состоит из рециркуляционной нейронной сети (RNN) и многослойного персептрона (MLP).

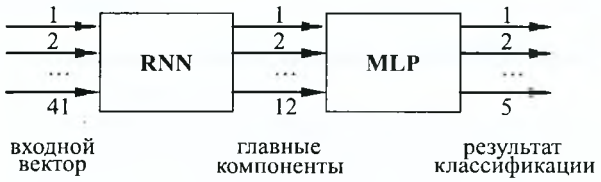

Рис. 1. Первый вариант IDS

Задача RNN – сжатие входного пространства образов с целью получения главных компонент [2]. Главные компоненты являются некоррелированными и содержат наиболее информативные признаки исходного пространства образов. Обучение RNN производилось в соответствии с правилом Ойя [3]. Многослойный персептрон осуществляет обработку сжатого пространства входных образов (главных компонент) с целью распознавания класса ата-

ки. Для обучения использовался алгоритм обратного распространения ошибки.

На рис. 2 приведена вторая схема системы обнаружения атак.

Она характеризуется тем, что главные компоненты с выходов RNN одновременно поступают на четыре отдельных многослойных

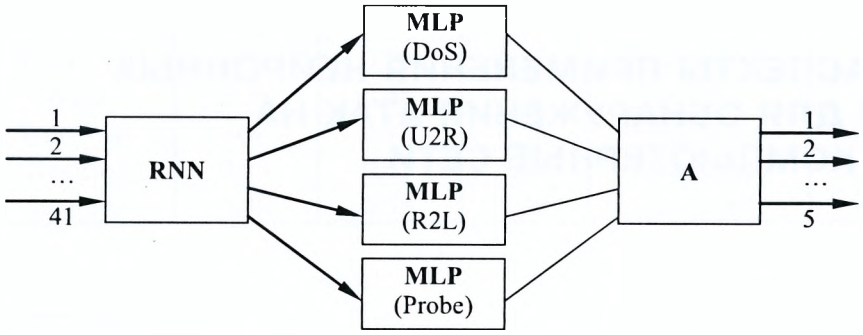

Рис. 2. Второй вариант IDS

персептрона, каждый из которых соответствует определенному классу атаки: DoS, U2R, R2L и Probe. С выходов MLP данные поступают на арбитр, который и принимает окончательное решение о состоянии системы. В качестве арбитра может использоваться линейный или многослойный персептрон. Тогда обучение его будет производиться после обучения RNN и MLP. Такая схема может осуществлять иерархическую классификацию атак. В этом случае арбитр определяет один из пяти классов атаки, а соответствующий многослойный персептрон – тип атаки.

В работе рассматриваются также другие варианты архитектур IDS.

Эксперименты проводились для каждой службы отдельно. Рассмотрим функционирование системы на примере модели 1. Сводные данные по результатам тестирования в режиме распознавания класса атаки по почти 30 службам приведены в таблице.

Наилучший результат был достигнут для атак класса DoS и Probe (почти однозначная распознаваемость). Несколько хуже определяются U2R и R2L, соответственно 83,7 и 89,4%. Кроме того, существует процент ложных срабатываний системы.

Путем комбинирования двух различных нейронных сетей, а именно RNN и MLP, можно идентифицировать и распознавать атаки на компьютерные сети с достаточно высокой степенью точности. В качестве базы данных для тестирования предложенных методов использовалась база KDD-99. Основными преимуществами применения подходов, основанных на нейронных сетях, является способность адаптироваться к динамическим условиям и быстрота функционирования, что особенно важно при работе системы в режиме реального времени.

Таблица. Статистика тестирования в режиме классификации атак (около 30 сервисов)

Класс	Всего	Обнаружено	Распознано
DoS	286369	286334 (99,9%)	286087 (99,9%)
U2R	49	41 (83,7%)	40 (97,6%)
R2L	1119	1000 (89,4%)	906 (90,6%)
Probe	1320	1312 (99,4%)	1308 (99,7%)
Нормальное состояние			
Normal	83281	-	82943 (99,6%)

Литература

1. 1999 KDD Cup Competition.– mode of access: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

2. Головко В.А. Нейронные сети: обучение, организация и применение. Кн. 4: учеб. пособие для вузов / Общ. ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.

3. Hyvaerinen A., Oja E. Independent component analysis: algorithms and applications // Neural Networks.– № 13.– 2000. – P. 411-430.