Секция X
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МОДЕЛИРОВАНИЕ

НЕЙРОСЕТЕВЫЕ ПОДХОДЫ ОБНАРУЖЕНИЯ АТАК TCP/IP

Л. Ю. Войцехович

Брестский государственный технический университет, Беларусь

Научный руководитель В. А. Головко

Введение

Одной из форм глобализации мирового пространства является информационная глобализация, которая связана с повсеместным распространением сети Интернет.

В результате этого значительно возросло количество атак и злоупотреблений в сфере высоких технологий. Поэтому вопросу безопасности компьютерных систем уделяется все больше и больше внимания.

Задачей Систем Обнаружения Атак (Intrusion Detection Systems – IDS) является защита компьютерных сетей. В последнее время системы IDS активно изучаются.

Эта статья является продолжением предыдущих работ [1], в которых предлагаются модели, основанные на применении рециркуляционной нейронной сети (RNN) и многослойного персептрона (MLP), а также рассматривается Ансамблевая нейронная сеть (Ensembling Network – EN).

Процесс обработки информации в IDS

Процесс обработки информации в IDS включает три этапа.

На первом этапе осуществляется захват трафика сети (feature selection). Сбор необходимых данных выполняет специальное программное средство (sniffer). В этой работе использована база данных KDD-99. Эта база содержит около 5 000 000 записей о соединениях. Каждая запись в этой базе представляет собой образ сетевого соединения, включает 41 параметр трафика и промаркирована как «атака» или «не атака».

Второй этап связан с уменьшением размерности входного вектора данных и получением главных компонент (feature extraction). Между используемыми параметрами существуют сложные взаимосвязи, которые достаточно тяжело проследить. Некоторые данные являются избыточными. Большое количество параметров может значительно увеличить время вычислений, поэтому этап получения главных компонент является важным этапом в процессе функционирования предлагаемых IDS.

Третий этап состоит в обнаружении и распознавании атак (classification). В базе KDD-99 атаки делятся на четыре основные категории: DoS, U2R, R2L и Probe. Каждый класс, в свою очередь, состоит из отдельных типов атак.

Архитектурные решения IDS

Рассмотрим различные архитектурные решения для построения систем обнаружения атак. В качестве входных данных используется 41-размерный вектор, который характеризует параметры соединения сети. Задачей IDS является обнаружение и

распознавание атак. Поэтому в качестве выходных данных используется 5-мерный вектор, где 5 – это количество классов атак плюс нормальное состояние.

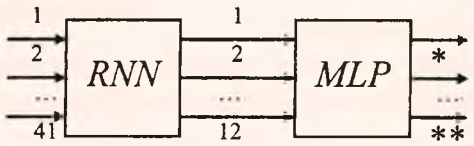

Рис. 1. Первый вариант IDS

На рис. 1 приведена система обнаружения атак, которая состоит из рециркуляционной нейронной сети и многослойного персептрона, которые соединены последовательно. Задачей RNN является сжатие входного 41-размерного вектора в 12-размерный выходной вектор (главные компоненты [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 с целью распознавания класса атаки.

На рис. 2 приведена вторая схема системы обнаружения атак. Она характеризуется тем, что главные компоненты с выходов RNN одновременно поступают на 4 отдельных многослойных 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 5 классов атаки, а соответствующий многослойный персептрон – тип атаки.

Следующий вариант структуры IDS основан на идее разбиения исходной задачи на множество небольших и простых задач среди нескольких экспертов с последующим объединением полученных решений (рис. 3). Каждый эксперт представляет собой отдельную систему классификации. В качестве эксперта мы использовали модель 1. Обучение эксперта происходит на отдельном множестве данных, т. е. данные для обучения каждого последующего эксперта формируются с учетом результатов обучения предыдущих экспертов. Алгоритм, используемый для такого обучения, называют алгоритмом усиления за счет фильтрации (boosting by filtering) [4].

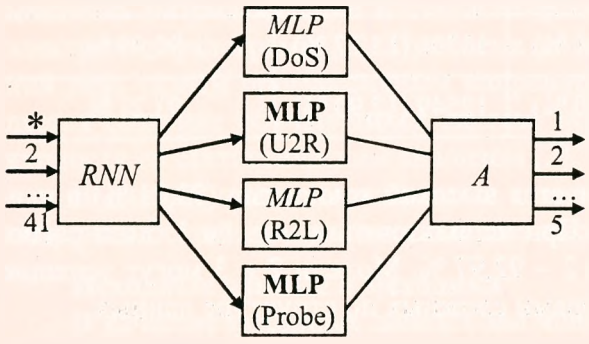

Рис. 2. Второй вариант IDS

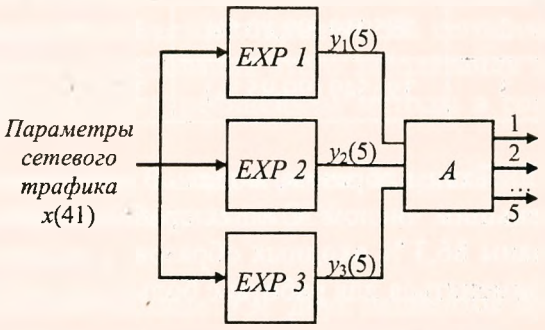

Рис. 3. Третий вариант IDS

Результаты экспериментов

Чтобы оценить эффективность предложенных подходов обнаружения вторжений, был проведен ряд экспериментов. База данных KDD Cup 99 использовалась для обучения и тестирования нейросетевых моделей.

Алгоритм усиления за счет фильтрации, который используется в случае модели 3, предполагает наличие большого (в идеале – бесконечного) множества примеров. Поэтому мы использовали 10%-ную выборку из базы KDD (почти 500 000 записей!). Для обучения нейронных сетей были отобраны 6186 примеров. Далее вся 10%-ная выборка применялась для тестирования.

Рассмотрим функционирование системы на примере модели 1. Эта модель достаточно проста. Результаты тестирования приведены в табл. 1.

Таблица 1

Результаты тестирования модели 1

Класс	Всего	Обнаружено	Распознано
DoS	391458	391441 (99,99 %)	370741 (94,71 %)
U2R	52	48 (92,31 %)	42 (80,77 %)
R2L	1126	1113 (98,85 %)	658 (58,44 %)
Probe	4107	4094 (99,68 %)	4081 (99,37 %)
normal	97277	–	50831 (52,25 %)

Наилучший результат был достигнут для атак класса DoS и Probe (почти однозначная распознаваемость). Несколько хуже определяются U2R и R2L, соответственно 80,77 % и 58,44 %. Кроме того, существует процент ложных срабатываний системы.

Сводные данные по каждому из вариантов построения системы обнаружения атак приведены в табл. 2:

Таблица 2

Сводные данные по результатам тестирования каждой модели

Модель	Обнаруженные атаки	Распознанные атаки	Ложные срабатывания	Общая доля распознанных, %
1	396696 (99,98 %)	375522 (94,65 %)	46446 (47,75 %)	86,30 %
2	395949 (99,80 %)	375391 (94,61 %)	13398 (13,77 %)	92,97 %
3	396549 (99,95 %)	375730 (94,70 %)	12549 (12,90 %)	93,21 %

Таким образом, модель 3 характеризуется высокой точностью (93,21 %) и наименьшим числом ложных срабатываний. При использовании модели 1 были распознаны 86,3 % входных образов, а модели 2 – 92,97 %. Модели 2 и 3 могут успешно применяться для работы с большими наборами сложных по структуре данных.

Заключение

Путем комбинирования двух нейронных сетей, а именно RNN и MLP, можно идентифицировать и распознавать атаки на компьютерные сети с достаточно высо-

кой степенью точности. В качестве базы данных для тестирования предложенных методов использовалась база KDD-99. Основными преимуществами применения подходов, основанных на нейронных сетях, являются способность адаптироваться к динамическим условиям и быстрота функционирования, что особенно важно при работе системы в режиме реального времени.

Литература

1. Golovko, V., Vaitsekhovich, L. Neural Network Techniques for Intrusion Detection // Proceedings of International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2006). – 2006. – P. 65–69.
2. Головко, В. А. Нейронные сети: обучение, организация и применение : учеб. пособие для вузов. Кн. 4 / под общ. ред. А. И. Галушкина. – Москва : ИПРЖР, 2001. – 256 с.
3. Oja, E. Principal components, minor components and linear networks // Neural Networks. – 1992. – Vol. 5. – P. 927–935.
4. Drucker, H. Improving performance in neural networks using a boosting algorithm / H. Drucker, R. Schapire, P. Simard // In S. J. Hanson, J. D. Cowan and C. L. Giles eds., Advanced in Neural Information Processing Systems 5, Denver, CO, Morgan Kaufmann, San Mateo, CA. – 1993. – P. 42–49.

НЕЙРОСЕТЕВЫЕ МЕТОДЫ ДЛЯ ДИАГНОСТИКИ ЭПИЛЕПСИИ НА ОСНОВЕ АНАЛИЗА ЭЛЕКТРОЭНЦЕФАЛОГРАММ

С. В. Безобразова

Брестский государственный технический университет, Беларусь

Научный руководитель В. А. Головко

Введение

Электроэнцефалография позволяет при помощи специального оборудования получать сигналы электроэнцефалограммы (ЭЭГ), которые отражают суммарную биоэлектрическую активность головного мозга и способны хранить в себе информацию о функциональном состоянии мозга, общемозговых расстройствах и их характере [1].

Применение электроэнцефалографического исследования дало толчок к развитию методов анализа ЭЭГ сигналов с целью обнаружить различные аномальные активности, в частности, эпилептические разряды. Значимость изучения проблем диагностики, терапии и прогнозирования эпилепсии обусловлена в первую очередь широким распространением этого нервно-психического заболевания. В настоящее время показатель распространенности достиг 1 % от всего человечества [1].

Для повышения качества диагностики эпилепсии в ранних исследованиях применялись математические и статистические методы, которые основаны на анализе электроэнцефалограмм [2]. Проблема до сих пор остается открытой. На сегодняшний день самым прогрессивным направлением исследования этого заболевания является создание обучающихся систем, использующих нелинейные методы в совокупности со статистическим анализом [2].

В данной статье описываются основные аспекты применения искусственных нейронных сетей для диагностики эпилепсии на основе анализа ЭЭГ.

Исходные данные и методика

В качестве исходных данных мы используем данные ЭЭГ двух пациентов Брестской областной больницы, описание этих данных приведены в таблице.