Разработка приложения для обнаружения и классификации атак на основе нейросетевой модели

Суворова Валерия Александровна

Студент

Механико-математический факультет Пермского государственного национального исследовательского университета, Пермь, Россия

E-mail: Valery.Suvorova@yandex.ru

На сегодняшний день обеспечение конфиденциальности и целостности данных в компьютерных сетях является одной из важнейших задач в области информационной безопасности. Для активного исследования защищенности информационных ресурсов широко применяются системы обнаружения вторжений (Intrusion detection system). Современные IDS требуют применения адаптивных методов, работающих в реальном режиме времени, обладающих высокой чувствительностью к изменениям в информационной среде.

В работе предлагается создание модуля для обнаружения и классификации атак на основе анализа сетевого трафика с использованием искусственной нейронной сети, а именно – многослойного персептрона [1].

Исходные данные для построения нейронной сети были взяты из общедоступной базы KDD Cup 1999 Data [2], содержащей сведения о легальных сетевых соединениях и 22 видах атак, где для каждой записи имеется 41 параметр (признак соединения).

На первом этапе с помощью функции автоматического построения нейронных сетей (ANS) пакета Statistica были построены нейронные сети, использующие полный набор входных параметров, способные выявлять атаку в соединении и определять её вид.

Были получены 5 наилучших вариантов построения нейронных сетей, каждая из которых позволяет с достаточно высокой точностью определить вид атаки – ошибка обучения не превышает 0,15%, ошибка тестирования не более 0,18% и ошибка проверки не превышает 0,16%.

Затем были проведены дополнительные исследования по оценке значимости входных признаков для дальнейшего устранения избыточности входных параметров. В результате были выявлены 10 признаков, которые являются наименее информативными при вычислении результата, и при построении нейронных сетей с сокращенным числом параметров они были исключены из входного множества.

Полученные результаты позволили сократить входное множество признаков с 41 до 21 параметра и построить нейронные сети с сокращенным набором параметров. В качестве входного множества использовались те же данные, что и для построения нейросетей с полным числом параметров. В результате была получена оптимальная модель нейронной сети MLP 98-6-23, ее характеристики представлены в таблице 1.

Таблица 1: Характеристики MLP 98-6-23

Название	Верность обучения (%)	Верность тестирования(%)	Верность проверки(%)
MLP 98-6-23	99,83	99,76	99,83

Несмотря на существенное сокращение числа входных параметров, полученная модель обладает высокой способностью распознавания атак: ошибка проверки не превышает 0,17%, что незначительно выше ошибки проверки для сетей с полным набором параметров.

Далее было выполнено сравнение модели MLP 98-6-23 с аналогичными нейронными сетями, решающими задачу распознавания сетевых атак, описанными в работах [3–5]. Результаты сравнения полученной модели с аналогичными нейросетями показывают высокую эффективность разработанной модели и сравнительно высокую точность определения видов атак.

На основе полученной нейросетевой модели в было разработано пользовательское приложение, которое запрашивает на вход информативные параметры о сетевом соединении (21 параметр) и выдает заключение о том, является ли соединение атакой, определяет вид атаки, а также уровень доверия (с какой точностью определен результат). Программа была протестирована на множестве записей, которые не входили в обучающее множество нейронной сети. Точность распознавания для различных видов атак варьируется от 94,5% до 99,99%. Следовательно, созданная программа в дальнейшем может быть успешно встроена в различные системы обнаружения атак в качестве одного из компонентов многоуровневой системы защиты от вторжений наряду со стандартными методами.

Литература

1. Ясницкий Л. Н. Интеллектуальные системы. —М.: Лаборатория знаний, 2016. — 221 с.
2. KDD Cup 1999 Data [Электронный ресурс] URL: http://kdd.ics.uci.edu/databases/kddcup99
3. Мустафаев А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика // Вопросы безопасности. 2016. № 2. С. 1–7. [Электронный ресурс] URL: http://e-notabene.ru/nb/article_18834.html
4. Жигулин П. В., Мальцев А. В., Мельников М. А., Анализ сетевого трафика на основе нейронных сетей // Электронные средства и системы управления. 2013. №2. С. 44–48.
5. Емельянова Ю. Г., Талалаев А. А., Тищенко И. П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: Теория и приложения. 2011. № 3(7). С. 3–15.