ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ В РЕАЛИЗАЦИИ ДЕТЕКТОРА СЕТЕВЫХ ВТОРЖЕНИЙ

Байтингер Г. Р.
Факультет математики и информатики, Гродненский государственный университет имени Янки Купалы
Гродно, Республика Беларусь
E-mail: grb007@rambler.ru

В представленной работе приведена классификация систем обнаружения вторжений, описаны подходы к обнаружению атак на информационные системы, описаны архитектуры искусственных нейронных сетей (далее – нейронных сетей), применимых в детекторах сетевых аномалий, а также, рассмотены методики увеличения эффективности и точности в обучении и применении нейронных сетей.

Введение

Наиболее интересной особенностью нейронных сетей является их обучаемость, способность корректировать собственные параметры для корректной обработки не встречавшихся ранее исходных данных. Именно это свойство нейронных сетей представляет особую ценность для комплексов обнаружения вторжений в информационные системы, так как позволяет значительно упростить и, в определённой мере, автоматизировать работу по их конфигурации и поддержке.

Не смотря на перспективность применения нейросетевых решений в системах обнаружения вторжений, такие комплексы всё ещё не распространены широко и многие свойства нейронных сетей не исследованы в достаточной мере.

I. Системы обнаружения вторжений

Системы обнаружения вторжений (СОВ) являются важным компонентом комплексного подхода к обеспечению безопасности информационных систем. Системы обнаружения вторжений можно классифицировать по способу обнаружения атаки, способу сбора данных об атаке, способу реагирования на неё.

По способу обнаружения атаки выделяют СОВ обнаружения аномалий и СОВ поиска злоупотреблений. Первые сравнивают текущую активность в ИС с образом «нормального» поведения. Обнаруженные отклонения (аномалии) могут восприниматься СОВ как атаки. Вторые сравнивают активность в системе с известными шаблонами поведения ИС соответствующего конкретной атаке. Найденные совпадения расцениваются СОВ как попытки реализации атаки.

Преимуществом первого подхода является отсутствие необходимости составления описаний конкретных атак и используемых в них уязвимостей. СОВ поиска злоупотреблений хотя и обладают довольно высокой точностью принимаемых решений, в то же время непосредственно зависят от актуальности и полноты базы известных атак и конкретная атака отсутствующая в базе данных СОВ замечена ситемой не будет. Недостатками в применении СОВ обнаружения аномалий являются трудоёмкость определения пороговых характеристик исследуемой ИС и потенциальная возможность обучения СОВ злоумышленником таким образом, чтобы атаки воспринимались СОВ как легитимное поведение ИС.

По способу сбора данных СОВ можно разделить на сетевые СОВ, СОВ уровня конечного устройства и СОВ уровня приложения. Сетевые СОВ располагаются на узле сети и анализируют сетевой трафик, проходящий через их сенсоры в реальном, или близком к реальному времени. СОВ уровня конечного устройства анализируют состояние конкретного узла сети и предназначены для обнаружения атак, направленных непосредственно против него. СОВ уровня приложения ориентированы на поиск проблем конкретного приложения. Так же широкое применение находят гибридные СОВ, как правило, включающие в себя свойства нескольких перечисленных категорий.

По способу реагирования различают пассивные и активные СОВ. Пассивные СОВ только фиксируют факт атаки, записывают данные в файл журнала и выдают предупреждения. Активные СОВ пытаются противодействовать атаке, например, путем реконфигурации межсетевого экрана или генерации списков доступа маршрутизатора.

Учитывая недостаточную исследованность поведения нейронных сетей, для реализации детектора сетевых атак наиболее целесообразно выбрать архитектуру пассивного детектора сетевых аномалий, для понижения вероятности ложных срабатываний СОВ посредством передачи результатов её работы администратору на проверку.

II. Нейронные сети в системах обнаружения вторжений

Простейшие нейронные сети содержат один слой нейронов, на каждый из которых поступают все входы сети. Далее каждый нейрон вычисляет взвешенную сумму входов сети, применяет активационную функцию и в случае превышения порога активации пускает на выход единичный сигнал. таким образом на выходе слоя получаем

бинарный вектор с размерностью равной количеству нейронов слоя.

Более сложные сети состоят из большего количества последовательно соединённых слоёв, возможно с наличием обратных связей (когда нейронные связи ведут от выходов текущего слоя ко входам этого или предшедствующих слоёв) и имеют большие вычислительные возможности.

Суть процесса обучения нейронных сетей заключается в последовательном предъявлении на вход сети некоторых векторов с одновременной подстройкой весов нейронных связей. Различают алгоритмы обучения с учителем и без учителя. В первом случае для обучения используются пары входных и соответствующих им выходных векторов. Подстройка сети для каждого вектора происходит до тех пор, пока отличие выхода сети от оджидаемого не становится минимальным (таким образом либо получаем достаточно малую погрешность, либо обучение зацикливается). Обучение без учителя ставит целью получение соголасованности на выходе нейронной сети, то есть чтобы предъявление достаточно близких входных векторов давало одинаковые выходы[1].

Проблема переобучения нейронной сети заключается в слишком сильной аппроксимации выходов сети к выходам обучающей выборки, тем самым получая сеть, которая выдаёт достаточно малые значения ошибки только на обучающей выборке, а на реальных данных этот показатель начинает расти. Для обнаружения переобучения можно применять резервирование подмножества обучающей выборки, на котором обучение не производится. Оно используется для контроля качества обучения сети. Для снижения риска переобучения может понадобиться, например, уменьшение количества нейронов в слоях, что может лишить сеть достаточной гибкости для решения поставленной задачи и обучение зациклится.

Ещё одной проблемой в работе нейронных сетей является чистота входных данных. Нейронные сети обучаются тому, чему обучиться проще. Это означает что в случае несбалансированного набора данных подаваемого на вход сети, она может начать учиться выдввать результаты близкие не той закономерности, которую мы хотели выделить. В таких ситуациях лучшим выходом будет обработка входного множества для достижения его большей однородности (например можно повторять редкие наблюдения, либо избавляться от часто встречающихся)[1].

Сети встречного распространения обладают способности к куда более быстрому обучению. Структурно в них объединены самоорганизующаяся карта Кохонена и звезда Гроссберга нейроны которых объединены в 2 последовательно соединённых слоя. В слое Кохонена единичный выход даёт только один из нейронов, получающий наибольшую сумму взвешенных входов.Принцип работы слоя Кохонена заключается в том, что близкие входные векторы в результате прохода через него активируют один и тот же нейрон, таким образом слой Кохонена занимается разбиением входных векторов по классам схожих. Слой Гроссберга получает выход слоя Кохонена (а это вектор с одной единицей и остальными координатамит равными нулю), то есть выходом слоя Гроссберга будет сумма весов нейронных связей соединяющих "победивший"нейрон слоя Кохорнена с нейронами слоя Гроссберга[1].

Обучение в сети встречного распространения отличается для слоя Кохонена и слоя Гроссберга. Обучение слоя Кохонена это обучение без учителя ставящее целью сгруппировать схожие входные векторы и отделить их от других групп. Для корректной работы слоя необходима предварительная нормализация входных векторов. Проблемой является потенциальная неравномерность распределения входных векторов, соответственно обучение слоя Кохонена будет заключаться в подстройке весового множества под обучающую выборку (распределить весовые векторы в соответствии с плотностью распределения входных).

Проблемой данного метода обучения может являться то, что некоторые нейроны слоя Кохонена не будут обучаться из-за того что входные векторы будут более близки к весам других нейронов. Решением может быть коррекция весов всех нейронов в соответствии с максимальным значением выхода слоя, или искуственное ументьшение выхода часто "побеждающих"нейронов чтобы дать возможность "победить"остальным нейронам слоя.

Обучение слоя Гроссберга является обычным обучением с учителем, модифицируются только веса соединённые с победившим нейроном слоя Кохонена.

Описанная выше архитектура встречного распространения является подходящей для реализации в составе СОВ: если считать принадлежность классам на которые слой Кохорнена разбивает входящие данные признаком принадлежности соответствующих данных тому или иному виду атаки на систему, то подобная сеть позволяет относительно быстро проводить классификацию событий в ИС и своевременно реагировать на аномальное поведение.

1. Основы теории нейронных сетей / Г. Э. Яхъева. – Национальный открытый университет «ИНТУИТ», 2016.
2. Применение искусственных нейронных сетей в системах обнаружения атак / В. А. Крыжановский. –Доклады ТУСУРа. Технические науки., 2008. №2(18), часть 1.
3. Лабораторный практикум по курсу «Введение в теорию нейронных сетей» / О. А. Мишулина, А. Г. Трофимов, М. В. Щербинина. –МИФИ, 2007.
4. Применение нейронных сетей для интеллектуального анализа данных при решении задач защиты информации: Методические указания / Г. Ф. Нестерук, Ф. Г. Нестерук. –СПбГУ ИТМО, 2008.