Анализируя траектории перемещения дисков по стержням, начиная с диска N, в обратном порядке, можно видеть, что схема перемещения четных дисков $\{i, j, 3\text{-}i\text{-}j\}$, а нечетных – $\{i, 3\text{-}i\text{-}j, j\}$. Отсюда следует, что младшая единица двоичного представления номера перекладываемого диска однозначно определяет закон его перемещения. Определив переменные состояния каждого стержня, легко записать одношаговый алгоритм перекладывания дисков, не используя память стека или поиск.

Преимуществом полученного алгоритма является возможность его продолжения с любого исходного распределения дисков по стержням, что весьма практично для реализации управления в реальном времени. Привязка переменных состояния основана на том, что перемещение диска с номером N на одну позицию вызывает 2^{N-i-1} перемещений для диска с номером i. Достаточно построить производный класс итератора, который в качестве аргумента конструктора принимает массив с положением дисков на стержнях и заполняет массив массив текущих точек траекторий.

ЛИТЕРАТУРА

1. Шалыто А., Туккель Н., Шамгунов Н. Ханойские башни и автоматы. – Программист, 2002. – С. 82-90.
2. Седжвик Р. Фундаментальные алгоритмы на C++. Части 1-4. Анализ. Структуры данных. Сортировка. Поиск – Киев: ДиаСофт, 2002.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

П.А. Кочурко
(БрГТУ, Брест)

Постоянное развитие Интернет-технологий остро ставит проблему обеспечения безопасности компьютерных систем. Среди других вредоносных воздействий на компьютерные сети резко возросло количество сетевых атак, равно как и ущерб, наносимый ими [1].

В системах обнаружения атак применяются сигнатурные методы, экспертные системы, статистический анализ и т. д. В последнее время многие исследователи используют и нейросетевые технологии.

Основные подходы к обнаружению атак – обнаружение аномалий и определение злоупотреблений. Применение только одного из них существенно ограничивает возможности системы. Объединение же их в рамках одной системы позволяет не только обнаруживать атаку, но и распознавать её тип.

В данной работе детектором аномалий является нелинейная рециркуляционная нейронная сеть (РНС), а распознавание типа атаки производится многослойным персептроном (MLP). На вход системы попадает сетевой трафик – пакеты протоколов TCP, UDP, ICMP. Пакеты анализируются модулем предобработки данных, после чего накопленные данные о соединениях подаются на вход обеих нейронных сетей для ответа на вопрос: является ли это соединение атакой, и если да, то какого типа.

Обучение РНС ведётся на нормальных соединениях таким образом, чтобы при подаче на неё параметров (продолжительность, количества переданных байт) нормального соединения на выходе сети были восстановлены те же самые параметры. В случае превышения ошибкой восстановления заданного порога соединение признаётся аномалией. Используется алгоритм послойного обучения.

Обучение MLP проводится как на нормальных соединениях, так и на атаках – при подаче параметров соединения (продолжительность, количества переданных байт, служба, протокол, флаг результата) на выходе должен быть активен только нейрон, соответствующий классу данной атаки. Используется алгоритм обратного распространения ошибки.

Для обучения и тестирования нейронных сетей использовалась база данных KDD'99 [2]. Результаты: на наборе данных, состоящем из 494021 записи о соединениях обнаруживается 395984 (99,81%) атак, из них 374149 (94,49%) верно распознаются, при 398 (0,41%) ложных срабатываниях.

Исследования производятся при поддержке БРФФИ при НАН Беларуси.

ЛИТЕРАТУРА

1. Лукацкий А. В. Обнаружение атак. – СПб.: БХВ-Петерург, 2003.
2. 1999 KDD Cup Competition http://kdd.ics.uci.edu/databases/kddcup99/