П.А. КОЧУРКО
Брестский государственный технический университет

НЕЙРОСЕТЕВОЕ РАСПОЗНАВАНИЕ КЛАССОВ СЕТЕВЫХ АТАК

Среди задач системы защиты информации, реализующей механизмы обнаружения атак, выделяют в том числе качественное распознавание. Недостаточно просто обнаружить атаку – необходимо определить ее тип, потому что от этого во многом зависит дальнейший алгоритм действий системы и персонала по защите информации и нейтрализации последствий атаки.

Специфика основных подходов к обнаружению атак – обнаружения аномальной сетевой активности и обнаружения злоупотреблений – накладывает соответствующие ограничения на их нейросетевую реализацию. При этом подсистема анализа трафика может включать в себя любое количество ИНС и связей между ними. В случае, если используются несколько ИНС, должна быть разработана схема определения результата исходя из нескольких результатов, представленных каждой ИНС.

В упрощенном виде схему работы системы обнаружения сетевых атак можно представить в следующем виде: производится перехват сетевого трафика; производится предварительная обработка трафика с выделением параметров TCP-соединений, которые поступают на обработку детекторами атак. Исходя из количества различных классов входных данных, целесообразно обучить детекторы для каждого из классов отдельно, не объединяя все классы атак в единое целое.

Рассмотрим методы распознавания классов сетевых атак с помощью различных нейросетевых подходов: с применением обучаемого векторного квантователя (LVQ), многослойного персептрона (MLP) и совокупного классификатора на основе рециркуляционных нейронных сетей (РНС).

1. LVQ может быть использован в качестве детектора злоупотреблений для распознавания типа атак. Так как база данных KDD [1] содержит атаки 22 типов и нормальные соединения, то получаем 23 класса, принадлежность к которым входных векторов можно определить. На вход LVQ поступает 41 параметр – по количеству параметров в записях KDD.

2. Обучим MLP из трех слоев с нелинейными функциями активации нейронов. Количество нейронных элементов в распределительном слое соответствует количеству параметров в базе данных KDD, в выходном слое – количеству типов соединений. В процессе функционирования при подаче параметров соединения на вход сети на выходе наибольшее значение будет иметь нейрон, соответствующий типу данного соединения.

3. Одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс A), или ко второму (класс $\bar{A}$), которому соответствуют далеко отстающие векторы [2]. Объединим обученные частные РНС-детекторы в один общий следующим образом: входной образ поступает после предобработки на вход всех частных детекторов, которые работают параллельно. Результаты их работы поступают в блок динамического выбора классификатора (DCS), который делает вывод о том, образ какого класса поступил на вход [3].

Сравним результаты, показываемые данными подходами (рис. 1). Отметим, что самый высокий уровень распознавания и классификации атак показывает технология совокупного классификатора на основе РНС, правда при достаточно высоком уровне FN. В свою очередь, очень хорошие результаты по уровню FN и FP показывают подходы на основе MLP, причем и качество классификации атак данными методами только чуть хуже, чем у совокупного классификатора. Если рассмотреть результаты с применением других технологий в дру-

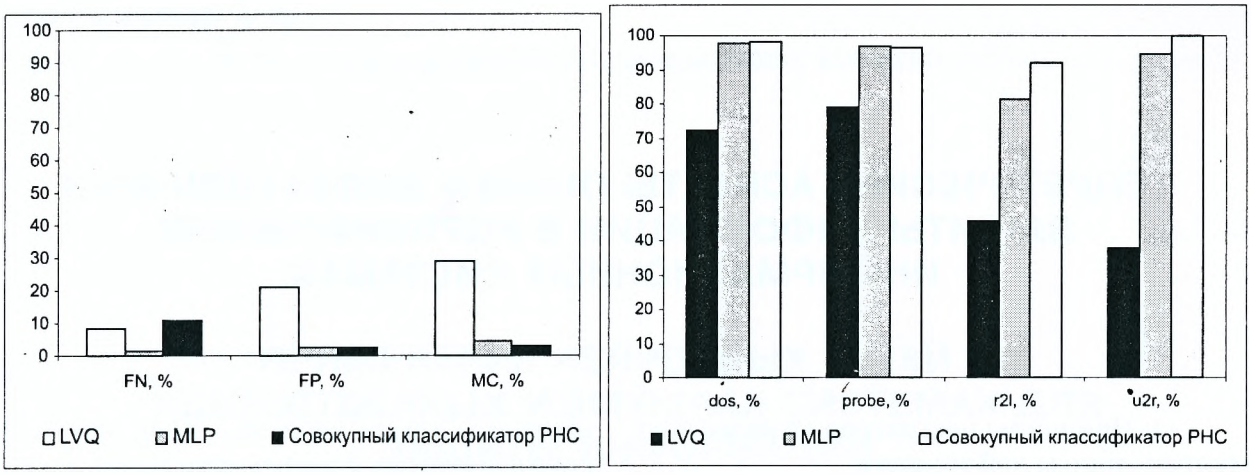

Рис. 1. Сравнение результатов, показанных детекторами с различными нейросетями (FN - false negative, FP - false positive, MC - misclassification)

гих исследованиях [4], то видно, что качество классификации с помощью совокупного классификатора на основе РНС существенно улучшает все применяемые технологии. Особенно это заметно на атаках классов u2r и r2l.

Исследования проводятся при поддержке БРФФИ при НАН Беларуси и Министерства образования Республики Беларусь.

Литература

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

2. Кочурко П. Нейросетевой детектор аномалий. Известия Белорусской инженерной академии, № 1(19)/2'2005 – с. 78-81.

3. Кочурко П. Совокупность детекторов на основе рециркуляционных нейронных сетей для распознавания класса сетевых атак // Вестник Брестского государственного технического университета. – 2005. – № 5: Физика, математика, информатика. – С. 61-65.

4. Sabhnani M. and Serpen G. Application of Machine Learning Algorithms to KDD Intrusion detection dataset within Misuse detection context // In Proceedings of the International conference on Machine Learning: Models, technologies and Applications. – 2003. – P. 209-215.

Студенты БГУ победили в конкурсе программных проектов Google

Студенты факультета прикладной математики и информатики Белорусского государственного университета Дмитрий Мазовка и Александр Казаченок стали победителями II Всемирного конкурса программных проектов компании Google.

Четверокурсник Дмитрий Мазовка разрабатывает проект генерации природных явлений в виртуальном трехмерном пространстве, Александр Казаченок (третий курс) работает над проектом создания самоадаптируемых генераторов типичных веб-приложений. Уровень этих проектов по критериям новизны и значимости соответствует требованиям, предъявляемым к докторским диссертациям в США.

Компания Google, принимающая участие в образовательных программах ООН, проводит среди студентов всего мира конкурс проектов по разработке актуального открытого программного обеспечения в интернете в режиме on-line. Исходный код разрабатываемого программного обеспечения свободно доступен в интернете. Представленные студентами проекты открыто обсуждаются во Всемирной паутине ведущими мировыми специалистами в соответствующих областях. Каждому студенту назначается научный руководитель. 13.09.06