С.В. БЕЗОБРАЗОВ, В.А. ГОЛОВКО
Брестский государственный технический университет

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМАХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Традиционный подход в обнаружении компьютерных вирусов, основанный на сигнатурном поиске, имеет существенный недостаток. Сигнатурный поиск не способен обнаруживать неизвестные вирусы. Поэтому для успешной борьбы с вредоносными программами необходимо постоянно пополнять антивирусные базы, которые, как правило, располагаются на веб-сайте разработчика антивирусного программного обеспечения. Компьютер с устаревшими антивирусными базами может оказаться бессильным перед угрозой заражения новым вирусом [1]. Сегодняшние исследования в области защиты информации направлены на то, чтобы «научить» антивирусные программы распознавать неизвестные вирусы. Такая система повысила бы уровень защиты компьютерных систем и избавила бы пользователей от неудобных операций.

В лаборатории искусственного интеллекта и нейронных сетей Брестского государственного технического университета под руководством д.т.н., профессора В.А. Головко проводятся исследования методов защиты информации в рамках проекта «Методы искусственного интеллекта для защиты информации» по заказу Министерства образования РБ. Исследования проводятся по двум направлениям:

- методы стеганографической защиты информации;
- методы создания искусственных иммунных систем для защиты от вирусов.

В данной работе представлен нейросетевой подход для формирования детекторов в искусственной иммунной системе для защиты информации. При формировании детекторов используется нейронная сеть для векторного квантования (LVQ-сеть). Представленный метод позволяет уменьшить временные и вычислительные затраты, связанные с проверкой файлов на наличие вирусов. Также метод сочетает в себе преимущества обоих методов (негативная и позитивная селекции) отбора нежелательных детекторов [2].

Нейросетевой подход для формирования детекторов

Нейронная сеть для векторного квантования была предложена в 1982 году Кохоненом и называется обучающим векторным квантователем (learning vector quantization – LVQ) [3]. LVQ-сеть представляет собой двухслойную нейронную сеть (конкурирующий и линейный слои) с прямым распространением сигналов (рисунок).

Рассмотрим процесс формирования детекторов на основе LVQ-сети. Первоначально определяется набор чистых файлов: это могут быть утилиты операционной системы, различные документы, файлы разнообразного программного обеспечения. Из этих файлов случайным образом выбираются участки определенной длины (к примеру, бинарные строки размерностью 128 бит) и подаются на вход векторного квантователя. Для обучения

Таблица. Результаты проверок

Имя вируса	Детектор 1	Детектор 2	Детектор 3	Имя файла	Детектор 1	Детектор 2	Детектор 3
Maslan	0,83	0,77	0,83	ctfmon.exe	0,83	0,84	0,81
DebPloit	0,94	0,92	0,73	dcomcnfg.exe	0,9	0,89	0,87
Lovesan	0,74	0,71	0,72	diskcopy.com	0,88	0,83	0,86
Hidrag	0,75	0,77	0,75	hh.exe	0,87	0,84	0,85
LazyMin	0,75	0,76	0,75	notepad.exe	0,85	0,83	0,86
Sober	0,68	0,71	0,69	regedit.exe	0,84	0,81	0,85
Trojan.VB	0,8	0,79	0,81	template.exe	0,85	0,83	0,85
Bagle	0,79	0,68	0,7	cacls.exe	0,84	0,82	0,87
Win95.cih	0,8	0,82	0,78	dbexplor.exe	0,91	0,89	0,9
Bagle.bn	0,69	0,67	0,68	dllhost.exe	0,87	0,87	0,85
Bagle.bj	0,96	0,93	0,79	etm70.exe	0,91	0,87	0,9

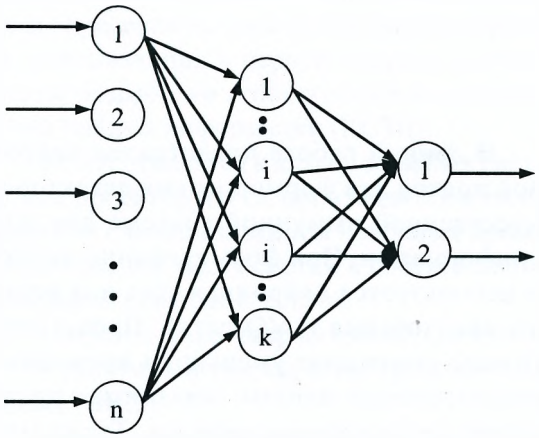

Рис. LVQ - сеть

нейронной сети также необходимо наличие какого-нибудь вируса (или его сигнатуры), из которого подобным образом выбирается битовая строка и подается на вход LVQ-сети. Таким образом, указывая нейронной сети явные структурные различия чистых файлов и вирусов (а компьютерные вирусы структурно отличаются от чистых файлов, так как подразумевают деструктивные действия), мы обучаем ее обнаруживать компьютерные вирусы. В процессе проверки файлов LVQ-сеть идентифицирует неизвестный образ и определяет его близость к тому или иному эталонному вектору. Наличие разнообразных чистых файлов для обучения и элемента случайности в формировании входных векторов дает возможность получить много различных по своей структуре детекторов.

Выводы

Таблица отображает способность детекторов отличать вирусы от чистых файлов.

Разработан метод формирования детекторов искусственной иммунной системы для защиты информации на основе LVQ-сети. Метод позволяет значительно уменьшить затраты на вычислительные ресурсы компьютерной системы, следовательно, сокращается время проверки файлов на наличие вирусов. Благодаря свойствам LVQ-сети уменьшается время, необходимое для обучения детектора. Размер детекторов увеличивается, однако это компенсируется повышением уровня обнаружения, т.е. один детектор способен обнаружить большее количество вирусов.

Литература

1. Почему не срабатывают антивирусы. –mode of access: http://www.i2r.ru, 2003.

2. Безобразов С.В. Искусственные иммунные системы для защиты информации: сравнительный анализ методов негативной и позитивной селекций детекторов // Инженерный вестник.– 2006.– № 1(21)/1.– С. 76-82.

3. Kohonen T. Sell-organised formation of topologically correct feature maps // Biological Cybernetics. – 1982. – N 43.– P. 59-69.