ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ ЗЛОУПОТРЕБЛЕНИЙ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Д. В. Сидорик

ВВЕДЕНИЕ

С расширением применения компьютерных технологий возрастает и зависимость в которой находятся частные компании и государственные организации от своих вычислительных сетей. Защита этих систем от атак становится одним из приоритетных направлений корпоративной политики. Для обеспечения безопасности внедряется ряд административных и технических мер, к которым относятся в частности брандмауэры и системы обнаружения вторжений (IDS – Intrusion Detection Systems), которые на сегодняшний день стали одним из ключевых компонент обеспечения безопасности вычислительных сетей.

В работе представлена реализация применения нейронных сетей для обнаружения атак, направленных против сетевых ресурсов. Представлены результаты тестов для сравнения возможностей НС с существующими системами на основе анализа сигнатур по масштабируемости и способности обнаруживать новые разновидности атак.

1. ОПИСАНИЕ ПРЕДЛАГАЕМОГО ПОДХОДА К ОБНАРУЖЕНИЮ

В данной работе рассматривается стек протоколов TCP/IP, как наиболее используемый как в локальных, так и в глобальных сетях.

Анализировались протоколы IP, TCP и UDP. Все поля, за исключением идентификатора IP, контрольных сумм и полей синхронизации SYN, ACK, URG были включены в набор входных данных. При этом потребовалась специальная предобработка для:

- идентификатора протокола верхнего уровня. Для каждого из двух обрабатываемых протоколов TCP и UDP был выделен отдельный бинарный вход НС.
- IP-адресов. Предварительно классифицировались на несколько групп, по выполняемым функциям и принадлежности к различным сетям, каждой группе поставлен в соответствие отдельный вход.
- номеров портов. НС, классифицируют входные векторы по расстояниям между ними и слабо реагируют на малые изменения

входных параметров, в то время как отличие между двумя разными номерами портов одинаково существенно, независимо от того, сколько составляет их разность. Вместо обычно используемого выделения портов или их групп в отдельные входы на основе статистики и априорных соображений [1], в данной работе номера портов подавались НС группами длиной в несколько бит (1, 2 или 4) каждая на отдельный вход. Таким образом, по сравнению с подачей номера порта числом на один вход, максимальный теоретический разброс расстояний между входными векторами уменьшается с 2^{16} до 4 при передаче побитно. Еще одним аргументом в пользу побитовой подачи является то, что при распределении портов в некоторых случаях использовались двоичные соображения.

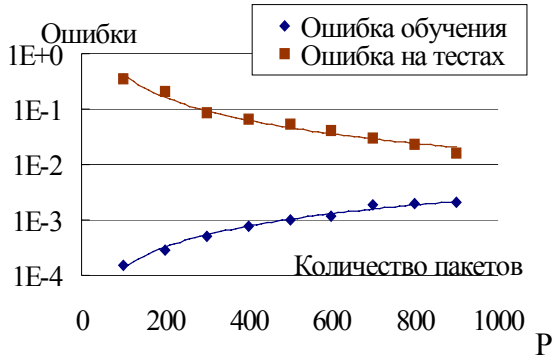
- Опции TCP. Существует весьма ограниченный список опций, наличие или отсутствие каждой которых кодировалось отдельным элементом входного набора данных НС.
- Область данных. Теоретические соображения, изложенные в литературе [2], указывают на противоречивость требований к применяемому преобразованию и низкую эффективность их применения к области данных. В то же время из анализа экспериментальных данных и спецификаций протоколов известно, что в большинстве протоколов прикладного уровня наиболее важная служебная информация, такая как команды и флаги, содержится в начале порции данных. Поэтому ввода данных в сеть был ограничен набором из 60 первых байт, каждый из которых подавался на отдельный вход.

В качестве НС использовался обычный многослойный персептрон. В обучающих данных выходы персептрона принимали значения [1 0] или [0 1] соответственно для «нормальных» и «плохих» пакетов.

2. ТЕСТИРОВАНИЕ

Для экспериментов использовался реальный сетевой трафик, снятый при помощи сниффера с компьютера, находящегося в том же сегменте сети, что и атакуемый. Для моделирования атак использовались отдельные примеры реализации (эксплойты), программы XSpider, Internet Security Scanner, исследованы уязвимости системы под управлением Windows NT. По используемым протоколам их можно разделить на 4 вида: Microsoft-DS, Telnet, HTTP, другие. Использовались 2 тестовых набора, в одном из которых содержание различных классов соответствовало обучающей выборке, а во втором – исходным данным.

Было проведено 2 серии испытаний, в первой из которых разделение по классам атак не учитывалось. В этом случае результаты обоих тестов эквивалентны. Результаты первой серии приведены на рис. 1, 2.



ис. 1. Зависимость оптимального размера сети от количества пакетов в обучающей выборке

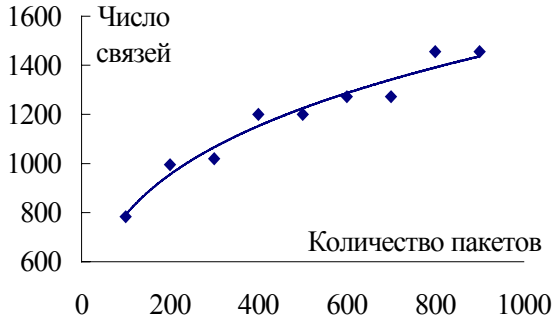


Рис. 2. Зависимость тестовой ошибки и ошибки обучения от количества пакетов в обучающей выборке для НС оптимального размера

Таблица 1

Результаты тестирования поведения нейронной сети при добавлении в обучающую выборку новых классов атак

Объем обучающей выборки	пакетов атак класса 1	пакетов атак класса 2	пакетов атак класса 3	пакетов атак класса 4	Размер сети	Ошибка обучения	Ошибка на тесте 1	Ошибка на тесте 2
100	100	0	0	0	[6 6 4]	0.00020	0.18665	0.45864
100	0	100	0	0	[6 6 4]	0.00022	0.16215	0.68521
100	0	0	100	0	[8 8 6]	0.00035	0.21008	0.38336
100	0	0	0	100	[6 6 6]	0.00027	0.14421	0.42256
200	100	100	0	0	[10 8 8]	0.00035	0.05988	0.20675
200	100	0	100	0	[12 10 10]	0.00062	0.06998	0.22541
200	100	0	0	100	[10 10 8]	0.00045	0.08533	0.24111
200	0	100	100	0	[12 10 10]	0.00066	0.09637	0.29021
200	0	100	0	100	[10 10 10]	0.00041	0.08667	0.28482
200	0	0	100	100	[12 10 10]	0.00073	0.10732	0.31404
300	100	100	100	0	[12 12 10]	0.00122	0.05604	0.18844
300	100	100	0	100	[12 12 10]	0.00130	0.06409	0.13261
300	100	0	100	100	[12 12 12]	0.00142	0.06033	0.22315
300	0	100	100	100	[12 12 12]	0.00149	0.05086	0.16558
400	100	100	100	100	[12 12 12]	0.00170	0.03450	0.08852

Во второй серии для обучения выбирались только некоторые классы атак по отдельности. Результаты приведены в табл. 1. В поле «Размер сети» в квадратных скобках указаны количества нейронов в каждом из 3 скрытых слоев сети.

Целью второго теста было изучение способности IDS на основе НС обнаруживать новые модификации известных атак. Для этого НС обучалась на наборе №1 из 400 пакетов, сгенерированных устаревшей версией XSpider 6.0 и 10000 пакетов «нормального» трафика . Затем проводилось тестирование на наборе №2 из 1000 пакетов, сгенерированном Internet

Security Scanner, выпущенном годом позже, и 50000 пакетов «нормального» трафика. Для сравнения оба набора данных пропускались через Agnitum Outpost и BlackIce Firewall с наборами сигнатур, также устаревшими на год.

Полученный результат показывает значительное преимущество НС при обнаружении неизвестных злоупотреблений.

Таблица 2

Результаты тестирования способности НС обнаруживать неизвестные атаки.

IDS	Набор 1 (обучающий)		Набор 2	
	Ложных тревог	Пропущенных пакетов атак	Ложных тревог	Пропущенных пакетов атак
Нейронная сеть	5	3	17	63
Agnitum Outpost	4	80	16	458
BlackIce Firewall	2	57	11	340

ЗАКЛЮЧЕНИЕ

Увеличение объема данных внутри одного класса сильно влияет только на ошибки, но мало сказывается на требованиях к НС, а добавление новых классов приводит к росту оптимального размера НС, который однако оказывается меньшим, чем в случае анализа сигнатур, в которых затраты на обработку растут пропорционально числу проверяемых сигнатур, что косвенно подтверждается литературой [3].

Результаты работы демонстрируют широкие перспективы применения нейронных сетей в IDS. Малые требования к вычислительной мощности системы после завершения обучения позволяют использовать НС в системах обнаружения, работающих в реальном времени. Лучшая, чем у анализа сигнатур масштабируемость дает выигрыш в производительности для больших и разнородных сетей.

Ведется работа по созданию коммерческого продукта, практически реализующего результаты проведенных исследований.

Литература

1. *Bivens A., Palagiri C., Smith R., Szymanski B., Embrechts M.,* 2000 Network-Based Intrusion Detection Using Neural Networks
2. *Kumar, S. & Spafford, E., 1994 A,* Pattern Matching Model for Misuse Intrusion Detection.
3. *Planquart J.-P.,* 2001, «Application of Neural Networks to Intrusion Detection»