5. Чигарев, А.В. ANSYS для инженеров /А.В. Чигарев, А.С. Кравчук, А.Ф. Смалюк. – М.: Машиностроение-1, 2004.
6. Зенкевич, О. Конечные элементы и аппроксимация /О. Зенкевич, К. Морган. – М.: Мир, 1986.

КОМБИНИРОВАННЫЙ НЕЙРОСЕТЕВОЙ ПОДХОД ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ

П.А. Кочурко

Учреждение образования «Брестский государственный технический университет», Беларусь

Научный руководитель В.А. Головко

Технологии обнаружения атак в последнее время стали стандартным средством в инфраструктуре информационной безопасности предприятия. Существует множество различных подходов к обнаружению аномалий и злоупотреблений. В данной статье рассматривается использование рециркуляционных нейронных сетей для обнаружения аномалий и методы улучшения данной технологии с использованием смешанных тренировочных наборов данных.

1. Введение

Системы обнаружения атак (СОА) используются для обнаружения различных типов атак. Они объединяются с межсетевыми экранами и другими средствами обеспечения безопасности для того, чтобы своевременно оповещать персонал в случае обнаружения подозрительной активности. На текущий момент в обнаружении атак используются различные технологии [1], в том числе и искусственные нейронные сети (ИНС), которые показали многообещающие результаты во многих работах. ИНС имеют потенциал для решения множества проблем, существующих в применении современных подходов к обнаружению атак.

Существует две основных технологии обнаружения атак: обнаружение аномального поведения и обнаружение злоупотреблений. Для улучшения результатов обнаружения атак следует применять оба подхода в рамках одной СОА. Рассмотрим упрощенную схему СОА на рис. 1. Детектор аномалий производит «отсеивание» большей части нормального трафика, после чего оставшиеся соединения классифицируются и распознаются. Ранее было показано, что хороший уровень обнаружения атак может быть достигнут с применением ИНС как в детекторе аномалий, так и в модуле распознавания. В данной статье заостряется внимание на улучшении и развитии техники обнаружения, применяемой в детекторе аномалий.

Обучение и тестирование ИНС производилось на выборке KDD’99, содержащей записи о TCP-соединениях, включающих 41 параметр, полученные из обработанной базы данных DARPA 1998 Intrusion detection evaluation [2].

2. Обнаружение аномалий

Как было сказано выше, задачей детектора аномалий является обнаружение аномальной сетевой активности. Решение о типе поведения принимается на основании некоторой меры аномальности, которая может превысить заданный порог [3]. Мы используем рециркуляционную нейронную сеть (РНС) для нахождения данного значения. РНС – многослойная ИНС, производящая отображение своих входов в идентичные им выходы.

Трехслойные полносвязные нелинейные нейронные сети (рис. 2) с 41 входом и выходом и 50 нейронными элементами в скрытом слое с функциями активации ги-

перболический тангенс в скрытом слое и логистической в выходном обучены на обучающем наборе из нормальных соединений. Количество входов и выходов выбрано в соответствии с количеством параметров соединений в базе KDD: информация о соединении, поданная на вход РНС, должна быть восстановлена в том же виде на выходе сети.

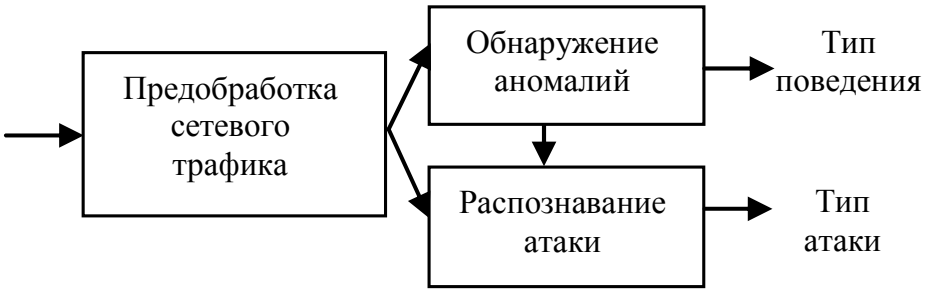

Рис. 1. Упрощенная структура СОА

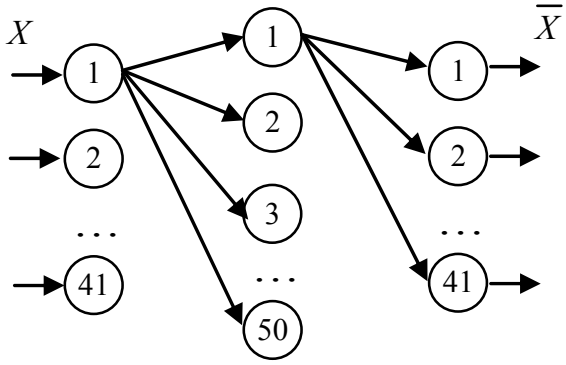

Рис. 2. Архитектура РНС

Ошибка реконструкции для одного входного образа используется в качестве меры аномальности данного соединения и определяется следующим образом:

$$E(k) = \frac{1}{n}\sum_{j=1}^{n}(\bar{X}_j - X_j)^2 , \qquad (1)$$

где X_j – значение *j*-го входа; $\bar{X}_j$ – значение *j*-го выхода; n – количество входов (равно 41). Если данная ошибка превышает заданный порог, то соединение помечается как «аномальное».

РНС обучались по методам послойного обучения и обратного распространения ошибки [4]. Тестирование обученных сетей производилось на тестовых наборах, содержащих нормальные соединения и атаки. Результаты для детектора «все службы» и отдельно HTTP, FTP_DATA и TELNET показаны в табл. 1. Значение порога выбиралось на основании минимизации суммы ошибок false positive и false negative.

3. Комбинированный подход

Две главных идеи хорошего обнаружения аномалий с использованием РНС: ошибка реконструкции нормального входного образа должна быть ниже порога, а ошибка реконструкции атаки – выше.

Достижение первой цели производится обучением нейронных сетей на нормальных образах по алгоритмам, которые минимизируют ошибку реконструкции. Для достижения второй цели мы не делали ничего: основывались на предположении, что атака, являясь аномалией, даст высокую ошибку реконструкции. Но иногда различие между нормальным и аномальным входными образами не настолько высоко, для того чтобы ошибка реконструкции превысила порог. А это приводит к ошибкам false negative.

Целью данного исследования было уменьшить количество ошибок false negative. Это означает, что нужно обучать РНС таким образом, чтобы аномальные входные образы приводили к более высоким ошибкам реконструкции. Обучение РНС только на нормальных соединениях не может привести к такому эффекту. Если же просто смешать нормальные и аномальные соединения, то количество ошибок false negative возрастет из-за того, что РНС будет трактовать аномальные соединения как нормальные.

Однако, если обучать РНС восстанавливать нормальные образы в аномальные, а атаки – в неравные им (все параметры умножены на некоторое k) выходы, цель будет достигнута. Мы обучаем РНС на следующих наборах данных: входы содержат равно нормальные и аномальные соединения; выходы содержат те же нормальные соединения и аномальные со значениями, умноженными на k. Цель обучения – минимизация среднеквадратичной ошибки между ожидаемыми и получаемыми выходами. При функционировании такой РНС ошибка реконструкции – мера аномальности – будет также считаться по (1). Однако входные образы с атаками уже будут давать на выходе не $\bar{X}$, а $k\bar{X}$ и ошибка реконструкции для данных образов будет:

$$E(k) = \frac{1}{n}\sum_{j=1}^{n}(k\bar{X}_j - X_j)^2, \qquad (2)$$

что выше, чем обычно.

Описанные в предыдущем разделе эксперименты повторены с использованием данного подхода (табл. 2). Тренировочные наборы данных содержат в 6 раз больше нормальных соединений, чем атак, выходы которых трансформируются в значения в k = 1,5 раза выше.

Таблица 1

Детектор аномалий

Служба	FP, %	FN, %
All	6,34	10,47
HTTP	0,30	0,10
FTP_DATA	2,00	8,09
TELNET	5,20	12,42

Таблица 2

Детектор аномалий излоупотреблений

Служба	FP, %	FN, %
All	8,16 (+1,80)	6,87 (-3,60)
HTTP	0,50 (+0,20)	0,06 (-0,04)
FTP_DATA	2,00 (0,00)	1,50 (-6,59)
TELNET	16,45 (+11,25)	1,92 (-10,5)

Видно, что цель – уменьшение количества ошибок false negative – достигнута, и только по сервису telnet ошибка false positive значительно изменилась.

4. Заключение

В данной статье описан нейросетевой подход к обнаружению аномалий. Показаны результаты экспериментов с использованием двух подходов – обучения на нормальных соединениях и комбинированных наборах данных. На основании данных результатов можно сделать вывод, что новый подход улучшает применявшуюся ранее технологию и может быть использован в дальнейших исследованиях.

Исследования проводятся при поддержке БРФФИ при НАН Беларуси.

Литература

1. S. T. Brugger. Data Mining Methods for Network Intrusion Detection. – http://www.bruggerink.com/ ~zow/Projects.html.
2. R. Lippman, J. Haines, D. Fried, J. Korba,, and K. Das, The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks, 34 (2000)* pp. 579-595.
3. S. Hawkins, H. He, G. Williams, R. Baxter. Outlier Detection Using Replicator Neural Networks. In *Proc. of the 4th International Conference on Data Warehousing and Knowledge Discovery (DaWaK02)* Lecture Notes in computer Science, Vol. 2454, Springer, Pages 170-180, ISBN 3-540-44123-9, 2002
4. V. Golovko, O. Ignatiuk, Yu. Savitsky, T. Laopoulos, A. Sachenko, L. Grandinetti. Unsupervised learning for dimensionality reduction. *Proc. of Second Int. ICSC Symposium on Engineering of Intelligent Systems EIS'2000*, University of Paisley, Scotland, June 2000. Canada / Switzerland: ICSS Academic Press, pp. 140 – 144, 2000

МАРКОВСКАЯ И ПОЛУМАРКОВСКАЯ МОДЕЛИ ОТКРЫТОЙ СЕТИ С ТРЕМЯ УЗЛАМИ

И.В. Гарбуза

Учреждение образования «Гомельский государственный университет имени Франциска Скорины», Беларусь

Научный руководитель Ю.В. Малинковский

Рассматриваются марковская и полумарковская модели открытой сети с тремя узлами, которые важны для информационных технологий и моделирования, так как предоставляют возможность для адекватного описания и анализа функционирования таких объектов, как телекоммуникационные сети, сети передачи данных, локальные сети, сети ЭВМ. Основной целью работы является исследование стационарного распределения сетей массового обслуживания, представление стационарного распределения исследуемых сетей в виде произведения, установление достаточных условий эргодичности, доказательство инвариантности стационарного распределения сетей.