ИЕРАРХИЧЕСКАЯ НЕЙРОСЕТЕВАЯ СИСТЕМА ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

УДК 004.8.032.26

Л.Ю. Войцехович, В.А. Головко
БрГТУ, г. Брест

Аннотация

В работе представлена иерархическая многоагентная система обнаружения атак в компьютерных сетях, описана ее структура и изложены основные результаты экспериментов. Отдельный агент представляет собой комбинацию нелинейной рециркуляционной нейронной сети и персептрона. Данная модель основана на многослойной архитектуре взаимодействия агентов, которая задается набором правил, представленных в виде графа. Модель может выполнять классификацию сетевых атак по классам и типам сетевой активности. Эксперименты свидетельствуют о том, что такое архитектурное решение позволяет сократить число ложных срабатываний, повысить точность распознавания и обнаруживать новые и модифицированные образы сетевых атак.

Введение

Безопасность компьютерных систем – одна из наиболее актуальных проблем современной индустрии информационных технологий. Ее актуальность постоянно возрастает, так как

с развитием информационного пространства увеличивается количество компьютерных атак и различных злоупотреблений в сфере высоких технологий, что увеличивает уязвимость компьютерных систем.

В настоящее время разрабатывается большое количество различных технологий защиты компьютерных сетей, которые базируются на применении нейронных сетей (neural networks), на технологиях извлечения данных (data mining), статистическом анализе и т.п. К недостаткам существующих технологий защиты, в первую очередь, можно отнести уязвимость к новым или неизвестным атакам, записи о которых отсутствуют в системе, низкая точность и скорость работы.

Существует две основные технологии обнаружения вторжений: обнаружение злоупотреблений и обнаружение аномалий. Обнаружение злоупотреблений (например, IDIOT [1] и STAT [2]) основано на использовании сигнатур о заранее известных атаках. Основным недостатком таких систем является их неспособность обнаруживать новые или неизвестные атаки, т.е. записи о которых в системе отсутствуют. Системы обнаружения аномалий [3] (например, система IDES [4]) идентифицируют атаку в случае значительного отклонения наблюдаемой сетевой активности от заданного профиля нормального поведения. Главным преимуществом таких систем является возможность определения ранее не встречавшихся атак, однако они характеризуются низкой точностью и скоростью работы.

Целью данной работы является разработка нейросетевой модели классификации для построения системы обнаружения сетевых атак (СОА) реального времени, способной обнаруживать модифицированные и неизвестные атаки, записи о которых изначально отсутствуют в базе данных системы. Предлагаемый подход базируется на нейросетевой иерархической многоагентной модели, где в качесве агента выступает детектор, состоящий из рециркуляционной нейронной сети и многослойного персептрона [5, 6, 7].

1 Архитектурное решение СОА

В работе в качестве основного агента (детектора) системы обнаружения атак предложена модель (рисунок 1), представляющая собой объединение нелинейной рециркуляционной нейронной сети (NPCA) и многослойного персептрона (MLP) [8]. В результате применения NPCA формируется сжатый набор исходных данных, который используются MLP непосредственно для выполнения классификации.

В результате специального объединения нейросетевых детекторов предложена иерархическая многоагентная система (рисунок 2) для обнаружения и классификации компьютерных атак. Такая система базируется на организации совместной работы заданного числа «интеллектуальных» агентов при помощи набора правил, которые задаются в виде направленного графа.

Рассматриваемая модель классификации включает три уровня, при чем каждый последующий уровень подтверждает или опровергает результаты, полученные детекторами на предыдущем этапе. Такая модель способна определить является ли входной образ нормальным соединением или это атака определенного класса. Кроме того, позволяет также установить тип атаки.

Результаты экспериментов демонстрируют возможности системы по обнаружению модифицированных образов сетевых атак. Кроме того, система способна обнаруживать новые атаки, если данные коррелируют с уже накопленными в ходе работы системы знаниями о злонамеренном трафике.

2 Результаты экспериментов

Для обучения и тестирования предложенной системы использовались данные, представленные в таблице 1. Сетевые вторжения, можно отнести к одному из четырех классов: DoS, Probe, U2R и R2L [9]: DoS – это атаки отказа в обслуживании, Probe – сканирование сети с целью обнаружения уязвимых хостов или служб, U2R-предполагает, что злоумышленник пытается получить привилегии root-а или администратора и, наконец, R2L – неавторизованный доступ со стороны удаленной машины. Каждая категория включает атаки различного типа.

В ходе экспериментов с базой сетевых атак [9], содержащей почти 500 тысяч записей о сетевой активности реальной компьютерной сети, подсчитывалась статистика обнаружения сетевых вторжений и распознавания записей. Распознавание выполняется на основании имеющейся у системы информации об атаках, образы которых были использованы на этапе обучения. Таким образом, часть данных применялась для настройки системы (обучения нейронных сетей) (см. таблицу 1), далее все данные (в том числе участвовавшие в обучении) подавались на многоагентный классификатор для тестирования системы.

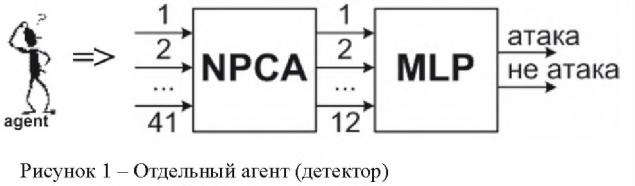

Рисунок 1 – Отдельный агент (детектор) для многоагентной системы

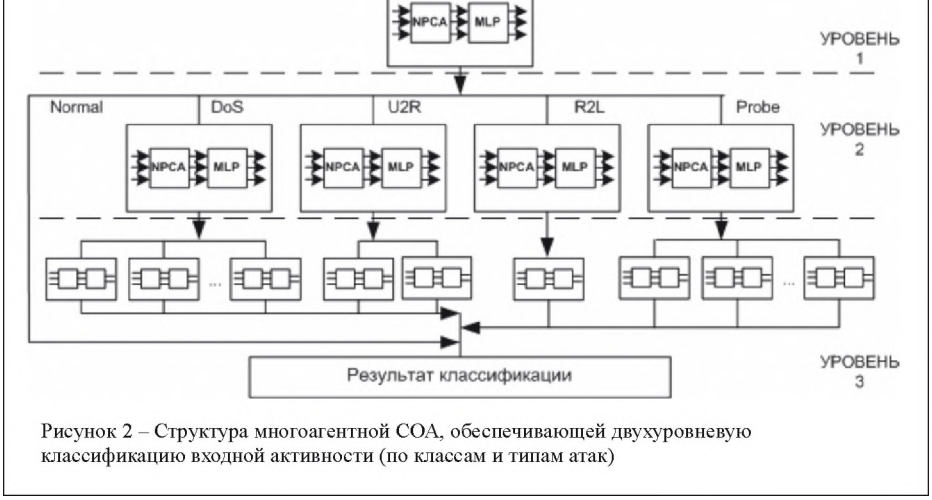

Рисунок 2 – Структура многоагентной СОА, обеспечивающей двухуровневую классификацию входной активности (по классам и типам атак)

Таблица 1 – Обучающая и тестовая выборки

	DoS	U2R	R2L	Probe	Normal	Итого
обучение	3571	37	278	800	1500	6186
тестирование	391 458	52	1126	4107	97 277	494 020

В таблице 2 отражены результаты распознавания детекторами второго уровня различных классов сетевой активности. Детекторы третьего уровня позволяют выявлять тип атаки.

Таблица 2 – Результаты обнаружения класса атаки

класс	кол-во	обнаружено	распознано
DoS	391 458	384 125 (98,13%)	370 658 (94,68%)
U2R	52	47 (90.39%)	45 (86.54%)
R2L	1126	1068 (94,85%)	1066 (94,67%)
Probe	4107	4056 (98,75)	4056 (98,75)

По сравнению с моделями, предложенными в [5, 6], предлженная система позволила повысить точность распознавания и снизить количество ошибок первого рода. Основные характеристики предложенной модели по обнаружению сетевых атак приведены на в таблице 3.

Таблица 3 – Результаты ROC анализа предложенной модели

чувствительность	специфичность	точность
0,98	0,96	0,98

Заключение

В данной работе была рассмотрена иерархическая многоагентная система обнаружения сетевых атак, которя базируется на объединении нейросетевых детекторов. Система может применяться для расширения возможностей современных коммерческих приложений защиты информационных систем, а также функционировать как отдельный модуль. Предложенный подход позволяет: выполнить двухуровневую классификацию как по классам, так и по типам сетевой активности; снизить количество ложных срабатываний благодаря формированию коллективного решения совокупностью детекторов; обнаруживать новые и модифицированные сетевые атаки.

Литература:

1. Kumar, S. A software architecture to support misuse intrusion detection / E.H. Spafford // In Proceedings of the 18th National Conference on Information Security. – 1995. – P. 194–204.

2. Ilgun, K. USTAT: A real-time intrusion detection system for Unix. Master's Thesis.University of California at Santa Barbara, Santa Barbara, CA – 1992.

3. Animesh Patcha, Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends // Computer Networks – 2007. – 51. – P. 3448–3470.

4. Lunt, T. Detecting intruders in computer systems // In Proceedings of the 1993 Conference on Auditing and Computer Technology. – 1993.

5. Golovko, V. Dimensionality Reduction and Attack Recognition using Neural Network Approaches / V. Golovko, L. Vaitsekhovich, P. Kochurko, U. Rubanau // In Joint Conference on Neural Networks (IJCNN-2007). – Orlando, FL, USA, 2007. – P. 2734–2739.

6. Vaitsekhovich, L. Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System / L. Vaitsekhovich, V. Golovko, U. Rubanau // In 10th International Conference on Pattern Recognition and Information Processing (PRIP-2009). – Minsk, Belarus, 2009. – P. 285–289.

7. Golovko, V. Neural Network and Artificial Immune System for Malware and Network Intrusion Detection / V. Golovko, S.Bezobrazov, P. Kachurka and L. Vaitsekhovich // Advanced in Machine Learning II. Springer Berlin Heidelberg. – 2010. – V. 263. – P. 485–513.

8. Головко, В.А. Нейронные сети: обучение, организация и применение: Кн. 4: учеб. пособие для вузов / В.А. Головко, общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.

9. 1999 KDD Cup Competition – Information on: http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html.

Abstract

In this article a hierarchical multi-agent model of intrusion detection system have been addressed. Its structure and operation algorithms are described. A single agent is represented by a combination of Nonlinear Principal Component Analysis Neural Network and Multi-layer Perceptron. The algorithm of agent interaction can be described with a directed graph. The model is able to perform a classification of network intrusions by classes as well as by types. Experiments indicate that the proposed model reduces the number of false positives, increases accuracy and can detect modified and even new attack instances.

Поступила в редакцию 18.05.2013 г.