УДК 004.056.53:004.492:004.89

М.П. Комар

Тернопольский национальный экономический университет, Тернополь

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ НА ОСНОВЕ МЕТОДА ГЛАВНЫХ КОМПОНЕНТ

Разработана интеллектуальная система обнаружения сетевых атак на информационные ресурсы, основным элементом которой является нейросетевой детектор. Приведена структура и метод обучения нейросетевых детекторов. Предложен способ улучшения качества обнаружения сетевых атак, основанный на применении метода главных компонент. Представлены результаты экспериментальных исследований.

Ключевые слова: *нейросетевой детектор, сетевая атака, метод главных компонент.*

Введение

На сегодняшний день сложилась ситуация, когда наиболее распространенные методы сигнатурного анализа для обнаружения вторжений или методы статистического анализа для выявления аномалий не способны на должном уровне обеспечить информационную безопасность. Компьютерные системы непрерывно подвергаются различного рода угрозам, и пользователь не может быть уверен в защищенности важной информации, поскольку киберпреступники продолжают совершенствовать и развивать методы и средства организации сетевых атак. Сложившаяся ситуация стимулирует поиск и разработку новых методов и решений, направленных на повышение уровня защищенности компьютерных систем от вредных воздействий.

В настоящее время все чаще используются эвристические методы, нейросетевые технологии и другие эволюционные механизмы, доказавшие свою эффективность в биологических системах. Значительное количество первых работ в данных направлениях показали серьезные научно-технические проблемы, существующие в развитии и реализации эволюционных подходов в задачах обнаружения вторжений в компьютерные системы.

Проведенный анализ известных методов обнаружения вторжений указал на необходимость решения и преодоления ряда сложных и актуальных научно-технических проблем, связанных с: непрерывным увеличением объемов памяти для хранения информации о вторжении, сложностью создания или выбора необходимых детекторов для обнаружения, значительными сложностями и затратами времени на вычисления, которые являются препятствием для обнаружения вторжений в реальном времени, высоким уровнем положительных ошибок и низким уровнем выявления.

Таким образом, разработка новых методов обнаружения вторжений в компьютерные системы, основанных на применении искусственных нейронных сетей, а также построение на их основе интеллектуальных систем обнаружения сетевых вторжений, что позволит повысить уровень защищенности компьютерных систем от несанкционированного воздействия, является актуальной и востребованной задачей.

Для увеличения скорости принятия решения в таких системах, а также для повышения качества обнаружения сетевых атак предложено применить метод главных компонент, что описано ниже.

Структура нейросетевого детектора для обнаружения сетевых атак

В [1 – 3] предложена система обнаружения сетевых вторжений, основанная на использовании метода нейронных сетей, и состоящая из нейросетевых детекторов, которые сканируют сетевой трафик с целью выявления его аномальности. В основе детектора лежит многослойная нейронная сеть с одним скрытым слоем, состоящим из нейронов Кохонена [4].

Первый слой нейронных элементов является распределительным и предназначен для распределения входных сигналов на нейроны скрытого слоя. Входными сигналами являются параметры сетевого соединения, которые характеризуют сетевой трафик и содержат информацию о времени соединения, типе протокола, количестве переданных байт, количестве возникновения ошибок во время соединения и т.д. Количество нейронных элементов распределительного слоя равняется количеству атрибутов сетевого трафика, т.е. n = 41.

Второй слой нейронной сети состоит из нейронов Кохонена [4]. Слой Кохонена играет ключевую роль в классификации данных и осуществляет кластеризацию входного пространства образов, в результате чего образуются кластеры различных образов, каждому из которых соответствует свой нейронный элемент. Для обучения нейронов скрытого слоя используется конкурентный принцип обучения в соответствии с правилом «победитель берет все» (winner-take-all) [4, 5]. Количество нейронов в слое Кохонена равняется m, которые связаны с двумя нейронами выходного слоя. Однако, особенностью предложенного нейросетевого детектора является то, что их количество разбито на две части: первые f нейронов слоя Кохонена соответствуют классу компьютерных атак и связаны с первым нейроном выходного слоя, а последние l нейронов соответствуют классу нормальных сетевых соединений и связаны со вторым нейроном выходного слоя.

Модифицированный нейросетевой детектор для анализа сетевого трафика представлен на рис. 1.

Третий слой состоит из двух линейных нейронных элементов, которые используют линейную функцию активацию [5] и осуществляют отображение кластеров, сформированных слоем Кохонена, в два класса, которые характеризуют нормальное соединение или атаку. Активность выходного нейрона, когда значение его равно единице, характеризует аномальный сетевой трафик, т.е. атаку. Ноль же на выходе характеризует нормальное, легитимное соединение.

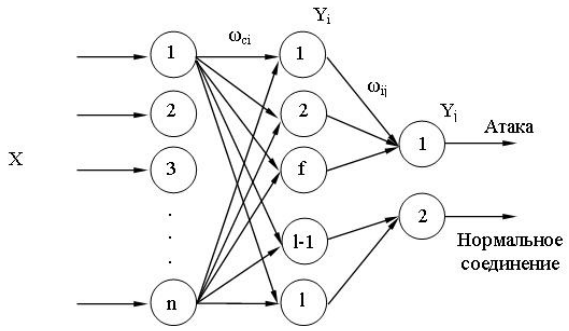

Рис. 1. Модифицированный нейросетевой детектор для обнаружения сетевых атак

В общем случае, выходное значение j-го нейрона третьего слоя определяется следующим образом:

$$Y_j = \sum_{i=1}^{m} \omega_{ij} \cdot Y_i,$$

где ω_{ij} – весовой коэффициент между i-м нейроном слоя Кохонена и j-м нейроном линейного слоя.

Если нейрон-победитель в слое Кохонена имеет номер k, то выходное значение j-го нейрона третьего слоя равняется

$$Y_j = \omega_{kj} \cdot Y_k .$$

Особенностью представленного детектора является то, что нейроны в скрытом слое разделены на две группы: первая группа характеризует класс сетевых соединений, относящихся к компьютерным атакам; вторая группа нейронов характеризует класс нормальных соединений.

Метод обучения нейросетевого детектора для обнаружения сетевых атак

Поскольку предлагаемый нейросетевой детектор содержит скрытый слой, состоящий из нейронов Кохонена, то для обучения такой сети применяется контролируемое конкурентное обучение [5] в соответствии с правилом «победитель берет все». Суть данного метода обучения заключается в том, что в процессе обучения происходит конкуренция между нейронными элементами слоя Кохонена, в результате чего определяется нейронный элемент-победитель, который и характеризует принадлежность к тому или иному классу предъявляемых данных. Для выявления нейрона-победителя может использоваться Евклидово расстояние, или расстояние Хэмминга и т.д. В процессе обучения синаптические связи для нейрона-победителя усиливаются, а для остальных нейронов не изменяются. Таким образом, после обучения нейронной сети, при подаче входного образа активность нейрона-победителя принимается равной единице, а остальные нейроны «сбрасываются» в ноль.

Так как в слое Кохонена используется разделение нейронов по классам, которые характеризуют

либо легитимное соединение, либо сетевую атаку, то корректная классификация происходит в том случае, когда при подаче на вход нейронной сети параметров соединения, относящемуся к классу компьютерной атаки, победителем является один из f нейронов слоя Кохонена, или, если при подаче на вход нейронной сети параметров нормального соединения победителем является один из l нейронов слоя Кохонена. В остальных случаях происходит некорректная классификация.

В результате методика обучения слоя Кохонена выглядит следующим образом:

1. Случайная инициализация весовых коэффициентов ω_{ci} нейронов Y_i слоя Кохонена.

2. Распределение входного образа (вектор, состоящий из 41 значений параметров сетевого соединения) из обучающей выборки на нейронную сеть и вычисление следующих параметров:

a) вычисляется Евклидово расстояние между входным образом и весовыми векторами нейронных элементов слоя Кохонена

$$D_i = |X - \omega_i| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + \ldots + (X_n - \omega_{ni})^2},$$

где i = 1,m;

b) определяется нейронный элемент победитель с номером k:

$$D_k = \min_j D_j;$$

c) производится модификация весовых коэффициентов нейрона-победителя. Причем, если при подаче на вход нейронной сети параметров сетевой атаки победителем является один из f нейронов, или, если при подаче на вход нейронной сети параметров нормального сетевого соединения победителем является один из l нейронов слоя Кохонена, то модификация весовых коэффициентов производится согласно следующему выражению:

$$\omega_{ck}(t+1) = \omega_{ck}(t) + \gamma(X_c - \omega_{ck}(t)),$$

где γ – шаг обучения.

В противном случае весовые коэффициенты нейронов слоя Кохонена модифицируются согласно выражению:

$$\omega_{ck}(t+1) = \omega_{ck}(t) - \gamma(X_c - \omega_{ck}(t)).$$

3. Процесс повторяется, начиная с пункта 2 для всех входных образов.

4. Обучение производится до желаемой степени согласования между входными и весовыми векторами.

Для обучения предложенного нейросетевого детектора используется обучающая выборка, состоящая из 80% соединений одного из типов атак и 20% нормального соединения. Такое соотношение было получено экспериментальным путем и показало наилучшие результаты классификации сетевого трафика. Также отметим, что наилучший результат в классификации сетевого трафика показали детекторы, в которых нейроны скрытого слоя также имеют отношение в разделении по классам, равное четыре к одному.

Улучшение качества обнаружения сетевых атак на основе метода главных компонент

В системе используются 22 детектора – по одному на каждый из классов сетевой атаки [6]. Весь сетевой трафик характеризуется 41 параметром соединения [7]. Выполненный анализ сетевого трафика показал, что указанная совокупность параметров несет в себе весьма избыточную информацию. В принципе можно игнорировать некоторые параметры соединения и добиться при этом увеличения скорости принятия решения, и за счет этого – повышения качества обнаружения сетевых атак.

Для нахождения параметров, которые несут в себе наибольшую значимую информацию, предложено использовать метод главных компонент [8], который позволяет уменьшить размерность данных с потерей наименьшего количества информации. При этом вычисление главных компонент сводится к нахождению собственных векторов и собственных значений ковариационной матрицы исходных данных.

Применение метода главных компонент для уменьшения размерности данных, описывающих сетевой трафик, показало, что в 11 главных компонентах содержится 99% информации о сетевом соединении [9]. Распределение информативности о сетевом соединении в зависимости от компоненты представлено в табл. 1.

Как видно из табл. 1, 41 параметры, описывающие сетевой трафик, по своей структуре избыточны, и для того, чтобы описать сетевой трафик, достаточно 11 – 20 главных компонент, в которых хранится 99,00 – 99,90 процентов информации. Таким образом, выглядит целесообразным применять данное преобразование данных перед тем, как их анализировать с помощью нейронных сетей.

Графическое отображение распределения в пространстве главных компонент для различных типов атак и нормального соединения иллюстрируется рис. 2.

Как видно из графиков, пространственное распределение атак (обведены линией) локально отличается от пространственного распределения нормальных соединений.

Результаты экспериментальных исследований показали, что при использовании метода главных компонент для предобработки данных о сетевом соединении качество обнаружения значительно улучшилось. Полученные результаты представлены в табл. 2 – 5.

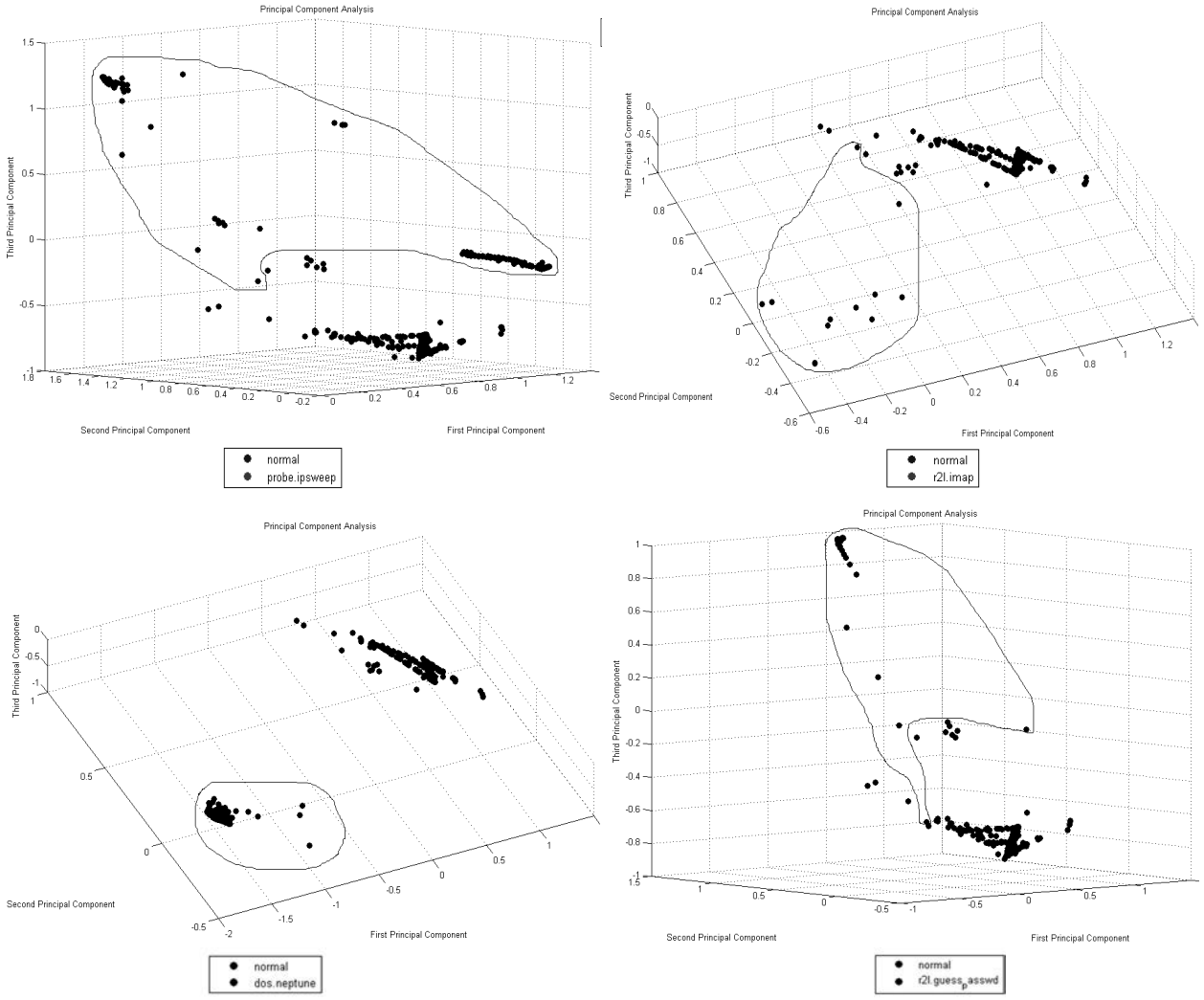

Рис. 2. Распределение главных компонент

Таблица 1

Распределение информации по компонентам

Номер компоненты	1	2	3	4	5	6
Количество информации, %	52,40	71,67	88,37	91,49	94,21	95,90
Номер компоненты	7	8	9	10	11	12
Количество информации, %	96,96	97,71	98,27	98,73	99,00	99,18
Номер компоненты	13	14	15	16	17	18
Количество информации, %	99,33	99,47	99,59	99,67	99,75	99,81
Номер компоненты	19	20	21	22	23	24
Количество информации, %	99,87	99,90	99,93	99,94	99,95	99,96
Номер компоненты	25	26	27	28	29	30
Количество информации, %	99,97	99,98	99,98	99,99	99,99	99,99
Номер компоненты	31	32	33	34	35	36
Количество информации, %	99,99	99,99	99,99	99,99	99,99	99,99
Номер компоненты	37	38	39	40	41	
Количество информации, %	99,99	100	100	100	100	

Таблица 2

Результаты обнаружения DoS-атак

Back, %	Land, %	Neptune, %	Pod, %	Smurf, %	Teardrop, %
99,5	100,0	100,0	98,1	100,0	100,0
Среднее = 99,6%					

Таблица 3

Результаты обнаружения Probe-атак

Ipsweep, %	Nmap, %	Portsweep, %	Satan, %
65,2	100,0	99,9	99,3
Среднее = 91,1%			

Таблица 4

Результаты обнаружения R2L-атак

Ftp_write, %	Guess_passwd, %	Imap, %	Multihop, %
100,0	94,3	83,3	57,1
Warezclient, %	Warezmaster, %	Phf, %	Spy, %
65,0	90,0	100,0	100,0
Среднее = 86,2%			

Таблица 5

Результаты обнаружения U2R-атак

Buffer_ overflow, %	Loadmodule, %	Perl, %	Rootkit, %
83,3	100,0	33,3	30,0
Среднее = 61,7%			

Выводы

Как видно из полученных результатов, качество обнаружения удалось значительно увеличить благодаря применению метода главных компонент к параметрам сетевого трафика. Так прирост в качестве обнаружения в среднем для DoS-атак составил 1,6 %, для Probe-атак составил 6,0%, для R2L-атак составил 49,3%, для U2R-атак составил примерно 41%.

Следует отметить, что процент возникновения ложного обнаружения составляет менее 1,7%. Также за счет того, что для анализа сетевого трафика теперь используются только 12 главных компонент, а не все 41 параметр, удалось повысить быстродействие системы в целом, что является важным критерием для систем защиты информации.

Однако, некоторые типы атак, такие как ipsweep, multihop, warezclient, perl и rootkit, разработанной системой недостаточно хорошо обнаруживаются. Для преодоления этого недостатка, а также для усовершенствования модели предлагается применить метод искусственных иммунных систем.

Список литературы

1. *Комар М.П. Система анализа сетевого трафика для обнаружения компьютерных атак / М.П. Комар // Вестник Брестского государственного технического университета: (Серия: физика, математика и информатика). – 2010. – №5. – С. 14-16.*
2. *Комар М.П. Методы искусственных нейронных сетей для обнаружения сетевых вторжений / М.П. Комар // Сборник тезисов седьмой международной научно-технической конференции "Интернет – Образование – Наука " (ИОН-2010) – Винница: Винницкий национальный технический университет, 2010. – С. 410-413.*
3. *Комар М.П. Интеллектуализированная информационная технология обнаружения компьютерных атак / М.П. Комар, Д.И. Боднар, А.А. Саченко // Измерительная и вычислительная техника в технологических процессах. – 2010. – № 2. – С. 133-137.*
4. *Kohonen T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. – 1982. – № 43. – P. 59-69.*
5. *Головко В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение: учеб. пос. / В.А. Головко. – М., 2001. – 256 с.*
6. *Mahbod Tavallaee. A Detailed Analysis of the KDD CUP 99 Data Set / Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, Ali, A. Ghorbani // Proceedings of the 2009 IEEE Symp. Computational Intelligence in Security and Defense Applications (CISDA 2009). DOI: 10.1109/CISDA.2009.5356528. Publication Year: 2009, Page(s): 1-8.*
7. *KDD Cup 1999 Data [Электронный ресурс]. – Режим доступа к ресурсу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.*
8. *Gorban. Principal Manifolds for Data Visualisation and Dimension Reduction / Gorban, B. Kegl, D. Wunsch, A. Zinovyev (Eds.) – LNCSE 58, Springer, Berlin – Heidelberg – New York, 2007.*
9. *Комар М.П. Использование метода главных компонент для решения задачи обнаружения компьютерных атак / М.П. Комар // Сборник тезисов третьей международной научно-практической конференции «Методы и средства кодирования, защиты и уплотнения информации». – Винница, 2011. – С. 131-132.*

Поступила в редколлегию 8.11.2011

Рецензент: д-р техн. наук, проф. Я.Н. Николайчук, Тернопольський национальный экономический университет, Тернополь.

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ НА ОСНОВІ МЕТОДУ ГОЛОВНИХ КОМПОНЕНТ

М.П. Комар

Розроблено інтелектуальну систему виявлення мережевих атак на інформаційні ресурси, основним елементом якої є нейромережевий детектор. Наведено структуру і метод навчання нейромережевих детекторів. Запропоновано спосіб поліпшення якості виявлення мережевих атак, заснований на застосуванні методу головних компонент. Представлені результати експериментальних досліджень.

Ключові слова: *нейромережевий детектор, мережева атака, метод головних компонент.*

INTELLIGENT SYSTEM FOR DETECTING NETWORK ATTACKS ON THE INFORMATION RESOURCES THAT ARE BASED ON THE PRINCIPAL COMPONENT ANALYSIS

M.P. Komar

The intelligent system of Intrusion Detection on the information resources is developed, the main element of which is the neural detector. The structure and method of neural detectors training are presented. A method for improving the detection of network attacks is proposed, that is based on the method of principal components analysis. The results of experimental studies are presented.

Keywords: *neural network detector, network attacks, the method of principal components analysis.*