ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 004.891.3
DOI: 10.17586/0021-3454-2016-59-10-795-800

МОНИТОРИНГ И ПРОГНОЗИРОВАНИЕ СОСТОЯНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ПРИМЕНЕНИЯ ГИБРИДНЫХ НЕЙРОННЫХ СЕТЕЙ

И. Б. Саенко[1], Ф. А. Скорик[2], И. В. Котенко[1]

[1]*Санкт-Петербургский институт информатики и автоматизации Российской академии наук, 199178, Санкт-Петербург, Россия*
E-mail: ibsaen@comsec.spb.ru
[2]*Военная академия связи им. С. М. Буденного, 194064, Санкт-Петербург, Россия*

Для мониторинга и прогнозирования состояния компьютерных сетей необходимо использовать средства, характеризующиеся высокой адаптивностью и устойчивостью к внешним шумам. Такими особенностями обладают гибридные нейронные сети. Рассматриваются основанные на гибридных нейронных сетях модели, позволяющие оценивать и прогнозировать состояние компьютерных сетей. Результаты проведенных экспериментов показали, что предложенные модели обеспечивают высокую точность классификации текущего и прогнозируемого состояния компьютерной сети.

Ключевые слова: *гибридные нейронные сети, карта Кохонена, прогнозирование, мониторинг, показатель состояния*

В настоящее время мониторинг и прогнозирование состояния компьютерных сетей — важнейшие компоненты сетевого администрирования [1, 2]. Однако высокая динамика и нелинейность процессов, протекающих в современных компьютерных сетях, а также сложность структурных связей между узлами сети определяют необходимость использовать для оценки состояния средства, имеющие высокую адаптивность и устойчивость к внешним шумам. В качестве таких средств могут использоваться гибридные, т.е. искусственные, применяющие символьные вычисления, нейронные сети [3, 4]. Гибридная нейронная сеть выполняет логический вывод на основе аппарата нечеткой логики, приобретает новые знания и использует их в дальнейшей работе. Подобные системы мониторинга успешно используются во многих областях (машинное обучение, распознавание лиц, медицина, обработка сигналов и т.д.) [5—8], они позволяют получить нужные результаты без участия человека и с небольшими вычислительными затратами.

Целью настоящей статьи является разработка и экспериментальная оценка моделей, предназначенных для мониторинга и прогнозирования состояния компьютерных сетей, основанных на комбинации самообучающихся и гибридных нейронных сетей.

Анализ показал, что в большинстве случаев области применения гибридных нейронных сетей как элементов систем мониторинга, удаленного контроля и администрирования сильно ограничены.

Так, в статьях [9, 10] рассматриваются вопросы реализации экспертных и самообучающихся систем, базирующихся на алгоритмах нечеткой логики и гибридных нейронных сетях. Основным недостатком предложенных решений является необходимость в существенных

временных, интеллектуальных и вычислительных затратах, что не всегда возможно и целесообразно.

В работах [11—14] предлагаются системы идентификации, выявления вторжений и аномального поведения пользователей, в которых используются модели гибридных нейронных сетей. Для функционирования этих достаточно простых в реализации систем не требуются значительные вычислительные ресурсы. Однако общим их недостатком является отсутствие возможности прогнозировать последствия воздействия выявленных аномалий, а также ограниченные возможности по интерпретации полученных результатов.

В статье [15] предлагается подход к прогнозированию состояния сетевых элементов на основе комбинирования вероятностной и обычной многослойной нейронных сетей. Комбинирование нейронных сетей различных типов позволяет существенно уменьшить время на обучение нейросетевой системы, однако недостатком этого подхода является низкая устойчивость к воздействию шумов на исходные данные, что характерно для реальных компьютерных сетей.

Полученные в работах [16, 17] результаты по реализации динамических эволюционных систем с нечеткой логикой позволяют производить адаптивное обучение в режиме времени, приближенном к реальному, и прогнозировать тенденции изменения входных параметров системы с течением времени. Однако для оценки состояния компьютерной сети такой подход достаточно сложен и не всегда приемлем.

Таким образом, анализ релевантных работ показывает, что гибридные нейронные сети обладают большими возможностями для решения поставленной задачи. В то же время известные модели гибридных нейронных сетей не могут быть напрямую использованы для этой цели.

На рис. 1 представлена обобщенная схема разработанной модели мониторинга состояния компьютерной сети.

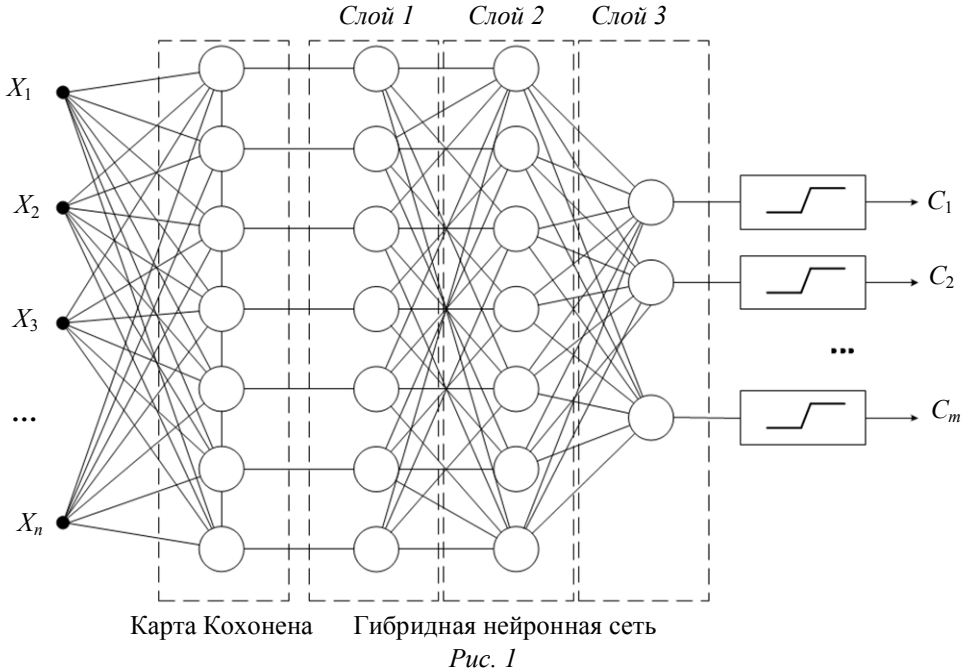

Рис. 1

В модели объединены две искусственные нейронные сети: самоорганизующаяся карта Кохонена и трехслойная гибридная нейронная сеть. Для фильтрации полученных на выходах гибридной нейронной сети значений показателей состояния и определения выходного класса (C_1, C_2, ..., C_m), соответствующего текущему состоянию компьютерной сети, используются блоки, реализующие ступенчатую функцию с заданным порогом активации.

В качестве исходных данных (X_1, X_2, ..., X_n) могут выступать значения показателей, полученные от клиентских приложений, результаты анализа сетевого трафика и накопленная статистическая информация.

Карта Кохонена используется для первоначальной сортировки и кластеризации поступающих значений, она обеспечивает структуризацию исходных данных для гибридной нейронной сети [18]. Гибридная нейронная сеть позволяет определить степень принадлежности совокупности значений показателей на своих входах определенному, ранее заданному классу, характеризующему текущее состояние компьютерной сети.

Функционирование модели предполагает:

1) кластеризацию значений показателей;

2) обработку полученных значений при помощи гибридной нейронной сети;

3) фильтрацию полученных значений и выделение целевого класса, определяющего текущее состояние компьютерной сети.

Следовательно, имея на входе рассмотренной модели определенную совокупность значений показателей, можно однозначно интерпретировать ее выходные значения как оценку текущего состояния компьютерной сети.

В отличие от рассмотренной выше модели, в предлагаемой модели прогнозирования состояния компьютерной сети (рис. 2) к выходам гибридной нейронной сети дополнительно подключен многослойный персептрон. Целесообразность использования этой нейронной сети определяется тем, что она имеет простую структуру и легко обучается, при этом точность выходных данных высока.

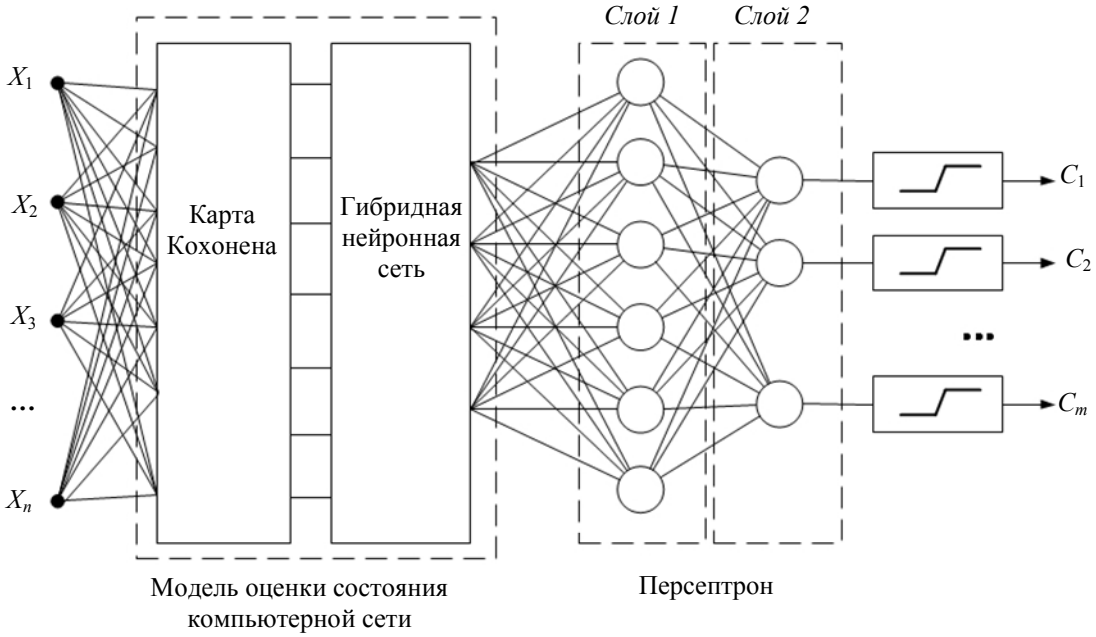

Рис. 2

Персептрон в модели играет роль модуля прогнозирования. Он получает на входы результаты работы гибридной нейронной сети, определяющие по совокупности показателей текущее состояние компьютерной сети. Затем он формирует на выходах прогнозные значения, отражающие принадлежность состояния сети к предопределенному классу состояний через заданный интервал времени.

Выступающие в качестве исходных данных значения показателей (X_1, X_2, ..., X_n) аналогичны значениям, рассмотренным в модели для мониторинга состояния компьютерной сети.

Результаты прогнозирования фильтруются блоками, реализующими ступенчатую функцию с заданным порогом активации. Тем самым обеспечивается определение одного из

результирующих классов (C_1, C_2, ..., C_m), характеризующих прогнозируемое состояние компьютерной сети.

Функционирование модели предполагает:

1) кластеризацию значений показателей;

2) обработку полученных значений при помощи гибридной нейронной сети;

3) формирование прогноза на основе выходных значений гибридной нейронной сети;

4) фильтрацию полученных значений и выделение целевого класса, определяющего прогнозируемое состояние компьютерной сети.

В результате по совокупности значений показателей на входе модели можно однозначно интерпретировать прогнозируемое состояние компьютерной сети через заданный интервал времени.

Экспериментальная оценка предложенных моделей мониторинга и прогнозирования состояния компьютерной сети осуществлялась для компьютерной сети, включающей в себя сервер баз данных, файловый сервер и десять рабочих станций.

Эксперименты проводились по следующей схеме. Первоначально накапливалась статистическая информация о значениях выбранных показателей, которая в виде временных рядов сохранялась в объеме, достаточном для корректного обучения искусственных нейронных сетей, входящих в состав моделей. После этого структура моделей формировалась в соответствии с конфигурацией сети и числом контролируемых показателей с последующим обучением искусственных нейронных сетей. Выходам каждой модели задавалось определенное число классов, каждый из которых соответствовал определенному, строго заданному состоянию компьютерной сети.

При обучении гибридной нейронной сети и многослойного персептрона использовался алгоритм обратного распространения ошибки. В результате тестирования было выявлено, что по сравнению с многослойным персептроном гибридная нейронная сеть в процессе обучения имеет более высокую точность и требует меньшего числа обучающих итераций. По завершении обучения искусственных нейронных сетей модели, предназначенные для мониторинга и прогнозирования состояния компьютерных сетей, полностью готовы к эксплуатации.

Результаты 320 проведенных тестовых опросов представлены в таблице. Класс C_1 соответствует состоянию, при котором все узлы нормально функционируют, а обмен информацией по сети минимален или отсутствует; в C_2 имеет место интенсивный сетевой обмен локальных узлов с сервером базы данных, а C_3 свойственна интенсивная работа пользователей с файловым сервером.

Класс	Оценка состояния		Прогнозирование состояния	
	число тестов	доля ошибки, %	число тестов	доля ошибки, %
1	87	1,7	91	2,5
2	122	4,8	128	7,2
3	111	2,2	101	3,4

Как видно из таблицы, предложенные модели мониторинга и прогнозирования состояния компьютерной сети обеспечивают высокую достоверность на этапе принятия решения. Максимальная ошибка классификации состояния компьютерной сети в первой модели не превышает 4,8 %, а во второй — не более 7,2 %. При этом соблюдается закономерность: классу, включающему большее число тестов, соответствует бóльшая ошибка классификации. Таким образом, полученные экспериментальные результаты свидетельствуют о высокой эффективности предложенных моделей.

Учитывая простоту структуры предложенных моделей и минимальные требования к используемым ими вычислительным ресурсам, можно сделать вывод, что эти модели могут

успешно применяться в системах удаленного контроля и мониторинга для компьютерных сетей произвольной конфигурации.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. *Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Тр. СПИИРАН. Вып. 1 (20). СПб: Наука, 2012. С. 27—56.
2. *Котенко И. В., Саенко И. Б.* К новому поколению систем мониторинга и управления безопасностью // Вестн. Российской академии наук. 2014. Т. 84, № 11. С. 993—1001.
3. *Awan Z. K., Khan A., Iftikhar A.* Hybrid Neural Networks: from Application Point of View. LAP Lambert Academic Publishing, 2012.
4. *Wermter S., Sun R.* An overview of hybrid neural systems // Hybrid Neural Systems. NY—Heidelberg: Springer, 2000.
5. *Chen Y., Kak S., Wang L.* Hybrid neural network architecture for on-line learning // Intelligent Information Management. 2010. Vol. 2. P. 253—261.
6. *Lawrence S., Giles C. L., Tsoi A. C., Back A. D.* Face Recognition: A Hybrid Neural Network Approach: Technical Report. 1996.
7. *Wan L., Zhu L., Fergus R.* A Hybrid neural network-latent topic model // Proc. of the 15th Intern. Conf. on Artificial Intelligence and Statistics (AISTATS). La Palma, Canary Islands, 2012. Vol. 22. P. 1287—1294.
8. *Psichogios D. C., Ungar L. H.* A Hybrid Neural Network-First Principles Approach to Process Modeling // AIChE J. 1992. Vol. 38, N 10. P. 1499—1511.
9. *Azruddin A., Gobithasan R., Rahmat B., Azman S., Sureswaran R.* A hybrid rule based fuzzy-neural expert system for passive network monitoring // Proc. of the Arab Conf. on Information Technology ACIT. 2002. P. 746—752.
10. *Mishra A., Zaheeruddin Z.* Design of hybrid fuzzy neural network for function approximation // J. of Intelligent Learning Systems and Applications. 2010. Vol. 2, N 2. P. 97—109.
11. *Bahrololum M., Salahi E., Khaleghi M.* Anomaly intrusion detection design using hybrid of unsupervised and supervised neural network // Intern. J. of Computer Networks & Communications (IJCNC). 2009. Vol. 1, N 2. P. 26—33.
12. *Garcıa-Teodoro P., Dıaz-Verdejo J., Macia-Fernandez G., Vazquez E.* Anomaly-based network intrusion detection: Techniques, systems and challenges // Computers & Security. 2009. Vol. 28. P. 18—28.
13. *Zhang Z., Manikopoulos C.* Neural networks in statistical anomaly intrusion detection // J. of Neural Network World. 2001. Vol. 3. P. 305—316.
14. *Souza L. G. M., Barreto G. A.* Nonlinear system identification using local arx models based on the self-organizing map. Learning and Nonlinear Models // Revista da Sociedade Brasileira de Redes Neurais (SBRN). 2006. Vol. 4, N 2. P. 112—123.
15. *Kotenko I., Saenko I., Skorik F., Bushuev S.* Neural network approach to forecast the state of the internet of things elements // Proc. of the XVIII Intern. Conf. on Soft Computing and Measurements (SCM'2015), IEEE Xplore. 2015. P. 133—135, DOI: 10.1109/SCM.2015.7190434.
16. *Kasabov N., Hamed H. N. A.* Quantum-inspired particle swarm optimization for integrated feature and parameter optimization of evolving spiking neural networks // Intern. J. of Artificial Intelligence. 2011. Vol. 7. P. 114—124.
17. *Kasabov N. K., Song Q.* DENFIS: Dynamic evolving neuro-fuzzy inference system and its application for time-series prediction // IEEE Transactions on Fuzzy Systems. 2002. Vol. 10(2). P. 144—154.
18. *Kohonen T.* The self-organizing map // Proc. of the IEEE. 1990. Vol. 78, N 9. P. 1464—1480.

Сведения об авторах

Игорь Борисович Саенко — д-р техн. наук, профессор; Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; E-mail: ibsaen@mail.ru

Фадей Александрович Скорик — канд. техн. наук; Военная академия связи им. С. М. Буденного; кафедра автоматизированных систем специального назначения; E-mail: work_bk@bk.ru

Игорь Витальевич Котенко — д-р техн. наук, профессор; Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; E-mail: ivkote@comsec.spb.ru

Рекомендована СПИИРАН

Поступила в редакцию
18.04.16 г.

Ссылка для цитирования: *Саенко И. Б., Скорик Ф. А., Котенко И. В.* Мониторинг и прогнозирование состояния компьютерных сетей на основе применения гибридных нейронных сетей // Изв. вузов. Приборостроение. 2016. Т. 59, № 10. С. 795—800.

MONITORING AND FORECASTING COMPUTER NETWORK STATE BASED ON THE USE OF HYBRID NEURAL NETWORKS

I. B. Saenko[1], F. A. Skorik[2], I. V. Kotenko[1]

[1]*St. Petersburg Institute for Informatics and Automation of the RAS,*
199178, St. Petersburg, Russia
E-mail: ibsaen@comsec.spb.ru

[2]*S. M. Budenny Military Academy of Telecommunications,*
194064, St. Petersburg, Russia

Application of for computer networks state monitoring and forecasting based on high adaptability and resistance of hybrid neural networks to external noise is considered. Models for monitoring and forecasting of computer network states using hybrid neural networks are analyzed. Results of experiments demonstrate that the proposed models afford a rather high precision of classification of current and predicted states of computer network.

Keywords: hybrid neural networks, Kohonen map, computer networks, forecasting, monitoring, state indicator

Data on authors

Igor B. Saenko — Dr. Sci., Professor; St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; E-mail: ibsaen@mail.ru

Fadey A. Skorik — PhD; S. M. Budenny Military Academy of Telecommunications; Department of Automated Control Systems for Special Purposes; E-mail: work_bk@bk.ru

Igor V. Kotenko — Dr. Sci., Professor; St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; E-mail: ivkote@comsec.spb.ru

For citation: *Saenko I. B., Skorik F. A., Kotenko I. V.* Monitoring and forecasting computer network state based on the use of hybrid neural networks // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 10. P. 795—800 (in Russian).

DOI: 10.17586/0021-3454-2016-59-10-795-800