ОБНАРУЖЕНИЕ И РАСПОЗНАВАНИЕ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ РЕЦИРКУЛЯЦИОННЫХ НЕЙРОННЫХ СЕТЕЙ

УДК 004.8.032.26

П.А. Кочурко,
БрГТУ, г. Брест

Аннотация

Представлены подходы к обнаружению и распознаванию сетевых атак с использованием рециркуляционных нейронных сетей. Реализованы технологии обнаружения аномалий и обнаружения злоупотреблений, объединение которых в рамках единого подхода позволяет получить высокую степень защищенности компьютерных систем. Приводятся экспериментальные результаты, подтверждающие эффективность технологии.

Введение

Технологии обнаружения атак – важное звено в цепи средств обеспечения информационной безопасности,

противостоящих угрозам реализации уязвимостей. Каждая вторая организация в течение 2009–2010 годов зафиксировала различные атаки на свои информационные ресурсы, а 45,6 % из них подверглись целенаправленному нападению [1]. В 2011 году глобальный ущерб от атак на компьютерные информационные технологии превысил 250 млрд долл. США в год [2].

Основными недостатками существующих подходов к обнаружению атак (в первую очередь – на основе правил) являются: слабая способность обнаружения новых, неизвестных ранее или модифицированных атак; недостаточно высокая степень адаптивности; необходимость постоянного обновления баз правил, а значит – зависимость качества функционирования системы от компании-разработчика и качества сигнатур, полученных от поставщика.

Исследователи обращаются к большому количеству технологий (статистический анализ, деревья решений, искусственные иммунные системы, нечеткая логика и др.), среди которых стоит выделить подходы на основе искусственных нейронных сетей (ИНС), поскольку они сочетают высокое качество распознавания и классификации со способностью к адаптации и обобщению данных. В данной работе предлагается новое решение задачи обнаружения и распознавания сетевых атак на основе нелинейных рециркуляционных нейронных сетей (РНС). Оно объединяет в едином подходе парадигмы обнаружения аномалий и обнаружения некорректного поведения для лучшего распознавания известных атак и обнаружения новых и модифицированных сетевых атак.

РНС как детектор далеко отстоящих векторов

Рециркуляционные нейронные сети отличаются от других ИНС тем, что информация, подающаяся на вход, в том же виде восстанавливается на выходе. В процессе обучения весовые коэффициенты РНС настраиваются таким образом, чтобы минимизировать среднеквадратичную ошибку для всех тренировочных входных векторов. Итогом такого обучения станет то, что в процессе функционирования РНС подаваемые на вход векторы будут восстанавливаться на выходе тем более точно, чем больше они схожи с векторами из тренировочного набора. Далеко отстоящие векторы, в свою очередь, будут восстанавливаться недостаточно корректно.

Численная характеристика, которая позволяет судить о том, насколько данный входной вектор «похож» или «не похож» на вектор из тренировочного набора – ошибка реконструкции вектора:

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

где $N(X)$ – количество параметров во входном векторе X (ранг первого и последнего слоев РНС). При этом, чем меньше ошибка реконструкции (1), тем больше входной вектор похож на векторы тренировочного набора.

РНС-детекторы атак и их совместное функционирование

В рамках СОА детекторы на базе нелинейных РНС могут использоваться в разных ролях в зависимости от того, на каком наборе данных они обучены.

Детектор аномалий. При обучении на нормальном трафике в автоматическом режиме РНС-детектор получает и сохраняет для дальнейшего использования информацию о явных и неявных закономерностях поведения. В процессе функционирования такой детектор определяет соединения, не принадлежащие к классу нормальных, то есть атаки (рисунок 1).

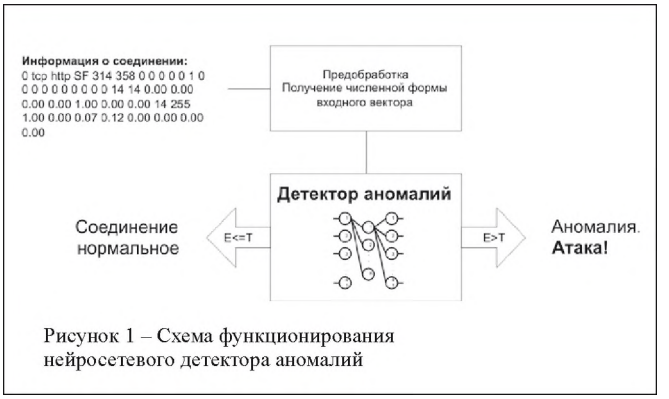

Рисунок 1 – Схема функционирования нейросетевого детектора аномалий

Детектор злоупотреблений. РНС может обучаться на соединениях-атаках, тем самым инкапсулируя информацию не о нормальном поведении, а шаблоны некорректного поведения. В этом случае в процессе функционирования сигналом об атаке будет ошибка реконструкции ниже установленного порога (2), в противном случае входной вектор не относится к атакам и является нормальным соединением (рисунок 2).

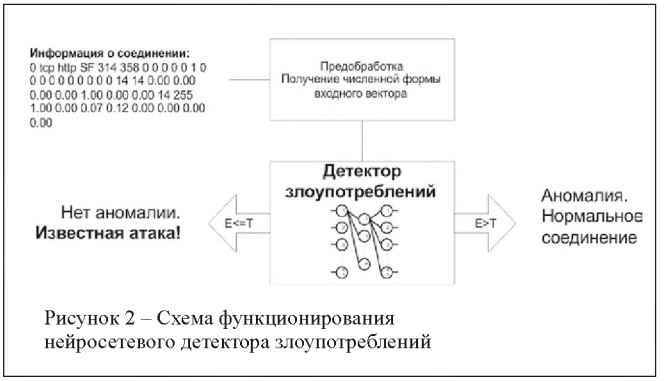

Рисунок 2 – Схема функционирования нейросетевого детектора злоупотреблений

Ансамбль детекторов аномалий и злоупотреблений. При совместном использовании детектора аномалий и детектора злоупотреблений на базе РНС решение принимается не по двоичным векторам результатов работы каждого детектора, а непосредственно по их выходным данным. Использование нейродетекторов аномалий и злоупотреблений на базе РНС одинаковой архитектуры, обученных до одинакового уровня ошибки, позволяет произвести принятие решения исходя из ошибок реконструкции (1) на обоих детекторах:

$$\begin{cases} X \in A_N, \ если \ \ E_A \le E_З, \\ X \in A_P, \ если \ \ E_A > E_З, \end{cases} \qquad (2)$$

где E_A – ошибка реконструкции детектора аномалий, $E_З$ – ошибка реконструкции детектора злоупотреблений, A_N – нормальные соединения, A_P – соединения-атаки (рисунок 3).

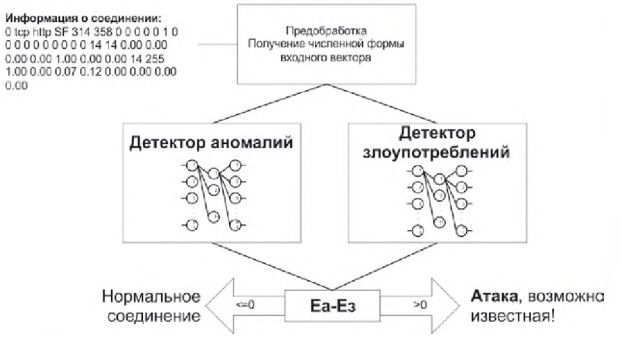

Рисунок 3 – Схема совместного функционирования нейросетевых детекторов аномалий и злоупотреблений

Детекторы отдельных классов атак являются производным от детекторов злоупотреблений на базе РНС. Нейросетевой детектор определяет сходство входного вектора с векторами из тренировочного набора. При обучении РНС не на всем наборе вредоносного трафика, а только на выборке из атак конкретного класса, детектор сможет определить принадлежность входного образа именно к данному классу атак. Далеко отстоящие вектора (ошибка реконструкции (1) превышает пороговое значение) в этом случае не будут являться нормальными соединениями, а могут быть охарактеризованы как соединения, не принадлежащие данному классу атак.

Классификатор на базе РНС-детекторов. Описанные выше детекторы отдельных классов способны оценивать принадлежность входного вектора к классам по отдельности. Для определения класса сетевой атаки детекторы отдельных классов объединяются в общий классификатор. Предложенный классификатор состоит из N детекторов отдельных классов на базе рециркуляционных нейронных сетей, каждый из которых имеет порог T_i, и при реконструкции входного образа выдает ошибку реконструкции E_i. Для приведения оценок детекторов, обученных в разных условиях, к сравнимым значениям, ошибка реконструкции масштабируется по порогу: $\delta_i = E_i / T_i$ – относительная ошибка реконструкции. Чем меньше δ_i, тем более вероятна принадлежность входного образа X к классу A_i.

Система, использующая метод совокупного классификатора, может гибко изменяться и подстраиваться под новые входные данные: соединения, определенные как аномальные по отношению ко всем детекторам, формируют новый класс, для которого обучается новый детектор. Таким образом, изначально в системе может быть только детектор аномалий, обученный на нормальном трафике. В дальнейшем, при обнаружении им аномальных соединений – атак – для их последующего распознавания могут быть обучены соответствующие детекторы (рисунок 4).

Результаты тестирования

В качестве критериев для сравнения эффективности предложенного подхода с существующими методами использовались следующие показатели: *FPR* – уровень ложных срабатываний, *FNR* – уровень пропуска цели,

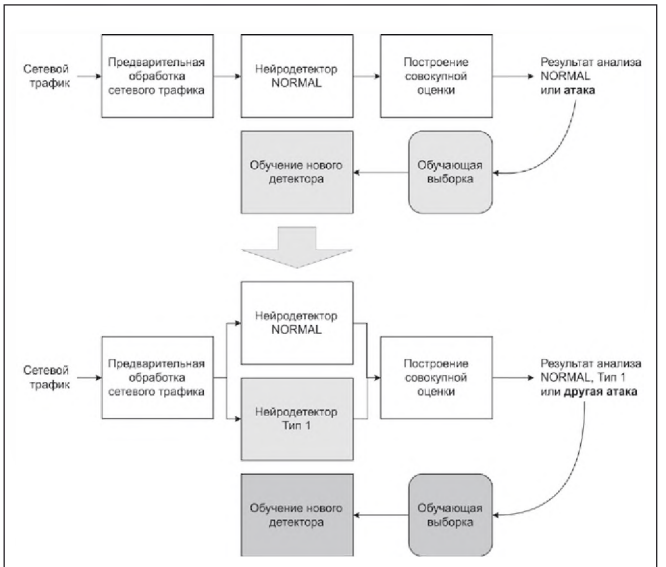

Рисунок 4 – Схема генерации и функционирования совокупного классификатора на базе нейросетевых детекторов атак

ACC – точность классификации, *CR* и CR_i – уровень распознавания в рамках всего набора данных или i-го класса атак. Для обучения и тестирования детекторов использовалась база данных DARPA/KDD [3], содержащая атаки 22 типов, принадлежащие четырем классам – DOS, U2R, R2L, Probe, а также нормальные соединения.

Лучшие методы, не использующие нейронные сети, имеют ошибки *FPR* и *FNR* до 10 %, а при высоком качестве распознавания атак класса DOS (*CRdos*=97–99 %), качество распознавания атак классов R2L и U2R значительно ниже – CR_{r2l}= 1–46 %, CR_{u2r}= 2–50 % [4–5]. В свою очередь, нейросетевые подходы показывают значительно более высокие результаты. Наименьший показатель вероятности ошибок первого и второго рода – 0,3–1,2 %, и распознавание всех классов атак на уровне 98–99 % [6–7]. Однако, при таких высоких показателях качества обнаружения и распознавания известных атак не обеспечивается обнаружение новых, неизвестных атак.

В таблицах 1 и 2 представлены результаты обнаружения и распознавания атак предложенными методами.

Таблица 1 – Результаты тестирования методик обнаружения атак

Технология	FPR, %	FNR, %	ACC, %
Детектор аномалий	12,93	0,36	97,18
Детектор злоупотреблений	0,04	2,73	97,96
Совместное функционирование	0,02	1,79	98,36
Совокупный классификатор 4-х классов атак	3,74	0,01	99,23
Совокупный классификатор 22-х типов атак	1,94	0,14	99,51

Таблица 2 – Результаты тестирования методики распознавания атак

	CR_{dos}, %	CR_{probe}, %	CR_{r2l}, %	CR_{u2r}, %	CR, %
Классификатор 4-х классов атак	99,31	99,12	97,86	100,0	98,78
Классификатор 22-х типов атак	99,78	95,18	97,60	100,00	99,40

Полученные результаты превосходят результаты распространенных подходов (см. таблицы 3–4), в том числе нейросетевых (см. таблицы 5–6).

Таблица 3 – Средние результаты обнаружения при помощи различных технологий [8, 9, 5, 10]

Технология	FPR, %	FNR, %
Победитель KDD-99, Bagged Boosting	0,5	25,4
Правила	2	10
Кластеризация	10	7
K-NN	8	9
SVM	10	2

Таблица 4 – Результаты распознавания классов атак в некоторых исследованиях [11, 10, 13]

	CR_{dos}, %	CR_{probe}, %	CR_{r2l}, %	CR_{u2r}, %
Гауссовский классификатор	82,4	90,2	9,6	22,8
K-NN	97,3	87,6	6,4	29,8
Алгоритм ближайшего кластера	97,1	88,8	3,4	2,2
Лидер-алгоритм	97,2	83,8	1,0	6,6
Алгоритм гиперсферы	97,2	84,8	1,0	8,3
Fuzzy Art Map	97,0	77,2	3,7	6,1
Дерево решений C4.5	97,0	80,8	4,6	1,8
Bagged Boosting	97,1	83,3	13,2	8,4
Деревья решений	99,8	50,0	33,3	50,0
Байесовы сети	99,7	52,6	46,2	25,0

Как видим, при достаточно высоком уровне распознавания атак классов probe и dos большинство подходов очень плохо распознают атаки наиболее опасных типов – u2r и r2l.

Таблица 5 – Результаты обнаружения при помощи известных нейросетевых методов

Технология	FPR, %	FNR, %
Модульная структура из MLP [11] на известных атаках	9	7
Модульная структура из MLP [11] на неизвестных атаках	18	14
MLP [14]	0,8	5,8
MLP [15]	3	23
MLP [16]	неизвестно	0,4
Сети Элмана [15]	0	23
Иерархия SOM [17]	1,4	9,3
Flexible Neural Tree [18]	0,3	1,2
Fuzzy NN [19] на неизвестных атаках	–	31,2

Таблица 6 – Результаты распознавания классов атак при помощи нейросетевых методов

	CR_{dos}, %	CR_{probe}, %	CR_{r2l}, %	CR_{u2r}, %
Flexible Neural Tree [18]	98,8	99,3	98,8	99,9
Fuzzy NN [19]	100,0	100,0	99,8	40,0
Иерархия PCA-сетей [20]	100,0	100,0	97,2	–
PCA-сети и SOM [20]	99,0	75,2	77,0	–
Иерархия SOM [17]	96,9	81,3	0,0	1,1
MLP и нечеткая кластеризация [11]	99,9	48,1	93,2	83,3
RBF [20]	98,8	98,0	97,2	–

Заключение

Экспериментальное тестирование показало, что точность обнаружения и распознавания известных атак совокупным классификатором на базе PHC-детекторов отдельных классов находится на уровне 99 %, а качество обнаружения неизвестных атак – на уровне 98 %. В зависимости от количества входящих в классификатор детекторов от 80 % до 98 % обнаруженных неизвестных атак распознаются как атаки класса «неизвестная атака». Совместное использование обнаружения аномалий и обнаружения злоупотреблений в рамках одного подхода позволяет увеличить точность обнаружения и распознавания, и обеспечить требуемую адаптивность и масштабируемость системы.

Литература:

1. CSI Computer Crime and Security Survey 2010 [Electronic resource] Mode of access: http://gocsi.com/survey. – Date of access: 11.01.2011.

2. Proposal for a Regulation Of The European Parliament And Council concerning the European Network and Information Security Agency (ENISA) [Electronic resource] Mode of access: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2010/sec_2010_1126_en.pdf. – Date of access: 11.01.2011.

3. KDD Cup'99 Competition. [Electronic resource] Mode of access: http://kdd.ics.uci.edu/databases/kddcup99/

kddcup99.html. – Date of access: 20.04.2009.

4. Srilatha, C. et al. Feature deduction and ensemble design of intrusion detection systems / C. Srilatha, A. Ajith, Th. Johnson. – Computers & Security. – 2005. – №24. – P. 295–307.

5. Eskin, E. A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data / E. Eskin // Data Mining for Security Applications; Eds.: D. Barbar, S. Jajodia. – Boston, Kluwer Academic Publishers, 2002.

6. Jahanbani, A. and Karimi, H. A new Approach for Detecting Intrusions Based on the PCA Neural Networks / A.Jahanbani, H.Karimi. – Journal of Basic and Applied Scientific Research. – 2012. – V. 2 (1). – P. 672–679.

7. Anyanwu, L.O. Scalable Intrusion Detection with Recurrent Neural Networks / L.O. Anyanwu, L. Keengwe, G.A. Arome. – International Journal of Multimedia and Ubiquitos Engineering. – 2011. – V. 6, №1.

8. Lee, W. A framework for constructing features and models for intrusion detection systems / W. Lee, S.J. Stolfo // ACM Trans. on Inform. and System Security. – 2000. – №3(4). – P. 227–261.

9. Frank, J. Artificial intelligence and intrusion detection: Current and future directions / J. Frank // The 17th National Computer Security Conference: proceedings, Baltimore, MD, 1999 / National Institute of Standards and Technology [Electronic resourse] – 1999. – Mode of access: http://svn.assembla.com/ svn/odinIDS/Egio/temp/ frank94artificialCiteSeer.pdf. – Date of access: 02.02.2010.

10. Pfahringer, B. Winning the KDD99 Classification Cup: Bagged Boosting / B. Pfahringer // SIGKDD Explorations. – 2000. – V. 1, №2. – P. 65–66.

11. Wang, G. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clastering / G. Wang, J. Hao, J. Ma, L. Huang // Expert Systems with Applications. – 2010. – №2. – P. 6225–6232.

12. Жульков, Е.В. Построение модульных нейронных сетей для обнаружения классов сетевых атак: дис. … канд. техн. наук: 05.13.19 / Е.В. Жульков. – СПб., 2007. – 155 л.

13. Sabhnani, M. Application of Machine Learning Algorithms to KDD Intrusion detection dataset within Misuse detection context / M.Sabhnani, G. Serpen // The international conference on Machine Learning: Models, technologies and Applications: proceedings, 2003. – 2003. – P. 209–215.

14. Saravanakumar, S. Development and Implementation of Artificial Neural Networks for Intrusion Detection in Computer Network / S. Saravanakumar, Umamahchwari, D. Jayalakshmi, R. Sugumar // International Journal of Computer Science and Network Security. – 2010. – V. 10, №7. – P. 271–275.

15. Ghosh, A.K. Learning program behavior profiles for intrusion detection / A.K. Ghosh, A. Schwartzbard, M. Schatz // 1st USENIX Workshop on Intrusion Detection and Network Monitoring: proceedings, Santa Clara, CA, 1999, 9–12 April / USENIX. – USENIX, 1999. – P. 51–62.

16. Ali, A. Intelligent Adaptive Intrusion Detection Systems Using Neural Networks (Comparative study) / A. Ali, A. Saleh, T. Badawy // International Journal of Video & Image Processing and Network Security. – 2010. – V. 10, №1. – P. 1–12.

17. Kayacik, H.G. A Hierarchical SOM-Based Intrusion Detection System / H.G. Kayacik, A.N. Zincir-Heywood, M. Heywood // Engineering Applications of Artificial Intelligence. – 2006. – №9. – P. 439–451.

18. Novosad, T. Fast Intrusion Detection System based on Flexible Neural Tree / T. Novosad, J. Platos, V. Snasel, A. Ajith // Sixth International Conference on Information Assurance and Security (IAS): proceedings, USA. – 2010. – P. 142–147.

19. Muna, M.J. Design Network Intrusion Detection System usin hybrid Fuzzy-Neural Network / M.J. Muna, M. Mehrotra // International Journal of Computer Science and Security. – 2010. – V. 4 (3). – P. 258–294.

20. Liu, G. A hierarchical intrusion detection model based on the PCA neural networks / G. Liu, Z. Yi, S. Yang // Neurocomputing. – 2007. – P. 1561–1568.

Abstract

The approach to network intrusion detection and recognition with use of recirculation neural networks is presented. The technologies of anomaly detection and misuse detection are utilized and combined into one technology. Such technology shows high degree of computer system protection. Experimental results prove efficiency of technology.

Поступила в редакцию 18.05.2013 г.