Предполагается, что разработка системы обнаружения компьютерных атак, основанной на применении методов искусственных иммунных систем и нейронных сетей, позволит существенно повысить вероятность обнаружения неизвестных сетевых вторжений.

Литература

1. Кашаев, Т.Р. Применение искусственной иммунной системы для решения задачи обнаружения атак / Материалы 3-й Всероссийской зимней школы – семинара аспирантов и молодых ученых / Т.Р. Кашаев. – Уфа: УГАТУ, 2008. – С. 326-332.

2. Дасгупта, Д. Искусственные иммунные системы и их применение / Д. Дасгупта; пер. с англ. под ред. А.А. Романюхи. – М.: ФИЗМАТЛИТ, 2006. – 344 с.

УДК 004.8.032.26

НАСТРОЙКА ПОРОГОВ НЕЙРОСЕТЕВЫХ ДЕТЕКТОРОВ ДЛЯ РАСПОЗНАВАНИЯ КЛАССОВ СЕТЕВЫХ АТАК

Кочурко П.А.

УО «Брестский государственный технический университет», г. Брест

При решении задач обнаружения попыток несанкционированного доступа к системе можно выделить два основных подхода: обнаружение аномалий и обнаружение злоупотреблений.

Нелинейные рециркуляционные нейронные сети (РНС) способны выступить в качестве детекторов СОА, реализующей обе технологии. Известно [1], что именно объединение обеих технологий в рамках одной системы может позволить повысить качество обнаружения и снизить уровень ложных срабатываний.

В случае применения нелинейных рециркуляционных сетей (РНС) в качестве детектора аномалий [2] обучение РНС производится на нормальных соединениях таким образом, чтобы входные вектора на выходе восстанавливались в себя, при этом, чем соединение более похоже на нормальное, тем меньше ошибка реконструкции:

$$E^k = \sum_j (\bar{X}_j^k - X_j^k)^2, \quad (1)$$

где X_j^k – *j*-й элемент *k*-го входного вектора, $\overline{X}_j^k$ – *j*-й элемент *k*-го выходного вектора. Если $E^k > T$, где T – некий заданный для данного дететора порог, то соединение признаётся аномалией, или атакой, иначе – нормальным соединением.

Таким образом, одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс A), или ко второму (класс $\overline{A}$), которому соответствуют далеко отстающие вектора. Объединив в одной системе *N* подобным образом обученных детекторов, каждый из которых отвечает за анализ принадлежности входного вектора к одному из классов A_i, можно успешно решать задачу распознавания типа или класса атаки. Для этого необходимо анализировать относительную ошибку реконструкции

$$\delta_i^k = \frac{E_i^k}{T_i}, \quad (2)$$

где T_i – порог *i*-го детектора, изначально $T_i = mean\delta_i^k$. Чем меньше δ_i^k, тем более вероятна принадлежность входного *k*-го образа к классу A_i.

После обучения нейродетекторов всех классов необходимо решить задачу настройки порогов T_i таким образом, чтобы уменьшить ошибки неверной классификации. Для этого применяется следующий алгоритм:

1) вычисляется матрица результатов классификации C, где C_{ij} – количество векторов класса A_i, определенных как вектора класса A_j; при этом если $i \neq j$, то это данное значение указывает, сколько векторов классифицированы ошибочно. Для того, чтобы уменьшить данное значение, необходимо уменьшить для каждого k-го вектора δ_i^k и увеличить δ_j^k. Исходя из (2), для этого вычисляются суммарные относительные ошибки для всех векторов, принадлежащих к классу A_i, но определенных как вектора класса A_j:

$$ER_{ij} = \sum_{k=1}^{C_{ij}} \left(\frac{E_i^k}{E_j^k} T_j - T_i \right), \tag{3}$$

для $\forall i = 1..N, j = 1..N, i \neq j$;

2) для $\forall i = 1..N$ вычисляется новое значение порога:

$$T_i = T_i + \alpha \frac{\sum_{j=1}^{N, i \neq j} ER_{ij}}{\sum_{j=1}^{N, i \neq j} C_{ij}} - \beta \frac{\sum_{j=1}^{N, i \neq j} ER_{ji}}{\sum_{j=1}^{N, i \neq j} C_{ji}}, \tag{4}$$

где $\alpha=\beta=0{,}01$;

3) если не достигнуто максимальное количество итераций, то – переход к пункту 1).

На рисунках 1 и 2 изображены графики суммарного изменения порогов и изменения ошибки неверной классификации MC.

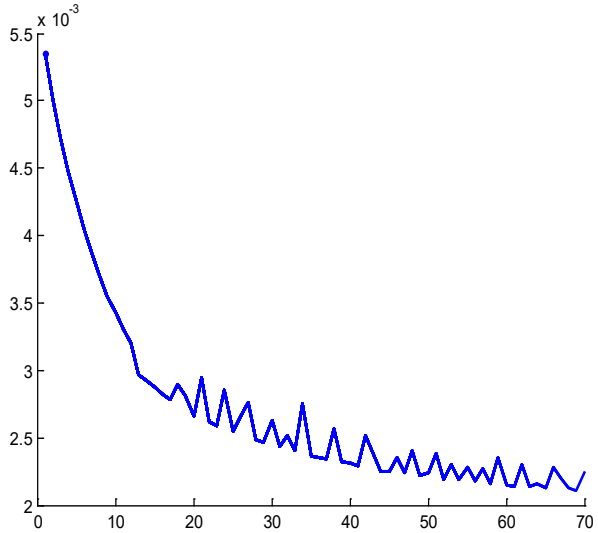

Рисунок 1 – Суммарное изменение

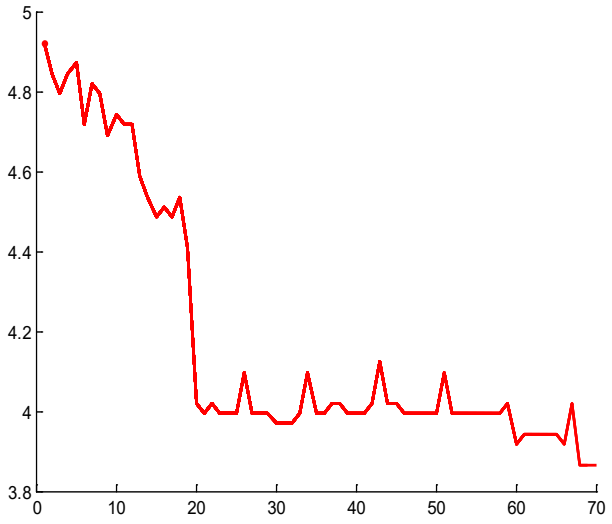

Рисунок 2 – Ошибка неверной значения порогов классификации

В таблицах 1–3 приведены результаты распознавания 23 типов атак [3] (в том числе 1-й тип – нормальные соединения) до и после настройки порогов, а также распознавания типов на тестовой выборке. Результаты представлены парой значений, выраженных в процентах: *DR* – процент корректно распознанных атак данного типа, *FAR* – процент ложных срабатываний, а также третьей синтетической характеристикой *SE* – суммой ошибок первого и второго рода.

Таблица 1 – Результаты распознавания типов атак до настройки порогов на обучающей выборке (3880 соединений), *MC* = 5,05%

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
DR	91,7	96,4	100	96,7	95	100	89,5	100	83,3	76,7	98,9	97,1	100	100	100	96,6	95	86,5	100	100	100	74	98
FAR	2,91					0,03		0,16				0,84			0,16	0,11	0,13	0,03				0,16	0,58
SE	11,2	3,6		3,3	5	0,03	10,5	0,16	6,7	23,3	1,1	3,74			0,16	3,51	5,13	13,5				26,2	2,6

Таблица 2 – Результаты распознавания типов атак после настройки порогов на обучающей выборке (3880 соединений), *MC* = 3,87%

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
DR	87,1	98,2	100	96,7	97,5	100	93,2	100	100	85,3	99,1	82,9	100	100	100	95,4	95	97	100	100	100	93,3	76
FAR	1,07					0,03	0,38			0,64		0,26			0,16	0,08	0,13	0,38				0,24	0,58
SE	14	1,8		3,3	2,5	0,03	7,18			15,3	0,9	17,4			0,16	4,68	5,13	3,4				6,94	24,6

Таблица 3 – Результаты распознавания типов атак после настройки порогов на тестовой выборке (505291 соединений), *MC* = 1,92%

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
DR	94,2	85,2	93,8	87,5	98,1	10,3	23,3	95,3	100	85,7	99,7	44,6	100	100	99,2	96,6	80	97,6	99,8	100	100	80,3	85
FAR	0,41	0,32		0,01	0,12		0,04		0,01		0,03	0,02				0,06	0,01	0,64				0,34	

Сравнивая результаты распознавания типов атак в первой и второй таблицах, можно сделать вывод, что на различных детекторах настройка порогов отражается по-разному: ухудшается качество распознавания (детекторы №№ 1, 12 и 23), остается на том же уровне или значительно улучшается (детекторы №№ 2, 5, 7 и, особенно, 10, 18 и 22). Это значит, что система пытается за счет проигрыша в небольшом количестве детекторов достичь выигрыша в большем количестве детекторов и в целом по системе.

Литература.

1. Giacinto, G. et al. Selection of image classifier // G. Giacinto, F. Roli, G. Fumera. – Electron. – №26(5), 2000. – P. 420-422.

2. Кочурко, П.А. Нейросетевой детектор аномалий / П.А.Кочурко // Известия Белорусской инженерной академии. – 2005. – № 1(19) – С. 78-81.

3. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.

УДК 004.8.032.26

ОПТИМИЗАЦИЯ НЕЙРОСЕТЕВОЙ СИСТЕМЫ ДЛЯ АНАЛИЗА ЭЛЕКТРОЭНЦЕФАЛОГРАММ

Лаврентьева С.В.

УО «Брестский государственный технический университет», г. Брест

Введение

Автоматическое обнаружение эпилептиформной активности в сигналах электроэнцефалограмм (ЭЭГ) является актуальной задачей. Результаты исследования динамики значения старшего показателя Ляпунова для сигналов электроэнцефалограмм (ЭЭГ) показывают неточность обнаружения интервала, содержащего эпилептиформную активность, а также высокий процент ложных срабатываний алгоритма [1]. Причиной таких результатов работы метода является анализ нестационарного сигнала. Когда в обучающую выборку