Литература

1. Иммунитет. Энциклопедия «Кругосвет». – 2004. – Режим доступа: http://krugosvet.ru.
2. Безобразов, С. В. Искусственные иммунные системы: принципы построения / С. В. Безобразов // Труды IV республиканской научной конференции молодых ученых и студентов «Современные проблемы математики и вычислительной техники», Брест, ноябрь, 2005 г. – Брест : БГТУ, 2005. – С. 3–5.
3. Kohonen, T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. – 1982. – № 43. – P. 59–69.

РЕЦИРКУЛЯЦИОННЫЕ НЕЙРОННЫЕ СЕТИ В ЗАДАЧАХ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

П. А. Кочурко

Брестский государственный технический университет, Беларусь

Научный руководитель В. А. Головко

Решения различных прикладных задач с помощью аппарата искусственных нейронных сетей (ИНС) широко известны и активно применяются на практике. В сфере обнаружения сетевых атак ИНС имеют потенциал для решения большого количества проблем, охватываемых другими современными подходами. Изначально ИНС были заявлены в качестве альтернативы компонентам статистического анализа систем выявления аномалий, в дальнейшем предлагались подходы и для обнаружения злоупотреблений и распознавания сетевых атак. В данной работе рассматриваются нейросетевые подходы, реализующие как технологию обнаружения аномалий, так и обнаружения злоупотреблений на основе нелинейных рециркуляционных нейронных сетей (РНС).

Рециркуляционные нейронные сети, называемые также иногда автоассоциативными, в общем случае представляют собой многослойный персептрон, производящий отображение входного образа в идентичный ему выходной. При этом, в зависимости от архитектуры сети, может производиться сжатие и восстановление информации или вычисляться главные компоненты – такие сети называют также PCA-сетями [1].

В процессе обнаружения аномалии система обнаружения атак (СОА) производит анализ входного образа, которым может являться информация о TCP-соединении или строка журнала регистрации сетевых событий, на предмет принадлежности его к одному единственному классу, который известен системе – классу нормальных образов. В случае, если делается вывод о его непринадлежности к данному классу, то данный образ считается атакой, т. е. относится ко второму классу. В процессе определения злоупотреблений СОА наоборот реализует поиск того класса атак из известных классов, к которому данный входной образ может относиться. Если такой класс не найден, то данный образ объявляется нормальным.

Нелинейные РНС способны выступить в качестве детекторов СОА, реализующей обе технологии. Опыт показывает [2], [3], что именно объединение обеих технологий в рамках одной системы может позволить повысить качество обнаружения и снизить уровень ложных срабатываний. При этом одинаковая природа детекторов позволяет избежать нежелательных издержек на реализацию и функционирование детекторов другой природы. Рассмотрим варианты применения РНС в качестве: а) детектора аномалий; б) комбинированного детектора; в) частного классификатора; г) основы для совокупного классификатора.

В случае применения нелинейных РНС в качестве детектора аномалий [4]: 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; $\bar{X}_j^k$ – j-й элемент k-го выходного вектора.

Если $E^k > T$, где T – некий заданный для данной РНС порог, то соединение признаётся аномалией, или атакой, иначе – нормальным соединением.

Иногда различие между нормальным и аномальным входными образами не настолько высоко для того, чтобы ошибка реконструкции превысила порог. Это означает, что нужно обучать РНС таким образом, чтобы аномальные входные образы приводили к более высоким ошибкам реконструкции. Цель будет достигнута, если обучать РНС восстанавливать нормальные образы в нормальные, а атаки – в не равные им (все параметры умножены на некоторое k) выходы. При функционировании такой РНС ошибка реконструкции – мера аномальности – будет также считаться по (1). Однако входные образы с атаками уже будут давать на выходе не $\bar{X}$, а $k\bar{X}$ и ошибка реконструкции для данных образов будет:

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

что выше, чем обычно. Экспериментальное сравнение двух данных подходов представлено в табл. 1. РНС обучались на выборках из базы KDD 99 [5], представляющих собой записи о TCP-соединениях из 41 параметра. При обучении комбинированных сетей количество нормальных соединений в обучающей выборке превышало в 6 раз количество внедренных записей об атаках, $k = 1{,}5$.

Таблица 1

Результаты обнаружения аномалий для соединений различных служб

Служба	Детектор аномалий		Комбинированный детектор	
	***FP*, %**	***FN*, %**	***FP*, %**	***FN*, %**
All	6,34	10,47	8,16	6,87
HTTP	0,30	0,10	0,50	0,06
FTP_DATA	2,00	8,09	2,00	1,50
TELNET	5,20	12,42	16,45	1,92

Если при обучении детектора аномалий использовались нормальные вектора, которые восстанавливались в себя, и на основании этого делался вывод об их принадлежности к классу «нормальных», то обучая детектор на соединениях-атаках, которые должны восстановиться в себя, можно делать вывод об их принадлежности к классу «атаки».

Таким образом, одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс A_i), или ко второму (класс $\overline{A}_i$), которому соответствуют далеко отстающие вектора:

$$\begin{cases} X^k \in A_i, & \text{если } \delta_i^k \le 1, \\ X^k \in \overline{A}_i, & \text{если } \delta_i^k > 1, \end{cases} \tag{3}$$

где $\delta_i^k = \dfrac{E_i^k}{T_i}$ – относительная ошибка реконструкции. При этом, чем меньше δ_i^k, тем более вероятна принадлежность входного образа X^k к классу A_i. База данных KDD [5], на которой производилось обучение и тестирование РНС, включает соединения нормальные, а также атаки четырёх классов, которые радикально отличаются друг от друга. Поэтому целесообразно обучить детекторы для каждого из пяти классов отдельно, не объединяя все классы атак в единое целое. Результаты тестирования представлены в табл. 2.

Таблица 2

Результаты тестирования частных детекторов

Класс	FP, %	FN, %	Класс	FP, %	FN, %	Класс	FP, %	FN, %	Класс	FP, %	FN, %
ALL			FTP_DATA			HTTP			TELNET		
normal	12,56	6,68	normal	6,8	2,72	normal	2,4	0,17	normal	44,4	1,31
dos	4,33	1,09	dos	0	0	dos	1,5	0	dos	0	0
probe	7,79	14,21	probe	0	0	probe	0	0	probe	0	0
r2l	2,87	5,38	*r2l*	5,17	0,25	*r2l*	0	0	*r2l*	3,33	0
u2r	7,07	5,54	*u2r*	0	0,07				*u2r*	5,91	2

Полученные частные детекторы в дальнейшем могут быть объединены в один совокупный, при этом независимость их оценок вкупе с их сравнимостью позволяют получить значительный выигрыш по сравнению с применением только частных детекторов (табл. 3).

Таблица 3

Результаты тестирования совокупного классификатора

Служба	FP, %	FN, %	Качество распознавания, %			
			dos	probe	*r2l*	*u2r*
ALL	10,80	2,34	98,17	96,55	91,88	100
HTTP	0	0,08	99,75	100	100	–
FTP_DATA	0,66	1,09	100	100	96,66	100
TELNET	0	5,03	97,75	100	98,00	85,50

Как видно из приведенных в таблицах 1–3 результатов, нелинейные РНС способны показывать высокое качество как обнаружения, так и распознавания типа атаки. Метод совокупного классификатора, показывающий наилучшие результаты, может с успехом применяться для решения задач распознавания сетевых атак и других задач распознавания образов.

Исследования проводятся при поддержке БРФФИ при НАН Беларуси и Министерства образования Республики Беларусь.

Литература

1. Unsupervised learning for dimensionality reduction / V. Golovko [et al.] // Second Int. ICSC Symposium on Engineering of Intelligent Systems EIS'2000: proceedings, Paisley, Scotland, June 2000, Canada / University of Paisley. – ICSS Academic Press, 2000 – P. 140–144.
2. Лукацкий, А. В. Обнаружение атак / А. В. Лукацкий. – Санкт-Петербург : БХВ-Петербург, 2003. – 596 с.
3. Brugger, S. T. Data Mining Methods for Network Intrusion Detection [Electronic resource] / S. T. Brugger. – Mode of access: http://www.bruggerink.com/~zow/Projects.html. – Date of access: 07.04.2005.
4. Кочурко, П. А. Нейросетевой детектор аномалий / П. А. Кочурко // Изв. Белорус. инженер. акад. – 2005. – № 1(19)/2. – С. 78–81.
5. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.

ФОРМАЛИЗАЦИЯ ТЕХНОЛОГИЧЕСКОЙ ЛИНИИ СОРТИРОВКИ ВАГОНОПОТОКОВ НА ЖЕЛЕЗНОДОРОЖНОЙ СТАНЦИИ

Е. А. Ерофеева

Белорусский государственный университет транспорта, г. Гомель

Научный руководитель И. В. Максимей

При планировании работы сортировочной станции Белорусской железной дороги обычно используются математические методы [1, глава 5]. Поскольку параметры технологического процесса переработки вагонопотока являются вероятностными и зачастую аналитические модели неадекватны, то поэтому необходимо использовать метод имитационного моделирования. С помощью имитации решаются задачи планирования грузоперевозок и разрабатываются средства исследования технологий переработки транзитного вагонопотока на железнодорожной станции [2]. При этом *объектом моделирования* в таких исследованиях является железнодорожная сортировочная станция, представляющая собой сложный комплекс технологически взаимосвязанных элементов и операций. *Предметом моделирования* в этом случае будет технологический процесс переработки транзитного вагонопотока (ТП ПТВ).

Формализация ТП ПТВ осуществляется поэтапно. На *первом этапе* осуществляется переработка содержательного описания технологического процесса сортировки вагонопотоков на железнодорожной станции, результатом которой является иерархический граф технологических операций (ТХО). На *втором этапе* формализации ТП составляется сетевой график взаимодействия элементов с элементами СМО. Вершинами сетевого графика будут свершения событий в ТП на станции. Ребрами являются сами технологические операции. Специфические процедуры начала и конца выполнения ТХО обозначим, как СНК, и, при этом, они не имеют продолжительности в модельном времени имитации.

Поезда, поступающие в расформирование на станцию и, соответственно, сформированные составы поездов представим в виде *сложных составных транзак-*