Как следует из рисунка, теоретическая вероятность хорошо аппроксимирует экспериментальную вероятность обнаружения вредоносных программ.

Выводы. Разработан алгоритм построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ, который характеризуется непрерывной эволюцией нейросетевых иммунных детекторов с целью эффективного обнаружения вредоносных программ. Предложенный алгоритм отличается от известных способом клональной селекции, когда мутация детекторов происходит в результате их дополнительного обучения, а отбор клонированных детекторов происходит в соответствии с их значениями суммарной квадратичной ошибки. Это позволяет адаптироваться нейросетевым иммунным детекторам к обнаружению вредоносных программ.

Разработана структура нейросетевого иммунного детектора для обнаружения вредоносных программ, которая состоит из трех слоев нейронных элементов и арбитра. Она характеризуется малым объемом обучающей выборки. Предложенный нейросетевой иммунный детектор способен обнаруживать неизвестные вирусы.

Литература

1. Искусственные иммунные системы для защиты информации: применение LVQ сети // IX Всероссийская научно-техническая конференция «Нейроинформатика - 2007»: сборник научных трудов. – М.: МИФИ, 2007. – Ч. 2.

2. Головко, В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение : учеб. пособие / В.А. Головко. – М., 2001 – 256 с.

УДК 004.8.032.26

МУЛЬТИАГЕНТНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Войцехович Л.Ю.

УО «Брестский государственный технический университет», г. Брест

Высочайший уровень угроз информационной безопасности из внешней среды сделал брандмауэр и *Систему Обнаружения Вторжений (Intrusion Detection System - IDS)* необходимой составляющей защищенной информационной системы. В современном мире развивающихся стремительными темпами компьютерных технологий и телекоммуникаций злоумышленникам стало гораздо легче достичь поставленных целей, благодаря невнимательности и неосведомленности своих жертв о существующих методах защиты.

Простейшим средством сетевой защиты может служить брандмауэр (межсетевой экран, firewall) - реализованное программно или аппаратно средство фильтрации сетевого трафика между двумя сетями или компьютером и сетью (персональный брандмауэр). При этом используются сетевые адреса отправителя и получателя запроса или конкретные службы, а анализа передаваемого трафика не происходит.

Для выполнения анализа передаваемых в сети данных необходимо более сложное и интеллектуальное средство – Система Обнаружения Вторжений [1]. Система обнаружения вторжений – программное и/или аппаратное средство для выявления фактов несанкционированной деятельности (вторжения или сетевой атаки) в компьютерной сети или отдельном узле.

В этой работе для построения системы обнаружения вторжений предлагается использовать *Мультиагентную нейронную сеть* на базе совмещения механизмов *Искусственной иммунной системы* и *Искусственных нейронных сетей*. Предполагается, что такая система обнаружения атак будет способна выполнять обнаружение злоупотреблений и обнаружение аномалий в режиме реального времени.

1. ИММУННАЯ СИСТЕМА

Перед тем как приступить непосредственно к рассмотрению искусственной иммунной системы для построения системы обнаружения атак вкратце остановимся на работе иммунной системы человека. Это описание будет поверхностно, поскольку нас интересуют лишь те механизмы, которые можно использовать в нашей предметной области.

Если так можно выразиться, то основным принципом работы иммунной системы человека является сравнение отдельных “образов” (шаблонов) с телами внутри организма человека. Таким образом, можно обнаружить инородные тела, которые называют антигенами.

В реальной жизни роль вышеупомянутых “шаблонов” выполняют лимфоциты. Они постоянно генерируются спинным мозгом и тимусом в соответствии с информацией, содержащейся в ДНК (эта информация накапливается, и такой процесс называется эволюцией генной библиотеки). Лимфоциты распространяются в организме через лимфатические узлы. Каждый тип лимфоцитов способен распознать некоторое ограниченное число антигенов. В процессе создания лимфоцитов имеется важный этап – негативная селекция. На этом этапе выполняется специальная процедура проверки на совместимость с родными клетками организма. Если лимфоцит несовместим, то он уничтожается. Иначе он будет бороться с клетками своего же организма. Таким образом, благодаря негативной селекции, “шаблоны” содержат информацию, которая отсутствует внутри организма. Если некоторое внешнее тело соответствует определенному “шаблону”, то оно воспринимается как инородное и должно быть немедленно уничтожено.

В случае если лимфоциты обнаруживают антиген, то на базе соответствующего шаблона создаются новые антитела, которые и уничтожают антиген. Существует также другой важный механизм – клональная селекция. Этот механизм подобен естественному отбору: выживают только те антитела, которые в наибольшей степени соответствуют обнаруженному антигену. Таким образом, данные о сформированных антителах попадают в так называемую иммунную память.

Одна из наиболее подходящих областей применения механизмов иммунных систем – это компьютерная безопасность, где аналогия между защитой человеческого тела и защитой нормально функционирующей компьютерной системы очевидна.

Эксперты, работающие в области искусственных иммунных систем, отмечают три основных свойства таких систем:

– во-первых, они распределенные;

– во-вторых, это самоорганизующиеся системы;

– в-третьих, такие системы не особенно требовательны к вычислительным ресурсам.

По мнению большинства экспертов, эффективная система обнаружения вторжений должна обладать всеми вышеперечисленными свойствами.

2. НЕЙРОСЕТЕВОЙ ДЕТЕКТОР

В рассматриваемой мультиагентной системе обнаружения атак нейросетевой детектор выполняет функции лимфоцита в иммунной системе человека. *Нейронные сети* обладают хорошими обобщающими способностями, могут эффективно решать задачи аппроксимации, классификации и обработки зашумленных данных, что особенно важно в такой области, как обнаружение вторжений.

В данной работе в качестве основного агента системы обнаружения атак (см. рисунок 1) предлагается использовать нейронную сеть, представляющую собой объединение *Рециркуляционной нейронной сети (RNN)* и *Многослойного персептрона (MLP)*.

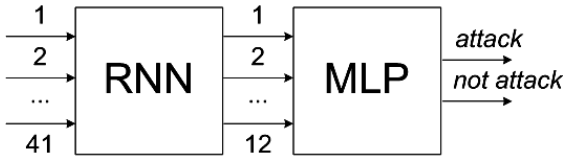

Рисунок 1 – Детектор для мультиагентной нейронной сети

На вход подается 41 параметр, определенный в базе KDD-99 [2]. Эта база содержит информацию о множестве соединений в компьютерной сети. RNN, применение которой с линейной функцией аналогично использованию *метода главных компонент*, выполняет сжатие 41 параметра входного вектора в 12-размерный выходной вектор. MLP обрабатывает полученные в результате сжатия данные и дает заключение относительно входного вектора: является ли он атакой определенного типа или же это нормальное соединение.

Такой детектор в проектируемой системе будет специализироваться на одном определенном типе атак. На выходе детектора возможны два состояния: “да” – если входной образ принадлежит заданному типу атаки, “нет” – входной образ не является атакой.

В мультиагентной системе можно использовать детекторы другого вида [3].

После выполнения процедуры обучения нейронные сети могут использоваться в задаче обнаружения вторжений.

3. МУЛЬТИАГЕНТНАЯ НЕЙРОННАЯ СЕТЬ

В мультиагентной нейронной сети применяется множество детекторов, специализирующихся в различных областях знаний.

Реальные иммунные системы слишком сложны, чтобы можно было применить все имеющиеся в них механизмы защиты. Но в данном случае не нужны все возможности биологических иммунных систем. В ходе построения мультиагентной системы для обнаружения вторжений использованы лишь основные принципы и механизмы реальных иммунных систем, такие как: генерация и обучение детекторов с различной структурой и специализацией, отбор подходящих детекторов, возможность детекторов обнаруживать аномальную активность, клонирование и мутация детекторов, формирование иммунной памяти.

4. РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Результаты эксперимента приведены в таблицах 1 и 2. Записи об атаках класса DOS и Probe распознаны системой в более чем 90% случаев. Несколько хуже результат в случае U2R и R2L. Также присутствуют так называемые ложные срабатывания системы.

Таблица 1 – Обучающая и тестовая выборка

	DoS	U2R	R2L	Probe	Normal	всего
обучающ выборка	3571	37	278	800	1500	6186
тестовая выборка	391458	52	1126	4107	97277	494020

Таблица 2 – Обнаружение атак при помощи мультиагентной НС

класс	кол-во	обнаружено	распознано
DoS	391458	386673 (98.78%)	368753 (94.20%)
U2R	52	47 (90.39%)	45 (86.54%)
R2L	1126	1097 (97.42%)	930 (82.59%)
Probe	4107	4066 (99.00%)	4016 (97.78%)
Normal	97277	---	82903 (85.22%)

Таблица 3 – Обнаружение неизвестных атак

тип	кол-во	обнаружено	тип	кол-во	обнаружено
Normal	75952	74340 (97.88%)	Multihop*	7	5 (71.43%)
Back	2203	2169 (98.46%)	Phf*	4	0 (0.00%)
Land*	1	1 (100.00%)	Spy*	2	0 (0.00%)
Neptune	901	900 (99.89%)	Warezclient	1015	981 (96.65%)
Buffer_overflow	30	26 (86.67%)	Warezmaster	20	19 (95.00%)
Loadmodule	9	9 (100.00%)	Ipsweep	9	9 (100.00%)
Perl*	3	0 (0.00%)	Nmap*	2	2 (100.00%)
Rootkit*	7	3 (42.86%)	Portsweep	15	15 (100.00%)
ftp_write*	6	5 (83.33%)	Satan	10	8 (80.00%)
Guess_passwd	53	53 (100.00%)			

** - атаки, которые отсутствовали в обучающей выборке*

Из таблицы 3 следует, что многие записи о неизвестных системе обнаружения вторжений атаках были правильно отработаны как “атака”. Это свидетельствует о том, что такая мультиагентная система обладает способностью к обобщению и может использоваться для обнаружения ранее неизвестных типов активности в сети.

ЗАКЛЮЧЕНИЕ

В данной работе предложена концептуальная модель построения мультиагентной нейронной сети на базе механизмов искусственных иммунных систем и искусственных нейронных сетей.

Такая система характеризуется: i) гибкостью, ii) распределенностью, iii) самоорганизацией, iv) возможностью дообучения в процессе работы.

Литература

1. Войцехович, Л.Ю., Головко, В.А., Кочурко П.А. и Войцехович Г.Ю. Система обнаружения атак как основной элемент защиты компьютерной сети / Л.Ю. Войцехович, В.А. Головко, П.А. Кочурко и Г.Ю. Войцехович // Вестник БрГТУ. – 2008. - №5(53): Физика, математика, информатика. – С. 12-19.

2. 1999 KDD Cup Competition. - Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

3. Vaitsekhovich, L. and V. Golovko. Employment of neural network based classifier for intrusion detection / L. Vaitsekhovich and V. Golovko // Acta Mechanica et Automatica. Bialostok Technical University. Faculty of Mechanical Engineering. – 2008. – Vol. 2, No 4(6). – P. 93-98.

УДК 62-529

ПРИМЕНЕНИЕ ПОСЛЕДОВАТЕЛЬНОГО НЕЙРОКОНТРОЛЛЕРА В АСУТП

Иванюк Д. С., Головко В.А., Шуть В.Н.

УО «Брестский государственный технический университет», г. Брест

ОАО «Савушкин продукт», г. Брест

Нейроуправление – наука относительно молодая, одна из задач которой заключается в построении систем управления (систем принятия решений), которые могут обучаться во время функционирования и таким образом улучшать свою эффективность работы.