ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В TCP/IP СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРИНЦИПОВ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И НЕЙРОСЕТЕВЫХ ТЕХНОЛОНИЙ

Л.Ю. Войцехович, В.А. Головко

Брестский государственный технический университет,
кафедра интеллектуальных информационных технологий
ул. Московская 267, 224017, г. Брест, Республика Беларусь
телефон: (+375 162) 426321; факс: (+375 162) 422127; e-mail: vspika@rambler.ru, gva@bstu.by

В этой статье рассматривается подход к построению системы обнаружения вторжений, основанный на использовании принципов искусственных иммунных систем и нейронных сетей. Искусственные иммунные системы способны обнаруживать неизвестные образы атак. А объединение двух технологий (иммунных систем и нейронных сетей) позволяет повысить степень защищенности. Детектор строится на базе двух различных нейронных сетей, а именно RNN и MLP. Для проведения экспериментов используется база данных KDD-99. Результаты показали, что такая система обнаружения вторжений способна эффективно обнаруживать компьютерные атаки.

Ключевые слова – обнаружение вторжений, нейронная сеть, искусственная иммунная система, метод главных компонент, мультиагентная система.

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 [2] 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 области компьютерной безопасности.

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 ан-

тителя, 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:

1 во-первых, они распределенные;

2 во-вторых, это самоорганизующиеся системы;

3 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. Рис.1) предлагается использовать нейронную сеть, представляющую собой объединение *Рециркуляционной нейронной сети (RNN)* и *Многослойного персептрона (MLP)*.

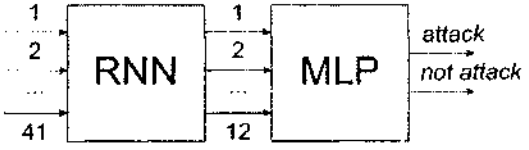

Рис.1. Детектор для мультиагентной нейронной сети.

На вход подается 41 параметр, определенный в базе KDD-99 [3]. 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 значения 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 (Рис.2), детальное описание которых дано в наших предыдущих работах [4, 5]. Но в дальнейшем мы будем ссылаться лишь на детектор, показанный на Рис.1.

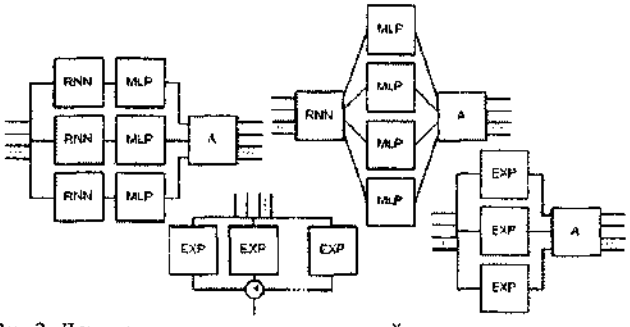

Рис.2. Другие варианты построения нейросетевого детектора.

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

3 МУЛЬТИАГЕНТНАЯ НЕЙРОННАЯ СЕТЬ

В мультиагентной нейронной сети (см. Рис.3) применяется множество детекторов, специализирующихся в различных областях знаний.

Рис.3. Общая схема мультиагентной системы обнаружения атак.

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.

Рассмотрим обобщенную схему функционирования

мультиагентной системы обнаружения вторжений (см. Рис.4).

При инициализации системы все известные образы нормальной активности в сети, а также атак размещаются в двух базах данных – нормальных соединений и атак соответственно. Каждая запись в такой базе данных промаркирована либо как атака определенного типа, либо как не атака. Эти базы используются для формирования обучающих выборок нейросетевых детекторов и для тестирования системы обнаружения атак.

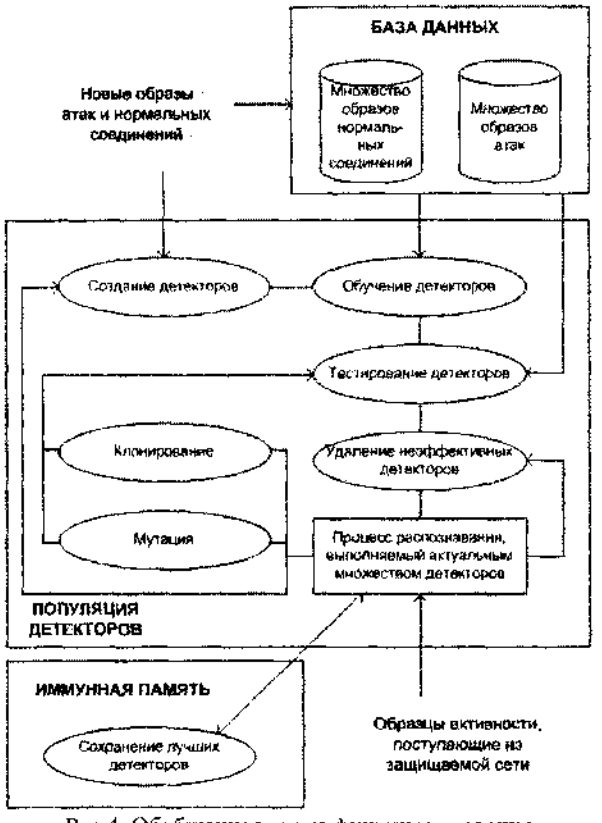

Рис.4. Обобщенная схема функционирования разрабатываемой IDS.

На следующем этапе инициализации системы обнаружения атак происходит создание популяции детекторов и выполняется процедура их обучения. Для формирования обучающей выборки отдельного детектора используются упомянутые выше базы данных сетевой активности.

Кроме того, необходимо предусмотреть специальную функцию контроля (проверки) текущего состояния системы обнаружения вторжений, чтобы "выбраковывать недообучившиеся" детекторы (такие детекторы сразу же должны удаляться из системы) и для расчета параметра эффективности отдельных детекторов.

Набор иммунных детекторов составляет популяцию, которая циркулирует в компьютерной системе и выполняет обнаружение и распознавание сетевых атак. Можно создавать сотни и тысячи детекторов, каждый из которых специализируется в своей области знаний и выполняет поиск характерных для него типов атак.

В процессе сканирования компьютерной сети детектор выполняет распознавание входного вектора, а совокупное заключение множества детекторов, составляющих популяцию, сообщается администратору сети, который и принимает решение, действительно ли наблюдаемая активность является атакой.

Динамические свойства предлагаемой системы обнаружения вторжений обусловлены постоянным обновлением детекторов в популяции. Это выполняется благодаря процедурам клонирования и мутации, пополнением популяции новыми детекторами и исключением из нее неэффективных или длительно используемых детекторов.

В случае если детектор достигает наилучших показателей эффективности среди детекторов, специализирующихся на определенном типе атак, то информация о нем сохраняется в иммунной памяти системы (для детекторов, построенных на базе нейронной сети, сохраняются значения весовых коэффициентов). Эта информация может быть легко извлечена оттуда и использована для инициализации новых детекторов.

Детекторы, которые работают с одним и тем же типом атак объединяются в группы от 3 до 10 детекторов. В общем случае предполагается, что детекторы в группе формируют различные заключения относительно входного образа, что является результатом случайных процессов в ходе обучения (для каждого детектора процесс обучения носит свой неповторимый характер). Теоретически количество детекторов в системе неограниченно и может легко изменяться в процессе выполнения программы, но в реальности могут возникать проблемы с производительностью компьютера (нехватка оперативной память, скорость и т.д.).

Процесс обработки подаваемого на вход системы вектора включает несколько этапов:

1. Входной образ попадает в мультиагентную систему;
2. Каждый детектор (или некоторое подмножество детекторов) дает свое заключение относительно поступивших данных;
3. Рассчитывается, так называемый, фактор поддержки заключения для каждой задействованной группы детекторов. Этот фактор отражает долю детекторов в группе, классифицирующих входной образ как атака определенного типа;
4. Выполняется сравнение факторов поддержки заключения, полученных для каждой группы детекторов. В качестве окончательного решения системы принимается заключение той группы, для которой фактор поддержки принимает наибольшее значение (процедура голосования).

Если в систему поступает информация о новой атаке, отсутствующей в системе (например, от администратора или из другого источника), то записи о такой атаке добавляются в базу данных, и создается новая группа детекторов, которая будет работать в дальнейшем с данным типом атаки. Таким образом, происходит добавление в систему новых знаний.

4 РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Рассмотрим работу мультиагентной системы на примере одной популяции детекторов. Допустим, популяцию составляют 110 детекторов. При чем на каждый определенный в KDD-99 тип записи в популяции приходится по 5-ть детекторов, которые образуют отдельную группу. Результаты эксперимента приведены в Таблицах 1 и 2.

ТАБЛИЦА 1

ОБУЧАЮЩАЯ И ТЕСТОВАЯ ВЫБОРКА

	DoS	U2R	R2L	Probe	Normal	всего
Обучающая 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 ПРИ ПОМОЩИ МУЛЬТИАГЕНТНОЙ НС

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

* - атаки, которые отсутствовали в обучающей выборке

Записи об атаках класса DOS и Probe распознаны системой в более чем 90% случаев. Несколько хуже результат для соединений U2R и R2L. Также присутствуют, так называемые, ложные срабатывания системы.

Результаты другого эксперимента (Таблицы 3) демонстрируют, что многие записи о неизвестных системе обнаружения вторжений атаках были правильно классифицированы 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.

5 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.

Результаты обнадеживают, поскольку выполненная модель системы обнаружения атак продемонстрировала способность не только распознавать образы атак с достаточно высокой степенью точности (в отдельных случаях свыше 90%), но и обнаруживать ранее неизвестные ей атаки, что повышает ценность такой системы.

ЛИТЕРАТУРА

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

[2] Animesh Patcha, Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends // Computer Networks – 2007. – 51. – P.3448–3470.

[3] 1999 KDD Cup Competition. - Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[4] V. Golovko and L. Vaitsekhovich. Neural Network Techniques for Intrusion Detection // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2006) / Brest State Technical University – Brest, 2006. – P. 65-69.

[5] V. Golovko, L. Vaitsekhovich, P. Kochurko and U. Rubanau. Dimensionality Reduction and Attack Recognition using Neural Network Approaches // Proceedings of the Joint Conference on Neural Networks (IJCNN 2007) / Orlando, FL, USA – IEEE Computer Society, Orlando, 2007. – P. 2734-2739.