$$P(A) = P(Ya_1 = Yb_1,\ Ya_2 = Ya_3,\ Yb_2 = Yb_3) = 1/8,$$
$$P(B) = P(Ya_1 \neq Yb_1,\ Ya_2 = Ya_3,\ Yb_2 \neq Yb_3) = 1/8,$$
$$P(C) = P(Ya_1 \neq Yb_1,\ Ya_2 \neq Ya_3,\ Yb_2 = Yb_3) = 1/8.$$
$$P(D) = 1 - (P(A) + P(B) + P(C)) = 5/8. \quad (7)$$

Заключение

1. Закон распределения разности весовых коэффициентов отличается от равномерного. Наиболее вероятны небольшие разности значений.

2. Направления движения начальных значений весовых коэффициентов равновероятны, что является положительным свойством, т.к. сохраняется максимальная неопределенность у внешнего наблюдателя относительно неизвестных ему значений весовых коэффициентов.

3. Более половины тактов синхронизации являются нерезультативными, что может составить предмет дальнейшего совершенствования архитектуры сети и алгоритма коррекции весовых коэффициентов.

4. Следует помнить, что данные выводы относятся к начальным значениям весовых коэффициентов двух сетей, поскольку они являются независимыми. В процессе синхронизации сетей A и B между соответствующими весовыми коэффициентами появляется корреляционная связь, которая усиливается с увеличением числа тактов синхронизации и приведенные соотношения становятся несправедливыми.

5. Остается открытым вопрос об определении момента полной синхронизации сетей, так как продолжение процесса синхронизации может позволить успешно завершиться одной из описанных атак.

Литература:

1. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W.Kinzel.−2005. – Vol. 5, n.1. – P. 130−140.

2. Kinzel, W. Neural Cryptography / W.Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

Abstract

IdoKanter andWolfgang Kinzel offer synchronizedneural networksusing for key derivation. Authors suppose that this approach should be investigated into the matter, algorithm convergence should be confirmed.Algorithm vulnerability is confirmed by attacks simulation. The initial weight vectors values influence on speed of synchronization wasanalyzed. Equal probability of initial weight vectors motion directions was found. On this base authors propose new line of research concerned with improvement of network architecture and correction algorithm.

Поступила в редакцию 18.05.2013 г.

ПРИНЦИПЫ ПОСТРОЕНИЯ АДАПТИВНОЙ СИСТЕМЫ КИБЕРЗАЩИТЫ

УДК 004.056.57:032.26

С.В. Безобразов, В.А. Головко,
БрГТУ, г. Брест

Аннотация

Методы искусственного интеллекта в целом, а также искусственные иммунные системы и искусственные нейронные сети в частности, являются мощным инструментом в области анализа данных. Они хорошо себя зарекомендовали в решении сложных инженерных задач в различных отраслях. Зачастую, интеграция методов искусственного интеллекта приводит к достижению лучших результатов, нежели использование их по отдельности. В данной статье мы описываем основные принципы построения интеллектуальной системы защиты информации от вредоносных программ и сетевых вторжений. Такая система базируется на интеграции методов искусственных иммунных систем и искусственных нейронных сетей. Основной упор будет сделан на исследование адаптивной способности предлагаемого подхода.

Введение

Современный мир переживает резкий рост числа и уровня сложности киберугроз, направленных как на отдельных пользователей сети Интернет, так и на информационные ресурсы национальных государств. В арсенале киберпреступников сегодня находятся разнообразные средства организации кибератак. Наиболее опасными атаками считаются сетевые атаки, осуществляемые посредством глобальной сети Интернет и разработка и распространение вредоносных программ. Так в 2010 году промышленные объекты Ирана были атакованы вредоносной программой Stuxnet с целью несанкционированного сбора данных и диверсий в автоматизированных системах управления промышленных объектов посредством физического разрушения инфраструктуры. Компьютерный червь оказался настолько сложным, что на его «расшифровку» понадобилось несколько месяцев упорных трудов. Многие специалисты по информационной безопасности заговорили о том, что за созданием Stuxnet стоят спецслужбы отдельного государства. В 2012 году антивирусной компанией «Лаборатория Касперского» были обнаружены другие системы кибершпионажа «Duqu», «Flame» и «Gauss», разработанные по всей вероятности спецслужбами отдельных государств. Примечательным в этих событиях является то, что перечисленные вредоносные программы оставались неизвестными и не детектируемыми на протяжении месяцев и даже лет.

Сетевые атаки также представляют большую угрозу информационным ресурсам. Так в 2013 году атакам подверглись некоторые правительственные и коммерческие сайты ряда государств. Так известная хакерская группа Anonymous организовала DDoS атаки на сайты министерства обороны и министерства образования Израиля, а также взломать web-сайт Министерства иностранных дел Палестины и похитить конфиденциальную инфор-

Рисунок 1 – Структура нейросетевой искусственной иммунной системы для обнаружения вредоносных программ

мацию. А неизвестные киберпреступники организовали успешную атаку на крупнейшую биржу Bitcoin, что стало причиной нарушения корректного осуществления транзакций, а также взлому электронных хранилищ.

Все это свидетельствует о том, что применяемые сегодня методы обнаружения вредоносных программ и сетевых атак не позволяют быть уверенными в надежности предоставляемой защиты компьютерных систем и сетей. Все они характеризуются рядом существенных недостатков, и позволяют киберпреступникам обходить существующие системы защиты. В связи с этим, актуальным является разработка и применение принципиально новых методов и алгоритмов защиты компьютерных систем от киберугроз. Современные системы защиты информации должны характеризоваться высокой степенью защиты, способностью к адаптации и эволюции с целью поддержания высокого уровня защиты.

В данной статье мы представляем систему защиты информации, которая базируется на методах искусственного интеллекта – искусственных иммунных систем и искусственных нейронных сетях.

На сегодняшний день существует несколько основных алгоритмов искусственных иммунных систем. Это такие общеизвестные алгоритмы как алгоритм негативного отбора (the negative selection algorithm) [1], алгоритм клонального отбора (the clonal selection algorithm) [2], алгоритм идиотипической сети (the idiotypic network) [3], алгоритм дендритных клеток (the dendritic cell algorithm) [4]. Перечисленные алгоритмы имеют свои сильные и слабые стороны. На наш взгляд существенным недостатком существующих разработок на основе алгоритмов искусственных иммунных систем является бинарная структура иммунных детекторов [1, 5], которая налагает ряд серьезных ограничений. В отличие от существующих подходов мы предложили в основу иммунного детектора положить нейронную сеть встречного распространения. Это позволило нам избавиться от ряда недостатков и повысить адаптивную способность иммунной системы для защиты информации.

Нейросетевая иммунная система киберзащиты

Для повышения уровня обнаружения вредоносных программ и сетевых атак нами была предложена система, базирующаяся на интеграции искусственных нейронных сетей и искусственных иммунных систем [6–9]. Структура предложенной системы представлена на рисунке 1.

Предложенная система основана на принципах и механизмах искусственной иммунной системы [8], где главную роль по обнаружению вредоносных программ и сетевых атак играют нейросетевые детекторы. Структура нейросетевого детектора представлена на рисунке 2.

Детектор состоит из нейронной сети встречного распространения [10] и арбитра. Нейронная сеть состоит из трех слоев. Первый слой является распределительным. Данные, поступающие на сеть, он распределяет на нейроны второго слоя. Второй слой – скрытый, и состоит из нейронов Кохонена, которые осуществляют кластеризацию входных образов, и использует правило конкурентного обучения [10]. Третий слой нейронной сети состоит из линейных нейронов и служит для отображения результатов классификации. Арбитр принимает окончательное решение о принадлежности того или иного образа к определенному классу. После процесса обучения нейросетевой детектор способен корректно классифицировать программные исполняемые модули и обнаруживать вредоносное ПО.

Искусственная иммунная система эмулирует основные принципы и механизмы биологической иммунной системы с целью построения распределенной самоорганизующейся системы для эффективного решения широкого круга инженерных задач, например – классификация образов, анализ и обработка больших массивов данных, оптимизация и т.д. Благодаря принципам и механизмам искусственной иммунной системы нейросетевые детекторы непрерывно эволюционируют и «подстраиваются» под особенности развития вредоносных программ и сетевых атак, позволяя системе киберзащиты адаптироваться к новым реалиям и поддерживать высокий уровень детектируемости вредоносных объектов.

Рассмотрим отдельный случай эволюции и адаптации нейросетевого иммунного детектора. Предположим, что *i*-й

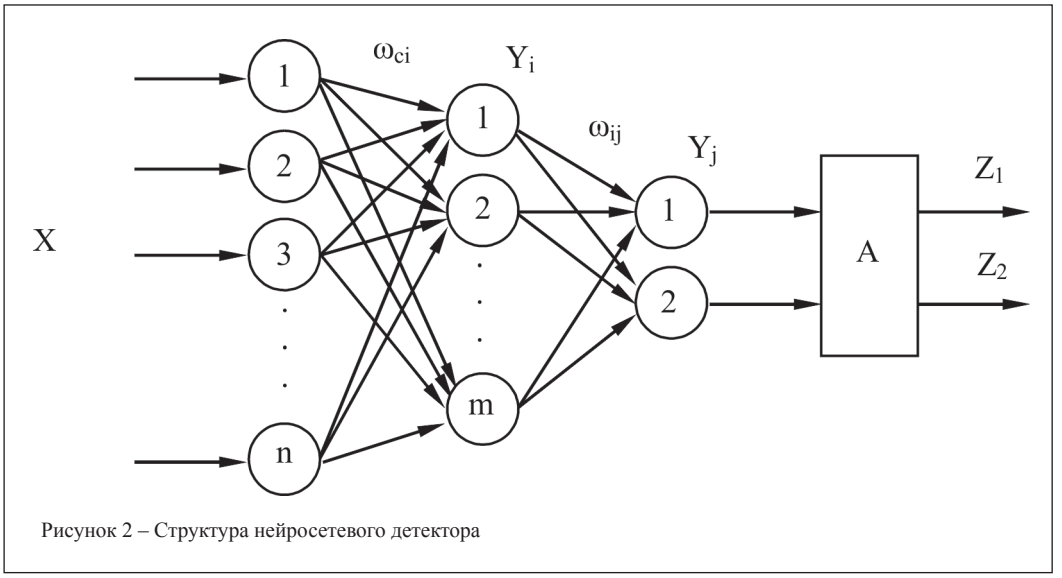

Рисунок 2 – Структура нейросетевого детектора

детектор обнаружил вредоносный объект и инициировал соответствующий сигнал. После этого он подвергается процедурам клонирования и мутации. В результате, в системе образуется некоторое количество новых однотипных детекторов, обучение которых проводилось на обнаруженном вредоносном объекте. Т.е. обнаруженный вредоносный объект инициировал механизмы эволюции. В общем случае алгоритм эволюции в нейросетевой искусственной иммунной системе может выглядеть следующим образом (рисунок 3):

1. Создание популяции *D* детекторово-клонов. Родителем является детектор, обнаруживший вредоносный объект.

2. Создается обучающая выборка *L* на основе обнаруженного вредоносного объекта.

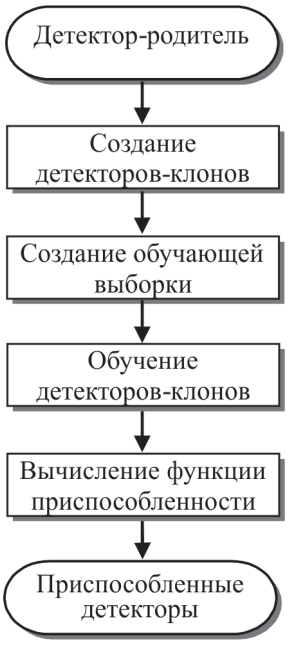

Рисунок 3 – Схема эволюции нейросетевых иммунных детекторов

3. Обучение детекторов-клонов на созданной обучающей выборке.

4. Вычисление функции приспособленности *F* обученных клонов. Если функция приспособленности детектора-клона ниже чем детектора-родителя, то детектор-клон уничтожается.

Функция приспособленности (фитнесс-функция) используется для определения «качества», или точности, обнаружения. В качестве функции приспособленности может использоваться среднеквадратичная ошибка между входным и выходным вектором нейросетевого иммунного детектора:

$$E_i = \frac{1}{2}\sum_{k=1}^{L}\sum_{j=1}^{2}(Z_{ij}^k - l_{ij}^k)^2, \quad (1)$$

где Z_{ij}^k – значение *j*-го выхода *i*-го детектора при подаче на вход его *k*-го образа; l_{ij}^k – эталонное выходное значение *i*-го детектора-клона.

Каждый иммунный детектор в системе имеет определенное время жизни в течении которого он сканирует программные объекты. Если на протяжении этого времени детектор не обнаруживает вредоносное ПО он уничтожается как заведомо «слабый» детектор, а на его место приходит новый. Однако не все детекторы заменяются на новые. Из списка детекторов-клонов, полученных в результате процесса эволюции, отбираются детекторы с наивысшим показателем функции приспособленности и трансформируются в так называемые детекторы иммунной памяти. Такие детекторы существуют в системе на протяжении всего периода ее функционирования и являются некоторым аналогом антивирусной базы сигнатур. Такие детекторы быстро реагируют на повторное проникновение в компьютерную систему вредоносного ПО, блокируют его и уничтожают.

Заключение

Сложившаяся ситуация требует совершенствования методов защиты компьютерных систем от новых киберугроз. Мы разработали и предложили принципиально новые алгоритмы организации системы киберзащиты, основанные на применении методов искусственного интеллекта. Разработанная система способна не только обнаруживать ранее известные вредоносные программы, но повысить уровень детектирования новых, ранее неизвестных вредоносных объектов. Предложенная система киберзащиты имеет способности к адаптации и эволюции. Разработанный подход можно применять не только для обнаружения вредоносных файловых объектов, но и для обнаружения сетевых вторжений [11]. Проведенные эксперименты [7, 11] подтверждают эффективность системы в обнаружении кибератак.

На сегодняшний день разработан действующий прототип, который выставлялся на многочисленных национальных и международных выставках и завоевал высокие награды. Разработанные методики и алгоритмы защищены патентом. Исследовательская работа поддерживалась рядом государственных грантов.

Литература:

1. Forrest, S. Self-nonself discrimination in a computer / S. Forrest, A. Perelson, L. Allen, R. Cherukuri // In Proceedings of the IEEE Symposium on Security and Privacy, 1994. – P. 202–212.

2. Burnet, F. The Clonal Selection Theory of Acquired Immunity / F. Burnet. – Cambridge University Press, 1959.

3. Jerne, N. Towards a network theory of the immune system. Ann. Immunology (Inst. Pasteur), 125C / N. Jerne. – 1974. – P. 373–389.

4. Greensmith, J. The deterministic dendritic cell algorithm / J. Greensmith, U. Aickelin // In Proc. of the 7th International Conference on Artificial Immune Systems (ICARIS). – Springer, 2008. – P. 291–302.

5. Harmer, P. An artificial immune system architecture for computer security applications / P. Harmer, P. Williams, G. Gunsch, G. Lamont // IEEE Transaction on Evolutionary Computation, 2002. – 6(3). – P. 252–280,

6. Безобразов, С.В. Нейросетевая искусственная иммунная система для обнаружения вредоносных программ: принципы построения / С.В. Безобразов, В.А. Головко // Вестник БрГТУ. Физика, математика, информатика. – 2009.

7. Безобразов, С.В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головко // Научная сессия НИЯУ МИФИ «Нейроинформатика»: материалы Всеросс. науч. конф., МИФИ, Москва, 25–29 янв. 2010. – Москва, 2010. – С. 273–287.

8. Головко, В.А. Проектирование интеллектуальных систем обнаружения аномалий / В.А. Головко, С.В. Безобразов // Материалы международной научно-технической конференции «Открытые семантические технологии проектирования интеллектуальных систем OSTIS-2011». – Минск: БГУИР, 2011. – С. 185–196.

9. Golovko, V. Evolution of Immune Detectors in Intelligent Security System for Malware Detection / V. Golovko, S. Bezobrazov, V. Melianchuk, M. Komar // Proceedings of the 6th IEEE international conference on intelligent data acquisition and advanced computing system IDAACS-2011. – Prague: Technical university, 2011. – P. 722–726.

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

11. Komar, M. Intelligent System for Detection of Networking Intrusion. / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov – In Proc. 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing System (IDAACS-2011). – Prague, Czech Republic, 2011. – P. 374–377.

Abstract

Artificial immune systems (AIS) and artificial neural networks (ANN) are very powerful technique for data mining and pattern recognition. Over the past few decades, application of these approaches has been growing rapidly in different domain. However, to date a consistent performance of AIS and ANN has not achieved. We sincerely believe that integration of these both techniques can allow constructing an intelligent system for information security. In this research we report a novel method for malicious code detection. It is based on main principles of AIS, which consist of different immune detectors and each immune detector represents counterpropagation neural network. The main goal of proposed approach is to detect unknown, previous unseen threat (malicious code, intrusion detection, etc.). It is achieved by the adaptation of the neural network immune detectors to the continually changeable computer environment. As a result the immune detectors have capability to evolve during a life. The evolution ability of neural immune detectors in artificial immune system is presented. The results of the experiments are shown the performance of the algorithm in increasing the quality of new, unknown threat detection.

Поступила в редакцию 18.05.2013 г.

ПОДХОД К ПОСТРОЕНИЮ СРЕДСТВ ЗАЩИТЫ «ОБЛАЧНЫХ» СИСТЕМ

УДК 004.3'2

В.И. Хведчук, В.В. Буслюк, С.С. Дереченник,
БрГТУ, г. Брест

Аннотация

В работе предлагается подход к хранению личных данных в корпоративной системе, базирующейся на «облачной» технологии. Проводится обзор известных решений в данной области. Рассмотрены базовые решения на базе протокола NFC. Выделены, в качестве основных, решения фирм Inside Secure и Texas Instruments. Предложена структура устройства на базе протокола, используемого в стационарных линиях связи с использованием отечественной элементной базы. В результате получается защищенная среда, позволяющая обеспечить доступ к «облачным» ресурсам и обеспечивающая мобильность корпоративных систем, построенных на современной основе. При этом необходимо решение дополнительно проблем с обслуживанием такого рода структур, связанных, прежде всего, с человеческим фактором. Здесь, конечно же, важную роль должно сыграть обучение кадров. Предполагается к использованию в корпоративной среде университета.

Введение

В настоящее время информационные технологии проникают в различные сферы деятельности человека, общества, государства. Происходит изменение обычных для нас процессов и объектов. Меняются способы оплаты услуг и