

РАЗДЕЛ I. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И НЕЙРОННЫЕ СЕТИ

ИСКУССТВЕННЫЕ ИММУННЫЕ СИСТЕМЫ: ПРИНЦИПЫ ПОСТРОЕНИЯ

Безобразов С. В., БГТУ, Брест

Современные компьютерные системы нуждаются в надежной системе защиты информации. Число компьютерных преступлений растет и по оценке специалистов, ущерб от них увеличивается на 35 процентов в год [1]. Современные антивирусные программы не обеспечивают должный уровень защиты компьютерных систем от вирусов и сетевых атак. Все это привело к поиску нетрадиционных методов в построении антивирусных программ. Изучая биологическую иммунную систему человека, мы приходим к выводу, что это совершенный механизм по защите человеческого организма от опасных бактерий и инфекций. Мы полагаем, что система, построенная на принципах биологической иммунной системы, значительно повысит уровень защиты компьютерных систем.

Основными элементами иммунной системы являются лимфоциты – белые клетки [2]. Существуют две разновидности лимфоцитов, которые образуются из стволовых клеток в костном мозге. После синтеза лимфоциты попадают в кровяное русло. Некоторые из них направляются к тимусу (вилочковой железе), где происходит их созревание (Т-лимфоциты). Другие же попадают в лимфатические узлы, и их созревание происходит там (В-лимфоциты). Процесс созревания незрелых лимфоцитов играет большую роль в иммунной системе и называется селекцией антител. В результате селекции уничтожаются нежелательные для организма лимфоциты. Зрелые лимфоциты имеют на своей поверхности детекторы, которые способны обнаруживать специфический антиген (вредные бактерии, вирусы). Контакт В-клеточных рецепторов со специфическим антигеном и связывание определенного его количества стимулируют рост этих клеток и последующее многократное деление. В результате образуются многочисленные клетки двух разновидностей: плазматические и «клетки памяти». Плазматические клетки синтезируют антитела, тем самым увеличивая количество клеток, способных обнаруживать вирус. Клетки памяти являются копиями В-клеток, однако имеют гораздо больший период жизни, что обеспечивает защиту организма от повторного заражения вирусом. При связывании определенного количества вируса, Т-клетки секретируют особую группу веществ, называемую лимфокинами. Некоторые лимфокины способны сами разрушать антиген и зараженные клетки. Другие лимфокины способствуют делению Т-клеток, в результате чего появляется большое количество антител, способные реагировать на обнаруженный антиген.

Биологическая иммунная система обладает качествами, которые необходимы для защиты компьютерных систем: способность защищать как организм, так и саму себя; распределенность, т.е. отсутствие центрального органа управления; динамичность; способность к адаптации, т.е. обнаружение и уничтожение новых, неизвестных вирусов; наличие иммунной памяти, в которой хранится информация о встречавшихся ранее вирусах.

Анализируя структуры различных вирусов, мы пришли к следующему выводу, что они разительно отличаются от «чистых» файлов, так как их действия направлены на нарушение нормального функционирования системы.

Основную роль в искусственной иммунной системе (ИИС) по обнаружению вирусов играют антитела, которые способны распознавать вредоносные программы.

Механизм генерации антител представляет собой случайный процесс. Суть его заключается в том, чтобы сгенерировать такую последовательность бит, которая была бы

максимально схожа со структурой возможного вируса. Каждый детектор наделяется жизненным циклом – промежутком времени, в течение которого антитело находится («живет») в компьютерной системе. Если, по истечении данного промежутка времени, антитело не обнаружило вирусов, оно должно быть уничтожено, и его место занимает другое антитело. Если же обнаружение произошло, то жизненный цикл данного антитела увеличивается. Этот механизм не только предотвращает систему от переполнения антителами, но и обеспечивает ИИС разнообразными по структуре детекторами.

Так как процесс создания антител по своей сути случайный процесс, то имеется вероятность создания таких антител, которые вместо вируса будут обнаруживать «чистый», незараженный файл. Механизм селекции предотвращает распространение таких антител по всей системе. Наиболее распространенным методом селекции антител является метод негативной селекции. Целью данного метода является отбор тех антител, которые по своей структуре не похожи на структуру «чистых» файлов. Таким образом, искусственная иммунная система получает способность реагировать на вредоносные программы, но не на «чистые» файлы.

После селекции, «зрелые» антитела попадают в систему и, на протяжении жизненного цикла, выполняют функцию по обнаружению вирусов, проверяя различные файлы. Основным методом обнаружения является строковое сравнение антитела и файла по соответствующим правилам. Правила сравнения могут быть различными, например: вычисление Евклидова расстояния, или расстояние Хэмминга, или правило r -смежных бит [3].

При обнаружении вируса в системе происходит мобилизация ИИС. Для успешной борьбы с найденным вирусом и зараженными им файлами необходимо иметь большое количество детекторов, одинаковых по своей структуре. Это обеспечивается путем создания большого количества копий детектора, который первый обнаружил вирус. Механизм создания большого количества копий называется клонированием [3]. Антитело, которое первым обнаружило вирус, и копии которого появляются в результате клонирования, называется «родителем». Сами же клоны называются «потомками». Существует многоуровневая система клонирования, т.е. «потомки», в свою очередь также могут стать «родителями» и иметь своих «потомков». Чем больше клоны структурно будут походить на вирус, тем быстрее и надежнее будет происходить обнаружение всех проявлений вируса. Для реализации этого процесса используется механизм внесения незначительных изменений в структуру клонов, который позволяет улучшить их характеристики. Этот механизм называется мутацией. С помощью механизмов клонирования и мутации ИИС адаптируется к обнаруженному вирусу, вырабатывает большое количество антител, что помогает ей успешно бороться с обнаруженным вирусом. После уничтожения всех следов вируса активность ИИС приходит в норму, общее количество всех антител восстанавливается, так как антитела имеют срок жизни, по истечении которого они уничтожаются.

Иммунная память ИИС является механизмом быстрого реагирования на повторные заражения вирусами, т.е. вирусами, которые когда-либо обнаруживались в компьютерной системе [3]. Иммунная память способна длительное время хранить информацию о встречавшихся ранее вирусах. Детектор, обнаруживший вирус, кроме того, что является объектом клонирования, еще делает полную копию самого себя. Эта копия детектора называется клеткой памяти и наделяется дополнительными свойствами. Совокупность клеток памяти образует иммунную память ИИС.

Описанная нами искусственная иммунная система обладает рядом особенностей, которые в выгодную сторону отличают ее от традиционных систем защиты информации. Мы полагаем, что искусственная иммунная система, построенная по принципу биологической иммунной системы, позволит поднять уровень безопасности компьютерных систем.

Литература

1. Почему не срабатывают антивирусы – <http://www.i2r.ru>, 2003
2. Иммунитет – <http://krugosvet.ru>, 2004
3. D. Dasgupta, Z. Ji, F. Gonzales. Artificial Immune System (AIS) research in the last five years. – issrl.cs.memphis.edu, 2003

ПРОГНОЗИРОВАНИЕ ПРИСТУПОВ ЭПИЛЕПСИИ

Безобразова С. В., БГТУ, Брест

Эпилепсия является распространенным нервно-психическим заболеванием. Согласно статистике лечебно-профилактических учреждений в последнее время наблюдается рост заболеваемости эпилепсией.

Основные исследования данного заболевания проводятся по средствам электроэнцефалографии. Электроэнцефалограмма (ЭЭГ) представляет собой суммарную запись электрической активности мозга, по которой можно судить не только о наличии эпилепсии, но и о причинах ее возникновения, очагах заболевания. Также по данным ЭЭГ производятся попытки предсказать появление приступов, что может значительно облегчить жизнь больным. Фактор «непредсказуемости» болезни затрудняет ее лечение, а также вызывает социально-психологические комплексы у больных эпилепсией, что усугубляет их психическое состояние.

Многие считают, что предсказание наступления припадков эпилепсии невозможно, так как между ними нет временных закономерностей, и они могут быть спровоцированы различными раздражающими факторами окружающей среды. Однако на сегодняшний день существует ряд подходов, направленных на предсказания эпилептических приступов и ориентированных на предиктальное состояние больного (состояние перед приступом):

- Сбор информации о жизни больного, развитии болезни, очень подробное описание приступов, а также состояний, им предшествующих, по возникновению которых в дальнейшем можно определить наступление новых приступов [5]. Важное значение играет способность больного описать свои ощущения, отметить повторяющиеся проявления (например: головные боли или слабость).

- Анализ ЭЭГ, который показывает, что при приближении приступа происходит синхронизация работы некоторых нейронов на уровне значений старшего показателя Ляпунова, что позволяет предсказать появление приступа, используя хаотическую природу сигналов ЭЭГ [2]. Требуется тщательной обработки данных (разделение сигналов, устранение шумов и помех).

Однако этими методами нельзя точно определить момент наступления приступа и тем более его продолжительность; также нельзя утверждать будет ли приступ один или их будет несколько (существуют случаи с часто повторяющимися приступами, которые следуют один за другим с малыми временными перерывами).