Использование иммунной сети для обнаружения атак на ресурсы распределенных информационных систем[1]

Н.А. Магницкий

Аннотация. Определен спектр информационных угроз и предложен оригинальный иммунносетевой метод обнаружения и анализа информационных атак в распределенных информационных системах.

Введение

Распределённая информационная система (далее РИС) представляет собой совокупность взаимосвязанных программных и аппаратных ресурсов, которые необходимо защищать от злоумышленных действий (атак) нарушителей. Обнаружение атак - процесс выявления таких злоумышленных действий, нацеленных на РИС.

Будем предполагать, что каждый ресурс РИС характеризуется состоянием, которое известно в любой момент времени. Для каждого состояния известен способ оценки его влияния на информационную безопасность РИС. Будем также предполагать, что для каждого ресурса смена его состояния наблюдаема и что наблюдатель имеет средства сбора информации о состояниях всех ресурсов РИС.

Состояние ресурса считается безопасным в текущий момент времени, если все использующие его объекты имеют права доступа к данному ресурсу и характеристика загруженности ресурса меньше порога загруженности. Состояние ресурса считается опасным в текущий момент времени, если хотя бы один из использующих его объектов не имеет права доступа к данному ресурсу или характеристика загруженности ресурса равна емкости ресурса. Информационно безопасное состояние - это состояние РИС, при котором все ресурсы РИС находятся в безопасном состоянии. Атака на РИС - это последовательность действий, производимых нарушителем и ведущих к нарушению информационной безопасности системы. Цель атаки - перевод системы в опасное состояние, при котором для одного или нескольких ресурсов нарушена конфиденциальность, целостность или доступность. Нарушение конфиденциальности - ситуация, когда информацией обладает посторонний субъект. Нарушение целостности - ситуация, когда произошло умышленное искажение (модификация или удаление) данных, хранящихся в РИС или передаваемых из одной РИС в другую. Нарушение доступности - ситуация, когда доступ к данному ресурсу для легальных пользователей блокирован. Блокирование может быть постоянным либо вызывать задержку, достаточно долгую для того, чтобы ресурс стал бесполезным.

Атаки, направленные на различные объекты РИС и различающиеся по своей реализации, можно разделить на пять классов [1,2]: атаки на сетевые ресурсы – связанные группы хостов, коммутационных элементов и каналов передачи данных; атаки на файловые ресурсы - данные, представленные в форме файлов; атаки на программные ресурсы - программы, находящиеся в стадии исполнения; атаки на ресурсы баз данных - точки доступа, дисковое про-

[1] Работа поддержана программами фундаментальных научных исследований ОНИТ РАН, проект № 2.4. и проект № 3.5.

странство, файловые и системные утилиты, утилиты администратора; атаки на вычислительные ресурсы - процессоры, память.

1. Математическая постановка задачи обнаружения атак

Состояние РИС в момент времени t определим вектором наблюдаемых параметров $x(t) = (x_1(t), x_2(t),...,x_n(t))$. Будем рассматривать конкретную атаку определенного класса как траекторию в n - мерном пространстве параметров: $L_i = (x(t), x(t+\tau),...,x(t+k\tau))$, где τ - период замеров значений параметров. Обозначим через $L=(L_1, L_2,...,L_m)$ множество траекторий всех атак данного класса. Пусть L_i - наблюдаемая в процессе функционирования РИС траектория. Тогда если $L_i \in L$, то на РИС осуществлена атака. Таким образом, для обнаружения атак необходимо построить множество L и определить принадлежность наблюдаемой траектории L_i к этому множеству.

Пусть T - конечная длительность атаки заданного класса и τ – период времени замера наблюдаемых параметров, т.е. на траектории проведения атаки задано $k = T/\tau$ состояний РИС. Для каждого замера параметров в пространстве параметров существует набор несвязных областей, таких, что попадание замера в одну из этих областей означает принадлежность траектории множеству L на данном замере (т.е. возможность принадлежности наблюдаемой траектории к одной из возможных траекторий атак при условии, что все предшествующие замеры принадлежали множеству L). Полагаем, что если в ходе k замеров состояний РИС траектория на каждом замере попадала в одну из таких областей, то она принадлежит множеству L – множеству траекторий соответствующего класса атак.

Пусть $G(t)=\{G_1(t), G_2(t),...,G_l(t)\}$ - множество областей таких, что попадание замера x(t) в одну из этих областей означает принадлежность траектории к множеству L на данном замере. Таким образом, задача обнаружения атак сводится к задачам: построения несвязного множества областей G для каждого интервала k-го замера; определения принадлежности замеренного состояния РИС к одной из этих областей $x \in G$. Следовательно, задача обнаружения атак для одного замера параметров может быть сформулирована следующим образом: задана обучающая выборка x^j, j=1,...,J, такая, что для любого x^j известно, что $x^j \in G$ или $x^j \notin G$. Требуется построить иммунную сеть, решающую задачу принадлежности наблюдаемого состояния РИС к одной из областей множества G. Решение поставленной задачи методом искусственных нейронных сетей представлено автором в [3]. Метод решения аналогичной задачи обобщенной искусственной иммунной сетью предложен автором ниже.

2. Решение задачи методом искусственных иммунных сетей

2.1. Определение искусственной иммунной сети

В то время как в основе искусственной нейронной сети лежит понятие искусственного нейрона, в основе искусственной иммунной сети лежит понятие формального монопептида. Следуя [4], формальным монопептидом без ограничения общности будем называть кватернион вида

$$Q(\psi) = \begin{pmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix} \cos(\psi/2) + \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \sin(\psi/2), \quad (1)$$

зависящий от угла ψ, называемого торсионным углом, $-\pi < \psi < \pi$.

Свободной энергией формального монопептида будем называть функцию

$$V(\psi) = -v_{11} \cos^2(\psi/2) - v_{12} \cos(\psi/2)\sin(\psi/2) - v_{22} \sin^2(\psi/2), \quad (2)$$

где v_{11}, v_{12}, v_{22} – постоянные управления формальным монопептидом. В зависимости от значений торсионного угла ψ формальный монопептид может находиться в разных состояниях, отвечающих различным значениям свободной энергии $V(\psi)$. Наибольший интерес представляют устойчивые стационарные состояния формального монопептида, отвечающие локальным минимумам свободной энергии. Такие состояния являются устойчивыми особыми

точками нелинейного дифференциального уравнения

$$\dot{\psi}(t) = -\frac{\partial V(\psi)}{\partial \psi}.$$

С математической точки зрения основным достоинством представления формального монопептида в виде (1) является возможность записи полипептида - произведения формальных монопептидов, зависящих от разных углов, в виде одного формального монопептида, зависящего от суммы углов, т.е.

$$\begin{aligned} &Q(\psi_1)Q(\psi_2)\cdot\ldots\cdot Q(\psi_{n-1})Q(\psi_n) = \\ &= Q(\psi_1 + \ldots + \psi_n) = \\ &= \begin{pmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix} \cos((\psi_1 + \ldots + \psi_n)/2) + \\ &+ \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \sin((\psi_1 + \ldots + \psi_n)/2), \end{aligned}$$

Последнее представление дает возможность формально определить искусственную иммунную сеть как сеть, состоящую из n формальных монопептидов, состояния которых определяются функцией свободной энергии, являющейся суммой свободных энергий отдельных монопептидов и свободной энергии полипептида, представляющего собой произведение

$$V(\psi_1,\ldots,\psi_n) = V_0(\psi_1 + \ldots + \psi_n) + \sum_{i=1}^{n} V_i(\psi_i). \quad (3)$$

При этом устойчивые стационарные состояния иммунной сети будут являться устойчивыми особыми точками нелинейной автономной системы обыкновенных дифференциальных уравнений относительно торсионных углов $\psi_1, \ldots, \psi_n$:

$$\dot{\psi}_i(t) = f_i(\psi_1,\ldots,\psi_n) = -\frac{\partial V(\psi_1,\ldots,\psi_n)}{\partial \psi_i}, \quad i = 1,\ldots,n \quad (4)$$

Будем интерпретировать конечномерный куб векторов $\psi=(\psi_1,\ldots,\psi_n) \in K^n = \{\psi: -\pi \le \psi_i \le \pi\}$ как пространство параметров (признаков) задачи обнаружения атаки определенного класса. При этом процедура обучения иммунной сети (2)–(4) решению задачи обнаружения атаки сводится к выбору управляющих параметров формальных монопептидов и полипептида таким образом, чтобы все векторы ψ^m, $m = 1,\ldots,M$, обучающей выборки являлись устойчивыми особыми точками системы нелинейных дифференциальных уравнений (4). Тогда пространство параметров окажется разбитым на области притяжения устойчивых особых точек (векторов обучающей выборки), и для любого нового вектора $\psi \in K^n$ его принадлежность (или не принадлежность) множеству атак G будет вытекать из принадлежности (или не принадлежности) множеству атак G того вектора обучающей выборки, к которому сойдется решение системы нелинейных уравнений (4) с начальным условием $\psi(0) = \psi$.

К сожалению, запись свободной энергии классического формального монопептида в виде (2) с постоянными управлениями, предложенная в [4], не дает возможности решить поставленную задачу. В связи с этим для решения этой задачи предлагается использовать построенную ниже обобщенную иммунную сеть, в которой управления формальными монопептидами и полипептидом зависят от торсионных углов и строятся соответствующим образом по векторам обучающей выборки.

2.2. Построение обобщенной иммунной сети

Функцию свободной энергии формального монопептида (2) можно, очевидно, записать в виде

$$V(\psi) = -[v_{11}(1+\cos\psi) + v_{12}\sin\psi + v_{22}(1-\cos\psi)]/2 = a + h\sin(\psi + c),$$

где a,h,c – новые независимые управления. Тогда $\partial V/\partial\psi = h\cos(\psi+c)$. Из последнего представления видно, что на самом деле независимыми являются только два управления: модуль h и фаза с производной свободной энергии.

Сделаем следующие обобщения. Будем считать модуль h последнего выражения зависящим от угла ψ, т.е. $\partial V/\partial\psi = h(\psi)\cos(\psi+c)$. Тогда функция свободной энергии формального монопептида запишется в виде

$$E(\psi) = \int h(\psi)\cos(\psi + c)d\psi. \qquad (5)$$

В выражении для частной производной свободной энергии формального полипептида будем считать переменной фазу $c(\psi)$. При этом функция свободной энергии полипептида запишется в виде

$$E_0(\psi_1,...,\psi_n) =$$

$$= -\int \cos(g(\psi_1 + ... + \psi_n))d(\psi_1 + ... + \psi_n), \quad (6)$$

где g – некоторая функция суммы торсионных углов. Тогда система дифференциальных уравнений, описывающая процесс изменения состояний обобщенной таким образом иммунной сети, примет вид

$$\dot{\psi}_i(t) = f_i(\psi) =$$

$$= \cos(g(\sum_{k=1}^{n}\psi_k)) - h_i(\psi_i)\cos(\psi_i + c_i), \quad (7)$$

$i = 1,...,n.$

Обобщенная иммунная сеть (5)-(7) имеет n неопределенных параметров c_i, n неопределенных функций $h_i(\psi)$ и одну неопределенную функцию $g(\psi_1+\ldots+\psi_n)$. Определение этих параметров и функций должно происходить в процессе обучения сети.

2.3. Алгоритм обучения обобщенной иммунной сети

Рассмотрим всю обучающую выборку из N векторов

$$\psi^m = \left(\psi_1^m,..., \psi_n^m\right)^T, \ m = 1,..., N,$$

принадлежащих как к изучаемому классу атак, так и к другим классам атак, либо вообще не являющихся атаками. Определение параметров c_i, функций $h_i(\psi)$ и $g(\sum\psi_i)$ иммунной сети (5)-(7) должно осуществляться, исходя из двух условий:

1) все векторы ψ^m обучающей выборки должны быть особыми точками системы дифференциальных уравнений (7), т.е. для всех $m = 1,..., N$ должны выполняться равенства

$$\cos(g(\sum_{k=1}^{n}\psi_k^m)) = h_i(\psi_i^m)\cos(\psi_i^m + c_i), i = 1,..., n;$$

2) особые точки системы дифференциальных уравнений (7), отвечающие векторам обучающей выборки, должны быть устойчивыми, т.е. для всех $m = 1,..., N$ собственные значения всех матриц Якоби правой части системы (7), вычисленных в особых точках, должны иметь отрицательные вещественные части.

Для каждого $i = 1,...,n$ параметр c_i выбираем из условия, что для всех $m = 1,..., N$ $\cos(\psi_i^m + c_i) \neq 0$. Функцию $g(x) = g(\psi_1 + ... + \psi_n)$ определим следующим образом

$$g(x) = \prod_{m=1}^{N}(x - x_m), \text{ где } x_m = \sum_{k=1}^{n}\psi_k^m. \qquad (8)$$

Ясно, что $g(x_m) = 0$ для любого $m = 1,..., N$, т.е. в любой точке обучающей выборки функция g обращается в нуль. Поэтому из условий (1) следует, что

$$h_i(\psi_i^m) = 1/\cos(\psi_i^m + c_i) = p_{im}, i = 1,..., n. \qquad (9)$$

Из выражения (8) для функции $g(x)$ следует, что якобиан правой части системы дифференциальных уравнений (7), вычисленный на любом векторе ψ^m обучающей выборки, является диагональной матрицей с диагональными элементами

$$a_{ii} = -h_i'(\psi_i^m)\cos(\psi_i^m + c_i) + h_i(\psi_i^m)\sin(\psi_i^m + c_i).$$

Величины a_{ii} являются в данном случае собственными значениями якобиана, поэтому для удовлетворения условия устойчивости особой точки приравняем их некоторому отрицательному значению, например, $d < 0$. Тогда, учитывая выражение (9), получаем формулы для определения производных искомых функций $h_i(\psi)$ в точках ψ_i^m:

$$h_i'(\psi_i^m) = (d\cos(\psi_i^m + c_i) +$$

$$+ \sin(\psi_i^m + c_i))/\cos^2(\psi_i^m + c_i) = q_{im}. \quad (10)$$

Итак, процедура обучения обобщенной иммунной сети свелась к построению n функций одной переменной $h_i(\psi)$, $i = 1,...,n$, имеющих в заданных точках ψ_i^m заданные значения p_{im} самих функций и заданные значения q_{im} их производных. Простейшим способом решения последней задачи является выбор непрерывных кусочно-линейных функций $h_i(\psi)$. С этой целью для каждого i упорядочим значения i-ых координат векторов обучающей выборки

$$\psi_i^{j_1} \le \psi_i^{j_2} \le \ldots \le \psi_i^{j_m} \le \ldots \le \psi_i^{j_M}.$$

На отрезках, содержащих значения $\psi_i^{j_m}$, функцию $h_i(\psi)$ строим следующим образом

$$h_i(\psi) = q_{ij_m}(\psi - \psi_i^{j_m}) + p_{ij_m},$$
$$a_i^{j_m} \le \psi \le b_i^{j_m},$$

где

$$a_i^{j_m} = \psi_i^{j_m} - (\psi_i^{j_m} - \psi_i^{j_{m-1}})/3,$$
$$b_i^{j_m} = \psi_i^{j_m} + (\psi_i^{j_{m+1}} - \psi_i^{j_m})/3.$$

Вне этих отрезков функцию $h_i(\psi)$ достраиваем линейно по значениям этой функции $h_i(a_i^{j_m})$ и $h_i(b_i^{j_m})$, уже вычисленным в концах отрезков, содержащих точки $\psi_i^{j_m}$:

$$h_i(\psi) =$$
$$= (h_i(a_i^{j_m}) - h_i(b_i^{j_{m-1}}))(\psi - b_i^{j_{m-1}})/(a_i^{j_m} - b_i^{j_{m-1}}) + h(b_i^{j_{m-1}}),$$
$$b_i^{j_{m-1}} \le \psi \le a_i^{j_m}.$$

Построенные таким образом функции $g(x)$ и $h_i(\psi_i)$ удовлетворяют условиям (1)-(2) устойчивости всех векторов обучающей выборки как особых точек нелинейной автономной системы обыкновенных дифференциальных уравнений (7).

2.4. Применение обобщенной иммунной сети

Решение задачи о принадлежности некоторого вектора $\psi \in K^n$ множеству $G \subset K^n$ атак заданного класса с использованием обученной обобщенной иммунной сети (7)-(10) происходит следующим образом. Координаты вектора ψ задают начальное условие для решения системы дифференциальных уравнений (7). При этом решение $\psi(t)$ системы (7) с заданным начальным условием $\psi(0) = \psi$ будет стремиться при $t \to \infty$ к некоторой устойчивой особой точке системы, являющейся вектором обучающей выборки. Тогда принадлежность (или не принадлежность) вектора ψ множеству атак G будет вытекать из принадлежности (или не принадлежности) множеству атак G того вектора обучающей выборки, к которому сойдется решение системы нелинейных уравнений (7) с начальным условием $\psi(0) = \psi$.

Заключение

Построенная обобщенная иммунная сеть (7)-(10) обладает по крайней мере двумя важными достоинствами, позволяющими говорить о возможности ее использования для решения задачи обнаружения атак: 1) она применима к решению задач, множества входной информации которых имеют сложную многосвязную структуру; 2) метод ее обучения является прямой вычислительной процедурой и не сводится к поиску глобального экстремума какой-либо сложной нелинейной функции, что не накладывает никаких принципиальных ограничений ни на размерность задачи, ни на размерность обучающей выборки.

Литература

1. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. - СПб.: БХВ - Петербург, 2001.
2. Лукацкий А. Обнаружение атак, - СПБ.: БХВ - Петербург, 2000.
3. Магницкий Н.А. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем. // Труды ИСА РАН, 2008.
4. Тараканов А.О. Математические модели обработки информации на основе результатов самосборки. Диссертация д.ф.-м.н. С.-П., 1999.

Магницкий Николай Александрович. Заведующий лабораторией Института системного анализа РАН. Окончил МГУ в 1974 году. Доктор физико-математических наук, профессор кафедры НДС и ПУ ф-та ВМК МГУ, академик РАЕН. Автор более 150 публикаций, в том числе 5 монографий. Область научных интересов – нелинейные дифференциальные уравнения, хаотическая динамика, нейронные сети, математическое моделирование. E-mail: nmag@isa.ru; mag@su29.ru