Управление рисками и безопасностью

Обнаружение информационных атак в компьютерных сетях методом распределенных нелинейных динамических систем*

Н. А. Магницкий

Аннотация. В работе предложен оригинальный метод анализа информационных атак в компьютерных сетях с использованием аттракторов распределенных динамических систем, описываемых нелинейными системами дифференциальных уравнений с частными производными. Предлагаемый подход позволяет детектировать, запоминать и классифицировать непрерывные траектории векторов наблюдаемых параметров информационных систем с целью обнаружения производимых на них компьютерных атак. Метод может быть использован также для распознавания и классификации непрерывных двумерных и трехмерных графических объектов и образов.

Ключевые слова: *компьютерные атаки, нелинейная распределенная система, распознавание образов.*

Введение

Распределенная 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. 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 пространство, файловые и системные утилиты, утилиты администратора; атаки на вычислительные ресурсы—процессоры, память.

Состояние РИС в момент времени t характеризуется вектором наблюдаемых параметров $x(t) = (x_1(t), x_2(t), ..., x_m(t))$. В работах [3, 4] каждая конкретная атака определенного класса рассматривалась как траектория в n-мерном пространстве параметров: $L_i = (x(t), x(t+\tau), ..., x(t+k\tau))$, где τ — период замеров значений параметров. Множество траекторий всех атак данного класса обозначалось через $L = (L_1, L_2, ..., L_l)$. 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 было построить множество L и определить принадлежность наблюдаемой траектории L_i к этому множеству.

* Работа выполнена при поддержке РФФИ (проект №11–07–00126а) и программы ОНИТ РАН №4 (проект 2.5).

В настоящей статье рассмотрен случай, когда замеры значений параметров РИС происходят непрерывно во времени. Пусть T — конечная длительность атаки заданного класса. В этом случае вектор наблюдаемых параметров $x(t)$ представляет собой непрерывную траекторию в пространстве параметров, заданную на отрезке $[0, T]$, и в пространстве параметров существует набор несвязных областей таких, что попадание вектора $x(t)$ в одну из этих областей означает принадлежность траектории множеству L.

Пусть $G = (G_1, G_2, ..., G_j)$ множество областей таких, что попадание вектора $x(t)$ в одну из этих областей означает принадлежность траектории к множеству L. Таким образом, задача обнаружения атак сводится к задачам: 1) построения несвязного множества областей G; 2) определения принадлежности замеренной траектории состояний РИС к одной из этих областей $x(t) \in G$. Следовательно, задача обнаружения атак в данном случае может быть сформулирована следующим образом: задана обучающая выборка непрерывных векторов $x^k(t), k = 1, ..., n$ такая, что для любого $x^k(t)$ известно, что $x^k(t) \in G$ или $x^k(t) \notin G$. Требуется построить алгоритм в некотором функциональном пространстве непрерывных траекторий, решающий задачу принадлежности наблюдаемого вектора состояний РИС к одной из областей множества G.

1. Метод распознавания траекторий распределенной динамической системой

Не накладывая фактически никаких ограничений на рассматриваемые траектории (образы траекторий), будем считать в самом общем виде, что траектория описывается вещественной квадратично интегрируемой функцией $f(x) \in L_2(\Omega)$, где Ω произвольная область в конечномерном евклидовом пространстве. В нашем случае обнаружения компьютерных атак — это пространство наблюдаемых параметров РИС, в случае, например, распознавания печатных, рукописных текстов или фотографических изображений $n = 2$, $f(x)$ — интенсивность изображения, Ω — область, геометрически совпадающая с естественным носителем изображения (листом бумаги, фотокарточкой и т. д.).

Пространство $L_2(\Omega)$ является гильбертовым пространством со скалярным произведением

$$(f, v) = \int_{\Omega} f(x)v(x)\,dx, \;\; (f, f) = \|f\|^2 .$$

Пусть заданы n прототипов образов: f_1, f_2, ..., f_n. Без ограничения общности считаем их линейно-независимыми квадратично интегрируемыми вещественными функциями. Будем хранить прототипы образов в ЭВМ в виде ортогональной системы функций v_1, v_2, ..., v_n, построенной по функциям f_1, f_2, ..., f_n:

$$v_k = \frac{y_k}{\|y_k\|},$$

$$y_k = \begin{vmatrix} (f_1, f_1)\ (f_1, f_2)\ \dots\ (f_1, f_{k-1})\ f_1 \\ (f_2, f_1)\ (f_2, f_2)\ \dots\ (f_2, f_{k-1})\ f_2 \\ \hline (f_k, f_1)\ (f_k, f_2)\ \dots\ (f_k, f_{k-1})\ f_k \end{vmatrix}, \qquad (1)$$

$$y_1 = f_1, k = 1, \dots, n.$$

Ясно, что $(y_k, f_i) = 0$, $i = 1, \dots, k-1$, следовательно, $(y_k, y_i) = 0$, $i = 1, \dots, k-1$. Кроме того, $(y_k, f_k) = \Delta_k$ — определитель Грамма, и $\|y_k\|^2 = (y_k, y_k) = \Delta_{k-1}\Delta_k$ ($\Delta_0 = 1$). Заметим, что для получения ортонормальной системы прототипов образов v_k, $k = 1, \dots, n$, достаточно вычислить скалярные произведения $\left(f_i, f_j\right)$, $i, j = 1, \dots, n$. Для того, чтобы добавить к системе $\{v_k\}$ еще один прототип, достаточно вычислить дополнительно скалярные произведения (f_{n+1}, f_k), $k = 1, \dots, n+1$. Таким образом, процесс обучения системы может идти очень просто и быстро, а сама система может содержать любое количество прототипов образов.

Пусть нам теперь задан некоторый образ $v_k \in \in L_2(\Omega)$. Построим алгоритм идентификации заданного образа такой, что если $u(x, 0) = v(x)$ при $t = 0$ лежит в окрестности прототипа $v_k(x)$, то $u(x, t) \to v_k(x)$ при $t \to \infty$. Рассмотрим функционал

$$J(u) = -\frac{1}{2}\sum_{k=1}^{n}(u, v_k)^2 + \\ +\frac{1}{2}\sum_{k\neq i}(u, v_k)^2 (u, v_i)^2 + \frac{1}{4}\|u\|^4 . \qquad (2)$$

Оказывается, искомый алгоритм распознавания образов сводится к решению задачи Коши для уравнения

$$\frac{\partial u(x, t)}{\partial t} = -gradJu, \quad u(x, 0) = v(x). \qquad (3)$$

Если предъявленный образ $v(x)$ находится в окрестности одного из прототипов образов $v_k(x)$, то для решения задачи Коши (3) имеет место

$$u(x, t) \to v_k(x), \quad t \to \infty.$$

Заметим, что уравнение (3) может быть записано в виде

$$\frac{\partial u(x,t)}{\partial t} = \sum_{k=1}^{n} (u, v_k)\, v_k(x) - \\ - \sum_{k\neq i} [(u, v_k)^2 (u, v_i)\, v_i(x) + \\ + (u, v_i)^2 (u, v_k)\, v_k(x)] - \\ - (u, u)\, u(x); \quad u(x,0) = v(x). \tag{4}$$

Вернемся теперь к постановке задачи, когда прототипами образов являются не ортонормальные функции $v_k(x)$, но произвольные линейно-независимые функции $f_1(x)$, $f_2(x)$, ..., $f_n(x)$; $f_k(x) \in L_2(\Omega)$, а предъявленный к распознаванию образ описывается функцией $g(x) \in L_2(\Omega)$, лежащей в окрестности одного из прототипов $f_k(x)$. Построим отображение $v = v(g)$ такое, что окрестность точки f_k при отображении v переходит в окрестность точки v_k. Способы построения такого отображения, вероятно, могут быть различными. Мы полагаем

$$v(g)(x) = \sum_{k=1}^{n} \left(\prod_{i\neq k} \frac{\|g - fi\|^2}{\|fk - fi\|^2} \right) v_k(x). \tag{5}$$

Ясно, что $v(f_j) \equiv v_j$ и, следовательно, если образ g лежит в окрестности прототипа f_k, то $v(g)$ лежит в окрестности v_k, что вытекает из непрерывности отображения (5). Для вычисления выражения (5) необходимо знание величин (g, g), (g, f_k) и(f_k, f_i), $k, i = 1, \ldots, n$. Так как скалярные произведения (f_k, f_i) уже вычислены при построении ортонормальной системы функций v_1, ..., v_n, то для вычисления выражения (5) требуется найти только значения скалярных произведений (g, g) и (g, f_k), $k = 1, \ldots, n$. Таким образом, при идентификации предъявленного произвольного образа $g(x)$ последовательность действий должна быть следующей:

1) вычисление функции $v(g)(x)$ по формуле (5);
2) решение уравнения (4) с начальными условиями $u(x, 0) = v(g)(x)$;
3) определение функции $v_k(x) = \lim u(x, t)$, $t \to \infty$;
4) отождествление предъявленного образа $g(x)$ с прототипом $f_k(x)$.

2. Теоретическое обоснование метода.

Приведем две теоремы, доказывающие возможность применения рассмотренного выше метода к решению поставленной задачи.

Теорема 1. *Функционал $J(u)$ не может иметь локальных минимумов в точках, отличных от точек $\pm v_k$, $k = 1, \ldots, n$.*

Действительно, функционал $J(u)$ не может иметь локальных минимумов в подпространстве, ортогональном подпространству $L(v)$, натянутому на ортонормальную систему функций $\{v_k\}$, так как при движении по перпендикуляру в сторону подпространства $L(v)$ значение функционала $J(u)$ уменьшается (первые два слагаемых остаются неизменными, третье — уменьшается). Значение функционала $J(u)$ уменьшается также и при движении по подпространству $L(v)$ в сторону ближайшей координатной оси v_k при $\|u\| = \text{const}$ (первое и третье слагаемые остаются неизменными, второе — уменьшается). На координатных осях, когда $u = \alpha v_k$, функционал $J(u) = -\alpha^2/2 + \alpha^4/4$ может иметь минимумы только в точках $\alpha = \pm 1$.

Теорема 2. *Функционал $J(u)$ имеет локальные минимумы $J(u) = -1/4$ в точках $u = \pm v_k$, $k = 1, \ldots, n$, причем в окрестности каждой точки $\pm v_k$ функционал $J(u)$ является строго выпуклым. Других локальных минимумов функционал $J(u)$ не имеет.*

Действительно, вычисляя градиент $J'(u) = \text{grad}\ J(u)$ и гессиан $J''(u)\psi$ функционала $J(u)$, получим

$$J'(u) = -\sum_{k=1}^{n} (u, v_k)\, v_k + \sum_{k\neq i} [(u, v_k)^2 (u, v_i)\, v_i + \\ + (u, v_i)^2 (u, v_k)\, v_k] + \|u\|^2 \tag{6}$$

и

$$J''(u)\psi = -\sum_{k=1}^{n} (v_k, \psi)\, v_k + \sum_{k\neq i} [(u, v_i)\, v_k + \\ (u, v_k)\, v_i]\, [(u, v_k)\, (v_i, \psi) + (u, v_i)\, (v_k, \psi)] + \\ + 2\,(u, \psi)\, u + (u, u)\, \psi. \tag{7}$$

Нетрудно показать, что для $\forall k$ существует окрестность $O(\pm v_k)$ и $\alpha > 0$ такие, что для $\forall u \in O(\pm v_k)$ и $\forall \varphi \left(J''(u)\varphi, \varphi\right) \geqslant \alpha \|\varphi\|^2$, откуда и из $J'(\pm v_k) = 0$, $k = 1, \ldots, n$, вытекает, что функционал $J(u)$ имеет локальные минимумы в точках $\pm v_k$ и является строго выпуклым в окрестностях этих точек. Последнее утверждение теоремы следует из теоремы 1.

3. Заключение

Предложенный метод анализа информационных атак в компьютерных сетях с использованием аттракторов распределенных динамических систем обладает по крайней мере несколькими важными достоинствами по сравнению с предложенными автором ранее методами бинарных нейронных сетей и иммунных сетей [3, 4]: метод применим к решению задачи в случае непрерывного отслеживания

вектора наблюдаемых параметров информационной системы; метод не накладывает никаких принципиальных ограничений ни на размерность задачи, ни на размерность обучающей выборки, ни на гладкость траекторий векторов наблюдаемых параметров. Кроме того, предложенный метод может быть использован для распознавания и классификации других непрерывных двумерных и трехмерных графических объектов, таких, например, как распознавания печатных и рукописных текстов или фотографических изображений и образов.

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. М.: Ленанд/URSS, 2008. Т. 33. С. 200–205.
4. *Магницкий Н. А.* Использование иммунной сети для обнаружения атак на ресурсы распределенных информационных систем // Информационные технологии и вычислительные системы. 2009. Вып. 3. С. 22–26.

Магницкий Николай Александрович. Зав. лаб. ИСА РАН. Д. ф.-м. н., профессор. Окончил в 1974 г. МГУ им. М. В. Ломоносова. Количество печатных работ: более 200, 6 монографий. Область научных интересов: интегральные и дифференциальные уравнения, нелинейные хаотические динамические системы, нейронные сети и математическое моделирование. E-mail: nikmagn@gmail.com