Секция «Дифференциальные уравнения, динамические системы и оптимальное управление»

Алгоритм анализа критичности узлов системы защиты на основе безмасштабных сетей

Сусакин Павел Алексеевич
Выпускник (специалист)
Московский авиационный институт (национальный исследовательский университет), Москва, Россия
E-mail: pavelsusakin@yandex.ru

Современное общество с каждым годом все более становится зависимым от информационной инфраструктуры, в которую на ряду с потребительскими службами плотно интегрируются государственные службы, автоматизированные системы управления в различных областях промышленности. Такая среда активно используется не только рядовыми гражданами, но и преступными лицами с целью нарушения целостности данных систем, компрометации конфиденциальной информации, а также получения несанкционированного доступа к контролю управляющих узлов систем. Таких лиц будем называть злоумышленниками.

В настоящее время основу информационной инфраструктуры составляют глобальные и локальные вычислительные сети, которые строятся с использованием как проводных, так и беспроводных технологий. Поэтому злоумышленнику зачастую нет необходимости напрямую воздействовать на потенциальный объект системы, а в зависимости от наличия у него необходимой информации об узлах системы достаточно выбрать критические узлы, защита которых ниже, чем у центральных. С помощью реализации различных методов воздействия (угроз) злоумышленник поражает критические узлы и может нарушить работу центральных узлов.

Таким образом, необходимо иметь эффективные методы выявления критических узлов, которые требуют дополнительных мер безопасности в целях снижения риска возникновения таких состояний системы, когда она становится неуправляемой.

Достижение цели системы защиты, заключающейся в защите центральных узлов системы и предупреждении атак злоумышленника, возможно за счет решения следующих задач:

- выявление критических узлов системы;
- определение вероятных угроз злоумышленника при атаке системы, на основе информации из внешней среды;
- повышение защищенности критических узлов системы, на основе проведенного анализа.

Для достижения поставленных задач разработаны алгоритмы поиска критических узлов системы и определения вероятных угроз злоумышленника и программа, реализующая данные алгоритмы.

Оценка критичности узлов основана на возможности управления системой злоумышленником. Динамическая система является управляемой, если с подходящим набором входов она может быть переведена из любого начального состояния до любого желаемого конечного состояния в конечное время.

Состояние системы описывается с помощью системы дифференциальных уравнений:

$$\dot{s}(t) = A(t)s(t) + B(t)z(t) + f(t), \tag{1}$$

где s – n-мерный вектор фазового состояния;

z – k-мерный вектор управлений;

A(t) и *B(t)* – матрицы соответствующих размерностей с вещественными, непрерывными при $t \in [0, +\infty)$, элементами;

f(t) – непрерывная при $t \in [0, +\infty)$ вектор-функция.

В случае, когда матрицы A и B стационарны, существует достаточное условие полной управляемости (критерий Калмана) [2]: для того, чтобы система (1) с постоянными матрицами A и B была полностью управляемой, необходимо и достаточно, чтобы:

$$rank(S) = rank(B, AB, ..., A^{n-1}B) = n. \tag{2}$$

Чтобы применить критерий Калмана в произвольной системе, необходимо знать веса всех связей (то есть, $a_{i,j}$), которые для большинства реальных систем или неизвестны, или известны только примерно и зависят от времени. Даже если все веса известны, грубый поиск требует, чтобы мы вычислили ранг S в течение $2^N - 1$ различных операций, что является вычислительно недостижимой задачей для крупных систем.

Чтобы обойти необходимость измерения весов связей и вычисления ранга, отметим, что система *(A,B)* является *структурно управляемой*, если возможно выбрать ненулевые веса в A и B так, что система будет удовлетворять (2). Для достижения структурной управляемости, необходимо определить набор управляющих узлов, достаточный для контроля системы в целом [4].

Доказано, что минимальное число входов или управляющих узлов, необходимых для поддержания полного контроля над системой, определяется максимальным паросочетанием в системе [5]. Чтобы оценить критичность каждого узла, необходимо составить набор максимальных паросочетаний V.

Для определения критических узлов системы введено понятие *степени критичности* k узла. Узел s является критическим узлом степени $k \in \overline{1, n}$, если существует такой максимальный по мощности набор $\{V_1, V_2, ..., V_k\} \subseteq V$, что

$$s \in \bigcap_{i=1}^{k} V_i. \tag{3}$$

.

Определим V^k как множество всех узлов системы со степенью критичности, равной k. Каждому узлу $s \in V^k$, где $k \in \overline{1, n}$, поставим в соответствие коэффициент критичности – число, равное отношению k/n.

Таким образом, полученный коэффициент критичности отражает, в какой доле возможных структурных управлений, данный узел является критическим (управляющим) узлом системы. Защита узлов с наибольшим коэффициентом критичности является первоочередной задачей с целью предупреждения атаки злоумышленника.

Определение вероятных угроз злоумышленника возможно на основе информации, доступной из внешней среды.

Пусть имеется множество EE автоматизированных систем управления $S \in EE$. Угрозы АСУ опишем в виде множества $Z = \{z_1, z_2, ..., z_k\}$.

Искомый вектор реальных угроз можно представить с помощью информационно-параметрического базиса [2], исходя из знания информации из внешней среды:

$$V(z, S) = \{z \in Z : I_n(z, S) \cap I_o(z, S) \neq \varnothing\}. \tag{4}$$

где $I_n(z, S)$ – информация "провоцирующая"в отношении системы S угрозу z;

$I_o(z, S)$ – информация о реализации угрозы z в отношении системы S.

Поиск данного вектора равносилен решению задачи определения системы общих представителей [1] угроз для узлов исследуемой системы.

В результате проведенной работы разработаны методы и алгоритмы оценки критичности узлов системы и определения вероятных угроз злоумышленника, а также разработана программа, реализующая данные алгоритмы.

Источники и литература

1) Райгородский А.М. Ситемы общих представителей в комбинаторике и их приложения в геометрии. – М.: МЦНМО, 2009. – 136 с.
2) Смирнов Н.В., Смирнова Т.Е., Тамасян Г.Ш. Стабилизация программных движений при полной и неполной обратной связи: Учебное пособие. – СПб.: «СОЛО», 2013. – 131 с.
3) С.В. Смуров, А.М. Гладков, П.В. Воронов. Формализованное представление субпроблемы «системности» в общей проблеме обеспечения безопасности автоматизированных систем // Известия Института инженерной физики. – 2014. – № 4 (34). – С. 2-8.
4) Lin, C.-T. Structural controllability // IEEE Trans. Automat. Contr. – 1974. – № 19. – С. 201-208.
5) Y.-Y. Liu, J.-J. Slotine, A.-L. Barbasi Controllability of Complex Networks // Nature. – 2011. – № 473. – С. 167-173.