Построение логических моделей опасных состояний комплексов средств автоматизации автоматизированных систем

О.В. Сидельников, email: olegvsk@mail.ru

Краснодарское высшее военное училище
им. генерала армии С.М. Штеменко

Аннотация. *Рассмотрен способ построения логических моделей опасных состояний комплекса средств автоматизации (КСА) автоматизированных систем (АС) на основе метода логического вывода. Распознавание опасных состояний КСА сводится к логическому выводу, т.е. к выбору значений целевого признака, не вступающих в противоречие с системой, обнаруживаемых на этапе обучения закономерностей.*

Ключевые слова: *опасное состояние, комплексы средств автоматизации автоматизированных систем, логические модели.*

Введение

Опасное состояние КСА АС – это синоним чрезвычайного состояния, при котором возник ущерб «большого» масштаба [1]. Низкая своевременность обнаружения опасных состояний КСА АС, выхода контролируемых параметров за пределы допустимых значений, выхода из строя одного элемента или нескольких элементов системы может повлечь отказ всей системы. Отказ всей системы может развиться за достаточно короткий промежуток времени, что может вызвать развитие опасной ситуации.

Проблемы анализа состояния надежности и безопасности, своевременность выявления перехода в опасное состояние АС рассмотрены в трудах Дружинина Г.В., Ушакова И.А., Можаева С.А., Рябинина И.А., Острейковского В.А., Швыряева Ю.В. и др. В данных работах рассматриваются фундаментальные основы логико-вероятностного анализа безопасности и надежности объектов мониторинга АС, аналитические и графические формы представления опасного состояния системы [1,2].

1. Опасное состояние КСА АС

В статье [3] рассмотрена адаптация метода логического вывода закономерностей состояний информационно-телекоммуникационных

систем (ИТКС). Автор предлагает основывать классификацию сигнатур опасных состояний КСА АС в булевом пространстве признаков на предварительном построении «области запрета», описываемой посредством дизъюнктивной нормальной формы (ДНФ) с конъюнкциями ограниченного ранга. Данные конъюнкции задают запретные интервалы в булевом пространстве и интерпретируются как импликативные закономерности. Простота этой закономерности оценивается числом переменных, входящих в нее, т.е. рангом конъюнкции, а мощность – объемом области запрета. Распознавание опасных состояний основано на решении задачи реконструкции множества «реальных» объектов, подчиняющегося определенным импликативным закономерностям по его случайной выборке. Распознавание опасных состояний КСА сводится к логическому выводу, т.е. к выбору значений целевого признака, не вступающих в противоречие с системой, обнаруживаемых на этапе обучения закономерностей.

2. Построение логических моделей опасного состояния комплексов средств автоматизации

Описание возможного сценария опасных состояний (СОС) КСА АС в процессе его функционирования представляет наибольшую трудность при исследовании безопасности. Описание СОС не имеет алгоритма и является творческим процессом. В логико-вероятностной теории безопасности СОС осуществляется с помощью логической функции опасности системы (ФОС), аргументами которой выступают инициирующие события (ИС) и условия, в качестве которых могут быть короткие замыкания в электросети, разряды молнии, искрение электрооборудования, сварочные работы, диверсионные акты, отказы, нарушения правил эксплуатации, ошибки операторов, деструктивные воздействия, в том числе, заключительная фаза компьютерной атаки, различные повреждающие воздействия и иные причины, приводящие к чрезвычайной ситуации [1,2]. На основании СОС с помощью кратчайших путей опасного функционирования (КПОФ) либо с помощью минимальных сечений предотвращения опасности составляется логическая ФОС.

КПОФ – это конъюнкция инициирующего события (y_i), ни одну из компонент которой нельзя изъять, не нарушив опасного функционирования системы. Функция алгебры логики (ФАЛ) этой конъюнкции имеет вид (формула 1).

$$\Phi_i = \bigwedge_{i \in K_{\Phi_i}} y_i \qquad (1)$$

где K_{Φ_i} – множество номеров ИС, соответствующих данному i-му КПОФ.

Следовательно, КПОФ описывает один из возможных вариантов попадания системы в опасное состояние с помощью минимального набора ИС, абсолютно необходимых для его осуществления, т.е. данного варианта опасного состояния системы [2]. Аналитические и графические формы представления опасного состояния системы, СОС, структурные модели систем в виде схем подробно рассмотрены в работах [1,2].

Рассмотрим способ построения логических моделей опасного состояния КСА АС на основе выявления целевого признака класса опасных состояний на основе поиска импликативных закономерностей в форме конъюнкций ограниченного ранга.

Шаг 1. Формирование пространства признаков.

Допустим, предметами мониторинга параметров сетевого трафика ЛВС КСА АС служат объекты некоторые класса (сетевые пакеты протокола IP), моделируемые в булевом пространстве признаков $x_1, x_2, ..., x_n$.

Для мониторинга опасных состояний КСА АС построим матрицу информативности признаков опасных состояний. Логические переменные описывают параметрами инициирующего состояния (значение «1» соответствует появлению инициирующего события; значение «0» соответствует отсутствию инициирующего события).

Поиск закономерностей опасных состояний КСА АС будем осуществлять в форме конъюнкций. На практике используют различные эвристики для сокращённого целенаправленного поиска конъюнкций, близких к оптимальным. Идея всех этих методов заключается в том, чтобы не перебирать огромное количество заведомо не информативных предикатов [4].

Шаг 2. Построение модели исследуемого класса в алгебраической форме в виде ДНФ запрета.

При рассмотрении булевых функций с большим числом переменных описанные способы приведут к слишком громоздким таблицам и матрицам. В этих случаях более практичным окажется алгебраический способ представления, когда булева функция записывается формулой, задающей некоторую суперпозицию достаточно простых и имеющих специальные обозначения функций, которые образуют базис алгебраического представления.

Элементами булевой алгебры являются булевы константы, булевы переменные и булевы функции. Булевых констант всего две, и их

принято обозначать через 0 и 1. Значениями булевых переменных могут служить только булевы константы. Булевы функции, называемые иногда ФАЛ, также принимают значения из множества $\{0,1\}$. Аргументами булевых функций являются булевы переменные. Будем полгать, что их число всегда конечно. Комбинации значений булевых переменных $x_1,x_2,...,x_n$ называют наборами. Множество наборов образуют булево пространство M, содержащее 2^x элементов. Наборы будем рассматривать как булевы векторы, в которых последовательно перечисляются значения переменных. Например, вектор 111010 задает следующую комбинацию значений переменных: $x_1 = 1$, $x_2 = 1$, $x_3 = 1$, $x_4 = 0$, $x_5 = 1$, $x_6 = 0$. Чтобы задать булеву функцию, надо определить ее значения на всех наборах, тогда функция будет полностью, или всюду, определена. Мы будем рассматривать в основном именно такие функции. Случаи, когда значения функции определены лишь на некоторых наборах называются не полностью, или не всюду, определенными. Простейшим способом задания булевой функции является табличный, при котором строится таблица всех наборов и соответствующих им значений функции. Можно ограничиться перечислением лишь тех наборов, на которых булева функция f принимает значение 1. Множество таких наборов называется характеристическим множеством функции f и обозначается через M_f. Это представление более компактно, особенно в тех случаях, когда мощность (для конечного множества – число элементов) множества M_f относительно невелика. Множество M_f удобно представлять при этом в форме булевой матрицы, строками которой служат отдельные элементы из M_f. Назовем этот способ задания булевой функции поэлементным. При рассмотрении булевых функций с большим числом переменных описанные способы приведут к слишком громоздким таблицам и матрицам. В этих случаях более практичным окажется алгебраический способ представления, когда булева функция записывается формулой, задающей некоторую суперпозицию достаточно простых и имеющих специальные обозначения функций, которые образуют базис алгебраического представления. Наиболее известен и во многих отношениях удобен булев базис, состоящий из одноместной функции «отрицание» ($\neg x$, или $\overline{x}$) и двуместных функций «конъюнкция» и «дизъюнкция». Эти функции, называемые также функциями НЕ, И и ИЛИ соответственно. Конъюнкция и дизъюнкция

являются коммутативными и ассоциативными операциями, что означает выполнение равносильностей: $x_1 x_2 = x_2 x_1$, $x_1 \vee x_2 = x_2 \vee x_1$, $(x_1 x_2) x_3 = x_1 (x_2 x_3)$, $(x_1 \vee x_2) \vee x_3 = x_1 (x_2 \vee x_3)$. Это позволяет ввести в рассмотрение соответствующие многоместные функции: дизъюнкцию $x_1 \vee x_2 \vee \ldots \vee x_k$ принимающую значение 1 тогда и только тогда, когда хотя бы один из аргументов примет значение 1, и конъюнкцию, принимающую значение 1 в том и только том случае, если все аргументы примут это значение. Многоместная конъюнкция различных переменных, когда некоторые из них могут быть заменены их отрицаниями, называется элементарной конъюнкцией (минтерм). Элементарная дизъюнкция (макстерм) образуется дизъюнкцией конечного множества логических переменных (аргументов) и их отрицаний. Число аргументов, образующих элементарную конъюнкцию или дизъюнкцию, является её рангом. Если логическая функция представлена через инверсию, конъюнкцию и дизъюнкцию, то такая форма ее представления называется нормальной. Любая булева функция может быть представлена в дизъюнктивной нормальной форме (ДНФ), из чего следует полнота системы функций, образующих булев базис, т.е. возможность представления суперпозициями этих функций любых булевых функций. При использовании аналитических форм представления логических функций используется принцип суперпозиции, заключающийся в замене одних аргументов данной функции другими. Существует простой способ перехода от табличной формы представления булевой, функции к частному случаю ДНФ, а именно к совершенной дизъюнктивной нормальной форме (СДНФ), в которой все элементарной конъюнкции должны быть полными. Члены СДНФ получаются из элементов характеристического множества M_f путем замены их компонент символами соответствующих переменных и простановки знаков отрицания над символами переменных, принимающих в рассматриваемом наборе значение 0. Например, $M_f = \{000, 001, 101\}$, то СДНФ функции f представляется выражением $\overline{x_1}\,\overline{x_2}\,\overline{x_3} \vee \overline{x_1}\,\overline{x_2}\,x_3 \vee x_1\,\overline{x_2}\,x_3$.

Представим каждую элементарную конъюнкцию рассматриваемой ДНФ троичным вектором, компоненты которой получают значения «–», «0», «1». Символ «–» является символом неопределенности. Интерпретируем этот вектор как множество двоичных векторов, которые можно получить из него заменой значений «–» всевозможными комбинациями нулей и единиц, данное множество, называемое

интервалом булева пространства M, оказывается характеристическим множеством рассматриваемой элементарной конъюнкции. В множество M попадают $2k$ наборов, где k – число значений «–» в троичном векторе, или, что то, же самое, число переменных, символы которых отсутствуют в рассматриваемой элементарной конъюнкции. Характеристическое множество булевой функции, представленной некоторой ДНФ, оказывается равным объединению всех интервалов, соответствующих элементарным конъюнкциям, входящим в состав данной ДНФ. Элементарная конъюнкция $\overline{x_1 x_4 x_6}$ представляется троичным вектором $0--1-1$ (полагаем $n=6$), которое можно представлять сжатое представление множества, образованного наборами 000101, 000111, 001101, 001111, 010101, 010111, 011101, 011111, легко получаемого из вектора $0--1-1$. Подставляя вместо «–» произвольные комбинации нулей и единиц, получаем все элементы интервала. Поэтому множество рассматриваемого типа называется интервалом.

Булевы функция, заданная посредством ДНФ $(\overline{x_1}\,\overline{x_3 x_4} \vee x_2 x_3 \vee x_1 x_2 x_4)$ может быть отображена троичными векторами, объединение этих интервалов приведет к характеристическому множеству данной функции, упорядочив его $\{0110, 0111, 1000, 1100, 1101, 1110, 1111\}$. Анализ ДНФ и их характеристических множеств в ряде случаев существенно облегчается, если представляющие их множества троичных и булевых векторов группируются в матрицы. Заданная ДНФ, может быть задана троичной матрицей (формула 2).

$$\begin{bmatrix} 1 & - & 0 & 0 \\ - & 1 & 1 & - \\ 0 & 1 & - & 0 \end{bmatrix} \qquad (2)$$

Кроме операций булева базиса (отрицания, конъюнкции и дизъюнкции), в алгебраических представлениях используются иногда двуместные операции «дизъюнкция с исключением» $x_1 \oplus x_2$, «эквиваленция» $x_1 \sim x_2$ и «импликация» $x_1 \to x_2$. Таким образом, в алгебраическом представлении булева функция выражается формулой в виде некоторой последовательности символов переменных, операторов $\neg, \wedge, \vee, \oplus, \sim, \to$, а также скобок, указывающих порядок применения операторов. Существуют правила использования формул:

1) любой символ булевой переменной ($x_1, x_2, \ldots x_n$ могут использоваться также символы $a, b, \ldots z$) являются формулой;

2) если A – формула, то $\neg A$, или $\overline{A}$, – тоже формула;

3) если A и B – формулы, то выражения $(A \vee B)$, $(A \wedge B)$, $(A \oplus B)$, $(A \sim B)$, $(A \to B)$ также являются формулами. Совокупность правил задает порождаемый синтаксис формул. Существуют классы операторов. Оператор связывает формулы тем сильнее, чем меньше номер класса, к которому он принадлежит:

1 класс: $\neg$;

2 класс: $\wedge$;

3 класс: $\vee, \oplus$;

4 класс: $\sim, \to$.

Преобразование алгебраических выражений логических функций основано на том, что возможно изменение структуры цепей логических схем без изменения их результирующего действия.

Часть из них совпадает с соответствующими законами, применяемыми при преобразовании обычных алгебраических выражений, часть же является специфичной для алгебры логики.

В нашем рассматриваемом примере при построении модели класса системы видим пустыми интервалы третьего ранга и выдвигаем гипотезу о соответствующих импликативных закономерностях.

Предположим, что среди интервалов, ранги которых не превышают трех, пустыми оказались лишь те, которые представлены строками следующей троичной матрицы, где компоненты принимают значения из трехэлементного множества $\{0,1,-\}$ (формула 3). Столбцы наборов в матрице импликативных закономерностей T соответствуют слева на право: x_1, x_2, x_3, x_4, x_5, x_6.

$$T = \begin{bmatrix} 1 & - & 1 & - & - & 0 \\ - & 1 & - & - & 0 & 0 \\ 0 & - & - & 0 & 1 & 1 \\ - & 0 & - & 1 & - & 1 \\ - & 0 & 0 & 0 & - & 1 \end{bmatrix} \qquad (3)$$

Эта матрица импликативных закономерностей T будет моделью исследуемого класса опасных состояний. Строки интерпретируются как импликативные закономерности: первая строка утверждает, что в данном классе не существует объектов, обладающих признаками x_1 и x_3, но не обладающих в тоже признаком x_6.

Шаг 3. Выбор целевого признака из системы закономерностей и упрощение.

Пусть в данном примере роль целевого признака играет признак опасного состояния – x_6. При $x_2 = 0$ становится излишней строка 2, так как задаваемая ею область запрета не содержит элементов с таким значением признака x_2 ($x_2 = 1$ во второй строке) и следовательно, не пересекается с интервалом возможного существования объекта, не обладающего признаком x_2. Удалив ее вместе со столбцом x_2, получим остаток (формула 4).

$$T = \begin{bmatrix} 1 & 1 & - & - & 0 \\ 0 & - & 0 & 1 & 1 \\ - & - & 1 & - & 1 \\ - & 0 & 0 & - & 1 \end{bmatrix} \qquad (4)$$

Если, $x_2 = 1$, следует анализировать остаток матрицы T (выпадают строки 4 и 5, где x_2 соответствуют $\{0,-\}$ (формула 5).

$$T = \begin{bmatrix} 1 & 1 & - & - & 0 \\ - & - & - & 0 & 1 \\ 0 & - & 0 & 1 & 1 \end{bmatrix} \qquad (5)$$

Таким образом, из остатка матрицы T можно записать в алгебраической форме представление признака x_6 через другие признаки (формула 6).

$$x_6 = \overline{x_5} \vee \overline{x_1} \wedge \overline{x_4} \wedge x_5 \qquad (6)$$

Обнаружение (поиск и выявление) импликативных закономерностей опасных состояний КСА АС основано на выборе целевого признака из системы закономерностей и снижении размерности векторов образов сигнатур опасных состояний.

Заключение

Таким образом, рассмотренный способ построения логических моделей опасных состояний КСА АС на основе логического вывода позволяет осуществлять не весь перебор возможных классификационных признаков состояний, а ограничиться сокращенным перебором.

Список литературы

1. Рябинин И.А. Надежность и безопасность структурно-сложных систем.– СПб.: Политехника, 2000.– 248 с.: ил. –98 с.

2. Острейковский, В.А. Безопасность атомных станций. Вероятностный анализ / В.А. Острейковский, Ю.В. Швыряев. – М: ФИЗМАТЛИТ, 2008.– 352 с.

3. Сидельников,О.В. Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах / О.В. Сидельников, В.Н. Лаптев, В.А. Шарай // Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2011. – № 72(08). – 10 с. – Режим доступа : http://ej.kubagro.ru/2011/08/pdf/37.pdf.

4. Закревский, А.Д. Логика распознавания / Изд.2-е, доп. – М.: Едиториал УРСС, 2003. – 144 с.