УДК 004.621:681.322 Капустян М.В., Хорошко В.А., Чирков Д.В. (ГУИКТ)

ПРИМЕНЕНИЯ СЕТЕЙ ПЕТРИ ДЛЯ ОЦЕНКИ ТЕХНИЧЕСКОГО СОСТОЯНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Разработка и исследование математических моделей технических систем защиты информации (ТСЗИ) требует значительных затрат времени. Как показывает опыт, применения сетей Петри (СП) для этих целей ускоряет процесс их создания. Однако их математический аппарат несколько громоздок и при реализации на ПЭВМ занимает большие объемы памяти. Для решения практических задач требуется компактная отражающая сущность поведения ТСЗИ модель. Особенно остро этот вопрос стоит для моделирования в реальном масштабе времени при эксплуатации.

Анализ последних достижений

Известные на сегодняшний день интерпретации расширения и модификации сетей Петри [1,2] позволяют в основном моделировать параллельные одновременные процессы в программном (алгоритмическом) обеспечении вычислительных систем (на разных уровнях – от системного до микропрограммного), т.е. для моделирования выполнения двух и более различных алгоритмов на одной и той же вычислительно-управляющей системе требуется при известных подходах создание двух или более сетей Петри для изучаемых алгоритмов. Кроме того, в таких случаях традиционно требование отсутствия критических свойств в построенных моделях. В случае обнаружения какого-либо критического свойства делается вывод о неработоспособности рассматриваемого алгоритма и выполняются действия по такому изменению алгоритма, чтобы во вновь построенной адекватной модели критические свойства не были обнаружены. Основной недостаток такого подхода заключается в большой трудоемкости процесса многократного построения и изменения моделей алгоритма для изучения их работоспособности.

Цель работы

Целью работы является рассмотрение возможности применения сетей Петри для оценки технического состояния технических систем защиты информации.

Основная часть

Таким образом, опыт использования модификации сетей Петри для моделирования сложных систем и оценки технического состояния их позволяет утверждать, что средства моделирования должны обладать следующими свойствами:

- иерархическое представление моделей;
- единые средства построения и описания моделей на всех уровнях иерархии;
- простота детализации моделей;
- легкость машинного представления создаваемых моделей;
- возможность концентрации внимания только на необходимых (анализируемых) состояниях и режимах работы системы;
- возможность использования одной модели в разных целях;
- возможность моделирования до уровня логических элементов;
- использование формальных методов оптимизации процесса моделирования и анализа;
- наличие способов контроля корректности построения модели и исследование свойств модели;
- возможность представления всего моделируемого и анализируемого процесса в динамике;
- простота и наглядность при формулировке проблемы или алгоритма оценки технического состояния (ТСЗИ).

В результате проведенного анализа известных попыток использования сетей Петри для анализа технического состояния ТСЗИ была разработана оригинальная модификация – аппаратные СП [3].

Для эффективного использования широкого спектра возможностей АСП необходимо создание на базе АСП-системы специального математического обеспечения с набором средств описания, ввода, трансляции, компоновки, имитации модели, обработки результатов моделирования и анализа.

В настоящее время известен ряд способов описания исходных моделей и внутримашинного представления моделей ТСЗИ для проведения имитационных экспериментов на базе СП.

При построении системы имитационного моделирования на СП существенную роль играет выбор:

1) способа описания исходных моделей;
2) способа внутримашинного представления описанной модели и на его основе – организации алгоритма моделирования.

Внутримашинное представление СП может быть организовано в виде матриц либо в виде списковых структур.

В нашем случае внутримашинное представление в матричной форме СП может быть описана двумя матрицами: матрицей инцидентности E размерностью nxm , где n - число вершин мест, m - число вершин переходов модели, и матрицей движения меток F размерностью , которые определяются следующим образом:

1) $E(i,j)=1$, если $P_i \in P_{ij}^I$; $E(i,j)=0$, если $P_i \notin P_{ij}^I$;

2) $F(i,j)=\alpha+\beta$, где $\alpha=1$, если $P_i \in P_{ij}^I$; $\alpha=0$, если $P_i \notin P_{ij}^I$; $\beta=-1$, если $P_i \in O_{ij}^0$; $\beta=0$, если $P_i \notin O_{ij}^0$

Обозначим A^j - j-й столбец матрицы A. Тогда можно утверждать:

а) переход t_j может быть запущен, если $E^j - \overline{m_0}^{(k)}$;

б) последующая разметка после срабатывания t вычисляется по формулам

$$\overline{m_0}^{(k+1)} = \overline{m_0}^{(k)} + F^{(j)},$$

$$\neg[E_j \to \overline{m_0}^{(k)}] \equiv [E^j \overline{m_0}^{(k)}] = [E^j / \overline{m_0}^{(k)} = 0].$$

Следовательно, условие запуска перехода t_j состоит в выполнении условия $E^j \overline{m_0}^{(k)} = 0$, а последующая разметка вычисляется так: $\overline{m_0}^{(k+1)} = \overline{m_0}^{(k)} \oplus B^j$, где $\oplus$ - обозначение операции, исключающее ИЛИ; $B(i,j)=1$, если $F(i,j) \neq 0$; $B(i,j)=0$, если $F(i,j)=0$.

Здесь все операции выполняются над векторами булевых переменных, что позволяет достаточно эффективно реализовать этот способ на ПЭВМ.

Недостаток указанного способа заключается в необходимости проверки на каждом шаге моделирования разметки всех входных мест каждого из переходов, что приводит к значительным неэффективным затратам времени. Более высокое быстродействие достигается путем представления каждого из переходов t_v одним из мест $P_\varepsilon^r \in P_{tv}^I$. Для запуска перехода t_v необходимо (но недостаточно) выполнение $m(P_\varepsilon^r)=1$.

Определим вектор булевых переменных D размерностью mx1, а также матрицы A и C размерностью mxm:

- $D(j)=1$, если $m(P_i^r)=1$, $P_i^r \in P_{ij}^I$;
- $C(i,j)=1$, если t_j и t_i представлены одним и тем же местом P_ε^r;
- $A(i,j)=1$, если t_j представлено местом $P_\varepsilon^r \in Q_{ij}$.

Тогда после срабатывания t_i последующая разметка вычисляется по формуле $D^+ = D \oplus A^j \oplus C^j$ и моделирующий алгоритм выглядит следующим образом:

DATA INPUT
FOR j:=1 TO m DO
IF D(j)=1
THEN IF $\overline{m_0}^{(k)} E_j = 0$

THEN <генерация действий, соответствующих t_j>

$$\overline{m_0}^{(k+1)} = m_0^{(k)} \oplus B_j$$

$$D^+ = D \oplus L^j,$$

Здесь $L^j = A^j \oplus C^j$ позволяет экономить объем используемой памяти. При таком подходе можно сократить время выполнения программы с одновременным увеличением объема занимаемой памяти (за счет матрицы L и вектора D). Для снижения объема занимаемой памяти целесообразно внутримашинное представление моделей в виде стековых структур, так как E, F, L – разреженные матрицы. В результате размер используемой памяти линейно зависит от значений m и n, тогда как в случае матричного представления этот размер пропорционален mxn.

Одним из способов достижения компромисса между сложностью и достоверностью математической модели является упрощение эквивалентный объекту сети производящееся с помощью маршрутов функционирования системы [1] на основе аппарата нечетных множеств и нечетких отношений в пространстве определяемом расширяемой базой делимых ТСЗИ. В эту же базу данных заносятся сведения о поведении системы при внешних воздействиях. Модели получаемые таким способом, имеет управляемую размерность и на основе строгих математических правил преобразуется либо в компактный либо в расширенный вид. Достоверность модели ТСЗИ является не выходным а входным параметром для моделирования. Отсюда и главное достоинство такого подхода маршрутная модель с заранее задеваемой достоверностью позволяющая прогнозировать динамику состояния ТСЗИ.

Рассмотрим принципы построения маршрутов, маршрутных моделей и моделирующей базы данных (БД). Примем за X универсальное множество возможных соотношений X моделируемого объекта. Пусть X моделируется с требуемой достоверностью φ множеством описаний M_0, состоящем из элементов $\overline{m}$.

Поэтому:

$$M_0 \le x;$$

$$M_0 = \{M / \overline{M} \in X, \mu(\overline{M}) \ge 1 - \varphi\}, \quad (1)$$

где $\mu(M)$-функция принадлежности описания $\overline{M}$ множеству X.

Маршрут , как отображение марковского процесса с нечеткими начальными условиями по отношению к нечеткому множеству описаний M_0, является множеством уровня $\alpha \ne 1 - \varphi$;

$$M = \{\overline{M} / M_0, \mu(\overline{M}) > \alpha\}. \quad (2)$$

Однако учитывая правила упорядочения элементов в M_0 маршрут можно представить в виде $A\overline{P}N = (P, T, K, S)$, где M_0 отображает характер компонента APN.

Будем считать, что множество отношений, соответствующих «нормальному» маршруту (НМ) $M_н$, определяется как:

$$M_H = \{\overline{M} / \overline{M} \in M_0, \mu_H(\overline{M}) > \beta\}, \quad (3)$$

где β - параметр задаваемой устойчивости ТСЗИ к внешним воздействиям.

В то же время для «экспериментального» маршрута (ЭМ) $M_Э$ справедливо следующее утверждение.

$$M_Э = \left\{ M / \overline{M} \in M_0, \mu_Э(\overline{M}) > \beta' \right\}, \quad (4)$$

где β' - параметр задеваемой границы неустойчивости ТСЗИ.

При расширении и сужении множеств моделирующих отношений следует руководствоваться следующими принципами: расширения НМ с учетом ЭМ;

$$M_1 = \left\{ \overline{M} / \overline{M} \in \overline{M}_0, M_1(\overline{M}) \right\}, \quad (5)$$

где

$$M_1(\overline{M}) = \begin{cases} 0, если (\mu_Э(\overline{M}) X \mu_H(\overline{M})) < \beta; \\ \max\left[\mu_Э(\overline{M})\right] если \left[\mu_Э(\overline{M}) V \mu_H(\overline{M})\right] \geq \beta; \end{cases}$$

Сужение ЭМ с учетом НМ

$$M_2 = \left\{ \overline{M} / M \in \overline{M}_0, M_2(\overline{M}) \right\}, \quad (6)$$

где

$$M_2(M) = \begin{cases} 0, если \left[M_Э(\overline{M}) V \mu_H(M)\right] \geq \beta, \\ \max\left[M_Э(M), M_H(M), если \left[M_Э(M) M_H(M)\right]\right. \end{cases}$$

Из условий (5) и (6) следует:

$$\lim_{\beta \to 0} M_1 = \lim_{\beta \to 0} M_2 = M_0 \quad (7)$$

Скорость переходов и достоверность размещений для позиций моделирующей СП является мерой информативности соответствующим им отношений.

При $\beta = 1$ в СП, синтезируемую на маршрутных множествах, войдут наиболее «живые» переходы СП, построенной на M_0 [3]. По мере роста количества узлов СП функция СП функция принадлежности перехода множеству «живых» переходов убывает. Заменив понятия скорость на экспертную оценку принадлежности перехода множеству «живых» переходов, удается обойти от непосредственного решения вопроса о возможности срабатывания того или иного перехода.

Для множеств состояний типа маршрутных множеств исходное состояние обозначим через M_P, а достижимое из него как M_P^+ . Тогда прогноз как линейный оператор описывается следующим образом:

$$F = M_P^- = M_P^+, \quad (8)$$

где F – линейный оператор прогноза:

$$M_P^- \subseteq \text{и } M_P^+ \subseteq M_1.$$

Прогноз как функционал определяется в базисе M_0 как функция принадлежности состояния M_P^- множеству оценок технического состояния ТСЗИ. Аспекты прогноза имеют свои прогнозы в APN и формализуется как линейный оператор в пространстве, порождаемом M_0, и как функционал, определяемый линейной формой в пространстве M_0.

Из соотношения (8) видно, что прогноз как линейный оператор и как функционал образует дерево возможностей, так как по определению из выражений (5) и (6) следует, что мощность M_1 больше, чем M_2. При машинной реализации это приводит к решению задач комбинаторного типа и к экспоненциальному росту размерностей модели. Вследствие этого проводим отсечение ветвей, т.е. принимаем к рассмотрению только те ветви дерева возможностей, функция принадлежности которых M_0 не менее β. Основой для реализации приведенного подхода на ПЭВМ служит выделение и анализ так называемых стационарных состояний ТСЗИ. По отношению к M_0 множество стационарных состояний определяется как

$$M_0 \leq M_C,$$
$$M_C\left\{ \overline{M} / \overline{M} \in M^0, M^C\left(\overline{M}\right) \right\} \cong 1,$$

где M_C - множество стационарных состояний. Все элементы M_C являются корнями НМ при отсутствии внешних воздействий. Внешнее воздействия образуют пространство возмущений, базисом которого является элементарные воздействия [4]. Каждому элементу M_C соответствует нечетко ограниченное подпространство пространства возмущений. Иными словами, элементам M_C присваивается чувствительность к элементам базиса пространства возмущений, тем самым давал начало ЭМ. OS каждого стационарного состояния ведет свое начало множество ЭМ, по одному на каждый нулевой элемент базиса подпространства возмущений. Отношений между маршрутным множествами и множеством стационарных состояний поля $M_Э \cap M_C = M_H \cap M_C = M_C$.

Другими словами, базисные воздействия порождают символы деревьев возможности.

Анализ стационарных состояний ТСЗИ должен выявить взаимосвязь между ними. В случае большой сложности оборудования применяются экспертные оценки взаимосвязанности элементов M_0. Результат анализа – СП стационарных состояний (СПСС), является основой для построения БД и прогнозирования технического состояния ТСЗИ.

Так как СПСС включает себя узловые моменты функционирования ТСЗИ, то она отражает характер поведения оборудования согласно заложенному алгоритму. Таким образом, СПСС является моделью штатной работы ТСЗИ. Прогнозируемость технического состояния ТСЗИ опирается на марковский характер функционирования оборудования, с одной стороны и на систему оценок ТСЗИ – с другой стороны.

Для корректного определения технического состояния ТСЗИ необходимая система оценок, которая удовлетворяет следующим требованиям [5]:

1) система оценок технического состояния должно содержать приоритеты (веса) соответствующих выходных ветвей СПСС, выражающихся в виде функций принадлежности состояний выходной ветви множеству технических состояний ТСЗИ;

2) глубина рассмотрений (детализации) технических состояний ТСЗИ определяется задаваемой достоверностью φ.

С учетом этих требований модель реализуемая на основе выражений (1).....(8), представляет собой модель, построенную на ассоциативных принципах. В зависимости от требуемой достоверности моделирования глубина поиска в БД и подключения узлов СП может измениться в широких приделах, так как данные в БД упорядочены в виде множества пересекающихся деревьев. Пересечения деревьев следует понимать как печатное отношение. Узел пересечения представляет собой нечеткие множества., которым придана мера в виде функции принадлежности узла дерева узлу ассоциации. В зависимости от переходных требований ассоциации могут расширятся, расподелится или образовывать с другими ассоциациями новую, более широкую. Сведенные в БД маршруты организуют ассоциативный доступ к характерным состояниям ТСЗИ, одновременно дополняя содержащуюся в БД информацию новой необходимой и при этом удаляя старую ненужную.

Выводы

Предложенный метод позволяет прогнозировать техническое состояние ТСЗИ на основании системы оценок с большой точностью, что позволяет обеспечивать требуемый уровень защищенности объекта.

Литература

1. Питерсон Дж. – Теория сетей Петри и моделирующие системы / Питерсон Дж. – М.: Мир, 1984. – 264 с.

2. Котов В.Е. – Сети Петри / Котов В.Е. – М.: Наука, 1984. – 160 с.

3. Хорошко В.А. – Применения сетей Петри для моделирования параллельных процессов / Хорошко В.А., Моржов С.В.// Проблемы управления и информатики. - №2, 2004. – с. 86-94.

4. Кобозева А.А, - Анализ информационной безопасности / Кобозева А.А., Хорошко В.А. – К:. Изд. ГУИКТ, 2009. – 215 с.

5. Хорошко В.А. Исследование процессов и структур систем защиты на основе аппарата Петри / Хорошко В.А., Чирков Д.В. // Системи обробки інформації. –Вип.7(88), 2010. – 236 с.

В работе рассматривается теория прогнозирования состояния технической системы защиты информации на основании сетей Петри.

Ключевые слова: техническая система защиты, прогнозирование состояния системы, сети Петри.

В роботі розглядається теорія прогнозування стану технічної системи захисту інформації на основі мереж Петрі.

The theory of prediction for technical system state on the basis of Petri nets is described in the article.

Рецензент:д.т.н., проф.Шелест М.Є.
Надійшла 10.09.2010

УДК 629.735.06:004.681

Пискун И.В.

МОДЕЛЬ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМ СОСТОЯНИЕМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Вступление

Модель управления техническим состоянием (ТС) систем защиты (СЗ) должна учитывать [1,2], что СЗ являются подсистемами сложной системой защиты информации (СЗИ) от утечки по одному из каналов несанкционированного получения информации, которые, в свою очередь, являются элементами комплексной системой технической защиты информации (КС ТЗИ), и что сама система управления ТС СЗ должна строиться, исходя из соблюдения принципа жизненного цикла СЗИ.

Относительно КС ТЗИ система управления ТС СЗ должна рассматриваться как система управления эффективностью и таким образом должна быть направлена на выполнения этой задачи путем выбора оптимальных решений, обеспечивающих минимизацию затрат на эксплуатацию СЗИ и обеспечения требуемого уровня защищенности объекта.

Основная часть

Применительно к ТЗИ безопасность информации характеризуется ее уровнем защиты. Таким образом, система управления состоянием СЗ должна быть направлена на поддержание требуемого уровня защищенности объекта СЗ.

Так как любая СЗ является элементом СЗИ, то система управления их состоянием должна разрабатываться от объекта – СЗИ, при этом в качестве критериев оценки оптимальности систем управления должны выбираться такие показатели, которые органически вытекают из показателей, выбранных для системы управления годностью СЗИ.

Следовательно, система управления ТС СЗ должна быть направлена на предотвращение функциональных отказов и построена таким образом, чтобы затраты на ее обслуживание и ремонт в процессе эксплуатации были минимальными.

Методологическая взаимосвязь указанных принципов организации системы управления ТС СЗ приведена в табл. 1 – 4.

Таблица 1. Методологическая взаимосвязь организации системы управления ТС СЗ в составе КСТЗИ

Объект	Характеристика	Система управления	Оценка
КСТЗИ	Эффективность эксплуатации СЗИ	Эффективностью	$С_э$, $Р_п$
СЗИ	Обеспечение требуемой защищенности	Требуемой защиты	$К_э$, $К_{тз}$
СЗ	Функциональное состояние	Технологическим состоянием	$К_{эф}$, $К_{фс}$