УДК 683.34

К ВОПРОСУ О ПРИМЕНЕНИИ АППАРАТА СЕТЕЙ ПЕТРИ-МАРКОВА ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК ДИНАМИКИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Ю.К. Язов, А. П. Панфилов

Приводятся аналитические соотношения для расчета вероятности срабатывания логических переходов при описании процесса реализации угроз безопасности информации в компьютерных сетях с использованием аппарата сетей Петри-Маркова

В [1] было отмечено, что наиболее полно учет основных факторов, влияющих на возможности реализации угроз безопасности информации в компьютерных системах, сегодня можно провести, моделируя процессы их реализации с использованием перспективного аппарата сетей Петри-Маркова, в основе которого лежат теории сетей Петри и полумарковских процессов [2]. Однако в этой работе были рассмотрены только два логических перехода типа "И" и "ИЛИ", в то время как на практике могут иметь место и другие логические условия. В данной статье предлагаются соотношения для расчета вероятностно-временных характеристик "срабатывания" логических переходов, которые могут встречаться при моделировании процессов реализации угроз безопасности информации в компьютерных сетях.

Динамика реализации угроз в сети Петри-Маркова описывается множеством $\mathrm{M} = \{P, Q(t), \mathrm{Y}\}$, где P – вектор вероятностей, описывающих возможность появления состояния процесса в начальный момент времени, $Q(t)$ – полумарковская матрица, характеризующая временные и стохастические параметры модели, Y – матрица логических условий, элементы которой равны:

$$\upsilon_{i(a),j(z)} = \begin{cases} L[s_{1(a),j(z)},\ldots,s_{i(a),j(z)},\ldots s_{K(a),j(z)}], & \text{если } a_{i(a)} \in O_A(z_{j(z)}); \\ 0, & \text{если } a_{i(a)} \notin O_A(z_{j(z)}), \end{cases}$$

приведенных в табл. 1.

где $O_A(Z)$ – входная функция переходов, отображающая множество позиций A в множество переходов Z;

$O_Z(A)$ – входная функции позиций, отображающая множество позиций Z в множество переходов A.

Пусть на траектории h имеется переход с логическим условием, и на этом переходе "встречаются" несколько траекторий. Если общий номер (по нумерации СПМ) такого перехода обозначить как $\alpha(z)$, а текущий номер этого перехода как c_h, то указанная вероятность для различных логических условий рассчитывается из соотношений,

Расчет по указанным формулам при произвольных плотностях распределения времени перемещения в переходы сети Петри-Маркова оказывается крайне сложным, поэтому для практики целесообразно применять пуассоновское приближение. При этом плотности вероятности срабатывания перехода с логическим условием, определяются из соотношений, приведенных в табл. 2.

По найденной плотности распределения $f_L(h,t)$ рассчитывается математическое ожидание времени до срабатывания логического перехода: $\bar{\tau}_L = \int_0^\infty t \cdot f_L(h,t) \cdot dt$.

При этом ориентировочно может быть оценена вероятность срабатывания перехода

по простой формуле:

$$\Phi_{ij}(h,t) \approx 1-\exp(-t/\overline{\tau}_L).$$

В частности, когда в логическом переходе встречаются не более четырех траекторий, что наиболее часто имеет место в практике моделирования, соотношения для расчета математического ожидания времени срабатывания логического перехода приведены в табл. 3.

Таблица 1

Соотношение для расчета вероятности срабатывания перехода с различными логическими условиями

Логическое условие	Соотношение для расчета вероятности срабатывания логического перехода	Обозначения
"И"	$\Phi_{\alpha(z)}(h,t)=\prod_{h\in H_\alpha}\Phi_{i+c_h,r+c_h}(h,t)$	$\Phi_{\alpha(z)}(h,t)$ - вероятность срабатывания логического перехода с номером $\alpha(z)$; $\Phi_{i+c_h,r+c_h}(h,t)$ - вероятность перемещения процесса из состояния с номером $i+c_h$ (здесь c_h - количество промежуточных переходов) в переход с номером $r+c_h$; $H_\alpha, \hat{H}_\alpha, \overline{H}_\alpha$ - множества траекторий, сходящихся в переходе с номером $\alpha(z)$ и обеспечивающих условие "И", "ИЛИ", "НЕ" соответственно
"ИЛИ"	$\Phi_{\alpha(z)}(h,t)=1-\prod_{h\in\hat{H}\alpha}[1-\Phi_{i+c_h,r+c_h}(h,t)]$	
"И" – "НЕ"	$\Phi_{\alpha(z)}(h,t)=\prod_{h\in H_\alpha}\Phi_{i+c_h,r+c_h}(h,t)\prod_{h\in\overline{H}_\alpha}[1-\Phi_{i+c_h,r+c_h}(h,t)]$	
"ИЛИ" – "НЕ"	$\Phi_{\alpha(z)}(h,t)=(1-\prod_{h\in\hat{H}_\alpha}[1-\Phi_{i+c_h,r+c_h}(h,t)])\prod_{h\in\overline{H}_\alpha}[1-\Phi_{i+c_h,r+c_h}(h,t)]$	
"И" – "ИЛИ"	$\Phi_{\alpha(z)}(h,t)=\prod_{h\in H_\alpha}\Phi_{i+c_h,r+c_h}(h,t)\cdot(1-\prod_{h\in\hat{H}\alpha}[1-\Phi_{i+c_h,r+c_h}(h,t)])$	

Таблица 2

Соотношение для определения плотности вероятности срабатывания перехода с различными логическими условиями

Логическое условие	Соотношения для расчета вероятности срабатывания логического перехода	Обозначения
"И"	$f_\cap(h,t)=\sum_{i\in I_\alpha}f_i(h,t)\cdot\frac{\prod_{j\in I_\alpha}F_j(h,t)}{F_i(h,t)}$	f, F - плотность вероятности и интегральная функция распределения времени срабатывания перехода; I_α - множество всех дуг, входящих в переход α; $\overline{I}_\alpha$ - множество дуг, входящих в переход α и соответствующих условию "НЕ"; $I_{\alpha\cap}$ - множество дуг, входящих в
"ИЛИ"	$f_\cup(h,t)=\sum_{i\in I_\alpha}f_i(h,t)\cdot\frac{\prod_{j\in I_\alpha}[1-F_j(h,t)]}{1-F_i(h,t)}$	
"И" – "НЕ"	$f_{\overline{\cap}}(h,t)=\sum_{i\in I_{\alpha\cap}}f_i(h,t)\frac{\prod_{j\in I_\alpha}F_j(h,t)}{F_i(h,t)}-\prod_{i\in I\alpha\cap}F_i(h,t)\sum_{k\in I_\alpha}f_k(h,t)\frac{\prod_{m\in I_\alpha}[1-F_m(h,t)]}{1-F_k(h,t)}$	
"ИЛИ" – "НЕ"	$f_{\overline{\cup}}(h,t)=\sum_{i\in I_{\alpha\cup}}f_i(h,t)\frac{\prod_{i\in I_{\alpha\cup}}1-F_j(h,t)}{1-F_i(h,t)}\prod_{m\in\overline{I}_\alpha}[1-F_m(h,t)]-\{1-\prod_{i\in I_{\alpha\cup}}[1-F_i(h,t)]\}\sum_{m\in\overline{I}_\alpha}f_m(h,t)\frac{\prod_{m\in\overline{I}_\alpha}[1-F_k(h,t)]}{1-F_m(h,t)}$	

"И" – "ИЛИ"	$f_{\cap\cup}(h,t)=\sum_{i\in I_{\alpha\cap}} f_i(h,t)\cdot\frac{\prod_{j\in I_\alpha}F_j(h,t)}{F_i(h,t)}\{1-\prod_{m\in I_{\alpha\cup}}[1-F_m(h,t)]\}+\prod_{j\in I_\alpha}F_j(h,t)\sum_{m\in I_{\alpha\cup}} f_m(h,t)\frac{\prod_{k\in I_{\alpha\cup}}[1-F_k(h,t)]}{1-F_m(h,t)}$	переход α и соответствующих условию "И"; $I_{\alpha\cup}$ - множество дуг, входящих в переход α и соответствующих условию "ИЛИ"

Таблица 3

Соотношение для определения математического ожидания времени срабатывания перехода с различными логическими условиями

Логическое условие	Соотношение для расчета плотности вероятности времени срабатывания перехода	Соотношение для расчета математического ожидания времени срабатывания перехода	Обозначения
"И" (для двух входящих дуг)	$f_L = f_1F_2 + f_2F$	$\bar{\tau}_L = \frac{\bar{\tau}_1^2 + \bar{\tau}_1\cdot\bar{\tau}_2 + \bar{\tau}_2^2}{\bar{\tau}_1 + \bar{\tau}_2}$	
"ИЛИ"(для двух входящих дуг)	$f_L = f_1(1-F_2)+f_2(1-F_1)$	$\bar{\tau}_L = \frac{\bar{\tau}_1\cdot\bar{\tau}_2}{\bar{\tau}_1+\bar{\tau}_2}$	
"И" – "НЕ" (для трех входящих дуг)	$f_L = f_1F_2(1-F_3)+f_2F_1(1-F_3)-$ $-f_3F_1F_2$	$\bar{\tau}_L = \bar{\tau}_{13}+\bar{\tau}_{23}-\bar{\tau}_3-\bar{\tau}_{123}$,	$\bar{\tau}_{ij} = \frac{\bar{\tau}_i\bar{\tau}_j}{\bar{\tau}_i+\bar{\tau}_j}$, $\bar{\tau}_{ijk} = \frac{\bar{\tau}_i\bar{\tau}_j\bar{\tau}_k}{\bar{\tau}_i\bar{\tau}_j+\bar{\tau}_i\bar{\tau}_k+\bar{\tau}_j\bar{\tau}_k}$
"ИЛИ" – "НЕ" (для трех входящих дуг)	$f_L = f_1(1-F_2)F_3+f_2(1-F_1)F_3+$ $+f_3[1-(1-F_1)(1-F_2)]$	$\bar{\tau}_L = \bar{\tau}_{12}+\bar{\tau}_3-\bar{\tau}_{123}$	
"И" – "ИЛИ" (для четырех входящих дуг)	$f_L = f_1F_2[1-(1-F_3)(1-F_4)]+$ $+f_2F_1[1-(1-F_3)(1-F_4)]+$ $+f_3F_1F_2(1-F_4)+f_4F_1F_2(1-F_3)$	$\bar{\tau}_L = \bar{\tau}_1+\bar{\tau}_2-\bar{\tau}_{12}+\bar{\tau}_{34}-\bar{\tau}_{134}-\bar{\tau}_{234}+$ $+\bar{\tau}_{1234}$	$\bar{\tau}_{ijkm} = \frac{1}{\frac{1}{\bar{\tau}_i}+\frac{1}{\bar{\tau}_j}+\frac{1}{\bar{\tau}_k}+\frac{1}{\bar{\tau}_m}}$

Литература

1. Язов Ю.К. Моделирование динамики реализации угроз несанкционированного доступа к информации в компьютерных системах на основе аппарата сетей Петри-Маркова/ Ю.К. Язов, А.П. Панфилов//Журнал "Информация и безопасность". Воронеж: Воронеж. гос. ун-т. 2006. Вып.1. с. 117 – 123

2. Ю.И. Сабо. Применение сетей Петри с марковскими свойствами для анализа отказоустойчивости систем с резервированием. Изв. вузов. Приборостроение 2004, т. 47, №12, с. 18 – 23.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю
г. Воронеж

State science research experimental institute of technical information protection problems of technical and export control Federal service
Voronezh

TO THE QUESTION ON APPLICATION OF PETRI-MARKOV'S NETWORKS DEVICE FOR THE ESTIMATION OF IS LIKELIHOOD-TIME CHARACTERISTICS OF THE INFORMATION SAFETY THREATS REALIZATION DYNAMICS IN COMPUTER SYSTEMS

J.K. Jazov, A.P. Panfilov

Analytical parities for calculation of logic transitions operation probability are resulted at the description of the information safety threats realization process in computer networks with use of Petri- Markov's networks device