А.А. Бурушкин, А.А. Панфилов, Ю.К. Язов
Россия, г. Воронеж, Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю

ИСПОЛЬЗОВАНИЕ АППАРАТА СЕТЕЙ ПЕТРИ–МАРКОВА ДЛЯ ОЦЕНКИ ХАРАКТЕРИСТИК ДИНАМИКИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Количественные оценки возможности реализации сетевых атак непосредственно связаны с аналитическим или имитационным моделированием динамики их выполнения. Наиболее приемлемым для практики было бы иметь аналитические модели, однако их разработка до сих пор сдерживалась сложностью моделирования многочисленных параллельных во времени процессов, свойственных таким атакам. Подобные процессы сегодня наиболее полно могут быть описаны с использованием аппарата сетей Петри-Маркова, в основе которого лежат теории сетей Петри и полумарковских процессов [1-3].

Под сетью Петри-Маркова понимается множество $\Psi = \{\text{П}, \text{М}\}$, при этом П-сеть Петри – двудольный граф вида

$$\text{П} = \{A, T, O_A(T), O_T(T)\}, \quad (1)$$

где A – множество позиций сети Петри, моделирующих состояние рассматриваемого процесса;

T – множество переходов сети Петри, моделирующих условия перехода, из состояния в состояние;

$O_A(T)$ – входная функция переходов (выходная функция позиций), отображающая множество A в множество T;

$O_T(A)$ – входная функция позиций (выходная функция переходов), отображающая множество T в множество A.

Особенность сети Петри-Маркова (СПМ) заключается в том, что наряду с использованием полумарковской матрицы $Q(t)$, характеризующей временные и стохастические параметры модели, и вектора вероятностей P, описывающих вероятности появления состояний процесса в начальный момент времени, вводится матрица - логических условий Υ, элементы которой равны:

$$\upsilon_{j(z),i(a)} = \begin{cases} L[s_{1(a),j(z)},..., s_{i(a),j(z)},....s_{K(a),j(z)}], & \text{если} \quad a_{i(a)} \in O_A(z_{j(z)}); \\ 0, & \text{если} \quad a_{i(a)} \notin O_A(z_{j(z)}). \end{cases} \qquad (2)$$

В данном случае функция $L-$ это логическая функция, разрешающая выполнение полушагов из переходов в состояния в соответствии со структурой сети Петри, где полушаг от позиции с номером $i(a)$ к переходу с номером $j(z)$,

$$s_{i(a),j(z)} = (a_{i(a)}, z_{j(z)}),\ 1(a) \le i(a) \le K(a) \qquad (3)$$

определяет условия срабатывания перехода $z_{j(z)}$ в позицию $a_{j(a)} \in O_Z(a_{j(a)})$. Два последовательных полушага образуют шаг. Кроме того, особенность такой сети, отличающая ее от обычной сети Петри, заключается в том, что каждый переход срабатывает только с определенной вероятностью.

Полумарковская матрица представляет собой произведение матрицы вероятностей переходов $\{\pi_{ij}\}$ и матрицы плотностей вероятностей времен пребывания процесса в каждом i-м состоянии $\{f_{ij}(t)\}$, если считать, что сам переход происходит мгновенно, то есть

$$Q(t) = \{\pi_{ij} \cdot f_{ij}(t)\}. \qquad (4)$$

Таким образом, процесс реализации угрозы представляет собой последовательность перемещений, реализуемых в виде полушагов по СПМ, при этом СПМ пребывает в каждом состоянии некоторое случайное время, определенное соответствующей этому состоянию плотностью распределения вероятности для случайного времени пребывания, и затем выполняется полушаг и проверка логических условий переключения сети в следующее состояние. Последовательность состояний СПМ называется траекторией

моделируемого процесса. Аналитическое описание процесса осуществляется, как и для обычных полумарковских процессов, в виде интегро-дифференциальных уравнений по траекториям перемещений из начального состояния в конечное [2, 3].

Пусть $h(tr:1(a)\to j(a))=h(tr_1)$ – номер траектории перемещения из состояния $a_{1(a)}$ (здесь индекс с буквой означает номер состояния) в состояние $a_{j(a)}$, которая содержит последовательность полушагов из состоянии в переход, затем из перехода в состояние и т.д.:

$$s_{1[h(tr)]}, s_{2[h(tr)]},\ldots, s_{i[h(tr)]},\ldots, s_{j[h(tr)]}, \tag{5}$$

где второй индекс соответствует каждый раз или номеру состояния или номеру перехода, входящих в выбранную траекторию $h(tr)$. Количество таких траекторий равно $H(tr)$. Вероятность и плотность распределения времени выполнения соответствующего полушага определяются как $p_{j(a)j(z)}$ и $f_{j(a)j(z)}$. Тогда вероятность и плотность распределения времени перемещения из состояния из состояния $a_{1(a)}$ в состояние $a_{j(a)}$ по траектории $h(tr_{1j})$ определяется из соотношений:

$$p_{h(tr_{1j})}=\prod_{j[h(tr_{1j})]=1}^{J[h(tr_{1j})]} p_{j[h(tr_{1j})]}; \tag{6}$$

$$f_{h(tr_{1j})}=f_{1[h(tr_{1j})]} * f_{2[h(tr_{1j})]} * \ldots * f_{i[h(tr_{1j})]} * \ldots * f_{J[h(tr_{1j})]}, \tag{7}$$

где $J[h(tr_{1j})]$ общее количество позиций и переходов в траектории $h(tr_{1j})$;

* – операция свертки,

а по всем возможным траекториям из соотношений [4]:

$$p_{1(a)j(a)}=\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}; \tag{8}$$

$$f_{1(a)j(a)}=\frac{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}\cdot f_{h(tr_{1j})}}{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} p_{h(tr_{1j})}}. \tag{9}$$

В качестве примера логическая функция для атаки типа "Анализ сетевого трафика", вид сети Петри для которой показан на рис.1, может быть представлена (без учета направленности дуг графа) в следующем виде:

$$v_{1(a)5(a)} = \begin{array}{c|ccccc} & 1(z) & 2(z) & 3(z) & 4(z) & 5(z) \\ \hline 1(a) & 1 & 0 & 0 & 1 & 0 \\ 2(a) & 0 & 1 & 0 & 0 & 0 \\ 3(a) & 1 & 0 & 1 & 0 & 1 \\ 4(a) & 0 & 1 & 1 & 0 & 0 \\ 5(a) & 0 & 0 & (3(a),3(z) \cap (4(a),3(z))) & 0 & 0 \end{array} \quad (10)$$

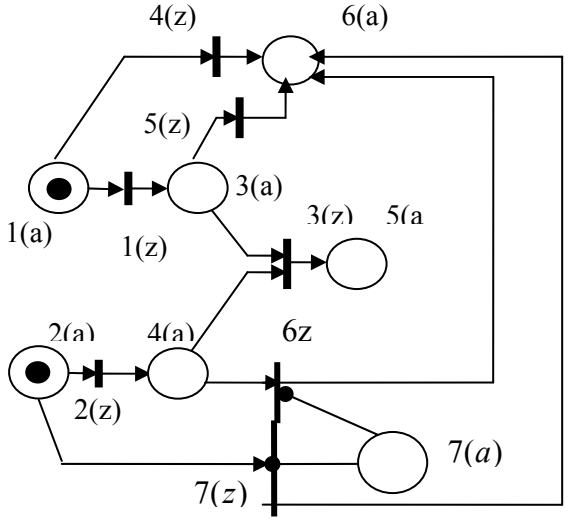

Рис. 1

Сеть Петри, моделирующая атаку типа "Анализ сетевого трафика" при отсутствии мер защиты: 1(a) – атакуемый хост включился в сеть общего пользования; 2(a) – хост злоумышленника включился в сеть общего пользования; 3(a) – атакуемый хост установил TCP-соединение с абонентом и начал обмен данными (наличие трафика хоста с абонентом); 4(a) – злоумышленник получил доступ к серверу (хосту), через который проходит трафик атакуемого хоста; 5(a) – злоумышленник получил имя пользователя и пароль; 6(a) – атака сорвана; 7(a) – условия для перехвата пакетов отсутствуют; 1(z) – установление TCP-соединение между хостом и абонентом; 2(z) – получение злоумышленником доступа к серверу, через который проходит трафик атакуемого хоста; 3(z) – анализ трафика (перехват пакетов атакуемого хоста); 4(z), 5(z), 6(z) и 7(z) – срыв атаки

Здесь полушаг $3(z) \to 5(a)$ может быть выполнен только в случае выполнения полушагов $3(a) \to 3(z)$ и $4(a) \to 3(z)$, знак $\cap$ означает операцию "и", единица означает значение, равное "истина", а ноль – отсутствие полушага.

Поскольку полушаг из перехода в позицию (например, $3(z) \to 5(a)$) срабатывает мгновенно, то динамика срабатывания СПМ определяется только вероятностями срабатывания СПМ (перемещения из состояния в переход) и плотностями распределения времени нахождения процесса в каждом состоянии. Тогда в данном примере достаточно рассмотреть процесс перехода СПМ по двум траекториям из состояний $1(a)$ и $2(a)$ в переход $3(z)$.

Если в СПМ имеются переходы с логическими условиями, то тогда СПМ разбивается на участки, соответствующие а) перемещениям из начального состояния до первого такого перехода, б) между переходами и в) после них до конечного состояния (рис. 2).

Вероятность перемещения процесса из начального состояния $i(a)$ в конечный переход $j(z)$ (что равносильно перемещению в конечное состояние) по траектории h определяется на основе решения системы интегро-дифференциальных уравнений обычного вида:

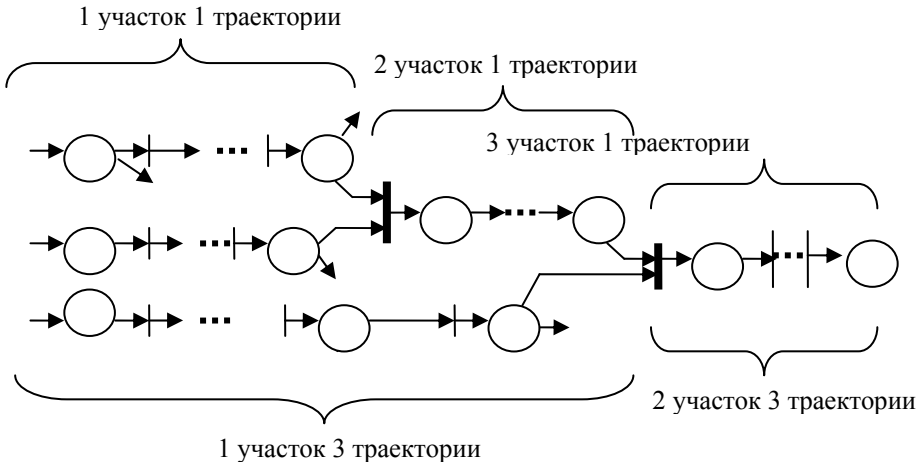

Рис. 2. Пример разбиения траекторий сети Петри–Маркова на участки

$$\Phi_{ij}(h\ ,t) = \pi_{ik} \cdot \int_0^t f_{ik}(h,\tau) \cdot \Phi_{kj}(h,t-\tau) \cdot d\tau\ , \qquad (11)$$

где учтено, что поскольку траектория выбрана, то альтернативные варианты перемещения по дугам, инцидентным позиции $i(a)$, не рассматриваются. Однако, если на траектории h имеется переход с логическим условием и при этом на этом переходе "встречаются" несколько траекторий, то необходимо рассчитать вероятность того, что этот логический переход сработает. Пусть общий номер (по нумерации СПМ) такого перехода обозначен как α, а текущий номер этого перехода в соответствии с нумерацией траектории h соответствует величине c_h, тогда указанная вероятность определяется из соотношения:

$$\Phi_\alpha(t) = \begin{cases} \prod_{h \in H} \Phi_{i+c_h, r+c_h}(h,t) - \textit{для логического условия "И"}; \\ 1 - \prod_{h \in H} [1 - \Phi_{i+c_h, r+c_h}(h\ ,t)] - \textit{для логического условия "ИЛИ"}, \end{cases} \qquad (12)$$

где переходные вероятности $\Phi_{i+c_h, r+c_h}(h,t)$ определяются на основе решения системы уравнений (7) до перехода с логическим условием.

Если больше логических переходов по траектории СПМ не имеется, то вероятность того, что процесс к моменту времени достигнет конечного перехода j, а значит, попадет в последнюю позицию, находится следующим образом:

$$\Phi_{i,j}(t) = \prod_{k=1}^{j} \pi_{suc(\alpha),k(\alpha,j)} \cdot \int_0^t \Phi_\alpha(\tau) \cdot f_{suc(\alpha),j}(t-\tau) \cdot d\tau\ , \qquad (13)$$

где $suc(\alpha)$ – номер позиции по СПМ, которая следует непосредственно за переходом под номером α;

$k(\alpha, j)$ – номер перехода по порядку при перемещении по СПМ от перехода с номером α к переходу с номером j.

Вероятность $\Phi_{i,j}(t)$ является, по сути, вероятностью реализации угрозы. Если по данной траектории имеются еще переходы с логическими условиями, то для них изложенная процедура повторяется. Расчет по

указанным формулам оказывается весьма громоздким, поэтому для практики целесообразно применять пуассоновское приближение для плотностей распределения вероятностей времени перемещения в переходы СПМ. Для обычных переходов такое время рассчитывается путем дифференцирования в точке 0 соответствующей характеристической функции. Расчеты показывают, что ошибка в оценке вероятности реализации угрозы при замене произвольного распределения времени перемещения на пуассоновское приводит к ошибкам, не превышающим десяти процентов.

Рассмотрим, каким образом можно рассчитать среднее время перемещения в переход с логическими условиями. Пусть имеется две траектории, которые сходятся на переходе с логическим условием "И", и плотности распределения времени перемещения к данному переходу по обеим траекториям распределены приближенно по экспоненциальным законам с параметрами $\bar{\tau}_1$ и $\bar{\tau}_2$. Тогда плотность распределения вероятности для времени от начала процесса до срабатывания перехода с логическим условием "И" и "ИЛИ" определяется из соотношений:

$$\begin{aligned} f_{1\cap 2}(t) &= f_1(t)\cdot F_2(t) + f_2(t)\cdot F_1(t); \\ f_{1\cup 2}(t) &= f_1(t)\cdot [1-F_2(t)] + f_2(t)\cdot [1-F_1(t)], \end{aligned} \qquad (14)$$

где $F_1(t), F_2(t)$ – функции распределения времени от начала процесса до срабатывания перехода с логическим условием "И".

При этом математическое ожидание указанного времени рассчитывается обычным образом:

$$\bar{\tau}_{1\cap 2} = \int_0^\infty t\cdot [f_1(t)\cdot F_2(t) + f_2(t)\cdot F_1(t)]\cdot dt, \qquad (15)$$

аналогично для перехода с логическим условием "ИЛИ":

$$\bar{\tau}_{1\cup 2} = \int_0^\infty t\cdot \{f_1(t)\cdot [1-F_2(t)] + f_2(t)\cdot [1-F_1(t)]\}\cdot dt. \qquad (16)$$

В случае экспоненциального приближения формулы имеют следующий вид:

$$\bar{\tau}_{1\cap 2} = \frac{\bar{\tau}_1^{-2} + \bar{\tau}_1\cdot\bar{\tau}_2 + \bar{\tau}_2^{-2}}{\bar{\tau}_1 + \bar{\tau}_2} \text{ и } \bar{\tau}_{1\cup 2} = \frac{\bar{\tau}_1\cdot\bar{\tau}_2}{\bar{\tau}_1 + \bar{\tau}_2}, \qquad (17)$$

где $\bar{\tau}_1, \bar{\tau}_2$ – средние времена перемещения в переход с логическим условием по первой и второй траектории соответственно.

Громоздкость проводимых расчетов несколько затрудняет практическое применение аппарата сетей Петри-Маркова для моделирования рассматриваемых процессов. Однако в экспоненциальном приближении расчет вероятности реализации атаки оказывается достаточно простым. Приведенный подход позволяет перейти к количественным процедурам оценки возможностей реализации угроз в компьютерных сетях с учетом фактора времени и тем самым повысить обоснованность проводимых мероприятий по защите информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Котов В.Е. Сети Петри*. – М.: Наука. Главная редакция физ.-мат. Литературы, 1984.- 160с.

2. *Сильвестров Д.С.* Полумарковские процессы с дискретным множеством состояний (основы расчета функциональных и надежностных характеристик стохастических систем). – М.: Сов. Радио, 1980 – 272 с. (Библиотека инженера по надежности).

3. *Тихонов В.И., Миронов М.А.* Марковские процессы. – М., "Сов. радио", 1977.

4. *Сабо Ю.И.* Применение сетей Петри с марковскими свойствами для анализа отказоустойчивости систем с резервированием // Известия вузов. Приборостроение. Т. 47. №12. 2004. – С 18–23