СПИСОК ЛИТЕРАТУРЫ

1. *Carlet C., Guillot P.* A new representation of Boolean functions // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 13th International Symposium, AAECC-13, Lecture Notes in Computer Science. Vol. 1719. Springer-Verlag, 1999. P. 94–103.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптографии. М.: МЦНМО, 2004.
3. *Логачев О. А., Сальников А. А., Ященко В. В.* Комбинирующие k-аффинные функции // Математика и безопасность информационных технологий. Материалы конференции в МГУ, 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 176–178.

В. Г. Криволапов
Московский инженерно-физический институт (государственный университет)

РЕАЛИЗАЦИЯ МОДЕЛИ СИСТЕМЫ РЕАГИРОВАНИЯ НА DOS-АТАКИ СЕТЯМИ ПЕТРИ

Понятие системы довольно многогранно. Так, С. Кельтон и Дж. Лоу в своей книге «Имитационное моделирование» дают следующее определение: система — это совокупность объектов, например, людей или механизмов, функционирующих и взаимодействующих друг с другом для достижения определенной цели [1. С. 20–23]. Для анализа системы используют проведение опытов с реальной системой либо эксперименты с моделью этой системы. Когда модель достаточно проста, можно вычислить ее соотношения и параметры и по-лучить точное аналитическое решение. Однако некоторые аналитические решения могут быть чрезвычайно сложными и требовать при этом огромных компьютерных ресурсов. В этом случае модель следует изучать с помощью имитационного моделирования, то есть многократного испытания модели с нужными входными данными, чтобы определить их влияние на выходные критерии оценки работы системы. Применительно к модели процесса защиты, исходя из того, что процесс защиты довольно трудно представить аналитически, предпочтительнее имитационные методы как наиболее универсальные, поэтому в качестве подхода к моделированию системы информационной безопасности предлагается использовать аппарат сетей Петри [7].

Сети Петри — это инструмент для математического моделирования и исследования сложных систем. Цель представления системы в виде сети Петри и последующего анализа этой сети состоит в получении важной информации о структуре и динамическом поведении моделируемой системы. На данный момент теория сетей Петри довольно хорошо изучена и используется в различных предметных областях, к примеру [2, 3, 4, 5, 6]. Что особенно важно, так это существование для сетей Петри алгоритмически эффективных способов решения задач достижимости, безопасности и конечности сетей, представляющих основной интерес при моделировании задач информационной безопасности.

В сети Петри условия моделируются позициями, события — переходами. При этом входы перехода являются предусловиями соответствующего события; выходы — постусловиями. Возникновение события моделируется запуском соответствующего перехода. Выполнение условия представляется фишкой в позиции, соответствующей этому условию. Запуск перехода удаляет фишки, представляющие выполнение предусловий, и образует новые фишки, которые представляют выполнение постусловий.

Важная особенность сетей Петри — это их асинхронная природа. В сетях Петри отсутствует измерение времени. В них учитывается лишь важнейшее свойство времени — частичное упорядочение событий.

В данной статье мы будем рассматривать упрощенную ситуацию, моделирующую процесс перенаправления пакетов с заглушенного (атакованного) канала на свободный. Эта модель описывает систему, когда имеет место тип атаки «отказ в обслуживании». На рис. 1 представлена соответствующая сеть Петри.

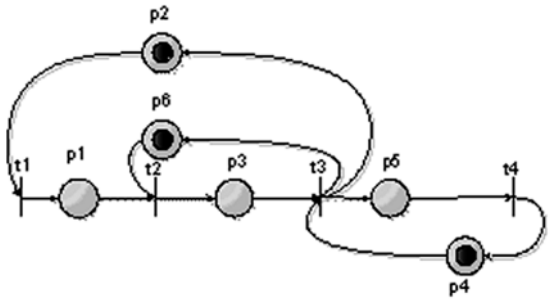

Рис. 1. Сеть Петри, моделирующая процесс перенаправления пакетов с заглушенного (атакованного) канала на свободный

Представим сеть в виде основополагающих понятий: событий и условий.

Условиями для сети являются:

ρ1: число заглушенных каналов, ожидающих поиска;

ρ2: число активных каналов;

ρ3: число каналов, ожидающих перенаправления;

ρ4: число свободных запасных каналов;

ρ5: число заглушенных неактивных каналов;

ρ6: количество возможностей (ресурса) поиска заглушенных каналов.

Событиями для сети являются:

t1: атака обнаружена;

t2: поиск заглушенного канала завершен;

t3: перенаправление пакетов на свободный канал завершено;

t4: канал восстановлен.

Запишем сеть Петри виде пар переходов:

(ρ2,t1),(t1,ρ1),(ρ1,t2),(ρ6,t2),(t2,ρ3),(ρ3,t3),(ρ4,t3),(t3,ρ6),(t3,ρ2),(t3,ρ5),(ρ5,t4),(t4,ρ4).

Определим расширенную входную функцию I и выходную функцию O.

Ниже представлена структура сети Петри, которая состоит из множества позиций (P), множества переходов (T), входной функции ($I : P \to T\infty$) и выходной функции ($O : P \to T\infty$).

$$\boldsymbol{I : P \to T\infty,\ O : P \to T\infty}$$

Таким образом, что

$$\boldsymbol{\#(t_j, I(\rho_j)) = \#(\rho_j, O(t_j)),\ \#(t_j, O(\rho_j)) = \#(\rho_j, I(t_j)).}$$

I (ρ1)={t1}, O (ρ1)={t2},

I (ρ2)={t3}, O (ρ2)={t1},

I (ρ3)={t2}, O (ρ3)={t3},

I (ρ4)={t4}, O (ρ4)={t3},

I (ρ5)={t3}, O (ρ5)={t4},

I (ρ6)={t3}, O (ρ6)={t2}.

C = (P, T, I, O),

P = {ρ1, ρ2, ρ3, ρ4, ρ5, ρ6},

T = {t1, t2, t3, t4},

I (t1)={ρ2 }, O (t1)={ρ1},

I (t2)={ρ1, ρ6}, O (t2)={ρ3},

I (t3)={ρ3, ρ4}, O (t3)={ρ2, ρ5, ρ6},

I (t4)={ρ5}, O (t4)={ρ4}.

Используем матричные уравнения для анализа данной сети Петри. Альтернативным по отношению к определению сети Петри в виде (P, T, I, O) является определение двух матриц D+ и D- , где D = D+ - D- — составная матрица изменений. Каждая матрица имеет m строк (по одной на переход) и n столбцов (по одному на позицию). Определим D- [j, i] = # (ρj, I(tj)), а D+[j, i]= # (ρj, O(tj)). D- определяет входы в переходы, D+ — выходы.

$$D^- = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad D^+ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad D = \begin{bmatrix} +1 & -1 & 0 & 0 & 0 & 0 \\ -1 & +1 & 0 & 0 & 0 & -1 \\ 0 & +1 & -1 & -1 & +1 & +1 \\ 0 & 0 & 0 & +1 & -1 & 0 \end{bmatrix}$$

В начальной маркировке μ=(0,1,0,1,0,1) переход t1 разрешен и приводит к маркировке μ`, где

$$\mu` = (0,1,0,1,0,1) + (1,0,0,0) \cdot \begin{bmatrix} +1 & -1 & 0 & 0 & 0 & 0 \\ -1 & +1 & 0 & 0 & 0 & -1 \\ 0 & +1 & -1 & -1 & +1 & +1 \\ 0 & 0 & 0 & +1 & -1 & 0 \end{bmatrix} = (1,0,0,1,0,1)$$

После анализа данной сети постоим дерево достижимости (рис. 2).

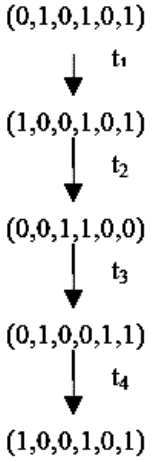

Рис. 2. Дерево достижимости

Данная сеть состоит из 6 мест и 4 переходов. Мы рассматриваем простейшую ситуацию: у нас есть один активный канал (рис. 3). Об этом свидетельствует наличие фишки в P2. Наличие фишки в P6 говорит о том, что у системы есть ресурсы для поиска заглушенных каналов, а наличие фишки в P4 обозначает наличие свободных каналов. При обнаружении атаки срабатывает переход T1. Фишка из P2 попадает в P1, что говорит о появлении каналов, ожидающих перенаправления.

После этого происходит поиск заглушенного канала, и по завершении поиска срабатывает переход T2.

Фишка, оказавшись в P3, свидетельствует о том, что появился канал, ожидающий перенаправления. Наличие фишек в P3 и P4 говорит о том, что есть свободный канал, на который можно перенаправить пакеты с заглушенного канала.

После перенаправления пакетов и срабатывания перехода T3 фишки оказываются в P2, P6, P5.

После восстановления работоспособности канала фишка из P5 через переход T4 оказывается в P4, и система переходит в начальное, восстановленное состояние.

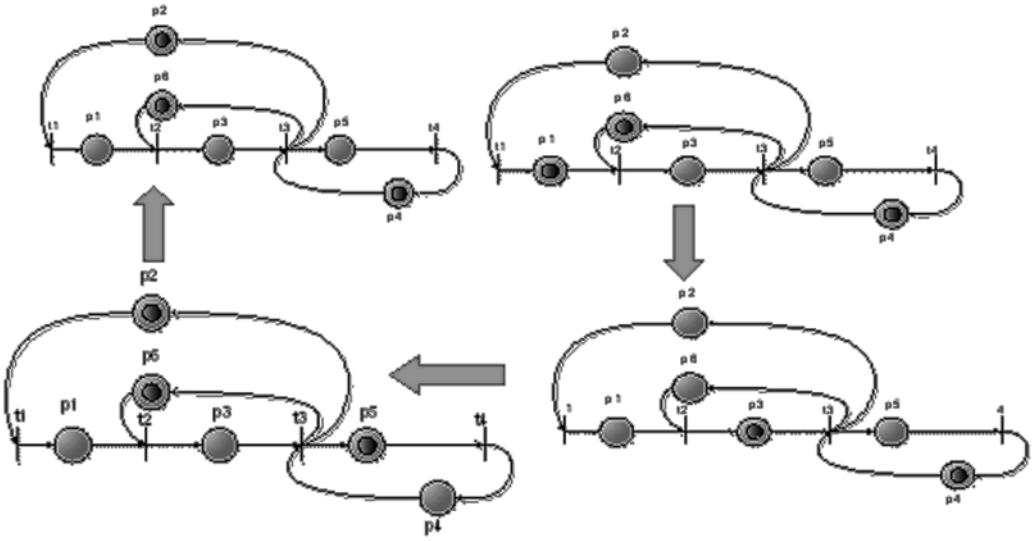

Рис. 3. Движение фишек в сети Петри

Таким образом, этот пример ярко демонстрирует использование в качестве модели сети Петри для наглядного моделирования системы, рассмотренного с точки зрения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. *Кельтон С., Лоу Дж.* Имитационное моделирование. Классика Computer Science. СПб.: Питер, 2004.
2. *Котов В. Е.* Сети Петри. М.: Наука, 1984.
3. *Питерсон Дж.* Теория сетей Петри и моделирование систем. М.: Мир, 1984.
4. *Kristensen Lars M., Christensen S., Jensen K.* The practitioner's guide to Coloured Petri Nets. Springer-Verlag, 1998.
5. *Netjes M., etc.* Analysis of resource-constrained processes with Coloured Petri Nets. Eindhoven University of Technology, Netherlands.
6. *Ломазова И. А.* Моделирование мультиагентных динамических систем вложенными сетями Петри // Программные системы: Теоретические основы и приложения. М.: Наука. Физматлит, 1999.
7. *Питерсон Дж.* Теория сетей Петри и моделирование систем / Пер. с англ. М.: Мир, 1984.