В докладе приводятся результаты разработки и исследования моделей атак этого типа.

Процесс атаки рассматривается как случайный поток транзакций на ИС в течение времени атаки T. для исследования таких процессов обычно используются аналитические и имитационные модели массового обслуживания с блокировкой.

Обсуждаемая в докладе модель атак относится к классу аналитических моделей массового обслуживания с дискретным временем. Состояния модели рассматриваются в равноотстоящие интервалы времени Λt. Модель содержит генератор потока атак, блок моделирования глубины защиты (накопитель атак), блок моделирования защиты. В случае, когда ресурсы защиты исчерпаны, модель переходит в заблокированное состояние (накопитель атак заполнен, блок моделирования защиты занят устранением предыдущей атаки потока, ИС неработоспособна).

Для моделирования атак используется просеянный случайный поток, в котором с вероятностью π в момент модельного времени t атака происходит, и с вероятностью $1-\pi$ не происходит. Состояние потока в следующий момент наблюдения системы $t+\Lambda t$ не зависит от его состояния в момент t (поток без последействия). Глубина защиты моделируется накопителем атак, который может хранить в очереди до n атак. Параметр n будем называть глубиной защиты. Блок моделирования защиты при возникновении атаки в момент t с вероятностью ρ к моменту $t+\Lambda t$ устраняет ее, и вероятностью $1-\rho$ продолжает ее устранение. На интервале времени воздействия потока атак модель рассматривается как стационарная. В момент времени t может произойти одна атака (ординарность потока атак).

Использование моделей с блокировкой позволило определить:

– вероятность блокировки ИС (отказ в обслуживании);

– зависимость времени блокировки от эффективности (глубины) защиты;

– время нахождения ИС в заблокированном и рабочем состоянии в процессе атаки;

– вероятность нахождения ИС в рабочем (незаблокированном) состоянии в процессе атаки.

СЕГМЕНТАЦИЯ СКРЫТНЫХ ОБЪЕКТОВ ИЗОБРАЖЕНИЙ

А.И. МИТЮХИН

В ряде специальных приложениях требуется произвести оценку скорости движения скрытного объекта, направления его движения, пройденного расстояния. Предлагается сегментацию динамических изображений осуществлять на основе корреляционного подхода. Так, скорость можно оценить через промежуточное вычисление диадной корреляционной функции. Пусть имеется последовательность из K изображений $g_{x,\,y,\,t}$ с пространственными переменными (x, y) по оси x и по оси y двумерного евклидового пространства. Рассматривается подход анализа изображений на основе использования циклической группы с операцией диадного сдвига на конечных интервалах. С помощью операцией диадного сдвига формируются мажоритарные последовательности на диадной группе.

Проекции изображений каждого кадра на ось x (ось y) выразим линейной комбинацией мажоритарных последовательностей множества $\{a_i(t)\}$. В результате получается множество последовательностей $g_i=(t)$. Сдвигу изображения за временной интервал между двумя кадрами на $\tau_t=i$ пикселей по оси $x(y)$ будет соответствовать значение отсчета последовательности $g_i=(t)$. Величина сдвига $\tau_x=j$

будет пропорциональна составляющей скорости движения объекта в пикселях на кадр по оси x. Таким образом, для вычисления составляющей скорости по оси x следует найти значение τ_x. Определение сдвига сводится к сравнению последовательности $g(t)_x$ с каждой последовательностью множества $\{a_i\}$ и выбору ближайшей из них по расстоянию Хэмминга. Максимальное значение коэффициента $r_{t\,x}$ определяет величину τ_t. Следовательно, коэффициенты корреляции $\max r_{t\,x}$ формируются в точках с теми номерами t функций $g_{t,\,x}$, координаты которых пропорциональны скорости движения объекта. Аналогичные рассуждения справедливы для получения коэффициентов диадной корреляционной функции для направления y.

В работе представлены результаты анализа движения трудноразличимого (скрытного) объекта на изображениях, искаженных аддитивным шумом. Объем вычислений параметров движения можно существенно сократить, если воспользоваться структурными свойствами мажоритарных последовательностей множества $\{a_i(t)\}$ и их упорядочением определенным способом.

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ АППАРАТНЫЕ РЕАЛИЗАЦИИ ПРОЦЕССОРОВ АЛГОРИТМА ШИФРОВАНИЯ DES НА БАЗЕ ПЛИС С АРХИТЕКТУРОЙ FPGA

М.М. РОДИОНОВ, М.И. ВАШКЕВИЧ, А.А. ПЕТРОВСКИЙ,
А.В. СТАНКЕВИЧ, АЛ.А. ПЕТРОВСКИЙ, М.В. КАЧИНСКИЙ

Предлагаются два варианта аппаратной реализации процессора шифрования алгоритма DES на основе последовательной и конвейерной архитектуры. В последовательном процессоре все циклы алгоритма DES последовательно выполняются на одном вычислительном ядре (далее подход 1). За счет этого возможна экономия аппаратных ресурсов, что позволяет реализовать специализированный процессор со средней производительностью и сравнительно невысокими аппаратными затратами.

В конвейерной архитектуре каждый цикл шифрования реализуется на отдельной вычислительной ступени. Данный вариант позволяет получать выходные результаты в каждом такте работы специализированного процессора. В результате исследований реализаций конвейерного процессора на базе ПЛИС с архитектурой FPGA было установлено, что лучшие показатели производительности достигаются при использовании распределенной памяти кристалла ПЛИС (далее подход 2.1) вместо блочной памяти (далее подход 2.2) для хранения таблиц замен алгоритма DES. Также был реализован конвейерный процессор на основе известного модифицированного представления алгоритма DES (далее подход 2.3), в котором за счет математических преобразований две операции сложения по модулю два с двумя операндами заменяются на одну операцию с четырьмя операндами, что позволяет более эффективно использовать ресурсы ПЛИС.

Для кристалла xc5vlx110 были получены следующие характеристики (логические секции/максимальная тактовая частота, МГц): подход 1 — 151/200; подход 2.1 — 1063/374; подход 2.2 — 997/300, 32 блока памяти; подход 2.3 — 991/377.

Предложенные подходы могут использоваться в приложениях, требующих высокой производительности при шифровании данных.