A.V. Epishkina, S.A. Kiryakina

Simulation Modeling As A Tool For Building High-Speed Encipherer

Keywords: encipherer, model, simulation modelling.

The paper presents a classification of models and the choice of modeling system to simulate a high-speed encipherer. The features of simulation have been examined. The authors justified the choice of simulation environment GPSS World for further research in the area. The possibility of using the simulation tools to construct a high-speed encipherer was proved.

А.В. Епишкина, С.А. Кирякина

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ КАК ИНСТРУМЕНТ ДЛЯ ПОСТРОЕНИЯ ВЫСОКОСКОРОСТНОГО ШИФРАТОРА

Введение

Модель и моделирование – эти сущности помогают ученым и инженерам в различных областях в решении межпредметных проблем, служат для унификации алгоритмов и упрощения процедуры понимания идеи в кругу специалистов. Также модели могут служить для качественных оценок функциональности, возможности применения для конкретных задач и т.д. Построение модели является системной задачей, для решения которой требуются анализ и синтез исходных данных, различных теорий и знаний специалистов. Согласно [1], основная цель моделирования – как можно точнее отображать функциональные способности моделируемой системы.

Модели выполняют важные функции во многих сферах жизни общества. Ежедневно люди сталкиваются с необходимостью представить что-то в удобной для понимания, изучения и анализа форме.

Можно выделить несколько основных направлений использования моделей и моделирования в жизни общества: обучение, разработка теоретических аспектов системы, автоматизация, прогнозирование, управление.

Современное общество повсеместно использует информационные технологии. Массовое применение компьютеров позволяет решать задачу автоматизации обработки информации, поднимая другую проблему – проблему защиты информации.

Алгоритмы защиты информации, а именно шифрования, можно реализовать программным, аппаратным и программно-аппаратным способами. Рассмотрим преимущества аппаратных методов криптографической защиты информации: ведь именно их считают более надежными и лучшими в области защиты информации.

Аппаратный шифратор представляет собой периферийное устройство, выполненное или в виде отдельной платы и подключенное посредством интерфейса ISA или PCI к системной плате персонального компьютера (ПК), или в виде отдельного корпуса. Примером может служить сетевой шифратор, который коммутируется в серверную стойку и является прозрачным для пользователя. Логично предположить, что занимать разъем исключительно шифратором – неыгодное решение в условиях больших рабочих масштабов, именно поэтому часто шифраторы «нагружаются» дополнительными функциями, такими как генерация случайных чисел, контроль целостности файлов операционной системы (ОС), контроль входа на ПК [2]. В итоге получается не только устройство, способное зашифровать данные, а весьма мощный инструмент контроля и разграничения доступа, контроля целостности файлов.

Необходимо заметить, что всегда будут существовать области задач, в частности, связанные с защитой информации, относящейся к государственной тайне, в которых предпочтение однозначно будет отдаваться аппаратным методам шифрования. Высокоскоростные шифраторы используются при обработке больших объемов данных, например, аудио- и видеопотоков. Аппаратная реализация исключает какое-либо стороннее вмешательство в процесс шифрования: весь процесс выполняется «внутри коробки».

Методами моделирования, без проведения дорогостоящего эксперимента, предполагается обосновать методику разделения нагрузки между низкоскоростными шифраторами, а также схему их соединения для построения высокоскоростного.

Системы моделирования и классификация моделей

Рассмотрим различные виды моделей, применительно к различным рассматриваемым задачам:

- статическая модель – в таком типе моделей отсутствует параметр времени, модель представляет собой вид исследуемой системы в каждый момент времени;
- динамическая – отображает систему во времени, присутствует временной параметр;
- дискретная – представляет вид системы в дискретные моменты времени;
- непрерывная – характеризует систему для каждого момента времени из указанного интервала;
- имитационная – применяется для изучения, разработки систем, могут изменяться некоторые (или даже все) параметры;
- детерминированная – для любого входного набора параметров можно сопоставить определенный набор выходных параметров;
- функциональная – представление имеет вид системы функций;
- теоретико-множественная – система представляется в виде множеств и отношений над этими множествами;
- логическая – такая модель представляет собой набор функций логики;
- игровая – такой моделью можно описать какую-либо игру, игровую ситуацию, а также сформировать методы принятия решений в условиях неполной информации;
- алгоритмическая – при описании используется набор алгоритмов или алгоритм; при использовании такого типа моделей следует помнить, что не все модели реализуемы алгоритмически и могут быть использованы в таком представлении;
- структурная – система описывается структурой данных (структурами данных) и отношениями в них;
- иерархическая – модель такого вида имеет древовидное представление;
- сетевая – система представляется в виде некоторой сетевой структуры;
- геометрическая – система представляется с использованием геометрических объектов.

Существуют и другие типы моделей, однако их рассмотрение не является необходимым в рамках настоящей работы.

Проведенный анализ возможностей различных систем моделирования позволяет сделать вывод о том, что для решения поставленной задачи – исследования методики

построения высокоскоростных шифраторов, наиболее подходит система имитационного моделирования.

Имитационное моделирование и его особенности

Рассмотрим подробнее систему имитационного моделирования.

Имитационное моделирование – один из самых мощных инструментов анализа, которыми располагают специалисты, ответственные за разработку и функционирование сложных процессов и систем [3], управление которыми может быть связано с принятием решений в условиях неопределенности.

Имитационное моделирование позволяет работать с реальной или предполагаемой системой в случае, когда проведение эксперимента на реальной системе невозможно или нецелесообразно, либо в процессе замены нескольких составляющих системы. Имитационное моделирование базируется на теории вероятностей и математической статистике, следовательно, оно применимо в системах со стохастическими процессами. Как и любой другой вид экспериментирования, имитационное моделирование не может давать абсолютный результат, поэтому необходимо рассмотреть вопрос об оценке погрешностей и выборе определенных условий, при которых получено решение.

Для рационального использования ресурсов в процессе моделирования следует разрабатывать план, где будут определены не только контрольные точки мероприятия, порядок статистического анализа результатов, но и в целом успешное выполнение задания и конкретных его этапов.

Планирование процесса эксплуатации модели также необходимо; его цель – глубокое изучение поведения моделируемой системы при наименьших затратах, причем точность результатов определяется флуктуацией случайного фактора, а именно, его дисперсией [4]. В зависимости от точности полученного результата следует говорить о степени доверия к полученным материалам, а также о возможных условиях и ограничениях при применении этой модели.

Требуемую степень точности можно задать в различных формах, таких как доля стандартного отклонения, процент от среднего значения, абсолютное значение и т.д. Существующие погрешности вычислений можно уменьшить, например, методом повторения эксперимента, более точным способом формирования случайных выборок.

Для качественного использования результатов имитационного моделирования и проведения эксперимента по моделированию необходимо детально изучить причины возможных успехов и неудач, в частности, модель может содержать несущественные переменные, может вообще не содержать существенных переменных, одна или более существенных переменных могут быть оценены или представлены неточно [4].

Сфера применения систем имитационного моделирования обширна, начиная от науки, техники и технологий и заканчивая системами поддержки принятия решений и управления рисками. Существуют как «заточенные» под определенные направления исследований системы, так и системы, позволяющие решать разнообразные задачи. Важным аспектом в рамках работы является проприетарная или свободная лицензия на программное обеспечение. Также заметим, что существует спектр покрытия средами имитационного моделирования различных ОС, есть возможность выбрать среду не только под решаемую задачу, но и под наличие определенного оборудования. А наличие определенных требований к ОС является скорее недостатком некоторых сред имитационного моделирования.

Выполненный анализ различных сред имитационного моделирования позволяет выбрать систему моделирования GPSS.

Среда имитационного моделирования GPSSWorld

Проведенный анализ различных сред имитационного моделирования позволяет выбрать систему моделирования GPSS, которая наиболее подходит для решения поставленной задачи по своим целевым и алгоритмическим особенностям. Также ее преимуществом является доступность среды разработки и большая популярность, благодаря которой существует достаточное количество материалов и примеров, иллюстрирующих решение практических задач.

Система GPSS World – это мощная среда компьютерного моделирования общего назначения; является комплексным инструментом, применимым в областях как дискретного, так и непрерывного компьютерного моделирования, обладающим высоким уровнем интерактивности и визуального представления информации [5]. Среда GPSSWorld позволяет проводить анализ сложных конструкторских решений, что необходимо для получения решения задачи данной работы. Среда разработана с целью получения достоверных результатов при наименьших временных затратах программиста. Процесс построения моделей обладает хорошей визуализацией, также возможна статистическая обработка данных. GPSSWorld прозрачна для пользователя: возможен просмотр полного процесса разработки, нет «потайных моментов», в связи с чем можно безошибочно определить, что именно предполагалось под тем или иным действием, доработать конструкцию, использовать какие-то фрагменты повторно. Можно контролировать внутреннюю динамику процессов; полученный результат будет справедлив для конкретной разрабатываемой модели – гарантировано, так как все необходимые требования прописаны при создании модели.

Среда GPSS World поддерживает объектно-ориентированное программирование, является интерактивной, именно благодаря этому возможно проводить исследование и управлять процессами моделирования. Возможности визуального представления информации позволяют наблюдать и фиксировать внутренние механизмы функционирования моделей.

В среде GPSSWorld предусмотрены многопоточность и вытесняющая многозадачность, что позволяет достигать высоких скоростей реакции на управляющие воздействия и дает возможность системе одновременно выполнять несколько задач.

С помощью встроенных средств анализа данных можно легко выполнить статистическую обработку данных, в том числе вычислять доверительные интервалы и проводить анализ основных характеристик распределений. Кроме того, есть возможность автоматически создавать и выполнять сложные отсеивающие и оптимизирующие эксперименты.

Разработка в среде GPSSWorld ведется с помощью языка компьютерного моделирования GPSS. GPSS – язык программирования, используемый для имитационного моделирования различных систем, в основном систем массового обслуживания. По этому языку программирования существуют доступные пособия, что также упростит процесс разработки.

Применение средств имитационного моделирования
при проектировании шифраторов

Авторами проведена классификация шифраторов по скорости обработки данных, проанализированы их реализации, основные свойства и характеристики, проведено исследование принципов работы шифратора в целом. Полученные результаты позволяют сделать вывод о том, что наибольшей скоростью обработки данных обладает Senetas CN6 [6]. Высокие скорости работы шифратора обеспечивают ему хорошие перспективы: использование шифратора как в настоящее время (существуют каналы, поддерживающие такие скорости обработки данных), так и в обозримом будущем. Однако Senetas CN6 реализует алгоритм шифрования AES [7], следовательно, актуальной задачей является изучение возможности достичь таких же скоростей для моделируемого высокоскоростного шифратора, реализующего алгоритм ГОСТ 28147-89 [8].

Конечно, необходимо заметить, что активно применяются каналы с меньшей скоростью обработки данных, поэтому шифраторы, имеющие меньшие скорости обработки данных, используются во многих областях. В настоящее время необходимо работать над проектированием оборудования, которое сможет соответствовать растущим скоростям шифрования, ведь даже 100 Гбит/с – не предел в условиях постоянного совершенствования технологий.

Очевидно, для решения задачи моделирования высокоскоростного шифратора крайне нецелесообразно проведение дорогостоящего эксперимента для определения параметров схемы соединения низкоскоростных шифраторов и оценки нагрузки на каждый узел. Проведенный авторами анализ показывает, что для решения поставленной задачи наилучшим образом подходит аппарат имитационного моделирования.

В настоящей работе исследуется возможность применения систем моделирования для повышения скоростных характеристик шифраторов. На рис. 1 приведена обобщенная схема высокоскоростного шифратора и используются следующие обозначения: НШ – низкоскоростной шифратор, ВШ – высокоскоростной шифратор, f_i – разбиение функции шифрования на подзадачи для распределения между НШ, i находится в интервале от *1* до n, где n – количество НШ.

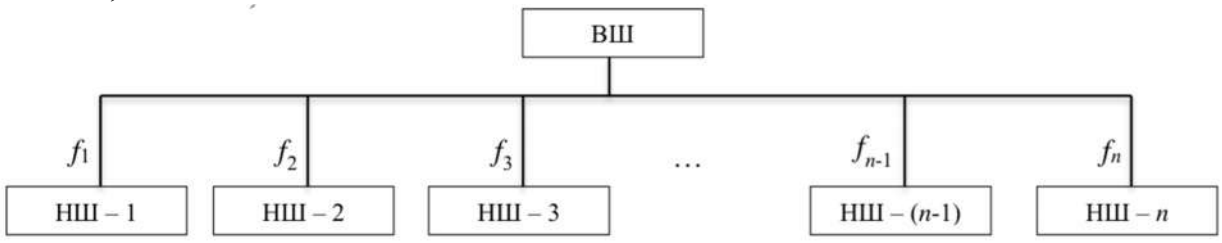

Рис. 1. Схема высокоскоростного шифратора на основе параллельного соединения нескольких низкоскоростных шифраторов

Одна из подзадач, возникающих при разработке ВШ на основе параллельного соединения нескольких низкоскоростных, заключается в разделении функций алгоритма шифрования на каждый из НШ. Также необходимо правильно объединить результаты работы каждого из НШ и вычислить общий ответ, более того, необходимо спроектировать алгоритм коммутации шифраторов, чтобы сохранилась логика шифрующего преобразования.

Уточним описание процесса работы каждого НШ. Его схематическое изображение приведено на рис. 2, где базовые блоки НШ обозначены рамкой, состоящей из одной линии, дополнительные блоки – из двойной.

Рис. 2.Уточненная схема НШ

Необходимо уточнить, что представленная схема является частным случаем устройства шифратора. К примеру, как было сказано ранее, существуют сетевые шифраторы, функционирование которых в настоящей работе не рассматривается.

Перечислим основные блоки шифратора, представленные на рис. 2:

- блок управления – основной модуль шифратора, отвечает за работу всех остальных компонентов, обычно реализуется на базе микроконтроллера, при выборе которого основными параметрами являются быстродействие, достаточное количество внутренних ресурсов для осуществления решения задачи, а также количество внешних портов;
- контроллер системной шины ПК (например, PCI), осуществляет основной обмен данными между шифратором и компьютером;
- флэш-память – представляет собой энергонезависимое запоминающее устройство, используемое для размещения программного обеспечения микроконтроллера, которое выполняется при инициализации устройства;
- память журнала – энергонезависимое запоминающее устройство, реализуемое флэш-микросхемой, причем во избежание возможных коллизий память для программ и память для журнала не должны объединяться;
- шифропроцессор – это специализированная микросхема или микросхема программируемой логики PLD, отвечает за шифрование данных;
- генератор случайных чисел – устройство, выдающее статистически случайный и непредсказуемый сигнал, к примеру, белый шум, может быть выполнено в виде шумового диода, выходной сигнал которого преобразуется по специальным правилам в цифровую форму;
- блок ввода ключевой информации – служит для обеспечения защищенного приема ключей с ключевого носителя, посредством этого блока вводится идентификационная информация о пользователе;
- блок коммутаторов – предоставляет возможность запрещать работу с внешними устройствами: дисководами, CD-ROM и т.д.

Помимо перечисленных выше, существуют и другие блоки, рассмотрение которых не является необходимым на данном этапе работы.

Как было сказано выше, *n* НШ коммутируются параллельно. Осуществить это можно, к примеру, посредством существующих плат расширения, содержащих несколько портов PCI, далее обработать результат работы шифраторов с помощью интерфейсной микросхемы и выдать общий результат на порт PCI ВШ.

Обобщая вышесказанное, получаем, что работу шифратора возможно разделить на несколько подзадач:

- перехват управления на шифратор при включении компьютера – производится один раз, следовательно, можно выполнить эту задачу на одном устройстве;
- ввод ключевой информации – является разовым действием, можно нагрузить этой функцией одно устройство;
- шифрование – данную задачу необходимо разбить между несколькими шифраторами – именно она дает наибольшую нагрузку на аппаратуру и влияет на конечную скорость выполнения процедуры шифрования;
- работа с внешними устройствами – указанная задача не требует больших мощностей для выполнения, можно добавить этот блок лишь к одному из НШ.

Следовательно, возможно некоторые блоки расположить только на одном из НШ, т.е. помимо функций шифрования данных нагрузить устройство еще какой-нибудь подзадачей.

На рис. 2 представлена схема шифратора, в которой отмечены базовые блоки. Таких шифраторов будет $(n-k)$ штук, где k – количество шифраторов, имеющих в своем составе блок, выполняющий дополнительную функцию.

Аналогичным образом будет построен шифратор с дополнительными блоками, представленный на рис. 2.

Заключение

В процессе выполнения работы были получены следующие основные результаты:

- предложена классификация методов моделирования, на основе которой был обоснован выбор имитационного моделирования для дальнейших исследований;
- систематизированы современные системы имитационного моделирования;
- произведен выбор системы GPSS для дальнейшей работы, сформулированы ее преимущества и недостатки;
- обоснована возможность применения систем имитационного моделирования для разработки высокоскоростного шифратора, основанного на параллельном соединении низкоскоростных шифраторов;
- исследован принцип работы шифратора в целом, выделены его основные и дополнительные блоки;
- систематизированы различные методики построения высокоскоростных шифраторов;
- предложен подход к разработке высокоскоростного шифратора.

В рамках дальнейших исследований планируется произвести необходимые расчеты для последующего моделирования высокоскоростного шифратора, определить параметры используемых устройств и сети, а также уточнить предложенную схему моделируемого устройства.

СПИСОК ЛИТЕРАТУРЫ:

1. Введение в анализ, синтез и моделирование систем. Лекция 10. Основы моделирования систем. – http://www.intuit.ru/studies/courses/83/83/info
2. Аппаратные шифраторы. –http://www.osp.ru/pcworld/2002/08/163808/
3. Шеннон Р. Имитационное моделирование систем – искусство и наука. М.: Мир, 1978.
4. Строгалев В.П., Толкачева И.О. Имитационное моделирование. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008.
5. Общецелевая система моделирования GPSS World. http://www.exponenta.ru/soft/Others/gpss/gpss.asp
6. Новый сетевой шифратор компании Senetas позволяет защищать данные на скорости до 100 Гб/с. – http://www.osp.ru/resources/releases/?rid=11006
7. Advanced Encryption Standard.Federal Information Processing Standards Publications, FIPS-197, 2001.
8. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

REFERENCES:

1. Vvedenie v analiz, sintez i modelirovanie system. Lekcija 10. Osnovy modelirovanija sistem. – http://www.intuit.ru/studies/courses/83/83/info
2. Apparatnye shifratory. – http://www.osp.ru/pcworld/2002/08/163808/
3. Shennon R. Imitacionnoe modelirovanie sistem – iskusstvo i nauka. M.: Mir, 1978.
4. Strogalev V.P., Tolkacheva I.O. Imitacionnoe modelirovanie. M.: Izd-vo MGTU im. N.Je. Baumana, 2008.
5. Obshhecelevaja sistema modelirovanija GPSS World. – http://www.exponenta.ru/soft/Others/gpss/gpss.asp
6. Novii setevoi shifrator kompanii Senetas pozvolaet zatshitshat’ dannie na skorosti do 100 Gb/s. – http://www.osp.ru/resources/releases/?rid=11006
7. Advanced Encryption Standard. Federal Information Processing Standards Publications, FIPS-197, 2001.
8. GOST 28147–89. Systemi obrabotki informacii. Zatshita kriptorgaficheskaia. Algoritm kriptograficheskoro preobrazovania.