УДК 004.056:004.272.23:004.75

С.Я. Гильгурт, к.т.н., ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев
А.К. Гиранова, аспирантка ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев

О ПРИМЕНЕНИИ РЕКОНФИГУРИРУЕМЫХ ВЫЧИСЛИТЕЛЕЙ ДЛЯ РЕШЕНИЯ ВОПРОСОВ ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕСЫЛАЕМОЙ В ГРИД-СРЕДЕ

The application of RUCs (FPGA-based Reconfigurable Unificated Coprocessors) to solve the information security tasks in the Grid-computing is investigated.

В настоящее время технология распределенных вычислений грид находит широкое применение при проведении ресурсоемких инженерных и научных расчетов в различных областях, в том числе, в энергетике. Огромная вычислительная мощность географически и административно разделенных ресурсов объединяется для пользователя в виртуальный метакомпьютер, по своим возможностям намного превосходящий любую современную супер-ЭВМ.

Для подключения к грид-системе, как правило, используют персональный компьютер, возможностей которого в большинстве случаев вполне достаточно. Но иногда невысокая производительность локальной ПЭВМ становится «узким местом». Такая ситуация возникает, в частности, когда необходимо предварительно обработать большой объем исходных данных перед их отправкой для расчетов в грид. Примером может служить случай, когда данные, подлежащая обработке конфиденциальны, а штатных средств системы безопасности грид-среды недостаточно для обеспечения требуемого уровня защищенности информации. Как следствие, ее приходится дополнительно шифровать с применением ресурсоемких алгоритмов.

Возникает противоречие: с одной стороны, грид предоставляет неограниченные возможности по производительности вычислений, с другой – ресурсоемкую процедуру необходимо выполнить на рабочем месте пользователя, что приводит либо к существенному увеличению времени решения задачи в целом, либо к замене компьютера пользователя на более мощный.

Разрешить данное противоречие позволяет применение реконфигурируемых унифицированных вычислителей (РУВ) на базе программируемых логических интегральных схем (ПЛИС), совмещающих производительность аппаратных ускорителей с гибкостью и доступностью универсальных компьютеров.

В настоящей работе рассмотрены вопросы применения РУВ для защиты данных, передаваемых в грид-среде.

Анализ последних достижений и публикаций по тематике грид-вычислений свидетельствует, что данная область находится в стадии

интенсивного развития. Большая часть информации содержится в виде кратких сообщений, тезисов докладов и статей. Число монографий крайне мало. Некоторые аспекты практически не освещены в литературе, что обусловлено незавершенностью, недостаточной проработанностью как отдельных компонентов, так и целых уровней существующих на сегодня реализаций грид-структур. В частности, система безопасности грида в настоящее время не сформировалась окончательно и продолжает совершенствоваться.

Целью настоящей статьи является изучение принципов организации передачи данных, а также исследование механизмов обеспечения защиты информации в грид-сети на предмет применения реконфигурируемых вычислителей для повышения безопасности передачи обрабатываемых данных при максимальном использовании имеющихся возможностей.

1. Концепция грид

Термин «грид» был введен в начале 1998 года в книге «Грид. Новая инфраструктура компьютинга» Яна Фостера (Ian Foster) и Карла Кессельмана (Carl Kesselman) [1]. Собственно идея метакомпьютинга возникла намного раньше, однако, с появлением данной книги обозначилось начало новой эры в распределенных вычислениях и возникновение нового поля исследования, называемое грид-компьютинг или метакомпьютинг.

Грид можно определить как инфраструктуру, предназначенную для распределенных вычислений, состоящую из отдельных географически распределенных компьютерных ресурсов: процессоров, оперативной памяти, файлов, баз данных. Основоположники грида ввели следующее определение данного понятия: «грид – это аппаратно-программная инфраструктура, которая обеспечивает надежный, устойчивый, повсеместный и недорогой доступ к высокопроизводительным компьютерным ресурсам» [1]. В дальнейшем определение было уточнено: «грид-компьютинг – это скоординированное разделение ресурсов и решение задач в динамически меняющихся виртуальных организациях со многими участниками» [2].

Инфраструктура грид включает в себя:

- вычислительные ресурсы – отдельные компьютеры, кластеры;
- ресурсы хранения данных – диски и дисковые массивы, системы массового хранения данных;
- скоростные каналы связи;
- специализированное программное обеспечение среднего уровня, так называемое middleware.

Следует заметить, что технологии распределенных вычислений существуют давно. Грид отличается от них, прежде всего тем, что максимально использует отработанные, проверенные временем интернет-решения – стандарты, протоколы, сервисы.

Ключевыми характеристиками грид-среды являются:

- координация использования ресурсов при отсутствии централизованного управления;
- использование стандартных, открытых, универсальных протоколов и интерфейсов;
- обеспечение высококачественного обслуживания.

Кроме того, грид-среда должна обладать гибкостью, масштабируемостью, безопасностью, простотой управления ресурсами.

Существенным моментом, отличающих грид-технологию от прочих подходов к организации распределенных вычислений является скоординированный способ управления ресурсами. По данному признаку, в частности, грид-сеть легко отличить и от вычислительного кластера с его централизованным контролем, и от интернета в целом, характеризующегося полностью децентрализованным управлением.

Вопросы информационной безопасности электронных систем в последнее время приобретают все большее значение. Применительно к грид-среде актуальность данной проблемы возрастает на порядок. В самом деле, грид-сервисы дают пользователю намного больше прав по запуску на выполнение программных модулей, чем традиционные интернет-приложения, то есть, теоретически, предоставляют потенциальному злоумышленнику больше возможностей для злонамеренных действий.

В этой связи защита информации в гриде имеет определенные особенности. Здесь ключевыми моментами являются:

- аутентификация – процесс проверки подлинности идентификационных данных или удостоверений, участника взаимодействия;
- механизмы авторизации определяющие, допускает ли система реализацию затребованной операции;
- конфиденциальность и целостность данных;
- контроль и подсчет объема использованных ресурсов, аудит выполненных операций;
- строгое выполнение обязательств участниками грид-сообщества.

2. Структура грид-системы

Изнутри грид представляет собой многоуровневую структуру взаимодействующих протоколов, сервисов и интерфейсов, определяющих базовые механизмы, посредством которых пользователи устанавливают соединения с грид-системой, совместно используют вычислительные ресурсы для решения различного рода задач. Структура грид-протоколов разделена на уровни (рис. 1), компоненты каждого из которых могут использовать возможности компонентов любого из нижерасположенных уровней [3].

Базовый уровень (Fabric Layer) описывает службы, непосредственно работающие с ресурсами.

Уровень связи (Connectivity Layer) определяет коммуникационные

протоколы и протоколы безопасности. Коммуникационные протоколы обеспечивают обмен данными между компонентами базового уровня. Протоколы безопасности, основываясь на коммуникационных протоколах, предоставляют криптографические механизмы для идентификации, защиты сообщений и проверки подлинности пользователей и ресурсов.

Рис. 1. Соответствие уровней протоколов грид уровням интернет

Ресурсный уровень (Resource Layer) построен над протоколами коммуникации и безопасности уровня связи архитектуры грид. Этот уровень реализует протоколы, обеспечивающие выполнение следующих функций:

- согласование политик безопасности использования ресурса;
- процедура инициации ресурса;
- мониторинг состояния ресурса;
- контроль над ресурсом;
- учет использования ресурса.

Коллективный уровень (Collective Layer) отвечает за глобальную интеграцию различных наборов ресурсов, в отличие от ресурсного уровня, сфокусированного на работе с отдельно взятыми ресурсами.

Прикладной уровень (Application Layer) описывает пользовательские приложения, работающие в среде виртуальной организации. Приложения функционируют, используя сервисы, определенные на нижележащих уровнях.

Остановимся подробнее на уровне связи. Для обеспечения безопасности в грид-среде используется Инфраструктура безопасности грид (Grid Security Infrastructure – GSI). Эта технология обеспечивает безопасную работу в незащищенных сетях общего доступа (интернет), предоставляя такие сервисы, как аутентификация, конфиденциальность передачи информации и единый вход в грид-систему. Под единым входом подразумевается, что

пользователю достаточно один раз пройти процедуру аутентификации, а далее система обеспечивает его автоматическую аутентификацию на всех необходимых ресурсах. Реализация протоколов безопасности выполнена в виде расширения протокола TLS (Transport Layer Security) [4] и основана на криптографических алгоритмах и технологии открытых (публичных) ключей. TLS предоставляет возможность аутентификации и безопасной передачи данных через интернет с использованием шифрования данных. Часто происходит лишь аутентификация сервера, в то время как клиент остается незарегистрированным. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытого ключа (Public Key Infrastructure – PKI), которая позволяет защитить клиент-серверные приложения от перехвата, редактирования и подделки сообщений.

В качестве идентификаторов пользователей и ресурсов в GSI используются цифровые сертификаты X.509. В процедуре выдачи/получения таких сертификатов, а также при работе с ними задействованы три стороны:

1) Сертификационный центр (СЦ) (Certificate Authority – CA) – специальная организация, обладающая полномочиями выдавать (подписывать) цифровые сертификаты. Отношения между СЦ и его клиентами регулируются специальным документом.

2) Подписчик – физическое лицо, либо ресурс, пользующийся сертификационными услугами. СЦ включает в сертификат данные, предоставляемые подписчиком (имя, название организация и т.п.) и заверяет их своей цифровой подписью.

3) Пользователь – физическое лицо либо ресурс, полагающийся на информацию из сертификата при получении его от подписчика. Пользователи могут принимать или отвергать сертификаты, подписанные каким-либо СЦ.

Проанализировав рассмотренные выше сведения с точки зрения задачи защиты пересылаемых в грид-среде данных, выделим следующие моменты.

Как правило, защищенные протоколы, применяемые для передачи данных на удаленный грид-узел, используют симметричное, то есть более слабое по сравнению с асимметричным, шифрование.

В то же время, все узлы и все пользователи грид-сообщества обязаны иметь цифровые сертификаты. Следовательно, подписчик в обязательном порядке имеет пару ключей (открытый и закрытый), которую может использовать как для цифровой подписи, так и для криптозащиты данных с применением соответствующего асимметричного алгоритма. Другими словами, существующие и активно используемые механизмы безопасности грид-системы могут с минимальными доработками быть использованы для решения сформулированной выше задачи защиты передаваемых данных.

Но для ее полного решения недостаточно наличия и доступности открытого ключа. Дело в том, что шифрование больших объемов данных асимметричным алгоритмом может оказаться ресурсоемкой процедурой в смысле вычислительных затрат. И, если ее выполнение не представляет

проблемы на грид-узлах, базирующихся, как правило, на мощных вычислительных кластерах, то на компьютере пользователя процесс шифрования может существенно усложнить взаимодействие с грид-системой.

Для решения этой проблемы в настоящей работе предлагается применять реконфигурируемые вычислители на базе программируемой логики. Прогресс микроэлектроники в последние годы привел к широкому распространению приложений на базе ПЛИС в различных областях цифровой техники, в том числе и в области высокопроизводительных вычислений [5, 6].

В работе [7] исследованы принципы построения, основные преимущества и особенности РУВ. Главным достоинством реконфигурируемых унифицированных вычислителей является способность в значительной степени разрешить противоречие между гибкостью и доступностью универсальных компьютеров, с одной стороны, и высокой производительностью специализированных аппаратных решений – с другой.

Прежде чем перейти непосредственно к вопросам применения РУВ для шифрования данных в грид-компьютинге, рассмотрим основные этапы взаимодействия пользователя с грид-средой в процессе решении задач.

3. Механизмы решения задачи в грид-системе

Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, в котором выполнялась данное исследование, с 2008 года является активным участником проекта Украинский Академический Грид (УАГ). На сегодняшний день УАГ, являясь членом сообщества североевропейских государств NorduGrid, в качестве программного обеспечения промежуточного уровня использует платформу ARC (Advanced Resource Connector). Поэтому при дальнейшем изложении материала для конкретности будем рассматривать эту разновидность грида, что не снижает общности полученных результатов.

Для выполнения необходимых функций среда NorduGrid поддерживает свои собственные грид-сервисы: Grid Manager, ARC Grid FTP server, SSE, User Interface, Broker, LIS, xRSL, Certification Authority и Grid Monitor.

Для запуска задания в грид-сеть пользователь использует команду в виде строки на языке xRSL, которая содержит имя скрипта и запрос ресурсов. Клиентское программное обеспечение выделяет запрос и передает его поисковому брокеру, осуществляющему поиск по базе данных MDS (Monitoring and Directory Service). Возвращаемая информация содержит сетевые адреса тех GRIS (Grid Resource Information Service), которые обладают требуемыми ресурсами. На этом этапе можно запросить цифровой сертификат, содержащий открытый ключ. Далее по полученному адресу пересылается задание, которое требуется выполнить, а также сертификат.

В общем случае задание пользователя может решаться одновременно на нескольких разнесенных в пространстве узлах. При этом выполняемая программа может находиться в другом месте. Обрабатываемые данные также

могут располагаться на произвольном грид-узле (на котором эти данные должны быть размещены до начала вычислений), в общем случае не совпадающем ни с одним из вышеупомянутых мест.

Модифицированный с целью применения РУВ алгоритм взаимодействия пользователя с грид-средой выглядит следующим образом.

Перед запуском задания на исполнение, в ПЛИС реконфигурируемого вычислителя загружается структура аппаратного шифратора, реализующая нужный криптоалгоритм. Высокая гибкость РУВ предоставляет широкие возможности для достижения этой цели.

После запуска задания и определения нужных GRIS запрашивается цифровой сертификат узла, на котором необходимо разместить обрабатываемые данные. Содержащийся в полученном сертификате открытый (публичный) ключ используется для шифрования данных асимметричным алгоритмом, обладающим повышенной криптостойкостью. Благодаря высокой производительности реализованного на базе РУВ криптопроцессора, исходные данные шифруются с высокой скоростью, почти не нагружая центральный процессор компьютера пользователя, и передаются по коммуникационным каналам на целевой грид-узел.

В случае необходимости дальнейшей передачи данных между грид-узлами, задействуется аналогичный механизм. Его осуществимость обусловлена наличием цифрового сертификата у каждого ресурса-участника процесса метакомпьютинга.

Если данные, вычисленные в результате решения задачи в гриде, также требуют дополнительной криптозащиты, они шифруются в месте получения. Необходимая для этого информация о ключах поступает из узла-приемника. Таких узлов в общем случае может быть тоже несколько. Конечным пунктом перемещения результатов счета является пользователь, запустивший задание на исполнение, который также в обязательном порядке имеет цифровой сертификат, содержащий публичный ключ.

Выводы

Необходимость в шифровании больших объемов данных, посылаемых для обработки в грид-систему с рабочего места пользователя, может оказаться «узким местом», сводящим на нет преимущества метакомпьютинга.

Реконфигурируемые унифицированные вычислители позволяют разрешить данное противоречие за счет совмещения высокой производительности специализированных вычислений с гибкостью и доступностью технического решения.

Используемые в грид-системе механизмы аутентификации, основанные на применении цифровых сертификатов, позволяют без существенных изменений принципов функционирования грид-среды реализовать на РУВ асимметричные алгоритмы шифрования, обладающие повышенной крипто-

стойкостью.

1. *I. Foster, C. Kesselman.* The Grid: Blueprint for a New Computing Infrastructure. – Morgan Kaufmann Publishers, 1998.
2. *I. Foster, C. Kesselman, S. Tuecke.* The Anatomy of the Grid: Enabling Scalable Virtual Organizations. – International J. Supercomputer Applications, 15(3), 2001.
3. *Кирьянов А.К., Рябов Ю.Ф.* Введение в технологию Грид: Учебное пособие. – Гатчина: ПИЯФ РАН, 2006. – 39 с.
4. *T. Dierks, C. Allen.* The TLS Protocol Version 1.0. January 1999. RFC-2246.
5. Реконфигурируемые вычислительные системы: Основы и приложения. / А.В. Палагин, В.Н. Опанасенко. – К.: «Просвіта», 2006. – 280 с.
6. *Каляев И.А., Левин И.И., Семерников Е.А., Шмойлов В.И.* Реконфигурируемые мультиконвейерные вычислительные структуры / Под общ.ред. И.А.Каляева. Ростов н.Д: Издательство ЮНЦ РАН, 2008. 320 с.
7. *Гильгурт С.Я.* Обзор современных реконфигурируемых унифицированных вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 49. – Київ: 2008. – С. 17–24.

Поступила 26.03.2009р.

УДК 37:65.012

М.С.Кулик, д.т.н., професор, ректор НАУ
О.К.Юдін, д.т.н., завідувач кафедри НАУ
О.В.Матвійчук-Юдіна, доцент кафедри НАУ

КОНЦЕПЦІЯ РОЗВИТКУ ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТУ

Вступ

Вітчизняна система освіти є важливою соціальною платформою забезпечення рейтингу України, як провідної країни світу з урахуванням її міжнародного престижу - держави, що володіє високим рівнем технологій, культури, науки і освіти. Головні напрями та завдання державної освітньої політики є – створення сучасної системи якісної і фахової освіти на основі фундаментальності, відповідності вітчизняним та світовим вимогам й стандартам, а також потребам особистості, суспільства і держави. Інформаційне суспільство вимагає особливого характеру діяльності системи вищої освіти - інноваційно-творчої і науково-навчальної, що носить професійне спрямування і має альтернативність, багатоваріантність рішень в сучасних умовах інтеграції України до світової спільноти.

Постановка задачі

Однією з необхідних умов і ключових факторів, що визначають успіх

