УДК 519.872, 519.688, 681.63

МОДЕЛИРОВАНИЕ РАБОТЫ GRID-СИСТЕМЫ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

А.Ю. Шелестов,
Институт космических исследований НАНУ и НКАУ
С.И. Лавренюк,
Институт кибернетики и.м. В.М.Глушкова НАНУ
А.Н. Лавренюк
Национальный технический университет Украины «Киевский политехнический институт»

В статье рассматривается задача построения модели доверия по уровню качества сервиса в Grid-системах. Данная модель основана на оценке репутации с вычислением функции полезности с учетом функциональных особенностей составляющих Grid-системы, а также загруженности информационных ресурсов, которые входят в их состав.

На сегодняшний день имеет место широкое распространение Grid-систем, и их всестороннее использование для решения разнообразных научных задач [1, 2, 3]. Сложность задач, которые решаются такими системами, возрастает. Сегодня Grid-системы становятся более доступными возрастающему числу пользователей. При функционировании Grid-системы возникает вопрос об уровне качестве сервиса предоставляемого такой системой для пользователей в целом и ее узлами, компонентах и сервисами в отдельности.

При выполнении задач в Grid-системе для пользователя важно то, чтобы его задача гарантированно выполнилась в положенные сроки и при этом в системе были доступны запрошенные ресурсы и сервисы.

Для того чтобы Grid-задача заведомо выполнилась на узлах, которые имеют не только достаточно для нее вычислительных ресурсов, а также на узлах, которые имеют репутацию надежных сервисов (соотношение успешно завершенных задач к общему количеству задач стремиться к 1), необходимо оценивать состояние узлов. Данные об оценке должны сохраняться на протяжении определенного периода в доступной для Grid-сообщества базе данных. По таким данным можно впоследствии оценивать коэффициенты доверия и функцию полезности [4] для использования в планировщиках заданий Grid-систем [5] с целью выбора надежных узлы с высоким коэффициентом доверия.

На сегодняшний день для Grid-систем особенно актуальны задачи по обеспечению следующих двух свойств: соглашение об уровне качества сервиса (или его доступности) (SLA) или качества обслуживания (QoS) [6, 7].

Grid-систему можно рассматривать как объект управления, функционирующий в условиях неопределенности, к которому можно применять методы идентификации и оценивания [8]. При этом на основе обратной связи можно обеспечить управление этим объектом. В то же время следует отметить, что до сих пор теория управления в области разработки и исследования Grid-систем практически не использовалась, поскольку такие системы являются сложными и иерархическими, что и обуславливает объективную трудность их строгого аналитического описания [9].

Для решения данной задачи авторами предлагается стоить модель, основанную на моделях доверия с разделением на две подзадачи: оценивания уровня доступности и оценивания гарантированного предоставления сервисов на протяжении длительного периода (уровень качества сервиса). Затем на основании этих данных вырабатывать критерии функции полезности для существующих узлов, а также начальные критерии доверия для новых узлов и сервисов, которые еще не имеют истории работы.

Для выработки критериев и параметров модели проведены оценки рисков и выработаны критерии оценки надежности узлов и качества сервиса.

В работе [9] частично описаны методики оценивания рисков связанных с надежностью и доступностью компонентов Grid-систем. Результат оценивания рисков показал, что с точки зрения надежности информации в данной системе и уровня качества сервиса наиболее важным является обеспечение доступности информации и сервисов за определенное длительное время, а также их работоспособность на протяжении этого времени с заданным уровнем сервиса. Т.е., в первую очередь, необходимо обеспечить беспрерывную работу всех Grid-сервисов, причем данные, поступающие в систему извне, должны быть актуальными.

Традиционные методы оценивания уровня доступности информации на основе теории надежности не позволяют проводить оценивания с достаточной эффективностью. Об этом свидетельствуют результаты многочисленных исследований атак на компьютерные системы. Наиболее популярным типом атак на доступность ресурсов и информации являются DoS (denial-of-service) атаки [10, 11] и их распределенный вариант — DDoS (distributed denial-of-service). По

данным [12], в начале 2007 г. сети botnets охватывали около 650 миллионов компьютеров.

Одним из наиболее распространенных подходов к оценке доступности ресурсов и информации является общая теория надежности [13, 14], которая развивается с середины 1950-х годов в результате широкого применения методов и средств автоматики и телемеханики.

Другой подход к оцениванию доступности информации базируется на применении теории нечетких множеств и функций [15]. В рамках этого подхода доступностью считается способность системы ответить на авторизованные запросы в пределах допустимого времени. Однако приемлемое время отклика может зависеть от решаемой прикладной задачи, ее требований и контекста. Основным недостатком этого подхода является то, что никаким образом не учитываются функциональные особенности вычислительной системы и ее компонентов (Grid-сервисов).

Авторы предлагают определить комплексную методику оценивания уровня доступности информации в распределенных Grid-системах. Данная методика позволит учесть функциональные особенности исследуемой системы и проводить подобное оценивание в пределах небольшого промежутка времени.

Для оценивания уровня доступности информации в Grid-системе, а также уровня качества сервиса предоставляемого Grid-системой для построения функции репутации необходимо провести сбор и анализ уже существующих данных о работе Grid-системы, а также провести эксперименты для получения недостающих данных.

На сегодня существует некоторое количество порталов, которые собирают информацию о том, как работают узлы Grid-сети (например, для EGEE http://grid-observatory.org).

Еще одним источником информации о состоянии Grid-системы является подсистема аудита и учета регистрации событий (Audit Logging). Эта система была введена в ПО Globus Toolkit, начиная с версии 4.0.5. Информация, собираемая данной подсистемой, в основном касается подсистемы запуска и выполнения задач (GRAM).

Однако пассивный сбор и анализ системных характеристик некоторого информационного ресурса не может гарантировать того, что система работает в нормальном режиме.

Для оценивания доступности ресурсов и информации в данной вычислительной системе, особенно для оценивания уровня сервиса, необходимо выделить и проанализировать некоторые другие дополнительные характеристики.

Для реализации проверки доступности информации и качества уровня сервиса целесообразно периодически проводить некоторый активный эксперимент по проверке работоспособности каждого Grid-сервиса в системе с помощью дополнительного программного компонента, который имитирует работу легитимного пользователя. Такой активный эксперимент позволяет однозначно определить, способен ли каждый конкретный компонент (Grid-сервис) предоставлять и обрабатывать необходимую информацию в пределах допустимого промежутка времени. При решении поставленной задачи необходимо исследовать всю совокупность Grid-сервисов, работающих в рамках Grid-системы.

Также необходимо выделить некоторые функциональные особенности каждого типа Grid-сервиса, представляющего интерес с точки зрения вклада, который вносит каждая конкретная функция в обработку информации, за которую отвечает этот тип сервисов.

На основе описанных выше функциональных особенностей каждого типа Grid-сервиса становится возможной разработка тест-планов, которые содержат сценарии по проверке работы каждой из необходимых функций. Такие тест-планы необходимо положить в основу активного эксперимента по проверке работы всех Grid-сервисов Grid-системы.

В результате проведения описанного активного эксперимента мы получаем набор результатов выполнения тестов для всех компонентов (Grid-сервисов) системы, значение характеристик загруженности информационных ресурсов, а также качество выполнения тестовой задачи на разных узлах.

При построении модели нам необходимо определить как, имея полный набор результатов выполнения тестов, которые проверяют работу всех Grid-сервисов в данной вычислительной системе, определить оценку доступности информации в ней и качества сервиса.

В докладе будут рассмотрены результаты, полученные при реализации предложенной методики.

Литература.

1. Foster I., Kesselman C. The Grid 2: Blueprint for a New Computing Infrastructure. — Morgan Kaufmann, San Francisco, Calif, 2003. — 748 p.

2. Сергієнко І.В. Про основні напрямки створення інтелектуальних інформаційних технологій // Системні дослідження та інформаційні технології. — 2002. — № 1. — С. 39–64.

3. Грід — нова інформаційно-обчислювальна технологія для науки/ А.Г. Загородній, Г.М. Зінов'єв, Є.С. Мартинов, С.Я. Свистунов, В.М. Шадура // Вісник НАН України. — 2005. — № 6. — С. 17-25.

4. Zheng Yan and Silke Holtmanns. "Trust Modeling and Management: from

Social Trust to Digital Trust", book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global, 2007.

5. E. Elmroth and J. Tordsson. Grid Resource Brokering Algorithms Enabling Advance Reservations and Resource Selection Based on Performance Predictions. Future Generation Computer Systems. The International Journal of Grid Computing: Theory, Methods and Applications. Elsevier, Vol 24, No. 6, pp. 585-593, 2008.

6. Qin Liu , Xiaohua Jia , Chanle Wu, Optimal precomputation for mapping service level agreements in grid computing, Future Generation Computer Systems, v.24 n.8, p.849-859, October, 2008.

7. Qin Liu , Xiaohua Jia , Chanle Wu, Optimal precomputation for mapping service level agreements in grid applications, Proceedings of the 1st international conference on Scalable information systems, p.11-es, May 30-June 01, 2006, Hong Kong

8. Кунцевич В.М. Управление в условиях неопределенности: гарантированные результаты в задачах управления и идентификации. — К.: Наукова думка, 2006. — 206 с.

9. Куссуль Н.Н., Шелестов А.Ю. Grid-системы для задач исследования Земли. Архитектура, модели и технологии. — К.: Наук. думка, 2008. — 452 с.

10. Уланов А., Котенко И. Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Информационно-методический журнал "Защита информации. Инсайд". — 2007. — № 1. — С. 20–30.

11. Handley M., Rescorla E. Internet. Denial-of-Service Considerations. RFC4732. - IETF. Network Working Group, 2006. - 38 p.

12. Markoff J. Attack of the Zombie Computers Is Growing Threat // The New York Times. — 2007. — 1. — P. 10–15.

13. Синопальников В.А., Григорьев С.Н. Надежность и диагностика технологических систем. — М:. "Высшая школа", 2005. — 343 с.

14. Матвеевский В.Р. Надежность технических систем. Учебное пособие. — М.: МГИЭМ, 2002. — 113 с.

15. Tryfonas T. An Alternative Model for Information Availability. — http://www.unob.cz/spi/2007/presentace/2007-May-03/03-Tryfonas-Alternative_Model.ppt.

Получено 28.05.09