УДК 519.872, 519.688, 681.63

МОДЕЛИ ДОВЕРИЯ В GRID-СИСТЕМАХ

Куссуль О.М., Новиков А.Н.
Национальный технический университет Украины «Киевский политехнический институт»

В работе рассматриваются модели управления доверием в Grid-системах. Такие модели строятся на основе оценки репутаций ресурса или пользователя путем построения соответствующих функций полезности.

1. Введение.

С развитием электронной коммерции в Интернет доверию стали уделять повышенное внимание. Клиенты должны доверять продавцу, поскольку передают ему личные данные, а продавец должен доверять клиенту для того, чтобы предоставлять ему свои услуги. В Grid-системах ключевой идеей является совместное использование ресурсов [1], поэтому возникает необходимость во взаимном доверии пользователей и поставщиков ресурсов. В Grid-системах небольшого размера все участники находятся в отношении полного доверия. Например, в Украинском Академическом Grid-сегменте все участники принадлежат к НАН Украины, и на этом основании возникает полное доверие. Но в более масштабных Grid-системах участники зачастую могут быть напрямую не связанны друг с другом, и существует риск того, что кто-то из участников окажется недобросовестным и злоумышленным. Уменьшить эти риски и призваны механизмы доверия. На сегодняшний день уже существует множество концепций доверия и их реализаций [2, 3, 4, 5, 6].

В работе [7] показано, что доверие – это высокоэффективная технология, и ее внедрение позволит обезопасить электронные транзакции. При этом доверие описывается как важный и сложный предмет, связанный с честностью, правдивостью и надежностью доверенной особы или сервиса. Однако единой формулировки понятия доверия так и не достигнуто [8]. Приведем основные два определения доверия.

Когда мы говорим, что доверяем кому-то или что кто-то заслуживает доверия, то мы неявно имеем в виду, что возможность выполнения действия, которое будет полезным или как минимум не нанесет ущерб нам, является достаточно высокой, чтобы вступить с ним в определенные отношения [9].

В работе [10] доверие определяется как предел, до которого одна сторона хочет полагаться в определенной ситуации на что-то или

кого-то с ощущение относительной безопасности, даже если возможны негативные последствия.

2. Актуальность управления доверием в Grid.

В общем случае, целью механизмов безопасности является обеспечение защиты от злоумышленников. При этом различают два подхода [11]: „жесткая безопасность”, которая используется для описания традиционных механизмов, таких как аутентификация и контроль доступа; „мягкая безопасность” для, так называемых механизмов социального контроля, примером которых и является доверие. Доверие определяется в терминах отношений между доверителем (субъектом), который что-то доверяет, и доверенным лицом, которому что-то доверяют. Как отмечается в работе [10], традиционные механизмы безопасности („жесткая безопасность”) не могут предоставить защиту от угроз, вызванных злоумышленными ресурсами, или от злоумышленных действий авторизованных пользователей. В свою очередь, системы доверия могут предоставить защиту от таких угроз, которые являются специфичными для Grid-систем.

Ключевой концепцией Grid-сообщества являются виртуальные организации. Виртуальная организация (ВО) – это временное или постоянное объединение географически распределенных отдельных особ, групп, подразделений организаций или целых организаций, которые делятся ресурсами, возможностями и информацией для достижения общих целей [1]. Организация OGF (Open Grid Forum) инициировала построение нового поколения программного обеспечения среднего уровня путем расширения современных технологий Web-сервисов в рамках Open Grid Services Architecture (OGSA) Рабочая группа OGF OGSA Security Workgroup выделела следующие актуальные задачи обеспечения безопасности в Grid:

– решения, направленные на интеграцию. В этом случае существующие сервисы и интерфейсы необходимо сделать более абстрактными для обеспечения расширяемой архитектуры;

– решения, направленные на интероперабельность с тем, чтобы сервисы, принадлежащие различным организациям с разными механизмами и политиками безопасности, могли взаимодействовать друг с другом;

– решения, направленные на определение, управление и внедрение политик доверия в динамические Grid-организации.

Виртуальные организации динамически формируются, существуют некоторое время и распадаются. Поэтому эффективность

их работы зависит от доверия. В простом случае, когда одна сторона ручается за другую, вопрос доверия решается на основе «личного контакта». Другим примером таких «личных контактов» является вариант, где авторизированная организация выдает сертификаты. Однако такие «личные контакты» не масштабируемы в случае нетривиальных ВО. Для этого необходимы другие технологии, основанные на управление доверием на основании репутаций с тем, чтобы создавать и проводить мониторинг таких ВО.

3. Существующие подходы управления доверием в Grid.

В современных Grid-системах доверие реализуется путем использования механизмов безопасности [12]. Существующие механизмы обеспечивают одноразовую аутентификацию, которая основана на сертификатах, гарантирующих принадлежность узла к доверительной организации. Если какая-то организация желает присоединиться к некоторой ВО, она должна выполнить требования сертификационного центра (СЦ). Этот процесс обычно не обходится без участия человека. Поскольку Grid-системы постоянно развиваются и расширяются, возникает необходимость оценки и управления доверием организаций, участвующих в Grid-вычислениях. На сегодняшний день такие модели доверия строятся на основе оценки репутации сущности и существуют в основном для других прикладных областей.

В общем случае, под репутацией подразумевается мера надежности. Посредством репутации можно построить доверие от одной сущности к другой. Согласно [13], репутация – это предположение о поведении агента на основе имеющейся информации или наблюдений о его поведении в прошлом. В таком случае, для оценки репутации необходимо наличие данных о поведении агента в пошлом. Можно выделить следующие свойства систем обеспечение доверия на основе репутации:

– метрики доверия и репутации: обычно используют значения в диапазоне -1...+1, или 0...1. В последнем случае значение соответствующей метрики может интерпретироваться как вероятность;

– тип обратной связи: информация о репутации может быть позитивной или отрицательной. Некоторые системы основаны на сборе информации любого типа, в то время как другие системы только одного. Например, после выполнения транзакции данные о репутации могут быть представлены в бинарном, дискретном или непрерывном виде;

– надежность: модель доверия должна защитить пользователей от злоумышленной информации, в том числе неверных метрик доверия или репутации, распространяемой внутри системы другими пользователями.

Что касается непосредственно Grid-систем, следующие два свойства являются особо важными:

– обсуждение соглашения об уровне услуг (SLA) или качестве обслуживания (QoS): модели доверия должны учитывать выполнение данных соглашений и обеспечения необходимого качества;

– агрегирование доверия: это особенно важно в концепции ВО. Здесь актуальны две задачи: получение уровня доверия ВО в целом на основе уровня доверия ее участников и оценка уровня доверия некоторой организации, участвующей в определенной ВО.

Модели репутации могут обеспечить в Grid большую надежности путем решения проблемы устойчивости к отказам или путем улучшения распределения ресурсов и планирования. В любом случае, использование моделей на основе репутации дает возможность системе создавать «мягкую» версию доверия. На сегодняшний день существуют несколько подходов к построению моделей, основанных на репутации для Grid-систем.

PathTrust [14] – это система репутаций, предложенная для выбора членов ВО на этапе формирования. Для того чтобы войти в процесс формирования ВО, организация должна зарегистрироваться с инфраструктурой сети предприятия (enterprise network) путем предоставления некоторых сертификатов. Помимо управления пользователями, сеть предприятия предоставляет централизированный сервис репутаций. Когда разрушается виртуальная организация, каждый член оставляет определенные значения обратной связи для сервера репутаций для других членов, с кем он вступал во взаимодействие. Эти значения обратной связи могут быть положительными или отрицательными. Система требует, чтобы после каждого взаимодействия участниками были выставлены оценки. PathTrust является одной из первых попыток применить методы репутации к Grid-системам и подходы к управлению ВО. Однако при этом в этой системе не рассматриваются организационные аспекты. Предложенной модели не хватает динамики, так как обратную связь собирают только в момент разрушения ВО.

В работе [15] предложена модель доверия, основанная на модели репутации для ВО, которая может быть использована для оценки пользователей, ресурсов или поставщиков ресурсов. Эта

модель основана на вычислении функции полезности, которая выражает удовлетворенность одного объекта его взаимодействием с другими объектами, принимая во внимание ключевые качества свойственные оцениваемому объекту. Для оценки репутации ресурсов эта модель доверия требует наличия системы мониторинга для сбора данных о качестве обслуживания. Для определения функции полезности вводится договоренность об уровне обеспечения качества услуг между пользователем и поставщиком для конкретного ресурса в ВО. Фактически, это ожидаемое качество обслуживания на ресурсе. Функция полезности определяется путем сопоставления реальных результатов мониторинга и ожидаемым уровнем обеспечения услуг. Таким образом, репутация каждого ресурса формируется в соответствии со значением функции полезности, которые агрегируются для одного ресурса и всех пользователей, которые с ним взаимодействовали. Аналогично, оценивается репутация пользователя: однако для определения функции полезности вместо договоренности об уровне предоставленных услуг используются заданные правила поведения пользователя на ресурсе, которые сопоставляются с результатами мониторинга реальной деятельности. Такая модель может быть адаптирована для Grid-систем, поскольку не требует прямого ответа от пользователя, а функция полезности является мерой удовлетворенности пользователя. Однако в данной работе не рассматривается вопрос, как устанавливается начальный уровень доверия для новых ресурсов или пользователей.

В работе [16] решается задача оценки уровня доверия между агентами мультиагентной системы, используя данные непосредственных наблюдений и информации о репутации. В отличие от существующих подходов, которые основаны на использование эвристик, предложенный подход HABIT (Hierarchical And Bayesian Inferred Trust Model) использует статистические байесовские методы. В частности, модель HABIT не ограничена к способам описания поведения агентов и в общем случае может быть адаптирована для предсказания как дискретного, так и непрерывного описания. Еще одним преимуществом данной модели является возможность получения оценок доверия, которые вычисляются путем поиска корреляций с поведением групп известных агентов. Это особенно важно в тех случаях, когда у доверителя нет предыдущего опыта или данных о репутации. Такая ситуация возникает для новых агентов, и во многих методах полагается, что уровень доверия для таких агентов минимален, что не всегда верно.

В рассматриваемой модели «доверитель»-«доверенная особа» (truster-trustee) [16] доверие рассматривается с точки зрения обеспечения желаемого уровня качества сервиса. Очевидно, что рациональный агент функционирует так, чтобы достичь максимума ожидаемой полезности, которую можно вычислить следующим образом:

$$EU = \int_{\mathcal{O}^C} U(O_{tr\to te}) p(O_{tr\to te})\, dO_{tr\to te}$$

.

В данном случае, $O_{tr\to te}$ представляет результат (историю) взаимодействия доверителя» и «доверенной особы» (O^C – все возможные варианты взаимодействия в рамках контекста C), $p(\bullet)$ – распределение вероятности, U: $O^C \to \mathrm{R}$ – функция полезности. Для вычисления функции распределения модель HABIT включает две составляющие: *модель репутации*, которая учитывает групповое поведение и репутацию путем описания отношений между поведением и наблюдением между различными агентами; и многими *моделями доверия*, которые строятся для каждой пары «доверитель»-«доверенная особа». Модели доверия описывают уровень доверия между двумя конкретными агентами. Эти модели образуют двухуровневую иерархию и формируют Байесовкую сеть. Верхний уровень такой сети описывает взаимосвязи между разными группами агентов, в то время как нижний – индивидуальное поведение агента. При построении модели доверия необходимо оценить распределение вероятности $p(O_{tr\to te} \mid \theta_{tr\to te})$ наблюдений $O_{tr\to te}$, где $\theta_{tr\to te}$ – вектор параметров распределения. Именно эти параметры распределения и определяют взаимодействие «доверителя» и «доверенной особы» и какую полезность из такого взаимодействия может извлечь «доверитель». Например, если в качестве сервиса используется поисковая система, тогда $O_{tr\to te}$ может представлять время, необходимое для поиска необходимой информации. В случае с Grid-системой, такой характеристикой может быть время нахождения задачи на ресурсах системы. Если предположить, что распределение будет гауссовым, тогда вектор параметров $\theta_{tr\to te}$ будет включать среднее μ и дисперсию σ^2. Очевидно, что сервис с меньшими значениями μ и σ^2 будет обеспечивать большее значение функции полезности. Однако, в общем случае модель параметров может меняться для в зависимости от агента и его целей. Стоит отметить, что при построении модели HABIT необходимо оценивать большое количество параметров распределений, что может повлечь к большим вычислительным затратам. В этом случае авторами предложено использовать метод Монте-Карло. Для проверки адекватности модели

проведены эксперименты по сравнению предложенной модели с существующими.

4. Постановка задачи и метод решения.

В данной работе ставится задача адаптации абстрактных моделей управления доверием на основе репутаций для Grid-систем. Для оценки репутации пользователей, ресурсов и поставщиков сервисов применяется подход, основанный на использовании функций полезности. Для пользователей такая функция полезности учитывает взаимосвязь прав, необходимых пользователю для выполнения заданий, и локальных политик безопасности ресурса. Если права пользователя не нарушают политик, уровень доверия к пользователю увеличивается (или не уменьшается), в противном случае – уменьшается. Для ресурсов и сервисов функция полезности строится, учитывая такие параметры как время пребывания задания в очереди, время выполнения и т.д. Для получения оценок уровня доверия используются данные, собранные системой мониторинга Grid-системы.

Для новых пользователей или ресурсов, для которых нет записей в журналах системы мониторинга, необходимо оценить начальный уровень доверия. Во многих работах таким ресурсам или пользователям предполагается установить нулевой уровень доверия, что не всегда соответствует действительности. В данной работе предлагается следующий поход. Каждый ресурс или пользователь характеризуется некоторой априорной информацией, например, принадлежностью к определенной организации, техническими параметрами и т.д. На основе этих признаков существующие участники Grid-системы разбиваются на разные кластеры. Поведение элементов одного и того же кластера в Grid-системе является сходным. Для кластеризации можно воспользоваться существующими методами, например, нейронными сетями Кохонена. Таким образом, построив систему кластеризации и подав на вход априорную информацию о новом пользователе или ресурсе, он будет отнесен к одному из существующих кластеров. Тогда уровень доверия для нового элемента можно приравнять к значению элемента с минимальным уровнем доверия в этом кластере. Другой подход в оценке функции полезности для нового ресурса состоит в использовании активного эксперимента. В этом случае в системе имеется набор тестовых задач, для которых известны параметры или метрики выполнения на характерных ресурсах. При добавлении нового ресурса на него отправляется на выполнение тестовая задача. Сравнивая реальные и эталонные

значение параметров выполнения задачи, принимается решение о присвоении ресурсу соответствующего значения уровня доверия.

В докладе будут рассмотрены результаты проверки эффективности предложенного подхода на реальных данных, собранных системами мониторинга проекта EGEE и Украинского академического Grid-сегмента.

Литература.

1. Foster I., Kesselman C., Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations // International Journal of Supercomputing Applications, 15(3), 200-222, 2001.
2. Castelfranchi C., Falcone R., Sadighi B., Tain Y.-H. Guest Editorial. Applied Artificial Intelligence, 14(9),Taylor & Frances, 2000.
3. Waidner M.. Ercim News, Special Theme: Information Security. No 49, 2002
4. Nixon P., Terzis S. First International Conference on Trust Management // Lecture Notes in Computer Science, vol. 2692, Springer, 2003.
5. Jensen C.D., Poslad S., Dimitrakos T. Second International Conference on Trust Management // Lecture Notes in Computer Science, vol. 2995, Springer, 2004.
6. Hermann P., Issarny V., Shue S. Third International Conference on Trust Management // Lecture Notes in Computer Science, vol. 3477, Springer, 2005.
7. Grandison T., Sloman M. A Survey of Trust in Internet Applications // IEEE Communications Survey and Tutorials, 3, 2000.
8. McKnight D.H., Chervany N.L. The Meaning of Trust // Technical Report MISRC Working Paper Series 96-04, University of Minnesota. Management Information Systems Research Center, 1996.
9. Gambetta D. Can We Trust Trust? In D. Gambetta (editor). Trust: Making and Breaking Cooperative Relations. Department of Sociology, Univ. of Oxford, 1988.
10. Josang A., Ismail R., Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision // Decision Support Systems, 43(2), pp 618-644, 2007.
11. Rasmusson L., Janssen S. Simulated Social Control for Secure Internet Commerce // In C. Meadows. Proceedings of the 1996 New Security ParadigmsWorkshop. ACM.
12. CoreGrid. D.ia.03 survey material on trust and security. Technical Report D.IA.03, CoreGrid, October2005. http://www.coregrid.net/mambo/images/stories/Integration Activities/TrustandSecurity/d.ia.03.pdf.
13. Abdul-Rahman A., Hailes S. Supporting trust in virtual communities. In HICSS ’00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 6, page 6007, Washington, DC, USA, 2000. IEEE Computer Society.
14. Kerschbaum F., et al. A trust-based reputation service for virtual organization formation. In Proceedings of the 4th International Conference on Trust Management, vol. 3986 of Lecture Notes in Computer Science, pp. 193–205. Springer, 2006.
15. Arenas A.E., Aziz B., Silaghi G.C. Reputation Management in Grid-Based Virtual Organisations // Proc. International Conference on Security and Cryptography (SECRYPT 2008), Porto, Portugal, 26-29 Jul 2008, INSTICC.
16. Luke T.W.T., Jennings N.R., Rogers, Luck M. A Hierarchical Bayesian Trust Model based on Reputation and Group Behaviour // 6th European Workshop on Multi-Agent Systems, 18th-19th December, 2008, Bath, UK.

Получено 29.05.09