УДК 681.3 DOI: 10.18664/ikszt.v0i2.51949

КОРЫТЧИНКО Т.И., аспирант (Украинский государственный университет железнодорожного транспорта)

Применение методов повышения живучести для обеспечения защищенности в распределенных телекоммуникационных системах

В статье представлены методы повышения живучести для обеспечения защищенности в распределенных телекоммуникационных системах. Сформулирована задача реконфигурации распределенных телекоммуникационных систем.

Ключевые слова: *телекоммуникационная система, распределенная систем, технология, сеть, живучесть, защищенность.*

Введение

Распределенные телекоммуникационные системы (РТС) – это системы, которые осуществляют обмен информации на больших расстояниях. Они объединяют целые регионы. Концептуальным преимуществом сетей, которое вытекает из их принадлежности к распределенным системам, перед автономно работающими компьютерами является их способность выполнять параллельные вычисления. За счет этого в системе с несколькими обрабатывающими узлами в принципе можно достичь производительности, превышающей максимально возможную на данный момент производительность любого отдельного, сколь угодно мощного, процессора. Распределенные системы потенциально имеют лучшее соотношение производительность/стоимость, чем централизованные системы.

Еще одно очевидное и важное достоинство распределенных систем - это их более высокая отказоустойчивость. Под отказоустойчивостью следует понимать способность системы выполнять свои функции (может быть, не в полном объеме) при отказах отдельных элементов аппаратуры и неполной доступности данных. Основой повышенной отказоустойчивости распределенных систем является избыточность. Избыточность обрабатывающих узлов (процессоров в многопроцессорных системах или компьютеров в сетях) позволяет при отказе одного узла переназначать приписанные ему задачи на другие узлы. С этой целью в распределенной системе могут быть предусмотрены процедуры динамической или статической реконфигурации. В вычислительных сетях некоторые наборы данных могут дублироваться на внешних запоминающих устройствах нескольких компьютеров сети, так что при отказе одного из них данные остаются доступными [1].

Использование территориально распределенных вычислительных систем больше соответствует распределенному характеру прикладных задач в некоторых предметных областях, таких как автоматизация технологических процессов. В этом случае имеются рассредоточенные по некоторой территории отдельные потребители информации - сотрудники, организации или технологические установки. Эти потребители автономно решают свои задачи, поэтому следовало бы предоставлять им собственные вычислительные средства, но в то же время, поскольку решаемые ими задачи логически тесно взаимосвязаны, их вычислительные средства должны быть объединены в общую систему. Оптимальным решением в такой ситуации является использование вычислительной сети [2].

Для пользователя распределенные системы дают еще и такие преимущества, как возможность совместного использования данных и устройств, а также возможность гибкого распределения работ по всей системе. Такое разделение дорогостоящих периферийных устройств - таких как дисковые массивы большой емкости, цветные принтеры, графопостроители, модемы, оптические диски - во многих случаях является основной причиной развертывания сети на предприятии. Пользователь современной вычислительной сети работает за своим компьютером, часто не отдавая себе отчета в том, что он пользуется данными другого мощного компьютера, находящегося за сотни километров от него. Он отправляет электронную почту через модем, подключенный к коммуникационному серверу, общему для нескольких отделов его предприятия. У пользователя создается впечатление, что эти ресурсы подключены непосредственно к его компьютеру или же "почти" подключены, так как для работы с ними нужны незначительные дополнительные действия по сравнению с использованием действительно собственных ресурсов [3].

Интенсивное развитие технических средств телекоммуникационных систем (ТС), которые осуществляют распределенные функции управления, привело к отставанию разработки и производству средств их контроля и диагностирования [4].

В данной статье продолжаются исследования, посвященные вопросам повышения живучести для обеспечения защищенности в распределенных телекоммуникационных системах [1-8], в направлении обеспечения безопасности ТС.

Анализ последних исследований и публикаций, в которых начато решение проблемы диагностирование ТС и выделение нерешенных ранее частей общей проблемы

Часто термины "диагностика" и "тестирование" употребляются как синонимы. Это не совсем верно. Как правило, под диагностикой сети принято понимать измерение характеристик работы сети в процессе ее эксплуатации (без остановки работы пользователей). Диагностикой сети является, в частности, измерение числа ошибок передачи данных, степени загрузки (утилизации) ресурсов сети или времени реакции прикладного ПО, которую администратор сети должен осуществлять ежедневно. Диагностика бывает двух типов: упреждающая (proactive) и реактивная (reactive). Упреждающая диагностика должна проводиться в процессе эксплуатации сети ежедневно. Основная цель упреждающей диагностики — предотвращение сбоев в работе сети. Реактивная диагностика выполняется, когда в сети уже произошел сбой и надо быстро локализовать источник и выявить причину [3, 9].

Научно обоснованное планирование и оптимизация ТС и сетей, которые обеспечивают предоставление запрашиваемых услуг с заданными показателями качества обслуживания, является очень сложной научно-технической и экономической проблемой, без решения которой невозможное создание информационной инфраструктуры, которая отвечает потребностям развитого общества. В развитии бизнеса отдельных телекоммуникационных компаний этот фактор является важнейшим при обосновании действий администрации, направленных на повышение эффективности работы сети и качества обслуживания пользователей.

Решение данной проблемы основывается на решении задач анализа и синтеза телекоммуникационных систем. Анализ – это получение и сравнение реальных характеристик качества функционирования системы с проектными и предоставление объективных оценок, которые позволят установить причины снижения качества обслуживания и выдать рекомендации по устранению этих причин. Синтез – это определение структурных параметров системы при заданных потоках, дисциплине и качестве обслуживания. Комплексное решение приведенных задач позволяет оптимизировать структуру сети на длительную перспективу. При условиях развития телекоммуникаций в соответствии с основными положениями концепции сетей следующего поколения NGN (Next Generation Networks), которые обеспечивают предоставление неограниченного набора услуг с заданными характеристиками качества обслуживания QOS (Quality of Service), отмеченные вопросы становятся еще актуальнее. Выбранная технология распределения информации в NGN определяет степень сложности узлов коммутации, что, безусловно, влияет на качество обслуживания обмена информацией между терминалами пользователей. Кроме того, качество обслуживания потоков информации влияет и на сами характеристики передачи информации (например, задержки пакетов IP-телефонии приводят к снижению качества телефонной связи) [4].

Таким образом, расширение спектра предоставляемых услуг и растущая сложность телекоммуникационных систем и сетей требует решения проблемы разработки адекватных методов анализа и синтеза этих систем с целью получения достоверных оценок их характеристик, реализации задач их оптимизации, относительно избранного критерия качества обслуживания и разработки соответствующих алгоритмов управления ими [9-10]. А решение задачи реконфигурации распределенных телекоммуникационных систем является актуальной научно-технической проблемой.

Изложение основного материала исследования, посвященного повышению живучести ТС для обеспечения защищенности в распределенных телекоммуникационных системах

Технические методы диагностики ТС и сетей можно успешно применять только тогда, когда удается построить формальную модель составных частей системы или сети. Но в процессе диагностики часто придется прибегать к услугам экспертов, которые знают те или иные особенности ТС и сетей, что трудно формализировать. Для сохранения и использования знаний экспертов в процессе диагностики эффективным является применение экспертных систем, которые способны быстро диагностировать любое состояние ТС или сети. Центральным вопросом построения экспертных систем является выбор формы представления знаний – способа формального выражения знаний о предметной отрасли. Форма представления знаний существенно влияет на характеристики и свойства экспертной системы, потому представление знаний является одной из наиболее важных проблем, что характерны для экспертных систем. Наиболее распространенной формой представления знаний эксперта в системах диагностики ТС и сетей являются продукционные

системы, но существующие методы их построения не гарантируют диагностику произвольного состояния исследуемого ими объекта. Следовательно, актуальным является последующее развитие методов диагностики ТС и сетей, направленное на повышение эффективности процесса диагностирования за счет усовершенствования способов представления знаний экспертов в экспертных системах реального времени и их аппаратной реализации [5].

Широкое внедрение распределенных информационных систем (РИС) является характерным сегодня почти для всех отраслей человеческой деятельности, где на них возлагается решение все более важных задач. От качества функционирования РИС существенно зависит качество наработки и принятия решений и эффективность функционирования многих социальных, экономических, военных, политических структур и тому подобное. Современным РИС присущие иерархичность, функциональная распределенность, высокая степень распараллеливания ресурсов (обслуживания, логики, программного и аппаратного обеспечения, телекоммуникаций), и практически полное отсутствие централизованного управления. С точки зрения системного анализа, РИС — это сложные технические системы, которые функционируют в условиях действия случайных факторов, при активном взаимодействии с внешней средой, при наличии негативных влияний разной природы и при высокой стоимости последствий возможных нарушений или ошибок в работе системы [6, 7].

На практике условия функционирования большинства РИС достаточно трудно определить формально, исчерпывающе, они могут нарушаться из-за негативного влияния как человеческих, так и технических факторов, поэтому возможное возникновение непредвиденных проблемных ситуаций, которые нуждаются в адекватной реакции системы. Для прогнозирования, установления, избежания, преодоления таких ситуаций, используются механизмы и средства повышения живучести систем, невзирая на все сложности их реализации.

Живучесть как свойство РИС характеризует ее способность избирать оптимальный режим функционирования за счет собственных внутренних ресурсов, перестройки структуры, изменения функций и поведения отдельных подсистем, в связи с изменением внешних условий и в соответствии с целью ее функционирования [6]. Для обеспечения живучести в РИС предусматривается наличие механизмов:

- мониторинга состояния системы и влияния среды;
- адаптации при незначительном изменении условий для оптимизации функционирования системы соответственно заданным критериям;
- восстановление функционирования после сбоев, отказов, ошибок;
- перераспределения ресурсов системы для выполнения цели ее функционирования в новых условиях.

Задачи, которые решаются с помощью этих механизмов в РИС, очень похожи на те задачи, которые должны решаться для создания защищенной информационной среды при использовании адаптивных систем защиты. Среди механизмов повышения живучести обычно выделяют механизмы реконструкции, реорганизации, реконфигурации, распознавания, противодействия, возобновления, адаптации.

Механизмы распознавания в РИС позволяют, на основе данных мониторинга системы и среды, обнаружить потенциально опасные состояния и вскоре адекватно на них реагировать (фиксировать структурные изменения в системе в результате отказов ее компонентов, повышения риска выхода из строя критических компонентов систем, обнаруживать атаки, успешные вторжения, риски потери или искривления информации и тому подобное).

Механизмы противодействия в РИС направленные в поддержку определенных условий функционирования и минимизацию убытков, которые возможны в связи с возникновением новых условий функционирования и непредвиденных влияний. Эти механизмы базируются на классических методах обеспечения безопасности, надежности и отказоустойчивости информационных систем, включая резервирование критических компонентов, контроль доступа и использование ресурсов системы, отвлечения вирусных атак, и тому подобное.

Механизмы адаптации дают возможность приспосабливаться к внешним изменениям среды функционирования РИС, компенсируя нежелательные влияния и позволяя системе оптимизировать свою работу в соответствии с установленными критериями, и даже изменить цель функционирования, если этого требуют новые условия.

Механизмы возобновления в РИС обеспечивают возобновление функциональности и работоспособности компонентов системы и РИС в целом при нежелательных влияниях, а также после прекращения влияний. Механизмы возобновления должны выполнять идентификацию и локализацию неисправностей, исправления ошибок в программах и данных, установление задержки во времени, перераспределение ресурсов между процессами, замену и отключение неисправных элементов, ремонт, регистрацию наблюдений и выполненных действий, возобновление работы (полное или частичное) или завершение последовательности операций безопасной остановки.

Механизмы реорганизации обеспечивают перераспределение функций компонентов РИС, которые вышли из строя, между работоспособными компонентами системы или, в случае невозможности перераспределения, — переход системы к новой цели функционирования.

Механизмы реконфигурации реализуют автоматическую перестройку структуры сети обмена информацией для достижения наибольшей эффективности выполнения цели функционирования на имеющихся работоспособных ресурсах РИС.

Механизмы реконструкции выполняют редукцию цели функционирования и ресурсов системы к определенным базовым уровням, когда система может выполнять четко очерченное множественное число функций, или обеспечить плавность деградации определенных параметров (безопасная остановка).

Конкретная реализация этих механизмов предусматривает использование как известных технических и технологических решений и средств, так и разработку новых, в соответствии со спецификой задач системы. Внедрение механизмов повышения живучести в распределенные информационные системы нуждается в проведении анализа рисков, учета особенностей и целей функционирования каждой конкретной системы, оценки экономической целесообразности.

Сегодня существенным является использование имеющихся системных средств и возможностей распределенной информационной системы для обеспечения безопасной работы с информационными ресурсами. Для решения этой проблемы, кроме уже упомянутых выше специальных средств и технологий защиты, могут быть использованы присущие РИС механизмы повышения живучести, развитые для решения задач безопасности, например, при создании адаптивных систем защиты, которые ориентированы на активное противостояние угрозам безопасности. Особенностью использования механизмов и средств обеспечения живучести является то, что они позволяют отреагировать на нежелательное влияние, и обеспечить переход системы в безопасное для нее состояние еще к проведению анализа причин события (например, нарушение безопасности). Следовательно, опираясь на механизмы обеспечения живучести, системы защиты информационной среды и информационного ресурса, можно строить на схемах «что, если», а не на классических схемах «защита от» Принятие своевременных и эффективных решений относительно защиты информационных ресурсов РИС возможно при использовании механизмов реконструкции и реорганизации, механизмы противодействия и возобновления позволят сохранить критические информационные ресурсы системы, механизмы адаптации позволят компенсировать нежелательные влияния на информационные ресурсы РИС [8, 10].

Уже сегодня механизмы повышения живучести могут применяться для целеустремленного изменения конфигурации программно-аппаратных средств РИС с целью улучшения защиты системы и ее информационных ресурсов, осложнения реализации атак на систему, отвлечения атак, противодействия возникновению нештатных ситуаций, продолжения или удлинения функционирования системы в нештатных ситуациях, «безопасной остановке», полного или частичного возобновления функционирования системы и тому подобное. Использование системных средств и механизмов повышения живучести возможно после проведения исследований анализа рисков, выявления критических функций и ресурсов системы, разработки политики безопасности, выбора традиционных средств защиты, реализации средств, для противодействия определенным угрозам. Аудит безопасности и мониторинг состояния системы механизмами распознавания и противодействия позволят распознавать и оперативно реагировать на риски безопасности, выполняя, например, такие функции, необходимые для повышения защищенности информационного ресурса в распределенных системах:

— разоблачение несанкционированной деятельности (преднамеренной или случайной) и предотвращение возможных последствий в реальном масштабе времени;

— предотвращение хакерских атак на критические дополнения и системные сервисы;

— выполнение заданной последовательности соответствующих действий при выявлении попыток вторжения в систему (с целью прекращения соединения с нарушителем, изменения конфигурации узлов сети, сообщения администратору, и тому подобное);

— регистрация деятельности пользователей системы и анализ полученных данных с целью отвлечения последующих попыток нарушения политики безопасности по уже известным схемам; — анализ существующей конфигурации системы с целью выявления и устранения чувствительности.

Благодаря применению механизмов реконфигурации могут быть выполнены:

— автоматическая реконфигурация межсетевых экранов, маршрутизаторов, коммутаторов и других средств, для отражения атаки на РИС в реальном масштабе времени;

— создание границы и предотвращение последующего проникновения нарушителя в сеть;

— динамическое формирование надежной конфигурации систем защиты для разных групп пользователей в соответствии с их полномочиями [8].

Выводы

Необходимую пропускную способность сети или ее надежность нельзя оценить без детального анализа ее нынешнего состояния. Посредством различных диагностических средств можно осуществить прогнозирование аварийных ситуаций в ТС и ликвидацию их последствий. Принятие своевременных и эффективных решений относительно защиты информационных ресурсов РИС возможно при использовании механизмов реконструкции и реорганизации, механизмы противодействия и возобновления позволят сохранить критические информационные ресурсы системы, механизмы адаптации позволят компенсировать нежелательные влияния на информационные ресурсы РИС.

Литература

1. Национальный открытый университет [Офиц. сайт]. URL: http://www.intuit.ru/studies/courses/1/1/lecture/20 (дата обращения: 26.01.2015).
2. Поморова О.В. Теоретические основы, методы и средства интеллектуального диагностирования компьютерных систем: автореф. дис. ... канд./д-ра техн. наук. Нац. университет "Львовская политехника", Львов, 2007.
3. Юдицкий С.И. Основы диагностики сети. / С.И. Юдицкий, В.В. Борисенко, О.В. Овчинников // LAN/Журнал сетевых решений. – 1998. – №12. – С. 1–2.
4. Ложковський А.Г. Аналіз і синтез систем розподілу інформації в умовах мультисервісного трафіка: автореф. дис. .канд./д-ра техн. наук. Одес. нац. академія зв'язку ім. О.С. Попова, Одесса, 2010.
5. Хабіс А. А. Зідат. Методи діагностики комп'ютерних систем та мереж з використовуванням експертних систем реального часу : автореф. дис. .канд. техн. наук. Хар. нац. університет радіоелектроніки, Харків, 2007.
6. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – К.: Наук. думка, 1990. – 184 с.
7. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Живучесть и надежность сложных систем. Методическое пособие. — Международный научно-учебный центр ЮНЕСКО/МПИ информационных технологий и систем. – 2001. – 163 с.
8. Кузнєцова М. Г. Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах. Методи інформації в комп'ютерних системах і мережах. – 2006. – № 3. – С.8.
9. Мирошник М.А. Методы защиты цифровой информации в распределенных компьютерных сетях. Інформаційно-керуючі системи на залізничному транспорті. – 2014. – №5. – С. 66-70.
10. Мирошник М.А. Разработка средств защиты информации в распределенных компьютерных системах и сетях. Інформаційно-керуючі системи на залізничному транспорті. – 2015. – №1. – С. 18-25.

Коритчінко Т.І. Застосування методів підвищення живучості для забезпечення захищеності в розподілених телекомунікаційних системах. Наведено методи підвищення живучості для забезпечення захищеності в розподілених телекомунікаційних системах. Сформована задача реконфігурації розподілених телекомунікаційних систем.

Ключові слова: телекомунікаційна система, розподілена система, технологія, мережа, живучість, захищеність.

Korytchinko T.I. The application of methods to increase survivability for ensuring security in the distributed telecommunication systems. The article presents the application of methods to increase survivability for ensuring security in the distributed telecommunication systems. The problem of distributed telecommunication systems reconfiguration has been defined.

Key words: telecommunication system, distributed system, technology, network, survivability, security.

Рецензент Мирошник М.А., д.т.н., профессор кафедры СКС (УкрГУЖТ)

Поступила 20.03.2015г.