УДК 004.738

ПРОКСИ-СЕРВЕРЫ В РАСПРЕДЕЛЕННЫХ ГЕТЕРОГЕННЫХ МУЛЬТИСЕТЕВЫХ СРЕДАХ

Р.Э. Асратян, В.Н. Лебедев

Рассмотрены методы организации информационного взаимодействия в распределенных системах, основанные на применении технологии прокси-серверов. Описаны основные направления применения этой технологии в разработках организационных и экономических систем управления на базе Web-технологии и архитектуры .NET. Приведены примеры применения технологии прокси-серверов для решения таких задач, как контроль и мониторинг запросов к Web-сайтам, организация взаимодействия между удаленными частными сетями и защита SOAP-сообщений в информационных запросах, в частности, дан пример взаимодействия с Системой межведомственного электронного взаимодействия, которая играет важную роль в инфраструктуре Электронного правительства.

Ключевые слова: распределенные системы, Интернет-технологии, прокси-серверы, информационная безопасность.

ВВЕДЕНИЕ

Технология прокси-серверов (ПС) возникла практически одновременно с технологией Web [1, 2] во второй половине 1990-х гг. и может рассматриваться как важное дополнение последней. Совсем не случайно идея взаимодействия через «сервер — посредник» была упомянута в стандарте на протокол HTTP: именно в применении к этому протоколу она оказалась особенно эффективной и востребованной. Практически сразу появились самые различные применения этой технологии: от безопасного подключения частных сетей к Интернету и кэширования сетевых данных до фильтрации информационных запросов и «анонимизации» их источников. В данной работе мы будем рассматривать только ПС, ориентированные на протокол HTTP.

За прошедшие годы «рейтинг» протокола HTTP никогда не падал, но непрерывно возрастал. Изначально спроектированный для поддержки электронной прессы и массовых коммуникаций, он довольно рано нашел применение в организации технологического удаленного взаимодействия в архитектуре «клиент — сервер», а после появления технологии .NET [2, 3] занял доминирующие позиции в разработках распределенных систем.

Все это время технология ПС также оставалась вполне востребованной. Работая на уровне HTTP и будучи совершенно прозрачной для любых «надстроек», она одинаково успешно применялась как для организации обращения к новостным сайтам, так и для вызовов методов удаленных Web и WCF-сервисов.

В последние годы наблюдается новая волна интереса к технологии ПС не только у администраторов, но и у разработчиков распределенных систем. Это обусловлено повышением требований к таким системам, связанных с обеспечением информационной безопасности и работой в сложных гетерогенных, мультисетевых средах (т. е. в средах, характеризующихся не только платформенной неоднородностью, но и сложной сетевой структурой, включающей в себя множество сетей разного размера и административной подчиненности). Разработчики таких систем все чаще сталкиваются с ситуацией, требующей включения дополнительной функциональности в средства удаленного взаимодействия, причем с обязательным соблюдением принципа прозрачности дополнительных средств для клиентской и серверной компонент. В ряде случаев эта функциональность может быть эффективно реализована на уровне специализированного сервера-посредника.

В данной работе сформулирован и решен ряд задач, часто возникающих в практике разработки распределенных информационно-управляющих систем и связанных с проблемой организации сетевого взаимодействия в таких системах. Ключом к предлагаемому решению каждой из них служит технология ПС, оснащенных дополнительной функциональностью.

1. ЗАДАЧА МОНИТОРИНГА ИНФОРМАЦИОННЫХ ЗАПРОСОВ

Рассмотрим довольно часто встречающуюся ситуацию: в распределенной системе, ориентированной на «тонкого клиента», требуется обеспечить контроль и мониторинг обращений из рабочих станций, подключенных к частной сети предприятия, к информационному Web-сайту (порталу), расположенным вне этой сети и вне управления руководством предприятия. Под контролем в данном случае подразумевается разграничение прав доступа сотрудников к информационным ресурсам, размещенным на этих сайтах, а под мониторингом — регистрацию всех обращений в специальной базе данных с группировкой этих обращений по конкретным пользователям и сеансам связи. Наиболее существенно в данном примере то, что никаких средств по ограничению прав доступа и регистрации обращений на упомянутом Web-портале не предусмотрено.

Один из эффективных путей решения этой задачи заключается в организации обращений через специализированный ПС, размещенный на «пограничном» сетевом узле (т. е. узле, подключенном к двум сетям одновременно) и оснащенный дополнительной функциональностью для обработки информационных запросов. В предлагаемом решении функции проверки прав пользователя, открытия сеансов связи и регистрации обращений к ресурсам проводится на уровне ПС. Именно ПС предоставляет экранную форму ввода имени и пароля пользователя, формирует уникальный идентификатор сеанса связи и обеспечивает «привязку» каждого запроса к конкретному пользователю и сеансу связи с помощью механизма временных cookie, действующих только в течение сеанса Web-браузера.

На рис. 1 приведен алгоритм обработки запроса в ПС, обеспечивающей контроль и мониторинг доступа. В алгоритме использованы строковые переменные и функции:

Username — переменная для хранения имени пользователя;

SessionId — переменная для хранения уникального идентификатора сеанса связи;

URL — переменная для хранения URL (Интернет-имени) адресуемого ресурса;

Check (username, URL) — функция проверки права доступа пользователя (username) к ресурсу (URL);

Register (username, sessionid, URL) — функция регистрации обращения пользователя (username) к ресурсу (URL) в рамках сеанса sessionid.

Как видно из рисунка, ПС достаточно активно вмешивается в диалог между Web-браузером и Web-сервером. В самом начале сеанса связи он отправляет в браузер собственную экранную форму, содержащую два текстовых поля ввода для параметров: имени (Login) и пароля (Password) пользователя. После приема заполненной пользователем формы ПС проверяет правильность имени и пароля и открывает сеанс связи: формирует новый идентификатор сеанса и инициирует обращение к стартовой странице портала.

После получения HTTP-ответа от портала ПС добавляет в заголовок ответа два предложения Set-cookie, сообщающих Web-браузеру имя пользователя и идентификатор сеанса связи. С этого момента и до завершения работы Web-браузер будет автоматически добавлять имя пользователя и идентификатор сеанса в заголовок каждого запроса к порталу (предложения Cookie в HTTP-заголовке), обеспечивая возможность группировки запросов по пользователям и сеансам.

Предполагается, что ПС имеет доступ к базе данных пользователей, в которой хранятся их имена и пароли, а также списки имен информационных ресурсов, к которым разрешен доступ каждому пользователю.

Разумеется, описанная организация контроля и мониторинга запросов не предназначена для защиты от технически изощренных форм взлома (например, основанных на sniffing — «прослушивании» сетевого трафика в целях определения чужих имен и паролей).

2. ЗАДАЧА ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ МЕЖДУ УДАЛЕННЫМИ ЧАСТНЫМИ СЕТЯМИ

В последние годы наблюдается все больший рост интереса к методам построения территориально-распределенных систем, ориентированных на работу в сложной мультисетевой среде, включающей в себя множество частных локальных сетей предприятий, соединенных ведомственными и интернациональными глобальными сетями. Главные проблемы, которые приходится решать разработчикам подобных систем, — проблемы межсетевой маршрутизации информационных запросов и защиты данных от несанкционированного доступа.

Именно из соображений защиты владельцы информационных ресурсов обычно «прячут» их в частных локальных сетях, защищенных от внешней атаки. Однако в данной ситуации возникают две проблемы: проблема недоступности ресурсов из-за пределов частной сети и проблема неодно-

значности IP-адресов: в разных частных сетях они могут повторяться.

Первая из этих проблем обычно решается с помощью технологии виртуальных частных сетей (VPN) [4, 5], обеспечивающей построения защищенных каналов взаимодействия между удаленными частными сетями через общедоступную глобальную сеть. Фактически, эта технология позволяет связать две или более удаленные локальные сети в одну территориально-распределенную частную сеть с единым жестким администрированием, гарантирующем уникальность IP-адресов в пределах всей распределенной сети. Однако при наличии большого числа частных сетей, принадлежащих различным организациям, требование жесткого централизованного администрирования становится практически нереализуемым.

Очевидно, что общепринятые средства маршрутизации данных в сети на уровне IP-пакетов [6, 7] могут оказаться несостоятельными, если не гаран-

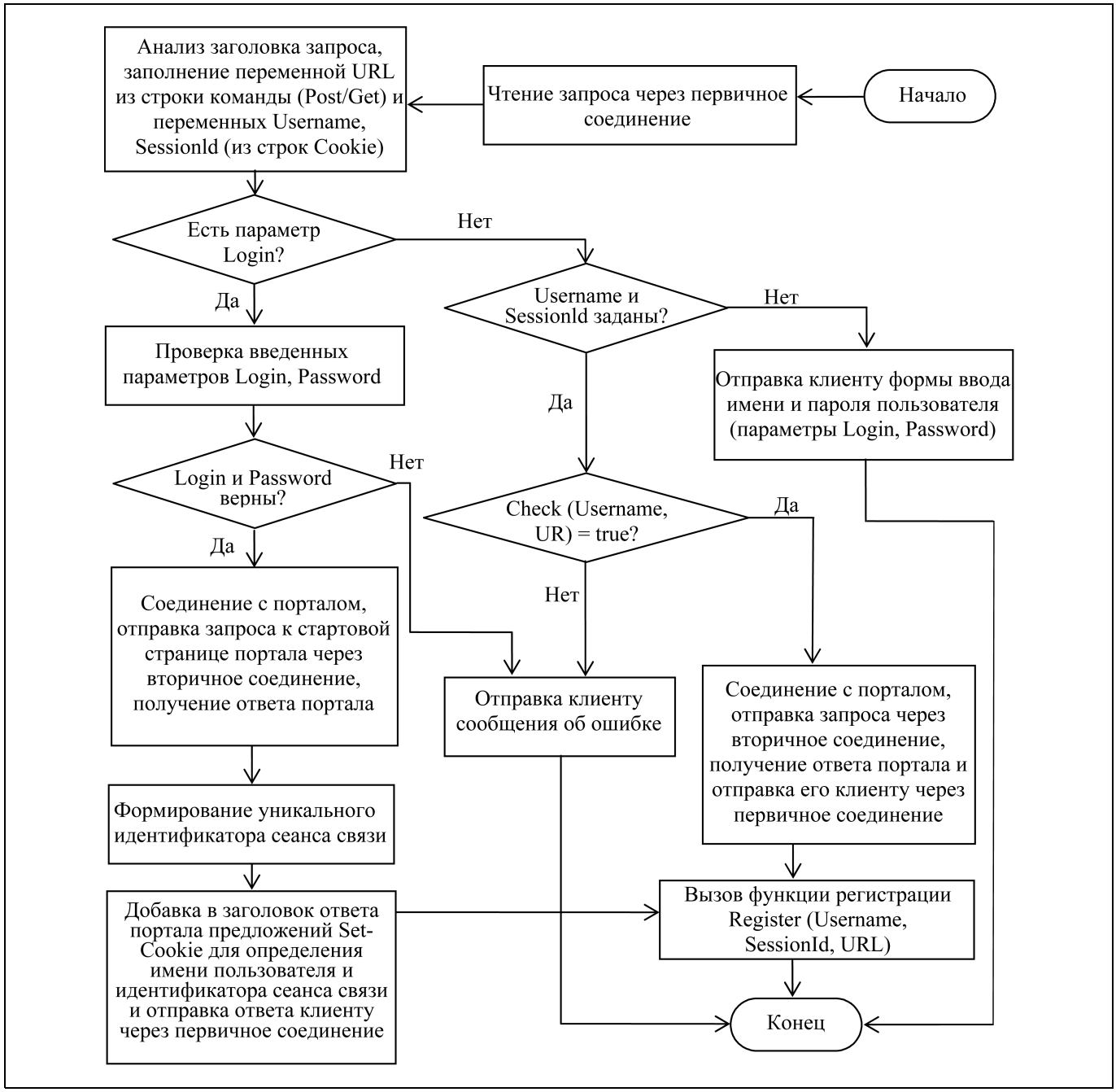

Рис. 1. Алгоритм контроля и мониторинга

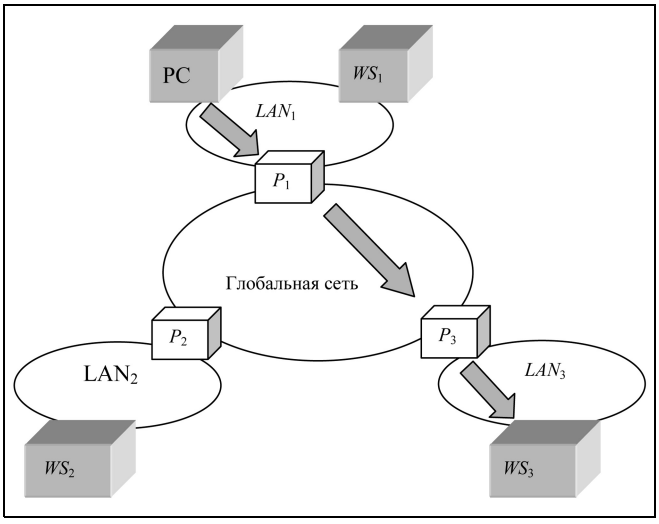

Рис. 2. Маршрутизация запросов между частными сетями: *LAN* — частотная локальная сеть; PC — рабочая станция; *WS* — сервер; *P* — *ПС*-маршрутизатор; ⇨ — информационный запрос

тирована уникальность IP-адресов серверов и клиентов в пределах всей совокупности взаимодействующих частных сетей. Идея рассматриваемого подхода заключается в создании специальных каналов межсетевого взаимодействия в мультисетевой среде, основанных на маршрутизации запросов по символическим именам узлов и ресурсов [8]. Эти каналы базируются на технологии специализированных ПС: серверов-посредников, обеспечивающих последовательную передачу информационных запросов из сети в сеть и оснащенных средствами маршрутизации и защиты данных (рис. 2). Ключевой момент в работе канала — высокоуровневая маршрутизация запросов по символическим именам информационных ресурсов, что позволяет осуществлять доступ, даже если различные ресурсы имеют одинаковые IP-адреса.

Как видно из рисунка, частные сети содержат в своем составе специализированные ПС, функционирующие на «пограничных» узлах и выполняющие функции межсетевых маршрутизаторов. Каждый запрос, направленный из одной частной сети в другую, проходит, по крайней мере, через два ПС и через два этапа маршрутизации. Из ближайшего ПС запрос сначала передается в удаленный ПС по глобальной сети, а уже потом — к адресуемому информационному ресурсу. На каждом этапе маршрутизация проводится на основе символического имени адресуемого ресурса, содержащегося в HTTP-заголовке запроса, с помощью двух таблиц маршрутизации: «глобальной», связывающей имя ресурса с адресом удаленного ПС, и «локальной», связывающей имя ресурса с его URL в частной сети.

Предположим, например, что в сети LAN_2 имеется Web-сервис http://192.168.0.20/persondb/service.asmx, а в сети LAN_3 — Web-сервис http://192.168.0.20/persondb/person.asmx (т. е. обоим сервисам соответствует один и тот же IP-адрес). Предположим, что эти сервисы анонсированы для «внешних» пользователей под символическими именами http://mysys.kaluga.person.ws и http://mysys.omsk.person.ws соответственно. Для организации доступа к сервисам по этим именам в локальную таблицу маршрутизации для LAN_2 следует внести строку, связывающую символическое имя с URL: http://mysys.kaluga.person.ws http://192.168.0.20/persondb/service.asmx, а в таблицу маршрутизации для LAN_3 — строку http://mysys.omsk.person.ws http://192.168.0.20/persondb/person.asmx.

Предположим, что ПС P_2 соответствует IP-адрес 193.232.208.2 в глобальной сети, а ПС P_3 — IP-адрес 193.232.208.3. В этом случае в глобальную таблицу маршрутизации (все ПС используют одну и ту же глобальную таблицу для обработки «исходящих» запросов) должны быть добавлены две строки, связывающие символические имена с адресами ПС:

http://mysys.kaluga.* 193.232.208.2;

http://mysys.omsk.* 193.232.208.3.

Легко заметить, что в обеих строках использованы усеченные символические имена, оканчивающиеся символом «*». Такая нотация обеспечивает маршрутизацию множества имен одной строкой. В данном случае, например, любой запрос к ресурсу с именем, начинающимся с http://mysys.kaluga., будет перенаправлен в сеть LAN_2.

Отметим три важных обстоятельства.

- При изменении URL информационного ресурса в частной сети достаточно внести соответствующую коррекцию в локальную таблицу маршрутизации, чтобы никто из «внешних» клиентов не заметил этого изменения.
- Для защиты информационных ресурсов от внешних атак взаимодействие между ПС должно быть построено на одной из безопасных сетевых технологий. Например, здесь может быть использован протокол HTTPS или уже упоминавшаяся технология VPN (в данном случае — HTTP-взаимодействие «поверх» безопасного протоколов IPsec или PPTP) [6, 7].
- Однажды созданная система каналов межсетевого взаимодействия может быть использована различными распределенными системами, работающими в одной и той же сетевой среде.

3. ЗАДАЧА ЗАЩИТЫ SOAP-СООБЩЕНИЙ

По мере проникновения информационных технологий в сферы госуправления и бизнеса все больше возрастают требования к средствам обеспечения информационной безопасности. Это в полной мере относится и к сетевым технологиям и организации удаленного взаимодействия в распределенных системах. В этой связи были разработаны несколько международных стандартов, касающихся защиты и удостоверения подлинности XML-документов вообще и, в частности, запросов к Web и WCF-сервисам и их ответов (так называемых SOAP-сообщений [2, 3]). В последние годы эти стандарты начинают все более широко применяться в разработках распределенных систем.

В качестве примера можно привести Систему межведомственного электронного взаимодействия (СМЭВ), обеспечивающую информационный обмен между органами госуправления с помощью технологии Web-сервисов. Она представляет собой федеральную государственную информационную систему, предназначенную для интеграции информационных ресурсов различных органов государственной власти на основе единых стандартов защиты информации и сетевых технологий.

Обеспечение информационной безопасности в СМЭВ основано на стандарте 200401 международного консорциума OASIS и стандарте XMLDSIG международного консорциума W3C, описывающих

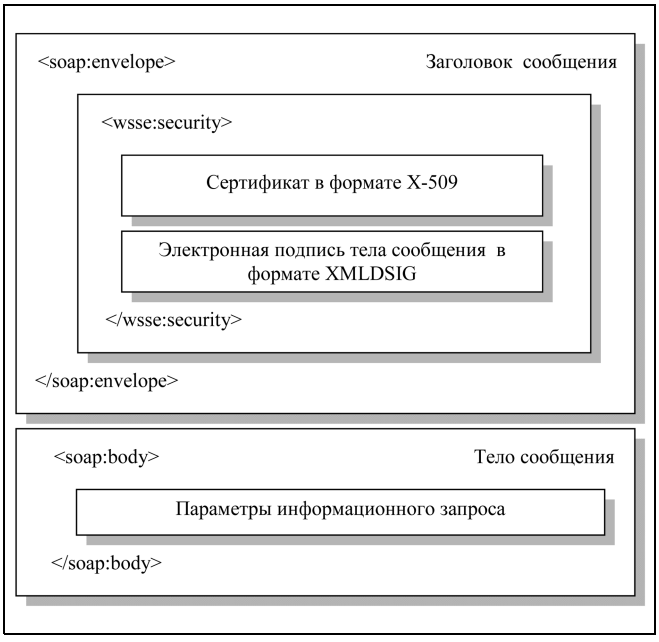

Рис. 3. Размещение электронной подписи в SOAP-сообщении

форматы и правила внедрения электронной подписи в SOAP-сообщения. Причем подпись организации помещается в заголовок сообщения, а подпись исполнителя — в его тело. Формат SOAP-сообщения с электронной подписью, внедренной в его заголовок, проиллюстрирован на рис. 3 (предполагается, что soap и wsse — префиксы пространств имен http://schemas.xmlsoap.org/soap/envelope/ и http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd соответственно).

Каждая организация, стремящаяся подключить своих клиентов к информационным ресурсам СМЭВ или экспортировать в СМЭВ собственные информационные ресурсы (Web-сервисы) должна, так или иначе, решить проблему формирования электронных подписей в «своих» SOAP-сообщениях и проверки электронных подписей у «чужих» в соответствии с принятыми стандартами. К сожалению, в настоящее время не существует ни сколько-нибудь универсальных готовых программных средств для выполнения этих функций, ни описанных подходов к их созданию. Такое положение заставляет разработчиков тратить время и силы на создание множества «частных решений» этой задачи, привязанных к архитектуре и особенностям конкретных систем.

Сформировать подпись тела SOAP-сообщения в его заголовке или проверить такую подпись может только программный компонент, способный «увидеть» сообщение целиком. Поэтому «общее решение» указанной задачи может быть найдено путем размещения этого компонента в специализированном ПС, выполняющем роль посредника между клиентскими рабочими станциями и Web-сервисами организации с одной стороны и СМЭВ — с другой. Таким образом, обеспечивается полная разгрузка клиентов и сервисов организации от каких-либо «забот», связанных с формированием и проверкой электронных подписей в заголовках SOAP-сообщений. Эффективность данного решения заключается в его независимости не только от структуры вызовов и логики работы тех или иных Web-сервисов, но и от систем программирования, задействованных в разработках серверов и клиентов.

Принципы обработки потока SOAP-сообщений (запросов и ответов) в ПС проиллюстрированы на рис. 4. Как видно из рисунка, и поток запросов, направленный от клиентов организации в СМЭВ, и поток запросов, направленный из СМЭВ в сервисы организации, обрабатываются по аналогичным правилам. Важно, что, как и в предыдущем примере, в данном случае ПС должен быть оснащен механизмом маршрутизации запросов — пе-

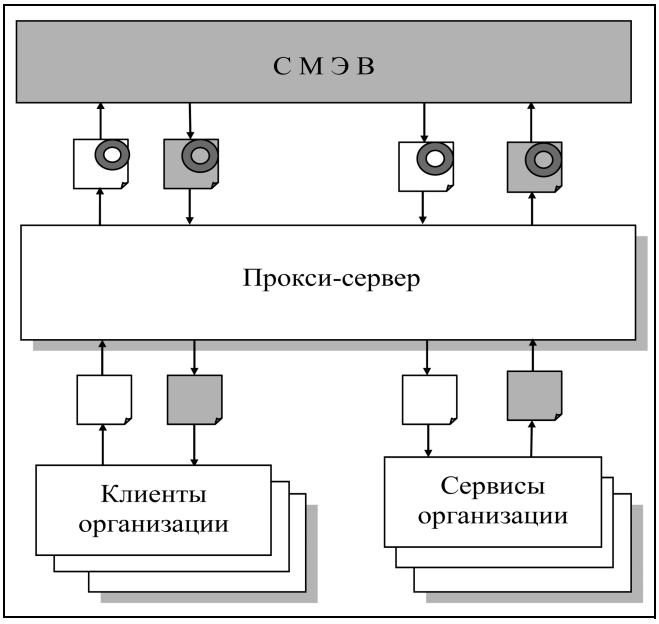

Рис. 4. Обработка потока SOAP-сообщений в ПС:
□ — SOAP-запрос; ■ — SOAP-ответ; ◎ — подпись организации

ренаправления каждого входящего запроса в тот или иной сервис в зависимости от URL в HTTP-заголовке.

ЗАКЛЮЧЕНИЕ

Разумеется, возможности применения ПС в разработках распределенных систем не исчерпываются примерами, рассмотренными в данной статье. На этих примерах авторы попытались показать, что возникшая полтора десятилетия назад технология ПС и в наши дни не потеряла своей актуальности, но может быть применена в сочетании с самыми передовыми сетевыми технологиями для решения самых разных задач в разработках распределенных систем.

В каждом из рассмотренных примеров потребовалась разработка нового специализированного ПС, что, конечно же, было связано с определенными трудозатратами. Однако опыт применения рассмотренного похода показывает, что при наличии опыта сетевого программирования эта задача вполне разрешимая даже для небольшого коллектива разработчиков (в каждом из примеров объем ПС не превышал нескольких тысяч строк кода на языке (C++ или C#). Кроме того, ни одно из рассмотренных технических решений не привязано жестко к конкретному проекту, а является достаточно общим и может быть использовано в разработках различных организационных и экономических систем управления.

ЛИТЕРАТУРА

1. *Фролов А.В., Фролов Г.В.* Глобальные сети компьютеров. — М.: Диалог-МИФИ, 1996. — 256 с.
2. *Шапошников И.В.* Web-сервисы Microsoft.NET. — СПб.: БХВ-Петербург, 2002. — 336 с.
3. *Мак-Дональд М., Шпушта М.* Microsoft ASP.NET 3.5 с примерами на C# 2008 и Silverlight 2 для профессионалов. — М.: Вильямс, 2009. — 1408 с.
4. *Widows* 2000: Server и Professional / А.Г. Андреев, Е.Ю. Беззубов, М.М. Емельянов и др. — СПБ.: БХВ-Санкт-Петербург, 2001. — 1055 с.
5. *Хант К.* TCP/IP. Сетевое администрирование — СПб.: Питер, 2007. — 816 с.
6. *Джамса К., Коуп К.* Программирование для Интернет в среде Windows. — СПБ: Питер, 1996. — 659 с.
7. *Снейдер Й.* Эффективное программирование TCP/IP / Библиотека программиста. — СПб.: Символ-Плюс, 2002. — 320 с.
8. *Асратян Р.Э., Лебедев В.Н.* Организация защищенного http-взаимодействия в мультисетевой среде // Управление большими системами. — 2012. — Вып. 36. — С. 285—300.

Статья представлена к публикации членом редколлегии В.Г. Лебедевым.

Рубен Эзрасович Асратян — канд. техн наук,
вед. науч. сотрудник, ☎ (495) 334-88-61, ✉ rea@ipu.ru,

Виталий Николаевич Лебедев — канд. техн наук,
зав. лабораторией, ☎(495) 334-92-81, ✉ lebvini@ipu.ru,

Институт проблем управления им. В.А. Трапезникова РАН,
г. Москва.