УДК 004.773

ПРОТОКОЛ ДЕЦЕНТРАЛИЗОВАННОЙ СЛУЖБЫ МГНОВЕННЫХ СООБЩЕНИЙ

Бабкин А.А.
Донецкий национальный технический университет г.Донецк
Кафедра компьютерной инженерии
E-mail: pingvinchick@yandex.ru

Аннотация

Бабкин А.А. Протокол децентрализованной службы мгновенных сообщений. *В статье рассматриваются возможности протокола децентрализованной службы мгновенных сообщений (IM службы), а также способы решения недостатков протоколов IM служб, используемых в данное время.*

Общая постановка проблемы. В данный момент в коммуникационной среде большую популярность получает такой сетевой сервис, как служба мгновенных сообщений (а также IP телефония). Это обусловлено тем, что при использовании данных сервисов возможна большая экономия средств в общении с людьми на дальних расстояниях и в других странах.

Также службы предоставляют в большинстве случаев заметное увеличение качества связи, чем обычный телефон. Более того существуют такие удобные возможности, как передача видео и создание конференций, передача файлов (удобно в документообороте).

IM остается выбором способа общения для многих людей, так как предоставляет более «личное» общение нежели электронная почта, но менее навязчивое, чем телефон. IM удобно при двойном общении. Например, вы можете общаться с коллегами посредством IM и одновременно разговаривать по телефону с клиентом.

IM также полезно при общении в чрезвычайных ситуациях, так как Интернет может функционировать во время неполадок на телефонной линии.

Но, тем не менее, данные сервисы не лишены недостатков. Вот главные из них:

- Спам. IM сервис также является объектом нежелательной рекламы (IM спам иногда называют spim). Спам – наиболее раздражающая проблема для пользователей сервисов мгновенных сообщений. Многие организации намеренно используют возможности сервиса для «бесплатной рекламы» путем массовой рассылки спама большому количеству пользователей. Кроме того, такой тип рассылки получил популярность у групп людей, целью которых есть хищение информации либо нанесения намеренного вреда системе пользователя.
- Избыточность передаваемой информации. Данная проблема характерна для таких протоколов, как XMPP (Jabber). Если в корпоративной сети много работников, вовлеченных в чат, это может ударить по загруженности сети и производительности.
- Недостаточные вычислительные возможности сервера. Нередки отключения от сервера пользователей в таких протоколах, как ICQ. Многие пользователи встречались с такими сообщениями, как «лимит подключений превышен». Также были замечены периодические отключения от серверов Skype.
- Низкий уровень сетевой безопасности. Особенно данный недостаток опасен в корпоративных сетях, которые разрешили использовать сервисы мгновенных сообщений среди персонала. Данный пункт заслуживает особого внимания и более детально рассматривается ниже.

Сетевая безопасность служб мгновенных сообщений.

Разные IM приложения используют разные проприетарные протоколы и стандартная конфигурация брандмауэра может не обнаружить их. Многие IM программы могут обходить системы аутентификации. Некоторые IM клиенты могут использовать порты отличные от тех, которые ассоциируются с IM, даже обычно открытые порты, такие как 80.

Основные проблемы безопасности IM сервисов:

- P2P обмен. Данный вид обмена происходит при передаче файлов такими протоколами, как ICQ. P2P обмен дает возможность узнать IP адрес клиента и напрямую подключиться к компьютеру и использовать его уязвимости.
- Шифрование данных и безопасная аутентификация. Многие протоколы на сегодняшний день часто не используют шифрование во время чата и/или передают пароли от учетных записей в открытом виде. Данный недостаток недопустим в корпоративных сетях, которые подразумевают пересылку конфиденциальной информации и конфиденциальное общение.

Таким образом, исходя из перечисленных недостатков IM сервиса, предлагается разработка нового протокола децентрализованной службы мгновенных сообщений DMP (decentralized messaging protocol). Целью разрабатываемого протокола является ликвидация или, по крайней мере, снижение указанных недостатков.

Решение поставленной задачи.

Обзор статистики. Поиск и анализ существующих решений.

Наиболее популярная служба мгновенных сообщений в странах СНГ – ICQ, использующая протокол OSCAR. Однако многие встречались с сообщениями «лимит подключений превышен», а также большое количество спама, рассылаемого ботами. Рассылка спама облегчается способом представления протоколом OSCAR идентификации контактов – по номерам. Таким образом, рассылка спама заключается в переборе номеров из заданного диапазона.

Другой протокол, набирающий популярность - XMPP, также известный как jabber, основанный на XML, открытый, свободный для использования протокол для мгновенного обмена сообщениями и информацией о присутствии в режиме, близкому к режиму реального времени, который также является децентрализованным, но тоже имеет слабые стороны:

- избыточность передаваемой информации: Как правило, более 70 % межсерверного трафика XMPP составляют сообщения о присутствии, около 60 % которых являются излишними.
- масштабируемость: XMPP сейчас фактически страдает от той же проблемы избыточности, но применительно к чат-комнатам и возможностям публикации информации.
- неэффективность передачи бинарных данных: Так как XMPP является, по сути, одним длинным XML-документом, невозможно передать немодифицированную двоичную информацию.

Большинство других протоколов проприетары, поэтому они не рассматриваются.

Решение задачи.

1. Решение проблемы недостаточных вычислительных возможностей сервера, недостаточной ширины канала.

Протокол DMP (decentralized messaging protocol), разрабатываемый автором статьи, ориентирован прежде всего на уменьшение нагрузки на сервер и количества передаваемой информации.

Протокол является децентрализованным, т.е. использующим несколько серверов для распределения нагрузки на каждый из них. Как показывает статистика, около 90% контактов пользователя территориально находятся в пределах одной административной единицы. Таким образом, для обслуживания данной территории эффективно использование отдельного сервера, а для оставшихся 10% контактов – межсерверного обмена. Это решает проблему вычислительных возможностей сервера.

Проблема же ширины канала решается практикой использования протокола XMPP – открытие стандартов разрабатываемого протокола, а также возможность любому желающему поднять сервер службы мгновенных сообщений. Т.е. серверы обслуживаются не единой организацией, а многими частными или юридическими лицами, имеющими разные возможности по передаче трафика.

В отличие от протокола XMPP, маршрутизатор выделен из состава сервера и является отдельной программной единицей, которая может быть установлена как на отдельную машину, так и на машину с установленным сервером DMP.

Также возможно прямое подключение серверов между собой минуя маршрутизатор для разгрузки последнего, а также ускорения обмена между серверами (см. рис. 1).

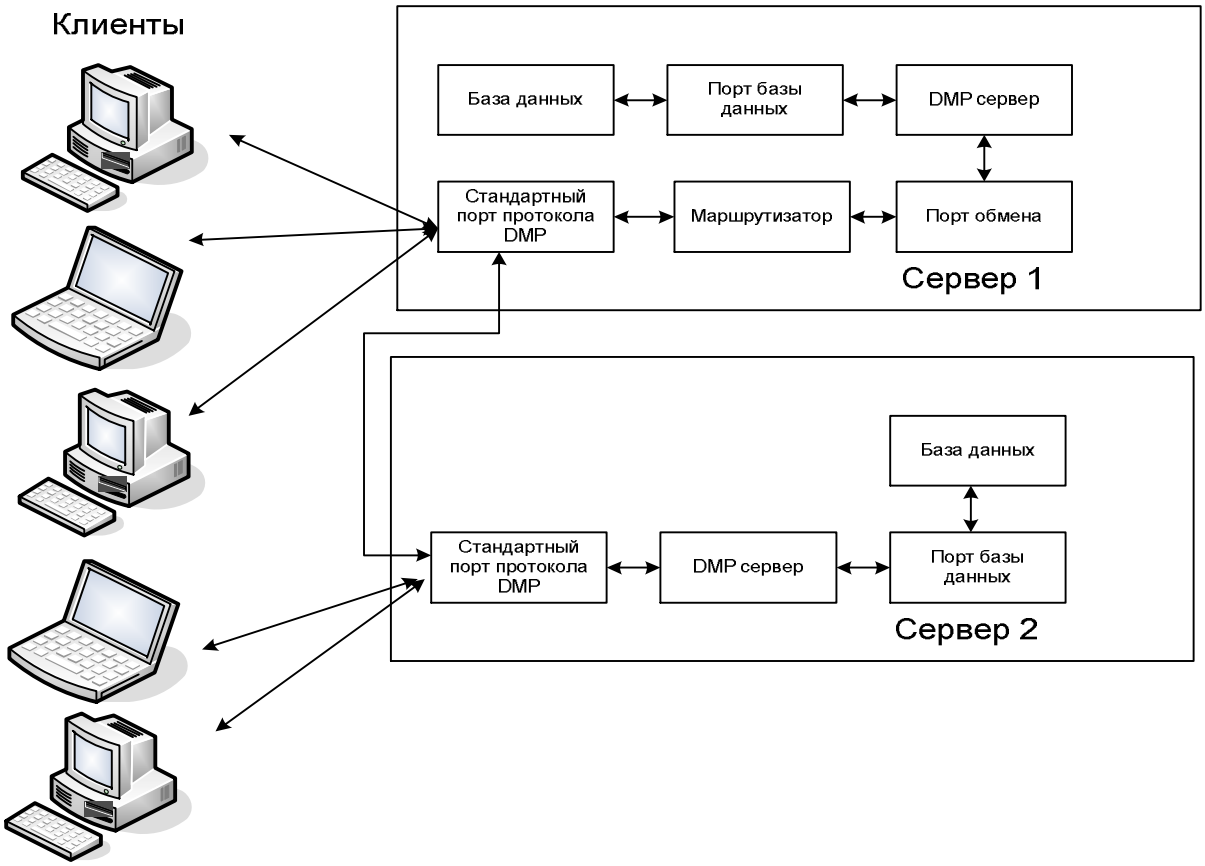

Рисунок 1 - Вариант организации работы службы DMP

Из рисунка **Ошибка! Источник ссылки не найден.** можно увидеть пример возможной структуры службы DMP. На сервере 2 возможно как присутствие маршрутизатора, так и его отсутствие.

Кроме того, протокол предполагает сжатие данных различными компрессорами, формат которых устанавливается активной версией протокола. Для бета-версии протокола устанавливается компрессор bzip2. bzip2 является свободным ПО с открытым исходным кодом. Для последующих версий возможно расширение протокола более эффективными компрессорами. Кроме того, сжатие передаваемой информации должно быть оправдано. К

примеру, компрессия бинарной информации, например, при передаче файлов далеко не всегда себя оправдывает. Данную эффективность следует определять на стороне клиента, что является уже пожеланием для разработчиков клиентского ПО (это не является требованием в условиях сложности контроля для открытого ПО).

Для снижения трафика используется минимализм в организации пакетов, структура которых рассмотрена ниже.

Протокол подразумевает возможность использования количества маршрутизаторов, ограниченного лишь эффективностью их использования.

Также недостатком является сложность контроля возможностей, надежности и безопасности сервера. Данная проблема решается скорее опытом использования конкретного сервера, а также отзывами пользователей.

2. Решение проблем безопасности.

Протокол DMP имеет возможность исключения P2P обмена при передаче файлов. Повышение безопасности реализуется обменом исключительно через сервер. Данный подход явно нагружает как канал, так и сервер всей службы DMP в целом. Однако, информационная безопасность, вне сомнения, важнее, так как, протокол ориентирован на использование в корпоративных сетях, где присутствует конфиденциальная информация.

Кроме того, протокол подразумевает шифрование передаваемых данных и безопасную аутентификацию. Шифрование необходимо для исключения возможных перехватов передаваемой информации и прослушивания.

Кроме того, делается попытка в борьбе со спамом. А именно: лимитация количества передаваемой информации в единицу времени, а также сравнение отпечатков MD5 или SHA частей сообщений или сообщений целиком одного контакта. Если они одинаковы, то при превышении определенного количества совпадений возможна блокировка контакта сервером, как подозрение на рассылку спама ботом. Однако, последний способ является экспериментальным и весьма сомнительным по мнению автора и требует дополнительного тестирования и исследования на практике.

3. Общее описание возможностей протокола.

Предоставляемые возможности протокола DMP представлены в следующих пунктах:

- Протокол использует учетные записи вида nickname@serverdns либо просто nickname с явным указанием IP адреса сервера при подключении, если таковой не имеет доменного имени. Отсутствие требования DNS при подключении дает возможность настройки и использования сервера в локальных сетях без доступа в интернет.
- Существует поддержка списка контактов с указанием статусов присутствия. Также допустимо ведение списков видимости и игнорирования.
- Планируется поддержка передачи звука и видео, организация конференций. Но данные функции пока что отключены, ввиду состояния протокола на уровне бета-тестирования.
- На данном этапе разработки протокол предоставляет возможность использования сервером любой из баз данных. Единственным требованием является соблюдение структуры организации хранения информации о пользователях, а также обеспечение надлежащей безопасности (например, запрет хранения паролей в открытом виде и т. д.).

4. Краткая спецификация протокола.

В данном разделе рассматривается основная единица протокола – пакет. Длина пакета не фиксирована, но не должно превышать фиксированного значения – 1Мбайт. Структура пакета изображена на рисунке 2.

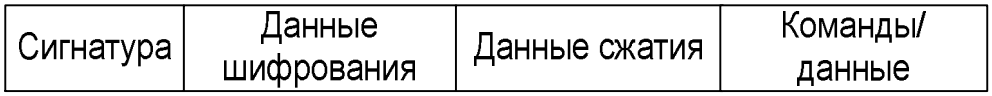

Рисунок 2 - Структура пакета протокола DMP

Как видно из рисунка 2, пакет содержит 4 поля: сигнатуру, данные шифрования, сжатия, а также поле команд и данных.

Для минимизации трафика протокол исключает такие избыточные способы организации информации, как XML.

Сигнатура содержит версию протокола.

Формат команд имеет вид: ID команды:параметры. ID команды представляет собой числовое поле размером 16 бит, т.е. максимальное число команд равно 65536.

Следует отметить, что шифрование и сжатие может отсутствовать.

Выводы. Основываясь на опыте использования служб мгновенных сообщений ICQ и XMPP, разрабатывается протокол DMP. Протокол уменьшает воздействие общих недостатков для служб мгновенных сообщений, а именно:

- снижает объемы передаваемой информации посредством сжатия данных и минимализма в организации команд протокола;
- распределяет нагрузку на сервер и канал путем организации сети серверов;
- повышение безопасности средствами шифрования передаваемой информации, а также исключение P2P обмена;
- осуществляется борьба со спамом путем анализа отпечатков сообщений и количества пользователей, кому адресованы сообщения, а также объема текстовой информации, передаваемой в единицу времени.

Протокол находится на стадии разработки и тестирования, в дальнейшие версиях планируется включение поддержки передачи звука и видео. На текущем уровне развития возможны передачи только текстовой и бинарной информации.

Список литературы:

1. AIM/Oscar Protocol Specification [Электронный ресурс]: спецификация протокола OSCAR– Режим доступа к ресурсу: http://www.oilcan.org/oscar/

2. XMPP RFCs [Электронный ресурс]: спецификация протокола XMPP – Режим доступа к ресурсу: http://xmpp.org/rfcs/

3. ICQ [Электронный ресурс]: Материал из Википедии — свободной энциклопедии – Режим доступа к ресурсу: http://ru.wikipedia.org/wiki/Icq

4. XMPP [Электронный ресурс]: Материал из Википедии — свободной энциклопедии – Режим доступа к ресурсу: http://ru.wikipedia.org/wiki/Jabber

5. Global Instant Messaging Market Share – Open Data [Электронный ресурс]: Статистика использования служб мгновенных сообщений – Режим доступа к ресурсу: http://ru.wikipedia.org/wiki/Jabber

6. 6 IM Network Market Share by Country, July 2008 (%) [Электронный ресурс]: электронная таблица: статистика использования служб мгновенных сообщений – Режим доступа к ресурсу: http://spreadsheets.google.com/ccc?key=p5D5M7Vy6XNdfLH8xX9lbHw&hl=en