УДК 534.29

ПЕРЕДАЧА МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ НА БАЗЕ IP-ТЕЛЕФОНИИ

Ю.Г. ВАШИНКО, А.В. БУДНИК

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 24 января 2008

Рассмотрены различные варианты реализации сетевого телефона в рамках корпоративной сети, а также технология установления сеанса связи для каждой из представленных схем. Проанализирован аспект безопасности и определены основные преимущества и недостатки сетевого телефона.

Ключевые слова: IP-телефония, безопасность в корпоративной сети, сетевой телефон, передача мультимедийной информации.

Введение

На сегодняшний день IP-телефония представляет собой альтернативу классическим телекоммуникационным системам (GSM, ISDN и классическая телефонная связь). Это вызвано, в первую очередь, бурным развитием локально-вычислительных сетей (ЛВС). В 1996 г. сетевой трафик по ЛВС впервые превысил речевой по классическим линиям связи. Этот рост демонстрировал огромные темпы, и уже к 1999 г. в большей части мирового сообщества сетевой трафик использовался активнее, нежели телефонные линии [1].

Понятие VoIP (voice over IP) или IP-телефония подразумевает использование сети Интернет не столько в качестве средства передачи речи, сколько сам протокол IP и технологии, обеспечивающие надежную и высококачественную передачу речевой информации.

Теоретический анализ

Первоочередная цель развертывания сетей на базе IP — это снижение общих расходов на приобретение, установку и содержание телекоммуникационного оборудования. Теоретически, одна объединенная сеть (для передачи данных и для передачи речи) уменьшила бы потребность в квалифицированном персонале — одни и те же люди стали бы заниматься и телефонией, и системой передачи данных. По данным одного из представителей международного оператора связи, переход на технологию IP-телефонии позволит ему сэкономить порядка 70% средств на капитальные затраты, 60–80% — на организацию каналов доступа и 50% — на текущее обслуживание [2].

Основными преимуществами IP-телефонии являются: высокое качество при значительном снижении расходов на обслуживание; возможность существенного повышения безопасности и конфиденциальности обмена данных; гибкость в управлении и развертывании системы.

Необходимо также отметить, что технология передачи информации по сетям привлекает своей универсальностью. Речь преобразуется в последовательность бит и далее может быть

как непосредственно передана получателю, так и подвергнуться дополнительной обработке алгоритмами шифрования и кодирования.

Что касается корпоративной связи, то на сегодняшний день в Республике Беларусь преобладает стационарная телефонная сеть (аналоговая или цифровая). IP-телефония если и применяется, то только в качестве эксперимента, параллельно со стационарной сетью.

Стационарная телефонная сеть подвержена "прямому" прослушиванию канала речи. И если не применять дополнительного оборудования, то злоумышленнику не составит труда подключиться к такой сети. Если применить дополнительные устройства аналогового или цифрового скремблирования (в зависимости от типа автоматической телефонной станции), то линии становятся более защищенными [3]. Но даже для большой компании может быть накладна покупка оборудования скремблирования для каждого стационарного аппарата.

Проанализируем, какие возможности предоставляет IP-телефония для корпоративных сетей.

На рис. 1,*а* представлен самый простой способ установления сеанса связи. Клиент 1 связывается непосредственно с клиентом 2, если он знает местонахождение второго (IP-адрес). При установлении соединения клиент 1 высылает запрос (в открытом виде) клиенту 2 с информацией о методе сжатия или о применении скремблирования. При необходимости (в зависимости от настроек клиента) высылается уведомление на сервер с информацией о начале и завершении сеанса связи. Это используется для учета и протоколирования сетевых разговоров.

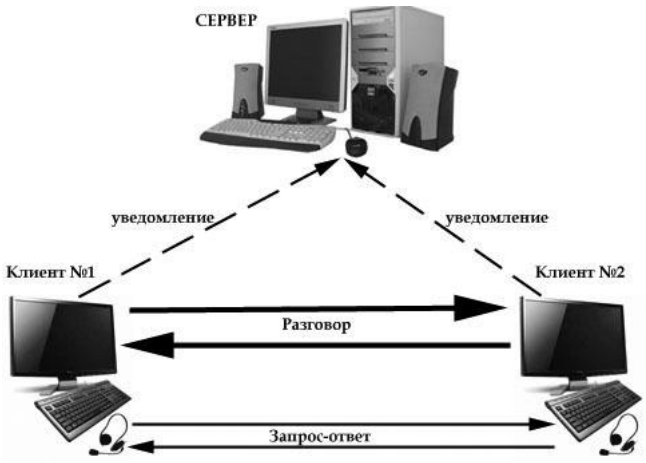
Данная схема соединения обеспечивает наиболее быструю передачу данных, но наименьшую степень безопасности, что вполне приемлемо для "обычных телефонных разговоров". Вызов абонента может осуществляться с любого компьютера от имени любого пользователя.

На рис. 1,*б* представлен второй вариант реализации сетевого телефона, в котором программа-сервер выполняет функции диспетчера или "мини-АТС". Также программа-сервер содержит "абонентскую книгу" клиентов, которая включает такие параметры, как IP-адрес, состояние клиента, имя, по которому зарегистрирован клиент и т.д. При установлении связи программа-клиент (далее "абонент", "клиент") отправляет запрос на сервер. Данный запрос содержит информацию о вызываемом абоненте, а также может содержать информацию о типе шифрование дальнейшего сеанса связи. В свою очередь сервер, получив запрос, отыскивает IP-адрес нужного клиента, определяет его состояние и отправляет запрос на соединение. В случае, если клиент 2 свободен и готов принять "звонок", то клиенту 1 отправляется необходимая информация для установления соединения. Сам сеанс связи осуществляется между клиентами 1 и 2 непосредственно. По окончании разговора серверу отправляется уведомление о завершении сеанса связи. Вся информация такого рода, включая запросы на соединения и их результаты, сохраняется на управляющей машине в зашифрованном виде.

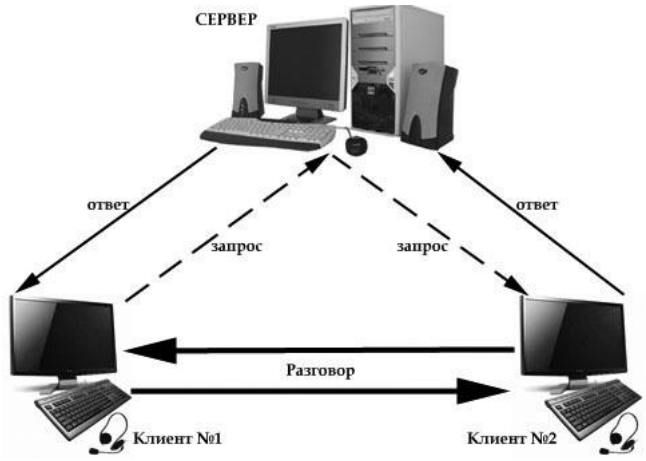
Для обеспечения безопасности данных, передаваемых по схеме, изображенной на рис. 1,*б*, при установке соединения отправляется запрос, в котором содержится информация о виде кодирования или шифрования, которое будет применяться во время сеанса связи. Таким образом, злоумышленник, решив просмотреть сетевой трафик, будет видеть только пакеты зашифрованных данных. Вид шифрования клиент может выбирать сам в зависимости от секретности разговора. Шифрование передаваемой речи осуществляется после преобразования речевого аналогового сигнала в цифровой вид. Перед шифрованием могут применяться различные алгоритмы сжатия для уменьшения передаваемой информации.

При реализации схемы, представленной на рис. 1,*в* весь сеанс связи (передаваемая информация) будет проходить через сервер. Это несколько усложнит и замедлит передачу данных, но данная схема обеспечивает большую безопасность. При подключении нового абонента на сервер высылается запрос о добавлении клиента в адресную книгу. Запрос зашифрован открытым ключом RSA, который объявлен в программе-клиенте как константа инициализации. Запрос содержит в себе, помимо служебной информации, следующее: первоначальные данные о компьютере, IP-адрес, а также значение хэш-функции информации, специфической для данного компьютера (серийный номер логического диска, адрес сетевой карты). Полученная информация хранится на сервере в базе данных. Открытый ключ RSA программы-клиента может изменяться по требованию управляющей машины. При установке соединения клиент 1 отправляет зашифрованный запрос, который, кроме служебной информации, содержит значение хэш-

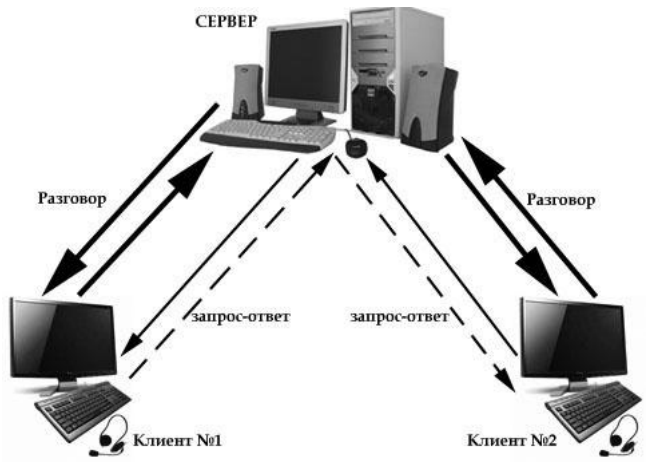
функции уникальной информации в данном компьютере. Сервер при обработке запроса проверяет совпадение хэшей (сравнивается присланный хэш и полученный при регистрации клиента). Если значения не совпадают, то запрос отклоняется с уведомлением (или без него в зависимости от настроек) для клиента 1. Несовпадение хэшей означает, что компьютер, с которого был зарегистрирован абонент и с которого отправили запрос на соединение — различные аппаратные средства. Это может свидетельствовать о проникновении злоумышленника в корпоративную сеть.



а



б



в

Схемы реализации сетевого телефона

В случае, если запрос на соединение от клиента 1 не отклонен, то сервер запрашивает информацию о готовности клиента 2 принять "звонок". В свою очередь, клиент 2 высылает на сервер ответ в зашифрованном виде, который также проходит идентификацию, как и при аутентификации клиента 1. Далее устанавливается соединение таким образом, что вся информация проходит через управляющую машину. Необходимо отметить, что шифрование передаваемой информации может быть различным на этапах клиент 1-сервер и сервер-клиент 2. Для дополнительного обеспечения конфиденциальности связи управляющая машина периодически запрашивает значение хэш-функции уникальной информации компьютеров клиентов. Если данные значения будут отличаться от сохраненных в базе данных, то сервер разрывает соединение принудительно. Изменение хэшей уникальной информации компьютера свидетельствует о смене компьютера после установки соединения, то есть о проникновении злоумышленника.

При такой схеме соединения сервер может осуществить дополнительное управление сеансом связи (например, запись разговора). Как и в схеме рис. 1,*б* все запросы и операции, выполняемые на сервере, сохраняются с указанием времени.

Необходимо также отметить, что вместо наушников и микрофона может быть и другое оборудование, позволяющее считывать и воспроизводить голосовую информацию. К примеру, это могут быть USB-телефоны [4, 5]. Использование такого рода телефонов может исправить недостаток неудобства общения в наушниках с микрофоном.

Заключение

Таким образом, из рассмотренных выше способов организации связи защита передаваемой информации может быть обеспечена схемами, представленными на рис. 1,*б, в*. Кроме того, расширение функциональных возможностей сетевого телефона (передача текстовой и видео информации, организация конференц-связи, размещение досок объявлений) не требует дополнительных затрат на покупку оборудования.

Исходя из возможной функциональности и характеристик безопасности, сетевые телефоны успешно могут заменить стационарную телефонную сеть, обеспечив при этом лучшее качество и защищенность сеанса связи. Уровень защиты передаваемых данных позволяет применять IP-телефонию не только в корпоративных сетях общего назначения, но и в закрытых сетях служб специального назначения.

MULTIMEDIA INFORMATION TRANSMISSION BY IP-TELEPHONY ON A CORPORATE NETWORK

Y.H. VASHINKO, A.V. BUDNIK

Abstract

Different variants of a network telephone implementation and the technology of call establishment for each variant are described. Security aspect is analyzed and advantages and disadvantages of the network telephone are defined.

Литература

1. *Hersent O., Gurle D., Petit J.* IP-Telephony. Packet-based Multimedia Communications Systems. Boston,1999.
2. *Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л.* IP-телефония. М., 2001.
3. *Гольдштейн Б.С., Фрейнкман В.А.* Call-центры и компьютерная телефония. СПб., 2001.
4. *Запечников С.В., Милославская Н.Г., Толстой А.И.* Основы построения виртуальных частных сетей. М., 2003.
5. *Росляков А.В., Самсонов М.Ю., Шибаева И.В.* IP-телефония. М., 2003.