УДК 681.3.06:519.248.681

А. А. ЗАМУЛА, канд. техн. наук, Ю. С. ПАВЛЕНКО

ЗАЩИТА ИНФОРМАЦИИ В IP-ТЕЛЕФОНИИ

Введение

В настоящее время особое развитие получила цифровая телефония. При этом цифровая телефония способствовала улучшению качества телефонных сетей и дала возможность более эффективного их объединения с сетями передачи данных. Это позволило снизить стоимость услуг, а так же удовлетворить возросшие запросы на пропускную способность. К качеству цифровой телефонии предъявляется ряд противоречивых требований – минимизация скорости передачи данных, сохранение приемлемой узнаваемости, сложности реализации, задержек, а в ряде случаев и требования конфиденциальности передачи информации. Особо проблематичными являются задачи аутентификации, так как современные технологии синтеза речи позволяют подделывать ее с высоким качеством.

В связи с вышеуказанным весьма актуальными являются следующие задачи:

1) проведение сравнительного анализа и выбор методов высококачественного сжатия речи, позволяющего с одной стороны минимизировать необходимую пропускную способность, а с другой – обеспечить требуемое качество узнаваемости;

2) поиск и применение методов аутентификации (своего рода узнаваемости) за счет применения криптографических методов аутентификации;

3) выбор и реализация методов криптографической защиты с целью обеспечения конфиденциальности и аутентичности;

4) разработка принципов организации связи для сети общего пользования, обоснование и разработка состоятельных протоколов работы с ключами и режимов работы системы в целом;

1.Анализ методов сжатия речи

Частотный диапазон человеческого голоса равен примерно 20-20000 Гц и может значительно отличаться у отдельных людей. Исследования показали, что без существенных потерь диапазон может быть уменьшен до 100-6000 Гц. Но в самом начале строительства телекоммуникаций предоставить такую полосу частот каждому абоненту было невозможно, и пришлось ради удешевления услуг связи пойти на большее сокращение частотного диапазона до полосы 200-3400 Гц. Это привело к ухудшению разборчивости, но она осталась все же на достаточном уровне. В этой полосе частота выборок согласно теореме Котельникова должна составить не менее 8 кГц, и если при этом использовать 8-разрядный код, то необходимая пропускная способность должна составить не менее 64 кбит/с.

Для уменьшения этой величины применяются различные методы сжатия речи. Одним из первых стандартов, получивших широкое распространение, был G.726 ADPCM (адаптивная дифференциальная импульсно-кодовая модуляция)[3]. При его использовании оцифровывался не сам сигнал, а только его отклонения от предсказанного значения. На каждый отсчет затрачивалось по 4 бита, что позволяло снизить скорость до 32 кбит/с. Позже появилась его разновидность, позволившая еще снизить скорость до 24 кбит/с. По-настоящему снизить скорость удалось только с распространением кодеков на базе линейного предсказания, которые хоть и появились в конце 60-х, но до сих пор остаются основным способом сжатия речи.

В табл. 1 приведены характеристики кодеков и их применение.

Таблица 1

Скорость передачи, кбит/с	Субъективное качество	Название стандарта	Год выпуска	Алгоритм	Область применения
64	4,1	ITU-T G.711	1960	PCM	Телефонные сети
32	3,8	ITU-T G.726	1984	ADPCM	Телефонные сети
6,4	3,1	INMAR-SAT-M	1990	IMBE	Спутниковая телефония
13	3,3	ETSI GSM	1992	RPE-LTP	Сотовая телефония (Европа)
16	3,6	ITU-T G.728	1992	LD-CELP	Телефонные сети

Продолжение таблицы 1

Скорость передачи, кбит/с	Субъективное качество	Название стандарта	Год выпуска	Алгоритм	Область применения
4,8	3,4	ETSI TETRA	1996	ACELP	Сотовая телефония (Европа)
6,3	3,9	ITU-T G.723.1	1996	MP-MLQ	Телефонные сети
5,3	3,7	ITU-T G.723.1	1996	ACELP	Телефонные сети
8	3,9	ITU-T G.729	1997	CS-ACELP	Телефонные сети
2,4	3,5	США (проект)	1998	MELP	Мин. Обороны США

Из относительно новых алгоритмов стоит назвать совместную разработку фирм Audiocodec (Израиль) и DSP Group (США) - кодек с линейным предсказанием и скоростью выходного потока информации 6,3 кбит/с[4]. Несмотря на значительно большую, чем у АДИКМ, среднеквадратичную погрешность синтеза, получена лучшая (3,9 балла MOS) оценка качества, чем у АДИКМ. Это достигнуто благодаря двум усовершенствованиям алгоритма линейного предсказания алгебраического CELP. Первое: длина сглаживающего окна трехкратно увеличена относительно длины анализируемого сегмента речи, что ослабило искажения, вносимые асинхронностью анализируемых сегментов речи и интервалов основного тона. Второе: метод более точного формирования сигнала возбуждения синтезирующего фильтра, названный авторами MP-MLQ (Multipulse Maximum Likelihood Quantisation). Еще одним важным преимуществом этого алгоритма является более надежное, по сравнению с предшественниками, вычисление параметров основного тона голоса. Алгоритм MP-MLQ относится к семейству analysis-by-synthesis алгоритмов. В кодере построенном на MP-MLQ используется линейное прогнозирование 10-го порядка и может работать на скоростях 4.8, 6.4, 7.2 и 8.0 кбит/с. Гибкость алгоритма дает возможность выполнять перепрограммирование в ходе разговора при ухудшении связи, а также снизить скорость до 4.0 кбит/с. Все эти особенности, а также заявленное качество речи, склонили нас к выбору именно этого кодека.

Для существующих и распространенных реализаций кодеков авторами было проведено исследование по качеству сжатия и размерам полученного сжатого файла. Для этого была написана программа, позволяющая преобразовать WAV файл в формате PCM в WAV файл, где речь записана в другом формате[1]. В качестве исходного файла был взят файл длиной 4,25 секунды и размером 76612 байт. Результаты приведены в табл. 2.

Таблица 2

Алгоритм	Размер, байтов	Время, сек	Примечание
PCM	76612	4,25	1
CCITT A-Law	38342	4,50	1
CCITT u-Law	38342	4,50	1
DSP Group TrueSpeech™	5178	4,74	1
GSM 6.10	7860	4,46	1
IMA ADPCM	19260	4,98	1
Lernout & Hauspie CELP 4.8kbit/s	2926	4,66	3
Lernout & Hauspie SBC 16kbit/s	11358	4,48	3
Lernout & Hauspie SBC 12kbit/s	6470	2,98 ?	4
Lernout & Hauspie SBC 8kbit/s	3676	1,54 ?	4
Microsoft ADPCM	19694	4,97	1
MPEG Layer-3	9356	4,00	2

В графе примечания указаны особенности преобразования речи:

1. Отличная разборчивость, помех практически нет. Фраза звучит полностью.
2. Отличная разборчивость, но фраза звучит не полностью (несколько последних букв отсутствуют).
3. Разборчивость хорошая, но есть заметные (не мешающие восприятию) искажения. Фраза звучит полностью.
4. Достаточная разборчивость, но искажения почти на всем протяжении фразы. Фраза звучит не полностью (несколько последних букв отсутствуют). Непонятны значения длительности записи, так как фраза реально звучала в обоих случаях более 4 секунд.

2. Протоколы обеспечения конфиденциальности и установления подлинности абонентов защищенного канала

Обеспечение высокого уровня аутентичности корреспондентов только за счет узнаваемости на слух нельзя считать эффективным методом решения этой задачи. Она должна решаться комплексно – с учетом принципов узнаваемости, а также с применением несимметричной криптографии на этапах вхождения в связь и ведения связи. Принципы несимметричной криптографии в данном случае предполагает применение личных ключей каждого из абонентов и состоятельных протоколов на комбинации долговременных и сеансовых ключей.

Конфиденциальность цифровой телефонии предпочтительно обеспечивать за счет применения симметричного шифрования. Для этих целей можно использовать такие стандарты, как ГОСТ 28147, IDEA, Rijndael. Кроме непосредственно шифрования речевой информации с помощью вышеуказанных алгоритмов требуется создание защищенной сети со станцией генерирования и распределения ключей. Сгенерированные долговременные ключи распределяются корреспондентам с использованием состоятельных протоколов. Доступ к системе пользователь получает после ввода личного ключа, носителем которого является смарт-карта. После этого производится синхронизация и аутентификация обеих сторон связи и вырабатываются сеансовые ключи.

Передача речевой информации происходит в обоих направлениях и логичной была бы организация полнодуплексного канала связи. Но так как разговор идет обычно по очереди (абоненты слушают друг друга) и вычислительное устройство, производящее кодирование и декодирование, работает в последовательном режиме обработки команд, то здесь нужно использовать многозадачность с разделением по времени, т.е. кодированию и декодированию поочередно выделяют небольшой промежуток времени. Связь при этом получается полудуплексной. Рассмотрим протоколы используемые для шифрования информации во время разговора и установления связи. В начале установления сеанса связи каждый из абонентов вырабатывает личный сеансовый ключ и абоненты производят обмен данными ключами по схеме Диффи-Хелмана.

После этого вырабатывается общий секрет K, который и служит в дальнейшем для образования сеансового ключа симметричной системы шифрования r.

На этом ключе формируется сеансовый ключ для шифра Rijndael функционирующего в потоковом режиме, а также шифруют пакеты с ключевой информацией.

Схема выработки сеансового ключа K для схемы Диффи-Хелмана указана в таблице 3.

Таблица 3

A		B
$Y_A = \Theta^{X_A} \bmod N$	⟷	$Y_B = \Theta^{X_B} \bmod N$
S_A		S_B
$D_A = \Theta^{S_A} \bmod N$	⟷	$D_B = \Theta^{S_B} \bmod N$
$K_{AB} = D_B^{S_A} \cdot Y_B^{X_A} \bmod N = \Theta^{S_B \cdot S_A} \cdot \Theta^{X_B \cdot X_A} \bmod N$		$K_{BA} = D_A^{S_B} \cdot Y_A^{X_B} \bmod N = \Theta^{S_A \cdot S_B} \cdot \Theta^{X_A \cdot X_B} \bmod N$

После этого производят выработку сеансового ключа для алгоритма шифрования Rijndael по правилу:

$$r = Rijndael(H(K), R_{дол г}),$$

т.е. путем шифрованием хеш-функции сеансового ключа K на долговременном ключе для алгоритма Rijndael $R_{долг}$.

Полученный сеансовый ключ r объединяется с возможной другой служебной информацией, шифруется на сеансовом ключе K и отправляется другому абоненту.

В результате получается трехуровневый протокол управления ключами:

1) долговременные ключи X,R;
2) сеансовый ключ для схемы Диффи-Хелмана K;
3) сеансовый ключ для потокового режима передачи речевой информации r;

При этом долговременные ключи используются для формирования сеансовых ключей и никогда – для передачи речевой информации, что существенно снижает возможность перехвата и накопления статистического материала.

Заключение

Существующие разработки в области защиты речевой информации основываются на различных методах скремблирования речи, однако применение таких методов не позволяет обеспечить аутентификацию участников обмена информацией. Предложенная выше схема совместного использования преобразования речи в цифровой вид и цифровых методов шифрования и аутентификации позволяет обеспечить как требуемый уровень надежности аутентификации и сокрытия смысла информации, так и снизить требования к пропускной способности, а значит увеличить количество одновременных разговоров по стандартной линии передачи информации.

Список литературы: **1.** *Секунов Н.Ю.* Обработка звука на PC. С-Пб.: БХВ-Петербург, 2001. 1248 с. **2.** *Назаров М.В., Прохоров Ю.Н.* Методы цифровой обработки и передачи речевых сигналов. М: Радио и связь, 1985. 176 с. **3.** *American National Standards Institute*, Inc. 1987. American National Standard for Telecommunications: Digital Processing of Voice-Band Signals-Algorithm and Line Format for 32kbit/s. Adaptive Differential Pulse-Code Modulation (ADPCM). New York: ANSI, Inc. **4.** *ITU-T Recommendation G.723.1* Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 27.03.2001