В. П. З я з и н, **М. В. Ф е д ю к и н** (Москва, МИРЭА, ООО «Линфо»).
О скрытой передаче информации в потоке данных IP-телефонии.

В современных публикациях по стеганографии рассматриваются подходы использования пакетов RTP-трафика для построения скрытых каналов передачи информации на основе модификации содержимого сетевых пакетов и времени их доставки (например, [1–4]).

В развитие этого направления нами предлагается применять адаптивное управление задержкой части пакетов, передаваемых в сеансах IP-телефонии. Суть метода такова. Со стороны отправителя некоторые выбранные аудио пакеты искусственно задерживаются перед отправкой. Если временной интервал задержки получателем пакетов (который, вообще говоря, может и не знать о скрытых каналах) определяется недопустимым, то искусственно задержанные пакеты не участвуют в реконструкции аудио потока. Для организации скрытого канала следует использовать именно эти, «утраченные» пакеты. Рассматриваются четыре сценария работы этого метода. В первом случае один пакет, взятый из потока RTP, и его содержание (поля, содержащие фреймы аудио потока) заменяются битами стеганограммы. Во втором случае выбранные из потока пакеты задерживаются на определенное время и затем отправляются получателю. В третьем случае, если какой-то пакет, который был задержан перед отправкой, попадает получателю, не являющемуся участником стеганографического обмена, то такой пакет считается бракованным и игнорируется. В четвертом случае, если получатель осведомлен о наличии в потоке скрытой информации (т. е. участвует в стеганографическом обмене), то вместо удаления пакета он может извлечь содержимое этого пакета. Эффективность предлагаемого метода зависит от многих факторов: используемого кодека, размера аудио фрейма, частоты кодирования голоса, размера буфера при получении и т. д.) и от сетевого QoS (установок задержки и потери пакетов). Поскольку предлагается задействовать только пакеты, необходимые для передачи голоса (т. е. «лишние» пакеты не создаются), то возможно ухудшение качества звука. Поэтому реализация стеганографической процедуры должна учитывать приемлемый для IP-телефонии уровень потери пакетов. Известно, что уровень потери пакетов при использовании кодека G.711 может доходить до 5–8%. Учитывая этот факт, а также алгоритмы искусственной задержки сетевых пакетов, можно оценить пропускную способность соответствующего скрытого канала, которая зависит только от допустимого уровня потери пакетов.

Чтобы аудио пакет был распознан на принимающей стороне как утраченный, задержка должна иметь значение, превышающее определенный для протокола уровень. Для правильного выбора интервала задержки необходимо учитывать размер реконструирующего буфера получателя, обеспечивающего удаление эффекта дрожания звука. Очевидно, для снижения риска обнаружения скрытого канала следует выбирать интервал задержки насколько возможно малым. Кроме того, чтобы общий уровень потери пакетов в сети не превышал допустимых норм, необходимо постоянно следить за состоянием сети (задержки пакетов могут возникать также из-за особенностей и загрузки сети), через которую передаются потоки информации, и динамически изменять параметры предлагаемого скрытого канала.

СПИСОК ЛИТЕРАТУРЫ

1. *Mazurczyk W.*, *Szczypiorski K.* Covert Channels in SIP for VoIP signaling. — In: Proceedings of the 4th International Conference on Global E-security 2008 «Communications in Computer and Information Science» (CCIS 12). London, United Kingdom, June 23-25, 2008. Berlin–Heidelberg: Springer Verlag, 2008.
2. *Mazurczyk W.*, *Szczypiorski K.* Steganography of VoIP Streams. — In: Proceedings of OnTheMove Federated Conferences and Workshops OTM 2008: The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, November 9-14, 2008. Lecture Notes in Computer Science (LNCS) 5332. Berlin–Heidelberg:

Springer Verlag, 2008.
3. *Mazurczyk W.*, *Lubacz J.* Analysis of a Procedure for Inserting Steganographic Data into VoIP Calls. — In: Proceedings of the 5th Polish-German Teletraffic Symposium PGTS'08, Berlin, Germany, October 6–7, 2008.
4. *Mazurczyk W.*, *Lubacz J.*, *Szczypiorski K.* Hiding Data in VoIP. — In: Proceedings of the 26th Army Science Conference, December 1–4, 2008, Orlando, FL, USA.