

УДК 681.3

А.С.Куприянов (6 курс, каф. РВиКС), А.Ю.Глебовский, к.ф.-м.н. доц.

ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Глобальная видеоконференцсвязь (ВКС) через компьютерные сети находит все более широкое применение в научных и образовательных учреждениях как современное телекоммуникационное средство поддержки совместной работы распределенных исследовательских групп (CSCW – Computer Support for Collaborative Workgroups), а также в дистанционном обучении и в дистанционном управлении. Благодаря техническому прогрессу в области аппаратного и программного обеспечения ВКС эти системы становятся все более совершенными и доступными расширяющемуся кругу пользователей. В связи с этим возрастает актуальность проблемы защиты сеансов двухточечной и многоточечной связи от несанкционированного доступа (как со стороны злоумышленников, так и от несвоевременных дозвонов).

Типичная проблема возникает при использовании MCU (Multipoint Conferencing Unit), когда в назначенное время станция ожидает вызовов от запланированных участников сеанса связи (в стандартном случае одновременно подключаются до четырех удаленных станций). При этом в режиме ожидания обычно включается опция “разрешить автоматическое подсоединение” (enable auto-answer), что часто приводит к нежелательным подключениям, со всеми вытекающими отрицательными для участников конференции последствиям.

Оборудование, предназначенное для видеоконференций, не всегда сопровождается соответствующим программным обеспечением (ПО), что вынуждает либо покупать ПО за дополнительную плату, либо использовать свободно распространяемое ПО, либо, наконец, разрабатывать собственные программные средства предупреждения нежелательных “дозвонов”.

Одна из конкретных задач состоит в следующем. Установлен аппаратный комплекс Polysom ViewStation FX. Он совмещает в себе камеру, видеоконференционный терминал, сервер мультikonференций (MCU) и некоторые другие функции. В дальнейшем данное устройство будет именоваться терминал. Терминал подключен к двум сетям: к IP-сети (стек протоколов H.323) и к сети ISDN (стек протоколов H.320). Требуется разработать программные средства для выполнения функций органайзера.

Органайзер служит для управления терминалом Polysom ViewStation FX и реализован в виде программы или комплекса программ, выполняющихся на отдельном сетевом компьютере. Органайзер должен иметь расписание и набор правил, согласно которым он может осуществлять дозвон до абонентов, разрыв соединений, прием входящих звонков, отказ от входящих звонков.

Существует целый ряд программ, обеспечивающих функцию органайзера. К ним относятся как продукты компании Polysom, так и других фирм. Основные программы компании Polysom, обеспечивающие функцию органайзера – WebCommander и Network Aware Scheduler. Network Aware Scheduler позволяет назначать конференции заранее, управлять ресурсами, работать с оборудованием различных фирм, объединять различные сети, обнаруживать и исправлять неисправности и т.п. По сути, данный продукт рассчитан на сложную сеть со многими терминалами. Network Aware Scheduler управляется с использованием Outlook. WebCommander также служит для управления большой сетью с большим количеством терминалов, но в нем больше внимание уделяется администрированию и биллингу. WebCommander управляется как через Outlook, так и через

веб-интерфейс. Вариант установки платного ПО требует весьма значительных финансовых затрат.

Альтернативный путь заключается в установке и настройке свободно распространяемого гейткипера и написании ПО, управляющего им. Гейткипер – понятие, используемое в терминологии стека протоколов N.323. Гейткипер – необязательный программный комплекс, осуществляющий администрирование, разрешение и запрещение установки соединений, управление именами, управление зонами, контроль ширины полосы и некоторые другие функции. В стеке протоколов N.323 есть несколько протоколов для обмена данными между терминалом и гейткипером. В случае наличия, гейткипер берет на себя те или иные функции управления. На данный момент известны три свободно распространяемых гейткипера: GnuGK, OpenGK и OpenGatekeeper. Каждый из них имеет определенные преимущества и недостатки, однако, на данный момент трудно сказать, какой из них лучше всего подходит для решения поставленной задачи, поскольку данные гейткиперы не имеют подходящего интерфейса. Некоторые из них могут управляться файлом настроек, другие – командами поверх протокола TCP, третьи имеют графический интерфейс управления, однако, не удовлетворяющий некоторым требованиям. Поэтому после установки гейткипера потребуются написание управляющей части. Вариант с установкой гейткипера имеет существенный недостаток – гейткипер может работать только с протоколом N.323, в то время как необходимо управлять терминалом как при работе с протоколом N.323, так и при работе с протоколом N.320.

Третий путь – написание собственного программного обеспечения для управления терминалом. Для станций Polusom при этом возможны два подхода. Во-первых, можно использовать управление по протоколу HTTP. Другая возможность написания собственного органайзера заключается в управлении терминалом по протоколу telnet.

При решении поставленной задачи были изучены обе возможности и выявлены преимущества последнего подхода. На данный момент написан программный прототип собственного органайзера, управляющего терминалом по протоколу telnet. Текущая версия имеет графический интерфейс, управляет терминалом по протоколу telnet, имеет расписание и набор правил, описывающих поведение терминала в тех или иных случаях, может устанавливать и разрывать соединение, принимать или не принимать входящие вызовы.