# ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ МОБИЛЬНОГО УДАЛЕННОГО ДОСТУПА К ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ МОНИТОРИНГА ДЕЯТЕЛЬНОСТИ КАФЕДРЫ

## А. М. Бершадский, И. П. Бурукина, А. А. Акимов

Пензенский государственный университет

Пенза

bam@pnzgu.ru, burukina@rambler.ru, akimov1987@gmail.com

При построении информационно-аналитической системы мониторинга деятельности кафедры был реализован принцип «повсеместного» (ubiquitous) доступа к информационным ресурсами с поддержкой мобильности пользователей (технология u-learning). Подобный принцип предполагает широкое использование технологий беспроводной и мобильной связи (Bluetooth, WI-FI, WI-MAX, GPRS, EDGE, UMTS, WAP) [1, 2].

Современные беспроводные сети позволяют решать множество задач: от организации сети внутри помещения, Hot-Spotов до распределенных сетей в масштабах города, региона и даже целого государства. Низкая стоимость, быстрота развертывания, широкие функциональные возможности по передаче трафика данных, IP-телефонии, видео – все это делает беспроводную технологию одним из самых быстрорастущих телекоммуникационных направлений. Беспроводные технологии превосходят проводные по трем параметрам: по быстроте развертывания, удаленности и мобильности. Сегодня уже очевидно, что создание сплошной зоны покрытия беспроводного сигнала с использованием средств беспроводных средств связи различных стандартов – требование времени, и динамика распространения беспроводных технологий становится все более стремительной [1, 3].

При обеспечении мобильного удаленного доступа на базе беспроводной сети возникает ряд проблем. Наиболее важными из них являются информационная безопасность и построение интерфейса пользователя. Рассмотрим их подробнее.

Без обеспечения должной защиты конфиденциальности и целостности информации при ее передаче между рабочими станциями и точками доступа нельзя быть уверенным в том, что информация не будет перехвачена злоумышленником и что рабочие станции и точки доступа не будут подменены посторонним лицом. Стандарты беспроводных сетей 802.11X предусматривают несколько механизмов обеспечения безопасности [4, 5]:

* режим аутентификации и шифрования данных по протоколу WEP (Wired Equivalent Privacy);
* режим аутентификации и шифрования данных по протоколу WPA (Wi-Fi Protected Access);
* проверка подлинности 802.1X;
* режим скрытого идентификатора сети.

При включении протокола WEP производится настройка ключа безопасности сети. Этот ключ осуществляет шифрование информации, которую компьютер передает через сеть другим компьютерам. Принимающему компьютеру нужен ключ для расшифровки информации, поэтому посторонним пользователям или другим компьютерам сложно подключиться к сети и получить доступ к файлам без соответствующего разрешения.

Однако в структуре и реализации WEP имеются серьезные недостатки, а разгадать ключ шифрования и взломать защиту WEP можно с помощью целого ряда инструментов [6], что привело к созданию протокола WPA(Wi-FI Protected Access). Протокол был представлен в 2003 году, его отличительной чертой стал алгоритм по динамической генерации ключей при шифровании данных. Согласно данному протоколу, вектор инициализации является 48-битовым (а не 24-битовым, как при использовании протокола WEP), при этом реализуются изменения последовательности битов, благодаря чему исключается повторное использование одних и тех же ключей. Для любого передаваемого пакета данных генерируется новый 128-битный ключ. В каждый передаваемый кадр помещен особый 8-байтный код целостности, с помощью проверки которого становится возможным отражение атак с использованием подложных пакетов. В результате получается, что у каждого передаваемого по сети пакета данных есть свой уникальный ключ, при этом любое устройство беспроводных сетей наделено собственным динамически изменяющимся ключом.

Проверка подлинности 802.1X позволяет повысить уровень безопасности для беспроводных сетей стандарта 802.11X и проводных сетей Ethernet. 802.1X при помощи сервера проверки подлинности осуществляет проверку пользователей и предоставляет доступ к сети. В беспроводных сетях проверка подлинности 802.1X может применяться совместно с ключами протокола WEP или протокола WPA.

Еще одна мера предосторожности, которую часто используют в беспроводных сетях, – это режим скрытого идентификатора сети. Каждой беспроводной сети назначается свой уникальный идентификатор (SSID), который представляет собой название сети. При попытке пользователя войти в сеть драйвер беспроводного адаптера прежде сканирует эфир на предмет наличия в ней беспроводных сетей. При использовании режима скрытого идентификатора (Hide SSID) сеть не отображается в списке доступных и подключиться к ней можно только в том случае, если, во-первых, точно известен ее SSID, а во-вторых, заранее создан профиль подключения к этой сети.

Используя один или несколько способов защиты (при условии их правильной настройки), можно построить на базе стандартов серии 802.11X защищенную и устойчивую к атакам беспроводную сеть и быть уверенным в обеспечении необходимого уровня безопасности.

При создании интерфейса пользователя разработчики сталкиваются со следующими трудностями:

* отсутствие общепринятой модели представления контента;
* отсутствие стандарта представления информации для разных типов мобильных и стационарных устройств (характеризуемых разными размерами экрана, графическими возможностями и т.д.);
* отсутствие общепринятой концепции навигации, представления карты сайта и т.п.

В связи с перечисленными трудностями создание удобного и функционального интерфейса пользователя становится весьма нетривиальной задачей.

Функционирование системы происходит следующим образом:

* запросы пользователей поступают от браузеров клиентов и проходят через сеть связи;
* производится обработка полученной информации на веб-сервере и преобразование ее в последовательность обращений к серверу БД;
* осуществляется собственно обращение к серверу БД за результатами;
* формируются наборы данных от серверов БД на веб-сервере, и производится вывод данных на браузеры клиентов.

Взаимодействовать с системой посредством технологий беспроводного мобильного доступа могут следующие типы клиентов:

* Мобильное устройство (сотовый телефон, КПК, смартфон, коммуникатор или планшет), имеющий браузер, используется в качестве оконечного клиентского устройства. Используемый протокол передачи данных может обеспечивать как связь точка – точка, так и пакетную передачу на основе протокола GPRS.
* Переносной или стационарный компьютер с сотовым модемом. В этом случае для клиента сохраняются все средства полноэкранного браузера, а беспроводная сеть используется лишь в качестве среды передачи данных.
* Совместное использование компьютера (переносного или стационарного) и сотового телефона, имеющего средства синхронизации с компьютером, например соединение с компьютером через USB-порт.

Беспроводные сети являются сегодня одной из самых перспективных и развивающихся технологий, открывающей новые возможности. Использование средств беспроводного доступа к информационно-аналитической системе мониторинга деятельности кафедры обеспечило экономию времени и средств при развертывании системы, мобильности пользователей, доступ в реальном времени к общим информационным ресурсам посредством мобильных устройств.

Библиографический список

1. Финогеев А. Г. Беспроводные технологии передачи данных для создания систем управления и персональной информационной поддержки [Электронный ресурс] / / Обзорно-аналитическая статья по приоритетному направлению «Информационно-телекоммуникационные системы», 2008. С. 51. URL: http://www.ict.edu.ru/ft/005654/62331e1-st18.pdf
2. Финогеев А. Г. Обмен данными в информационном пространстве с использованием технологий беспроводной связи / А. Г. Финогеев, В. А. Маслов, А. А. Финогеев // Информатизация образования и науки. 2011. ¹ 1(9). С. 44–55.
3. Агаев Б. С. Анализ беспроводных сетевых технологий для распределенной обработки информации (обзор) / Б. С. Агаев, Т. С. Алиев. Баку, 2007. С. 120.
4. Сумина Г. А. Защита информации в беспроводных сетях / Г. А. Сумина, Е. А. Кожанов, А. Н. Степина // Телематика'2008: труды XV Всероссийской науч.-метод. конф. Т. 1. СПб.: СПбГУ ИТМО, 2008. С. 187–188.
5. Педжман Р. Основы построения беспроводных локальных сетей стандарта 802.11. Руководство Cisco / Р. Педжман, Д. Лиэри. М.: «Вильямс», 2004. С. 304.
6. Феллинг Д. Безопасность сетей 802.11g – это просто [Электронный ресурс]. URL: http://www.os
p.ru/win2000/2006/02/1156337/