А. А. Балаев, В. С. Горбатов, Д. Т. Сепашвили

ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ PLC-ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ[1]

Стремление к удобству, комфорту и эффективному использованию ресурсов бытового обеспечения актуализирует задачу построения так называемых «умных домов» («интеллектуальных зданий», «умных электросетей» и т. д.). Такие объекты являются ярким примером практической реализации на бытовом уровне концепции автоматизированных интеллектуальных систем [1], в которых в максимально достижимой на сегодня степени автоматизированы все процессы управления техническими средствами с минимальным вмешательством пользователей. Однако при этом не надо забывать, что без решения проблем информационной безопасности технологий передачи и/или обработки данных в таких системах реализация вышеуказанной концепции может привести к плачевным результатам.

Очевидно, что система управления «интеллектуальным зданием» является принципиально открытой распределенной компьютерной системой, в которой соответствующие угрозы, уязвимости и риски могут быть связаны как с недостаточностью знаний самих пользователей, так и с серьезными злоумышленными действиями третьих лиц. Последнее особенно актуально, если интеллектуальная система имеет выход в сети передачи данных общего пользования, что, например, для реализации «умных электросетей» просто необходимо.

Технология передачи данных в автоматизированных интеллектуальных системах, как правило, строится на основе выделенных проводных линий связи либо является беспроводной по технологии Wi-Fi. Конкурентом таких традиционных сетей в последнее время выступает менее известная технология PLC (Power Line Communications), использующая для передачи данных линии сетей электропитания. Развитием данной технологии и ее продвижением на рынок занимается группа компаний, объединенных в альянс под названием HomePlug Powerline Alliance [1].

У каждой из этих технологий передачи данных есть свои сильные и слабые стороны, поэтому задача их выявления и сравнительной оценки достаточно интересна. Наиболее отработанной и распространенной является технология выделенных линий связи, достаточно медленно, но верно оттесняемая мобильными беспроводными технологиями. Так, в случае реализации концепции интеллектуальных систем в зданиях старой постройки преимущества выделенных линий совсем неочевидны по сравнению с бурно развивающимися сетями Wi-Fi и PLC.

Целью настоящей работы явились тестирование технических средств относительно новой и имеющей свои специфичные слабые места PLC-технологии, в том числе в аспекте обеспечения безопасности передачи данных, и сравнительный анализ полученных результатов безопасности с более распространенной Wi-Fi-технологией.

Тестирование проводилось на образцовой сети, схема экспериментального стенда которой приведена на рисунке 1. Экспериментальный стенд состоял из трех компьютеров, объединенных в локальную сеть при помощи PLC-модемов, соответствующих спецификации Homeplug AV [1]. Программное и аппаратное обеспечение компьютеров специально выбрано различным, чтобы подчеркнуть возможность гетерогенности пользовательской среды, независимой от программной платформы и производителя аппаратуры.

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.

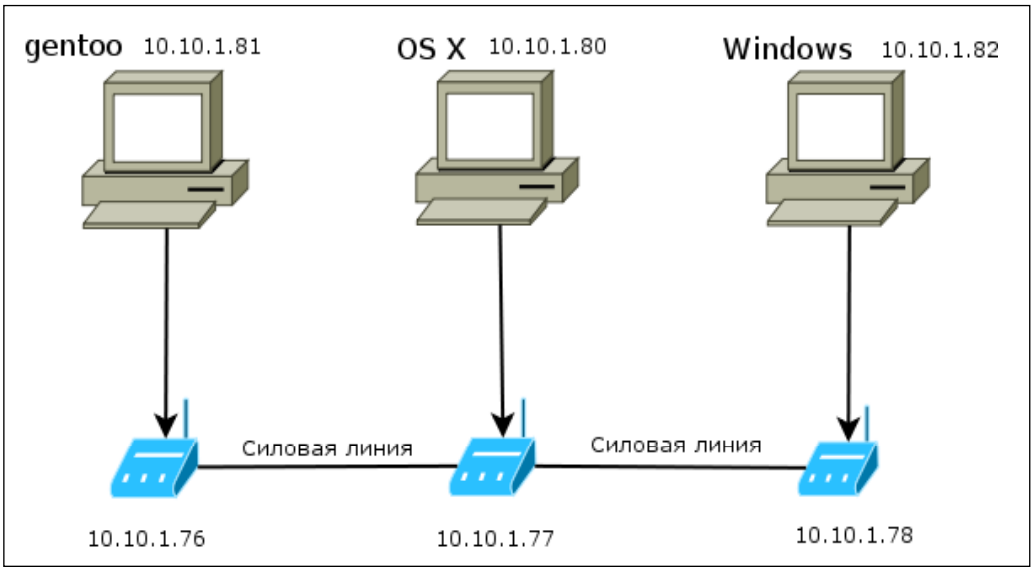

Рис. 1. Экспериментальный стенд по тестированию PLC-технологии

На рисунке 1 для простоты ссылок компьютерам присвоены символьные имена, которые также совпадают с операционной системой, установленной на конкретном компьютере:

1) ПЭВМ под управлением операционной системы gentoo, настроенная на IP-адрес 10.10.1.81;

2) ноутбук Macbook air под управлением mac OS X Snow leopard, настроенный на IP-адрес 10.10.1.80;

3) ноутбук asus-w7j под управлением Windows XP, настроенный на IP-адрес 10.10.1.82.

Все компьютеры соединены PLC-модемами TL-200 WM производства компании TelLink в единую сеть по линиям электропроводки.

Для установления соединения между описанными выше компьютерами потребовались лишь обычные навыки конфигурации компьютеров, что говорит об относительной легкости настройки средств PLC-технологии.

Одной из первых задач тестирования являлось определение скорости передачи данных между узлами сети при выборе протокола передачи FTP. В результате средняя скорость передачи данных оказалась равной 11,1 Мб/с.

Следующим экспериментом было измерение среднего значения времени оборота пакета (RTT, от англ. Round Trip Time), что позволяет нам определить двусторонние задержки. Этот показатель имеет ключевое значение для некоторого вида приложений, чувствительных к временным задержкам, например IP-телефония, аудио- и видеочаты, современные веб-приложения. При тестировании производилось по 10 замеров времени отклика между каждой парой компьютеров. Полученные результаты показаны на рисунке 2. Среднее арифметическое от полученных результатов принято как приблизительное время отклика, равное 3,7 мс.

Затем определялся уровень искаженных пакетов, т. е. отношение количества успешно переданных пакетов в сети к количеству искаженных пакетов. Для этого использовалась утилита ping, у которой есть режим бесперебойной отсылки, так называемый Flood mode. Он активируется добавлением параметра «-f» в командной строке. В этом режиме утилита ping начинает генерировать и отсылать в сеть запросы ICMP Echo-Request с максимально возможной плотностью, с ожиданием от цели ответа на каждый посланный пакет. В случае если ответа нет, пакет считается утерянным. Таким образом, можно выявить устойчивость к искажению и потере пакетов. В итоге был получен результат отсылки 50 000 пакетов, из которых 12 пакетов было утеряно. Это свидетельствует о потенциальной надежности PLC-технологии.

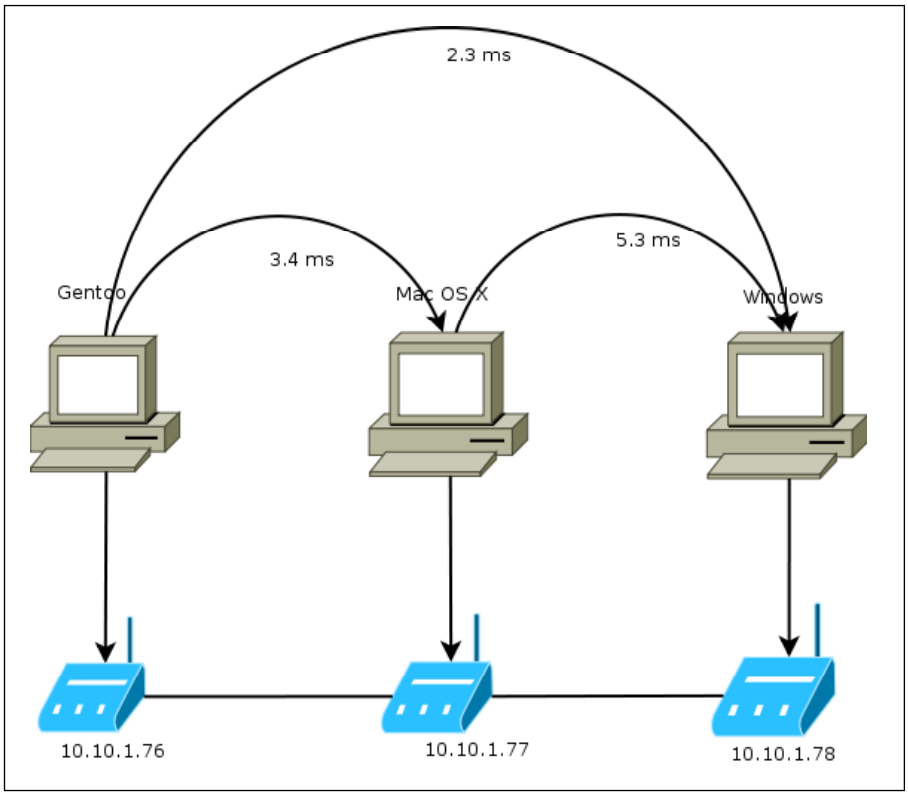

Рис. 2. Результаты среднего значения времени оборота пакета

Однако очевидной слабостью таких открытых и малоуправляемых сред, как силовые сети, является возможность проведения атак с нарушением всех характеристик безопасности информации, передаваемой по этим линиям связи. Последствия таких атак могут быть разнообразными: от утечки персональных данных до полного отключения систем управления зданием, в том числе отключения сигнализации, открытия дверей и т. д.

Серьезной уязвимостью передачи данных по силовым линиям является утечка информации по техническим каналам за счет ПЭМИН. Для ее тестирования была использована измерительная дипольная активная антенна АИ5-0, соединенная с анализатором спектра IFR 2394A, визуализирующим уровень напряжения в зависимости от частоты и передающим измеренные данные на компьютер. Расчеты и генерация отчета происходили с помощью программного комплекса СИГУРД.

В начале эксперимента проводился съем излучения от PLC-модема в обычном рабочем состоянии сети электропитания, т. е. без передачи данных. В этом случае анализатор спектра показал естественный сигнал в виде белого шума. Затем был запущен на передачу файл большого размера около 2,5 Гб, после чего измеряемое излучение сильно изменило свою форму, из которой с помощью специальных исследований можно выделить информативный сигнал.

Для предотвращения такой угрозы перехвата данных, циркулирующих в сетях электропитания, принятые стандарты и процедуры спецификации HomePlug AV [1] применения PLC-технологии предусматривают криптостойкий механизм 128-битного AES-шифрования, т. е. проблема конфиденциальности данных в определенной мере отпадает.

Проблема целостности, или защиты от НСД, в спецификации HomePlug AV также решается известными процедурами контроля доступа, что было подтверждено экспериментально. Пакеты, не предназначенные злоумышленнику, не поддаются съему программными методами, и соответственно нет возможности модификации данных.

Для тестирования характеристики доступности данных было решено провести DOS-атаку как на физическом, так и на логическом уровнях.

Суть атаки на физическом уровне заключалась в глушении сигнала в линии электропитания, для чего использован генератор шума в диапазоне частот от 0,1 до 300 МГц, в который входит диапазон, используемый PLC-технологией передачи данных. В результате тестирования полностью заглушить канал не удалось, однако скорость передачи данных упала в 2 раза, что является демонстрацией существенности этой угрозы.

DOS-атака на логическом уровне — это известная сетевая атака, в частности, в данном исследовании была проведена попытка нарушить сервис, предоставляемый PLC-модемом для удаленного конфигурирования. Этот сервис представляет собой html-страничку, открывающуюся по IP-адресу модема, которая в момент проведения атаки стала менее доступна.

Основные результаты тестирования в сравнении с Wi-Fi-технологией приведены в таблице 1.

Таблица 1. Сравнение параметров технологий Wi-Fi и PLC

Показатели	Wi-Fi	PLC
Средняя скорость передачи данных	1,4 Мбайт/сек	11,1 Мбайт/сек
Уровень настройки ЛВС	Сложно	Легко
Среднее значение времени оборота пакета	48 мс	4 мс
Уровень искаженных пакетов (на 50 000 пакетов)	31	12
Утечка информации по техническим каналам за счет ПЭМИН	Возможна	Возможна
Неавторизованное подключение к ЛВС	Возможно	Невозможно
Шифрование данных	AES 128-битным ключом	AES 128-битным ключом
Глушение канала связи	Возможно	Возможно
Реализация сетевой DoS-атаки	Успешно	Успешно

Заключение

Целью работы было тестирование малоизвестной PLC-технологии передачи данных и ее сравнение с конкурирующей сетевой технологией Wi-Fi. Очевидно, что по параметру мобильности Wi-Fi-технология не имеет себе равных. Но, с другой стороны, и сети, построенные на основе PLC-технологии, в должной степени обеспечивают необходимые характеристики систем передачи данных, в том числе в аспекте обеспечения безопасности информации, а по экономическим соображениям могут оказаться и предпочтительными, в частности, в системах «умного здания».

СПИСОК ЛИТЕРАТУРЫ:

1. http://www.homeplug.org.

2. *Хорев А. А.* Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1: Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. — 436 с.: илл.