

контроллера можно использовать путем добавления нужного модуля.

Поскольку ОС реального времени работает в специализированных устройствах, технические возможности которых ограничены в рамках решаемой задачи, следовательно, на ОС накладывается ряд ограничений, основные из которых – малый объем кода и необходимое быстродействие.

Операционная система реального времени должна обеспечивать следующие функции: функция управления памятью (доступ к памяти по средствам команд ОС); функция управления процессами (поскольку ОС реального времени многозадачные); функция управления периферийными устройствами (УВВ, ус-ва хранения и т.д.); функция поддержки коммуникационных протоколов (USB, Bluetooth и т.д.); функция поддержки протокола интернета.

В настоящее время спектр имеющихся операционных систем чрезвычайно широк. Условно все операционные системы можно разделить на три категории по заложенным в них возможностям:

– системы, обеспечивающие только управление памятью и задачами; подобные операционные системы присутствуют в том или ином виде практически в каждом устройстве и имеют очень малый объем (порядка двух-трех сотен строк кода); часто такая операционная система пишется индивидуально для каждого проекта (при этом она может и не выделяться из программного обеспечения в операционную систему как таковую); как правило, подобные операционные системы используются при создании относительно простых устройств;

– системы, имеющие жестко заложенные в них средства взаимодействия с внешним миром; подобные системы, как и предыдущие, разрабатываются для обеспечения надобностей конкретного проекта; такой подход позволяет минимизировать объем кода и добиться максимальной производительности в ущерб универсальности использования;

– системы, имеющие четко выраженную модульность; подобные операционные системы чаще всего имеют ядро, которое обеспечивает управление памятью и процессами, а также взаимодействие процессов между собой; кроме того, имеется набор драйверов для поддержки различных периферийных устройств, коммуникационных протоколов и т. п.; этот тип операционных систем является наиболее универсальным, причем, как правило, имеется несколько реализаций для различных аппаратных платформ.

Существует большое количество ОС реального времени, и все они выполняют одну задачу – управление функционированием системы. При выборе ОС необходимо учитывать все перечисленные выше особенности. Естественно, первоначально нужно выбирать ОС реального времени, которая сможет обеспечить требуемые для устройства характеристики (время отклика, наличие необходимых протоколов связи и т.д.), но поскольку ОС реального времени призвана упрощать и ускорять процесс проектирования, особое внимание следует уделить наличию средств (среды) разработки и службе поддержке. Ниже приведена таблица с характеристиками некоторых ОС реального времени.

Название ОС реального времени	Разработчик	Поддерживаемые процессоры	Требования к памяти		Поддерживаемые компиляторы и отладчики
			Объем ПЗУ, кбайт	Объем ОЗУ, кбайт	
Windows CE	Microsoft	ARM, MIPS, PowerPC, SH, x86, StrongARM	32	8	
QNX	QNX Software Systems	MIPS, PowerPC, x86 Protected Mode, x86 Real Mode	32	8	GNU GCC C/C++, Watcom C/C++
OnTime RTOS	On Time Software	x86 Protected Mode	8	8	Microsoft, Watcom, Borland
Nucleus PLUS	Accelerated Technology Inc.	6800, 68HC11, 68HC16, 68K, ARM, C16x, ColdFire, H8, MIPS, MPC8xx, PowerPC, SH, SPARC, TI DSPs, V800, x86, M-Core, C16A/B, CR32,...	3	2	GNU, ARM, Metaware, Microsoft, Borland, Watcom, IAR, Hitachi, Tasking, TI,...
e/BSD	Berkley Software Design	SPARC, Intel 386, 486, Pentium	2000	2000	
CMX-RTX	CMX Co.	68HC0/08/11/12/16, 68K, 78K, 80196, x51, ARM, C16x, ColdFire, H8, MELPS 7700, MPC8xx, PIC, PowerPC, SH, TI DSPs, x86, AVR, ST,...	1000	0,2	CMX-RTX CMX Co. CMX CMXBug, CMXTracker
RTX	Keil Software	80251, 8051, and derivatives, C166	8	11	dScope
OS-9	Microware Systems Corp.	68K, StrongARM, PowerPC, SH, x86 Protected Mode	128	128	UCC+GCC

Список литературы

1. Сулейманова А.М. Системы реального времени: учебное пособие. – Уфа: Уфимск. гос. авиац. техн. ун-т, 2004. – 292 с.
2. Переводчик: Ю. Асотов. Операционная система реального времени QNX Neutrino 6.3. Системная архитектура. – БХВ-Петербург, 2006.
3. В. Г. Олифер, Н. А. Олифер Сетевые операционные системы. – СПб.: Питер, 2001.
4. <http://www.swd.ru>.
5. <http://citforum.ru>.

КВАНТОВАЯ КРИПТОГРАФИЯ

Востоков Н., Борисова С.Н.

Пензенская государственная технологическая академия,
Пенза, e-mail: los@pgta.ru

Криптографические методы издавна и до сегодняшнего дня считаются надежным способом защиты

информации при передаче по незащищенным каналам связи. В последнее время исследуется новое направление в криптографии – квантовая криптография. *Квантовая криптография* – метод защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике информации, так как рассматривает случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приема информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание

может рассматриваться, как измерение определенных параметров физических объектов — в нашем случае, переносчиков информации. Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы — невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой. Это фундаментальное свойство

природы в физике известно как принцип неопределенности Гейзенберга, сформулированный в 1927 г.

На рис. 1 представлен случай перехвата и искажения передаваемой информации (абонент А и абонент Б обмениваются секретной информацией), когда они пытаются сохранить тайну шифровального ключа, передавая его в виде поляризованных фотонов по изображенной схеме:

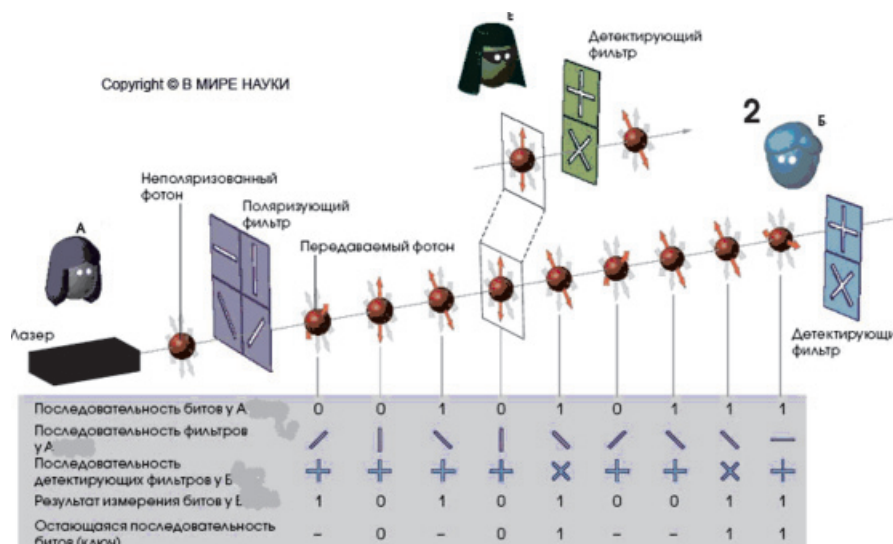


Рис. 1. Передача и перехват ключа шифрования

1. Для создания ключа абонент А посылает фотоны через прямой или диагональный полярирующий фильтр и записывает направление плоскости поляризации.

2. Для каждого поступающего бита абонент Б случайным образом выбирает фильтр для обнаружения и записывает поляризацию и значение бита.

3. Когда злоумышленник Е пробует отследить последовательность фотонов, принципы квантовой механики не позволяют ему использовать оба типа фильтров для выяснения направления поляризации одного фотона. Если Е выбирает неправильный

фильтр, то возникают ошибки, обусловленные изменением поляризации.

4. Получив все фотоны, абонент Б по открытому каналу сообщает абоненту А последовательность фильтров, которые он использовал для поступающих фотонов. О считанных значениях битов он ничего не сообщает.

Абонент А говорит абоненту Б, какие фильтры он выбрал правильно (рис. 2). Измеренные с их помощью биты будут использоваться при формировании ключа для шифрования сообщения.

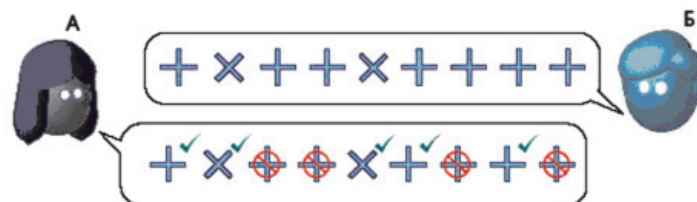


Рис. 2. Указание корректно выбранных поляризационных фильтров

Используя квантовые явления, можно спроектировать и создать такую систему связи, которая всегда может обнаруживать подслушивание. Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в нее нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

Первый протокол квантовой криптографии (BB84) был предложен и опубликован в 1984 году Беннетом и Брассардом и состоял в следующем:

1. Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.

2. Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).

3. Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга о полученных результатах. Последний бит каждого блока удаляется.

4. Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.

5. Чтобы исключить кратные ошибки, которые могут быть не замечены, операции пунктов 1-4 повторяются для большего значения k .

6. Для того чтобы определить, остались ли не обнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки:

7. Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.

8. Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.

9. Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.

10. Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2- m .

В настоящее время уже несколько фирм (например, компании id Quantique, Magic Technologies) предлагают первые коммерческие системы квантового распределения ключей. Эти системы имеют сходные характеристики: использование оптоволокна в качестве среды передачи, максимальная дальность связи в несколько десятков километров и невысокая скорость выработки ключа (порядка единиц килобит в секунду). Очевидно, что по массовости применения системы квантовой коммуникации еще очень не скоро смогут приблизиться к асимметричной криптографии, однако уже сейчас системы квантовой коммуникации могут найти применение для защиты особо важных каналов связи.

Список литературы

1. Магнитные молекулы и квантовая механика // http://vivovoco.rsl.ru/VV/JOURNAL/NATURE/12_00/MAGNET.HTM.

2. Quantum computing using shortcuts through higher dimensions // http://arxiv.org/PS_cache/arxiv/pdf/0804/0804.0272v1.pdf.

ОРГАНИЗАЦИЯ БЕСПРОВОДНОЙ СЕТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Гнусин П.В., Гнусина Э.В., Бершадская Е.Г.

Пензенская государственная технологическая академия,
Пенза, e-mail: los@pgta.ru

Современное промышленное предприятие – это множество взаимодействующих процессов и производств, цеха, административные здания, а зачастую и удаленные участки. Вопросом первостепенной важности является управление и контроль множества параметров. Для оперативного управления производственными процессами необходима автоматизация. А для работы систем управления необходима надежная инфраструктура.

Промышленное предприятие осуществляет сбор информации с механизмов специальными датчиками. Далее всю эту информацию нужно отправить в заводоуправление для обработки, анализа и принятия решений. Как и на любом промышленном предприятии, кабельные линии связи могут быть повреждены или выйти из строя из-за неблагоприятных условий, а в отдельных случаях их прокладка вообще невозможна. Беспроводные технологии свободны от этих недостатков и могут быть применены для решения задач организации каналов связи, попутно решая и другие задачи.

Беспроводная передача данных в настоящее время переживает своеобразный бум. А на фоне активного развития сетей супермаркетов, крупных медицинских центров, производственных объединений, где на части предприятий отсутствуют разветвленные кабельные инфраструктуры, организации различных временных инсталляций – вроде сетей на промышленных выставках и семинарах, использование беспроводной передачи данных становится наиболее актуальным.

В России беспроводные сети часто оказываются единственным средством организации корпоративных сетей или обеспечения доступа в Internet. Довольно большую область беспроводной передачи данных можно разделить на три подобласти: *мобильная связь, передача данных внутри зданий и между*

зданиями. Эта классификация достаточно условна, однако, она отражает основные виды задач, решаемых средствами беспроводной связи. Технические решения, применяемые в этих областях, значительно отличаются друг от друга.

Мобильные системы передачи данных распространены на Западе очень широко, и, в первую очередь, к ним относятся сотовые сети с коммутацией пакетов (Cellular Digital Packet Data, CDPD) и коммутацией каналов. Все они обеспечивают передачу данных на довольно низких скоростях (как правило, не выше 19,2 кбит/с) и рассчитаны в основном на индивидуальных пользователей.

В России же, наоборот, беспроводные технологии передачи данных используются преимущественно вне зданий. И главным образом, они нужны для организации информационного обмена на сравнительно большом расстоянии. Объясняется это, во-первых, отсутствием разветвленной кабельной инфраструктуры; а во-вторых, низкой плотностью населения и частым отсутствием вообще какой-либо инфраструктуры.

В ряде крупных городов России уже развернуты опорные сети с беспроводным доступом. Они, во-первых, расширяют возможности использования крупных информационных ресурсов и Internet, а во-вторых, позволяют организовывать корпоративные сети примерно так же, как это делается с помощью кабельных сетей. В тех городах (а таких пока большинство), где нет городских опорных сетей, организация может создать свою собственную беспроводную сеть, объединив радиомостом две удаленные друг от друга локальные сети.

Одним из перспективных направлений является беспроводной стандарт Wi-MAX, позволяющий развернуть беспроводную сеть на территории города. Эта технология беспроводной связи следующего поколения, где заявлена хорошая дальность, хорошие скорости, хорошие сервисные возможности. Wi-MAX позволяет осуществлять доступ в Интернет на высоких скоростях, с гораздо большим покрытием, чем у Wi-Fi-сетей. Это дает возможность использовать технологию в качестве «магистральных каналов», продолжением которых выступают традиционные DSL и выделенные линии, а также локальные сети. Название стандартов, на которых основаны эти технологии, похоже (стандарты разработаны IEEE, оба начинаются с «802.»), а также обе технологии используют беспроводное соединение и используются для подключения к интернету (каналу обмена данными). Но, несмотря на это, эти технологии направлены на решение совершенно различных задач. Реализация технологии беспроводной передачи данных показана на рисунке.

Wi-MAX – это система дальнего действия, покрывающая километры пространства, которая обычно использует лицензированные спектры частот для предоставления соединения с интернетом типа «точка-точка» провайдером конечному пользователю.

Разные стандарты семейства 802.16 обеспечивают разные виды доступа, от мобильного (схож с передачей данных с мобильных телефонов) до фиксированного (альтернатива проводному доступу, при котором беспроводное оборудование пользователя привязано к местоположению). В специальной литературе приведены сравнительные таблицы стандартов беспроводной связи.

Wi-Fi – это система более короткого действия, обычно работающая на десятки метров, которая использует нелицензированные диапазоны частот для обеспечения доступа к сети. Обычно Wi-Fi используется пользователями для доступа к их собственной