$$Î ÑØ = 10\lg\left(\frac{A^2/2}{q^2/12}\right) = 7,78 + 20\lg\left(A/q\right), \qquad (4)$$

де А – максимальна амплітуда синусоїдального сигналу.

Висновки

При вимірюванні потужності шуму квантування спектральні складові часто зважуються таким же чином, як і шуми в аналогових сигналах, але спектрально зважені вимірювання не завжди відображають дійсний рівень якості в мовному кодері/декодері. Якщо спектральний розподіл шуму квантування більш менш повторює спектр мовного сигналу, то шум екранується мовою і помітний в набагато меншому ступені, чим некорельований шум. З іншого боку, якщо в процесі квантування основна потужність доводиться на частоті мовної смуги, відмінної від частот окремих звуків, то шум помітніший.

У високоякісних ІКМ-кодерах шум квантування рівномірно розподілений в мовній смузі частот і не залежить від кодованих сигналів. Таким чином, ОСШ квантування, яке визначається виразом (4), добре відображає характеристики ІКМ-системи.

Література

1. J. Flanagan. M. Schroeder, B. Atal, R. Crochicre, N. Jayanl, and J. Tribolet. «Speech Coding», IEEE Transactions on Communications, Apr. 1979
2. Величкин А.И. Передача аналоговых сообщений по цифровым каналам. М.: Радио и связь, 1983. 240с.
3. Советов Б.Я. Информационная технология: Учеб. для вузов по спец. "Автоматизиров. системы обработки информ. и упр." - М.:Высш. шк., 1994
4. Клюев Л.Л. “Теория электрической связи». Минск, «Дизайн ПРО»,1998 г
5. Шувалов Б.П., Захарченко Н.Б., Шварцман В.О. и др ”Передача дискретных сообщений” Под ред. Шувалова -М.; Радио и связь 1990 г.

Статтю подано 9.10.2009

УДК 004.738.5

Гура В.И., Скопа А.А., Сыропятов А.А.

ПРЕДЛОЖЕНИЯ ПО МОДЕРНИЗАЦИИ СТАНДАРТА IEEE 802.11 С ЦЕЛЬЮ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Рассматривается проблема угроз информационной безопасности в беспроводных системах связи. Предлагается новый подход обеспечения защиты информации с применением стеганографических алгоритмов.

Постановка проблемы. Объектом исследований является система беспроводной передачи информации, являющиеся неотъемлемой составной частью современных телекоммуникационных комплексов. Использование беспроводных систем связи (БСС) исключает расходы на прокладку кабелей, связанные с этим неудобства, расширяет мобильность всей компьютеризированной системы связи.

Связь проблемы с важными научными и практическими заданиями. Одной из ключевых задач является обеспечение требуемого уровня безопасности информации с учетом среды передачи, особенно для ведомственных систем связи и систем двойного назначения. При работе локальных беспроводных сетей (БЛС) используются выделенные радиочастоты и покрывается расстоянии до 250-300 метров на открытом пространстве. Осущест-

вить перехват информации в радиоэфире значительно проще, чем в проводных и кабельных сетях. Меры защиты наиболее распространенного на практике оборудования беспроводных систем на основе стандарта IEEE 802.11 обеспечиваются применением специального протокола зашиты WEP (Wired Equivalent Privacy).

Анализ последних исследований и публикаций, в которых положено начало решения проблемы. Известны подходы разработки авторизированных систем защиты частных виртуальных систем (VPN) на основе семейства протоколов IPSec в сочетании с другими средствами и методами комплексного обеспечения безопасности. При этом выявлена необходимость на этапе проектирования учитывать неизбежность интеграции беспроводных систем связи в систему связи, содержащую средства проводной и кабельной коммуникации [1].

Раньше нерешенной частью общей проблемы. Основной проблемой обеспечения безопасности использования беспроводных сетей в современных телекоммуникационных системах является отсутствие системного подхода [2].

Постановкой задания для последующего решения является задача модернизации стандарта IEEE 802.11 производителями аппаратуры для БЛС, которая зачастую приводит к несовместимости оборудования различных фирм.

Перейдем к изложению **основного материала.** На практике традиционным при решении проблемы зашиты передаваемой по радиоканалу информации является решение следующего комплекса задач [3]:

- уменьшение зоны покрытия до предела контролируемой территории;
- применение протокола защиты WEP;
- усовершенствование системы генерации, хранения, передачи ключей протокола WEP;
- установка персональных межсетевых экранов, антивирусных программ;
- осуществление фильтрации по MAC-адресам, программно-аппаратную фильтрацию трафика;
- усовершенствование системы идентификации и аутентификации администраторов и пользователей;
- резервирование оборудования.

При распределении функций между иерархическими составляющими телекоммуникационной системы необходимо находить компромисс между сложностью и эффективностью реализации. Конкретизация системы обеспечения информационной безопасности беспроводных сетей возможна после определения особенностей практического использования, т.е. анализа потенциальных угроз, оценки рисков. Специфика беспроводных систем позволяет выявить наиболее типичные угрозы информационной безопасности.

Стандарт IEEE 802.11 предусматривает три средства защиты беспроводных сетей: контроль доступа по имени сети (ESSID); контроль доступа по MAC-адресам. На точке доступа задается список MAC-адресов, которым разрешена или запрещена авторизация; шифрование трафика по протоколу WEP. Шифрование использует алгоритм RC4 с длиной ключа 64 и 128 бит. Уязвимость протокола защиты WEP изначально обуславливает наличие слабых моментов системы обеспечения безопасности ЛВС. Более совершенный стандарт IEEE 802.1x используется при аутентификации и авторизации пользователей с последующим предоставлением доступа к среде передачи данных. При этом применяются динамические ключи вместо статических, используемых в стандарте IEEE 802.11. Отличительной чертой является совмещение протоколов EAP (Extensive Authentication Protocol) и RADIUS (Remote Access Dial-In User Server). Прежде чем получить доступ к сети, клиент должен пройти проверку на сервере RADIUS, пройти аутентификацию в соответствии с EAP и только в случае успешной аутентификации, разрешается досуп в сеть. Таким образом, передача данных становится возможной только после взаимного подтверждения подлинности участников сеанса. Дополнительное повышение надежности проведения процедуры аутентификации возможно, например, посредством использования цифровых сертификатов, про-

граммно закрытого канала для передачи цифровых сертификатов, усовершенствованием алгоритма распределения ключей при аутентификации и организации программно закрытого канала передачи

К следующему поколению стандартов по обеспечению информационной безопасности БЛС можно отнести стандарт WPA (Wi-Fi Protected Access). Протокол WPA реализует преимущества шифрования при помощи протокола целостности временных ключей (Temporal Key Integrity Protocol – TKIP). Аутентификация пользователей производится при помощи 802.1x и EAP. WPA предусматривает совместимость с будущим протоколом безопасности беспроводных сетей 802.11i. Отличительные особенности технологии WPA:

- усовершенствованная схема шифрования данных RC4 на основе TKIP протокола краткосрочной целостности ключей;
- улучшенные механизмы контроля доступа – обязательная аутентификация 802.1x посредством протокола EAP;
- реализация модели централизованного управления безопасностью и возможность интеграции с действующими схемами корпоративной аутентификации;
- возможность облегчения установки для домашних пользователей, которые могут применить специальный режим, автоматизирующий функции настройки безопасности WPA.

Стремительная динамика развития стандартов обеспечения безопасности БЛС очевидна. IEEE 802.11i – это недавно принятый стандарт безопасности, основой которого является криптографический стандарт AES (Advanced Encryption Standard). Иногда стандарт 802.11i называют WPA2. В настоящее время на практике используется стандарт 802.11b. Этот стандарт предусматривает передачу данных в диапазоне 2,4 ГГц со скоростью до 11 Мбит/с. При этом для организации доступа мобильных пользователей к цифровым сетям применяются комбинированные решения: одна часть сети строится на кабельной основе, а в другой ее части задействуется беспроводная связь. Стандарт 802.11g характеризуется более высокой пропускной способностью. В перспективе – стандарт 802.11a, работающий в диапазоне 5 ГГц.

Необходимо отметить, что при разработке стандартов, прежде всего, ставиться цель предотвратить атаку в процессе ее совершения. Наиболее распространенные атаки для рассматриваемых систем: расширение прав доступа; искажение информации или нарушение ее целостности; раскрытие информации или несанкционированное распространение среди лиц без права доступа. С другой стороны все атаки состоят из трех этапов: сбор информации, осуществление атаки, уничтожение последствий атаки. Как правило, традиционные средства защиты ориентированы на противодействие второму этапу атаки. В то время, как именно защита на первом этапе в большей степени позволила бы предотвратить ее проведение. Соответствующие меры на третьем этапе позволили бы привлечь злоумышленника к ответственности.

Таким образом, при реальной оценке угроз, правильном выборе технологий и оборудования защита БЛС весьма реальна. Однако оценка угроз должна быть динамичной. Описанные выше меры позволят установить минимальный уровень безопасности в беспроводной сети, т.е. ориентированный на фиксированную оценку угроз.

Суть предлагаемого подхода: если мы не можем построить защищенную с учетом изменения уровня угроз корпоративную систему связи, включающую в свой состав беспроводные сети и вычислительную технику, то необходимо изменить саму концепцию организации защиты: отказаться от методики усложнения возможности совершения несанкционированных действий, а на основании организации соответствующего мониторинга обнаруживать и персонифицировать сам факт совершения несанкционированных действий. Такой подход потребует совместной реализации правовых, организационных, технических мер по привлечению нарушителя к ответственности. Одним из вариантов реализации такого подхода является использование стеганографических технологий цифровых водяных знаков (ЦВЗ) для комплексной защиты беспроводных сетей позволяет решить следующие задачи:

– мониторинг трафика информации;
– исключение активных атак (несанкционированное использование передаваемого информационного объекта).

Для осуществления мониторинга каждому из клиентов присваивается персональный идентификатор, погружение и детектирование которого осуществляется с помощью специальных кодера и декодера ЦВЗ, при разработке которых необходимо обеспечивать стойкость к архивированию информационных потоков. Такой мониторинг позволит автоматически фиксировать и извлекать из архивов данные по сеансам связи. Свойства технологий ЦВЗ, а именно: сохранение размера информации, неотделимость ЦВЗ от первичной информации и невозможность устранения или изменения ЦВЗ без изменения надежности восприятия основного объекта, являются основой защиты от активных атак.

Выводы. При наличии соответствующей законодательной базы воспользоваться объектом, несущим информацию о несанкционированных действиях, не представляется возможным. Кроме того, погружение ЦВЗ в программные модули протоколов защиты на основе логической избыточности тоже позволит контролировать их целостность, упростить сложность процедуры, а значит повысить пропускную способность канала.

Т.о. основными положениями, **перспективными для последующего исследования**, являются серьезные моменты практической ценности такого подхода организации информационной безопасности и разработка соответствующей нормативно-правовой базы.

Литература

1. Маракова И.И., Скопа А.А., Сыропятов А.А. Защита информации в беспроводных системах связи // Матер. IV наук.-техн. конф. «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні», 1-3 березня 2006 р., К.: НТУУ «КПІ», 2006. – С. 86-92.
2. Корчинський В.В., Гура В.І. Аналіз функціонування інфомережі, побудованої на основі теорії марківських ланцюгів // Комп'ютерні технології, інформаційна безпека та дизайн: Матеріали IV наук.-практ. конф. проф.-викл. складу та студентства Міжнародного гуманітарного ун-ту (секції 7...13), 22 травня 2009 р. – Одеса: МГУ, 2009. – С.39-42.
3. Гура В.І. Перспективи використання бездротових комунікаційних технологій стандарту IEEE 802.11 в агропромисловому комплексі України / Вісник Львівськ. націон. аграрн. ун-ту: Агроінженерні дослідження. – Львів: Львівськ. нац. агроун-т, 2009. – (в друці).

Статтю подано 10.10.2009