ОПТИМИЗАЦИЯ ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛА СВЯЗИ ДЛЯ ЗАЩИЩЕННЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кутья А.С.

Дубровский Василий Викторович – к.т.н, доцент

В настоящей работа рассматриваются алгоритмы защиты информации в каналах передачи данных и способы оптимизации пропуснкой способности канала связи.

Деятельность людей всегда связана с передачей информации. Передача информации – физический процесс, посредством которого осуществляется перемещение информации в пространстве.

Для эффективного использвоания канала связи применяется оптимизация его пропускной способности, достигаемая путем оптимальной обработки сигналов.

В состав рассматриваемых систем передачи входят различные радиотехнические системы передачи информации (сообщений), назначением которых является передача информации на расстояния посредством электромагнитных колебаний.

Общедоступность каналов связи в современных сетях передачи данных делает их наиболее удобными и легко масштабируемыми среди прочих предоставляемых услуг. Однако этот факт обуславливает повышенные требования к обеспечению безопасности данных систем. Защита каналов связи от несанкционированного воздействия в таких сетях осуществляется с помощью использования метода шифрования или криптографии. Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст – ciphertext) или зашифрованных данных – в открытые по определенным правилам с применением определенных правил, содержащихся в ключах (шифре).

Под шифром в криптографии понимается совокупность обратимых преобразований множества возможных открытых данных во множество возможных зашифрованных данных, расшифровать и понять которые нелегальный пользователь (злоумышленник) не в силах. Эти преобразования осуществляются по определенному алгоритму с применением ключа – конкретного секретного состояния некоторых параметров криптоалгоритма, обеспечивающего выбор одного преобразования из всей совокупности вариантов, возможных для данного алгоритма.

Стандартно передача информации по защищенным каналам осуществляется следующим образом [1]. Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу. Для того чтобы злоумышленник не смог узнать содержание сообщения M, отправитель зашифровывает его по ключу K с помощью обратимого преобразования EK и создает шифртекст (или криптограмму) $C = E_K(M)$, который отправляет получателю. Законный получатель, приняв шифртекст C, расшифровывает его с помощью обратного преобразования $D_K(C) = E_{K^{-1}}(C)$ и получает исходное сообщение в виде открытого текста M: $D_K(C) = E_{K^{-1}}[E_K(M)]$. Данная система шифрования называется симметричной, поскольку шифрование и расшифровка производятся с помощью одного и того же ключа K. При этом необходимо обеспечение конфиденциальности этого ключа. Схема криптографической системы, обеспечивающей шифрование передаваемой информации, представлена на рисунке 1.

При этом различают два типа алгоритмов шифрования: симметричные (с секретным ключом) и асимметричные (с открытым ключом). В первом случае обычно ключ расшифровки совпадает с ключом шифрования, либо знание ключа шифрования позволяет легко вычислить ключ расшифровки. В асимметричных алгоритмах такая возможность отсутствует: для шифрования и расшифровки используются разные ключи, причем знание одного из них не дает практической возможности определить другой.

В современных телекоммуникационных системах, использующих в составе каналов связи открытые среды передачи данных, помимо стойкости дополнительно выдвигаются требования по оперативности и непрерывности доступа к информационному ресурсу. По причине больших объемов передаваемой информации использование долгосрочных ключевых данных создает угрозу успешного осуществления статистических атак, а по причине отсутствия реализации механизмов безопасной передачи ключевой информации по открытым каналам связи появилось семейство протоколов RSNA.

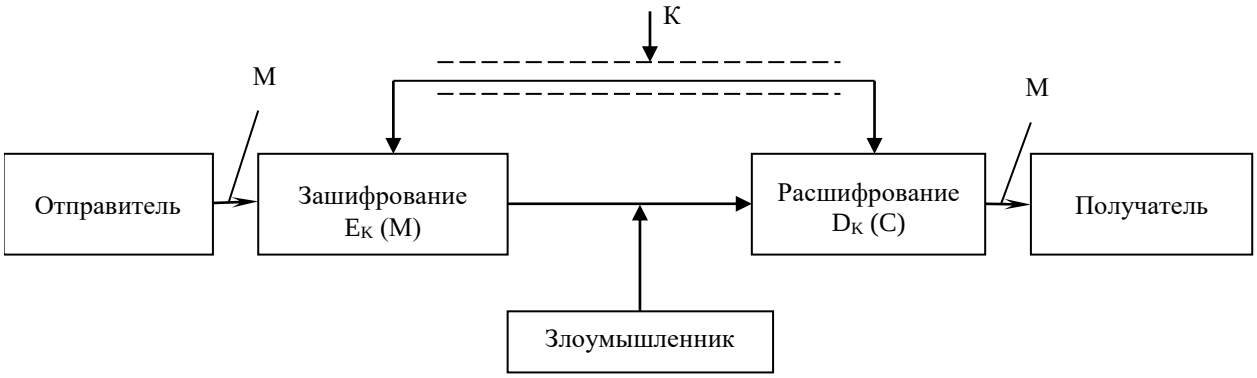

Рисунок 1 – Структурная схема радиоканала цифровой системы связи

В стандартах [2] предложено усиление безопасности сети по сравнению с протоколами семейства pre-RSNA, заключающееся в использовании инкапсуляции CCMP с применением алгоритмов шифрования, обладающей большей стойкостью к различным видам атак, а также динамической схемы формирования ключевого материала, согласно предложенной иерархии ключей. При этом предусмотрено использование ключей формирования имитовставки, шифрования данных и шифрования ключа шифрования данных. Аутентификация в данной модификации стандарта может выполняться на основе заранее распределенного ключа, или по протоколу EAPOL, но оба протокола аутентификации используют модель запрос – ответ.

По завершении протокола EAPOL между корреспондентами распределяется секретный мастер – ключ MSK (либо используется заранее установленный при аутентификации PSK), на основе которого, путем добавления случайных компонент и вычисления хеш-функций различного типа, вырабатываются ключи удостоверения подлинности (КСК), ключ шифрования трафика (ТК), ключ шифрования ключа (КЕК).

Стандартом предусмотрена выработка парных ключей для безопасной передачи данных в режиме туннелирования STSL (station-to-station link) в которой передаваемые данные от одного корреспондента к другому проходят через некоторый промежуточный узел связи. При данной топологии сети необходимо установление ассоциации безопасности STKSA, для чего узел в свою очередь должен установить RSNA с обоими корреспондентами. Узел связи является посредником между двумя своими абонентами и выполняет функции центра распределения ключей. Необходимо чтобы между узлом и каждым корреспондентом был установлен общий парный ключ PTK (КЕК, КСК, ТК), после чего выполняется протокол распределения мастер ключа SMK. Целостность ключевой информации обеспечивается за счет формирования обоими корреспондентами хеш-функций, аргумент которых состоит из случайных последовательностей rt и rp (обеспечение уникальности сообщений), адресов корреспондентов (обеспечение идентификации корреспондентов) и собственно зашифрованной ключевой информации.

Список использованных источников:

1. Голиков А.М. Сети и системы радиосвязи и средства их информационной защиты: Лабораторный практикум. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2007. – 228 с.

2. P802.11 – IEEE Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications // Scheduled System Maintenance [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/5595635. – Дата доступа: 12.12.2018.