УДК 004.05

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТС

В. Н. Никитин, доцент кафедры защищенных сетей связи СПбГУТ им. М. А. Бонч-Бруевича, к.т.н.; vnikitin@rdnet.ru
О. И. Лагутенко, доцент кафедры беспроводных телекоммуникаций НИУ ИТМО, к.т.н.
М. М. Ковцур, аспирант кафедры защищенных сетей связи СПбГУТ им. М. А. Бонч-Бруевича

Анализируются механизмы защиты информации стандарта IEEE 802.11-12, применяемые для обеспечения информационной безопасности ИТС. Сформулированы не регламентированные стандартом проблемы регулирования вопросов формирования, распределения и использования ключей для криптографической защиты информации.

Ключевые слова: *интеллектуальная транспортная система (ИТС), информационная безопасность, механизм защиты, шифрование, аутентификация, ключ.*

Введение. Проблема аварийности дорожного движения в последние годы становится все острее. Одним из инструментов ее решения является создание интеллектуальных транспортных систем (ИТС) [1]. Для функционирования ИТС необходимы подсистемы высокоточного навигационного обеспечения и подвижной радиосвязи. В основе построения ИТС лежат спецификации беспроводных сетей широкополосного радиодоступа малого радиуса действия (Dedicated Short Range Communication, DSRC), впервые описанные в IEEE 802.11p. При этом предполагалось, что проблемы обеспечения информационной безопасности будут решаться в рамках спецификации IEEE 802.11i.

Вместе с тем условия функционирования ИТС имеют существенные особенности, которые должны учитываться, когда речь идет об обеспечении информационной безопасности. Специфические требования к ИТС привели к необходимости использования технических решений, влияющих на эффективность ее применения. Они описаны в семействе стандартов IEEE 1609 [2]. Спецификация 1609.2 задает реализацию механизмов защиты в ИТС, основываясь на решениях, определенных в семействе стандартов IEEE 802.11 [3].

Технологии защиты информации стандарта IEEE 802.11-2012. С выходом этого стандарта задачи обеспечения информационной безопасности ИТС должны решаться в рамках рекомендуемых в нем технологий защиты информации. Спецификации IEEE 802.11p и IEEE 802.11i были отменены.

Все механизмы защиты теперь выведены в отдельный подуровень безопасности, реализующий функции шифрования ключей и данных, распределения ключей, аутентификации и имитозащиты. Стандартом предусмотрены две инфраструктурные функциональные модели: с аутентификацией по IEEE 802.1x, т.е. с применением протокола EAP, и с помощью заранее предопределенного ключа, прописанного на аутентификаторе и клиенте (режим Preshared Key, PSK). Так как алгоритмы шифрования, использующие процедуру TKIP, уже принято называть WPA, а процедуру CCMP — WPA2, можно сказать, что способами шифрования, удовлетворяющими требованиям построения безопасной сети (Robust Security Network Association, RSNA), являются WPA-EAP (WPA-Enterprise), WPA-PSK (WPA-Preshared Key, WPA-Personal), WPA2-EAP (WPA2-Enterprise), WPA2-PSK (WPA2-Preshared Key, WPA2-Personal) (таблица).

Это послужило поводом к разделению стандарта IEEE 802.11-2012 на две ассоциации безопасности:

- preRSNA, реализующую протокол шифрования WEP или появившийся позднее протокол WPA (TKIP), в котором добавлена функция контроля целостности сообщения MIC, и протокол односторонней аутентификации «запрос–ответ»;
- RSNA, реализующую протокол шифрования CCMP и протокол аутентификации EAP.

Стандартом IEEE 802.11-2012 определено, что в рамках RSNA протокол WPA2 является обязательным, а WEP и WPA — опциональными, предназначенными для обеспечения совместимости со старыми устройствами.

Возможности механизмов защиты, используемых в беспроводных сетях

Механизмы защиты	Протокол			
	WPA-PSK	WPA-EAP	WPA2-PSK	WPA2-EAP
Шифрование	RC4	RC4	AES	AES
Аутентификация	PSK	IEEE 802.1x	PSK	IEEE 802.1x
Длина ключа, бит	128 (шифр.), 64 (аутент.)	128 (шифр.), 64 (аутент.)	128	128
Повторяемость ключа	48-бит TSC	48-бит TSC	48-бит PN	48-бит PN
Целостность данных	Michael	Michael	AES (CBC—MAC)	AES (CBC—MAC)
Целостность заголовка	Michael	Michael	AES (CBC—MAC)	AES (CBC—MAC)
Управление ключами	Статич. для всей сети	На основе EAP	Статич. для всей сети	На основе EAP

Механизмы защиты информации в рамках RSNA. Для усиления безопасности беспроводной сети используется инкапсуляция CCMP с применением алгоритма шифрования AES, обладающего большей стойкостью к различного вида атакам, а также динамической схемы формирования ключевого материала согласно предложенной иерархии ключей. При этом предусмотрено использование ключей формирования имитовставки, шифрования данных и шифрования ключа.

Аутентификация в данной модификации стандарта может выполняться на основе заранее распределенного ключа или по протоколу EAP [4], но оба протокола аутентификации используют модель «запрос–ответ». По завершении протокола EAP 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 (KCK), ключ шифрования трафика (TK), ключ шифрования ключа (KEK). В данном стандарте ассоциации безопасности соответствуют распределенному между корреспондентами секретному ключу:

1. PMKSA — результат успешного завершения протокола EAP либо аутентификации с предварительно распределенным ключом, после которого корреспонденты формируют парный ключ (PMK).

2. PTKSA — результат выполнения протокола распределения ключа в модели обмена сигналами взаимодействия (так называемый протокол двойного квитирования — handshaking), по завершении которого корреспонденты формируют парный временный ключ (PTK).

3. GTKSA — результат выполнения протокола распределения ключа, по завершении которого корреспонденты формируют групповой временный ключ GTK. Протокол распределения этого ключа не является обязательным для установления защищенного соединения.

4. STKSA — результат выполнения протокола распределения ключа в модели обмена сигналами взаимодействия, по завершении которого корреспонденты формируют временный ключ STK для передачи данных между БС.

Аутентификация и распределение ключа RSNA. В архитектуре двусторонней аутентификации по протоколу EAP используется модель «запрос–ответ» с разделением общего секрета (MSK) через RADIUS либо на основе заранее распределенного ключа PSK (рис. 1).

Парный мастер-ключ PMK устанавливается корреспондентами после завершения протокола EAP и содержит 256 бит MSK. Далее корреспонденты вычисляют парный временный ключ (PTK) с использованием протокола обмена сигналами взаимодействия, добавляя к нему свои случайные последовательности $r_a r_s$, адреса SPA (адрес инициатора) и AA (адрес респондента), определяют функцию PRF.

Функция PRF использует циклическую конструкцию с вычислением ключевой хеш-функции HMAC, в основе которой лежит алгоритм SHA-1: HMAC = SHA (PMK, $A||Y||B||X$), где A и B — переменные; Y — нулевая последовательность; X — параметр, определяющий длину хеша (в зависимости от выбранного протокола шифрования $X \in [128,192,256,384,512]$). Эта последовательность длиной 384 бит является PTK для протокола CCMP. Из нее формируются ключи KCK (первые 128 бит), KEK (вторые 128 бит) и TK (оставшиеся 128 бит). Респондент вычисляет MIC для сообщения, содержащего случайную последовательность инициатора, и передает ему эту пару. Инициатор, со своей стороны, рассчитывает PTK и выполняет верификацию своего случайного числа, затем в случае успеха передает сообщение, содержащее данные об успешной установке текущего PTK, и MIC этого сообщения. При корректном завершении протокола устанавливается защищенное соединение.

При использовании группового ключа инициатор выполняет формирование GTK (как ведущей хеш-функции PRF от предварительно распределенного GMK и случайной последовательности, конкатенированной с адресом БС) с последующим вычислением MIC, шифрованием на ключе KEK и передачей его респонденту.

Стандартом предусмотрена выработка парных ключей для безопасной передачи данных в режиме STSL (station-to-station link), в которой данные, передаваемые от АС1 к АС2, проходят через БС. При такой топологии сети необходимо установление ассоциации безопасности STKSA, для чего БС, в свою очередь, должна установить RSNA с обеими АС. БС как посредник между АС1 и АС2 выполняет функции центра распределения ключей. Между БС и каждой АС должен быть установлен общий парный ключ PTK (KEK, KCK, TK), после чего выполняется протокол распределения мастер-ключа MSK. Целостность ключевой информации обеспечивается за счет формирования обоими корреспондентами хеш-функций, аргумент которых состоит из случайных последовательностей r_i и r_p (обеспечение уникальности сообщений), адресов корреспондентов (обеспечение идентификации корреспондентов) и собственно зашифрованной ключевой информации.

Когда протокол распределения MSK успешно завершен, АС1 и АС2, установив SMKSA, должны реализовать ассоциацию STKSA, которая предполагает распределение парных ключей SKEK, SKCK и STK. Формирование парного временного ключевого набора STK ассоциации STKSA выполняется корреспондентами путем вычисления функции PRF от случайных последовательностей (отличных от использованных при установлении ассоциации SMKSA), адресов корреспондентов (STA_I и STA_P) и ключа SMK. Таким образом, аналогично протоколу распределения PTK за счет данного преобразования достигаются проверка принадлежности ключевой информации корреспондентам и защита от повторного использования ключа.

В рамках RSNA стандартом IEEE 802.11—2012 дополнительно предусмотрена аутентификация корреспондентов

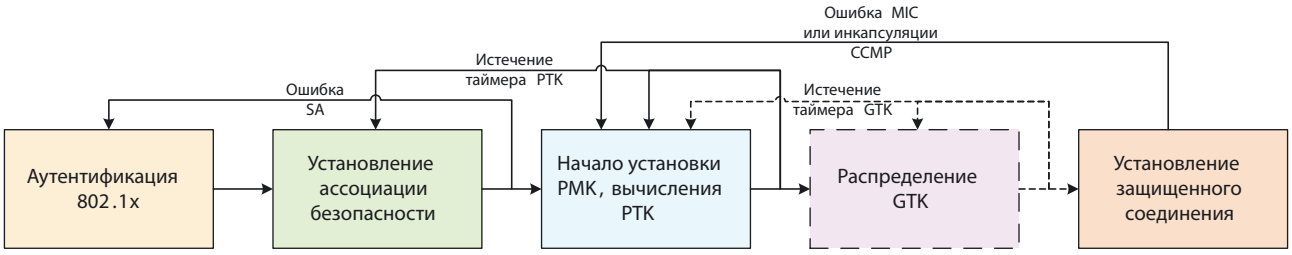

Рис. 1. **Установление защищенного соединения RSNA**

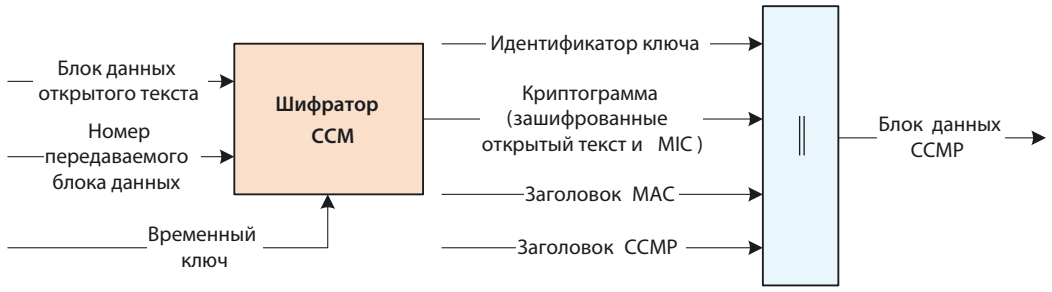

Рис. 2. **Шифрование блока данных CCMP**

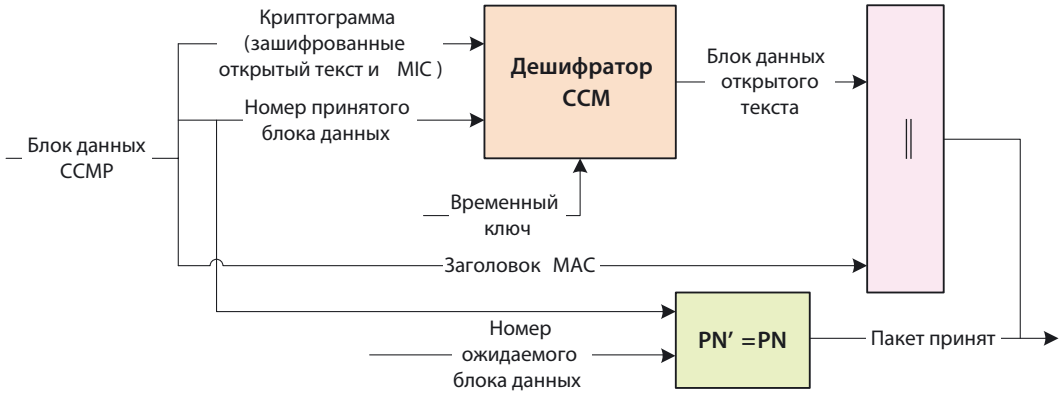

Рис. 3. **Дешифрование блока данных CCMP**

посредством алгоритмов несимметричной криптографии. При этом рассматривается возможность использовать два алгоритма:

- алгоритм над группой точек эллиптических кривых;
- алгоритм над группой дискретного поля.

Стойкость обоих алгоритмов определяется сложностью дискретного логарифмирования в конечном поле. Как показано в [5], алгоритм над группой точек эллиптических кривых имеет заметные преимущества, поскольку в настоящее время не известны алгоритмы нахождения дискретного логарифма на эллиптической кривой с субэкспоненциальной сложностью, хотя для разложения на множители такие алгоритмы существуют. Это позволяет использовать ключи меньшей длины.

Протокол инкапсуляции CCMP обеспечивает шифрование данных (AES-CCM), их аутентификацию (MAC) и целостность (MIC) наряду с защитой от повторной передачи (счетчики CTR). Алгоритм шифрования AES с длиной ключа 128 бит и такой же длиной блока используется в режиме CCM [4], при этом учитываются значения счетчика переданных кадров сообщений, случайных последовательностей (рис. 2).

Верификация и формирование MIC происходят в конструкции, реализующей алгоритм шифрования по схеме CCM, а проверка актуальности значения номера принятого пакета является обоснованием его уникальности. После выполнения указанных условий при дешифровании выносится решение о дальнейшей обработке блока данных (рис. 3).

Заключение. Протокол WEP, первоначально используемый в сетях беспроводного доступа, не обеспечивал должной безопасности передаваемых по радиоканалу данных из-за отсутствия в нем механизмов удостоверения подлинности и целостности сообщений, слабой, односторонней, аутентификации корреспондентов и недостаточно стойкого шифрования. В дальнейшем это послужило причиной разработки более совершенных протоколов инкапсуляции данных — WPA и WPA2.

Версия стандарта IEEE 802.11-2012, как показано в статье, является наиболее защищенной и совместно со спецификацией IEEE 1609.2 обеспечивает простоту реализации механизмов защиты информации в ИТС.

Вместе с тем для комплексного решения задач информационной безопасности ИТС в Российской Федерации необходимо предпринять ряд шагов в области нормативного правового обеспечения и стандартизации, направленных на легализацию криптографических алгоритмов, регулирование вопросов выработки, распределения и использования ключей.

ЛИТЕРАТУРА

1. **Крючков В. В.** Предпосылки создания конкурентоспособной и экологически рациональной транспортной системы в Российской Федерации /Матер. Межд. конф. «Безопасность дорожного движения и интеллектуальные транспортные системы на автомобильных дорогах общего пользования».— Санкт-Петербург, 24–26 мая 2011 г.
2. P1609.2/D9.0, May 2011 — IEEE Draft Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages.
3. IEEE 802.11-2012 — Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and metropolitan area networks. Specific requirements — Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 11: Security.
4. **Никитин В. Н., Юркин Д. В.** Сравнение стойкости реализаций протокола при выборе различных криптографических систем //Защита информации. INSIDE.— 2008.— № 6.
5. **Gura N., Patel A., Wander A.,** et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs /Sun Microsystems Laboratories.— URL: //http://www.research.sun.com/projects/crypto.

Получено 10.12.13