Механизмы защиты информации в сетях DSRC

Information security mechanisms in the DSRC networks

Ключевые слова: интеллектуальная транспортная система – intelligent transport system; информационная безопасность – information security; механизм защиты – protection mechanism; шифрование – encoding; аутентификация – authentication; ключ – key.

В статье описываются основные механизмы безопасности, применяемые в технологии широкополосного радиодоступа малого радиуса действия (DSRC) и впервые описанные в стандарте IEEE 802.11p. Обращается внимание на существенные особенности, которые необходимо учитывать при решении задач обеспечения информационной безопасности при реализации обмена информации между транспортными средствами. Описаны основные технические решения, определенные в стандарте IEEE 1609.2.

The article describes main security mechanisms, used in the Dedicated Short Range Communications (DSRC) technology that were first described in the IEEE 802.11p standard. Special attention is drawn to the essential features that have to be taken into consideration during solving the tasks informational security provision during data exchange between vehicles organization implementation. The main technical solutions determined by the IEEE 1609.2 standard are described.

НИКИТИН / NIKITIN V.
Валерий Николаевич
(vnikitin@rdnet.ru)
кандидат технических наук,
доцент кафедры Защищенных сетей связи,
Санкт-Петербургский государственный
университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ),
г. Санкт-Петербург

ХВОРОВ / KHVOROV I.
Игорь Алексеевич
(khvorov@labics.ru)
кандидат технических наук,
доцент кафедры Беспроводных телекоммуникаций,
Санкт-Петербургский национальный исследовательский
университет информационных технологий,
механики и оптики (НИУ ИТМО),
г. Санкт-Петербург

ТАРАКАНОВ / TARAKANOV S.
Сергей Александрович
(k.v.tarakanov@gmail.com)
кандидат технических наук,
директор Центра медицинского, экологического
приборостроения и биотехнологий,
НИУ ИТМО,
г. Санкт-Петербург

КОВЦУР / KOVTSUR M.
Максим Михайлович
(maxkovzur@mail.ru)
аспирант кафедры
Защищенных сетей связи,
СПбГУТ им. проф. М.А. Бонч-Бруевича,
г. Санкт-Петербург

ВВЕДЕНИЕ

Интеллектуальные транспортные системы (ИТС) – новое направление информационных технологий, одной из важнейших задач которых является решение задачи снижения аварийности в дорожном движении [1]. В основе построения ИТС лежат спецификации беспроводных сетей широкополосного радиодоступа малого радиуса действия (DSRC), впервые описанные в IEEE 802.11p. Вместе с тем, условия функционирования ИТС имеют существенные особенности, которые необходимо учитывать при решении задач обеспечения информационной безопасности. Специфические требования к ИТС привели к необходимости использования технических решений, определяющих эффективность ее применения. Эти решения описаны в семействе стандартов IEEE 1609 [2]. Спецификация 1609.2 в настоящее время находится на стадии разработки и должна определять реализацию механизмов защиты в DSRC, основываясь на решениях, определенных в семействе стандартов IEEE 802.11 [3].

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ СТАНДАРТА 802.11—2012

С выходом стандарта IEEE 802.11–2012 спецификации IEEE 802.11p и IEEE 802.11i отменены, а задачи обеспечения информационной безопасности ИТС должны решаться рамках механизмов защиты информации рекомендуемых данным стандартом.

Все механизмы защиты выделены в отдельный подуровень безопасности, реализующий функции аутентификации корреспондентов, распределения ключей, шифрования ключей и данных, имитозащиты данных.

Стандартом предусмотрены две инфраструктурные функциональные модели: с аутентификацией по IEEE 802.1x, т. е. применением протокола EAP для распределения ключей, и с помощью заранее предопределенного ключа, прописанного на аутентификаторе и клиенте (такой режим называется Preshared Key, PSK). Это послужило поводом к разделению стандарта IEEE 802.11 на две ассоциации безопасности:

– pre-robust security network association (preRSNA), реализованной протоколом шифрования WEP или появившимся позднее протоколом WPA (TKIP), в котором добавлена функция контроля целостности сообщения MIC, и протоколом односторонней аутентификации «Запрос-ответ»;

– robust security network association (RSNA), реализующей протокол шифрования CCMP и протокол аутентификации EAP.

Так как алгоритмы шифрования, использующие процедуру TKIP, уже принято называть WPA, а процедуру CCMP – WPA2, то можно сказать, что способами шифрования, удовлетворяющими требованиям построения безопасной сети (RSNA), являются: WPA2-EAP (WPA2-Enterprise), WPA2-PSK (WPA2-Preshared Key, WPA2-Personal). Их возможности в обобщенном виде представлены в таблице 1.

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

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАМКАХ RSNA

Усиление безопасности беспроводной сети заключается в использовании инкапсуляции CCMP с применением алгоритма шифрования AES, обладающего 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. 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.

Таблица 1

Протокол	**WPA2-PSK**	**WPA2-EAP**
Шифрование	AES	AES
Аутентификация	Preshared Key	IEEE 802.1x
Длина ключа, бит	128	128
Повторяемость ключа	48-бит PN	48-бит PN
Целостность данных	AES (CBC-MAC)	AES (CBC-MAC)
Целостность заголовка	AES (CBC-MAC)	AES (CBC-MAC)
Управление ключами	Статич. для всей сети	На основе EAP

2. PTKSA – результат выполнения протокола распределения ключа в модели двустороннего рукопожатия, 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 модели двустороннего рукопожатия, 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 (Pre-Shared Key) (рис. 1).

Парный мастер ключ (PMK) устанавливается корреспондентами после завершения протокола EAP и является старшими 256 битами MSK. Далее корреспонденты вычисляют парный временный ключ (PTK) по протоколу двустороннего рукопожатия, добавляя к нему свои случайные последовательности r_a r_s и адреса SPA (адрес инициатора) AA (адрес респондента), вычисляют от них 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 – это переменные, Y – это нулевая последовательность, X – это параметр, определяющий длину хеша (в зависимости от выбранного протокола шифрования может принимать значения $X \in [128,192,256,384,512]$). Эта последовательность длиной 384 бита 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 вычисляет со своей стороны PTK и выполняет верификацию своего случайного числа, в случае успеха передает сообщение, содержащее данные об успешной установке текущего PTK и MIC этого сообщения. При успешном завершении протокола устанавливается защищенное соединение.

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

Стандартом предусмотрена выработка парных ключей для безопасной передачи данных в режиме STSL (station-to-station link), в которой передаваемые данные от AC1 к AC2 проходят через БС. При данной топологии сети необходимо установление ассоциации безопасности STKSA, для чего БС в свою очередь должна установить RSNA с обеими AC. БС является посредником между двумя абонентами AC1 и AC2 и выполняет функции центра распределения ключей. Необходимо, чтобы между БС и каждой AC был 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.

При успешном завершении протокола распределения MSK AC1 и AC2, установив SMKSA, должны

Рис. 1. Установление защищенного соединения RSNA

установить ассоциацию STKSA, которая предполагает распределение парных ключей SKEK, SKCK и STK. Формирование парного временного ключевого набора STK ассоциации STKSA выполняется корреспондентами путем вычисления корреспондентами 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 достигается принадлежность ключевой информации корреспондентам и защита от повторного использования ключей.

В рамках RSNA стандартом IEEE 802.11–2012 дополнительно предусмотрена возможность аутентификации корреспондентов с использованием алгоритмов несимметричной криптографии.

При этом рассматривается возможность использования двух алгоритмов:

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

В сетях DSRC рекомендуется использовать алгоритм цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm), аналогичный стандарту X509[4]. ECDSA имеет существенные преимущества над алгоритмом RSA, определяемым рекомендацией, поскольку в настоящее время не известны алгоритмы нахождения дискретного логарифма на эллиптической кривой с суб-экспоненциальной сложностью, в то время как для разложения на множители такие алгоритмы существуют. Это позволяет использовать в ECDSA ключи меньшей длины.

ПРОТОКОЛ ИНКАПСУЛЯЦИИ CCMP

Протокол CCMP обеспечивает шифрование данных (AES режим CCM), их аутентификацию (MAC) и целостность (MIC) вместе с защитой от повторной передачи (счетчики CTR). Алгоритм шифрования AES с длиной ключа 128 бит и такой же длиной блока используется в режиме CCM [3], с учетом значений счетчика переданных

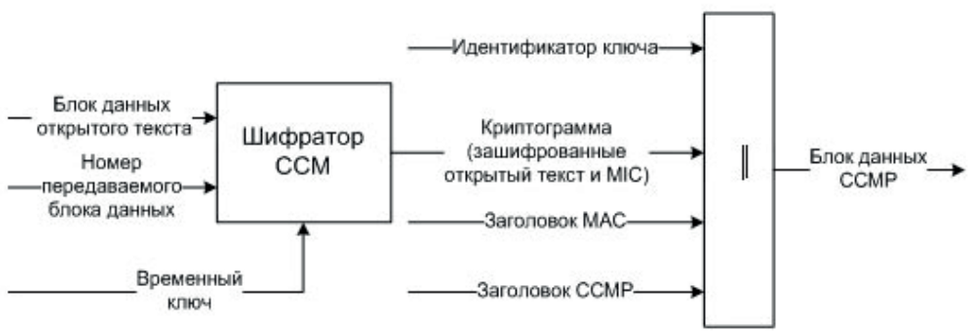


Рис. 2. Шифрование блока данных CCMP

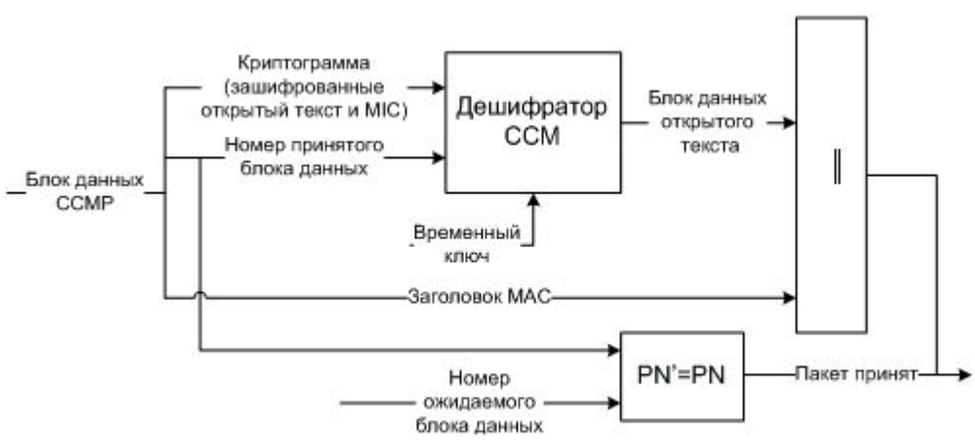


Рис. 3. Дешифрование блока данных CCMP

кадров сообщений, случайных последовательностей (рис. 2).

Верификация и формирование MIC происходит в конструкции, реализующей алгоритм шифрования по схеме CCM, а проверка актуальности значения номера принятого пакета является основанием его уникальности. По выполнении вышеуказанных условий при дешифровании выносится решение о дальнейшей обработке блока данных (рис. 3).

ЗАКЛЮЧЕНИЕ

Первоначально используемый в сетях беспроводного доступа протокол WEP не обеспечивал должную безопасность передаваемых по радиоканалу данных вследствие отсутствия в нем механизмов удостоверения подлинности и целостности сообщений, слабой односторонней аутентификации корреспондентов и недостаточно стойкого шифрования, что послужило в дальнейшем причиной разработки более совершенных протоколов инкапсуляции данных WPA и WPA-2.

Таким образом, можно отметить, что версия стандарта IEEE 802.11–2012 является наиболее защищенной и, совместно с спецификацией IEEE 1609.2, обеспечивает простоту реализации механизмов защиты информации в ИТС.

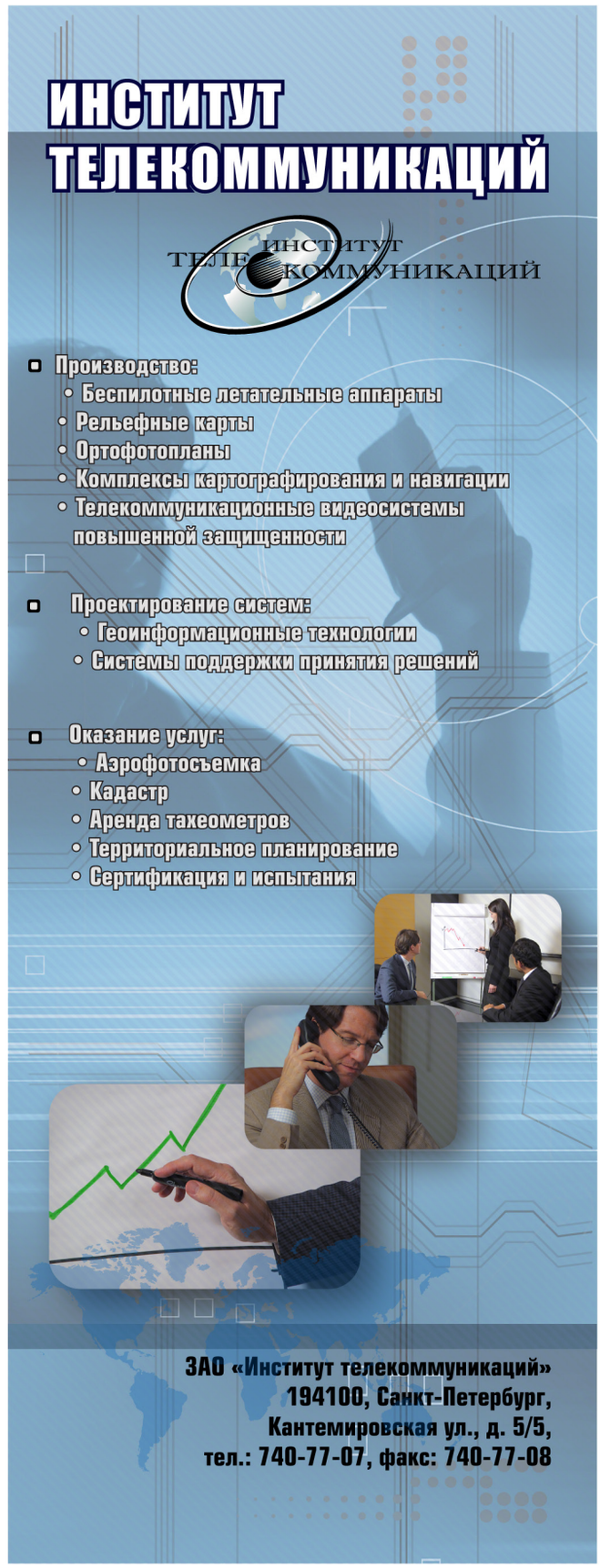
Вместе с тем, для комплексного решения задач информационной безопасности ИТС в Российской Федерации необходимо предпринять ряд шагов нормативно-правового обеспечения и стандартизации в части легализации криптографических алгоритмов, регулирования вопросов выработки, распределения и использования ключей.

Литература

1. *Крючков В.В.* Предпосылки создания конкурентоспособной и экологически рациональной транспортной системы в Российской Федерации/ Межд. конф. «Безопасность дорожного движения и интеллектуальные транспортные системы на автомобильных дорогах общего пользования». Санкт-Петербург, 24–26 мая 2011 г.

2. Draft Standard for Wireless Access in Vehicular Environments V Security Services for Applications and Management Messages, IEEE P1609.2/D9.0, May 2011.

3. IEEE Standard for Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks-Specific requirements – Part 11: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 11: Security: IEEE 802.11:-2012. Instute of Electrical and Electronics Engineers, 2012.

4. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile/D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. May 2008.

5. *В. Н. Никитин, Д. В. Юркин.* Сравнение стойкости реализаций протокола при выборе различных криптографических систем.// Зашита информации-Inside. – 2008. – № 6.