БЕЗОПАСНОСТЬ ДАННЫХ ЭНЕРГОЭФФЕКТИВНОЙ СЕТИ LORAWAN

DATA SECURITY OF THE ENERGY-EFFICIENT LORAWAN NETWORK

УДК 621.396.1, 004.056

Муртазин Марсель Маратович, бакалавр, Поволжский государственный университет телекоммуникаций и информатики, г. Самара
Шелашников Олег Алексеевич, бакалавр, Поволжский государственный университет телекоммуникаций и информатики, г. Самара

Murtazin M.M. murtazin998@gmail.com
Shelashnikov O.A. oselasnikov@gmail.com

Аннотация

Беспроводные сенсорные сети – это новая парадигма развития «цифрового» общества [1; 2]. Использование интернет-вещей является повседневной практикой. «Умные» технологии, осуществляют свою работу как в обычных домохозяйствах, так и на объектах производственной и непроизводственной сферы, специализированных структур, для чего требуется обеспечивать безопасность информационного обмена, в том числе телеметрических данных. Уникальность современных беспроводных систем с низкой мощностью излучения заключается в энергоэффективности и хорошем радиусе действия, способным покрыть зону в городе до 5 километров и 12 километров в пригороде при скорости передачи данных всего от 300 бит/с до 55 Кбит/с. Логично предположить, что безопасность передачи данных в сети становится её основным свойством и ключевым фактором доверия к ней со стороны пользователей и компаний. В связи с этим в сетях пониженного

излучения с большим радиусом действия для обеспечения безопасности коммерческих данных применяется развитые услуги шифрования AES, режимы счетчика CTR и режим с аутентификацией по коду в зашифрованном сообщении CMAC. Рассматриваются основные процедуры шифрования с использованием ключей и подключений. Приводится обобщенная схема алгоритма генерации подключей для обеспечения безопасности данных.

Annotation

Wireless sensor network is a new paradigm of the "digital" society [1; 2]. Internet of things using is an everyday practice. All «smart» technology, carry out its work both in ordinary households, and at the objects of industrial and nonindustrial sphere, specialized structures, which requires to ensure the security of information exchange, including telemetry. The uniqueness of modern wireless low radiation systems lies in its energy efficiency and wide transmission range, that covering an area up to 5 kilometers in the city and 12 km in the suburbs with a data transfer rate from 300 bit/s to 5 Kbit/s. It is reasonable to assume that the security of data transmission at wireless sensor network can be considered as main feature and key trust factors for users and companies. In this regard, in order to ensure the security of commercial data low radiation wide area network uses advanced encryption services, AES encryption and the Counter, CTR and cipher message authentication code, CMAC mode. The basic encryption procedures using keys and connections are discussed. A generalized scheme of the algorithm for generating connections to ensure data security is given.

Ключевые слова: LoRaWAN, AES, CTR, CMAC, безопасность, шифрование, блочный шифр, подключи, сеть пониженного излучения.

Keywords: LoRaWAN, AES, CTR, CMAC, security, encryption, block cipher, subkeys, low radiation network.

Стандарт энергоэффективной передачи телеметрических данных с широким покрытием LoRaWAN развивается последние 5 лет с учетом

требований сквозного шифрования данных, секретности и конфиденциальности [3; 4]. Для этого в рамках LoRaWAN широко используется стандарт шифрования под названием AES, который был создан Национальным институтом стандартов и технологий (NIST) в 2001 году.

Шифр AES есть симметричный блочный шифр, который для обеспечения безопасности данных использует криптографические ключи различной длины, а именно 128, 192 или 256 бит. Применяемый алгоритм шифрования данных здесь основан на симметричном ключе. В нем используются фиксированные блоки, а информация, размер которой превышает стандартный размер, разбивается на несколько блоков. AES используется с режимами работы, разработанными специально для использования с алгоритмами блочных шифров [5; 6].

Размер ключа, применяемого при шифровании, определяет количество преобразований для обеспечения требуемого уровня безопасности входных данных с разумным использованием вычислительных ресурсов и энергоэффективности. Поэтому в сетях LoRaWAN применяется 128-битный криптографический ключ AES, который устанавливает десять периодов при выполнении алгоритма.

Применение режима CTR обусловлено тем, что это режим конфиденциальности, который использует блочные шифры для создания потокового шифра. Входными данными являются конкатенация некоей случайной величины nonce, счетчика и криптографического ключа для выполнения алгоритма блочного шифра. Выход предыдущей операции шифрования объединяется через операцию XOR с открытым текстом для генерации шифротекста. Все конкатенации nonce и счетчика, которые применяются в операциях шифрования, должны быть разными в каждом блоке, который шифруется одним и тем же ключом. При таком условии все блоки будут разными, даже если они находятся в одном и том же сообщении, поэтому можно поддерживать высокий уровень безопасности LoRaWAN.

Последний блок может иметь фрагментарное количество битов, и наиболее значимые биты последнего выходного блока используются для операции XOR, а остаточные биты удаляются. Таким образом, входной и выходной блоки имеют одинаковую длину битов.

В сети LoRaWAN применяется CTR в сочетании с блочным шифром AES для шифрования полезной нагрузки, а конкатенация nonce и счетчика определена в спецификации. Блок-схема шифрования AES-CTR представлена схемой, где «Key» означает ключ, «Plaintext» означает открытый текст, «Ciphertext» означает зашифрованный текст (см. рис. 1.1).

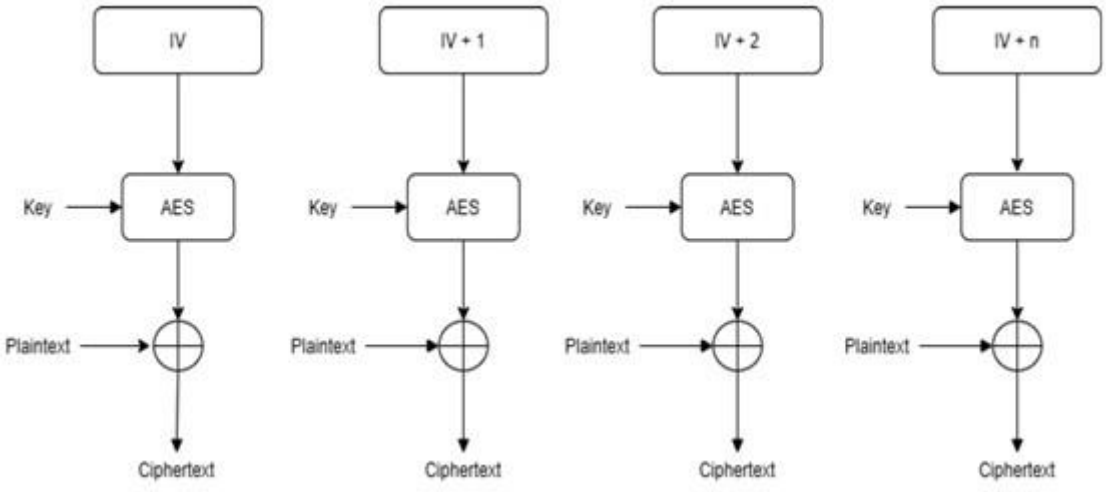

Рис. 1.1 – Шифрование AES-CTR в LoRaWAN версии 1.1

Режим работы CMAC предусматривает формирование хэш-функции, защищенной ключом, который поддерживается симметричным ключевой блочный шифр. Для того чтобы выполнить режим работы CMAC, необходимо получить от доверенного источника два дополнительных секретных значения, называемых подключами (subkeys). Блочный шифр применяется в блоке, состоящий полностью из нулевых битов. Затем, подключ 1 получается из результирующего значения путем сдвига влево на один бит и выполнения операции XOR с константой основанной на размере блока. Подключ 2 получается аналогичным способом из подключа 1. Известна блок-схема генерации подключей (см. рис 1.2).

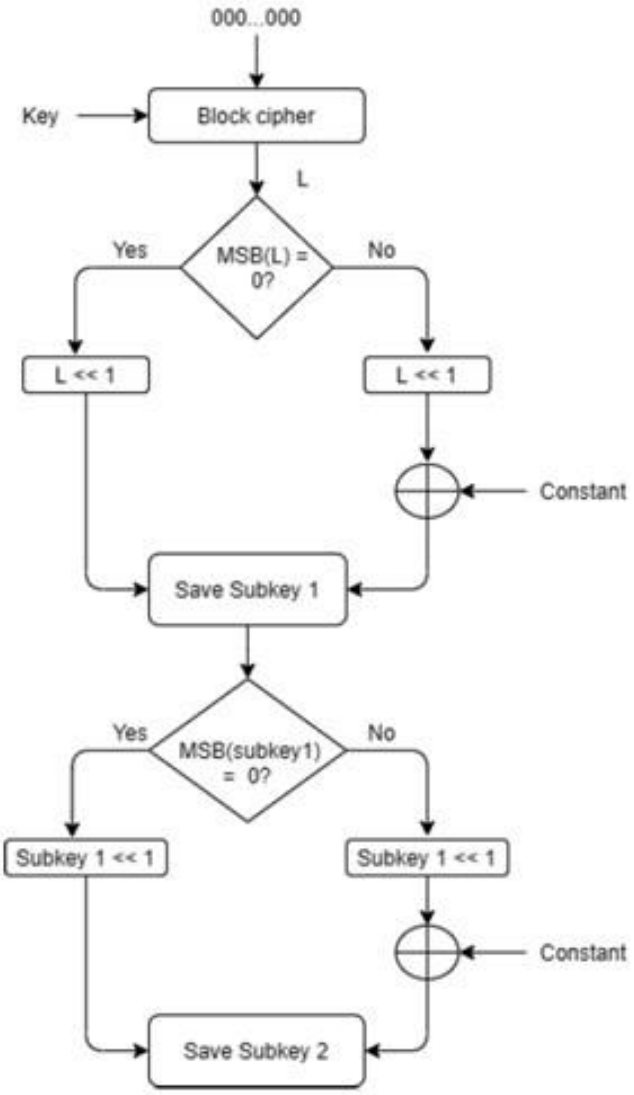

Рис. 1.2 – Генерация подключей AES-CTR в LoRaWAN версии 1.1

Здесь процесс генерации начинается с анализа старшего значащего бита MSB и далее делится на две процедуры в зависимости от соотношения между длиной передаваемого сообщения и размером блока. Если длина сообщения *L* кратна размеру блока, то сообщение разбивается на блоки, а последний блок заменяется операцией XOR последнего блока с подключом (Subkey). Если длина сообщения не является кратной размеру блока, то сообщение разбивается на блоки, и конечная битовая строка в разделе заполняется, а затем восстанавливается операцией XOR конечного блока с подключом №2.

Когда операция начинается, первый блок шифруется алгоритмом AES с использованием ключа. Выход предыдущей операции представляет собой

операцию XOR со следующим блоком и шифруется с помощью алгоритма AES с использованием ключа, пока не закончатся все блоки. Последний выходной блок ограничивается в соответствии с размером параметра и является кодом аутентификации сообщения. В сети LoRaWAN, CMAC применяется в сочетании с блочным шифром AES для защиты целостности и подлинности сообщений на сетевом уровне. Известна блок-схема для генерации AES-CMAC с целым числом, кратным размеру блока (см. рис. 1.3).

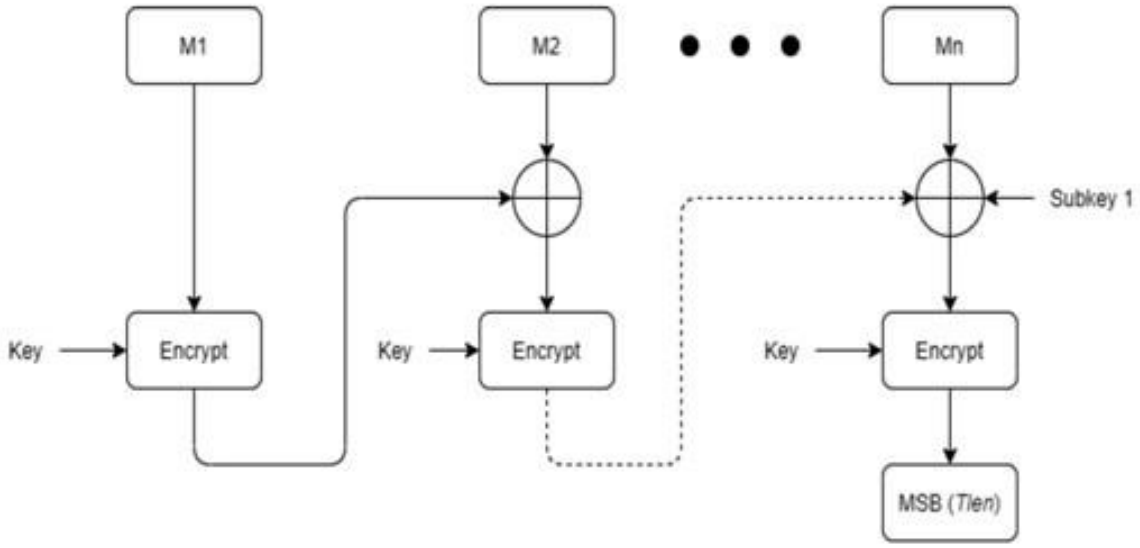

Рис. 1.3 – Последовательность процедур генерации AES-CMAC с целым числом, кратным размеру блока

Для проверки AES-CMAC описанный процесс выполняется применительно к полученному сообщению и конечный результат сравнивается с полученным результатом проверки целостности. Если значения равны, то сообщение успешно проверено на целостность. Недостатком рассмотренной системы защиты информации является то, что внедрение беспроводной генерации секретных ключей или оптимального алгоритма генерации ключей требует повышенного потребления энергии. Направлением дальнейших исследований является обеспечение оптимального энергопотребления с сохранением требуемой безопасности данных [7].

Литература

1. Угрозы безопасности ядра пакетной сети 4G [Электронный ресурс] / Компания «Positive Technologies». – Электрон. текстовые дан. и граф. дан. – М.: офиц. сайт, 2017. - Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/?sphrase_id=74511, свободный. – Заглавная с экрана.

2. Интернет вещей [Текст] / А. В. Росляков [и др.]. – Самара: ПГУТИ, ООО «Издательство Ас Гард», 2014. - 342 с.

3. Гребешков, А. Ю. Технологии будущих инфокоммуникационных сетей, ч.1.: учебное пособие [Электронный ресурс] / А.Ю. Гребешков. – Самара, ФГБОУ ВО ПГУТИ. – 2022. Лиценз. договор ПГУТИ № 67 от 28.04.2022 г. Режим доступа: http://elib.psuti.ru/Grebeshkov_tehnologii_budushchih_infokommunikacionnyh_setej_uchebnoe_posobie_ch1_2022.pdf, по паролю

4. Бутун И., Перейра Н., Гидлунд М. Анализ рисков безопасности LoRaWAN и будущие направления [Текст] // Будущий Интернет, 2019 – Том 11, №3. 22 с. doi: 10.3390/fi11010003

5. Ноздрунов, Н., Семенов, А. Подходы к криптографической защите коммуникаций в IoT и M2M [Электронный ресурс] / Владислав Ноздрунов, Александр Семенов. – Электрон. текстовые дан. – М.: [б. и.], 2019. Режим доступа: https://lib.itsec.ru/articles2/crypto/podhody-k-kriptograficheskoy-zaschite-kommunikatsiy-v-iot-i-m2m, свободный. – Заглавная с экрана.

6. Технологии LPWAN для приложений Интернета вещей и M2M / под ред. Чаудхари Б.С., Зеннаро М. – Academic Press Elsevier, 2020 (на англ. языке)

7. Раза, У., Кулкарни, П., Сооriябандара, М. Маломощные глобальные сети: обзор [Текст] / У. Раджан, П. Кулкарни, М. Сооriябандара // IEEE Communication Survey, 2017. – Т. 19. - С.855- 873 (на англ. языке)

Literature

1. Threats to the security of the core of the 4G packet network [Electronic resource] / Positive Technologies Company. – Electron. text data. and count. dan. – M.: ofits. website, 2017. - Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/?sphrase_id=74511 , free. – The title from the screen

2. Internet of Things [Text] / A.V. Roslyakov [et al.]. – Samara: PGUTI, Publishing House As Gard, LLC, 2014. - 342 p.

3. Grebeshkov, A. Yu. Technologies of future infocommunication networks, part 1.: textbook [Electronic resource] / A.Yu. Grebeshkov. – Samara, FGBOU IN PGUTI. – 2022. License. agreement of the State Technical University No. 67 dated 28.04.2022. Access mode: http://elib.psuti.ru/Grebeshkov_tehnologii_budushchih_infokommunikacionnyh_setej_uchebnoe_posobie_ch1_2022.pdf , by password

4. Butun I., Pereira N., Gidlund M. LoRaWAN security risk analysis and future directions [Text] // Future Internet, 2019 – Volume 11, No. 3. 22 pages. doi: 10.3390/fi11010003

5. Nozdrunov, N., Semenov, A. Approaches to cryptographic protection of communications in It and M2M [Electronic resource] / Vladislav Nozdrunov, Alexander Semenov. – Electron. text data. – M.: [B. I.], 2019. Access mode: https://lib.itsec.ru/articles2/crypto/podhody-k-kriptograficheskoy-zaschite-kommunikatsiy-v-iot-i-m2m , free. – The title from the screen.

6. LPWAN technologies for Internet of Things and M2M applications / ed. Chaudhary B.S., Zennaro M. – Academic Press is an imprint of Elsevier, 2020.

7. Raza, U., Kulkarni, P., Sooriyabandara, M. Low power wide area networks: an overview [Text] / U. Raza, P. Kulkarni, M. Sooriyabandara // IEEE Communication Survey. Tutor, 2017. – Vol. 19. – P.855- 873.