УДК 004

ТЕХНОЛОГИЯ БЕЗОПАСНОЙ КОММУНИКАЦИИ УСТРОЙСТВ С ОГРАНИЧЕННЫМИ РЕСУРСАМИ

Махмутов Амир Рашитович

Студент, Уфимский государственный авиационный технический университет, 450008, г. Уфа, ул. Карла Маркса 12, e-mail: makhmutovamir15@gmail.com

Высоцкий Никита Игоревич

Студент, Уфимский государственный авиационный технический университет, 450008, г. Уфа, ул. Карла Маркса 12, e-mail: chubays123@ya.ru

Миронов Константин Валерьевич

PhD., ст. преподаватель, Уфимский государственный авиационный технический университет, 450008, г. Уфа, ул. Карла Маркса 12, e-mail: mironovconst@gmail.com

Meisel Marcus

Univ.Ass. Dipl.-Ing., Institute of Computer Technology, Technische Universität Wien, 1040 Wien, Gußhausstraße 25-27, e-mail: marcus.meisel@tuwien.ac.at

Sauter Thilo

Ao.Univ.Prof. Dipl.-Ing. Dr.techn., Institute of Computer Technology, Technische Universität Wien, 1040 Wien**,** Gußhausstraße 25-27**,** e-mail: Thilo.sauter@donau-uni.ac.at

Аннотация: В статье представлена технология защищенной передачи данных, которая может быть применена при построении различных маломощных беспроводных сетей, например, в системах умного дома, промышленных беспроводных сенсорных сетях, коммуникационных сетей Smart Grid. Особенность таких сетей в том, что устройства, из которых они состоят, не обладают достаточной мощностью, чтобы поддерживать быстрое выполнение асимметричных криптоалгоритмов. В связи с этим предлагается использование инфраструктуры ключей, основанной на применении исключительно симметричной криптографии.

Ключевые слова: беспроводные сети, безопасная коммуникация, криптография, микроконтроллеры.

Цитирование: Махмутов А.Р., Высоцкий Н.И., Миронов К.В., Meisel M., Sauter T. Технология безопасной коммуникации устройств с ограниченными ресурсами // Информационные и математические технологии в науке и управлении. 2019. № 1 (13). С. 133–141. DOI: 10.25729/2413-0133-2019-1-12

Введение. По мере развития технологий интернета вещей все большее распространение получают локальные сети, узлами которых являются маломощные специализированные вычислительные устройства. Примеры таких сетей: системы умного дома [5], сети систем Smart Grid, промышленные беспроводные сети и пр.

Как и иные коммуникационные системы, подобные сети требуют защиты информации [9]. Особенно остро стоит вопрос защищенности в сетях, обслуживающих критическую инфраструктуру – электрические сети, крупные промышленные объекты и т. п. При этом стандартные меры криптографической защиты при построении таких сетей часто

игнорируются. Мощность используемых устройств не рассчитана на выполнение асимметричных криптографических алгоритмов.

Существуют криптографические системы с открытым и закрытым ключом, но конечного решения по выбору наилучшей нет [7]. Некоторые авторы поддерживают инфраструктуры с открытым ключом (PKI – Public Key Infrastructure), однако этот подход имеет ряд недостатков в случае применения в системах маломощных устройств, наиболее очевидным из которых является невозможность удовлетворить строгие требования в отношении затраченных ресурсов и времени вычислений, поскольку аппаратные возможности строго ограничены. Также процесс восстановления скомпрометированных ключей требует задействования более сложных механизмов, чем в симметричных системах шифрования [15]. Возможны иные действия без подключения к устройству [10, 8]. В таком случае регулярное обновление ключей не вызывает дополнительные расходы [15].

На рисунке 1 представлена обобщенная схема рассматриваемой сети.

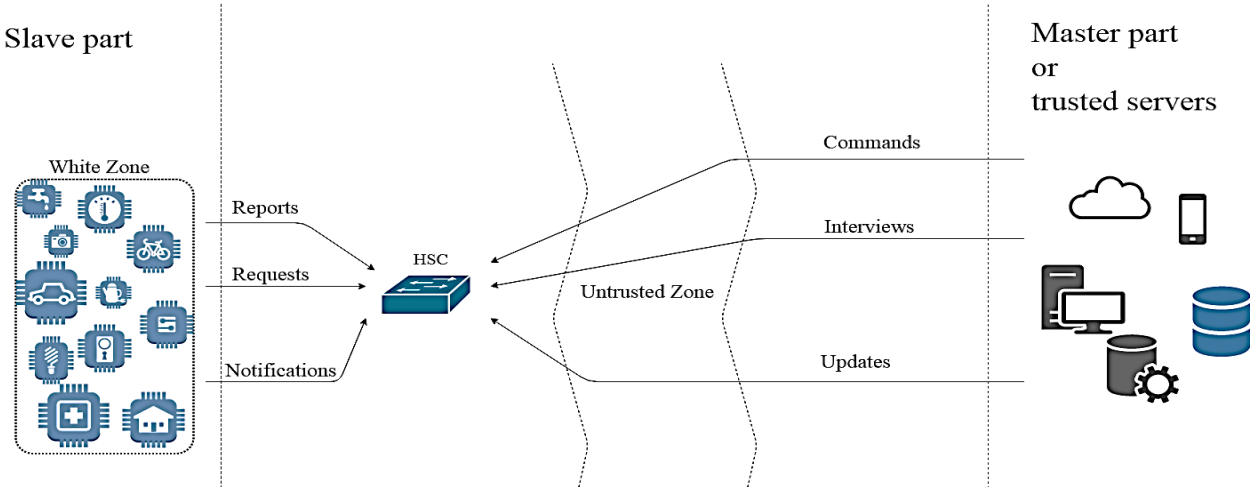

Рис. 1. Обобщенная схема рассматриваемой сети

В левой части рисунка представлена рабочая зона, в которой находится локальная сеть с подключенными устройствами интернета вещей. Примером такой сети может служить отдельная квартира «умного» дома. Правее, на границе рабочей зоны и зоны с низким уровнем доверия, размещено головное устройство локальной сети. Далее находится канал передачи информации, который обеспечивает соединение с зоной управления, в которой находятся различные устройства для управления рабочей зоной и головным устройством. К зоне управления относятся также сервера для обновления и регулярной проверки актуальности программного обеспечения головного устройства. Для связи между устройствами рабочей зоны и головным устройством используется беспроводной радиомодуль, для связи между зоной управления и головным устройством используется сеть Интернет.

Цель комплекса: обеспечить безопасное взаимодействие пользователя с устройствами интернета вещей. Задачи комплекса: 1) обеспечение криптографической защиты передаваемой информации между зоной управления и рабочей зоной; 2) фильтрация трафика, приходящего из канала передачи информации; 3) проведение автоматического обновления программного обеспечения компонентов комплекса; 4) защита домашней сети устройств интернета вещей от атак извне.

В работе Заутера и Тройтля [15] была представлена инфраструктура симметричных ключей для маломощных сетей, она является универсальной по отношению как к используемым симметричным алгоритмам, так и к аппаратному обеспечению. Была протестирована работа алгоритмов AES и DES на примитивном контроллере 8051.

В статье предлагается технология с использованием конкретного аппаратного обеспечения и криптографических алгоритмов. В первой части статьи описывается аппаратное обеспечение, которое предполагается использовать при построении защищенной сети маломощных устройств, во второй части обсуждается криптографическая составляющая.

1. Аппаратная часть. На данный момент существует множество алгоритмов шифрования, каждый из которых имеет свои преимущества и недостатки [11]. Для микроконтроллеров основной проблемой является необходимость большого числа математических операций, что, в свою очередь, может приводить к заметным временным задержкам при обработке данных.

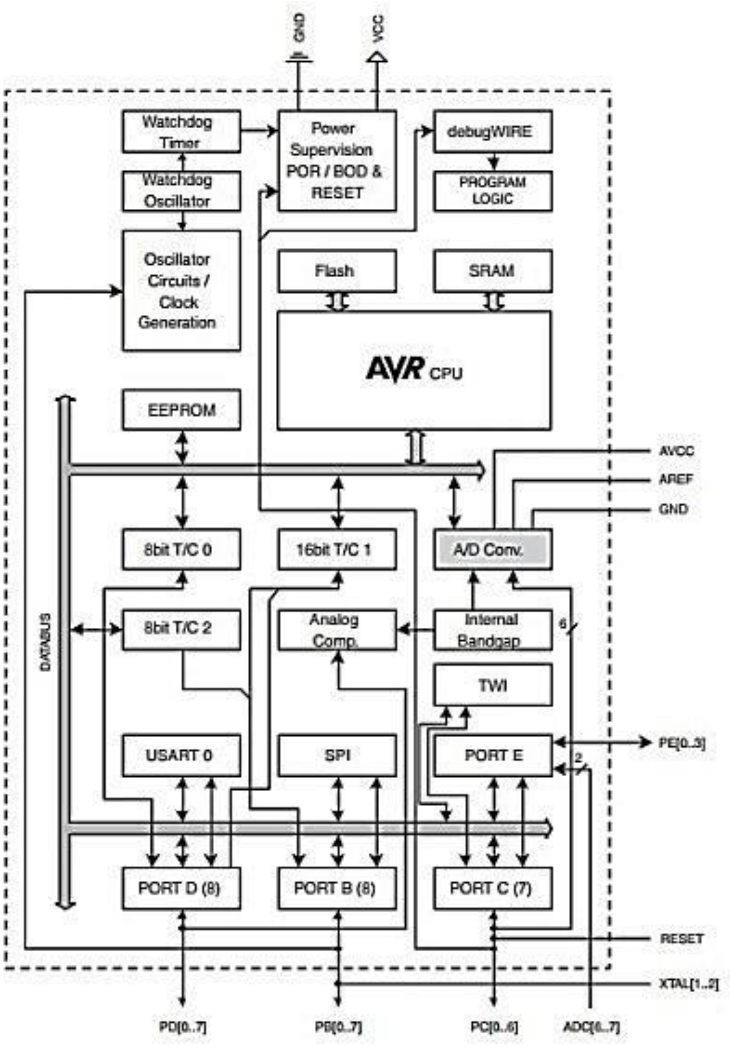

Рис. 2. Структурная схема ATmega328p

Для реализации алгоритмов понадобятся микроконтроллеры с достаточной производительностью и хорошим объемом памяти. В качестве основы для прототипа был выбран микроконтроллер на платформе AVR [12], а именно ATmega328P. Ниже приводятся его структурная схема и характеристики [13].

Характеристики:

- Память: 32 kB Flash, 2 kB RAM, 1 kB EEPROM
- 8-битная архитектура ATMEL AVR, тактовая частота до 20МГц, в Arduino работает на 16МГц. 1 MIPS/MHz
- Напряжение питания 5В или 3.3В

Благодаря среде разработки Arduino IDE процесс программирования микроконтроллера максимально упрощен, так как данная среда избавляет от необходимости установки множества ручных настроек и дополнительных конфигураций проекта.

После успешных испытаний на прототипе планируется сменить платформу разработки на STM, эти контроллеры имеют больше вычислительных ресурсов по сравнению с AVR. Так же одним из важных моментов является то, что STM дешевле AVR в

несколько раз и имеют при этом большие показатели по производительности. Недостатком является сложность разработки проектов из-за специфичности сред, могут возникать сложности [2] в создании и настройке конфигурационного файла. Ниже представлена структурная схема микроконтроллера STM32f103c8 (рис. 3) и его характеристики [17]. Позже возможна замена на другой микроконтроллер той же платформы [18].

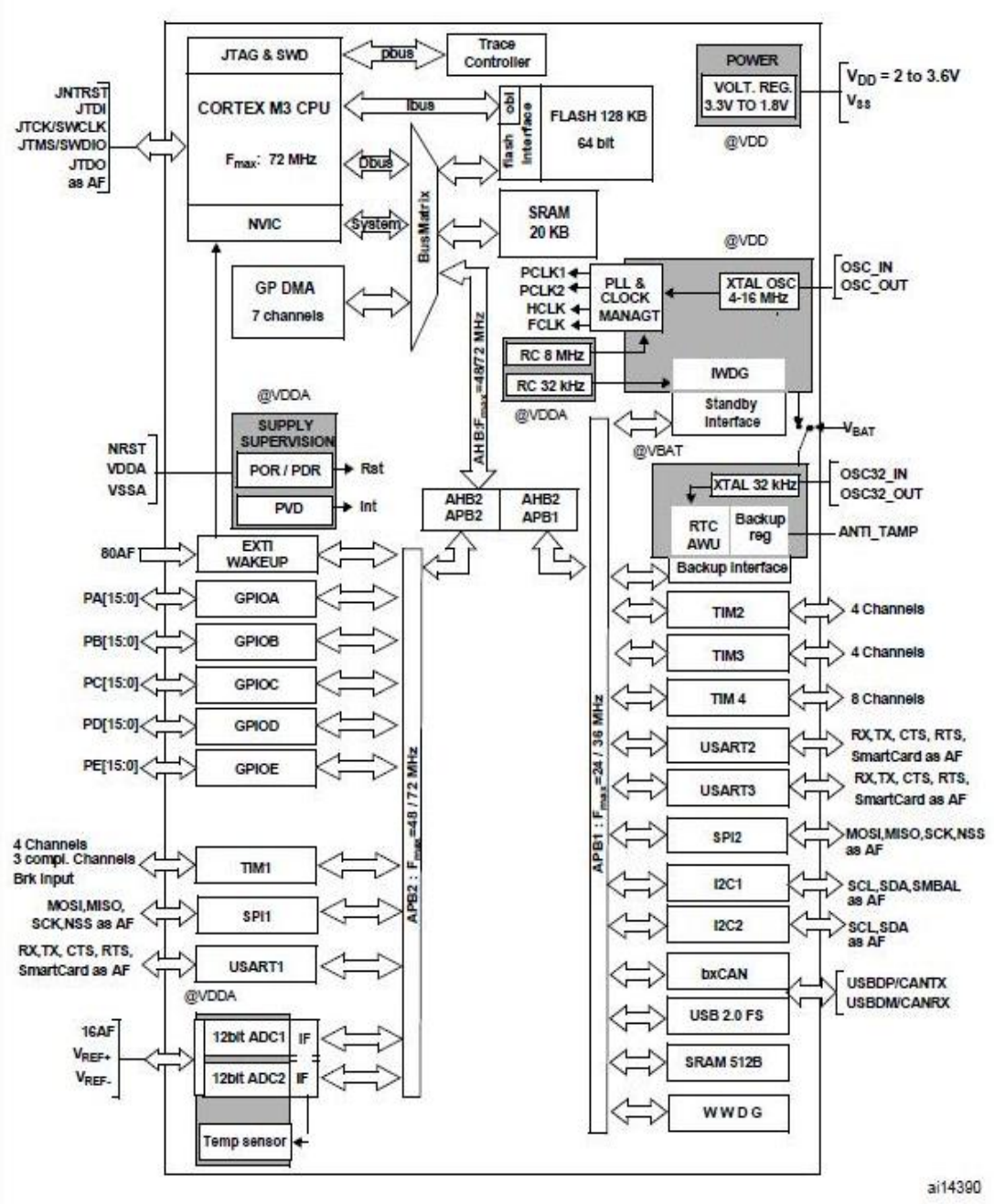

Рис. 3. Структурная схема STM32f103c8

Характеристики:

- Память: 64 kB Flash, 20 kB RAM
- 32-битная архитектура ARM CORTEX-M3, тактовая частота до 72МГц, 1.25MIPS/MHz
- Напряжение питания 3.3В (2.7-3.6)

Для передачи информации между контроллерами был выбран радиопередатчик HC-12. Это полудуплексный беспроводной последовательный модуль связи со 100 каналами в диапазоне 433.4-473.0 МГц, способный передавать данные на расстояние до 1 км [14].

Запланировано создание программных модулей, способных воссоздать самоорганизующуюся сеть наподобие ZigBee [6] или XBee [20]. Далее представлены характеристики передатчика HC-12.

Характеристики:

- Рабочая частота – 433,4 – 473,0 МГц.
- Используется только внешняя антенна.
- Дальность передачи информации – до 1000 - 1800 м на открытом пространстве в зависимости от режима работы.
- Мощность передатчика – до 100 мВт (доступны настройки для 8 уровней мощности).
- Количество каналов передачи данных – 100.
- Четыре рабочих режима.
- Встроенный микроконтроллер (присутствует на модуле) STM8S003F3.
- Интерфейс для коммуникации с внешними устройствами – UART.
- Потребляемый ток – от 3,6 мА до 16 мА в зависимости от режима работы.
- Пиковое потребление тока – до 100 мА (передача данных).
- Потребление тока в ждущем режиме – 80 мкА.
- Напряжение питания – от 3,2 В до 5,5 В.

2. Криптографическая составляющая. В настоящее время криптографическая защита информации не так широко распространена в сегменте интернета вещей, как того требует актуальное положение дел [1], в большинстве существующих на рынке решений она либо отсутствует, либо реализации, в которых она имеется, гораздо дороже. Для обеспечения безопасной коммуникации устройств в проекте используется криптографическая защита информации. На данный момент на стадии реализации и/или оптимизации программного кода находятся симметричные криптографические алгоритмы AES128, AES256, DES, RC4 и алгоритм с публичным ключом RSA. После реализации программных кодов алгоритмов запланирована оценка эффективности с учетом времени, затрачиваемого на обработку потока данных, стойкости к криптографическому анализу и энергопотребления на опытных образцах аппаратной части проекта. В случае неудовлетворительного результата будет выполняться дальнейшая оптимизация программного кода.

Система криптографической защиты информации в проекте строится следующим образом: поток обрабатываемых данных шифруется с помощью симметричного алгоритма, например, AES256 (в процессе генерации секретного ключа участвует алгоритм RC4 с учетом всех требований, повышающих его криптографическую стойкость [16]), а передача ключа шифрования происходит посредством асимметричного алгоритма, например, RSA. Объяснением выбора именно такой конфигурации системы шифрования является то, что симметричные алгоритмы требуют меньше времени на зашифровывание и расшифровывание информации по сравнению с асимметричными [15], а уровень криптографической стойкости определенных из них алгоритмов, например, все тот же AES256, достаточно высок [3]. Асимметричные криптографические алгоритмы затрачивают гораздо больше ресурсов, однако они позволяют передавать информацию (конкретный пример – ключ шифрования для симметричного алгоритма) в зашифрованном виде по незащищенным каналам передачи информации, при этом обеспечивая достаточный уровень защиты.

При использовании вышеупомянутой конфигурации системы шифрования данных происходит оптимальный расход ресурсов и обеспечивается достаточный уровень защиты передаваемых данных.

Результаты Заутера и Тройтля показывают, что расчет алгоритма Диффи-Хеллмана, применяемый в асимметричных криптосистемах, требует значительных вычислительных затрат, в результате чего операция зашифровывания выполняется на контроллере в тысячу раз медленнее, чем зашифровывание симметричным алгоритмом. С этой точки зрения предпочтительнее использовать исключительно симметричную инфраструктуру ключей.

В качестве симметричного алгоритма шифрования предлагается применить ARC4 (alleged RC4). Это один из наиболее простых с точки зрения программной реализации алгоритмов шифрования, который не требует значительных вычислительных ресурсов [19, 4]. Вместе с тем этот алгоритм должен использоваться с большой осторожностью в силу большого количества потенциальных уязвимостей. Требуется дополнительное исследование возможных уязвимостей алгоритма при реализации инфраструктуры симметричных ключей.

Заключение. В статье описывается технология обеспечения безопасной коммуникации между маломощными устройствами, в частности, статья является предложением концепции данной технологии в виде конкретной вариации реализации, с использованием определенной аппаратной части в совокупности с уже проверенными криптографическими алгоритмами. В ходе дальнейшей работы запланирована разработка программного обеспечения для обработки переданной и принятой информации, а также проверка уровня безопасности при передаче данных.

Благодарности. Исследование поддержано Российским Фондом Фундаментальных Исследований, гранты 17-07-00351 (Миронов К. В.) и 19-07-00972 (Махмутов А. Р.).

СПИСОК ЛИТЕРАТУРЫ

1. Безопасный умный дом: сложная технология, полезная каждому. Режим доступа: http://news.ifmo.ru/ru/startups_and_business/startup/news/5832/ (дата обращения 14.05.18)
2. Попытка подружиться с STM32. Режим доступа: https://geektimes.com/post/255334/ (Дата посещения 19.04.18)
3. Почему 256 бит хватит навсегда. Режим доступа: https://xakep.ru/2012/12/28/59888/ (Дата посещения 03.05.18)
4. Свойства программно реализуемых поточных шифров: На примере RC4, GI, Веста. Режим доступа: http://www.dissercat.com/content/svoistva-programmno-realizuemykh-potochnykh-shifrov-na-primere-rc4-gi-vesta (дата посещения 25.04.18)
5. Число умных домов в Европе и Северной Америке. Режим доступа: https://iot.ru/gorodskaya-sreda/kolichestvo-umnykh-domov-v-evrope-i-severnoy-amerike-v-2016-godu-dostiglo-30-3-mln (дата посещения 17.05.18)
6. ZigBee: Взгляд вглубь. Режим доступа: http://www.kit-e.ru/articles/wireless/2005_4_144.php (дата посещения 22.04.18)
7. S. Fuloria, R. Anderson, F. Alvarez, K. McGrath. Key management for substations: Symmetric keys, public keys or no keys? // IEEE/PES Power Systems Conference and Exposition (PSCE) 20-23 March 2011. 2011. Pp.1–6.

8. Sungwook Kim, Eun Young Kwon, Myungsun Kim, Jung Hee Cheon, Seong-ho Ju, Yong-hoon Lim, Moon-seok Choi. A Secure Smart-Metering Protocol Over Power-Line Communication // IEEE Trans. on Power Delivery. Oct. 2011. vol.26. no.4. Pp. 2370–2379.
9. Nian Liu, Jinshan Chen, Lin Zhu, Jianhua Zhang, Yanling He. A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid // IEEE Trans. on Industrial Electronics. Oct. 2013. vol. 60. no. 10. Pp. 4746–4756.
10. A. Treytl, T. Sauter. Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System // Int. Symp. on Power Line Communications and its Applications (ISPLC). Vancouver. 2005. Pp. 66–70.
11. A Glossary of Cryptographic Algorithms. Available at: https://www.globalsign.com/en-sg/blog/glossary-of-cryptographic-algorithms/ (accessed 01.05.18)
12. ATmega 2560 Dtasheet. Available at: http://www.alldatasheet.com/datasheet-pdf/pdf/107092/ATMEL/ATMEGA2560.html (accessed 29.04.18)
13. ATmega 328P Datasheet. Available at: http://mkprog.ru/wpcontent/uploads/2017/09/ATmega328-328P_Datasheet.pdf (accessed 05.05.18)
14. HC-12 Receiver Datasheet. Available at: http://avrproject.ru/112/rf_hc12/2016-01-14_122335_HC-12_v2.3B.pdf (accessed 29.04.18)
15. Hierarchical Key Management for Smart Grids. Available at: https://ieeexplore.ieee.org/document/7302803/ (accessed 04.05.18)
16. RC4 Vulnerabilities. Available at: https://paginas.fe.up.pt/~ei10109/ca/rc4-vulnerabilities.html (accessed 23.04.18)
17. STM32F405 Datasheet. Available at: http://www.st.com/resource/en/datasheet/dm00037051.pdf (accessed 29.04.18)
18. STM32F4Discovery Datasheet. Available at: http://www.st.com/en/evaluation-tools/stm32f4discovery.html (accessed 25.04.18)
19. What is RC4. Available at https://paginas.fe.up.pt/~ei10109/ca/rc4.html (accessed 23.04.18)
20. XBee Datasheet. Available at: https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf (accessed 20.04.18)

UDK 004

SECURE COMMUNICATION TECHNOLOGY FOR DEVICES WITH LIMITED RESOURCES

Amir R. Makhmutov
Student, Ufa state aviation technical university, 12, Karl Marx Str., 450008, Ufa, Russia, e-mail: makhmutovamir15@gmail.com
Nikita I. Vysotskiy
Student, Ufa state aviation technical university, 12, Karl Marx Str., 450008, Ufa, Russia, e-mail: chubays123@ya.ru
Konstantin V. Mironov
PhD., Senior Lecturer, Ufa state aviation technical university, 12, Karl Marx Str., 450008, Ufa, Russia, Researcher, Ural Federal University, 19, Mira Str., 620002, Ekaterinburg, Russia, e-mail: mironovconst@gmail.com
Marcus Meisel
Univ.Ass. Dipl.-Ing., Institute of Computer Technology, Technische Universität Wien, 1040 Wien, Gußhausstraße 25-27, e-mail: marcus.meisel@tuwien.ac.at
Thilo Sauter
Ao.Univ.Prof. Dipl.-Ing. Dr.techn., Institute of Computer Technology, Technische Universität Wien, 1040 Wien**,** Gußhausstraße 25-27**,** e-mail: Thilo.sauter@donau-uni.ac.at

Abstract: The paper contains a proposal for a secure data transmission technology. This technology can be used to build various low-power wireless networks, for example, in smart home systems, industrial wireless sensor networks, communication networks of Smart Grids. The peculiarity of such networks is that the devices from which they consist do not have sufficient power to support execution of asymmetric crypto algorithms.

Keywords: wireless networks, secure communication, cryptography, microcontrollers.

Acknowledgements. The research is supported by the Russian Fund for Basic Research, grant 17-07-00351 (Konstantin Mironov) and 19-07-00972 (Amir Makhmutov).

References

1. Bezopasnyy umnyy dom: slozhnaya tekhnologiya, poleznaya kazhdomu [Safe smart home: a complex technology, useful to everyone]. Available at: http://news.ifmo.ru/ru/startups_and_business/startup/news/5832/ (accessed 14.05.18) (in Russian)
2. Popytka podruzhit'sya s STM32 [How to start working with STM32]. Available at: https://geektimes.com/post/255334/ (accessed 19.04.18) (in Russian)
3. Pochemu 256 bit khvatit navsegda [Why 256 bits is enough forever]. Available at: https://xakep.ru/2012/12/28/59888/ (accessed 03.05.18) (in Russian)

4. Svoystva programmno realizuyemykh potochnykh shifrov: Na primere RC4, GI, Vesta [Properties of software-implemented stream ciphers for the example RC4, GI, Vesta]. Available at: http://www.dissercat.com/content/svoistva-programmno-realizuemykh-potochnykh-shifrov-na-primere-rc4-gi-vesta (accessed 25.04.18) (in Russian)
5. Chislo umnykh domov v Yevrope i Severnoy Amerike [Number of smart homes in Europe and North America]. Available at: https://iot.ru/gorodskaya-sreda/kolichestvo-umnykh-domov-v-evrope-i-severnoy-amerike-v-2016-godu-dostiglo-30-3-mln (accessed 17.05.18) (in Russian)
6. ZigBee: Vzglyad vglub' [ZigBee: Looking Deeper]. Available at: http://www.kit-e.ru/articles/wireless/2005_4_144.php (accessed 22.04.18) (in Russian)
7. S. Fuloria, R. Anderson, F. Alvarez, K. McGrath. Key management for substations: Symmetric keys, public keys or no keys? // IEEE/PES Power Systems Conference and Exposition (PSCE) 20-23 March 2011. 2011. Pp.1–6.
8. Sungwook Kim, Eun Young Kwon, Myungsun Kim, Jung Hee Cheon, Seong-ho Ju, Yong-hoon Lim, Moon-seok Choi. A Secure Smart-Metering Protocol Over Power-Line Communication // IEEE Trans. on Power Delivery. Oct. 2011. vol.26. no.4. Pp. 2370–2379.
9. Nian Liu, Jinshan Chen, Lin Zhu, Jianhua Zhang, Yanling He. A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid // IEEE Trans. on Industrial Electronics. Oct. 2013. vol. 60. no. 10. Pp. 4746–4756.
10. A. Treytl, T. Sauter. Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System // Int. Symp. on Power Line Communications and its Applications (ISPLC). Vancouver. 2005. Pp. 66–70.
11. A Glossary of Cryptographic Algorithms. Available at: https://www.globalsign.com/en-sg/blog/glossary-of-cryptographic-algorithms/ (accessed 01.05.18)
12. ATmega 2560 Dtasheet. Available at: http://www.alldatasheet.com/datasheet-pdf/pdf/107092/ATMEL/ATMEGA2560.html (accessed 29.04.18)
13. ATmega 328P Datasheet. Available at: http://mkprog.ru/wpcontent/uploads/2017/09/ATmega328-328P_Datasheet.pdf (accessed 05.05.18)
14. HC-12 Receiver Datasheet. Available at: http://avrproject.ru/112/rf_hc12/2016-01-14_122335_HC-12_v2.3B.pdf (accessed 29.04.18)
15. Hierarchical Key Management for Smart Grids. Available at: https://ieeexplore.ieee.org/document/7302803/ (accessed 04.05.18)
16. RC4 Vulnerabilities. Available at: https://paginas.fe.up.pt/~ei10109/ca/rc4-vulnerabilities.html (accessed 23.04.18)
17. STM32F405 Datasheet. Available at: http://www.st.com/resource/en/datasheet/dm00037051.pdf (accessed 29.04.18)
18. STM32F4Discovery Datasheet. Available at: http://www.st.com/en/evaluation-tools/stm32f4discovery.html (accessed 25.04.18)
19. What is RC4. Available at https://paginas.fe.up.pt/~ei10109/ca/rc4.html (accessed 23.04.18)
20. XBee Datasheet. Available at: https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf (accessed 20.04.18)