УДК 004

О РАЗРАБОТКЕ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ СЕНСОРНЫХ СЕТЕЙ

А. Р. Махмутов [2], А. М. Вульфин [1], К. В. Миронов [3]

[1] vulfin.alexey@gmail.com, [2] makhmutovamir15@gmaail.com, [3] mironovconst@gmail.com

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. Статья посвящена проблеме использования традиционных криптографических алгоритмов на малоресурсных микроконтроллерах *ATmega328P*. Производительность микроконтроллеров оценивалась при работе с криптографическими алгоритмами и хеш-функциями. На основании полученных результатов разработаны рекомендации по созданию систем безопасной передачи данных для промышленных гетерогенных сетей, сочетающих устройства с ограниченными вычислительными возможностями.

Ключевые слова: криптография, хеш-функции, микроконтроллер, распределенный реестр, Интернет вещей, распределенная сенсорная сеть, информационная безопасность.

ВВЕДЕНИЕ

В современном мире быстро растут объемы распределенных сенсорных сетей, равно как и сетей Интернета вещей и других разновидностей сетей связи «машина-машина» (M2M) [1]. На рис. 1 схематически представлена типичная архитектура таких сетей. В этой архитектуре устройства разделены на уровни от нижнего уровня (датчики, исполнительные механизмы и оконечные устройства) до верхнего (различные серверы). Обычно такие сети имеют дендритную структуру, в которой несколько ветвей нижнего уровня соединяются с одной ветвью верхнего уровня.

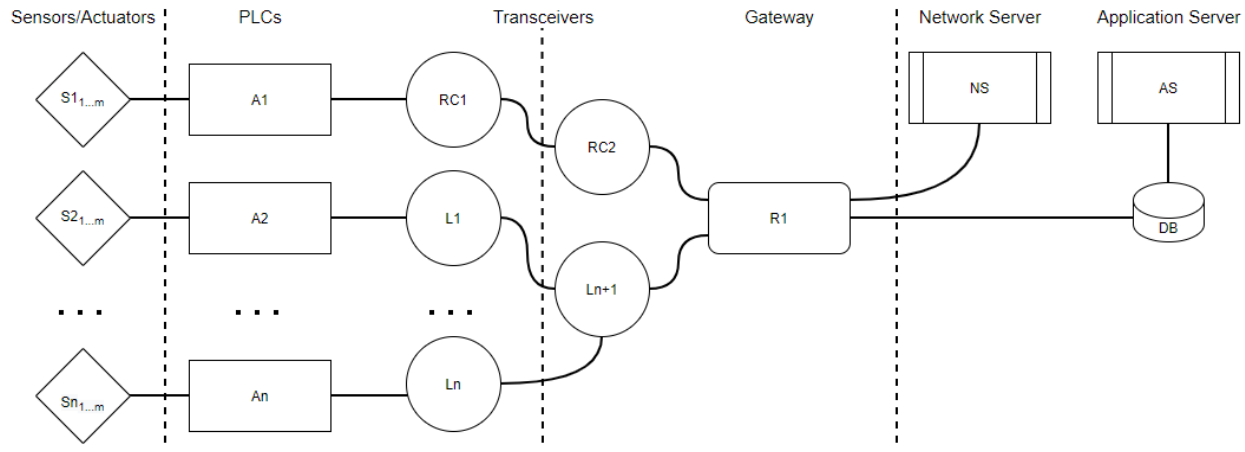

Рис. 1. Типичная сеть *IoT* в схематическом виде

Как и любые другие компьютерные сети, сети *IoT* также требуют применения мер ЗИ. В большинстве случаев есть как минимум один важный момент. Оборудование, используемое на низких уровнях, имеет низкие вычислительные возможности. Это связано с габаритами и энергопотреблением используемого оборудования. Этот нюанс является одним из движущих

факторов актуальности исследовательских работ по применению криптографических алгоритмов на устройствах с ограниченными ресурсами. Например, с точки зрения российского законодательства важность таких исследований явно показана в Приказе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 113 [2]. Эта тема популярна и за рубежом.

В этой работе будут рассмотрены широко используемые криптографические алгоритмы и хэш-функции, а также популярное и доступное оборудование. Также в этой статье мы дадим краткое описание разработанного стенда, имитирующего сегмент промышленного Интернета вещей (*IIoT*). Результаты важны с точки зрения исследований в области легковесной криптографии, поскольку их можно рассматривать как отправную точку в таких работах. Из этой же группы статей можно выделить следующие: [3], [4], [5], [6]. В упомянутых выше статьях мы можем найти различные аспекты применения криптографических алгоритмов на устройствах с ограниченными ресурсами и в распределенных сенсорных сетях.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Современные СЗИ для классических компьютерных сетей и сетей M2M используют различные криптографические алгоритмы. Это означает, что могут применяться алгоритмы шифрования, хэш-функции, алгоритмы *HMAC* и *CMAC*. В соответствии со спецификациями используемого в сетях M2M оборудования, в эту статью также включены разработанные ключевые требования к защите данных в таких сетях. Из-за невысокой вычислительной мощности рассматриваемого оборудования основной целью данной статьи является определение работоспособности криптографических алгоритмов на одноплатных микроконтроллерах на базе *ATmega328 (AVR)*. Полный список микроконтроллеров на базе *ATmega328 (AVR)* включает следующие: *Arduino Nano, Arduino Uno, Arduino Mini, Arduino Pro Mini, LilyPad Arduino, Arduino Pro, Arduino Fio*. Их технические характеристики приведены в таблице 1 [7 - 13]. Микропроцессор *ATmega328* был выбран из-за его высокой популярности и широкого применения во многих одноплатных микроконтроллерах, таких как *Arduino* и другие. Согласно [16], самой популярной платой *Arduino* среди всего семейства является *Uno*, ее доля составляет 55,1%. *Nest* идет *Arduino Nano* с популярностью 8,7%. Для этой работы был выбран самый популярный одноплатный микроконтроллер с самым популярным чипом. В таблице 1 представлены основные характеристики плат *Arduino* с процессором *ATmega328.*

Таблица 1

Сводная таблица характеристик

Характеристика	*Модели одноплатных микроконтроллеров*					
	Nano	*Uno*	*Mini*	*Pro Mini*	*Pro*	*Fio*
Напряжение, В	7-12	7-12	7-9	5-12	5-12	3.35-12
Цифровые контакты	14					
Аналоговые контакты	6	6	8	8	6	8
Flash память, КБ	32	32	32	16	32	32
SRAM, КБ	2	2	2	1	2	2
EEPROM, КБ	1	1	1	0.5	1	1
Тактовая частота, МГц	16					8

Данная работа проводилась в рамках разработки системы защищенной передачи данных для распределенной сенсорной сети. Соответственно, для этой работы использовались готовые аппаратные сборки. Такие сборки играют роль конечных устройств. Сборка имеет следующий принцип работы. После замыкания цепи питания кнопкой ВКЛ/ВЫКЛ напряжение от аккумулятора 18650 в диапазоне 3,2-4,2 В поступает на трансформатор, который выдает стабильные 5 В независимо от входного напряжения с аккумулятора. Это напряжение подается на контакты макетной платы, от которых питаются все остальные элементы: радиомодуль,

дисплей, датчик и микроконтроллер. Информация с датчика поступает в микроконтроллер и отображается на экране. С помощью радиомодуля микроконтроллер передает и принимает информацию по радиоканалу с частотой 433 МГц.

Следует отметить, что такой набор оборудования способен имитировать любое конечное устройство потребительского сегмента Интернета вещей. Кроме того, такой набор похож на устройства, которые используются в качестве конечных точек в промышленном Интернете вещей. Комплект используемого оборудования показан на рис. 2. Программное обеспечение разработано с помощью *Arduino IDE* с синтаксисом языка *C*. Результат алгоритма *AES* в режиме ECB с разной длиной ключа, алгоритма *AES* в режиме *CTR* с длиной ключа 128 бит, алгоритма *SHA-3* и алгоритма *SHA256* показаны в таблице 2.

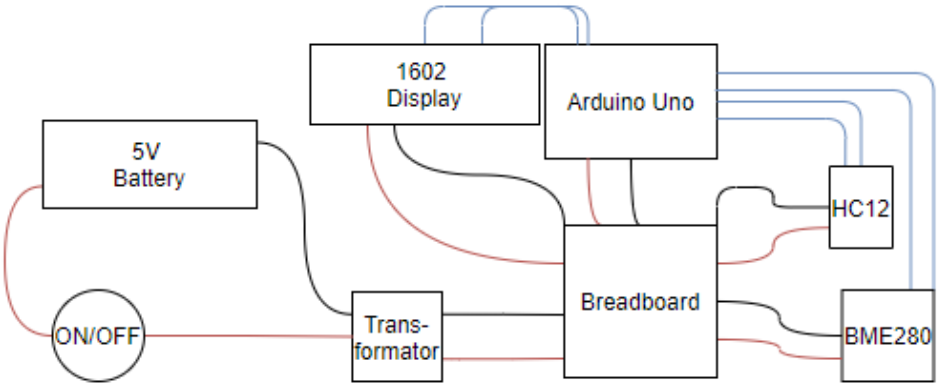

Рис. 2. Состав тестируемой сборки

Таблица 2

Сводная таблица результатов работы криптоалгоритмов

Алгоритм	*Режим*	*Результат, Б/с*
AES128 ECB	Шифрование	30 028,99
AES128 ECB	Расшифровка	13 860,32
AES192 ECB	Шифрование	25 016,10
AES192 ECB	Расшифровка	11 435,89
AES256 ECB	Шифрование	21 437,42
AES256 ECB	Расшифровка	9 733,36
AES128 CTR	Шифрование	27 758,50
AES128 CTR	Расшифровка	27 753,16
SHA-3	Хэширование	16 632,07
SHA256	Хеширование	22 345,31

Данные о памяти, занимаемой программами на плате *Arduino Uno*, приведены в Таблице 3.

Таблица 3

Занимаемая программными кодами память

Алгоритм	*Используемая флэш-память, байты (% от общего пространства)*	*Используемая динамическая память, байт (% от общего пространства)*
AES ECB	8318 (25)	1388 (67)
AES CTR	9078 (28)	1316 (64)
SHA-3	11610 (35)	1708 (83)
SHA 256	11064 (34)	1146 (55)

ОСНОВНЫЕ ЭТАПЫ НАЧАЛА РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ В БЕЗОПАСНЫХ РАСПРЕДЕЛЕННЫХ СЕНСОРНЫХ СЕТЯХ

Логика СЗИ в различных M2M сетях, включая распределенные сенсорные сети и сети *IoT*, выглядит следующим образом. На уровнях архитектуры выше шлюза ЗИ обеспечивается стандартными методами и не будет рассматриваться в этой статье. Сосредоточимся на части архитектуры ниже уровня шлюза. Как правило, любая успешная реализация любой атаки приводит к нарушению целостности и/или доступности и/или конфиденциальности информации, содержащейся в распределенной сенсорной сети. Соответственно, чтобы предотвратить это, защитные меры должны быть разработаны и реализованы еще на этапе проектирования любой новой распределенной сенсорной сети. Это решение поможет минимизировать возможные негативные последствия. Основываясь на наиболее популярных способах нарушения целостности, конфиденциальности и доступности информации, содержащейся в распределенных сенсорных сетях, были разработаны меры по защите информации в таких сетях. Также в таблице 4 показаны способы реализации разработанных требований. Следует отметить, что эти способы актуальны для распределенных сенсорных сетей и других сетей, содержащих оборудование с низким энергопотреблением и малой вычислительной мощностью.

Таблица 4

Требования к разработке систем защиты информации и мер их реализации

Требование	*Реализация*
Шифрование полезной нагрузки до передачи	Использование криптостойких симметричных алгоритмов
Наличие механизма контроля целостности	Использование функций хэширования, контрольных сумм или HMAC/CMAC
Высокая масштабируемость	Использование простых механизмов аутентификации устройств в сети
Наличие нескольких способов активации устройств	Использование способа"по воздуху" и "с завода"
Наличие фильтрации по силе принятого сигнала	Использование фильтра на основе RSSI
Наличие механизма игнорирования скомпрометированных устройств	Использование уникальных идентификаторов и черных/белых списков
Наличие мониторинга состояния устройств в сети	Периодическая рассылка сервисных сообщений
Постоянное применения мер ЗИ	Применение мер ЗИ абсолютно ко всем передаваемым данным
Исполнение оконечных устройств в едином блоке (по возможности)	Использование моноблочных корпусов. Если такие устройства не находятся под контролем, их необходимо размещать в незаметном или труднодоступном месте. По возможности это должны быть прочные корпуса, которые трудно вскрыть.
Наличие эталонной информации для оценки релевантности получаемых данных	Внедрение небольших обновляемых банков данных на шлюзе или сервере базы данных.
Возможность анализа степени зашумленности радиоканала	Регулярное прослушивание радиоэфира шлюзом. Информирование при высоком уровне шума используемого радиоканала
Контроль целостности используемого ПО	Наличие контрольных сумм

Исходя из широко используемых особенностей и особенностей функционирования распределенных сенсорных сетей, можно выделить, что наивысшим приоритетом в обеспечении защиты передаваемых данных является защита их целостности.

ЗАКЛЮЧЕНИЕ

В этой статье мы дали краткое описание разработанного стенда моделирования. Статья содержит анализ применимости популярных криптографических алгоритмов. В статье дано подробное описание состава тестовой аппаратной сборки.

На основании полученных результатов были сделаны следующие выводы:

- Протестированные алгоритмы нельзя использовать на платах *Arduino Pro Mini* из-за недостатка памяти.
- Другие платы Arduino на базе *ATmega328* способны работать как с проверенными криптографическими алгоритмами, так и с более легковесными.
- Для шифрования полезной нагрузки передаваемых сообщений рекомендуется использовать криптографические алгоритмы, требующие не более память не более, чем *AES128 CTR*. В противном случае будет нехватка оперативной памяти устройства для других функций.
- Хеш-функцию *SHA256* можно использовать для контроля целостности передаваемых сообщений, оставляя достаточно места в памяти для остальных функций программы.
- При использовании плат *Arduino* на микроконтроллере *ATmega328* невозможно использовать алгоритмы *AES* и *SHA256* на одном устройстве. Чтобы иметь возможность использовать как шифрование полезной нагрузки, так и контроль целостности при передаче информации в сетях M2M, необходимо использовать более легкие алгоритмы.

Результат тестирования производительности при работе с хеш-функциями показал, что указанные одноплатные микроконтроллеры (за исключением *Arduino Pro Mini*) имеет смысл проверить на возможность работы с распределенными реестрами, так как в таких система также применяется алгоритм *SHA256*. Необходимо продолжить такие исследования с использованием облегченных симметричных алгоритмов, а также российских шифров Магма, Кузнечик, Стрибог.

СПИСОК ЛИТЕРАТУРЫ

1. Прогноза развития Интернета вещей до 2030 года. URL:https://mipt.ru/upload/06d/92-96-arphj8g0g1k.pdf (дата обращения: 11.02.2022).

2. Приказ Министерства цифрового развития №113 от 29 Марта 2019 «Об утверждении Концепции построения и развития сетей узкополосной беспроводной связи «Интернет вещей» в Российской Федерации»

3. Легковесная криптография. Часть 1. URL: https://cyberleninka.ru/article/n/legkovesnaya-kriptografiya-chast-1 (дата обращения: 11.02.2022).

4. Легковесная криптография. Часть 2. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_10_01.pdf (дата обращения: 11.02.2022).

5. N. Vysotskiy, A. Makhmutov, K. Mironov, M. Meisel, T. Sauter, “Secure Communication Technology for Devices with Limited Resources”, Advances in Intelligent Systems Research, volume 158, pp. 207-210, Atlantis Press, 2018.

6. 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.

7. Список плат Ардуино. URL:https://doc.arduino.ua/ru/hardware/ (дата обращения: 23.10.2021).

8. Характеристики Arduino Uno. URL: https://doc.arduino.ua/ru/hardware/Uno (дата обращения: 24.10.2021)

9. Характеристики Arduino Mini. URL:https://doc.arduino.ua/ru/hardware/Mini (дата обращения: 24.10.2021)

10. Характеристики Arduino Nano. URL:https://doc.arduino.ua/ru/hardware/Nano (дата обращения: 24.10.2021)

11. Характеристики Arduino Pro Mini. URL:https://doc.arduino.ua/ru/hardware/ProMini (дата обращения: 24.10.2021)

12. Характеристики Arduino Pro. URL:https://doc.arduino.ua/ru/hardware/Pro (дата обращения: 24.10.2021)

12. Характеристики Arduino Fio. URL:https://doc.arduino.ua/ru/hardware/Fio (дата обращения: 24.10.2021)

13. Исследование Hewlett Packard Enterprise IoT. URL:https://json.tv/tech_trend_find/nauchnoe-issledovanie-interneta-veschey-ot-hewlett-packard-enterprise-20160503115845 (дата обращения: 15.01.2022)

14. K. Mironov, A. Makhmutov, V. Kartak, S. Trishin. Proceedings of the Seventh All-Russian Scientific Conference with International Participation INFORMATION TECHNOLOGIES AND SYSTEMS. Khanty-Mansiysk, Russia, March 12-16, 2019. - pp. 107-111.

15. Популярность среди плат Ардуино. URL:https://www.sparkfun.com/news/1982 (дата обращения: 10.02.2022).

ОБ АВТОРАХ

МАХМУТОВ Амир Рашитович, аспирант 2-го курса ФИРТ.
ВУЛЬФИН Алексей Михайлович, к.т.н., доцент каф. ВТиЗИ.
МИРОНОВ Константин Валерьевич, к.т.н., ст. преподаватель каф. ВТиЗИ.

METADATA

Title: On Developing Secure Distributed Sensor Networks

Affiliation: Ufa University of Science and Technology (UUST), Russia.

Email: [1]vulfin.alexey@gmail.com, [2]makhmutovamir15@gmaail.com, [3]mironovconst@gmail.com

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 1 (27), pp. 69-74, 2023. ISSN 2225-9309 (Print).

Abstract: This paper is devoted to the problem of using traditional cryptographic algorithms on low-resource ATmega328P microcontrollers. The performance of microcontrollers was assessed during working with cryptographic algorithms and hash functions. Based on received results, recommendations have been developed for the developing of secure data transmission systems for industrial heterogeneous networks that combine devices with limited computing capabilities.

Key words: cryptography, hash functions, microcontroller, distributed ledger, internet of things, distributed sensor network, information security.

About authors:

MAKHMUTOV, Amir Rashitovich, postgraduate student 2 year, Ufa state aviation technical University.

VULFIN, Alexey Mikhailovich, Ph.D., associate professor, Ufa state aviation technical University.

MIRONOV, Konstantin Valeryevich, PhD, art. Teacher, Ufa state aviation technical University.