Обеспечение безопасности в системах Интернета вещей методом малой криптографии

Security in Systems Internet of Things by the Method of Low-Resource Cryptography

УДК 004.021
Получено: 19.10.2021 Одобрено: 04.11.2021 Опубликовано: 25.12.2021

Супрун А.Ф.
Канд. техн. наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург
e-mail: afs 54@inbox.ru

Suprun A.F.
Candidate of Technical Sciences, Associate Professor, Peter the Great St. Petersburg Polytechnic University, St. Petersburg
e-mail: afs54@inbox.ru

Веселко А.А.
Канд. экон. наук, старший преподаватель кафедры таможенного дела Российского университета дружбы народов

Veselko A.A.
Candidate of Economic Sciences, Senior Lecturer of Customs Department, Peoples' Friendship University of Russia,
e-mail: veselko-aa@rudn.ru

Кастырин М.А.
аспирант кафедры таможенного дела Российского университета дружбы народов

Kastyrin M.A.
Postgraduate Student, Customs department, Peoples' Friendship University of Russia,

Аннотация
Предложен подход к обеспечению безопасности протоколов взаимодействия между узлами Интернета вещей, основой которого является применение средств низкоресурсной криптографии.
Взаимодействие между узлами Интернета вещей отличаются требованиями низкой нагрузки на узлы сети, малого объема пересылаемых данных и ограничениями энергопотребления узлов.
Предлагается использовать протокол, допускающий применение в сетях на базе маломощных вычислителей, с низкой пропускной способностью.
Ключевые слова: Интернет вещей, взаимодействие, низкоресурсная криптография, протокол.

Abstract
An approach to ensuring the security of protocols of interaction between nodes of the Internet of Things is proposed, the basis of which is the use of low-resource cryptography. The interaction between the nodes of the Internet of Things is characterized by the requirements of low load on

the nodes of the network, a small amount of transmitted data and restrictions on the energy consumption of nodes. It is proposed to use a protocol that allows use in networks based on low-power computers with low bandwidth.
Keywords: Internet of Things; interaction; low-resource cryptography; protocol.

Введение

IoT (internet of things, далее – Интернет вещей) представляет собой распределенную мультиагентную сеть, осуществляющую автономный сбор и обработку данных об окружающей среде. Интернет вещей имеет представление как в реальном, так и в виртуальном пространстве [1−5].

В последнее десятилетие наблюдается лавинообразный рост числа агентов ИВ: на февраль 2017 г. число упомянутых агентов составило порядка 10 миллиардов устройств. По прогнозам экспертов, к 2024 г. количество агентов Интернета вещей по всему миру может достигнуть 60 миллиардов устройств, а по самым оптимистичным прогнозам развития отрасли – 80 миллиардов. Подобный массив устройств, несмотря на малую среднюю мощность, нельзя оставлять беззащитным [6−11]. Это подтверждается значительными последствиями в результате пренебрежения безопасностью Интернета вещей [12−16]. Примерами могут служить нашумевшие в СМИ атаки ботнетов BrickerBot, Amnesia и Mirai, объединившие под собой сотни тысяч устройств, которые впоследствии были использованы для проведения массированных DDOS атак.

Основная часть

Низкоресурсная криптография (Lightweight Cryptography) – раздел криптографии, имеющий своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами (память, электропитание, размеры) для функционирования.

Низкоресурсная криптография позволяет решить проблему низкой производительности агентов Интернета вещей, обеспечив достаточный уровень защищенности системы. Она обладает следующими особенностями:

- применение модифицированных версий классических алгоритмов;
- использование быстрых математических операций;
- адаптация под аппаратуру.

В результате анализа для решения задачи по использованию низкоресурсной криптографии рассмотрены следующие алгоритмы [17, 18]:

- KATAN32, KATAN48, KATAN64;
- PRESENT-80, PRESENT-128;
- HIGHT;
- mCryption;
- LBlock;
- KLEIN-64, KLEIN-80, KLEIN-96;
- XXTEA.

Экспериментальные данные, подтверждающие возможность применения алгоритма, получены для алгоритмов PRESENT-80 и XXTEA [19].

Разработанный протокол позволяет осуществить безопасную аутентификацию устройства, подтвердить его наличие в сети и осуществить безопасный обмен информации с устройством.

Протокол использует следующие средства для выполнения данных задач:

- уникальные метки устройств;
- магические числа;
- шифрование каналов связи с использованием сессионных ключей.

При разработке протокола также были исследованы некоторые важные параметры способа защиты, такие как: минимальные требования к мощности контроллера и скорости передачи данных. Размер передаваемых пакетов в текущей версии минимизирован.

Инициализатором обмена информацией в рамках созданного защищенного соединения может выступать как базовая станция, так и внешний контроллер. Инициализатором замены ключа может выступать только базовая станция. Все наиболее затратные вычисления перенесены на базовую станцию.

На рис. 1 представлена структурная схема модели, задействованная в рамках исследования. Под внешним контроллером подразумевается любой контроллер, выполняющий роль концентратора для датчиков, выполняющий промежуточные вычисления, либо объединение данных для последующей отправки на базовую станцию. В роли агентов выступают маломощные контроллеры датчиков. Далее под внешними контроллерами подразумеваются все элементы сети, кроме базовой станции.

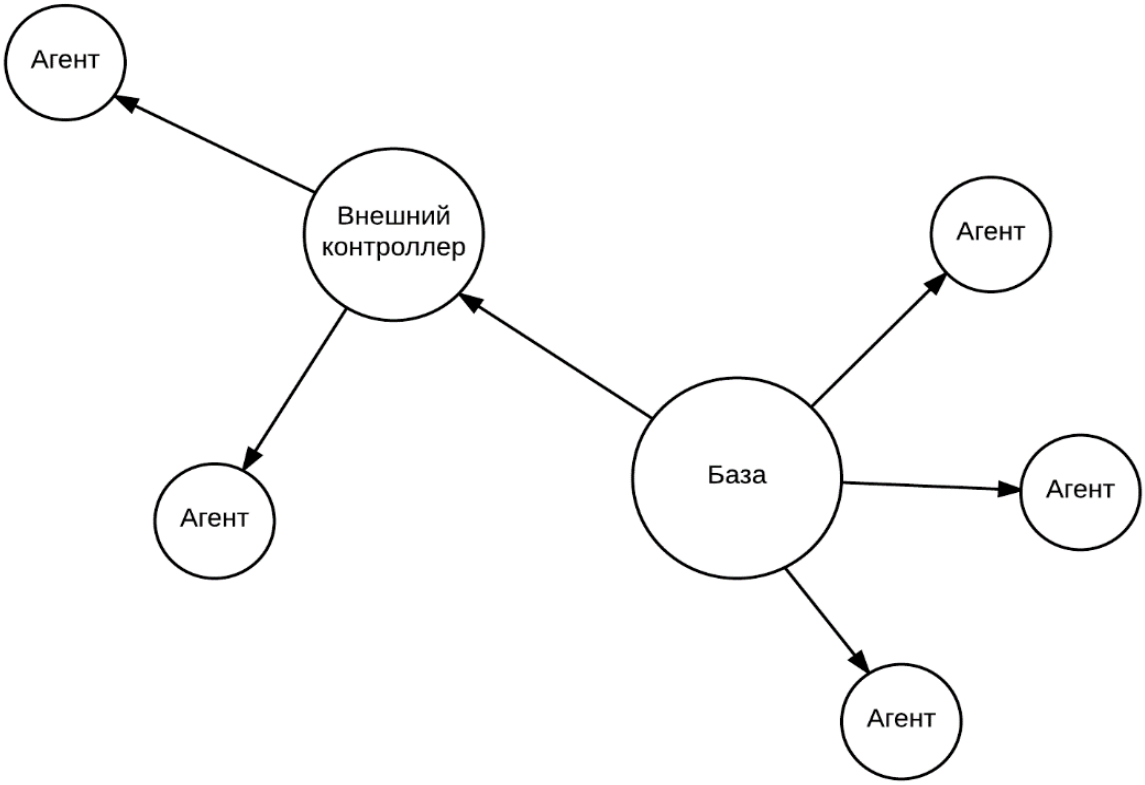


Рис. 1. Схема модели

Рассматривались следующие нарушения безопасности системы в рамках данной работы:

- атаки на отказ в обслуживании внешних датчиков;
- атаки на отказ в обслуживании базовой станции;
- перехват данных канала «базовая станция ←→ внешний контроллер»;
- подделка данных канала «базовая станция ←→ внешний контроллер».

Следующие модели нарушителя рассматривались в рамках данной работы:

- внешний нарушитель (отсутствие доступа в сеть);
- внутренний нарушитель (наличие доступа в сеть);
- внутренний нарушитель (контроль агента сети);
- внутренний нарушитель (подделка агента сети).

Схема алгоритма идентификации представлена на рис. 2. Алгоритм идентификации представлен следующими действиями:

1) Базовая станция отправляет запрос новому устройству. В случае, если устройств подключается несколько – запросы обрабатываются в порядке достижения базовой станции.

2) Если запрос верен – на основе R/O метки устройства происходит генерация основной метки и её установка на базовой станции.

3) Метка пересылается устройству и устанавливается.

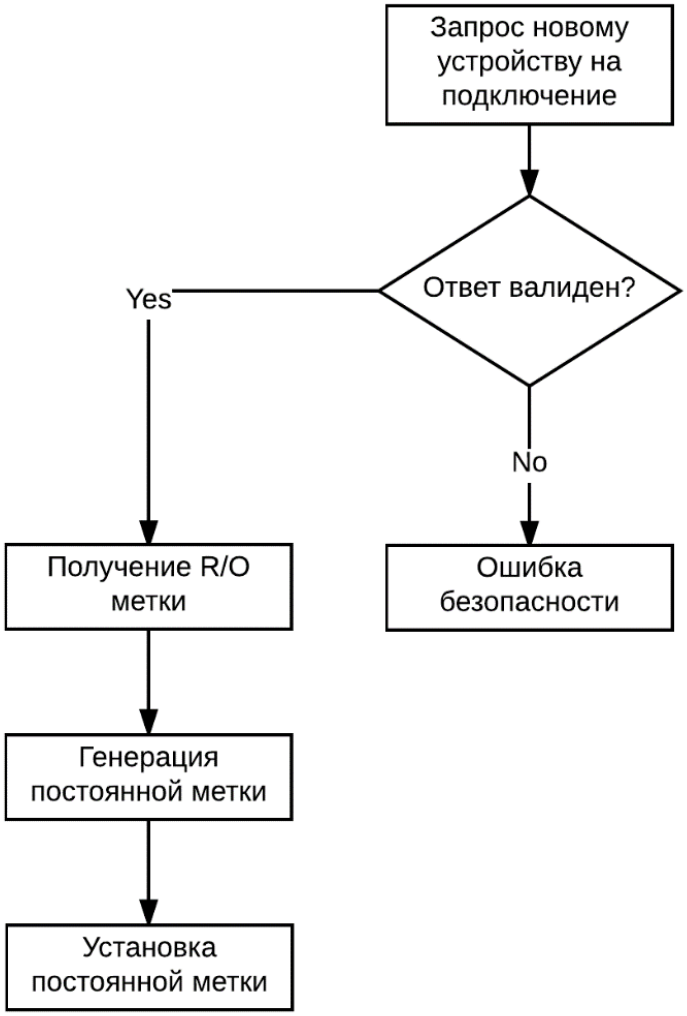


Рис. 2. Алгоритм идентификации

Внешний контроллер может исполнять роль базовой станции, собирая информацию с подчиненных ему агентов. В рамках экспериментов были рассмотрены следующие варианты делегирования:

1) Внешний контроллер получает собственную таблицу ключей и осуществляет взаимодействие с подчиненными агентами аналогично базовой станции, отправляя на неё итоговые данные. Базовая станция не хранит метки подчиненных внешнему контроллеру устройств.

2) Внешний контроллер получает права базовой станции аналогично первому пункту, но не имеет права инициировать замену ключей. Замена производится путем последовательных запросов к базовой станции, при этом базовая станция хранит полный набор меток.

3) Внешний контроллер запрашивает данные с базовой станции при каждом опросе подчиненных агентов.

Текущий протокол использует второй вариант. Таким образом, удалось избежать падения работоспособности внешнего контроллера с увеличением числа его агентов.

Обмен данными осуществляется посредством пакетов, длиной 312 бит. Структура пакета представлена в табл. 1.

Таблица 1

Представление пакета

Заголовок [8 бит]	Флаги [8 бит]	Данные [264 бита]	Магическое число [16 бит]	Метка [16 бит]

Заголовок позволяет устройству идентифицировать пакет и тип устройства, от которого пришло сообщение. Тип устройства применяется для подтверждения корректности пакета.

Поле флагов позволяет точно идентифицировать содержимое пакета и набор процедур, необходимый для его декодирования [20].

Данные, в зависимости от набора флагов, могут содержать либо ключ, либо данные с датчика, либо команду контроллеру. Размер в 264 бита информации позволяют, с одной стороны, достаточны для передачи ключа LW-алгоритма, а, с другой – позволяют закодировать и передать данные или команду без фрагментации [17, 21].

Структура поля представлена в табл. 2.

Таблица 2

Представление поля данных

Длина данных [8 бит]	Данные	Дополнение

Дополнение случайно генерируется отправителем (если поле не занято целиком) и занимает пустое пространство поля данных.

Магическое число используется для подтверждения сеанса общения между внешним контроллером и базовой станцией. Ответное магическое число вычисляется по формуле [22]:

$$Magic_{answ} = Magic + Int(addition)_8 \; mod \; 2^{16}$$

$Magic_{answ}$ – ответное магическое число;

$Magic$ – полученное магическое число;

$Int(addition)_8$ – целочисленное представление последних 8 бит поля данных.

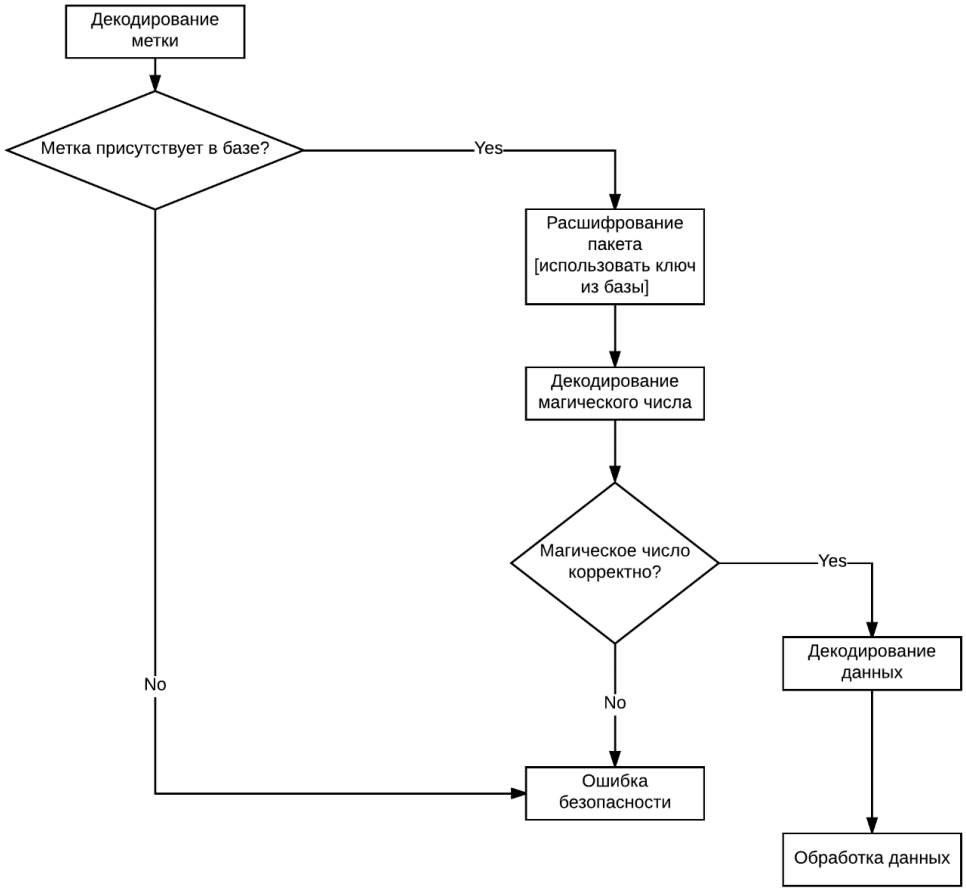
Метка позволяет идентифицировать устройство, с которым происходит общение.

Шифрованию в рамках общения подвергаются поля флагов, данных и магического числа.

Инициализатором общения может являться как базовая станция, так и внешний контроллер.

Алгоритм обработки пакета действиями [23]:

1) проверка существования метки в базе;
2) в случае успеха – расшифровка пакета;
3) декодирование и проверка магического числа;
4) в случае успеха – пакет принят и данные декодируются.



Инициатором обмена является базовая станция. Оптимальным решением для использования в рамках данного протокола является криптография на эллиптических кривых, за счет относительно высокой скорости работы, а также малого размера данных для обмена.

Наиболее перспективным вариантом является применение схемы ECDH для обмена сеансовыми ключами.

Параметры кривой, поставляемой на неинициализированном контроллере, должны храниться в памяти базовой станции без возможности их изменить.

Выводы

В рамках данной работы был разработан протокол, позволяющий устанавливать соединения и обмениваться данными внутри защищенного канала между узлами сети Интернета вещей. Разработанный протокол обладает следующими преимуществами:

- возможность однозначно идентифицировать устройство;
- многоуровневое подтверждение целостности сообщения;
- простота реализации;
- низкие требования к вычислительной мощности компонентов сети;
- низкие требования к пропускной способности канала сети.

Литература

1. *Тебекин А.В.* Квалиметрическая оценка уровня цифровизации экономики в Российской Федерации // Журнал технических исследований. − 2018. − Т. 4. − № 3. − С. 1-13.

2. *Паршина Л.Н., Корнилаев И.* Цифровые технологии в управлении экономикой Казахстана // Журнал технических исследований. − 2019. − Т. 5. − № 1. − С. 8-11.

3. *Анисимов Е.Г.* Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. − 2016. − № 7-8 (97-98). − С. 12-16.
4. *Белов А.С., Добрышин М.М., Шугуров Д.Е.* Алгоритм адаптивного управления удаленной аутентификацией в корпоративных сетях связи // Журнал технических исследований. − 2021. − Т. 7. − № 3. − С. 38-46
5. *Горшенев А.С., Савостикова О.Г.* Применение инструмента 5S в виртуальном рабочем пространстве // Журнал технических исследований. − 2019. − Т. 5. − № 3. − С. 31-36.
6. *Anisimov V.G., Zegzhda P.D., Anisimov E.G., Bazhin D.A.* A risk-oriented approach to the control arrangement of security protection subsystems of information systems // Automatic Control and Computer Sciences. − 2016. − Т. 50. − № 8. − С. 717-721.
7. *Гринюк О.Н., Сысоев К.А., Шевченко Е.В.* Исследование методов защиты информации в облачных сервисах // Журнал технических исследований. − 2019. − Т. 5. − № 1. − С. 12-14
8. *Анисимов В.Г., Селиванов А.А., Анисимов Е.Г.* Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства // Информация и космос. − 2016. − № 4. − С. 76-80.
9. *Зегжда П.Д.* Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем // Проблемы информационной безопасности. Компьютерные системы. − 2018. − № 1. − С. 43-47.
10. *Anisimov, V.G.,Anisimov, E.G.,Zegzhda, P.D.,Saurenko, T.N.,Prisyazhnyuk, S.P.* Indices of the effectiveness of information protection in an information interaction system for controlling complex distributed organizational objects // Automatic Control and Computer Sciences, 2017, 51(8), pp. 824–828. DOI: https://doi.org/10.3103/S0146411617080053.
11. *Гаршин А.П., Супрун А.Ф., Сысуев С.Ю.* Пористые композиционные материалы и повышение защищенности систем обработки информации // Журнал технических исследований. − 2021. − Т. 7. − № 3. − С. 47-57.
12. *Зегжда П.Д.* Методический подход к построению моделей прогнозирования показателей свойств систем информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2019. − № 4. − С. 45-49.
13. *Левашов А.И.* Токенизация в контексте совершенствования системы безопасности мобильных платежей // Журнал технических исследований. − 2019. − Т. 5. − № 3. − С. 54-58.
14. *Anisimov V.G., Anisimov E.G., Saurenko T.N., Zotova E.A.* Models of forecasting destructive influence risks for information processes in management systems // Information and Control Systems. 2019. № 5 (102). С. 18-23.
15. *Сауренко Т.Н.* Прогнозирование инцидентов информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2019. − № 3. − С. 24-28.
16. *Анисимов В.Г., Анисимов Е.Г., Зегжда П.Д., Супрун А.Ф.* Проблема инновационного развития систем обеспечения информационной безопасности в сфере транспорта // Проблемы информационной безопасности. Компьютерные системы. − 2017. − № 4. − С. 27-32.
17. Hannes Gross, Marko Holbl, Daniel Slamanig, and Raphael Spreitzer Privacy-Aware Authentication in the Internet of Things. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2015. – Режим доступа: https://eprint.iacr.org/2015/1110.pdf свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
18. Zheng Gong, Svetla Nikova, and Yee Wei Law KLEIN: A New Family of Lightweight Block Ciphers. [Электронный ресурс] / School of Computer Science, South China Normal University, China, Faculty of EWI, University of Twente, The Netherlands, Dept. ESAT/SCD-

COSIC, Katholieke Universiteit Leuven, Belgium, Department of EEE, The University of Melbourne, Australia. 2012. – Режим доступа: http://www.smartsantander.eu/downloads/Presentations/gong12klein.pdf, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. агл.
19. Ari Keränen, Carsten Bormann Интернет вещей: Стандарты и рекомендации. [Электронный ресурс] / Информационный сборник «Интернет изнутри». 2017 – Режим доступа: http://internetinside.ru/internet-veshhey-standarty-i-rekomenda, свободный (дата обращения: 5.06.2017). – Загл. с экрана. – Яз. рус.
20. Christophe De Canniere and Orr Dunkelman, Miroslav Knezevic KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. [Электронный ресурс] / Katholieke Universiteit Leuven, Department of Electrical Engineering ESAT/SCD-COSIC and Interdisciplinary Center for Broad Band Technologies Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, Ecole Normale Sup´erieure ´ D´epartement d'Informatique. 2010. – Режим доступа: h ttps://pdfs.semanticscholar.org/2686/044f8a972325e1b23824430dea731d8e2817.pdf, свободный (дата обращения: 1.06.2017). – Загл. с экрана. – Яз. англ.
21. Elias Yarrkov Cryptoanalysis of XXTEA. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2010. – Режим доступа: https://eprint.iacr.org/2010/254.pdf, свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
22. Wenling Wu and Lei Zhang LBlock: A Lightweight Block Cipher. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2011. – Режим доступа: https://eprint.iacr.org/2011/345.pdf, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.
23. HIGHT Algorithm Specification. [Электронный ресурс] / Korea Internet & Security Agency. 2009. – Режим доступа: h ttps://seed.kisa.or.kr/html/egovframework/iwt/ds/ko/ref/01.+HIGHT+Algorithm+Specification.pdf, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.