Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
Vol. 5, Is. 3, pp. 106-110, 2015

DOI: 10.13187/vesp.2015.5.106
www.ejournal21.com

Modern security

UDC 004.056

Analysis of Data Transmission Protocols to Implement Secure Automated Systems on the Example of "Smart Home"

[1] Alexander V. Nasteka
[2] Catherine E. Bessonova

[1] National research university of information technologies, mechanics and optics, Russian Federation
197101 Saint Petersburg, Kronverkskiy prospekt, 49
E-mail: nasteka.av@gmail.com
[2] National research university of information technologies, mechanics and optics, Russian Federation
197101 Saint Petersburg, Kronverkskiy prospekt, 49
PhD in Engineering sciences, Assistant
E-mail: merom812@gmail.com

Abstract

This article describes the modern data transfer protocol for implementing secure data transfer. The author describes interconnection with private security firms. This work describes the features of some wireless data transfer protocoland ensuring the confidentiality, integrity and availability of data. The result of the research is recommendation on the use of wireless protocols.

Keywords: information security, smart home, ZigBee, WeMo, Z-Wave, Thread, data transfer protocol, security system.

Введение

Одним из направлений защиты квартир, загородных коттеджей, дач и других жилых помещений, является использование услуг частных охранных предприятий с установкой систем сигнализации на случай несанкционированного проникновения. Подобные системы могут быть использованы как обособленно от других инфраструктур дома, так и быть их частью, чтобы обеспечить удобство управления и позволить снизить затраты на производство систем безопасности, исключая дублирование уже существующих аппаратных элементов. Однако в случае использования совместно с существующими системами жилого помещения, необходимо обеспечить конфиденциальность и целостность данных, передаваемых устройством сигнализации [1].

Для подобного критичного механизма безопасности необходимо найти протокол передачи информации, который бы удовлетворял критериям обеспечения конфиденциальности, целостности и доступности данных [5, 6]. Немаловажным пунктом будет способ общения с другими структурными элементами жилого помещения: развитие

систем «умный дом» и беспроводных модулей домашней автоматизации привело к частичной унификации данного сегмента и имеется возможность использования общей сетевой инфраструктуры.

Однако, несмотря на развитие и постепенную официальную и неофициальную стандартизацию технологий сегмента «умный дом» и любой домашней автоматизации, остается проблема выбора протоколов передачи информации между управляемыми устройствами, датчиками и другими элементами помещений. Особенно остро стоит проблема, когда необходимо обеспечить конфиденциальность и целостность циркулирующих данных [2, 3].

Целью исследования является поиск защищенного сетевого протокола, позволяющего при его использовании в устройствах автоматического сигнализирования исключить влияние на конфиденциальность, целостность информации без использования специальных программно-аппаратных решений. Также необходимо обеспечить доступность данных устройств путем возможности вести автономную работу.

Результаты

Основные защищенные протоколы можно условно разделить на два больших класса: применимые при проводных решениях (например, IPsec, SSL, TLS); применимые при создании беспроводных систем (ZigBee, Z-Wave, Thread, WeMo). В жилых помещениях применяются различные устройства и технологии, которые, как правило, является надстройкой к уже существующей инфраструктуре, поэтому основным направлением анализа являются беспроводные протоколы, позволяющие удобно реализовать сетевое взаимодействие. Проводные решения стоит рассматривать только в условиях внедрения домашней автоматизации на ранних этапах строительства отдельных помещений или квартир, а также при проектировании критических элементов системы.

При использовании беспроводных протоколов и устройств появляется вопрос их возможности обеспечить надлежащий уровень конфиденциальности и целостности данных. Это связано влиянием на уже существующие беспроводные сети в зоне применения, распространенность протокола связи, возможность перехвата управляющего сигнала с его последующим анализом или атакой. Также имеются дополнительные требования по обеспечению доступности данных в «умном доме» и способности вести автономную работу.

Рассмотрим четыре основных беспроводных технологии, с помощью которых можно реализовать систему автоматизации в защищенном исполнении [10]. В качестве сравнительных характеристик будем исследовать:

1) Шифрование данных: наличие и надежность технологии для создания конфиденциального канала передачи данных. Возможность использования в качестве основной или дополнительной возможности.

2) Топология сети: возможные варианты подключения устройств в сеть.

3) Обеспечение доступности и автономности: наличие дополнительных алгоритмов самоорганизации сети и самовосстановления

4) Скорость передачи данных: высокая пропускная способность для обеспечения быстрого отклика между запросом на действие и его выполнением, а также запасом ресурса при загрузке каналов передачи данных.

В первую очередь рассмотрим шифрование. Для создания защищенной передачи данных, данная характеристика будет ключевой. Все протоколы используют шифрование, однако оно очень сильно разнится. Если сравнивать Zig-Bee и Z-Wave, то они оба используют AES-128, ключевым отличием Z-Wave является возможность использования данной технологии только на отведенных узлах системы, а не повсеместно, как это реализовано у Zig-Bee. Threadиспользует современные протоколы на основе эллиптических кривых, для которых еще не найдено субэкспоненциальных алгоритмов решения. WeMов данном случае противоречив, его возможности шифрования целиком и полностью зависят от возможностей маршрутизатора, это TKIP/AES шифрование. С точки зрения доступности и возможностей среди перечисленных алгоритмов необходимо использовать Zig-Bee. В дальнейшем будущем протокол Threadимеет шансы заменить Zig-Bee, при условии, что сохранится скорость шифрования. Также если сравнить алгоритмы AES (Zig-Bee, WPA2, Z-Wave) и связку J-PAKE + NISTP-256 на рисунке 1, то можно убедиться в эффективности

алгоритма AES для быстрой передачи больших объемов данных. Однако на практике все алгоритмы стремятся использовать команды небольшой длины, поэтому критерий скорости будет заметен лишь при использовании протоколов для нестандартных ситуаций.

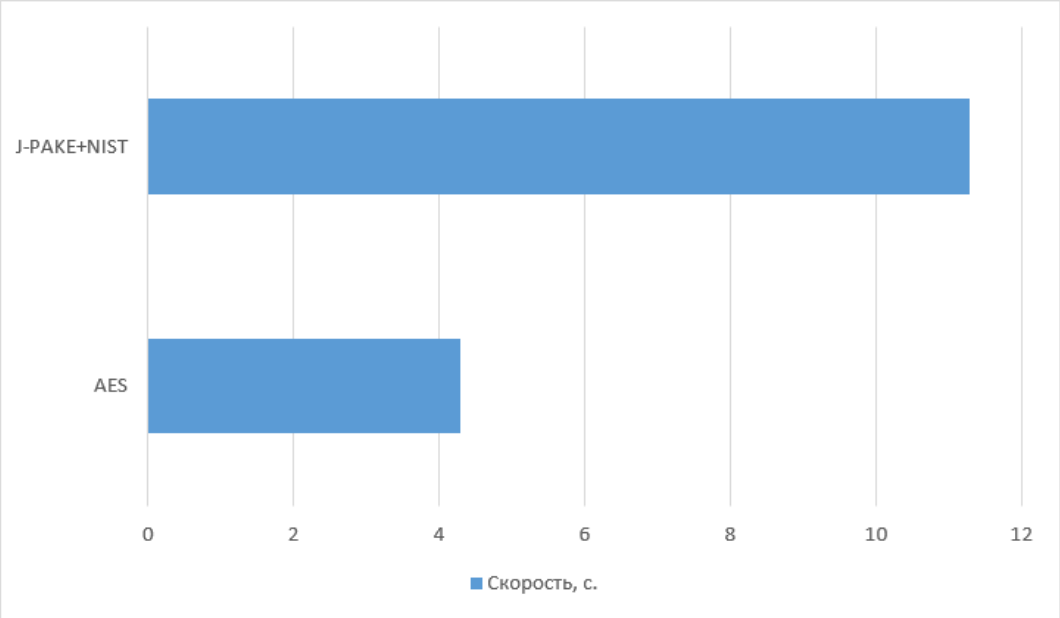

Рис. 1. Сравнение скорости шифрования протоколов AES и связки NISTP-256+J-PAKE на примере нескольких тестов (Меньше, лучше).

С точки зрения создаваемой топологии сети, существует два основных варианта в предлагаемых протоколах. Первый – сеть типа «звезда», имеется некоторое центральное устройство, которое выступает в роли связующего звена. Легко развернуть, однако имеются последствия в виде нарушения доступности, при выходе центрального блока из строя. Подобную сеть могут развернуть протоколы WeMo и Zig-Bee. Второй тип – ячеистая, децентрализованная сеть. Zig-Bee, Z-Waveи Threadподдерживают эту технологию, последние два используют как единственно возможную. Данная сеть, в силу своей децентрализованности, повышает показатели доступности всей сети.

Доступность является вторым важным критерием для организации защищенного «умного дома». Если в нужный момент не будут переданы данные с датчиков движения, датчиков пожара и других, могут произойти различные чрезвычайные ситуации. Протокол WeMo полностью зависит от маршрутизатора, поэтому в случае его отказа не имеет возможности обеспечения автономной работы устройств «умного дома. Если рассматривать Z-Wave, данный протокол сохраняет работоспособность при отсутствии основного источника электропитания [7].

Zig-Beeи Thread помимо питания от аккумуляторов имеют алгоритмы самоорганизации и самовосстановления сети, что позволяет сохранять доступность данных инфраструктуры помещений, в условиях недоступности отдельных ее узлов.

Скорость передачи данных протоколов, работающих на маломощных частотах, не является их сильной стороной, однако для передачи базовых команд их ресурсов более чем достаточно. В данном критерии выделяется лишь WeMo, скорость передачи данных в котором зависит от пропускной возможности маршрутизатора.

Отдельно необходимо отметить вопрос о замене защищенных беспроводных протоколов на российские аналоги. Несмотря на то, что имеются особые протоколы передачи информации, используемые в АСУ ТП (например, ОВЕН) или беспроводная технология MeshLogic, технические особенности не позволяют их правильно применять в системах домашней автоматизации в текущем виде.

Объединив данные вместе, мы получим сводную таблицу 1.

Таблица 1

Анализ протоколов передачи данных

Название протокола	Шифрование данных	Топология сети	Доступность и автономность	Скорость передачи данных
Zig-Bee	AES-128	Mesh/Звезда	Автономность, саморганизация, самовосстановление	До 250 кбит/с
Z-Wave	AES-128 (толькокритичныеузлы)	Mesh	Частичнаяавтономность	До 100 кбит/с
WeMo	TKIP/AES	Звезда	Отсутствует	Ограничена скоростью маршрутизатора
Thread	J-PAKE NISTP-256	Mesh	Автономность, саморганизация, самовосстановление	до 250 кбит/с

Заключение

Таким образом, с точки зрения основных характеристик больше всего подходит технология Zig-Bee, он максимально закрывает проблемы обеспечения конфиденциальности, целостности и доступности данных в системах с автоматическим сигнализированием [9]. Протокол Thread использует более современные технологии, однако недавний выпуск основных спецификаций и отсутствие дополнительной информации о применяемых устройствах не позволяет говорить о нем, как о полноценной замене Zig-Bee, возможно лишь в ближайшем будущем [8]. Протокол WeMo не подходит для создания защищенных систем «умный дом» [4]. Дальнейшей целью автора является проведение эксперимента по практическому анализу эффективности уровня конфиденциальности, целостности и доступности данных данным протоколом в сравнении с другими представленными в материале технологиями.

Примечания:

1. Бессонова Е.Е., Ефремов А.А., Настека А.В., Овсяникова В.В., Салахутдинова К.И., Трофимов А.А. Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики анализ защищенности систем «Умный дом» // Региональная информатика «РИ-2014» Материалы конференции 2014. (124). [Электронный ресурс]. URL: http://spoisu.ru/files/ri/ri2014/ri2014_materials.pdf

2. Гололобов В.Н. «Умный дом» своими руками. М.: НТ Пресс, 2007. с. 9-12, ISBN 5-477-00484-3

3. Стариковский А.В. Исследование уязвимостей систем умного дома [Текст] / А.В. Стариковский, И.Ю. Жуков, Д.М. Михайлов, А.М. Толстая, Ф.В. Жорин, В.В. Макаров, А.Б. Вавренюк // Спецтехника и связь. 2012. №2. С. 55-57.

4. BelkinWeMoSystem. [Электронный ресурс] URL: http://www. theaustralian.com.au/life/personal-technology/belkins-wemo-system-will-switch-you-on/story-e6frgazf-1226594969108

5. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. pp. 9-14.

6. Michael S., Ulf L., 7 Smart-Home-Starter-Kits imSicherheits-Test // AV-TEST-Studie. 2014. pp. 16-41.

7. OpenZwave. (n.d.). [Электронный ресурс]. URL: http://www.openzwave.net/dev/index.html

8. Thread Group, Thread Commissioning – 2015. [Электронный ресурс]. URL: http://threadgroup.org/Portals/0/documents/whitepapers/Thread%20Commissioning%20white%20paper_v2_public.pdf

9. ZigBeeAlliance, NewZigBeePROFeature:GreenPower – 2012. [Электронный ресурс] URL: http://www.zigbee.org/?wpdmdl=2121

10. ZigBee, Z-Wave, Thread and WeMo: What's the Difference? [Электронный ресурс]. URL: http://www.tomsguide.com/us/smart-home-wireless-network-primer,news-21085.html

References:

1. Bessonova E.E., Efremov A.A., Nasteka A.V., Ovsyanikova V.V., Salakhutdinova K.I., Trofimov A.A. Rossiya, Sankt-Peterburg, Sankt-Peterburgskii natsional'nyi issledovatel'skii universitet informatsionnykh tekhnologii, mekhaniki i optiki ANALIZ ZAShchISHchENNOSTI SISTEM «UMNYI DOM» // Regional'naya informatika «RI-2014» Materialy konferentsii 2014. (124). [Elektronnyi resurs]. URL: http://spoisu.ru/files/ri/ri2014/ ri2014_materials.pdf

2. Gololobov V.N. «Umnyi dom» svoimi rukami. M.: NT Press, 2007. c. 9-12, ISBN 5-477-00484-3

3. Starikovskii A.V. Issledovanie uyazvimostei sistem umnogo doma [Tekst] / A.V. Starikovskii, I.Yu. Zhukov, D.M. Mikhailov, A.M. Tolstaya, F.V. Zhorin, V.V. Makarov, A.B. Vavrenyuk // Spetstekhnika i svyaz'. 2012. №2. S. 55-57.

4. BelkinWeMoSystem. [Elektronnyiresurs] URL: http://www. theaustralian.com.au/ life/personal-technology/belkins-wemo-system-will-switch-you-on/story-e6frgazf-1226594969108

5. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. pp. 9-14.

6. Michael S., Ulf L., 7 Smart-Home-Starter-Kits imSicherheits-Test // AV-TEST-Studie. 2014. pp. 16-41.

7. OpenZwave. (n.d.). [Elektronnyi resurs]. URL: http://www.openzwave.net/ dev/index.html

8. Thread Group, Thread Commissioning – 2015. [Elektronnyi resurs]. URL: http://threadgroup.org/Portals/0/documents/whitepapers/Thread%20Commissioning%20white %20paper_v2_public.pdf

9. ZigBeeAlliance, NewZigBeePROFeature:GreenPower – 2012. [Elektronnyi resurs]. URL: http://www.zigbee.org/?wpdmdl=2121

10. ZigBee, Z-Wave, Thread and WeMo: What's the Difference? [Elektronnyi resurs]. URL: http://www.tomsguide.com/us/smart-home-wireless-network-primer,news-21085.html

УДК 004.056

Анализ протоколов передачи информации для реализации защищенных автоматизированных систем на примере системы «умный дом»

[1] Александр Владимирович Настека
[2] Екатерина Евгеньевна Бессонова

[1-2] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101, Санкт-Петербург, Кронверкский проспект, 49
[1] E-mail: nasteka.av@gmail.com
[2] Кандидат технических наук, ассистент
E-mail: merom812@gmail.com

Аннотация. Данная статья описывает современные протоколы передачи данных для реализации защищенного обмена информацией в системах сигнализации. Их взаимосвязь с правоохранительными органами. Подробно описаны возможности четырех беспроводных протоколов передачи и их возможности по обеспечению конфиденциальности, целостности и доступности данных. Предложена рекомендация для использования беспроводного протокола передачи данных для создания защищенного канала обмена информацией.

Ключевые слова: информационная безопасность, ZigBee, WeMo, Z-Wave, Thread, домашняя автоматизация, протоколы передачи данных, система безопасности.