ANALYZING SECURITY THREATS IN SMART HOMES TECHNOLOGY

Ekaterina M. Konstantinova, Tsvetoslav S. Tsankov

[1] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Student, katminkova2@gmail.com
[2] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Assoc. prof. Eng., PhD, c.cankov@shu.bg

***Abstract**: New technologies are entering our entire lives. The use of the Internet of Things in smart homes and buildings is already a fact. It is supported by ZigBee – an Internet protocol that provides the necessary automation. Here again, when the Protocol's mode of operation is analyzed, serious security threats are encountered. This post addresses the major issue and provides a good, low-cost solution.*

***Keywords**: Internet of Things, KillerBee suite, Trust Center, WLAN, ZigBee*

АНАЛИЗИРАНЕ НА ЗАПЛАХИТЕ ЗА СИГУРНОСТТА В ТЕХНОЛОГИИТЕ ЗА ИНТЕЛИГЕНТНИ ДОМОВЕ

Екатерина М. Константинова, Цветослав С. Цанков

Въведение

Интернет на нещата (Internet of Things – IoT) бързо става реалност и безжичните сензорни мрежи ще бъдат още по-широко внедрявани в близко бъдеще. Всъщност безжичните сензорни мрежи играят важна роля в IoT и се разглеждат като нововъзникваща технология с голям спектър от приложения в много области. Тяхното значение се увеличава с бързия напредък на тяхното изпълнение. Следователно сигурността става належаща необходимост.

Известно е, че ZigBee има много привлекателни предимства като ниска цена, висока надеждност и ниска сложност, както и широк обхват на приложение, независимо дали в индустриалната автоматизация, интелигентния контрол или здравеопазването и т.н. Но ZigBee все още се сблъсква с много предизвикателства, като ограничаване на изчисленията на възлите, пространството в паметта и енергетична възможност за потребление и комуникация. При тези ограничения е непрактично да се прилагат класически механизми за сигурност като криптография с публичен ключ. Ето защо е важно да се проучи допълнително тази тема и да се съсредоточат повече изследователки дейности в тази специфична област.

Тук е даден един различен подход към протокола, който може да помогне за решаването на належалите проблеми:

• В оригиналната си версия, ZigBee има девет съобщения за обмен. Този тип протоколи изискват редица операции, които са правопропорционални с броя на възлите в системата, което може да е непрактично, тъй като безжичните сензорни мрежи могат да се състоят от голям брой възли. Новият подход се нуждае от само четири съобщения за обмен, за да завърши напълно процеса на сигурна комуникация.

• Протоколът ZigBee страда от сериозни слабости, свързани с разпределението на ключовете, тъй като те се предават или по въздушен път, или са предварително инсталирани върху устройствата по несигурен начин. Освен това, всички възли споделят един и същ Универсален ключ.

По този начин компрометирането на един единствен възел застрашава цялата мрежа. В предложеното решение всеки възел има собствен ключ за ограничаване на успешните хакерски атаки. За защита на комуникацията между два възла се използва еднократен ключ, който не може да бъдат използван в по-нататъшната комуникация.

• Протоколът ZigBee използва брояч на кадри, за осигуряване на успешна комуникация между възлите. С други думи, за отхвърляне на кадри, които са били възпроизведени се използва подредената последователност на входовете. Този подход не е ефективен и предлага използвато на времеви етикети или случайни стойности за еднократна употреба, за да се предотвратят атаки при повторно възпроизвеждане.

• Предложеният подход разчита на прости операции и не включва скъпи изчислителни криптографски операции за осигуряване на защита срещу няколко атаки.

Осигуряването на предаваната информация между хостовете с конфигуриран сървър в локалната мрежа е много важна задача към всеки мрежов системен администратор, специалист по сигурността, мрежов архитект и специалист [1], [2], [3].

Защитна архитектура

В технологията ZigBee са налични три типа ключове: Универсални (Master), Свързващи (Link) и Мрежови (Network).

• Универсални: Считат се за най-важните ключове сред комуникационните възли. Използват се при Процедурата за установяване на ключове, наречена SKKE (Symmetric-Key Key Exchange – симетрична размяна на ключове), като осигурява поверителност при размяната на ключове между два възела. Те са предварително инсталирани във всеки възел по време на производството на устройствата или могат да бъдат настроени безжично в мрежата. Те обикновено се споделят между всички възли. Новите възли също използват главния ключ чрез SKKE процедура, за да настроят свързващите ключове с останалите възли.

• Свързващи: Те се използват за криптиране на цялата информация, обменена между два възела. Управляват според нивото на приложение и са уникални между всяка двойка възли.

• Мрежови: Първоначално генерирани от Trust Center, тези ключове имат за цел да защитават от външни атаки с нужда от малко ресурси. Те също могат да бъдат регенерирани през различни интервали и са необходими за присъединяване на новите възли в мрежата. Те са 128b ключове и се споделят между всички устройства.

Мрежата ZigBee използва Trust Center (Надежден център), за да реши дали новите възли са оторизирани да се присъединят към WLAN. Обикновено има само един Надежден център, който излъчва съобщения чрез мрежовия ключ, които могат да бъдат прочетени от всички членове. Старият мрежов ключ се използва и при разпространението на нов ключ през мрежата. Броячът на кадри се използва за отхвърляне на поворявми кадри и също се актуализира в по-познятия начин. При всяка двойка устройства могат да се инсталират както мрежови, така и свързващи ключове. Въпреки това, с цел повишаване на сигурността винаги се използва свързващия ключ, независимо че използва повече място в паметта.

Процедурата SKKE на ZigBee има два различни случая според конфигурацията на Надеждния център. В първия случай Центърът създава самия Свързващ ключ и го изпраща на всяко

главно устройство. Следователно изпращачът и получателят нямат роля в създаването на Свързващия ключ. Във втория случай, Надеждния център създава Универсален ключ и го изпраща на всяко главно устройство. Използвайки този ключ, A и B инициирт SKKE процедура за установяване на Свързващ ключ. В този случай двете главни устройства създават Свързващ ключ едновременно, използвайки SKKE протокол. В края на успешната операция главните устройства установяват сигурна комуникация, използвайки Свързващия ключ за криптиране (фиг. 1)

Фиг. 1: Сценарий за създаване на Свързващи ключове

Съобщение 1: Устройство A започва комуникацията с усторойство B, като изпраща първото съобщение за заявка до Надеждния център.

Съобщения 2 и 3: Центърът изпраща Универсален ключ на всяко от главните устройства.

Съобщение 4: A изпраща на B заявката си за стартиране на SKKE.

Съобщение 5: B получава SKKE заявката от A. Съобщенията (4) и (5) са кодирани от Универсалния ключ, който е получени в предишните две съобщения. Останалите четири съобщения представляват самата SKKE процедура.

Съобщения 6 и 7: Тези стъпки включват предизвикателствата (NA, NB) на главните устройства, шифровани от ключа.

Съобщения 8 и 9: Включват сложни съобщения, които могат да бъдат изчислени от двете страни, за да се проверят взаимно.

Слабости в сигурността

Съответните слабости в сигурността, свързани с протокола ZigBee, са представени, както следва:

1. Разпределение на ключовете: Първата уязвимост на мрежата ZigBee е разпределението на ключовете, тъй като те се предават безжично или са предварително инсталирани на устройствата по несигурен начин. Има различни подходи за дистрибуция в зависимост от нивото на сигурност:

Използвайки високо ниво на защита, Мрежовият ключ се криптира и предава по въздуха с помощта на Универсален ключ, който се споделя между всички възли. По този начин компрометирането на един единствен възел води до незащитена връзка между всички комуникационни устройства в мрежата.

Използвайки Стандартното ниво на сигурност, безопасността на системата става още по-критична, когато некриптирания Мрежов ключ се предава безжично. Следователно, Стандартното ниво на сигурност има сериозни уязвими места и не може да се препоръча за целите на сигурността [4], [6].

Използване на предварително инсталирани мрежови ключове на всяко устройство в мрежата. Това става ръчно и не е практично, когато мрежата е голяма.

2. Брояч на кадри: В спецификацията на ZigBee понятието брояч на кадри се описва като услуга за сигурност. Той използва подредена последователност от входове, за да отхвърли кадрите, които са били възпроизведени. Броячът обикновено се нулира, ако се създаде нов ключ. В този контекст последователността се използва за предотвратяване на злонамерени атаки. Въпреки това, не е добър подход по много причини. Например, злонамереният нарушител може да избере

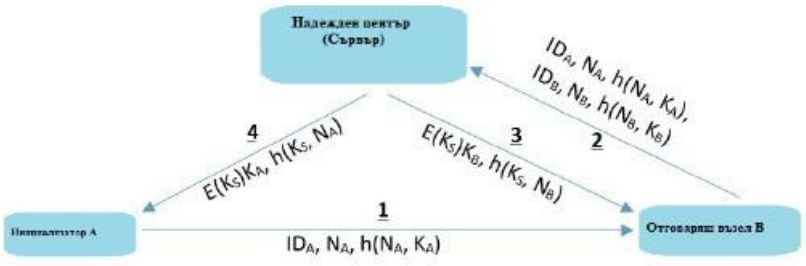
по-големи стойности, за да се избегне отхвърлянето на конкретни кадри, тъй като броячът на кадри използва увеличаващи се стойности, а не случайни такива. Друга слабост на броячите е, че лесно могат да бъдат претоварени и нарушителят да доведе до отхвърляне на по-нататъшни кадри и отказ на услуга, просто като подправи кадри с максималната стойност 0xFFFFFFFF.

3. Предоставяне на сигурност: Друга слабост, която може да бъде открита при модела на сигурност на ZigBee е, че изискването за препращане не е адресирано правилно (въпреки режим на висока сигурност). След напускане на мрежата даден възел все още е в състояние да получи достъп до мрежовата комуникацията, тъй като все още притежава Универсалния и Свързващия ключ, поради факта че не е направена правилна занулваща настройка. Всъщност, ако вземем за пример компания или институция, използваща ZigBee за отваряне на врати или подобряване на енергийната ефективност, това място се нуждае от добър подход за управление на хилядите ZigBee устройства. Често срещана ситуация е едно или много от устройствата да се загубят или откраднат и да бъде компрометирана цялата система. Проучванията показват, че извличането на защитни ключове е възможно и сравнително лесно [2], [4].

Поради тази причина, ако ключовете, съхранявани на устройствата, не са правилно нулирани, може да бъдат използвани за злонамерени атаки. Следователно, този тип атаки не трябва да бъдат вземани на сериозно.

4. Подслушване и манипулиране на данни: Това са още доказани уязвимости в сигурността със системи с активиран ZigBee. За атакуващи цели, като подслушване, инжектиране/манипулиране на данни или декодиране на пакети, може да се използва специален софтуер и хардуер. Нискобюджетни устройства като AVR RZ USB stick module (RZUSB) може да се използват за отстраняване на много уязвими места в сигурността. Освен това, Интегрирана среда за развитие (IDE), базирана на Компилатора на GNU (GCC) е свободно достъпна за разработка на софтуер. Друг пример е софтуерът KillerBee suite, който е модифицирана версия на фърмуера на RZUSB. Този инструмент е способен да използва и уязвимостите на ZigBee и е свободно достъпен софтуерен пакет. Очаква се тези инструменти да бъдат подобрени, за да бъдат още по-ефективни в близко бъдеще, излагайки повече неизвестни към момента слабости на ZigBee.

Предложено решение за подобряване на защитата



Фиг. 2: Предложение за подобряване на защитата

Три устройства участват в това предложение: Надежден център, възел инициатор A и отговарящ възел B (фиг. 2). Всеки възел i съхранява своя идентификатор IDi и секретен ключ Ki. Надеждният център има достъп до базата данни, където се съхранява информацията за мрежата (в този случай се интересуваме от идентификационните номера и секретните ключове, свързани с възлите). Никакви ключове не се споделят постоянно между възлите, което значително намалява възможността за компрометиране на мрежата при излагане дори и на един единствен възел. Ключът за временна сесия Ks, е ключ за еднократна употреба, споделен между възела инициатор и отговарящия възел по време на дадена комуникация. В този подход се предлага използването на произволни еднократни числа Ni, за да се гарантира сигурността на съобщенията, съдържащи

ключовете на сесията. След всяка комуникация Ni се актуализира за предотвратяване на повторни атаки. Използвани са следните обозначения:

TC	Надежден център
A	Възел инициатор
B	Отговарящ възел
IDi	Идентификатор на възел i
Ni	Произволни еднократни числа
Ki	Таен ключ на даден възел i
Hi	Резултати от хеширащата функция h(Ni,Ki)
EK(M)	Криптирано съобщение M с ключ K
KS	Еднократен сесиен ключ

• Стъпка 1: Инициаторът A изпраща заявка за установяване на комуникация с възел B. Съобщението (1) съдържа идентификаторът IDA на възела, еднократно NA, генерирано от A и HA, който е хеш на NA, заедно с частния ключ KA. Надеждният център има достъп до KA и може да възстанови HA, за да провери дали A е легитимен възел. HA е еднопосочна функция, тъй като хеш функциите се изисква да са необратими. Следователно, дори ако това съобщение бъде разкрито, то последващата атака ще бъде неуспешна, тъй като само оторизираните страни притежават секретния ключ KA за възстановяване на служебното съобщението при следващата стъпка.

• Стъпка 2: Отговарящият възел B изгражда собствено съобщение по същия начин и изпраща получената служебна информация от A заедно с основната информацията до Надеждния център като искане за удостоверяване, а също и за получаване на нов ключ за временна сесия.

• Стъпка 3: Центърът получава съобщението (2) от B и първо проверява дали препратеното съобщението е валидно или не, като възстановява H'A и H'B , използвайки KA и KB за съхранените съответно IDA и IDB. Сравняйки H'A с HA и H'B с HB доказва, че съобщението е легитимно, тъй като само A и B притежават тайните ключове KA и KB и могат да съставят валидно съобщение.

• Стъпка 4: Надеждният център генерира ключ за сесия KS и го изпраща съответно към A и Б в криптиран вид, използвайки KA и KB. Еднократните NA и NB осигуряват защита срещу атаки с повторно изпълнение. И двата възела A и B се удостоверяват като оторизирани възли и могат да проверят получените съобщения от Центъра.

• Стъпка 5: Накрая възлите A и B получават криптирана информация и извличат секретния сесиен ключ, като използват техните частни ключове KA и KB. A и B са сигурни, че полученото съобщение е не е било възпроизвеждано, тъй като съдържа еднократни NA и NB. В този момент и инициаторът A, и отговарящият възел B могат да комуникират по защитен начин, използвайки сесийния ключ KS.

Надеждният център може да прави периодична проверка и да верифицира дали всички възли все още са в WSN. Ако не са, Центърът може да оттегли достъпа от конкретен възел просто чрез изтриване или деактивиране на свързаната с него информация в базата данни. Тази техника предотвратява използването на секретна информация от недоброжелателни потребители.

Анализ на сигурността и ефективността

В предложената схема ключът на сесията не се разпространява с Универсален ключ. Следователно е малко вероятно мрежата да бъде компрометирана при разкриване на конкретен ключ (какъвто е случаят с Универсалния ключ в оригиналния протокол). Това е главно поради факта, че секретният ключ на всеки възел се използва за криптиране на съобщението, съдържащо временния сесиен ключ [3], [5].

Някои основни характеристики:

Криптиране на данните: Предаваната информация между Центъра и възлите A и B не е разбираема от потенциален злонамерен потребител, тъй като се използват различни частни ключове за комуникация с всеки възел

Предотвратяване на атаки с повторно възпроизвеждане: Във всяка сесия различни случайни числа са включени в обмена на съобщения, за да се предотврати този вид уязвимост.

Удостоверяване: Тази функция е важна за много приложения. В предложения подход, само оторизирани страни, които притежават секретните ключове KA и K могат да създават валидни съобщения и могат да извлекат сесионните ключове KS.

Изискване за съхранение: Всеки възел трябва да съхранява само частния си ключ, вместо три различни ключа в оригиналния Протокол. Изпълнението на хеш функцията и еднократния генератор на числа се съхранява в презаписваща се памет, защото се нуждае от актуализации. Това прави тази процедура лека и практична.

Изчислителна цена: Стандартните криптографски алгоритми като Системи с публичен ключ имат много висока цена за изчисления и се нуждаят от голямо пространство в паметта. Следователно тези методи не са подходящи за ограничени устройства като безжични сензорни възли. Това решение изисква да се реализира само хеш функция и генератор на произволни числа. И възлите, и Центърът имат достатъчно изчислителна мощност за работа с криптографски операции, базирани на системата със симетричен ключ.

Заключение

Представеният модел за сигурност на ZigBee, е подобрен значително чрез много експертизи. Но той представя недостатъци, които могат да ограничат приложението му и все още са възможни няколко атаки както е споменато в този доклад. Тази публикация е опит за изтъкване на най-сериозните слабости и предлага нов подход за повишаване на сигурността. Предложеното решение е ефективно и предотвратява множество атаки на сигурността без скъп софтуер и хардуер като разходите за съхранение са доста ниски в сравнение със стандартните решения.

References

1. Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Educational simulation the local area network of academic departments with securely configured FTP server*. International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, pp. 146-154.
2. Boyanov, P., Stoyanov St., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Routing information security in the local area network of academic departments using an enhanced distance vector routing protocol – EIGRP*. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, pp. 35-46.
3. Boyanov, P., Stoyanov St., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Security routing simulation the local area network of academic departments using a link-state routing protocol – OSPF*. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, pp. 47-58.
4. Razouka, W., Crosbyb, G., Sekkaki, A. (2014). *New security approach for ZigBee Weaknesses*. Procedia Computer Science 37, The International Symposium on Applications of Ad hoc and Sensor Networks, pp. 376-381. https://doi.org/10.1016/j.procs.2014.08.056
5. Wright, J. *KillerBee:Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic World"*. Available: https://www.willhackforsushi.com/presentations/toorcon11-wright.pdf.
6. ZigBee Alliance. *ZigBee Specification*. ZigBee Document 05-3474-21, August 5, 2015.