Атаки в ZigBee мрежите

Филип Цветанов, Иванка Георгиева, Теодор Илиев, Екатерина Оцетова-Дудин

Attacks on ZigBee networks: *Tendency to increased uses of wireless sensor networks for many applications, transmission and storage of important and confidential data from sensors placed high demands on safety and security of the data transmitted in these networks. The purpose of this paper was to investigate the possible types of attacks and their mechanism in order to take the most effective decision in the design and exploitation of ZigBee networks.*

Key words: *Attacks, wireless sensors network, ZigBee, security.*

ВЪВЕДЕНИЕ

В последните години се забелязва тенденция към увеличено приложение на безжичните сензорни мрежи (БСМ) в много търговски приложения, военни услуги, индустриални и научни изследвания, както и различни приложения в медицинската наука, за сградна и домашна автоматизация, за наблюдение на околната среда и т.н. [4]. Като стандарт за БСМ се приемат мрежите базирани на протокол 802.15.4 известен още като ZigBee.

Ако сигурността на мрежата е компрометирана това може да доведе до сериозни последици, като кражба на частни данни, нелегално сдобиване с данни от БСМ, които могат да бъдат данни от наблюдение на различни обекти, данни от военни системи. Използването на сензорите в критичните системи както в заводите, самолетите, кораби, системите за нуждите на болниците, требва да осигурят *автентичност* (authenticity), цялост (integrity) и поверителност (confidentiality) на предадените данни. Тези мрежи се характеризират с ограничени ресурси в сензорни възли и се нуждаят от специални изисквания за сигурност, за разлика от сигурността в традиционните мрежи. Целта на тази работа е да се изследват възможните видове атаки и техния механизъм, за да се предприемат най-целесъобразни решения при проектирането на сензорните мрежи.

ИЗЛОЖЕНИЕ

Инструменти за сигурност на ZigBee мрежите

ZigBee мрежите са хетерогенни системи, които съдържат много малки устройства, наречени сензорни възли и изпълнителни механизми, имащи възможностите на компютрите с общо предназначение. Сензорите в една БСМ може да бъдат от няколко стотин до хиляди. Тези сензорни възли са с ограничени енергийни ресурси, възможности за съхранение, обработка на данни и комуникация. [2] [3] [4]. Тъй като сензорни възли могат да събират поверителна информация за сигурността на индустриални процеси и неприкосновеността на личния живот на хората, въпросът с осигуряването на сигурност на данните в тези мрежи е особено актуален и стои на вниманието на академичната общност и на изследователите от индустрията [5]. Приложението на конвенционалните механизми за сигурност се оказват не подходящи, поради ограничените ресурси на сензорните възли, което от своя страна налага прилагането на специални механизми за сигурност [7]. Налице е също разбирането, че безжичните системи са по-уязвими към атака, защото всеки с подходящо радио може да комуникира с безжично устройство от известно разстояние [3].

Основните цели на сигурността в БСМ се базират на три елемента:

• *Конфиденциалност*: транспортираните данни в мрежата да не могат да се четат от всеки, а само от крайния получател.

• *Интегритет*: получените съобщения да са без допълнения, заличавания или изменения на съдържанието.

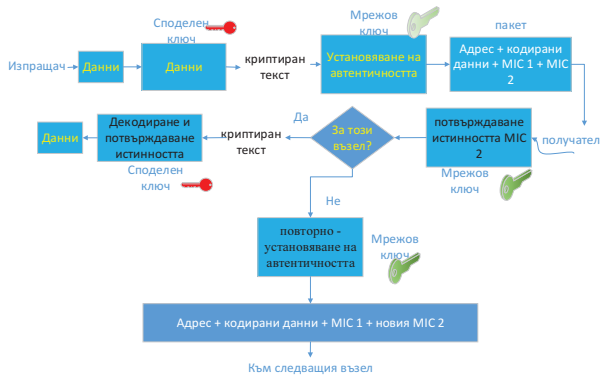
• *Автентичност*: да е сигурно, че съобщението е от точен източник в мрежата.

Конфиденциалността се изисква за приложения не само свързани със сигурността, но също така и за обикновените ежедневни приложения. Сензорните данни трябва да бъдат криптирани, така че само крайния получател да може ги използва. Информацията за данните и командата трябва да пристигнат до получателя непроменени. Например, ако сензорът *показва "нивото на резервоар е 72 cm"* или *„температурата е 20 градуса“* не трябва нито една от цифрите да се загуби, тъй като това може да е катастрофално за съответния управляван или наблюдаван процес. Доверието в източника на съобщението е от решаващо значение. Всяко едно от горните послания може да има много лоши последици, ако са изпратени от злонамерен хакер.

В процесите на индустриалната автоматизация последиците от атаките могат да бъдат много по-тежки, отколкото загубата на клиенти. Ако се доставя *неточна, невярна информация за наблюдаваните параметри* на системата за мониторинг и контрол, атакуващият може да причини физическо увреждане. Например, предаване на сензорни данни към контролера на двигател или клапан, показващи, че оборотите на двигателя или нивото на резервоара е нормално може да доведе до катастрофални повреди и човешки жертви.

Механизмите и инструментите за постигане на сигурността в безжични мрежи, базирани на стандарта ZigBee са разгледани в работа [7].

Повечето системи за сигурност при сензорните мрежи използват мрежови ключове. Всяка двойка ключове има уникален общ ключ за криптиране и автентификация (фиг.1).



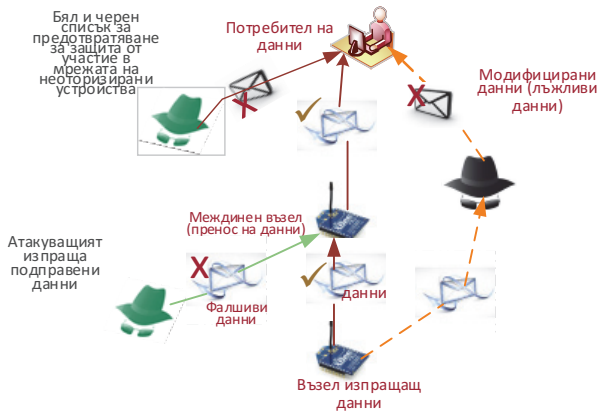
Фиг. 1 – Механизъм за осигуряване сигурността в БСМ

Проверката за целостта на съобщение (MIC) наричана още код за удостоверяване на съобщение (MAC), представлява криптографски контрол на съобщението. Подателя на съобщението създава късо криптирано обобщение на цялото съобщение, наречено проверка на целостта на съобщение. MIC се добавя към съобщението и изпраща заедно с него. Получателят използващ този ключ, може да изпълнява съобщението като разчита своя MIC и проверява съвпадението му с получения MIC. Всяко изменение в съобщението, дори на един бит, предизвиква промяна на MIC и отклонение на съобщението от получателя му. Криптирането на съобщенията в БСМ може да се извърши чрез генериране, но това обикновено е непрактично и в крайна сметка несигурно. Поради важността на уникалността на ключовете за криптиране най-често се приема случаен принцип за криптирането им посредством генератор на случайни числа (RNG). Най-простото решение на този инженерен проблем е да се гарантира, че всяка сесия за връзка (или поток от данни между две крайни точки) има свои собствени уникални ключове, които не са

известни на всички други възли в мрежата.

Атаки в ZigBee мрежите

Проведените изследвания установиха, че в литературните източници се срещат различни подходи при класифицирането и описването на различните видове атаки. След проведен анализ на възможните атаки в това изследване са систематизирани и анализирани атаките в ZigBee както следва [1], [4], [6]:



Фиг. 2 – Атаки в ZigBee мрежите

1) Отказ на услуги –denial of service (DOS)

Атаката *отказ на услуги* представлява опасност за цялата мрежа и се състои от блокиране (jamming) или интерференция на радио честотите, което инициира колизия в мрежата, наводняване с външни данни, до степен, че вече не може да се обработват данните си, или под формата на заглушаване, в която друг сигнал, или шум, се въвежда в комуникационните честоти на безжична мрежа така че мрежата вече не може да комуникира. Този тип атака е с голямо значение индустриални, военни и правителствени приложения.

2) Предаване на измислени данни-broadcasting spurious information. Тук влизат и лъжливите атаки (spoofing), атаки в които хакерът атакува с изпращане на измислени данни (broadcasting spurious information). Атаки при получаване и обработка на команди (Receive and Process Commands) чрез пращане на измислени (фалшиви) команди. Сензорния възел препредава команди за промяна на състояние или действия, които засягат техен съсед. Възможността за обработка на командите е от голяма полза за намаляване на количеството данни в сензорните мрежи. Командите могат да се пращат към всички възли (broadcast) или към един (unicast). При пращане на команди към един възел е нужно да се осигури адресиране на възлите. Тук идва атаката, при която злонамереният възел заема свойство на координатор и изпраща измислени фалшиви команди

3) Физически атаки–physical attack. Физическите проблеми варират от подправяне на сензорните данни чрез невярна информация (например, промяна на показанието на нивото на течност в цистерна за съхранение, за да покрият кражба) или временно забраняване или заглушаване изхода на сензор (например, да се преодолее сигнал за откриване на движение към централна станция за мониторинг на офис, аларма), до унищожаване на сензор или комуникационен възел в безжичната мрежа. В повечето случаи, единственото решение за предотвратяване на физическо проникване е сигурното локализиране и изолиране на мрежовите

елементи. Когато новите данни имат стойности аномални или извън очакваните параметри, може да се предизвика събитие или аларма за разследване.

4) Атаки с препращане на съобщения–Reply attacks. Сензорния възел извършва периодични измервания и изпраща данните на координатора на мрежата.

Атаките с препращане на вече пратено съобщение (replay attack) се извършват на мрежово ниво и биват: *черна дупка - Black Hole*, *селективно препращане* – Selective Forwarding, *корумпиране на данните* – Data Corruption, *изтощаване на ресурсите* - Resource Exhaustion.

Сензорът събира и праща данните на съседен сензор, които се намира на пътя до координатора на мрежата. При приемането на данни трансферният сензор не ги обработва, а само предава данните до достигане на крайната дестинация. В атаката *Black Hole* възела които препраща данните ги унищожава. *Атаката с корумпиране на данни променя съдържанието* на данните при предаване. Цел на тези атаки е контрол над мрежата. Атаката с изтощение на ресурсите се осъществява чрез изпращане на голямо количество на данни от хакера, което води до ненужно, но интензивно изтощаване на енергийните ресурси на сензорите (батерията). Когато пакета има експлицитно зададен път, който трябва да го подмине се извършва атака чрез селективно препращане.

5) Атаки към маршрутизиращите протоколи

ZigBee мрежите са безжични самоорганизиращи се мрежи с автономно управление на топологията. Информацията за топология на мрежата може да бъде позната само от координатора на мрежата, да бъде споделена с някои друг второстепенен главен възел или с всички възли. В този смисъл ZigBee мрежите са чувствителни към всички атаки, които се отнасят до маршрутизиращите протоколи като: фалшифициране (spoofed), промяна (altered), или препращане на информация за маршрутизирането, атаки върху координатора (sinkhole attacks), Сибил атаки (Sybil attacks), атаки тип червеи (wormholes), атаки HELLO, потвърждение за фалшиви атаки (acknowledgement spoofing).

При предаване на данни в мрежата хакерът може да променя данните, да фалшифицира данни и маршрути. Това застрашава истинската топология на мрежата, каква я вижда координатора.

Атаката срещу координатора *Sinkhole* се състои от внедряване на злонамерен сензорен възел, който се използва за предаване на данни до координатора. Така че всички съседни възли които искат да комуникират с координатора го използват като трансферен. Тази атака представлява селективно проследяване.

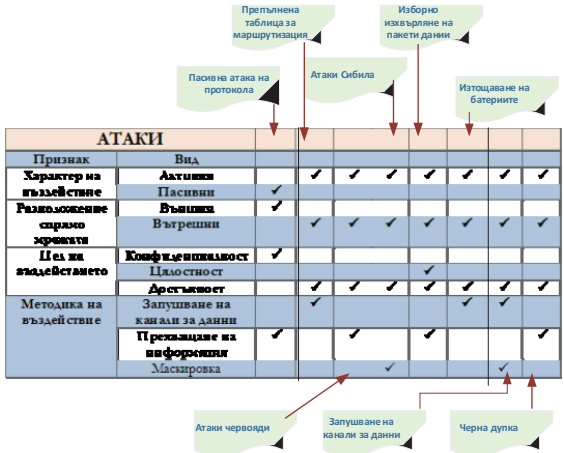
При атаката *Sybil* се внедрява злонамерен възел в мрежата, който намалява ефикасността на някои мрежови алгоритми, например за намиране на най-къси пътища, разпределена обработка на данни, запазване на топологията или проследяване.

Много от маршрутизиращите протоколи използват HELLO пакети за намиране съседни възли. Координатора излъчва HELLO пакети с доста силен сигнал (има по помощна антена от възлите) събирайки информация за мрежата.

Анализът на разгледаните атаки в ZigBee мрежите дава възможност те да бъдат класифицирани по критерии, представени на фиг.3

Инструменти за борба с атаките

KillerBeee [2] съвкупност от инструменти за изучаване на сигурността на мрежите базирани на стандарта 802.15.4 (ZigBee). Осигурява инструментални средства за прехващане, внедряване и възпроизвеждане на движения, декодиране на пакетите данни. Написан е на Python. Прилага се за оказване помощ и разкриване на атаки при експлоатация на ZigBee мрежите.



Фиг. 3 – Класификация на атаки в ZigBee мрежите

ЗАКЛЮЧЕНИЕ

Сензорните мрежи, базирани на протокола IEEE 802.15.4 ZigBee намират широко приложение в много области и представляват интерес за изследване от научната общност и за внедряване в практиката.

В работата са анализирани и систематизирани инструментите за безопасност в ZigBee мрежите и механизмите на възможните атаките в тях. Предложената класификация на атаките според: характера на въздействие, цел на въздействие, разположение спрямо мрежата и методиката на въздействие на различните атаки, както и резултатите от проведените атаки е полезен инструмент при проектирането на мрежи с висока сигурност.

БЛАГОДАРНОСТИ

Това изследване е подкрепено и финансирано от Университетския фонд за научни изследвания на Югозападен университет по проект SBR-B16/14.

ЛИТЕРАТУРА

[1] Kalpana S., Ghose K, Wireless Sensor Networks: An Overview on its Security Threats, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, p.p 42-45, 2010.

[2] KillerBee:Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic World, http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf

[3] Kris Pister, Jonathan Simon, Secure Wireless Sensor Networks Against Attacks, Electronic design, №6, p.p. 38-46, 2014.

[4] Thomas Reuter, Security analysis of wireless communication standards for home automation, Norbert Wiedermann, M.Sc., 2013.

[5] Yao-Tung Tsou, Chun-Shien Lu, MoteSec-Aware, A Practical Secure Mechanism for WSN, IEEE transaction on Wireless Communication Vol 12, No.6 2013.

[6] Москвин А,.Mesh network: защищенная сеть или "дыра" в безопасности? Новые безопасные технологии, 2014.

[7] Цветанов Ф, Кипрова Л., Георгиева И., Относно сигурността на предаваните данни в ZigBee, Общо университетска конференция на НВУ, Велико Търново, 2014.

За контакти:

ас. д-р инж. Филип Цветанов, ЮЗУ „Неофит Рилски“ Благоевград, катедра „Електронна и комуникационна техника и технологии“, e-mail: ftsvetanov@swu.bg

Докладът е рецензиран.