Т Е Х Н И Ч Е С К И У Н И В Е Р С И Т Е Т – В А Р Н А

Мариета Методиева Хъкъ

ПОДХОДИ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА НА IoT МРЕЖИ

А В Т О Р Е Ф Е Р А Т

на дисертация за получаване на образователна и научна степен „доктор”

по докторска програма „Компютърни системи, комплекси и мрежи“
към професионално направление „Комуникационна и компютърна техника“

Научен ръководител: проф. д-р инж. Венета Панайотова Алексиева

Рецензенти:
1.
2.

Варна, 2025 г.

Дисертационният труд е обсъден на …… в катедра „Компютърни науки и технологии“ и насочен за защита.

Докторантът работи в катедра „Компютърни науки и технологии“.

Автор: Мариета Методиева Хъкъ

Заглавие: Подходи за повишаване на сигурността на IoT мрежи

Т Е Х Н И Ч Е С К И У Н И В Е Р С И Т Е Т – В А Р Н А

Мариета Методиева Хъкъ

ПОДХОДИ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА НА IoT МРЕЖИ

А В Т О Р Е Ф Е Р А Т

на дисертация за получаване на образователна и научна степен „доктор”

Варна, 2025 г.

Дисертационният труд съдържа 229 страници, включително 126 фигури, 4 таблици и 4 приложения, оформени в 3 глави, общи изводи и списък на използваната литература от 166 заглавия, от които 1 на кирилица и 165 на латиница.

Защитата на дисертационния труд ще се състои на ..... г. от ..... ч. в ..... на открито заседание на жури сформирано със заповед на Ректора № ...../..... г.

Материалите по защитата (дисертацията, рецензиите и становищата) са на разположение на интересуващите се в Докторантски център, стая 318 НУК.

ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на проблема

Все по-широкото възприемане на Индустрия 4.0 и все по-масовото 5G покритие, осигурено от мобилните оператори, развитието на безжични технологии и усъвършенствани сензорни технологии, насочват научната мисъл към изследвания на иновативната технологична среда, базирана на Интернет на обектите (Internet of Things - IoT).

Приложенията на IoT се интегрират в широк спектър от индустрии, което води до бързото разширяване на пазара. Безжичните сензорни мрежи (WSN) играят критична роля във внедряването на IoT [89].

От гледна точка на Индустрия 4.0 ефективността на IoT зависи от нивото на развитие на средствата за автоматизация, наличието на сензори, съвместимостта с други технологии, безжичното предаване на данни, съхранението, извличането и анализа им. Прилагането на технологията позволява не само управление на производствени процеси, но и на всички дейности в живота на човека. Тези факти пораждат и притеснението на обществото по отношение на сигурността и ефективността на IoT поради ограниченото естество на ресурсите и безжичната комуникация с крайните устройства [113].

Традиционните схеми за сигурна комуникация в IoT мрежа се базират на основните математически операции – удвояване, скаларно умножение на базата на удвояване, билинеарно удвояване, експоненциална операция, скаларно умножение по елиптична крива или точково умножение.

Въпреки това, традиционните подходи, които се използват за сигурна комуникация в IoT мрежа са скъпи и изискват висока изчислителна мощност и претоварват честотната лента. Това се отразява на ефективността на тези подходи. Поради интензивния характер на разходите и високите изисквания към ресурсите, традиционните подходи не са подходящи за IoT устройства с ограничени ресурси. Освен това, липсата на основни атрибути за сигурност в традиционните схеми, като например непоправимост, възможност за публична проверка, неопровержимост и атаки за отказ на услуга, излага сигурността на данните на висок риск.

2. Цели и задачи на изследването

Основната цел на дисертационния труд е разработване на подходи за повишаване на сигурността в IoT мрежи, реализирани със ZigBee.

Задачите, които са формулирани за постигане на поставената цел са следните:

- Да се дефинира аналитичен подход за количествено измерване на степента на сигурност в IoT мрежа;
- Да се предложат подходи за сигурност в комуникациите в IoT мрежа, реализирана със ZigBee технология;
- Да се разработи симулатор за работата на ZigBee технология, с модули, реализиращи обмяна на ключове между IoT крайно устройство и център за сигурност (trust center- TC); кибератаки към мрежата и др.п.
- Да се разработи прототипна мрежа, базирана на ZigBee и да се докаже работоспособността на симулатора.

3. Обект и предмет на изследване

Обект на изследването е технологията ZigBee, тъй като е една от най-широко използваните технологии (след Wi-Fi и Bluetooth) за проектиране и внедряване на сензорни мрежи за управление на обекти.

Предмет на изследване в настоящия дисертационен труд е сигурността на IoT мрежи.

4. Методи на изследване

Използвани са емпирични методи като наблюдение, сравнение, експериментиране за изследване на сигурността в ZigBee мрежи за IoT. Въз основа на изследваните методи на сигурност в IoT мрежи и тези приложими в ZigBee е формулирана необходимостта от подобряване на съществуващите подходи за сигурност в ZigBee мрежи за IoT. Като емпирико-теоретичен подход за изследване на предложения в дисертационния труд подход за подобряване на сигурността в ZigBee мрежи е използвана симулация, а за валидиране на симулационните експерименти е използвана прототипна мрежа.

5. Място на изследване

Изследванията са проведени в лабораториите на катедра КНТ при ТУ – Варна.

6. Научна новост на изследването

Резултатите от проведените в съответствие с целта и задачите на дисертационния труд теоретични и експериментални изследвания се свеждат до следните основни приноси:

- Предложен е аналитичен израз за изчисляване на ниво на сигурност в ZigBee мрежи и скала за определяне на степените за ниво на сигурност.
- Предложен е адаптивен подход за подобряване на нивото на сигурност в ZigBee мрежи.
- Дефинирана е система от показатели за оценяване на симулационни продукти за изследване на сигурност в ZigBee мрежи.
- Разработен е симулатор за изследване на процесите за сигурност в ZigBee мрежи.
- Разработена е прототипна ZigBee мрежа за IoT, в която експериментално е изследвана сигурността и е приложена предложената скала за определяне на степените за ниво на сигурност.

7. Практическа ценност на изследването

Предложеният аналитичен израз за изчисляване на ниво на сигурност и скала за определяне на степените за ниво на сигурност могат да бъдат приложени за изразяване на качествения показател „сигурност“, както в ZigBee мрежа, така и в IoT мрежи, базирани на IEEE 802.15.4 стандарта. Предложеният адаптивен подход може да бъде приложен с цел подобряване нивото на сигурност чрез адаптиране на AES ключа за всяко устройство в ZigBee мрежа и в IoT мрежи, базирани на IEEE 802.15.4 стандарта.

Дефинираната система от показатели за оценяване на симулационни продукти за изследване на сигурност в ZigBee мрежи може да бъде използвана като базово средство за оценяване на симулатори от този тип. Разработеният симулатор дава възможност за внедряване и изследване на нови подходи, свързани със сигурността на ZigBee мрежи. Реализираната прототипна ZigBee мрежа може да се използва за експериментално валидиране на симулирани процеси, както и за внедряване на нови подходи, свързани със сигурността на мрежата.

8. Апробация на изследването

Основните етапи от разработването на теоретични и приложни резултати на дисертационния труд са докладвани и публикувани в общо 7 публикации, от които 6 са в международни конференции, реферирани в база данни „Scopus“, като 1 от тях е изнесена в чужбина, а останалите 5 в България. Приета е и 1 нереферирана статия за публикуване в списание в България – Journal of CIEES.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

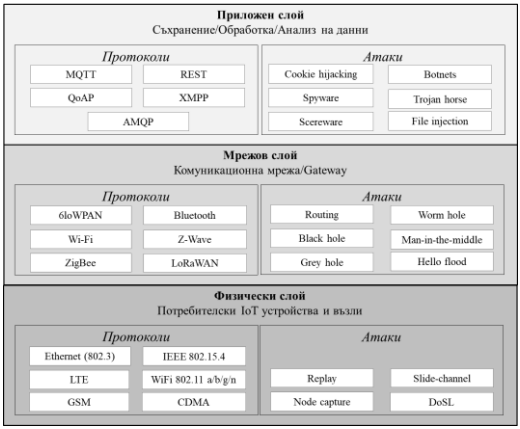
Глава 1: Анализ на подходи за повишаване на сигурността на IoT мрежи

В първа глава е представена същността на уязвимостите в сигурността на IoT мрежите. Разгледани са спецификите на различни подходи за гарантиране на сигурността на съхраняване на данни и постигане на интегритет и конфиденциалност при комуникациите между възлите в IoT мрежи (Таблица 1.1, Фиг. 1.1).

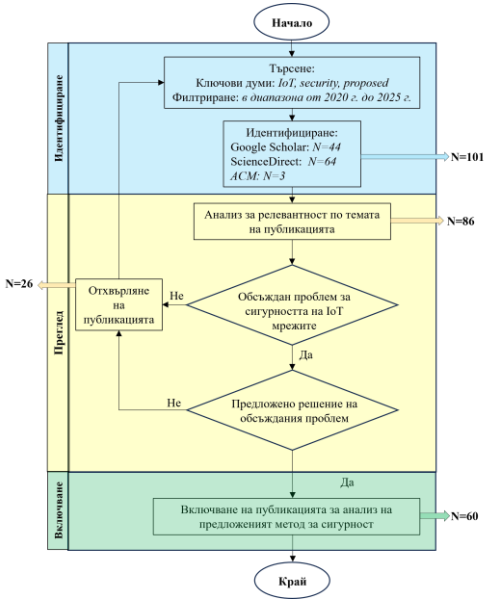
Анализът на предимствата и недостатъците на подходите за повишаване на сигурността на IoT мрежите е извършен, следвайки основните стъпки на актуализирания метод PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [49] (Фиг. 1.2). В Таблица 1.2 са представени най-често използвани методи за защита на IoT мрежи.

Таблица 1.1 Място за съхранение на IoT данни от разгледаните публикации

Тип данни	Място за съхранение на данни			
	Облак (Cloud)	IoT edge (GW, Edge router, Trust Center)	Крайно IoT устройство	Децентрализирано съхранение
Сензорни	[77]; [116]; [131]	[88]	[140]	[73]
Оперативни	[3]; [60]	[43]	[56]	[84]; [144]
Потребителски	[23]; [59]	[86]; [123]	[153]	[106]; [159]



Фиг. 1.1 Трислойна IoT архитектурна рамка



Фиг. 1.2 PRISMA анализ

Таблица 1.2 Съществуващи решения за защита на IoT мрежи

Подход	Метод		Литература				
			2024 г.	2023 г.	2022 г.	2021 г.	2020 г.
Blockchain	Консенсусни механизми	PoW	[104]; [122]	[129]			
		PoS	[122]				
		DPoS	[63]	[67]			
	Разпределен регистър	EOSIO	[63]				
		Hyperledger Fabric		[21]; [161]	[14]		
		Ethereum		[21]; [81]			
	Интелигентни договори		[63]; [104]	[21]; [67]; [81]; [144]; [161]	[2]; [14]; [28]	[38]; [95]	
Изкуствен интелект	Система за откриване на нарушение	SVM	[97]		[28]		
		RF	[128]				
		kNN		[22]; [81]			
		AE		[34]		[86]	
		RNN	[39]		[14]		
		GA		[93]		[86]	
	Система за предотвратяване на нарушение	FL		[45]			
		CNN		[137]			
Криптографски решения	Симетрични	AES	[165]	[100]	[125]		[70]; [123]
		Ascon					
		Blowfish	[10]				
	Асиметрични	ECC	[75]	[66]; [100]; [112]	[28]; [125]		
		ECDH		[6];[66]			
		RSA		[24]; [66]	[125]		
		HE	[92]		[14]	[138]	
		Digital Signatures – ECDSA	[75]	[144]	[28]	[95]; [155]	
		Digital Signatures – DSA		[6]			
		Digital Signatures – LMDS				[74]	
	Hash функции	SHA	[104]	[6]; [21]; [100]; [144]	[14]	[155]; [134]	[70]
		MD5				[86]; [134]	
		Ascon		[51]			

1.4 Изводи:

- С развитието на Индустрия 4.0 IoT мрежите намират все по-широко приложение в бизнеса. Те позволяват изграждане на сигурни транзакции.
- Прилагането на Blockchain за защитата на IoT данни предизвиква проблем с мащабируемостта, защото Blockchain мрежите създават затруднения при управлението на голямото количество данни, генерирани от IoT устройствата. Това може да доведе до трудности при управлението на голям обем данни и до забавяне в обработката.
- Сложността на интеграцията на Blockchain и IoT мрежи и липсата на стандартизация

увеличават разходите и предизвикателствата при внедряването на IoT екосистеми, които използват Blockchain. Тъй като не всички данни от IoT устройствата се съхраняват в Blockchain, остава проблема със сигурността на съхранените IoT данни в облак, както и проблема със сигурността по време на пренасянето им през мрежата (цялостност, интегритет, достоверност).

- Решенията за защита на IoT мрежи, базирани на Изкуствен интелект, позволяват проактивно откриване на нови и непознати заплахи чрез анализ на аномалии в мрежовия трафик. Те могат непрекъснато да се самообучават и адаптират към нови типове атаки, като DDoS или BotNet, и да идентифицират сложни модели на поведение в реално време. Подходящи са както за конвенционален мрежов трафик, така и за IoT мрежи. Но за IoT мрежи използването на системи с изкуствен интелект може да бъде скъпо и трудно за внедряване и увеличава потенциала за кибератаки, като създава нови рискове. Такива решения изискват голямо количество данни и изчислителни ресурси за обучение и анализ, което може да бъде предизвикателство за IoT устройства с ограничени ресурси. Нещо повече, при недостатъчно разнородни IoT данни изкуственият интелект може да създава неверни резултати, което усложнява откриването на нови заплахи и създава уязвимост към новите кибератаки.
- Установяването на надеждни и сигурни комуникационни канали е основно предизвикателство за IoT мрежите. Затова криптосистемите играят важна роля в IoT архитектурата, осигурявайки ефективна и сигурна комуникация, подобряваща поверителността, целостта и удостоверяването на предадените данни между IoT устройствата.
- Чрез използване на криптографски методи се подобрява защитата на комуникационните канали, данните генерирани от IoT устройства, както и управлението на тези устройства, като особен интерес представлява уязвимостта на обмяна на криптографските ключове между IoT устройствата.
- Криптографските решения са от решаващо значение за сигурността на IoT мрежите, като гарантират поверителност, цялостност и автентичност на данните, предотвратявайки неоторизиран достъп и манипулации.
- Различните методи като AES, RSA, SHA-256, MD5 и ECDSA се използват за шифроване, хеширане и подписване на данни, осигурявайки защита, когато устройствата обменят информация.
- Криптографските алгоритми като AES и RSA осигуряват защитена комуникация и са надеждни в критични системи, където поверителността е ключова. Чрез тях целостта на данните в рамките на WSN се защитават ефективно.
- Решения като ECC и оптимизирани версии на AES са подходящи за устройства с ограничени ресурси в IoT, предлагайки висока защита и минимално използване на ресурси.
- От разгледаните криптографски методи, най-използван е стандартизираният криптографски алгоритъм AES, тъй като е от съществено значение за сигурността на IoT мрежите.
- Въпреки, че протоколи като 6loWPAN, Wi-Fi, ZigBee, Bluetooth, Z-Wave и LoRaWAN са специално създадени за комуникация в IoT мрежа, все още съществуват уязвимости в сигурността по време на комуникационните сесии и не са открити напълно ефективни решения за предотвратяване на хакерски атаки. Затова особен интерес представлява изследването на подходи за повишавана на сигурността именно на тези протоколи.

Глава 2: Сигурност в IoT мрежи, базирани на ZigBee технология

Във втора глава са изложени мотивите за създаване на подход за повишаване на сигурността в IoT мрежи, реализирани със ZigBee безжична технология, чрез прилагане на криптографски алгоритми. Представена е структурата и функционалността на съществуващи подходи за управление на сигурността при обмена на ключове в ZigBee технология. Разгледани са съществуващи симулатори за ZigBee с техните предимства и недостатъци. Дефинирани са необходимите функционалности за симулатор, предоставящ възможността за изследване на сигурността в ZigBee мрежи за IoT. Представен е предложеният от автора на настоящия дисертационен труд специализиран симулатор за изследване сигурност в ZigBee мрежи за IoT.

2.1 ZigBee

Една от най-разпространените безжични технологии за IoT мрежи, предназначени за устройства с ограничени ресурси, използва комуникационния протокол ZigBee. Този протокол е проектиран така, че да осигури енергийно ефективна комуникация и минимално натоварване на паметта, което го прави подходящ за такива устройства [103]. ZigBee използва AES криптографски алгоритъм, заради ограничените изчислителни ресурси и памет на IoT устройствата. AES е основният алгоритъм за криптиране на данни, обменяни в ZigBee мрежи [48].

В настоящия дисертационен труд се изследват аспекти на сигурността на ZigBee технологията за IoT мрежи в симулационни условия и с реализация на ZigBee мрежи за различни случаи на употреба в контролирана лабораторна среда.

2.2 Сигурност в ZigBee мрежи

Сигурността на ZigBee мрежите се базира на стандарта IEEE 802.15.4 чрез използване на криптографски алгоритъм AES. Разработени са централизиран и разпределен модел за сигурност за управление на ключовете [40].

При централизирания модел, Trust Center (TC) отговаря за включването на устройства и сигурността на мрежата. Всички устройства в мрежата трябва да разпознават точно един активен TC [40].

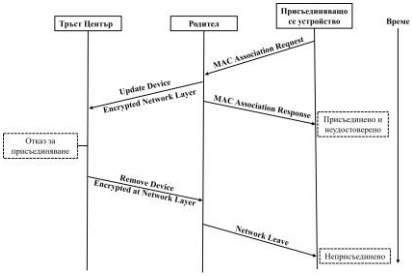
При мрежи с разпределен модел за сигурност мрежата се състои само от маршрутизатори и крайни устройства. В такъв модел всеки маршрутизатор може да удостоверява нови устройства при включването им в ZigBee мрежата.

За целите на сигурността, при използване на централизиран модел за сигурност, ZigBee стандартът дефинира ролята на TC. Тази роля е на устройството, на което се доверяват всички устройства в мрежата за разпространение и управление на ключове и мрежови конфигурации.

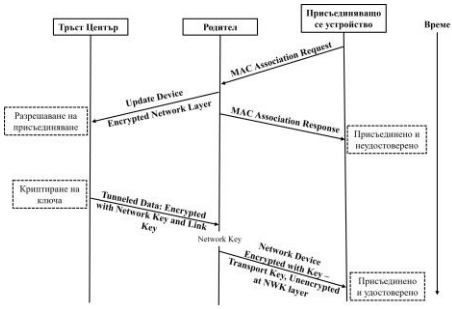
По време на процеса на присъединяване към ZigBee мрежа със сигурността, дефинирана по стандарт, устройството започва да използва MAC асоциация, за да се свърже със съвместимо родителско устройство. След като асоциацията е установена, то се присъединява към мрежата без удостоверяване, тъй като не притежава необходимия NWK. Преди да се присъедини устройството към мрежата, TC може да отложи изпращането на NWK и да оцени устройството, като изпрати произволни заявки за данни, за да събере повече информация за неговите възможности и характеристики, преди да вземе решение за удостоверяване [40].

При изпращане на успешен отговор на заявката за MAC асоцииране, маршрутизаторът комуникира с TC чрез изпращане на съобщение Update Device, показващо намерението на ново крайно устройство да се присъедини към ZigBee мрежата. Тъй като една от основните роли на TC е да оцени устройството дали е съвместимо с изискванията на мрежата, когато установи, че не отговаря на тези изисквания се инициира заявка от родителското устройство за неговото отстраняване (Фиг. 2.3) [40].

Ако устройството, изпратило заявка за присъединяване към мрежата, отговаря на изискванията за сигурност, поведението на TC варира в зависимост от това какъв предварително конфигуриран ключ (PLK) притежава крайното устройство и дали този ключ е съвместим с този на координатора и е 128-bit (Фиг. 2.4).



Фиг. 2.3 Отказан достъп за присъединяване към мрежата



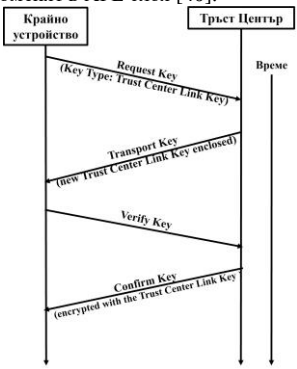
Фиг. 2.4 Присъединяване с помощта на PLK с TC

Според ZigBee стандарта предварително конфигурираните ключове за присъединяване към ZigBee мрежата могат да бъдат PLK, който е предварително конфигуриран от производителя за всички устройства, произведени от конкретен производител, Well-known Key (WK), дефиниран от ZigBee Alliance и Install Code (IC), който е предварително конфигуриран от производителя за всяко едно конкретно устройство [40].

Сигурността на APS подслоя работи независимо от сигурността на NW слой, тъй като според изискванията за сигурност в ZigBee мрежи, защитата на съобщенията, обменени в NW слоя са задължителни, за разлика от тези, които се обменят в APL слоя.

Съобщенията, обменящи се в APL слоя, които са некриптирани могат да бъдат приети или отхвърлени от отделни приложения. Съобщенията могат да бъдат криптирани като се използват едновременно APS и NW слоеве. В този случай първо се прилага защитата на APS подслоя, а след това защитата на NWK слой.

От край до край APS сигурността се реализира чрез обмен на ключ за връзка (LK) между източника и дестинацията – TCLK или APLK. При присъединяване към ZigBee мрежата, всяко устройство изисква нов, уникален TCLK, като изпраща заявка към TC. В отговор TC генерира индивидуален TCLK за устройството и го предава в криптиран вид, използвайки PLK. Устройството потвърждава получаването на ключа чрез командата APS Verify Key. След това TC изпраща финално потвърждение, криптирано с новия TCLK, което удостоверява успешното установяване на сигурна връзка (Фиг. 2.5). След установяването на връзката, TCLK се използва за сигурна комуникация, заместващи статичния LK и за изпращане и получаване на APS командни съобщения, които се обменят в APL слоя [40].



Фиг. 2.5 Заявка за нов TCLK

TCLK се използва в следните случаи:

- Криптиране на първоначалното предаване на NWK;
- Криптиране на актуализирано копие на NWK към възел, който повторно се присъединява и няма текущия NWK;
- Маршрутизатори, получаващи или изпращащи съобщения за сигурност в APS слоя от ZigBee стека. TC може да получава актуализации, които го информират за добавяне или повторно присъединяване към възли или да изпращат команди до маршрутизатори за изпълнение на функции за сигурност;
- APS криптиране чрез Unicast приложение, като получаващото или изпращащото устройство работи като TC.

Предназначението на ключовете APLK е да осигури криптиране на съобщения, които се обменят между две крайни устройства, комуникиращи в APL слоя или APS подслоя от ZigBee стека. Всяко крайно устройство може да притежава отделен APLK за комуникация с различни партньорски устройства. Ключът APLK може да бъде предварително конфигуриран от производителя или да бъде динамично генериран при установяване на връзка с друго устройство.

Когато крайното устройство няма предварително конфигуриран APLK, то изпраща заявка до TC, използвайки наличния TCLK за удостоверяване. Установяването на APLK може да се извърши по два подхода:

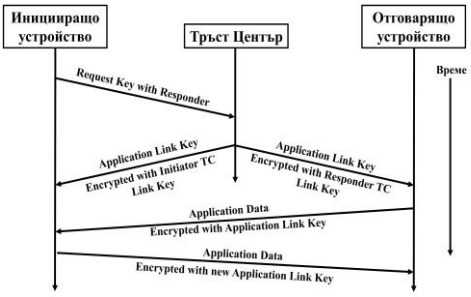
- Ръчно конфигуриране – ключът се въвежда в приложението чрез задаване на стойността за съответното партньорско устройство.
- Автоматично установяване – изпраща се заявка за създаване на криптиран канал между двете крайни устройства.

EmberZNet PRO стека предлага два метода за установяване на APLK чрез TC – стандартен (Фиг. 2.6) и нестандартен (Фиг. 2.7) [143].

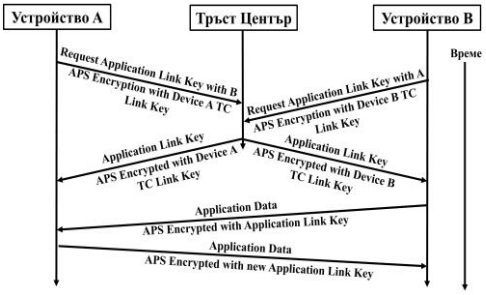
При стандартния метод, устройството изпраща заявка до TC, който генерира и изпраща APLK до двете устройства, независимо дали партньорското устройство е активно. Недостатъкът в този метод е възможността партньорското устройство да бъде неактивно.

В такъв случай ключът може да не достигне до него и комуникацията между устройствата да остане некриптирана.

При нестандартния метод всяко устройство в мрежата, включително и координатора трябва предварително да бъде конфигурирано за използването му. В такъв случай и двете крайни устройства изпращат заявка до TC за установяване на връзка чрез TCLK. След това, TC генерира произволен APLK и го предоставя на двете устройства. Методът се счита за по-надежден, тъй като потвърждава активното състояние на партньорското устройство и способността му да получава APLK. По този начин се намалява риска някое от устройствата да не получи ключа.



Фиг. 2.6 Заявка за APLK (стандартен метод)



Фиг. 2.7 Заявка за APLK (нестандартен метод)

2.3 Анализ на съществуващи симулатори за ZigBee мрежи

Съществуват симулационни продукти, които могат да се използват за симулиране на ZigBee мрежи за IoT. За целите на настоящия дисертационен труд са представени симулатори, с които може да се анализират определени аспекти на ZigBee мрежи.

Симулаторът NS2 поддържа различни протоколи за безжичен контрол на достъпа до средата (MAC), като IEEE 802.11 (Wi-Fi) и IEEE 802.15.4 (ZigBee) [115], но не предоставя възможност за визуализация на обменяните съобщения между устройствата в процеса на свързване към мрежата, не предоставя визуализация на формата на съобщенията, не предоставя възможност за изследване на сигурността на обменяните съобщения и как това влияе на сигурността на изградената мрежа [115].

Чрез вградените инструменти на NS3, могат да се наблюдават ключови показатели за производителност на ZigBee мрежата, включително и данни за производителността на мрежата в реално време [118], но не предоставя възможност за визуализация на обменените съобщения или тяхната форма, което затруднява задълбочения анализ на процесите, свързани със сигурността.

Симулаторът Cooja може да се използва за симулиране на различни алгоритми за маршрутизиране, както и за анализ на въздействието на определени хакерски атаки, при условие че те бъдат предварително моделирани от потребителя [37, 162], но не поддържа специфични компоненти на ZigBee като APS, ZDO и функционалност на TC.

Симулаторът CupCarbon е проектиран с цел симулиране на IoT мрежи в контекста на умни градове [7], но не предоставя възможност за детайлна визуализация на обменените съобщения и не поддържа ключови механизми за сигурност в ZigBee, като функции на TC и криптографски операции.

Симулаторът EmStar е инструмент за симулация, който предлага прост и ясен модел на среда за проектиране, изграждане и внедряване на разнородни сензорни мрежови приложения [36], но не поддържа ключови механизми за сигурност в ZigBee мрежи като функции на TC и криптографски операции.

Със SensorSim може да се симулират IEEE 802.15.4 мрежи, които са безжични сензорни мрежи с ниска мощност и ниска скорост на предаване на данни, поддържащи протоколи като ZigBee [126], но не предоставя възможности за реалистично моделиране на криптографски алгоритми и управление на ключове, нито поддържа функции на TC.

Симулаторът OpNet се използва за възпроизвеждане на различни ZigBee безжични мрежови топологии, включително конфигурации на „звезда“, „дърво“ и разширена „звезда“ [164], но не предоставя възможност за симулиране на криптографски процеси, а възможностите му за моделиране на TC процедури са ограничени.

2.4 Критерии за сравнение на симулатори за ZigBee мрежи

За изследване на сигурността в ZigBee мрежи е необходима както реална, така и симулационна среда. Необходимо е симулаторите, които се използват за такива изследвания, да отговарят на определени критерии, които са свързани с ефективното изследване на процесите, свързани със сигурност и надеждност на ZigBee мрежи.

Разгледаните симулатори могат да бъдат сравнени по следните критерии:

- Възможност да работи на повече от една операционна система – критична функционалност на симулаторите за осигуряване на гъвкавост и интеграция в различни изследователски среди. Ограничаването до една операционна система може значително да ограничи тяхната употреба и да намали ефективността на изследователските процеси [64];
- С отворен код – симулаторите с отворен код позволяват адаптиране на функционалността спрямо специфичните изисквания на проекта и осигурява прозрачността на симулациите [64];
- Симулиране на атаки – симулаторите, отговарящи на този критерий, позволяват изследване на уязвимостите на ZigBee мрежите и тестване на методи за тяхното предотвратяване.

Ограниченият набор от предварително дефинирани сценарии за атаки е недостатък [17];

- Възможност за симулиране на функционалности на мрежово ниво – симулаторите, предоставящи възможността за изследване на процесите и взаимодействията между слоевете като мрежовия и приложния, могат да бъдат ефективни в цялостното представяне на процесите за сигурност в мрежата [64];
- Възможност за симулиране на функционалности на приложно ниво.

За да се направи по-точна оценка на симулаторите, от гледна точка на възможности за изследване на сигурност в IoT мрежи, базирани на ZigBee протокол, в настоящия дисертационен труд са предложени следните специфични критерии:

- Тестване на криптиране – симулаторите, предоставящи реалистични криптографски модели позволяват оценка на устойчивостта на използваните алгоритми. Липсата на такива модели може да компрометира изводите относно сигурността на мрежата;
- Поддръжка на Trust Center процедури – реалистичното моделиране на функционалността на TC в симулатора е от съществено значение за представяне на процесите за сигурност;
- Управление на ключове – симулаторите, осигуряващи прозрачност на процесите, генериране и обмен на криптографски ключове, позволяват точна оценка на ефективността на управлението на ключове;
- Проследяване на състоянието на устройствата – функционалност на симулаторите, предоставяща възможност на изследователите да наблюдават състоянията на устройствата, които могат да бъдат активни или неактивни. Такава функционалност позволява да се направи ефективен анализ на мрежата;
- Подробна визуализация на процесите – функция, предоставяща възможност за по-добър анализ и интерпретация на резултатите. Липсата на такава визуализация може да затрудни анализа на проблемите, свързани с процесите за сигурност.

2.5 Предложен симулатор за изследване на процесите за сигурност в ZigBee мрежи

За целите на дисертационния труд е разработен симулатор ZBeeSiM за ZigBee мрежи, предназначен за анализ на процесите, свързани със сигурността на ZigBee мрежи, чрез моделиране на различни сценарии на реална употреба. Подробното описание на работата на симулатора е представено в Приложение 2.

Фиг. 2.8. Архитектура на ZBeeSiM

Симулаторът е реализиран с отделни модули с цел бъдещо разширение на функционалността му. Архитектурата му е представена на Фиг. 2.8. Алгоритъмът за работа с предложения в дисертационния труд симулатор е представен на Фиг. 2.9.

Симулаторът ZBeeSiM включва няколко основни модула, които дават възможност да се наблюдават процесите на заявка, генериране и обмен на ключове в NW и APL слоеве от ZigBee стека. Той предоставя възможност за анализ на ниво на сигурност при използване на трите видове PLK, дефинирани в ZigBee стандарта. За анализ могат да се използват параметри като размер на AES ключа, който в настоящата работа е 128-bit, тегловен коефициент според вида на използвания PLK, средно време за криптиране и количество обменени данни. Нивото на сигурност се изчислява на база на аналитичен израз, който включва тези параметри и е предложена в дисертационния труд (подробно представена в т.2.6).

За да се симулира свързването на крайните устройства към ZigBee мрежа е добавена опция за конфигуриране на координатора и крайното устройство с предварително конфигуриран ключ, който може да бъде PLK, WK и IC (Фиг. П2.5, Фиг. П2.6). Използвайки тези ключове, когато устройствата са свързани към мрежата, NWK и TCLK могат да бъдат получени криптирани [40].

Симулаторът предоставя възможност за проследяване на състоянието за свързване към мрежата, включително дали устройството е успешно свързано, поредният номер на NWK и криптираната му версия (Фиг. П2.8, Фиг. П2.9, Фиг. П2.10).

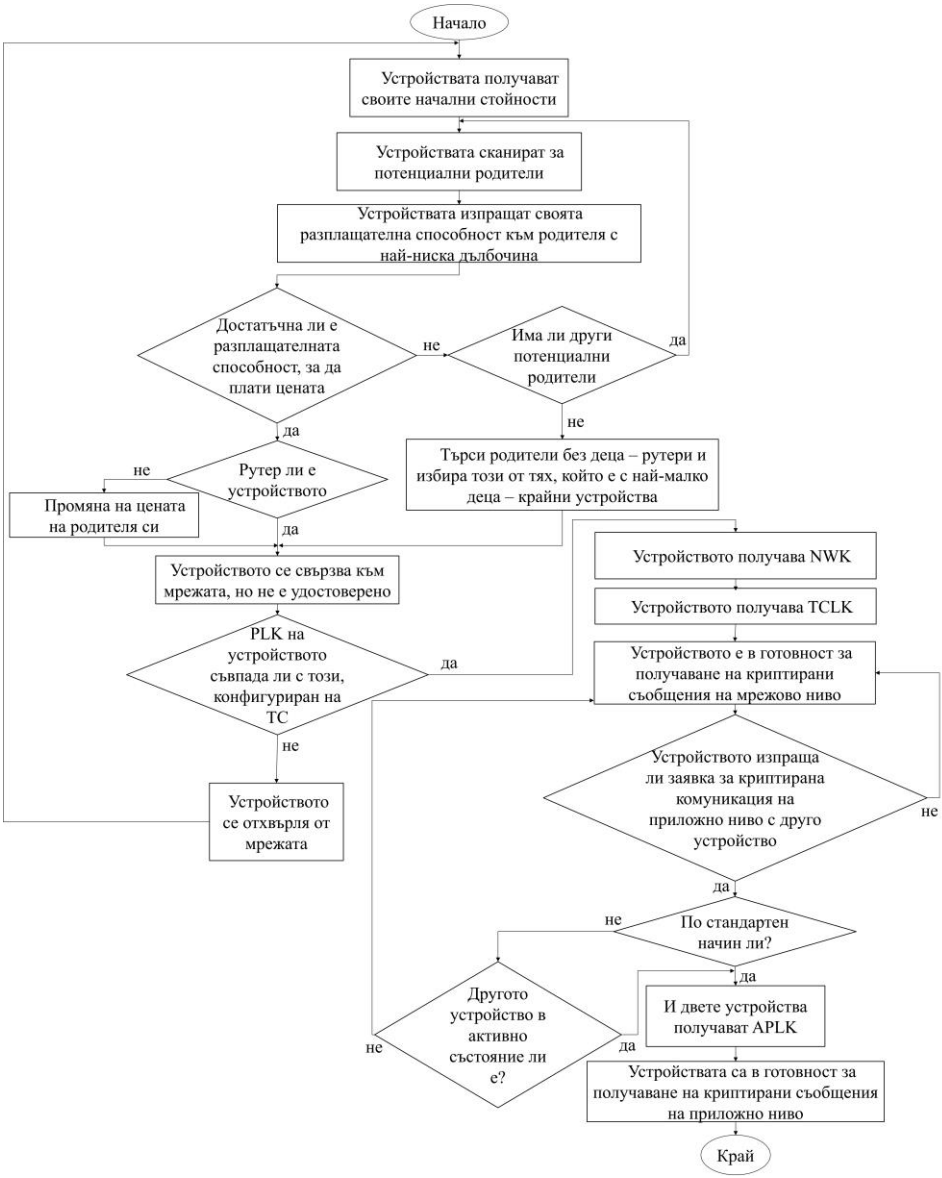
При избор на устройството, което ще инициира процеса на свързване към ZigBee мрежата се генерира визуализация на процеса на сигурна връзка със ZigBee координатора (Фиг. П2.8, П2.9). Представен е процесът, при който крайното устройство, след като се идентифицира и свърже към мрежата получава криптиран NWK от TC.

След като крайното устройство получава генерирания от TC ключ NWK, се симулира генерирането и получаването на TCLK, като ключовете се визуализират както в криптиран, така и в некриптиран вид (Фиг. П2.10). Симулаторът моделира заявките към TC за комуникация между крайните устройства, използвайки TCLK за генериране на APLK за криптиране на комуникацията, осъществена в APL слоя. (Фиг. П2.13, Фиг. П2.14)

В отделен раздел в симулатора се представя таблица с резултати от заявките за установяване на APLK, където може да се проследяват идентификатори, състояние за активност и неактивност на устройствата, генерираните ключове и криптираните им версии (Фиг. П2.16, Фиг. П2.17).

В отделен раздел в симулатора се предоставя възможност за симулиране на мрежови атаки в ZigBee мрежата (Фиг. П2.22, Фиг. П2.23, Фиг. П2.24).

Кодът на предложените функции в симулатора е представен в Приложение 4.



Фиг. 2.9 Алгоритъм за работа на ZBeeSiM

2.6 Сравнение на съществуващи симулатори с предложения симулатор ZBeeSiM

С така формирания набор от критерии, в т.2.4 на настоящия дисертационен труд за аспекти, свързани със сигурността на ZigBee мрежи, в Таблица 2.1. са сравнени съществуващите симулатори с предложения в дисертационния труд симулатор.

Таблица 2.1 Сравнение на предложения симулатор и разгледаните симулатори

	NS2	NS3	Cooja	CupCarbon	TOSSIM	EmStar	SensorSim	OpNet	ZBeeSiM
Възможност да работи на повече от една операционна система	да	да	не	да	не	не	не	да	не
С отворен код	да	да	да	да	да	да	да	не	да
Симулиране на атаки	да, частично	да, частично	да, частично	не	не	не	не	не	да
Възможност за симулиране на функционалности на мрежово ниво	да, частично	да, частично	да, частично	да, частично	да, частично	да, частично	да, частично	да, частично	да
Възможност за симулиране на функционалности на приложно ниво	не	не	не	не	не	не	не	да, частично	да
Тестване на криптиране	не	да, частично	да, частично	не	не	не	не	не	да
Поддръжка на Trust Center процедури	не	не	не	не	не	не	не	не	да
Управление на ключове	не	не	не	не	не	не	не	не	да
Проследяване на състоянието на устройствата	не	не	не	не	да, частично	не	не	не	да
Подробна визуализация на процесите	не	не	да, частично	да, частично	не	не	не	да, частично	да

2.7 Предложен аналитичен израз за изчисляване на ниво на сигурност в ZigBee мрежи и скала за определяне на степените за ниво на сигурност

Тъй като ZigBee стандартът дефинира 3 вида предварително конфигурирани ключове за присъединяване на устройствата към ZigBee мрежата, в настоящия дисертационен труд се анализира нивото на сигурност, използвайки всеки един от тези ключове. Освен предварително конфигурираните ключове на нивото за сигурност влияят и други фактори като: време за криптиране, количество данни, които се криптират и размер на криптографския ключ.

В редица изследвания се споменава терминът – ниво на сигурност. В разгледаната литература обаче няма ясно дефиниран подход или конкретен аналитичен израз за изчисляване на параметър ниво на сигурност [26, 33, 46, 57, 96, 110, 157].

В проучването [50] е представено, че когато се използва по-голям размер на криптографския ключ сигурността се увеличава. В ZigBee мрежата, по стандарт, сигурността се осигурява с

предварително конфигурирани ключове – WK, PLK и IC. В зависимост от използвания предварително конфигуриран ключ сигурността може да се подобри [40].

Според проучването [76] параметрите време за криптиране и размер на данните оказват отрицателно влияние върху сигурността. Колкото повече се увеличава времето за криптиране и размерът на данните, които трябва да бъдат криптирани, толкова повече сигурността намалява.

Тъй като в дисертационния труд обект на изследванията е ZigBee технологията за IoT, която е приложима за устройства с ограничени ресурси, в аналитичния израз за изчисляване нивото на сигурност се използват само параметрите, посочени в разгледаната литература.

За да се изчисли стойността на нивото на сигурност, се вземат предвид параметри, които имат както положително, така и отрицателно влияние върху сигурността в ZigBee мрежите, а именно:

Размер на AES ключа – по-големият размер на ключа повишава нивото на сигурност. В настоящия дисертационен труд е използван 128-битовият AES ключ, дефиниран в стандарта ZigBee. Единицата за този параметър е бит.

Тегловен коефициент за използвания предварително конфигуриран ключ – предлага се да се използват коефициенти на тегло 1, 2 и 3, като нивото на сигурност се увеличава с увеличаване на стойността. Използването на Well-known link key влияе най-малко на нивото на сигурност, следователно стойността е 1. Когато се използва Pre-configured link key, нивото на сигурност е по-високо, тогава стойността е 2, а когато се използва Install code, нивото на сигурност е най-високото и стойността е 3.

Средно време за криптиране от 10 измервания за дадено конкретно устройство – с увеличаване на времето за криптиране нивото на сигурност намалява. Единицата за този параметър е милисекунди (ms). Броят 10 е емпирично установен като оптимален, т.к. с увеличаване на броя на опитите над 10 (до максимум 100) средното време се различава в рамките на приетото допустимо отклонение от 0.1%, което не повлиява на оценката на нивото на сигурност, а времето за получаване на резултат при 10 измервания е значително по-кратко.

Количеството данни, обменящи се между устройствата – с увеличаване на количеството данни, времето и сложността за обработката им се увеличават, намалявайки нивото на сигурност. За целите на изследването в дисертационния труд данните представляват 128-битовия мрежов ключ, обменян от центъра за сигурност към крайното устройство. Мерната единица за този параметър е бит.

При така представените параметри, тези с положително влияние върху сигурността се дефинират като правопропорционални спрямо изменението на нивото на сигурност и могат да бъдат поставени в числител, а тези с отрицателно влияние върху сигурността се дефинират като обратнопропорционални спрямо изменението на нивото на сигурност и могат да бъдат поставени в знаменател при формиране на аналитичен израз за количествен измерител на нивото на сигурност. Предложеният аналитичен израз за изчисляване на нивото на сигурност в ZigBee мрежи е:

$$S = \frac{k.w}{T.D} \tag{2.1}$$

където:

- S – ниво на сигурност;
- k – размер на AES ключа;
- w – тегловен коефициент за използвания предварително конфигуриран ключ;
- T – средно време за криптиране от 10 измервания за конкретно устройство;
- D – количеството данни, обменящи се между устройствата.

За определяне на нивата на сигурност е предложена скала с ниско, средно и високо ниво на сигурност, които са дефинирани въз основа на резултатите от изчисленията на S по предложения аналитичен израз, а именно:

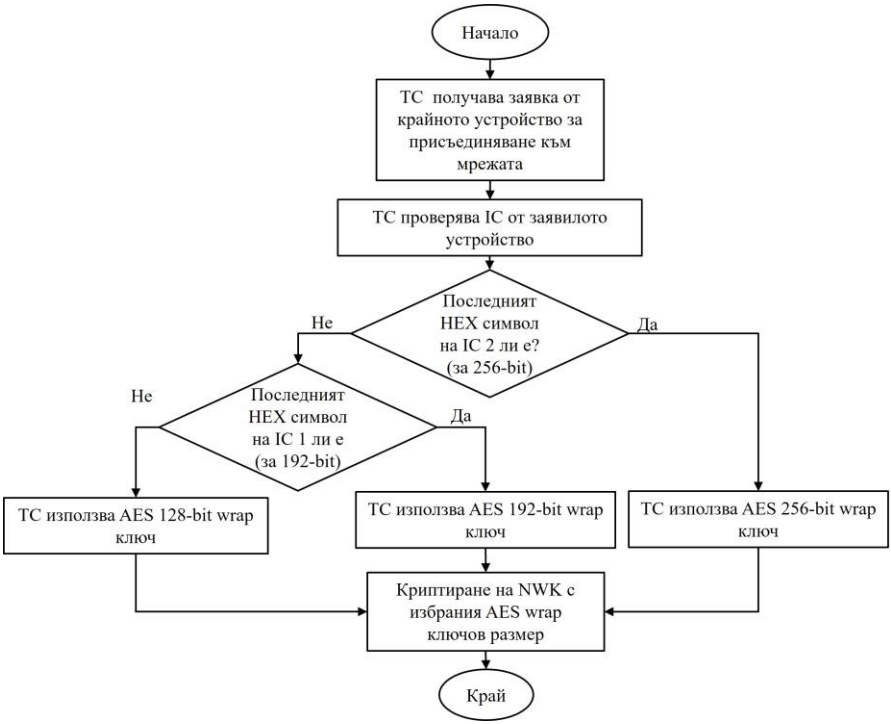
- От 0 до 1 се дефинира за ниско ниво на сигурност;
- От 1 до 2 се дефинира за средно ниво на сигурност;
- От 2 или повече от 2 се дефинира за високо ниво на сигурност.

Така предложеният аналитичен израз и скалата за измерване на ниво на сигурност са имплементирани в предложения симулатор ZBeeSiM за целите на анализа на сигурността в ZigBee мрежи.

2.8 Предложен адаптивен подход за подобряване на нивото на сигурност в ZigBee мрежи

В ZigBee PRO 2023 са въведени редица подобрения в сигурността, включително Dynamic Link Key и Device Interview [40]. Въпреки стандартните механизми, определени от ZigBee спецификациите, комуникационната среда остава уязвима на множество атаки [119]. Ограничената адаптивност към хардуерните възможности и липсата на гъвкави подходи за защита възпрепятстват установяването на сигурна и надеждна комуникация. Предаването на NWK обаче остава обвито в AES-128 wrap key, дори когато устройствата поддържат по-силни алгоритми като AES-192 и AES-256. Докато AES-192/256 са одобрени от NIST и широко използвани в други индустрии [48], настоящата спецификация на ZigBee няма механизъм за динамичен избор или договаряне на размера на wrap key въз основа на възможностите на устройството [40, 149]. Това ограничение води до неефективно използване на наличното хардуерно ускорение. В критични за сигурността среди това може да компрометира цялостната сигурност на мрежата и нейната устойчивост.

За подобряване на нивото на сигурност в ZigBee мрежите в настоящия дисертационен труд се предлага адаптивен подход, който позволява адаптиране на AES ключ за всяко устройство в мрежата чрез автоматизиран или ръчен режим. Подходът е приложим при използване на устройства с IC, тъй като ZigBee стандартът препоръчва използването на такъв вид PLK за по-добра сигурност. Независимо от използвания режим на конфигурация – автоматизиран или ръчен, TC определя поддържаните от устройството криптографски възможности чрез интерпретиране на последния символ на IC. По подразбиране крайните устройства използват IC, чрез който TC интерпретира максималните им криптографски възможности. В автоматичен режим TC интерпретира тази информация и избира най-големия AES wrap key размер за криптиране на NWK за всяко устройство, а в ръчен режим мрежовият администратор задава желания AES wrap key размер за всяко устройство по време на конфигурирането на системата чрез промяна на IC (Фиг. 2. 10).



Фиг. 2.10 Предложен адаптивен подход за вземане на решения за избор на размер на AES ключ в ТС въз основа на възможностите на устройството

2.9 Изводи:

- ZigBee технологията е една от най-разпространените технологии за изграждане на мрежи за IoT устройства.
- Значението на сигурността при ZigBee мрежите става все по-голямо.
- ZigBee мрежите използват криптографски алгоритъм AES за криптиране на данни.
- Подходящи за изследване на определени аспекти на сигурността на ZigBee технологията за IoT мрежи са както симулационни условия, така и изследване на ZigBee мрежи за различни случаи на употреба в контролирана лабораторна среда.
- Разгледаните симулатори предлагат възможност за симулиране на определени аспекти като производителност, мащабируемост и надеждност на протокола ZigBee в IoT мрежи.
- Разгледаните симулатори NS-3, Cooja и CupCarbon позволяват симулация на определени типове атаки, включително DoS и Spoofing атаки.
- Разгледаните симулатори нямат функционалност за детайлно представяне на съобщенията и процесите, свързани със сигурността в ZigBee – като генериране, управление и обмен на криптографски ключове за защита на информацията, която се пренася в съобщенията както и процесите в приложния слой от ZigBee стека.
- Разгледаните симулатори не предлагат инструмент за управление на ключове, който да

обхваща генерирането, разпространението и криптирането на NWK и APL ключове в реално време.

- Разгледаните симулатори не предоставят подробна визуализация за проследяване на състоянието на устройствата и криптографски операции като AES криптиране.
- Разгледаните симулатори не предлагат интегрирано решение за тестване на криптиране.
- Повечето от разгледаните симулатори имат висока цена за ползване на продукта, сложен графичен потребителски интерфейс, невъзможност за симулиране на мрежа с множество възли, сложна настройка на продукта, довеждат до натоварване на компютърната система, не предоставят или трудно се модифицира предоставеният код.
- Предложеният симулатор е с отворен код и е изграден на модулен принцип, което позволява допълване на неговите функционалности.
- Предложеният симулатор е с удобен интерфейс.
- Предложеният симулатор предлага следната функционалност по отношение на изследване на сигурност в IoT мрежи, реализирани със ZigBee като симулиране на процеса присъединяване на устройствата към ZigBee мрежа, възможност за криптиране на обменените съобщения и ключове, използвайки AES, възможност за анализ на ниво на сигурност на ZigBee устройства, реализиране на кибератаки като Sniffing, Brute Force и Dictionary.
- Предложена е система от показатели за оценяване на симулационни продукти за изследване сигурността в IoT мрежи, реализирани със ZigBee протокол и е направено сравнение на съществуващите симулатори и предложения такъв.
- Предложен е аналитичен израз, с който количествено може да се изрази качествения показател „сигурност“ в IoT мрежа.
- Предложеният аналитичен израз е имплементиран в симулатора ZBeeSiM.
- Предложеният адаптивен подход за подобряване нивото на сигурност в ZigBee мрежи е част от подхода за повишаване на сигурността в IoT мрежа, реализирана със ZigBee.
- Предложеният адаптивен подход за подобряване нивото на сигурност в ZigBee мрежи е имплементиран в модула за сигурност на симулатора ZBeeSiM.

Глава 3. Експериментални изследвания и резултати

В тази глава са направени експерименти за изследване на процеси, свързани със сигурността в ZigBee мрежи както в симулационна, така и в реална среда. Изследван и валидиран е предложеният подход за повишаване на нивото на сигурност, използвайки предложения в настоящия дисертационен труд симулатор ZBeeSiM.

Симулационните изследвания обхващат различни сценарии, като генериране, предаване и използване на криптографски ключове на мрежово и приложно ниво от ZigBee стека, проследяване на състоянията на устройствата. Направени са експерименти, свързани с ниво на сигурност при използване на различни предварително конфигурирани ключове и предложения в дисертационния труд подход за избиране на по-голям AES wrap ключ, според криптографските възможности на устройствата.

Извършен е комплексен сравнителен анализ на съществуващи симулатори, базиран на десет дефинирани критерия, чрез изчисляване на средна аритметична и средна геометрична оценка.

Изградена е и прототипна ZigBee мрежа с TI устройства, в която са проведени експерименти за удостоверяване чрез Well-Known Key и Install Code. Процесите на свързване и обмен на ключове са анализирани с помощта на Wireshark и sniffer устройство.

3.1 Качествени и количествени параметри за анализ на качествата на предложения симулатор в т.2.5 ZBeeSiM

За да се изчисли комплексният показател за качество, се избира една от следните математически зависимости – квадратична, геометрична, аритметична или хармонична.

Методът [1] с усреднени комплексни оценки може да се използва по подобен начин и за реализиране на сравнителен анализ между симулационни продукти за изследване на сигурността в ZigBee мрежи.

Комплексната оценка се извършва въз основа на десет критерия, представени в Глава 2. Те отразяват функционалности, свързани със симулиране и изследване на сигурността в мрежовия и приложния слой от ZigBee стека. Комплексният анализ се избира да се основава на средна аритметична и средна геометрична оценка, които се оценяват съответно по формулите (3.1) и (3.2).

$$R_a = \frac{\sum_{i=1}^{n} b_i d_i}{\sum_{i=1}^{n} b_i} \tag{3.1}$$

$$R_g = \left(\prod_{i=1}^{n} {d_i}^{b_i}\right)^{\frac{1}{\sum_{i=1}^{n} b_i}} \tag{3.2}$$

В (3.1) и (3.2) нормализираната количествена оценка на $i^{-тия}$ показател е:

$$0 \le d_i \le 1 \tag{3.3}$$

n – брой показатели, а b_i е $i^{-тият}$ тегловен коефициент, като

$$\sum_{i=1}^{n} b_i = 1 \tag{3.4}$$

За целите на изследването, тегловните коефициенти се избира да бъдат еднакви. Тъй като тегловните коефициенти са избрани да бъдат еднакви, формулите за средна аритметична (3.1) и средна геометрична (3.2) комплексна оценка може да се променят във вида представен съответно в (3.5) и (3.6).

$$R_a = \frac{1}{n}\sum_{i=1}^{n} d_i \tag{3.5}$$

$$R_g = \prod_{i=1}^{n} {d_i}^{\frac{1}{n}} \tag{3.6}$$

Реализирането на комплексен сравнителен анализ позволява да се избегне субективността на автора при оценяване на обекта на сравнение. Изборът на геометрична и аритметична математическа зависимост се определя като оптимален от гледна точка на състоятелност, нормираност и сравнимост. Грешките в оценките на единичните показатели при използване на геометрична и аритметична зависимост осигуряват компромисно изпълнение на условията за максимална чувствителност при влошаване на единичните показатели за качество и минимална чувствителност към грешките при определянето им.

За целите на сравнението, качествените оценки в Таблица 2.1 са количествено преобразувани по следния начин:

- да – със стойност 1, което означава, че се поддържа напълно;
- да, частично – със стойност 0.5, което означава, че се поддържа частично;
- не – със стойност 0, което означава, че не се поддържа.

В Таблица 3.2 е представена средна аритметична и средна геометрична комплексна оценка на всеки от симулаторите, представени подробно в таблица 3.1.

Според резултатите, получени за комплексните оценки, може да се твърди, че предложеният в дисертационния труд симулатор ZBeeSiM е по-добър от останалите.

Таблица 3.2. Средна аритметична и средна геометрична комплексна оценка на симулаторите по отношение на функционалности, свързани с изследване на сигурност в ZigBee мрежи

Комплексна оценка	NS2	NS3	Cooja	CupCarbon	TOSSIM	EmStar	SensorSim	OpNet	ZBeeSiM
R_a	0.3	0.35	0.35	0.3	0.25	0.2	0.2	0.25	0.9
R_g	0.71	0.66	0.56	0.71	0.59	0.63	0.63	0.59	1.00

Това се дължи на широкия спектър от поддържани функции, свързани със симулиране и изследване на сигурността в ZigBee мрежи, включително пълната поддръжка на процедури на Trust Center, управление на криптографски ключове и детайлна визуализация на криптографските процеси.

При детайлен анализ на отделните критерии се наблюдава, че някои симулатори предлагат частична поддръжка на специфични функционалности, като симулиране на атаки или визуализация, но не покриват пълноценно целия набор от изисквания за изследване на сигурността.

Изчислените комплексни оценки осигуряват сравнимост на резултатите и намаляват субективността в оценяването на симулационните среди. Според представените резултати от изследването поради широкия набор от разглеждани критерии най-подходящи за изследване на сигурността в ZigBee мрежи са както предложения в настоящия дисертационен труд симулатор, така и в достатъчна степен NS2 и CupCarbon, докато EmStar и SensorSim предоставят най-малко функционалности, свързани с аспектите на сигурността.

Предложеният симулатор ZBeeSiM е най-добър сред разгледаните според предложените критерии, като същевременно предоставя полезни възможности както за научни анализи, така и за образователни цели.

3.2 Изследване на времето за криптиране с различни размери на AES

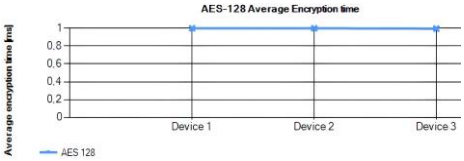
Целта на този експеримент е да се изследва времето за криптиране на ключовете при различни размери на AES ключа. За тази цел е използван предложеният в дисертационния труд симулатор ZBeeSiM.

Докато ZigBee мрежата теоретично поддържа до 65 000 устройства, в практиката броят е по-малък и зависи от конкретната конфигурация. IoT устройства, захранвани от батерии, имат по-ограничени възможности за предаване на сигнали, което може да намали броя на устройствата, които могат да бъдат свързани в мрежата. Директно свързани устройства в топология „звезда“ към ZigBee координатора могат да бъдат до 64. В дисертационния труд за целите на сравнимост на получените резултати с реална мрежа са направени изследвания в ZigBee мрежа, състояща се от 3, 5 и 7 едновременно свързани крайни устройства към координатора в топология „звезда“, конфигурирани с IC (Фиг. 3.1, Фиг. 3.5, Фиг. 3.9). Разгледани са 2 различни сценария.

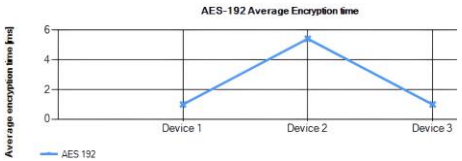
В първия сценарий се изследва времето за криптиране при увеличаване на броя устройства за всеки от различните размери на AES:

- 3 крайни устройства – средното време за криптиране от 10 независими измервания с AES 128-битово криптиране е 1 ms. При използване на AES 192-битово криптиране за първото и третото устройство средното време е 1 ms, а за второто е близо 6 ms. При AES 256-битово

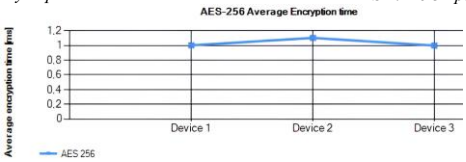
криптиране средното време за първото и третото устройство е 1 ms, а за второто е близо 1,2 ms (Фиг. 3.5, Фиг. 3.6, Фиг. 3.7).



Фиг. 3.5 Средно време за криптиране при използване на AES 128 с 3 крайни устройства

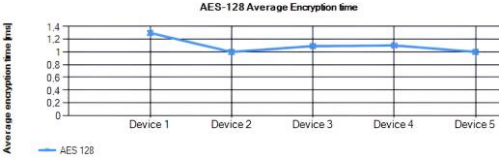


Фиг. 3.6 Средно време за криптиране при използване на AES 192 с 3 крайни устройства

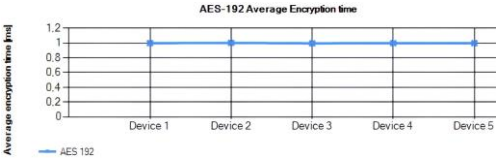


Фиг. 3.7 Средно време за криптиране при използване на AES 256 с 3 крайни устройства

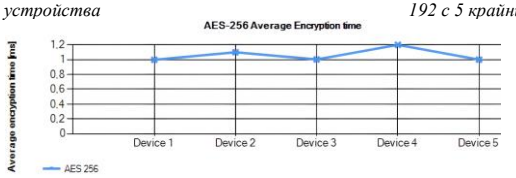
- 5 крайни устройства – средното време за криптиране от 10 независими измервания при използване на AES 128-битово криптиране за второто и петото устройство е 1 ms, а при използване на AES 256-битово криптиране за първото, третото и петото устройство е 1 ms. При използване на AES 192-битово криптиране всички устройства са със средно време 1 ms. Отклонения в средното време за криптиране се наблюдават при използване на AES 128-битово и 256-битово криптиране. При използване на AES 128-битово криптиране е 1,3 ms за първото устройство, 1,1 ms за третото устройство и 1,1 ms за четвъртото. При използване на AES 256-битово криптиране е 1,1 ms за второто устройство и 1,2 ms за четвъртото устройство (Фиг. 3.12, Фиг. 3.13, Фиг. 3.14).



Фиг. 3.12 Средно време за криптиране при използване на AES 128 с 5 крайни устройства

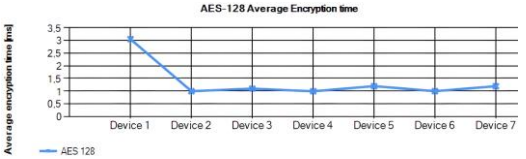


Фиг. 3.13 Средно време за криптиране при използване на AES 192 с 5 крайни устройства

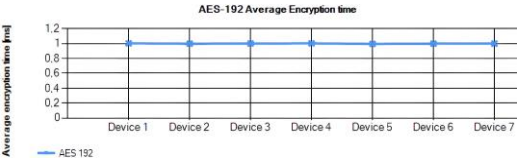


Фиг. 3.14 Средно време за криптиране при използване на AES 256 с 5 крайни устройства

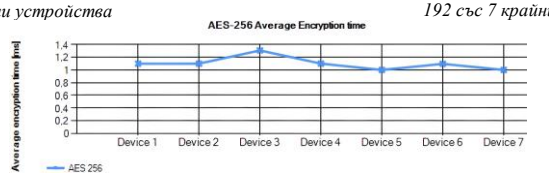
- 7 крайни устройства – средното време за криптиране с AES 128 битово криптиране за устройствата 2, 3, 4 и 6 е 1 ms за десет независими измервания. За устройствата 5 и 7 средното време е 1,2 ms, а най-голямото отклонение е за устройство 1 и достига 3 ms. При използване на AES 192-битово криптиране всички устройства показват средно време от 1 ms. При използване на AES 256-битово криптиране устройствата 5 и 7 отчитат време от 1 ms, докато устройствата 1, 2, 3, 4 и 6 показват малко отклонение от 1,1 ms. Най-голямото отклонение при използване на AES 256 е за устройство 3, което е 1,3 ms (Фиг. 3.19, Фиг. 3.20, Фиг. 3.21).



Фиг. 3.19 Средно време за криптиране при използване на AES 128 със 7 крайни устройства



Фиг. 3.20 Средно време за криптиране при използване на AES 192 със 7 крайни устройства

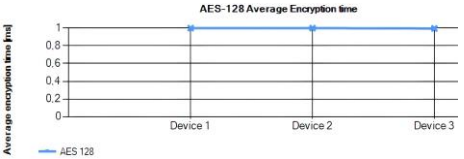


Фиг. 3.21 Средно време за криптиране при използване на AES 256 със 7 крайни устройства

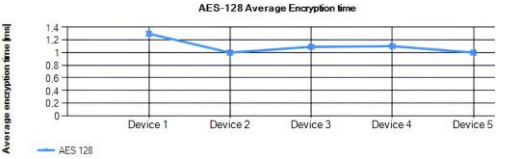
Времето за криптиране при използване на 128-, 192- и 256-битови AES ключове остава приблизително 1 ms, независимо от броя на устройствата (3, 5 или 7), включени в мрежата. Въпреки това за мрежа от 7 устройства се наблюдават по-големи отклонения, като най-значителното е 20 ms при използване на 128-битово криптиране. Въпреки тези редки отклонения, средното време за криптиране запазва стабилност, което показва добра мащабируемост и устойчивост на криптиращия процес при нарастващ брой устройства.

Във втория сценарий се изследва времето за криптиране за един и същ размер на AES ключа, но с различен брой устройства. Топологиите с 3, 5 и 7 крайни устройства са представени съответно на Фиг. 3.1, Фиг.3.8 и Фиг. 3.15. Работи се с три различни размера на ключа:

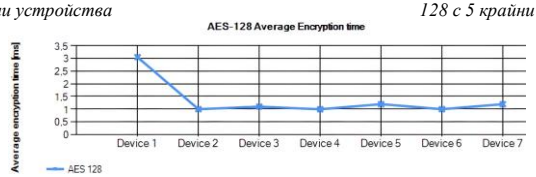
- Използване на AES 128 – средното време за криптиране с 3, 5 и 7 устройства е 1 ms, като най-големите отклонения с 5 и 7 устройства са отчетени за устройство 1 и са съответно 1,3 ms и 3 ms (Фиг. 3.25, Фиг. 3.26, Фиг. 3.27).



Фиг. 3.25 Средно време за криптиране при използване на AES 128 с 3 крайни устройства

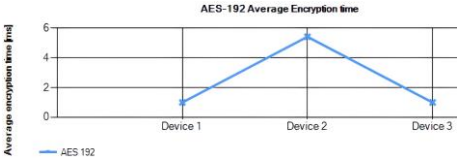


Фиг. 3.26 Средно време за криптиране при използване на AES 128 с 5 крайни устройства

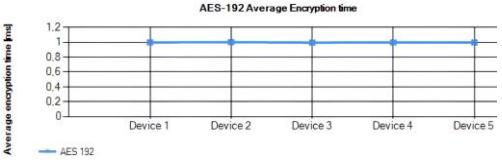


Фиг. 3.27 Средно време за криптиране при използване на AES 128 със 7 крайни устройства

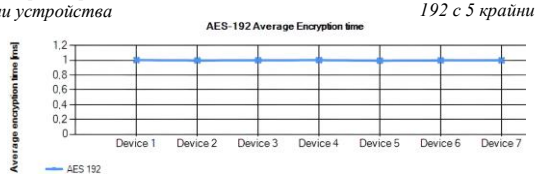
- Използване на AES 192 – средното време за криптиране с 3, 5 и 7 устройства е 1 ms, като отклонение се наблюдава само при 3 устройства – за устройство 2, което достига близо 6 ms (Фиг. 3.31, Фиг. 3.32, Фиг. 3.33).



Фиг. 3.31 Средно време за криптиране при използване на AES 192 с 3 крайни устройства

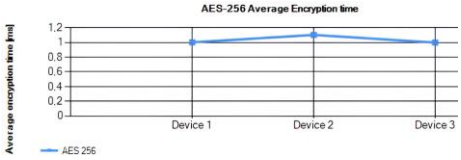


Фиг. 3.32 Средно време за криптиране при използване на AES 192 с 5 крайни устройства

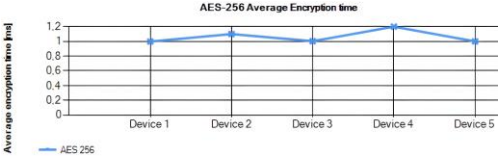


Фиг. 3.33 Средно време за криптиране при използване на AES 192 със 7 крайни устройства

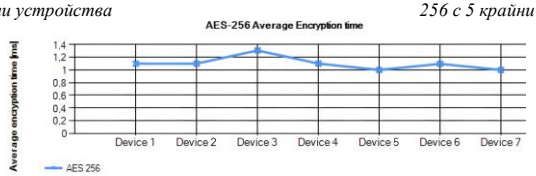
- Използване на AES 256 – с 3 устройства средното време за криптиране е 1 ms за 1 и 3 устройство, като отклонение се наблюдава за 2 с 1,1 ms. С 5 устройства средното време за криптиране е 1 ms за устройства 1, 3 и 5, като отклонения се наблюдават за 2 устройство, което е с 1,1 ms. Най-голямото отклонение е 1,2 ms за 4 устройство. Със 7 устройства средното време за криптиране е 1 ms за 5 и 7 устройство като отклонение се наблюдава за 1, 2, 3, 4 и 6 устройство с 1,1 ms. Най-голямо отклонение се наблюдава за 3 устройство, което е 1,3 ms (Фиг. 3.37, Фиг. 3.38, Фиг. 3.39).



Фиг. 3.37 Средно време за криптиране при използване на AES 256 с 3 крайни устройства

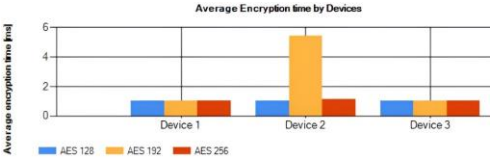


Фиг. 3.38 Средно време за криптиране при използване на AES 256 с 5 крайни устройства

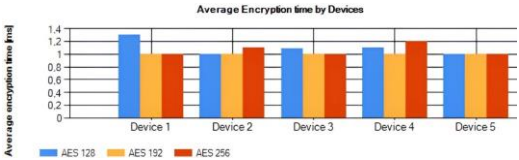


Фиг. 3.39 Средно време за криптиране при използване на AES 256 със 7 крайни устройства

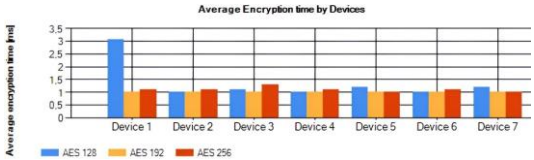
Времето за криптиране при увеличаване на размера на AES ключа от 128 към 192 и 256 бита остава приблизително 1 ms за различен брой устройства. Редките отклонения в отделни измервания не влияят значително на средното време, което потвърждава, че размерът на ключа няма влияние върху производителността на криптиране. Това е важен показател за ефективността на използваните криптографски алгоритми при различни настройки на мрежата (Фиг. 3.40, Фиг. 3.41, Фиг. 3.42).



Фиг. 3.40 Резултат от изчислено средно аритметично време за криптиране при използване на трите размера на AES с 3 крайни устройства



Фиг. 3.41 Резултат от изчислено средно аритметично време за криптиране при използване на трите размера на AES с 5 крайни устройства



Фиг. 3.42 Резултат от изчислено средно аритметично време за криптиране при използване на трите размера на AES със 7 крайни устройства

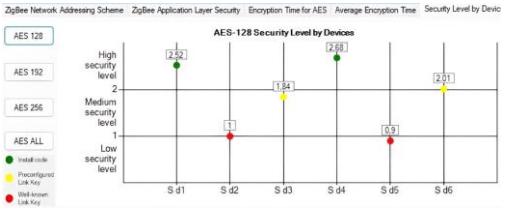
3.3 Изчисляване на ниво на сигурност с предложения аналитичен израз в т. 2.7. и скала

Целта на този експеримент е да се валидира предложеният аналитичен израз в Глава 2 т.2.7 и предложената скала в Глава 2 т.2.7 за определяне на ниско, средно и високо ниво на сигурност чрез изчисляване на сигурността на крайните устройства в ZigBee мрежа, свързващи се с различни PLK – IC, PLK и WK. За тази цел се използва предложеният симулатор ZBeeSiM.

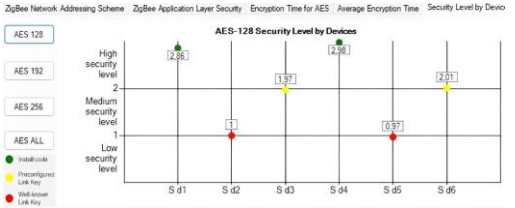
Изследванията са направени в ZigBee мрежа, състояща се от един координатор и шест крайни устройства, свързани в топология „звезда“. Координаторът е конфигуриран да приема устройства, присъединяващи се чрез IC, PLK и WK. Използваната дължина на ключа е 128-bit. Трите двойки крайни устройства са конфигурирани съответно с IC, PLK и WK. Направени са три групи експерименти:

- Първа група – всички крайни устройства са свързани към мрежата с IC, като резултатите са визуализирани чрез предложения симулатор ZBeeSiM (Фиг. 3.43, Фиг. 3.44, Фиг. 3.45).
- Втора група – всички крайни устройства са свързани към мрежата с PLK, като резултатите са визуализирани чрез предложения симулатор ZBeeSiM (Фиг. 3.46, Фиг. 3.47, Фиг. 3.48).
- Трета група – всички крайни устройства са свързани към мрежата с WK, като резултатите са визуализирани чрез предложения симулатор ZBeeSiM (Фиг. 3.49, Фиг. 3.50, Фиг. 3.51).

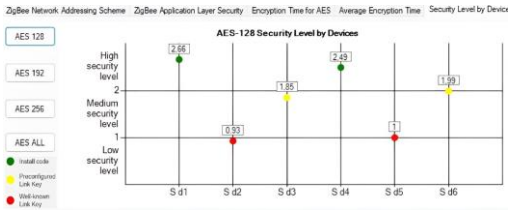
Резултатите от изчисленията с предложения аналитичен израз показват, че при използване устройства с IC, нивото на сигурност е най-високо, след това са тези, които използват PLK и с най-ниско ниво на сигурност са устройствата, които използват WK (Фиг. 3.52, Фиг. 3.53, Фиг. 3.54).



Фиг. 3.52 Ниво на сигурност на устройствата, конфигурирани с различен PLK – експеримент 1



Фиг. 3.53 Ниво на сигурност на устройствата, конфигурирани с различен PLK – експеримент 2

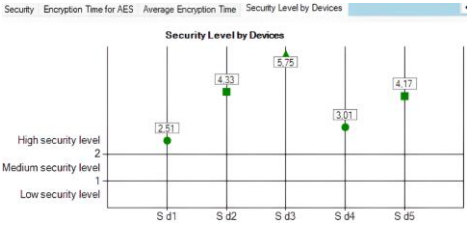


Фиг. 3.54 Ниво на сигурност на устройствата, конфигурирани с различен PLK – експеримент 3

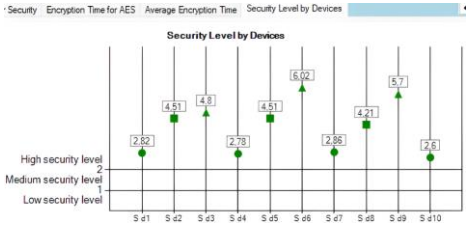
3.4 Изследване на ниво на сигурност при използване на предложения в т.2.8 адаптивен подход за подобряване на нивото на сигурност в ZigBee мрежи

Целта на този експеримент е да се изследва нивото на сигурност на устройства в ZigBee мрежа при използване на адаптивен подход за избор на размера на AES wrap ключа за криптиране на NWK, като се вземат предвид криптографските възможности на всяко устройство. Например, при ZigBee устройствата на TI максималния брой директно свързани устройства към координатора е 20, докато при ZigBee устройствата на Sonoff са максимум 24. Професионалния форум на ZigBee препоръчва за оптимална работа на мрежата да се свързват до 20 устройства директно към координатора. Предложеният симулатор позволява и по-големи стойности, но проведените експерименти са направени в ZigBee мрежа, свързваща в топология „звезда“ един координатор и съответно 5, 10, 15 и 20 крайни устройства. За провеждането на експериментите за този подход, координаторът е конфигуриран да разпознава използваният размер на AES от крайното устройство по последния символ на IC (0 – за тези които използват 128-битов ключ; 1 – за тези, които използват 192-битов ключ и 2 – за тези с 256-битов ключ).

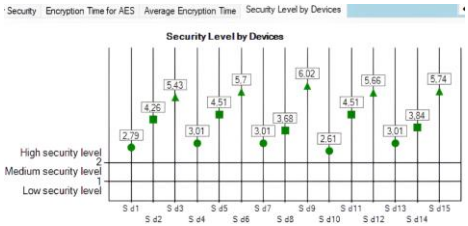
За валидиране на предложения адаптивен подход са реализирани три серии експерименти, при които при които устройствата са конфигурирани с различен размер на AES wrap ключа. Във всяка серия устройствата са разпределени в три групи, всяка използваща различен размер AES wrap ключ – 128, 192 и 256 бита.



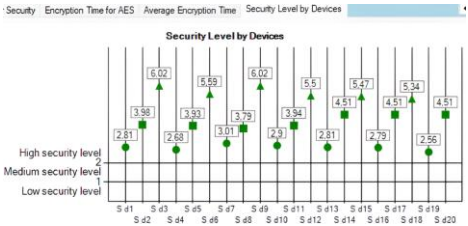
Фиг. 3.63 Ниво на сигурност при различни размери на AES wrap ключове в мрежа с 5 крайни устройства – експеримент 3



Фиг. 3.64 Ниво на сигурност при различни размери на AES wrap ключове в мрежа с 10 крайни устройства – експеримент 3



Фиг. 3.65 Ниво на сигурност при различни размери на AES wrap ключове в мрежа с 15крайни устройства – експеримент 3



Фиг. 3.66 Ниво на сигурност при различни размери на AES wrap ключове в мрежа с 20 крайни устройства – експеримент 3

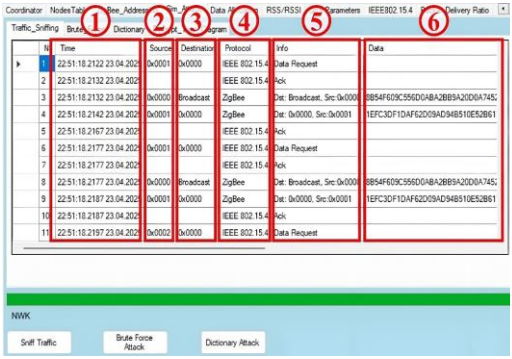
И трите серии експерименти показват последователна и устойчива зависимост между размера на AES ключа и нивото на сигурност на устройствата в ZigBee мрежа. Адаптивният подход успешно осигурява разпределение на ключовете според криптографските възможности на устройствата, като 256-битовите ключове винаги гарантират най-висока защита, 192-битовите осигуряват средно ниво, а 128-битовите остават с най-ниска степен на сигурност. Тази зависимост се запазва независимо от броя на устройствата и топологията на мрежата, което потвърждава ефективността и надеждността на предложения метод.

3.5 Изследване на времето за декриптиране на NWK при изпълнение на Sniffing, Brute Force и Dictionary атаки в ZigBee мрежа

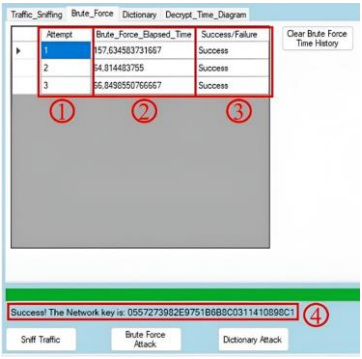
Целта на този експеримент е да се анализира поведението на ZigBee мрежите при симулиране на Sniffing, Brute Force и Dictionary атаки, както и да се изследва времето за декриптиране на NWK при тяхното изпълнение. За тази цел е използван предложеният в дисертационния труд симулатор ZBeeSiM. Експериментът е направен в ZigBee мрежа, съставена от един координатор и осем крайни устройства, свързани в топология „звезда“(Фиг.3.67). След конфигуриране на устройствата, мрежата е инициирана, като координаторът генерира и разпределя NWK към всяко устройство.

Изследването включва изпълнението на три вида атаки, при които се наблюдава времето за декриптиране на NWK:

- Sniffing – симулира се прехващане на трафика между координатора и крайните устройства. Наблюдават се времето на прехващане (Фиг.3.68-1), източникът (Фиг.3.68-2), дестинацията (Фиг.3.68-3), използваният протокол (Фиг.3.68-4) и криптираните данни (Фиг.3.68-5). Резултатът от тази атака е успешното прехващане на трафика, който обаче остава криптиран поради липсата на NWK (Фиг.3.68-6).
- Brute Force – проследяват се броят на опитите, времето за декриптиране и успешността на атаката. Средното време за откриване на NWK е 96,43 минути. Резултатът от тази атака е успешно намиране на NWK (Фиг.3.69-3), но времето за декриптиране е значително продължително (Фиг.3.69-2). След намирането на NWK се декриптира прехванатият трафик (Фиг. 3.70).



Фиг. 3.68 Резултат при изпълнение на Sniffing атака

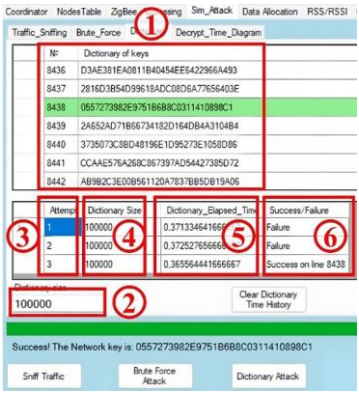


Фиг. 3.69 Резултат при изпълнение на Brute Force атака

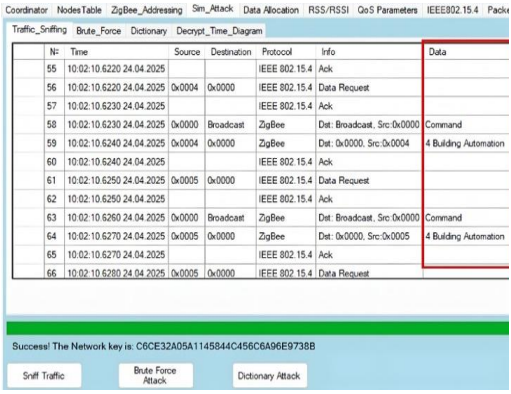
- Dictionary – симулира се използването на речник с обем от 10 000 ключа, който съдържа потенциални NWK (Фиг.3.71-1). Проследяват се размерът на речника (Фиг.3.71-2, Фиг.3.71-4), броят на опитите (Фиг.3.71-3), времето за декриптиране (Фиг.3.71-5) и успешността на атаката (Фиг.3.71-6). Средното време за откриване на NWK е 1,78 минути. Резултатът от тази атака показва, че NWK може да бъде открит при определени условия, но успехът не е гарантиран поради ограниченото множество ключове. След намирането на NWK се декриптира прехванатият трафик (Фиг. 3.72).

Експериментът потвърждава, че различните видове кибератаки имат различно въздействие върху сигурността на ZigBee мрежите, като времето за откриване на NWK силно варира според метода на атаката. Sniffing атаката позволява прехващане на трафика, но без наличието на NWK данните остават криптирани и неразчетени. Brute Force атаката гарантира откриване на NWK, но

с висока времева цена, докато Dictionary атаката може да бъде значително по-бърза, но успехът ѝ зависи от размера и съдържанието на речника, като не гарантира откриване на ключа.



Фиг. 3.71 Резултат при изпълнение на Dictionary атака



Фиг. 3.72 Декриптиран трафик в резултат на Dictionary атака

3.6 Изследване на процесите, реализиращи сигурност в мрежовия слой от ZigBee стека в реална мрежа и в предложения симулатор ZBeeSiM

Целта на този експеримент е да се изследват процесите на присъединяване на крайните устройства към ZigBee мрежа и установяване на двата основни ключа за сигурност NWK и TCLK в реална и симулационна среда, като по този начин се оценява коректността на предложения в дисертационния труд симулатор ZBeeSiM и надеждността му при изследване на мрежовата сигурност в ZigBee мрежите.

За изследванията в реална среда са използвани устройства на Texas Instruments (TI), като изграждането на прототипната мрежа е представено в Приложение 3. В реална среда ZigBee мрежата се състои от един координатор (Launchpad-CC1352R1) и едно крайно устройство (LP STK-CC1352R), които са част от мрежа с топология „звезда“ (Фиг. П3.2). Координаторът е конфигуриран като TC, който позволява на устройствата да се присъединяват към мрежата както с WK, така и с IC (Фиг. П3.5, Фиг. П3.7), а крайното устройство е конфигурирано да се присъединява с WK.

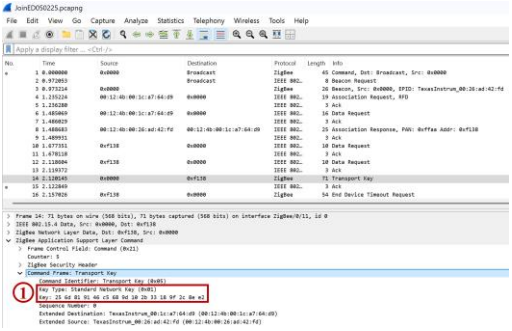
В симулационната среда на предложения в дисертационния труд симулатор ZBeeSiM, ZigBee мрежата също се състои от един координатор, който е конфигуриран като TC и позволява присъединяване на устройства с WK и IC, а крайното устройство е конфигурирано да се присъединява с WK. Устройствата в симулатора са свързани в топология „звезда“. За проследяване на трафика се използва опцията „Traffic_Sniffing“ на симулатора.

При реализиране на мрежата се наблюдават съобщенията, които се обменят между устройствата (Фиг. 3.73). Съобщението „IEEE 802.15.4: Association Request, RFD“ съответства на съобщението „Association Request“ в симулационната среда (Фиг. 3.74). Това е заявка от крайното устройство към TC за присъединяване към мрежата. В отговор координаторът изпраща WPAN адрес, генериран за крайното устройство, чрез съобщението „MAC Association Response“(„WPAN: 0xfffa, Addr: 0xf138“) в реалната среда, което съответства на „Association Response, PAN:0x0001, Addr: 0003“ в симулационната среда (Фиг. 3.73, Фиг. 3.74).

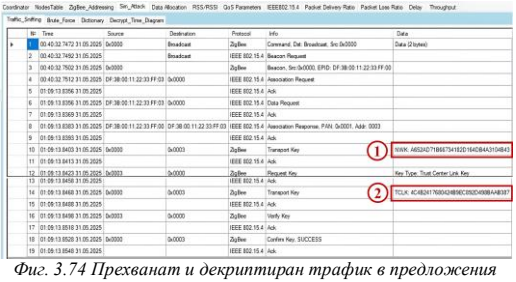
След като крайното устройство се присъедини към мрежата с този WPAN адрес, то изпраща заявка за NWK към TC за криптирана комуникация на мрежовия слой. TC генерира уникален NWK за крайното устройство (Фиг. 3.73-1, Фиг. 3.74-1) и го изпраща криптиран с WK

посредством съобщението „Transport Key“ в реалната среда (Фиг. 3.73), което съответства на „Transport Key“ в симулационната среда (Фиг. 3.74).

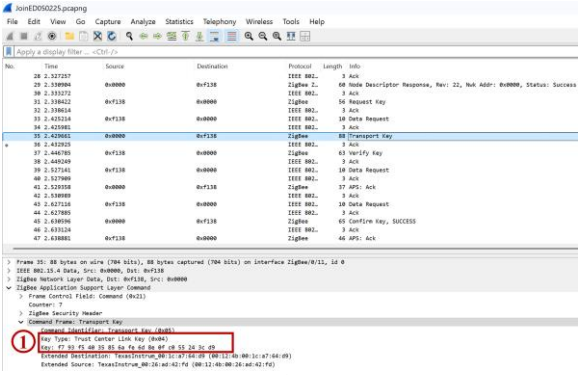
След получаване на NWK крайното устройство изпраща заявка за TCLK, като използва съобщението „Data Request“ в реалната среда (Фиг. 3.75), съответстващо на „Request Key“ в симулационната среда (Фиг. 3.74). ТС генерира уникален TCLK за крайното устройство (Фиг. 3.74-2, Фиг. 3.75-1) и го изпраща криптиран с NWK чрез съобщението „Transport Key“, което е идентично и в двете среди. След това крайното устройство изпраща TCLK обратно към ТС за проверка чрез съобщението „Verify Key“ (Фиг. 3.74, Фиг. 3.75). След успешната проверка координаторът потвърждава полученият ключ с „Confirm Key, SUCCESS“ в реалната среда, което съответства на „Confirm Key, SUCCESS“ в симулационната среда. (Фиг. 3.74, Фиг. 3.75).



Фиг. 3.73 Прехванат и декриптиран трафик в реална среда и установяване на NWK



Фиг. 3.74 Прехванат и декриптиран трафик в предложения симулатор ZBeeSiM и установяване на NWK и TCLK



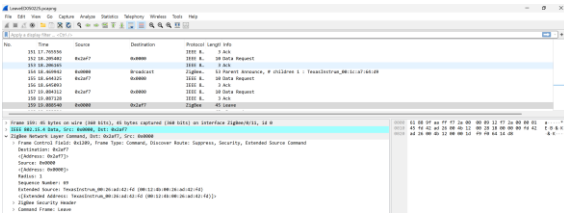
Фиг. 3.75 Прехванат и декриптиран трафик в реална среда и установяване на TCLK

При сравнение на обменените съобщения се установява, че в реалната среда са повече, заради допълнителните съобщения за потвърждение и поддържане на връзката, които не са реализирани в симулационната среда. Въпреки това структурата и последователността на съобщенията съответстват на стандартите и основните съобщения са еднакви в двете среди.

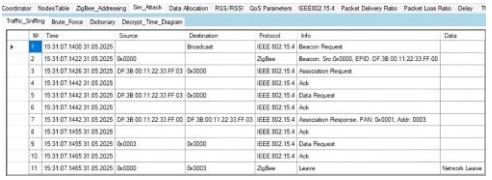
За да бъде изследван сценарий, при който крайното устройство не може да се присъедини към мрежата, координаторът в реална и симулационна среда е конфигуриран да приема само устройства с IC, а крайното устройство остава с конфигурация с WK.

В реалната среда това е реализирано чрез добавяне на допълнителен код към файла zcl_samplelight.c, който задава IC като статичен масив от тип uint8_t с дължина INSTALL_CODE_LEN + INSTALL_CODE_CRC_LEN и примерна стойност 83FED3407A939723A5C639B26916D505C3B5. В същия файл, в рамките на функцията zclSampleSw_Init, е добавен код, който задава TCLK на локалното устройство, генериран чрез преминаване на IC и CRC през MMO хеш функция. Освен това функцията BDB_DEFAULT_JOIN_USES_INSTALL_CODE_KEY във файла bdb_interface.h е настроена на TRUE, за да позволи на устройствата с IC да се присъединяват към мрежата. В симулационната среда координаторът също е конфигуриран да приема в мрежата само устройства, които са конфигурирани с IC, а крайното устройство остава с конфигурация с WK.

При опит за присъединяване крайното устройство изпраща заявка „Beacon Request“, на която координаторът отговаря с генерирания WPAN адрес в съобщението „Association Response“. След получаване на WPAN адрес крайното устройство изпраща NWK заявка към TC. В този експеримент, тъй като устройството не притежава IC, координаторът му отказва достъп и го премахва от мрежата чрез команда „leave“. Този процес е проследен и в двете среди и е показан в съответните графики за трафик (Фиг. 3.76, Фиг. 3.77).



Фиг. 3.76 Прехванат и декриптиран трафик в реална среда с командата „Leave“



Фиг. 3.77 Прехванат и декриптиран трафик в симулационна среда с командата „Leave“

Резултатите от експеримента показват, че симулационният продукт коректно възпроизвежда процесите по присъединяване, обмен и проверка на ключове, както и отхвърлянето на устройства без необходимите идентификатори. Това потвърждава, че предложеният в дисертационния труд симулатор ZBeeSiM е надежден инструмент за изследване на сигурността на ZigBee мрежи и може да се използва за провеждане на допълнителни експерименти и анализи в контролирана среда.

3.7 Изводи:

- Изчислените комплексни оценки на разгледаните симулатори, заедно с предложения в дисертационния труд симулатор ZBeeSiM е на база на предложените в дисертационния труд разнородни критерии, което намалява субективизма при оценяване на симулационните продукти и повишава обективността на получените резултати.
- Комплексните оценки на съществуващите симулатори и ZBeeSiM показват, че предложеният симулатор е най-подходящ за изследване на сигурността на ZigBee устройства.
- Предложеният симулатор ZBeeSiM позволява наблюдение на процесите на присъединяване на устройства към мрежата, установяване на NWK и TCLK, както и генериране и обмен на APLK.
- Изследванията на времето за криптиране при различни размери на AES ключове показват, че средното време остава приблизително 1 ms, независимо от броя на устройствата в мрежата, което доказва мащабируемостта и устойчивостта на ZigBee мрежата, моделирана с предложения симулатор ZBeeSiM.
- Предложеният в дисертационния труд аналитичен израз за изчисляване на нивото на

сигурност и предложената скала с три нива (ниско, средно, високо) позволяват количествено оценяване на сигурността на крайните устройства и валидират различните методи за присъединяването им (IC, PLK, WK).

- Експериментите с помощта на ZBeeSiM показват, че устройствата с IC имат най-високо ниво на сигурност, следвани от тези с PLK и WK, като това съотношение остава стабилно при увеличение на броя на устройствата.
- Предложеният адаптивен подход за повишаване на сигурността на ZigBee устройства е валидиран чрез изчисляване на нивото на сигурност в реална и симулационна среда, което потвърждава неговата ефективност и надеждност.
- Изследванията на времето за декриптиране на NWK при Sniffing, Brute Force и Dictionary атаки показват, че криптираният трафик остава защитен, като Brute Force и Dictionary методите имат ограничена приложимост поради ограничения, свързани с ограничен брой ключове и високо време за успешно декриптиране.
- Сравнението на процесите по присъединяване и установяване на NWK и TCLK в реална и симулационна среда показва пълно съответствие със стандарта на основните съобщения и последователността им, което доказва коректността на предложения симулатор ZBeeSiM.

Заключение

В съответствие с основната цел, в дисертационния труд е направен анализ на съществуващи решения за подходи за повишаване на сигурността в IoT мрежи. Представени са техните предимства и недостатъци при тяхната реализация, като особен акцент е поставен върху криптографските методи и системи за управление на ключове, които осигуряват поверителност, цялост и автентичност на данните.

В дисертационния труд е обоснована необходимостта от дефиниране на критерии за оценка на симулатори, които позволяват изследване на сигурността в ZigBee мрежи. След установяване, че няма налични симулатори, които да покриват напълно критериите за подробно изследване на процесите за сигурност в дисертационният труд е предложен симулатор ZBeeSiM. На база на дефинираните критерии е извършен сравнителен анализ на съществуващите симулатори и ZBeeSiM, използвайки комплексни оценки – аритметична и геометрична. Резултатът от този анализ показва, че предложеният симулатор е най-подходящ за изследване на сигурността в ZigBee мрежи.

Със създаване на експериментална ZigBee мрежа е анализирано времето за криптиране при различни размери на AES ключове и различен брой устройства, като е установено, че производителността на мрежата остава стабилна и мрежата е мащабируема.

Предложен и валидиран е аналитичен израз за изчисляване на нивото на сигурност на крайните устройства в IoT мрежа (реализирана с протокола ZigBee) и скала с три нива – ниско, средно и високо. Чрез експерименти със ZBeeSiM е доказано, че устройствата с IC имат най-висока сигурност, следвани от PLK, а най-ниска – WK.

Предложен е адаптивен подход за повишаване на сигурността на ZigBee устройства, валидиран чрез ZBeeSiM. Резултатите потвърждават неговата ефективност и надеждност за защитата на крайните устройства.

За проверка на коректността и надеждността на ZBeeSiM е изградена прототипна ZigBee мрежа. Сравнени са процесите в реалната мрежа и симулирана същата мрежа с ZBeeSiM. Резултатите показват съответствие със стандарта на основните съобщения и процеси за присъединяване на устройствата в мрежата. Това потвърждава, че предложеният симулатор ZBeeSiM е надежден инструмент за изследване на мрежовата сигурност.

Приноси на дисертационния труд

Приноси с научен характер:

- Предложен е аналитичен израз за изчисляване на ниво на сигурност в ZigBee мрежи и скала за определяне на степените за ниво на сигурност.
- Предложен е адаптивен подход за подобряване на нивото на сигурност в ZigBee мрежи.

Приноси с научно-приложен характер:

- Дефинирана е система от показатели за оценяване на симулационни продукти за изследване на сигурност в ZigBee мрежи.

Приноси с приложен характер:

- Разработен е симулатор за изследване на процесите за сигурност в ZigBee мрежи.
- Разработена е прототипна ZigBee мрежа за IoT, в която експериментално е изследвана сигурността и е приложена предложената скала за определяне на степените за ниво на сигурност.

Публикации по темата на дисертационния труд

1. **Yordanova, M.**; Haka, A.; Aleksieva, V.; Valchanov, H. A Simulation Tool for Security in ZigBee–Based IoT Networks. Eng. Proc. 2024, 70, 21. https://doi.org/10.3390/engproc2024070021. **(Индексирана в Scopus)**
2. **M. Haka**, Analysis of modern approaches to security in IoT networks, the Jornal of CIEES, vol.4, No1 (2024), 2024, DOI: 10.48149/jciees.2024.4.1.5
3. **M. Haka**, A. Haka, V. Aleksieva and H. Valchanov, "Analysis the Security Level of End Devices in a ZigBee Network," 2025 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1–4, doi: 10.1109/ELMA65795.2025.11083387. Electronic ISBN:979–8–3315–2636–8. (**Индексирана в Scopus**)
4. **M. Haka**, A. Haka, V. Aleksieva and H. Valchanov, "Examining the Security Processes at the Zigbee Network Level in Real and Simulation Environments," 2025 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1–4, doi: 10.1109/ELMA65795.2025.11083450. Electronic ISBN:979–8–3315–2636–8. (**Индексирана в Scopus**)
5. **M. Haka**, A. Haka, V. Aleksieva and H. Valchanov, "Study of encryption time with the use of AES 128-, 192- and 256-bit keys," 2025 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1–4, doi: 10.1109/ELMA65795.2025.11083503. Electronic ISBN:979–8–3315–2636–8. (**Индексирана в Scopus**)

Научно-изследователска работа по други договорни теми и задачи:

- Научноизследователски проект НП6/2023г: „Изследване на модели, методи и алгоритми от машинно обучение за решаване на задачи в социалнозначими сфери“ с ръководител доц. д-р Жейно Иванов Жейнов
- Национална програма: „Млади учени и постдокторанти“ 2024г. – Етап 1.
- Научноизследователски проект НП3/2025г: „Подходи за обработка, анализ и защита на информация, базирани на Blockchain и машинно обучение“ с ръководител доц. д-р инж. Айдън Мехмед Хъкъ
- Национална програма: „Млади учени и постдокторанти“ 2025г. – Етап 2.

Специални благодарности на:

проф. д-р инж. Венета Алексиева, проф. д-р инж. Христо Вълчанов, доц. д-р инж. Айдън Хъкъ, моето семейство и на всички, които са били съпричастни към моята дисертационна работа.

ABSTRACT

Dissertation Title: Approaches to increasing the security of IoT networks of the Requirement for the Degree Doctor of Philosophy by Marieta Metodieva Haka

In accordance with the main objective, the dissertation analyzes existing solutions for approaches to improving security in IoT networks. Their advantages and disadvantages in implementation are presented, with particular emphasis on cryptographic methods and key management systems that ensure data confidentiality, integrity, and authenticity.

Chapter 1 presents the essence of the security vulnerabilities of IoT networks. Specific approaches are considered for ensuring security in data storage, as well as for achieving integrity and confidentiality in communication between nodes in IoT networks. The collection and analysis of publications offering solutions for improving IoT security were carried out using the PRISMA method.

Based on the existing solutions reviewed, it was found that cryptographic methods are most suitable for devices with limited resources, such as those used in IoT networks, providing a high level of protection with minimal resource consumption.

Chapter 2 justifies the need to enhance security in ZigBee networks through cryptographic algorithms. It analyzed the advantages and disadvantages of existing ZigBee simulators and defined the essential functionalities a simulator must possess to effectively study network security.

After identifying gaps in current tools such as insufficient support for cryptographic protection, key management, and process visualization, the ZBeeSiM simulator is proposed as a solution for analyzing and evaluating security-related processes in ZigBee networks.

A system of indicators and comparative analysis between existing and proposed simulators highlight ZBeeSiM as the most suitable tool for both scientific and applied research in the field of IoT security. An analytical expression and a three-level scale (low, medium, high) are proposed to assess the security level of end devices. The evaluation aligns with ZigBee standards, where Install Code (IC) offers the highest security, Preconfigured Link Key (PLK) medium, and Well-Known Key (WK) the lowest.

To further improve security, an adaptive approach is proposed for configuring AES keys per device, either automatically or manually. The Trust Center (TC) interprets the last character of the IC to determine each device's cryptographic capabilities. In automatic mode, TC selects the highest for the device AES wrap key size; in manual mode, the administrator adjusts it during setup by modifying the IC.

Chapter 3 presents experimental studies of security-related processes in ZigBee networks, conducted both in simulation and in real environments. The proposed approach to increasing security in the dissertation, as well as the analytical expression and the scale for determining the level of security, were validated using the developed ZBeeSiM simulator.

A comparative analysis of existing simulators was performed, based on ten criteria and evaluated using the arithmetic mean and geometric mean values. In parallel, a prototype ZigBee network with TI devices was built, in which experiments on authentication using Well-Known Key and Install Code were conducted. The connection and key exchange processes were analyzed using Wireshark and a sniffer device.