ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - ГАБРОВО”

Факултет “Електротехника и електроника”

Катедра “Комуникационна техника и технологии”

маг. инж. НИКОЛАЙ ПЕТКОВ МАНЧЕВ

РАЗРАБОТКА И ИЗСЛЕДВАНЕ НА ПЛАТФОРМА ЗА НИСКОЕНЕРГИЙНИ БЕЗЖИЧНИ КОМУНИКАЦИИ ЗА ИНТЕРНЕТ НА НЕЩАТА

А В Т О Р Е Ф Е Р А Т

на дисертационен труд за присъждане на
образователна и научна степен “**доктор**”

Област на висше образование: 5. Технически науки
Професионално направление: 5.3. Комуникационна и компютърна техника
по **Докторска програма**: “Комуникационни мрежи и системи”

Научни ръководители:

1. доц. д-р. инж. Боян Димитров Карапенев
2. доц. д-р. инж. Красен Киров Ангелов

Рецензенти:

1. проф. д-р. инж. Емил Иванов Йончев
2. проф. д-р. инж. Станимир Михайлов Садинов

гр. Габрово 2023г.

Дисертационният труд е обсъден и насочен за официална защита на заседание на Разширен катедрен съвет на катедра „Комуникационна техника и технологии” към факултет „Електротехника и електроника” на Технически университет – Габрово, проведен на 07.12.2023г.

Дисертационният труд съдържа 141 страници. Научното съдържание е представено в увод четири глави и заключение, включва 78 фигури и 6 таблици. Цитирани са 88 литературни източника и 42 Интернет адреса. Номерацията на фигурите, таблиците и формулите в автореферата е в съответствие с тази в дисертацията.

Изследванията по дисертационния труд са извършени в катедра „Комуникационна техника и технологии” към факултет „Електротехника и електроника” на Технически университет – Габрово и на територията на гр. Габрово.

Официалната защита на дисертационния труд ще се състои на 07.03.2024 г. От 13ч. в зала 2215, сграда Учебен корпус 2 (Баждар) на Технически университет – Габрово.

Материалите по защитата са на разположение за интересуващите се в кабинет 3209, корпус №3 на Технически университет – Габрово.

Рецензиите и становищата на членовете на научното жури и авторефератът са публикувани на сайта на университета: www.tugab.bg.

Заглавие: Разработка и изследване на платформа за нискоенергийни безжични комуникации за интернет на нещата
Тираж: 5 бр. (Бълг. език)
Място на отпечатване: Университетско издателство „Васил Априлов” при ТУ - Габрово

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема:

Широкообхватните мрежи с ниска консумация на енергия LoRa и LoRaWAN наречени още (LPWAN) дават възможност на все по-голям брой решения в контекста на интернет на нещата (IoT), както и приложения с голямо географско покритие, ниска но сигурна скорост на предаване на данни и дълъг живот на батерийните захранващи източници. Тези изброени качества водят до редица предизвикателства, които в текушата разработка са разгледани и разрешени. Основните проблеми са съхранението на данни идващи от различни интернет мрежи, към които са свързани приемо предавателните радиочестотни шлюзове, както и визуализацията на данните, както в реално време така и определен времеви диапазон. Основно предизвикателство е правилното географско разпроложение на шлюзовете в местността където ще се изгражда мрежата. Във все повече държави започна изграждането на такива мрежи използвайки LoRaWAN протокола и стандарта. Като за да могат те да са максмално ефективни потоците от данни от различни мрежи трябва да се обединяват в обща платформа както за визуализация на тези данни така и за използването им в последвие с цел анализи и оптимизация на процеси и услуги както в концепцията за Умен град (Smart City) така и в контекста на Индустрия 4.0 (Industry 4.0). Радиочестотните LoRaWAN мрежи са доста нови като разработка и все още в България не са намерили масово приложение. Основния полезен ефект от използването на LoRaWAN мрежи е спестяването както на ресурси при изграждане на двупосочна комуникация за мониторинг и управление на процеси.

Методи на изследване:

За постигане на целта и поставените задачи в изследването се прилага са аналитични, симулационни и практически. Като инструмент за симулационните изследвания са ползвани програмните среди Radio Mobile и The Thinks Network Mapper. Избраната методика за изследване е адекватна.

Новости:

Създадени са симулационни модели за нискоенергийни безжични комуникации, проведени са изследвания и са дефинирани приноси свързани с ефективно използване на честотен спектър, вид модулация и кодиране на канала с цел получаване на по-енергийно ефективни и постоянно качество на услугите при нискоенергийните мрежи. Реализирани са опитни постановки и са направени експериментални оценка на радио покритието в различни зони и точки, представени са графични и таблични зависимости даващи информация за възможностите на аналитичния модел сравнени с реалните изследвания.

Цел и задачи на изследването:

Целта на дисертационния труд е да се разработи и изследва платформа за нискоенергийни безжични комуникации в контекста на Интернет на нещата, като се използват нискоенергийни хардуерни компоненти с достатъчно голям изчислителен капацитет, които използват софтуерни инструменти с отворен код или с крайно завършен софтуерен продукт с невъзможност за промяна.

За реализирането на формулираната цел е необходимо решаването на следните *обобщени задачи*:

1. Да се идентифицират рисковете за нискоенергийните комуникации, посредством теоретично изследване и анализ на съществуващите заплахи за информационните ресурси при тези комуникации и платформи.

2. Аналитично да се моделират трафици от данни при различни условия на преносната среда (градска и извънградска) на база на съществуващата теория и практика в областта на нискоенергийните безжични мрежи.

3. Да се създаде симулационен модел на безжичен пренос на ~~много~~ данни, за да се предскаже капацитета на мрежата и да се оцени работоспособността на платформата за нискоенергийни комуникации.

4. Да се синтезира и практически да се реализира примерна нискоенергийна платформа, на която да се направят експериментални тестове и изследвания и да се създадат препоръки за нейното приложение и изграждане в контекста на дисертационния труд.

Предмет и обект на изследване на дисертационния труд:

Предмет на изследване са процесите, свързани с обработката, предаването и приемането на данни през изграден комуникационен канал базиращ се на LoRaWAN технологията нейните приемници и предаватели – модулация, кодирането на канала, мултиплексирането, характеристиките на приемо/предавателния комплекс, синхронизация и конфигурация на софтуерни и хардуерни модули изграждащи платформата. Като критерии за определяне на качеството на обслужване са използвани различни оценъчни параметри и качествени показатели като еквивалента изотропна излъчвана мощност (EIRP), напрегнатостта на полето, спектралните и векторни характеристики на сигнала и съотношението сигнал/шум при заложени критерии за максимално допустими стойности на параметрите широчина на честотната лента, индикатор за силата на получения сигнал (RSSI) и др.

Апробация на дисертационния труд:

Основните етапи от разработване на дисертационния труд са представени в шест публикации на международни конференции и научни издания, напълно покриващи минималните изисквания относно разглеждания критерий. Три от трудовете са изнесени на Международна научна конференция „Унитех“ два в национална конференция „TechCo“ и един в рецензирано международно списание „JESTR”, като един от тях е самостоятелен, а останалите пет са изготвени в съавторство с научния ръководител и авторски колектив. Публикациите са издадени в сборници с научно рецензиране от международна научна конференция „Унитех“, национална конференция „TechCo“ и рецензирано международно списание „JESTR” в периода на обучение 2019-2022 г.

II. КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА I. ТЕОРЕТИЧЕН ОБЗОР НА НИСКОЕНЕРГИЙНИТЕ БЕЗЖИЧНИ КОМУНИКАЦИИ И ПРОБЛЕМИТЕ В ТЯХ

В първа глава е направен теоретичен обзор на методите, средствата и комуникационните протоколи подходящи за създаване на нискоенергийни платформи при прилагане в IoT или IIoT. Разгледани са механизмите за осигуряване на информационна сигурност, както и проблеми обхващащи нискоенергийният протокол LoRaWAN.

1.7 Изводи към глава първа

1. При разгледаните нискоенергийни протоколи при LoRaWAN протоколът се използват доказали се алгоритми за криптиране на съобщенията. Методът със скачаща честота също допринася, за защитеността на данните. Също така по този начин се използва по-малка част от честотната лента заделена за работа в стандарта.

2. При този ниско енергиен протокол данните са криптирани от край до край, което е един от факторите за внедряването на този протокол в контекста на Интернет на нещата и Индустрия 4.0.

3. В най-съвременната ревизия на протокола с версия 1.0.4 са направени сериозни подобрения в сигурността, а именно въведени са задължителни 32-битови броячи на кадри и запазването им в постоянна част от паметта. Премахването на брояча на кадри при устройства с активиране чрез персонализиране не може да се нулира по време на работа на устройството.

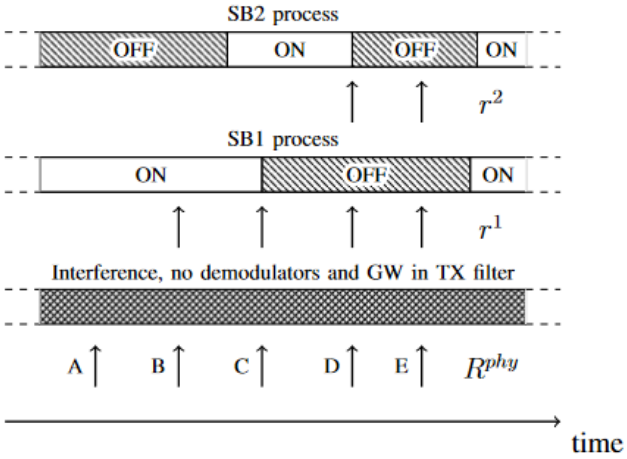
ГЛАВА II. СЪЗДАВАНЕ НА АНАЛИТИЧНО МОДЕЛИРАНЕ НА ТРАФИЦИ ОТ ДАННИ ПРИ НИСКОЕНЕРГИЙНИ БЕЗЖИЧНИ КОМУНИКАЦИИ

2.1 Принципи на аналитичното моделиране

За решаването на проблема с грешното приемане на данни е необходимо обстойно и задълбочено теоретично изследване на проблемната област. Въз основа на теоретичния обзор в Първа глава са направени изводи относно недостатъците на някои от предходните ревизии на нискоенергийния протокол LoRaWAN, като някои от тях са информационната сигурност и получаването на пакет с данни в зависимост от времето на получаване.

2.2 Етапи на аналитичното моделиране

Целта на модела е да характеризира поведението на LoRaWAN мрежа с един GW, който получава пакети с данни от набор от крайни устройства и трябва да отговори в един от двата прозореца за получаване, (като те представляват честотни канали специално отделени за целта, с определена честотна лента). Използват се когато крайното устройство изисква потвърждение. Оценява се производителността на системата по отношение на вероятността за успех на пакета, следвайки подхода, използван в [22] и разширявайки го с по-точно характеризиране на поведението на GW[A1]. Този показател за ефективност е апроксимация на други основни показатели, като пропускателна способност и капацитет на мрежата, които могат да бъдат директно получени от него. При референтният сценарий, предположенията на модела, системните параметри и техните ефекти са описани в т.2.2.1.Случай-А, заедно с кратко представяне на структурата на модела и неговата основна обосновка; В т.2.2.1. Случай-В се описват някои съответни количества и параметри на предложения модел. Аналитична формулировка чрез отделяне на анализа на UL (UpLoad) трафика (т.2.2.1. Случай-С и Случай-D) и DL (DownLoad) трафика.



Фиг. 2.1 Представяне на структурата за филтриране на пакети на модела. Rphy е скоростта на UL трафик, докато r1 и r2 представляват скоростта на ACK, изпратени съответно в SB1 и SB2

съобщения (2.2.1. Случай-E) са изведени формулите за вероятностите за успех на DL в 2.2.1. Случай-F. Накрая 2.2.1. Случай-G, описва различни показатели за ефективност и тяхното изчисляване. Може да се изведе съответното уравнение, като в този случай в текста се предоставят препратки.

2.2.1. Предложения за сценарий при избор на архитектурна свързаност

Разглежда се сценарий, при който крайните устройства са произволен брой и са равномерно разпределени около един GW. Пакетите от приложния слой се генерират съгласно процес на Поасон[93] с агрегатна скорост на генериране на пакети λ [pck/s] , като пакетите могат да бъдат потвърдени или непотвърдени. За максимално използване на аналитичния модел се приема перфектна ортогоналност между различни SF, т.е. само пакети използващи един и същ SF може да се сблъскат. В този случай един от двата пакета може да оцелее, ако неговата получена мощност е достатъчно по-висока от тази на сблъскващия се пакет (сблъсъци с повече от два пакета се случват с незначителна вероятност и не се вземат предвид).

2.2.2. Възможности на модела

Моделът предлага някои регулируеми параметри за увеличаване на неговата гъвкавост, което позволява оценката на производителността на мрежата в различни конфигурации с минимални усилия. Параметри на моделът:

• SF = {7, . . . , 12} показва множеството от всички SF.

• α: част от трафика на приложния слой, изискващ потвърждение;

• p_i^u,p_i^c - част от устройствата, генериращи непотвърден и потвърден трафик с конкретен SF, $i \in SF$, съответно $\sum i \in SF\ p_i^u = \sum i \in SF\ p_i^c$=1;

• h: брой предавания на непотвърден пакет от приложния слой;

• m: максимален брой опити за предаване на потвърдени пакети;

• δSB1 и δSB2: съотношението между времето на мълчание и времето за предаване в SBк, съответстващо на ограничение зададено от брояча на пакети. Например в Европа имаме δSB1 = 99 и δSB2 = 9, съответстващи на

DC от 1% в SB1 и 10% в SB2. Като цяло, когато δSBk > 0 се прилага DC ограничението към всички устройства, предаващи в подканал SBк. Вместо това съответства настройката δSBк

= 0 до DC ограничение от 100%, което означава, че няма ограничение на предаваното време[3] (това важи само за целите на модела);

• τ1 и τ2: са флагове за приоритизиране. Ако τk = 0, GW дава приоритет на операциите по приемане предаване по време на k-тия прозорец за получаване, с k = 1, 2. В този случай GW ще откаже всяко DL съобщение, което трябва да бъде предадено, докато тече UL приемане. Вместо, ако TX е с приоритет (τk = 1), приемането на всеки входящ пакет ще бъде прекъснато защото изпращането на ACK е с приоритет;

2.2.3. Изчисляване на скоростта на трафика при UpLink съобщения

Предположението за перфектна ортогоналност между различните SF фактори прави възможно разделянето на мрежовия трафик в различни логически канали, които не си пречат един на друг. Натоварването на трафика за всеки SFi се разделя равномерно по дадените C честотни канали (тъй като крайните устройства избират случаен UL честотен канал при всеки опит за предаване). По този начин трафикът, генериран на приложния слой от крайните устройства, използващи потвърдени и непотвърдени съобщения, се дава от:

$$R_i^{c,app} = \frac{p_i^c.\lambda}{C}.\alpha, \qquad (2.1)$$

$$R_i^{u,app} = \frac{p_i^u.\lambda}{C}.(1-\alpha), \qquad (2.2)$$

Тъй като ED, използващи непотвърден трафик, ще извършат h предавания на всеки пакет, PHY скоростта на пакетите от тези устройства може да се изчисли като $R_i^{u,phy} = R_i^{u,app}.h$, за предаване на потвърдени съобщения от крайното устройство Вместо това броят на повторно предадените пакети зависи от успеха на както UL предаването, така и съответното ACK. Посочва се като $P_{i,j}^{DL}$ вероятността, че потвърден UL пакет, изпратен с SFi, е успешно получен и потвърден на j-тия опит за предаване, който ще бъде получен в (2.29). Следователно потвърдената скорост на пакети, предадени на SFi, $R_i^{c,phy}$, е дадена от произведението на скоростта на ниво приложение, $R_i^{c,app}$, и средният брой предавания на потвърден пакет на ниво PHY.

$$R_i^{u,phy} = R_i^{u,app}\left[\sum_{j=1}^{m-1} j\,.\,p_{i,j}^{DL} + m\left(1-\sum_{j=1}^{m-1} p_{i,j}^{DL}\right)\right]. \qquad (2.3)$$

Първото сумиране в квадратните скоби на (2.3) взема предвид предаванията, които са успешно получени преди m-тия опит, докато вторият термин разглежда случая, когато пакетът се предава m пъти (независимо дали последното предаване е успешно или не).

Следователно общият трафик за един честотен канал и за SFi се дава от:

$$R_i^{phy} = R_i^{u,phy} + R_I^{C,phy} \qquad (2.4)$$

Като цяло разпределението на факторите на разпространение за предадените пакети на PHY слоя ще се различава от разпределението на SF между устройствата, $\{p_i^u, p_i^c\}$, поради повторни предавания. По този начин се определя:

$$d_i = \frac{R_i^{phy}}{\sum_j R_j^{phy}} \qquad (2.5)$$

като съотношението на пакетите на PHY слоя, които се предават при SF$i \in$ SF.

2.2.4. Възможни вероятности при PHY слоя

UL пакет се получава успешно от GW, ако са изпълнени всички следните условия:
(i) да не се припокрива с други UL предавания, които използват същият SF на същата честота, или се припокрива с друг UL пакет, но получената мощност е достатъчно голяма, за

да позволи правилно декодиране въпреки смущенията;
(ii) да не се припокриват с GW и DL предаване във всеки канал;
(iii) трябва да има наличен свободен демодулатор;

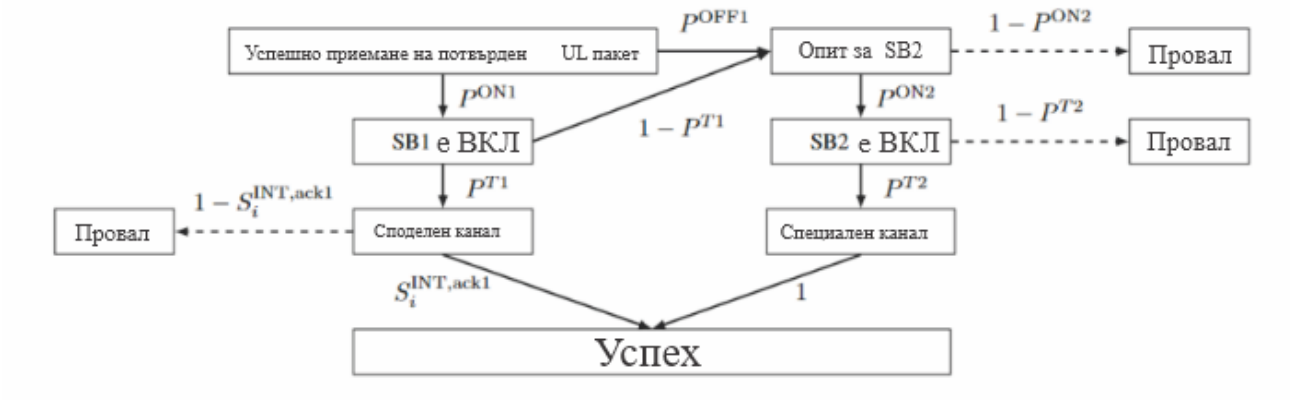
Тези условия са представени от първият филтър на Фиг. 2.1. Тъй като пакетите се генерират след процес на Поасон, е дадена вероятността за събитие (i) от два компонента. Първият е вероятността да няма други пристигания по време на $2T_i^{data}$ период на уязвимост в момента на пристигането на пакета. Вторият, разглежда сблъсък с един пакет и фактът, че приемникът успешно е прихванал кадъра(пакета). За UL се счита вероятност за улавяне W^{GW} както е изчислено в (2.6). Тъй като тези две събития са различни, вероятността на оцелелите смущения (събитие (i)) се дава от сумата на двата компонента, която се получава от:

$$S_i^{INT} = e^{-2T_i^{data}R_i^{phy}} + 2T_i^{data}R_i^{phy}e^{-2T_i^{data}R_i^{phy}}.W^{GW}, \qquad (2.6)$$

2.2.5. Диаграма на предаване на потвърждение при ACK съобщения

След като потвърден пакет бъде правилно получен от GW, трябва да се изпрати обратно ACK към крайното устройство. (2.15) дава вероятността за успешно приемане на пакет в GW. Следователно, скоростта на ACK съобщенията, които GW ще се опита да изпрати в SB1 е:

$$r_i^1 = R_i^{c,phy}.S_i^{UL} \qquad (2.16)$$



Фиг. 2.2. Диаграма показваща успешно приемане на ACK заявка

2.2.6. Пример за потвърдена вероятност при DL съобщение

Като се има предвид, че потвърден UL пакет, изпратен с определен SFi , е успешно получен от GW, може да се изрази вероятността, че съответното ACK съобщение също е успешно върнато към крайното устройство като:

$$S_i^{DL} = S_i^{SB1} + S^{SB2}, \qquad (2.25)$$

където S_i^{SB1} описва вероятността за успешно предаване на ACK съобщение в SB1 с SFi, докато S^{SB2} отчита вероятността SB1 да не е наличен и ACK съобщението да бъде изпратено успешно към SB2. Тези вероятности от своя страна могат да бъдат изразени по следния начин:

$$S_i^{SB1} = P^{ON,1}.P^{T,1}.S_i^{INT,ack1}, \qquad (2.26)$$

$$S^{SB2} = [P^{OFF,1} + P^{ON,1}.(1 - P^{T,1})].P^{ON,2}.P^{T,2}, \qquad (2.27)$$

Фиг. 2.2. може да се използва като справка за изчисляване на това количество. И накрая, може да се изчисли вероятността за успех на m предавания. За опростяване на изразите се пренебрегва времевата корелация на повторното предаване на пакети поради ограниченията наложени от брояча на пакети (въздействието на това приближение ще бъде анализирано чрез

симулация). $P_{i,j}^{UL}$ показва вероятността UL пакет с SFi да бъде успешно получен в GW в точно j-тия опит за предаване, който може да се изчисли като:

$$P_{i,j}^{UL} = S_i^{UL}\left(1 - S_i^{UL}\right)^{j-1} \quad (2.28)$$

След това крайното устройство ((ED)End Device)) успешно получава ACK точно при j-тия опит, ако и UL, и DL предаванията са успешни. Вероятността $P_{i,j}^{UL}$ на това събитие се дава от:

$$P_{i,j}^{UL} = \left[1 - \left(S_i^{UL}S_i^{DL}\right)\right]^{j-1}.\left(S_i^{UL}S_i^{DL}\right) \quad (2.29)$$

След като всички междинни количества са изчислени, моделът може да бъде обобщен от две взаимозависими уравнения:

$$\begin{cases} S^{UL} = f(S^{UL}, S^{DL}), \\ S^{DL} = g(S^{UL}, S^{DL}), \end{cases} \quad (2.30)$$

2.2.7. Показатели за ефективност при приемане и декодиране на данни

За да се оцени производителността на системата, се разглеждат три класа ключови показатели за производителност, а именно: показатели за надеждност, забавяне и справедливост/достоверност, които са разгледани по-подробно в останалата част от тази подточка заедно с методологията за определяне на стойността им с помощта на предложения модел. Веднъж въведени подробен набор от параметри, моделът може да бъде решен и показателите за ефективност могат да бъдат оценени започвайки от S^{UL} и S^{DL}. Обратно, възможно е моделът да се използва за оптимизиране на дадена метрика на производителността, намиране на настройката на параметъра, която го максимизира, както е разгледано в т. 2.3.

1) Показатели за надеждност: Разглеждат се три индекса за скорост на доставка на пакети (Packet Delivery Rate (PDR)), а именно:

   - Непотвърден PDR за връзка нагоре (Unconfirmed Uplink (UU): част от непотвърдени пакети (на ниво приложение), които са успешно получени от GW;
   - Потвърден PDR за връзка нагоре (Confirmed Uplink(CU)): част от потвърдените пакети (на ниво приложение), които са успешно получен от GW, независимо дали е изпратен ACK съобщение към крайното устройство;
   - Потвърден PDR за връзка надолу (Confirmed Downlink(CD)): част от потвърдените пакети (на ниво приложение), които са успешно признати от (Network Server(NS)) Мрежовия сървър.

2.3 Създаване на модел и симулационни резултати

За да се валидира моделът, се сравняват оценките за ефективност, получени от модел с тези, наблюдавани в по-реалистични симулации, в които повечето от опростяващите предположения на модела се премахват. В тази точка се описва как се използва модула LoRaWAN ns-3, описан в [26] и как да се валидира модела. Трябва да се отбележи, че по-точното моделиране на LoRaWAN

SF	T^{data} [s]	T^{ack} [s]	p_{equal}	p_{EXPLoRa}
7	0.051	0.041	0.166	0.487
8	0.102	0.072	0.166	0.243
9	0.185	0.144	0.166	0.135
10	0.329	0.247	0.166	0.076
11	0.659	0.495	0.166	0.038
12	1.318	0.991	0.166	0.019

Табл. 2.1 Стойности на разпределенията T_i^{data}, T^{ack}, p и SF. Полезният товар на пакетите с данни е 10 байта; ACKs нямат полезен товар.

стандартът, разглеждан в симулатора, изисква по-голямо време за изчисление за да се оцени производителността на системата. Всъщност, за същия набор от параметри, оценката на ефективността е мигновен при използване на теоретичния модел, като той се изпълнява при всяка ns-3 симулация и отнема време от порядъка на десетки секунди, като времето за изпълнение бързо нараства с трафика на натоварване, броят на устройствата и броят на необходимите рандомизирани изпълнения на модела. Полезността на симулатора е, че той се стреми да бъде възможно най-реалистичен, като също така взема предвид някои фактори, които са пренебрегнати от модела от съображения за податливост. Например, премахва се предположението за перфектна ортогоналност между предавани пакети, използващи различни SF, симулаторът разчита на модела на ниво връзка, предоставен в [9], за да се определи действителното приемане и вероятност в случай на припокриващи се предавания, което също се отчита от ефекта на улавяне. Параметрите заложени в симулатора са следните:.

- Натоварване на трафика - Броят на ED е фиксиран на 1200 и приложният слой на ED е зададен за периодично генериране на пакети, които да се предават от MAC слоя. Натоварването на трафика в мрежата се модифицира чрез промяна на периода на генериране на пакети. Моделът на генериране на периодичен трафик е по-реалистичен от предполагаемия трафик на Поасон в модела. Независимо от това, доброто съвпадение на резултатите от симулацията и анализа се потвърждава, че предположението на модела е валидно, когато броят на възлите е достатъчно голям.

- Разпределение на канали – Разглежда се типичната последоваателност за разпределение на честотите за Европа, като те са описани в отчетени в табл. 2.2. Следователно броят на различните честотни канали за UL е C=3.

- Работен цикъл - Симулаторът отчита ограниченията поставени от брояча на пакети интегриран в сървъра, като тези ограничения се прилагат във всички страни, в зависимост от честотния им план [12], което съответства на следните стойности: $\delta_{SB1} = 99$ и $\delta_{SB2} = 9$ използвани в този модел

- Модел на канала - За разлика от модела, симулираните LoRaWAN крайни устройства изпитват загуба от разпространението на сигнала на логаритмично разстояние, както при сценарий на открито. По този начин по-далечните устройства имат увеличени загуби и тяхната производителност намалява по отношение на крайните устройства, които са близо до GW. Не се включват бързо затихващи компоненти, които се предполага да бъдат осреднени от модулацията LoRa, нито зависисещите от времето вариации в канала, който

остава постоянен през цялата симулация. Освен това се приема, че каналът е симетричен и DL предаванията ще претърпят същите увреждания, както при UL.

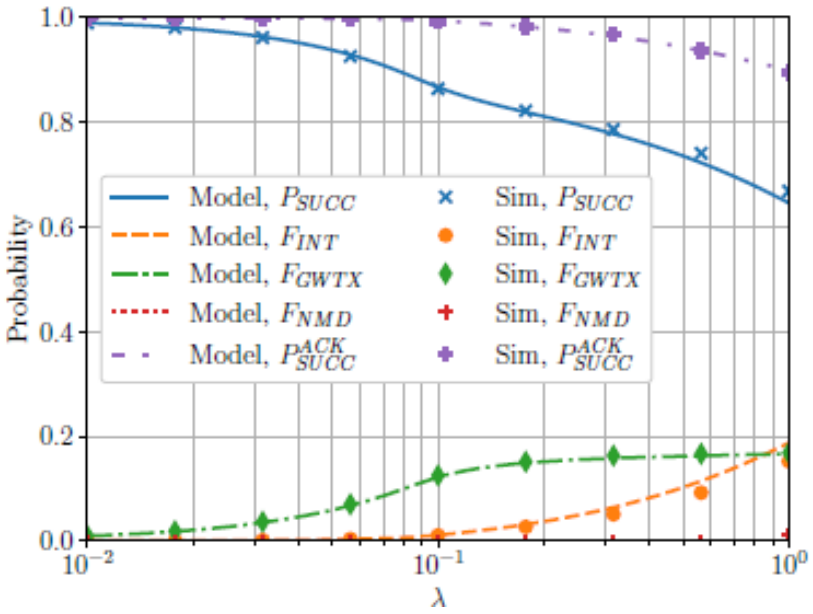
- SF разпределение – крайните устройства обикновено са разположени около GW в кръгова зона с радиус 2500 m, което и да е крайно устройство попадащо в тази зона може да изпраща пакети със всякакви SF с незначителна вероятност за грешка в канала (при липса на смущения). Вместо това, позициите на ED се избират на случаен принцип при всяко изпълнение на симулацията. SF са присвоени равномерно (виж табл.2.1.). В някои сценарии се разглежда различно разпределение на SF (pEXPLoRa), за да се оцени въздействието на този параметър върху различни показатели.

- Интерференция и захващащ ефект - За да се моделира смущение, в симулатора се разглежда матрица на сблъсък, предоставена в [9], и времето на припокриване между пакетите, както е описано в [23][4] Пакетът бива смущаван от сигнал, модулиран със същия SF, ако мощността му е поне $CR_{db} = 6\,dB$ по-висока от на другия постъпващ пакет. За да се осигури сравнение с този сценарий, в аналитичния модел се използва предположението за равномерно разпределени ED около GW, за да се изчислят вероятностите за прихващане на пакета, както е описано в (2.6), което води до $W^{GW} = 0.1796$, и $W^{ED} = 0.5682$. Отбелязва се, че при различни разпределения на ED около GW могат да бъдат моделирани чрез адаптиране на това извеждане. Тъй като реализацията на GW в симулатора се опитва да емулира поведението на реално устройство, UL пакетът се получава успешно, когато са изпълнени следните условия:

  1) Пакетът намира свободен демодулатор;

  2) Приемането на пакета не се прекъсва от DL предавания;

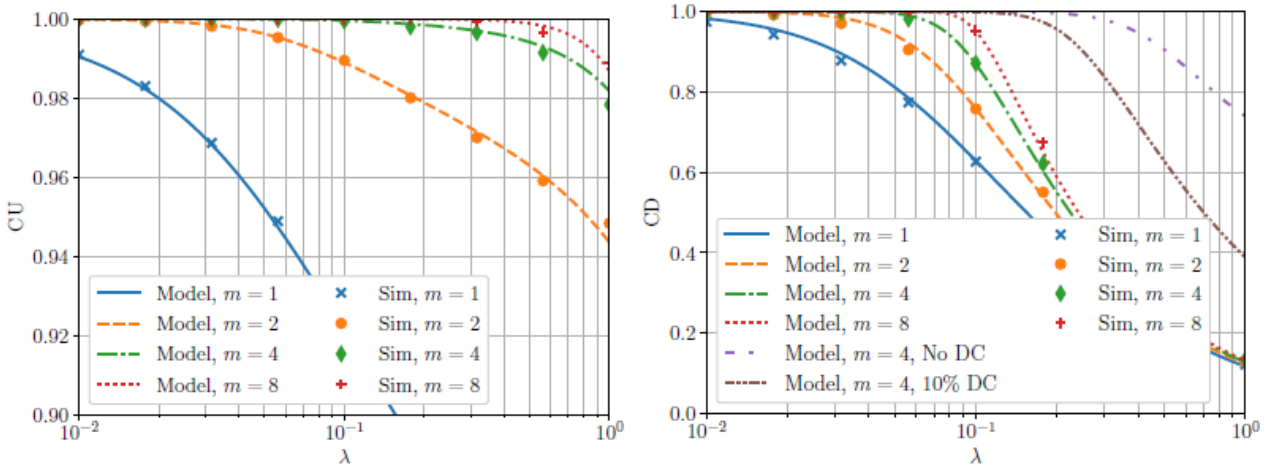
  3) След като приемането приключи, пакетът не е бил повреден от смущения.



Фиг. 2.3 Изпълнение на ниво PHY с $m = 8, \alpha = 1$.

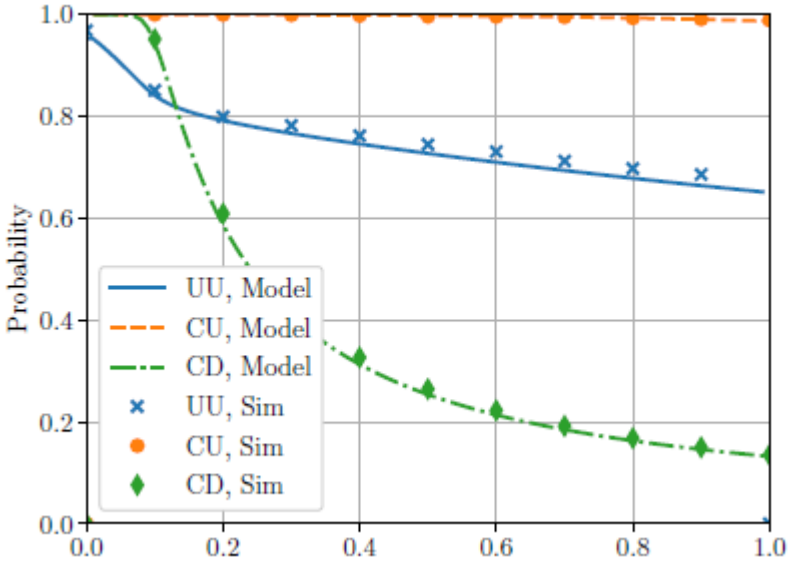
Чрез използване на (2.6), (2.8) и (2.14), където E_i показва очакваното разпределението на SF факторите и S^{demod} вероятността, че в симулациите пакетът може да използва наличен

демодулатор. Реално е описано сравнение между производителността, оценена с предложения модел и от симулатора ns-3. Резултатите са представени както за PHY, така и за MAC слоя и е показано, че предположенията на модела са приемливи. И накрая, някои резултати показват как моделът може да се използва за получаване на представа за поведението на технологията LoRaWAN за по-бърз и лесен начин, като се анализират ефектите на различни параметри върху производителността на мрежата. В графичните зависимости описани в тази точка в научният труд, аналитичните резултати са представени с линии, докато маркерите съответстват на резултатите от симулацията. Фиг. 2.3. показва вероятностите за изходен пакет на ниво PHY в мрежа, използваща потвърден трафик. Фактът, че тази загуба на производителност е причинена от DC на GW, се потвърждава от люляковата пунктирана линия на фиг. 2.4.б: за да се получат тези резултати, ограниченията от DC са премахнати чрез задаване на $\delta_{SB1} = \delta_{SB2} = 0$ в модела, като в резултат на това се получават значително по-добри резултати в сравнение със съответната зелена крива, където DC е активиран.



(а) CU за различни стойности на $m, \alpha = 1$ (б) CD за различни стойности на $m, \alpha = 1$

Фиг. 2.4 (а, б) Сравнение на резултатите от модела и симулацията на CU и CD.

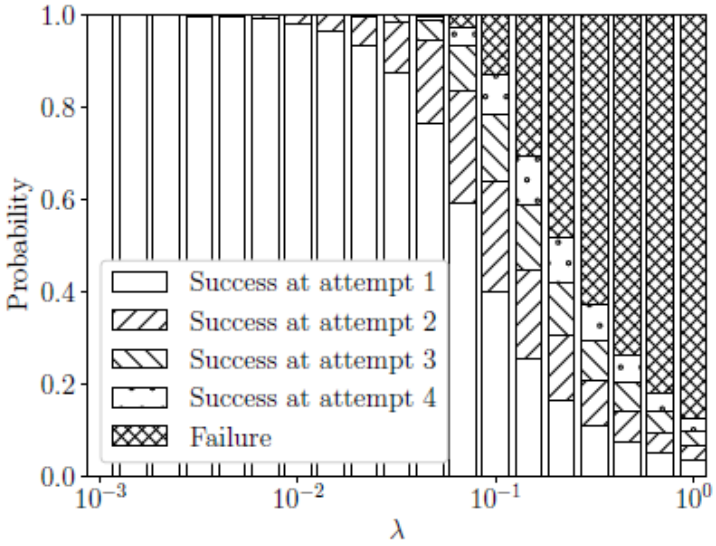


Фиг. 2.5. Ефективност при промяна на част от потвърдения трафик, със стойности $\lambda = 1, m = 8, h = 1$

Друг пример за гъвкавостта на модела, като се имат в предвид и нестандартните настройки, се дава от плътно пунктираната кафява линия, която представлява метриката на CD, когато $\delta_{SB1} = \delta_{SB2} = 9$ т.е., когато предавания в двата поддиапазона подлежат на DC от 10%.

2.4. Възможности на предложения аналитичния модел

Пример: какво аналитичният модел може да предложи, който е представен на Фиг. 2.8, която показва частта от трафика, която постига успех на приемане на пакети след определен брой повторни предавания при опит за различни натоварвания на трафика, получени от $P_{i,j}^{DL}$.

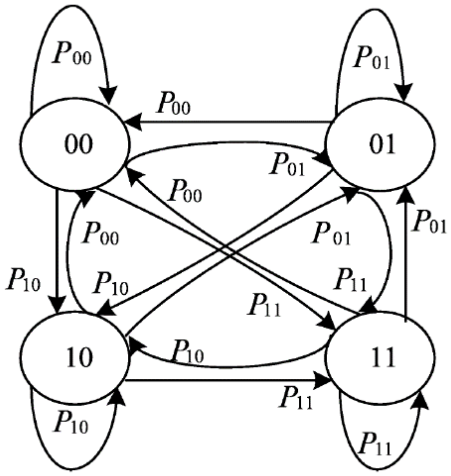


Фиг. 2.8. Разпределение при повторни предавания, $m = 4, \alpha = 1$.

Тези данни се използват за изчисляване консумацията на енергия на крайните устройства: при ниско натоварване на трафика по-голямата част от предаванията на пакети на MAC[91] ниво са успешни само с един опит за предаване на ниво PHY. С нарастването на натоварването на трафика съответно се увеличава частта от устройства, които се нуждаят от множество повторни предавания, за да получат правилно ACK отговори. След определен момент приемането на пакети се проваля с толкова висока честота, че повечето ED трябва да използват максималния брой предавания и въпреки високия разход на енергия, все още не успяват да получат ACK[92] отговор от GW.

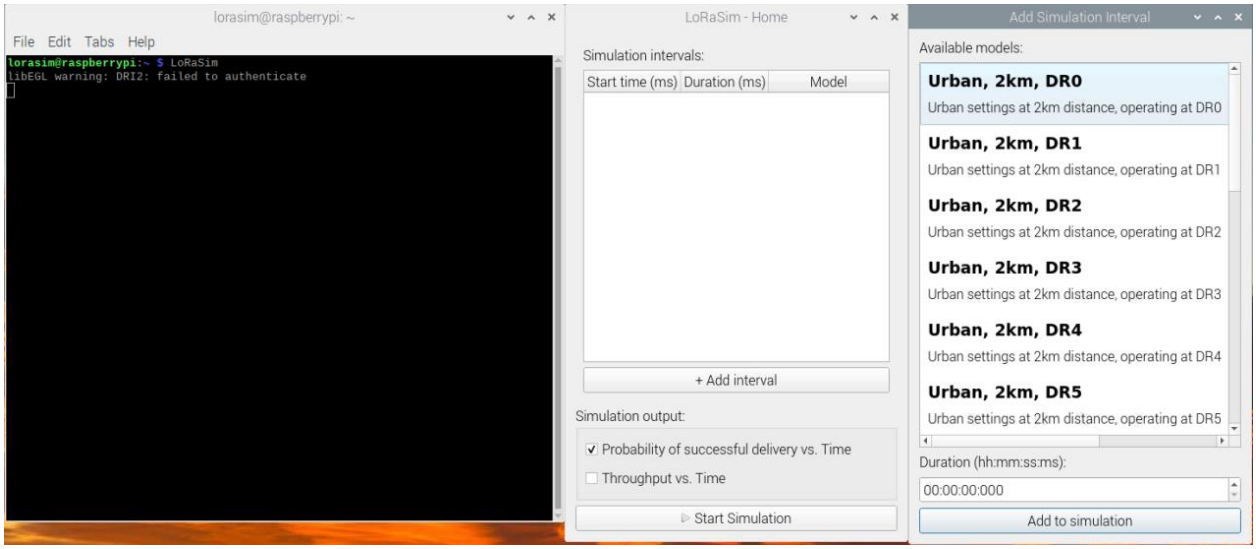
2.5. Софтуерно използване на възможностите на аналитичния модел

За целите на дисертационния труд е създаден софтуерен инструмент базиращ се на аналитичния модел разгледан в глава 2 на дисертационната разработка[96]. Моделът предсказва каква е вероятността за получаване на пакет от информация в зависимост от средата на разпространение(градска или извънградска). Няколко различни модела са заложени в софтуера, като могат да се създават още или да се редактират съществуващите. В зависимост от времето от предаването до приемането на пакет информация в модела са заложени различни времена на предаване имитирайки предаване на повече или по-малко информация. В модела е заложена матрица на Марков с 4 състояния показана на Фиг. 2.11.[46].



Фиг. 2.11. Матрица на Марков с 4 състояния

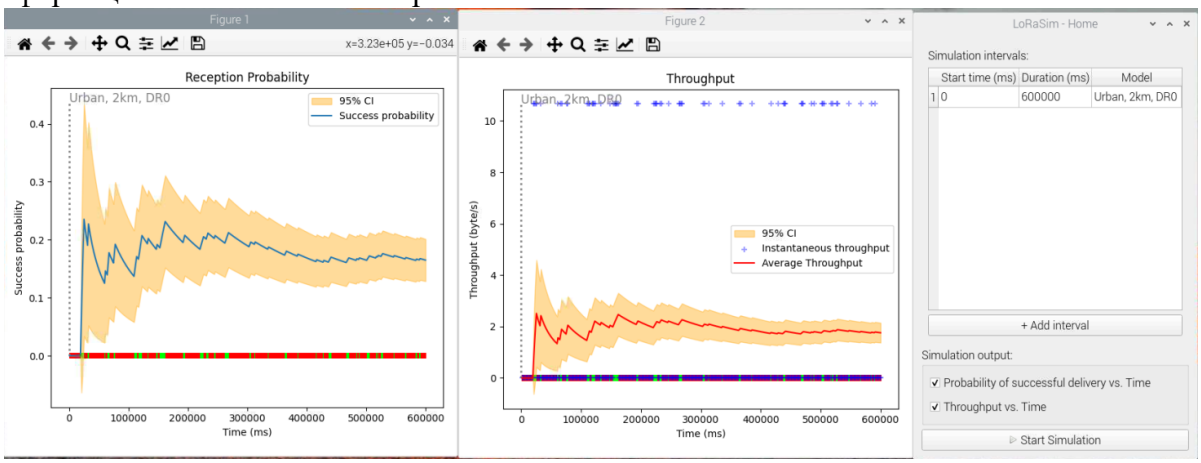
Използваната матрица изчислява вероятността $P(X_i)$, т.е вероятността да се съдържа X_i съединители между линии i и i+1. За всеки съединител където i и i+1 е изпълнено условието i<n-1, може да се изпълни матрицата на Марков с 4 състояния. Състоянията 00, 01, 10 и 11 представляват логически стойности на двете логически шини. Вероятността за преход от едно състояние в друго е: $P_{00} = P_{01} = P_{10} = P_{11} = 0{,}25$. Следователно вероятността за стационарно състояние е 0,25 виж израз (2.39). Софтуерният инструмент е написан с помощта на програмният език Python, повече информация за него може да се види тук: https://github.com/nikolaieniware/LoRaSim . Софтуера разполага с графичен интерфейс за задаване на различни модели за симулация показани на Фиг. 2.12. От нея може да се види и как изглежда графичния интерфейс на софтуера. Реализирания софтуерен инструмент за симулация на трафик използвайки вериги на Марков е инсталиран отново върху едноплатков компютър Raspberry Pi 3 B+. След инсталацията на софтуера следвайки стъпките описани в https://github.com/nikolaieniware/LoRaSim се пристъпва към стартиране на софтуера. За стартиране се изпълнява в команден прозорец командата LoRaSiM виж. Фиг. 2.12.



Фиг. 2.12. Стартиране на софтуера LoRaSiM

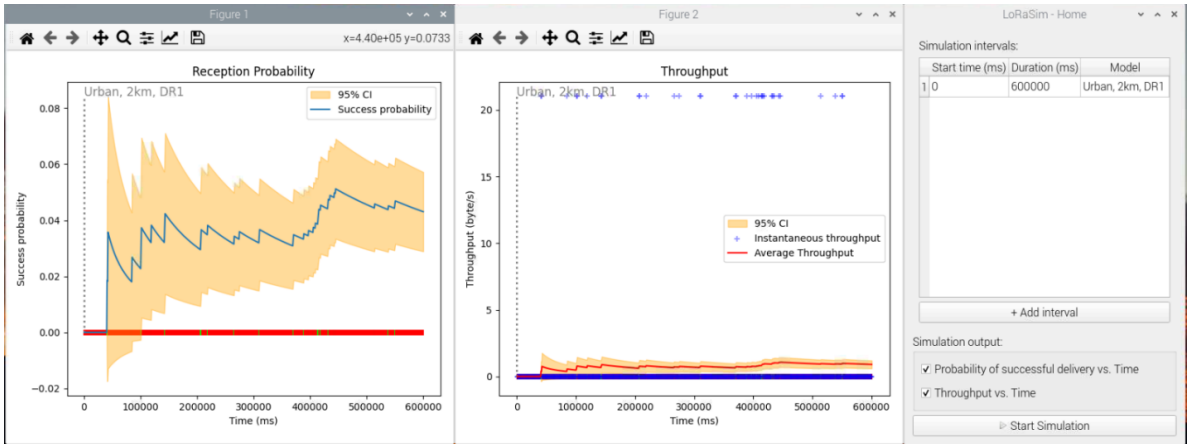
В дясната част на Фиг. 2.12. се вижда терминалния прозорец, в който е изписана командата LoRaSim, с която се стартира софтуера. Отваря се диалогов прозорец LoRaSim Home, от който с бутона +Add interval се добавят т.нар. Simulation interval. Те представляват

фиксирани разстояния от RF Шлюза до предавателя, при различни скорости на предаване на данните от DR0 до DR6, като те отговарят на различни SF фактори. В полето Duration се задава диапазона от време, за който предавателя да излъчи информацията на този SF и симулирана дистанция до приемника. На Фиг. 2.13. се вижда как е зададен един SF фактор, вероятността за приемане на данни от страна на RF Шлюза, а на графиката до нея възможното количество информация в байтове за това време.



Фиг. 2.13. Резултати от проведената симулация на предаване на данни при DR0 (време на предаване на информацията 1500ms.

На Фиг. 2.14. се вижда подобна графична зависимост при същата дистанция от 2км, но при DR1 при време за предаване на информацията 760ms.



Фиг. 2.14. Резултати от проведената симулация на предаване на данни при DR1 (време на предаване на информацията 760ms.

При сравнение между двете фигури се вижда, че при по-краткото време за изпращане вероятността за получаване на пакет от данни е по-малка 0.08, докато при скорост на изпращане от 1500ms вероятността е 0.4, което е доста по-приемлив резултат. При останалите стойности на разстоянието до RF Шлюза и различен DR коефициент не са правени сравнения и не са поместени в дисертационната записка.

2.6.Изводи към глава втора

На базата на разгледаният модел и възможностите за симулация на трафик в LoRaWAN мрежа може да се заключи, че технологията и безжичния стандарт дават възможност за предаване на информация на големи разстояния макар и с ниска скорост, но само ако

конфигурацията и настройката на крайните устройства и мрежовия сървър са конфигурирани правилно.

При симулацията на трафик в т. 2.2.7. са формулирани и определени показателите за ефективност, които са разграничени в три групи - надеждност, забавяне и достоверност.

Моделът е заложен в симулатора ns-3 и дава възможност за изчисляване на вероятността за загуби на пакет при липса на демодулатори използвайки определена математическа зависимост.

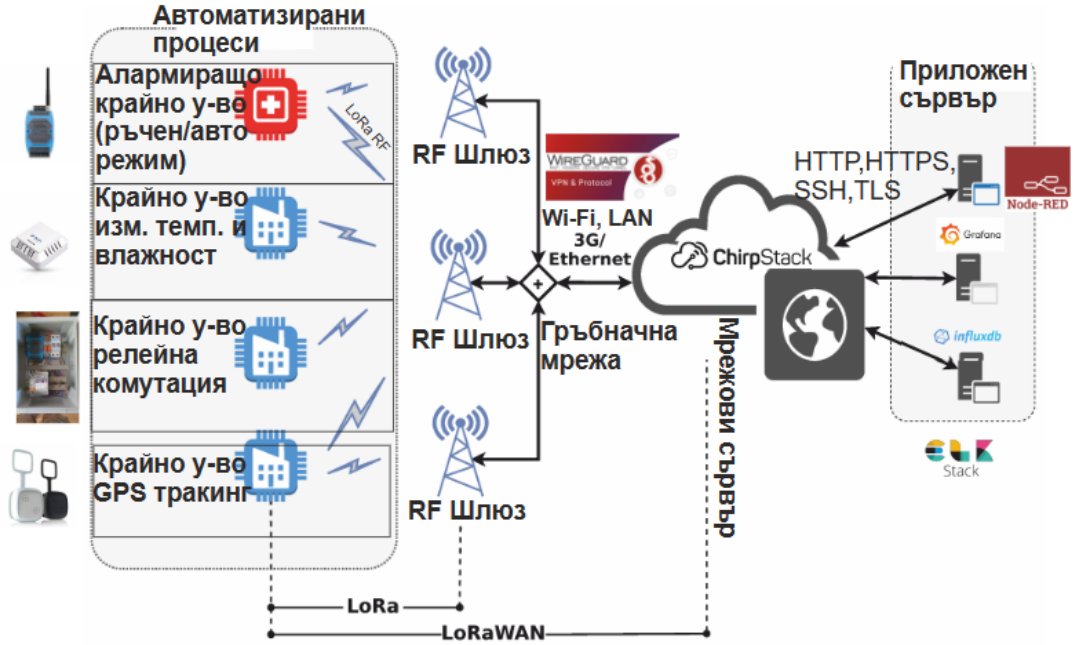
В точка 2.4 са представени възможностите на използвания модел при няколко различни сценария показани в табл. 2.2., а на Фиг. 2.9 са показани графични зависимости на различни производителности при различни мрежови конфигурации.

В точка 2.5 е заложено софтуерното използване на модела за вероятности при приемане и предаване на данни при различни разстояния в градска среда използвайки матрица на Марков с 4 състояния. На базата на този метод е създаден и софтуерен инструмент за симулация на трафик от данни при различни скорости за пренос на данните DR. Инструмента има възможност за наслагване на няколко различни DR фактора за различно време и наблюдаването на количеството предадена информация за това време.

ГЛАВА III. ПЛАНИРАНЕ, ИЗГРАЖДАНЕ И ИЗСЛЕДВАНЕ НА ВЪЗМОЖНОСТИ НА БЕЗЖИЧЕН ПРЕНОС НА ДАННИ ПРИ НИСКОЕНЕРГИЙНАТА ПЛАТФОРМА

3.1. Схема на опитната постановка

За целите на експерименталното изследване и анализ на предаването на данни посредством изградената нискоенергийна LoRaWAN мрежа е представена, опитната постановка с блокова схема на Фиг. 3.1.



Фиг. 3.1. Концептуална блокова схема за провеждане на експерименталните изследвания

3.2. Проектиране и асемблиране на RF Шлюз

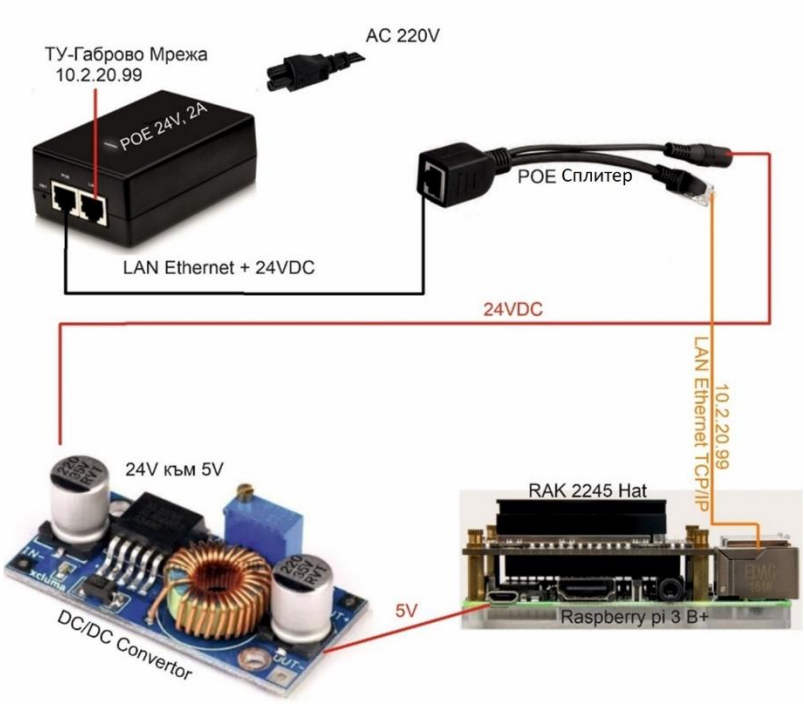
RF Шлюза още наречен LoRaWAN Gateway е съставен от два хардуерни модула:

-Едноплатков компютър Raspberry pi 3B+

-LoRaWAN концентратор RAK2245

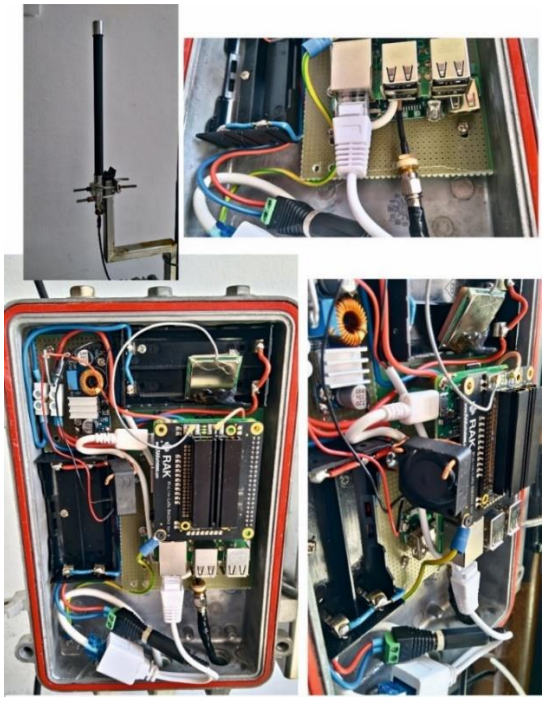
Двата модула са поместени в херметическа алуминиева кутия с подходящи монтажни елементи. Захранването на двата модула по изискване е 5V, 3A (на големи разстояния се

получават големи загуби по проводниците). Това предизвикателство е решено чрез използване на POE (Power Over Ethernet) захранващ блок с 24 волта стойност на захранващото напрежение. В кутията е поместен и преобразувател (DC/DC Convertor), с помощта на който напрежението се регулира до желаните 5V, необходими за захранване на модулите[А4]. Реализацията на захранването е показана на Фиг.3.2.



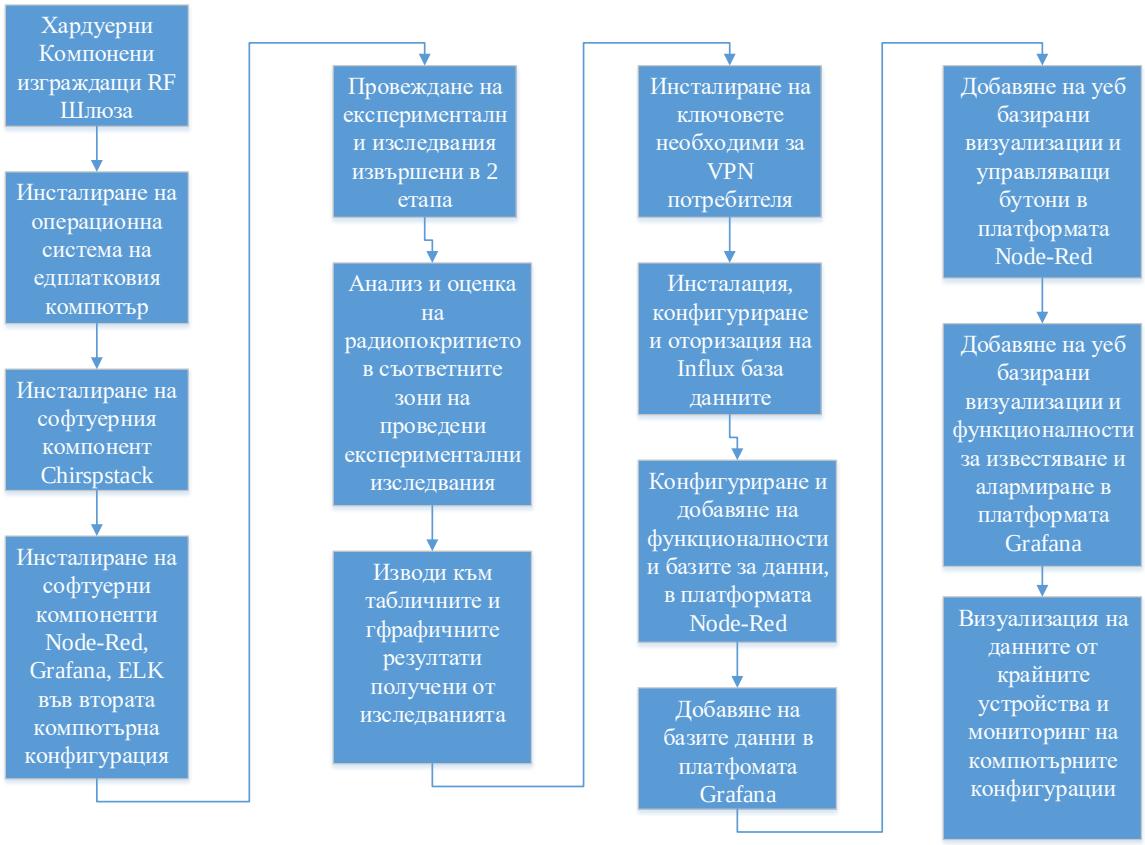
Фиг.3.2. Реализация на захранването на RF Шлюза

На Фиг.3.3. са показани батерийните гнезда, както и контролера за зареждането на батериите.



Фиг.3.3 Съставни модули на RF Шлюз

3.3. Алгоритъм и методология на синтезиране на опитна постановка и провеждане на изследването



Фиг. 3.4. Алгоритъм за методология на проектирането на платформа

3.4. Инсталиране и конфигуриране на Chirpstack LoRaWAN сървър

Цялостната инсталация на сървъра е разделена на няколко етапа или по-точно казано на 3 модула, които се инсталират поотделно върху едноплатковия компютър.

- **Модул 1:** Gateway Bridge. ChirpStack Gateway Bridge е услуга, която преобразува LoRa® Packet Forwarder протоколите в общ формат на данни на ChirpStack Network Server (JSON и Protobuf). Този компонент е част от стека на ChirpStack с отворен код LoRaWAN® Network Server.

За инсталацията му се използват следните команди:

1: `sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 1CE2AFD36DBCCA00`

2: `sudo echo "deb https://artifacts.chirpstack.io/packages/3.x/deb stable main" | sudo tee /etc/apt/sources.list.d/chirpstack.list`

3: `sudo apt update`

4: `sudo apt install chirpstack-gateway-bridge`

5: `sudo systemctl [start|stop|restart|status] chirpstack-gateway-bridge`

- **Модул 2:** Network Server. ChirpStack Network Server е реализация на LoRaWAN ® Network Server с отворен код . Този компонент е част от стека ChirpStack. Отговорността на компонента на мрежовия сървър е дедупликацията на получените LoRaWAN рамки от LoRa ® шлюзовете и за събраните рамки, обработващи:

  - Удостоверяване
  - LoRaWAN mac-слой (и mac-команди)
  - Комуникация със [сървъра за приложения ChirpStack]
  - Планиране на рамки за изпращане на данни

  За инсталацията му се използват следните команди:

  1: `sudo -u postgres psql`

  2: Създаване на база и роля в базата:

```
-- create the chirpstack_ns user with password 'dbpassword'
create role chirpstack_ns with login password 'dbpassword';
-- create the chirpstack_ns database
create database chirpstack_ns with owner chirpstack_ns;
-- exit the prompt
\q
```

  3: Проверка на базата и потребителя за правилна настройка:

```
psql -h localhost -U chirpstack_ns -W chirpstack_ns
```

  4: Изтегляне на инсталационния файл за Chirpstack Network Server:

```
    sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 1CE2AFD36DBCCA00
    sudo echo "deb https://artifacts.chirpstack.io/packages/3.x/deb stable main" | sudo tee /etc/apt/sources.list.d/chirpstack.list
    sudo apt update
```

  5: Инсталация на Chirpstack Network Server

```
sudo apt install chirpstack-network-server
```

  6: За автоматично стартиране на процеса

```
sudo systemctl [start|stop|restart|status] chirpstack-network-server
```

- **Модул 3:** ChirpStack Application Server. Отговаря за частта от „инвентаризация“ на устройствата на LoRaWAN инфраструктурата, обработката на заявки за присъединяване и обработката и криптирането на полезния товар(данните) на приложението. Сървъра притежава и [уеб интерфейс] , където могат да се управляват потребители, организации, приложения и устройства. За интеграция с външни услуги предлага [gRPC и RESTful] API.

Данните за устройството могат да се [изпращат и/или получават] през MQTT, HTTP и да се записват директно в InfluxDB база данни.

За инсталацията му се използват следните команди:

1: Създаване на потребител и база данни с командата: `sudo -u postgres psql`

2: Допълнителни настройки на базата с данни:

```
-- create the chirpstack_as user
create role chirpstack_as with login password 'dbpassword';
-- create the chirpstack_as database
create database chirpstack_as with owner chirpstack_as;
-- enable the trigram and hstore extensions
\c chirpstack_as
create extension pg_trgm;
create extension hstore;
-- exit the prompt
\q
```

3: За проверка на потребителя и базата: `psql -h localhost -U chirpstack_as -W chirpstack_as`

4: Изтегляне на инсталационния файл за Chirpstack Application Server:

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 1CE2AFD36DBCCA00
sudo echo "deb https://artifacts.chirpstack.io/packages/3.x/deb stable main" | sudo tee /etc/apt/sources.list.d/chirpstack.list
sudo apt-get update
```

5: Инсталация на Chirpstack Application Server: `sudo apt-get install chirpstack-application-server`

6: Автоматизирано стартиране на сервиза: `sudo systemctl [start|stop|restart|status] chirpstack-application-server`

7: Достъп до сървъра за приложения: Уеб интерфейс: https://localhost:8080/

С тази стъпка инсталацията на Chirpstack сървъра е завършена и може да се пристъпи към добавяне на устройство и приложение в сървъра.

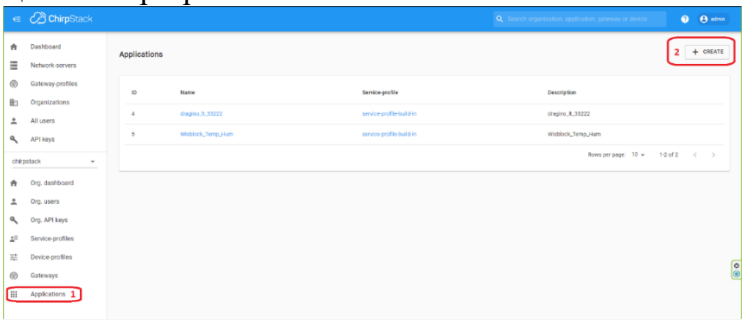
3.5.1. Създаване на приложения в Chirpstack LoRaWAN Сървър

За създаване на приложение в Chirpstack LoRaWAN сървъра се навигира до уеб интерфейса на сървъра, чрез IP адреса и мрежови порт 8080 на инсталацията се въвеждат потребителските данни за вход в системата:

Потребител: admin

Парола: admin

След това се навигира до менюто Applications (1), и след това се клика бутона + CREATE(2), виж. Фиг. 3.8. На Фиг. 3.8. се вижда, че вече има създадени две приложения, които участват в дисертационната разработка.



Фиг. 3.8. Създаване на приложение в Chirpstack LoRaWAN сървъра

3.6.1. Инсталиране и конфигуриране на Node-Red

Node-RED[25] е софтуерен инструмент за програмиране и свързване на хардуерни устройства, API и онлайн услуги по нов и интересен начини. Той предоставя онлайн базиран редактор, който улеснява свързването на потоци, като се използва широката гама от възли в палитрата от възможности, които могат да бъдат разгърнати във времето за изпълнение с едно щракване. За целите на дисертационната разработка Node-Red и Grafana са инсталирани на едноплатков компютър от типа Raspberry Pi 3 B+, както бе споменато по-нагоре в тази глава на втора компютърна конфигурация, като са инсталирани двата софтуерни инструмента Node-Red и Grafana. Преди да се пристъпи към последователността за инсталация трябва да се убедим, че използваме операционна система Raspberry Pi OS[41]. Стъпки при инсталация:

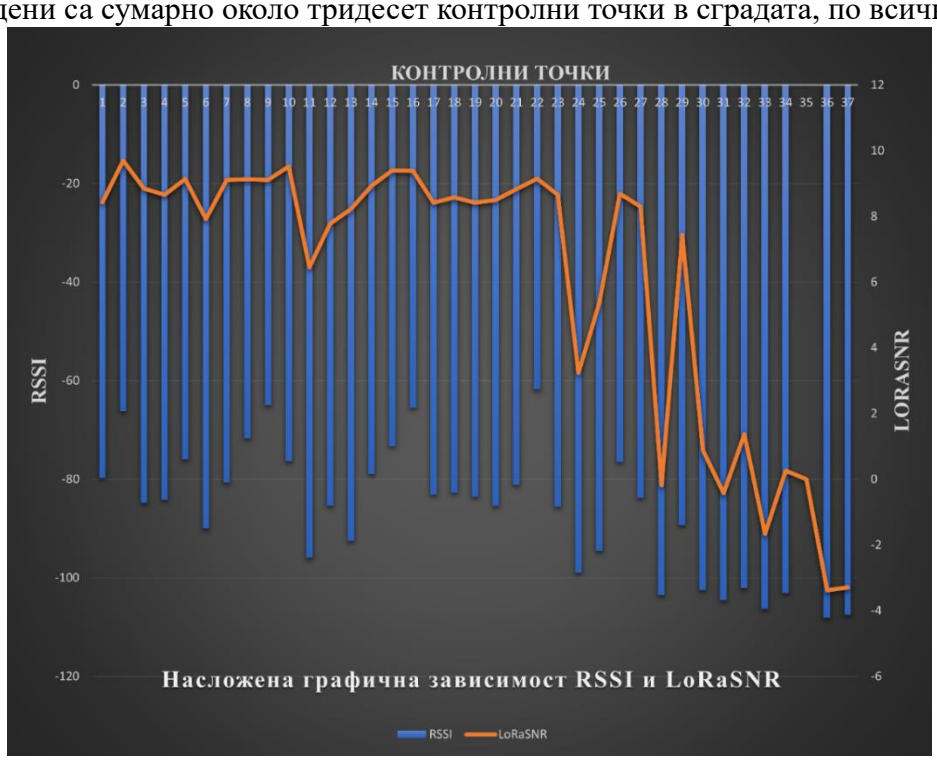
1. В терминален прозорец се изпълнява следната команда: **bash <(curl -sL https://raw.githubusercontent.com/node-red/linux-installers/master/deb/update-nodejs-and-nodered)**
2. За да се осигури автоматично стартиране при зареждане на операционната система се изпълнява командата: **sudo systemctl enable nodered.service**
3. За да се стартира автоматизираното разрешение се изпълнява командата: **sudo systemctl start nodered.service**

3.7.1. Експериментални изследвания в закрито помещение

Експерименталните изследвания в закрито помещение са проведени в сграда корпус 2 „Баждар“ на ТУ-Габрово, като са направени голям брой измервания във всяка една контролна точка с цел постигане на реален средноаритметичен коефициент на параметрите на сигнала. Параметрите, които се изследват в дисертационната разработка са:

- RSSI
- LoRaSNR

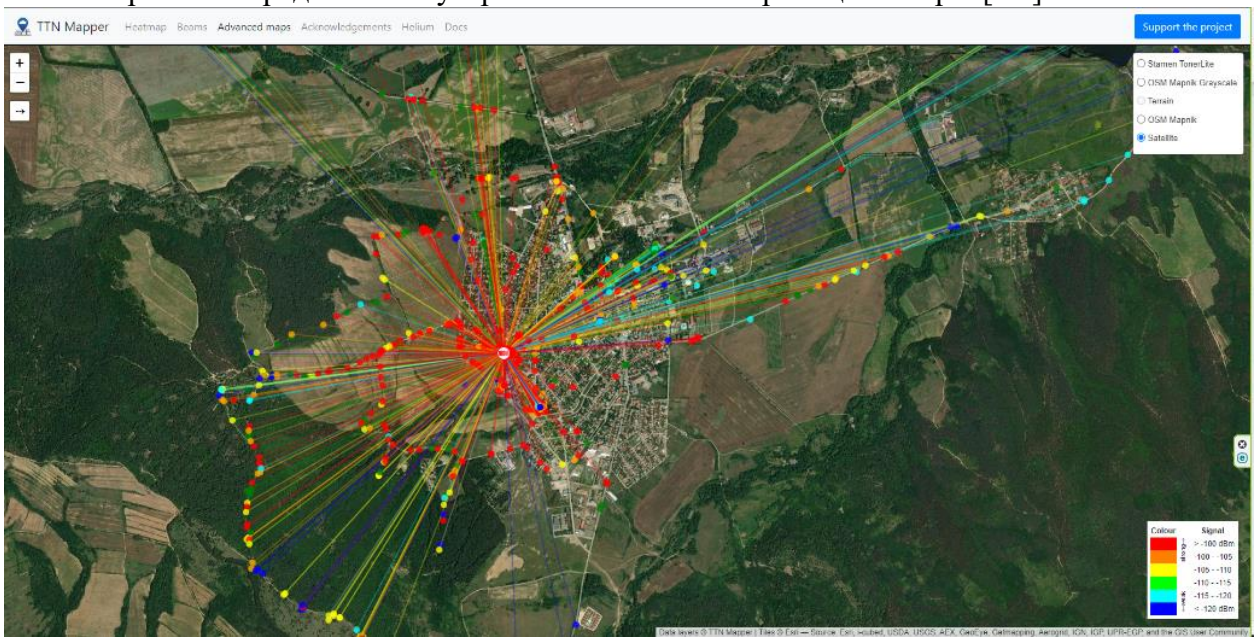
Обходени са сумарно около тридесет контролни точки в сградата, по всички етажи.



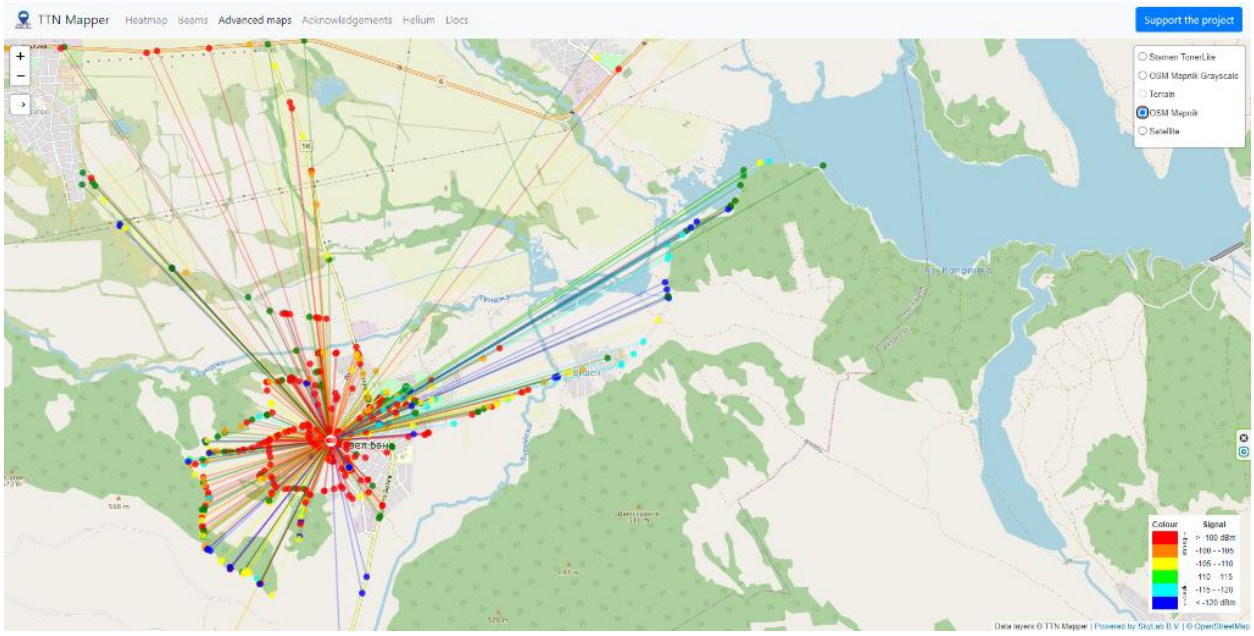
Фиг. 3.30. Графична зивисимост между параметрите RSSI и LoRaSNR спрямо контролните точки на измерването

3.7.2. Експериментални изследвания в открита зона

Изследванията за качеството на радиопокритието в открита зона са проведени на територията на гр. Павел баня, като повечето контролни точки са обходени с велосипед, а крайното предавателно устройство бе носено в раница на гърба[А6].

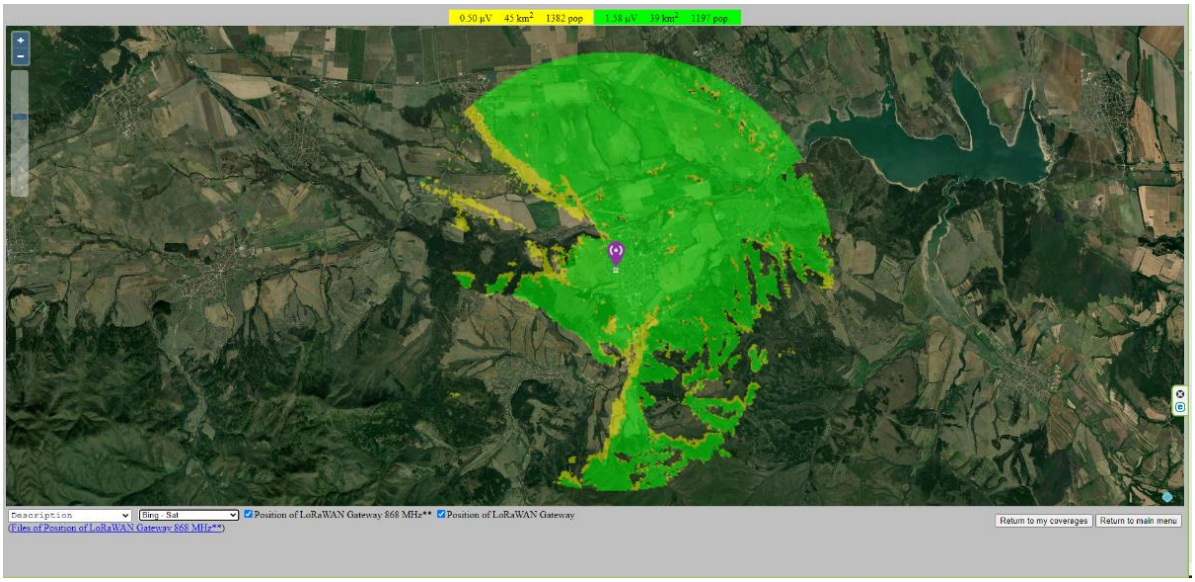


Фиг. 3.37. Сила на сигнала в различни контролни точки

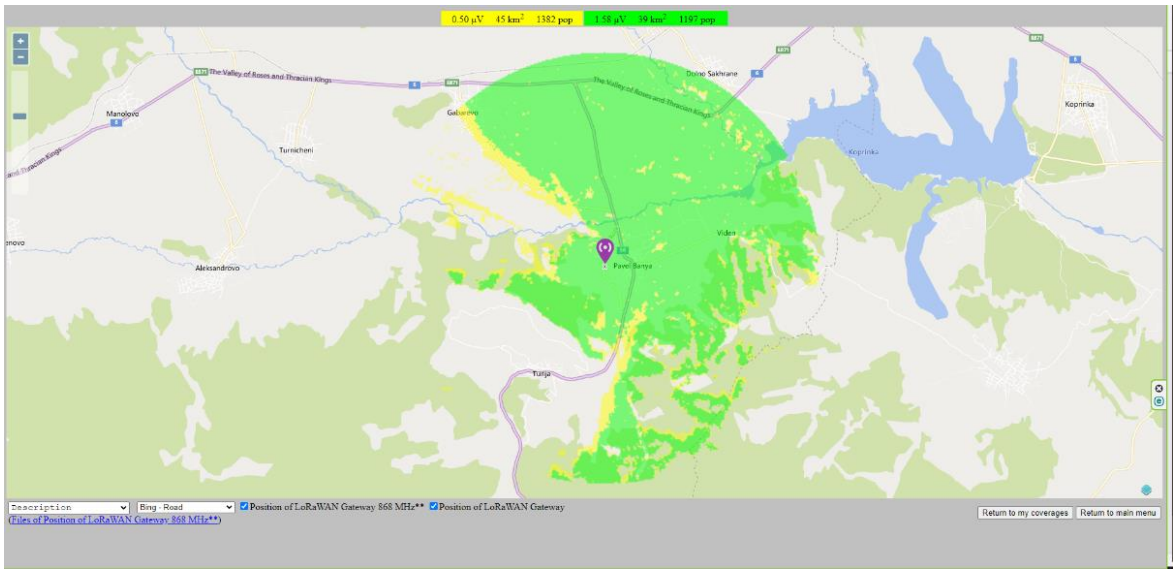


Фиг. 3.38. Контролни точки на брега на яз. Копринка

Резултатите от симулациите на радио покритието са представени на Фиг. 3.39А и Фиг. 3.39Б.



Фиг. 3.39А. Резултати от симулацията на радио покритие (сателитен изглед)



Фиг. 3.39Б. Резултати от симулацията на радио покритие (топографски изглед)

3.8. Изводи към глава трета

От изграденият RF Шлюз и направените с него експериментални изследвания в закрита зона може да се обобщи, че технологията LoRaWAN може да оперира и в закрити пространства, разбира се до определено разстояние, в зависимост от материалите, от които е изградена сградата тяхното затихване (поглъщане и отразяване), което определя и качеството на радио покритието в тази зона. Изследванията проведени в корпус 2 „Баждар“ на ТУ-Габрово доказват, че радио вълните успяват да преодолеят дебелите стени и плочи от бетон на сградата във всички контролни точки от измерванията, като RF Шлюза е разположен при всички сценарии на етаж 2 в средата на коридора.

Изследванията проведени в открита зона около гр. Павел баня също са успешни и доказват работоспособността на технологията в градска и извънградска зона. Резултатите са доказани с практически изследвания сравнени със симулационни изследвания в същата зона на радио покритие със взети в предвид параметри на крайното устройство и на RF Шлюза, затихване в коаксиалната линия и др.

Използваните софтуерни инструменти формират платформа за нискоенергийни безжични комуникации, която е гъвкава и универсална от гледна точка на различни устройства, които могат да се интегрират в нея.

Използването на модулацията LoRa се доказа, с устойчивост и безпогрешно предаване на данни, както в закрити така и в открити пространства, в следващи изследвания могат да се изследват и качествата на модулацията и при мобилни устройства, като това ще разшири спектъра на използване на технологията

ГЛАВА IV. ИЗСЛЕДВАНЕ НА ПРОИЗВОДИТЕЛНОСТТА НА ПЛАТФОРМАТА ЗА ПРЕНОС НА ДАННИ ПРИ НИСКОЕНЕРГИЙНИ БЕЗЖИЧНИ КОМУНИКАЦИИ

4.1 Анализ на производителността на платформата за нискоенергийни комуникации

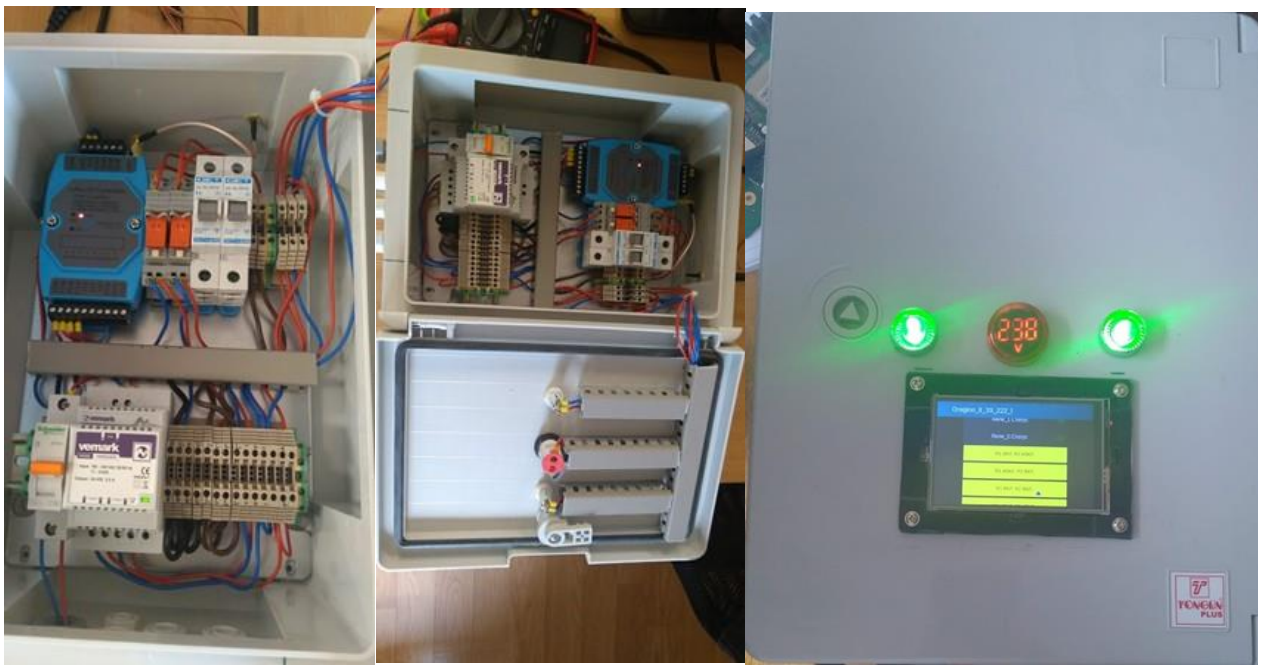
В бъдещите нискоенергийни безжични мрежи непрекъснато ще расте необходимостта да се осигури по-голям капацитет, за да се задоволи нарастващият трафик, изискван от потребителите, индустрията и научните среди. За момента мрежовите оператори в България имат слаб интерес към такъв тип мрежи, но все пак някои от тях пуснаха NB-IoT мрежа с платени мобилни карти в действие през 2020г. Разгледаната във втора и трета глава на дисертационния труд безжична технология дава възможност за изграждане на частна мрежа за пренос на данни, като тя не превишава стандартите за антенна мощност и здравните норми. Технологията е подходяща за StartUp компании с поглед към бъдещето и енергийно ефективни методи за пренос на данни на големи разстояния. Другият сериозен плюс, който притежава технологията LoRaWAN, е възможността да се изгради Mesh преносна мрежа и да се покрие по-голям диапазон от услуги и устройства. Достъпността на технологията, я прави подходяща за изграждане на мрежа от RF Шлюзове използващи тази технология от хора с техническа грамотност, като тя им дава възможност да станат конкурентни на пазара на услуги, както в концепцията „умен град“, така и в индустриалната автоматизация и научните изследвания. Нискоенергийната платформа включва в себе си редица под звена.

4.2.Изследване производителността на нискоенергийни крайни устройства изграждащи нискоенергийната платформа

Първото от няколкото нискоенергийни безжични устройства, които са създадени за целите на дисертационната разработка е Релейно комутационно устройство с обратна връзка за състоянието на контактите в релетата. Крайното устройство е изградено от LoRaWAN модула Dragino LT-33222, и два релейни контакта с максимален ток на комутация 5A при 240V AC захранване. Спецификацията на модула е описана в [48]. Управлението на релейните контакти може да се изпълни по два начина: автоматично или ръчно. Идеята на създаването на крайното устройство е автоматизирано и отдалечено управление на контур от градското улично осветление. Като с помощта на измерването на консумирания ток на контура, може да се предвидят и възможни дефектирали осветители според текущата консумация на ток. Логиката за автоматичното изпълнение за вкл. и изкл. на релейните контакти се управлява от средата Node-Red, където са зададени конфигурации за час на включване и изключване. Системата има опция за добавяне на сензор за осветеност, като чрез него се управлява и времето на включване и изключване на релейните контакти. По този начин се повишава ефективността на платформата, както и оптималното време на светене на осветителя. На Фиг. 4.1. може да се види външния изглед на модула Dragino LT-33222.

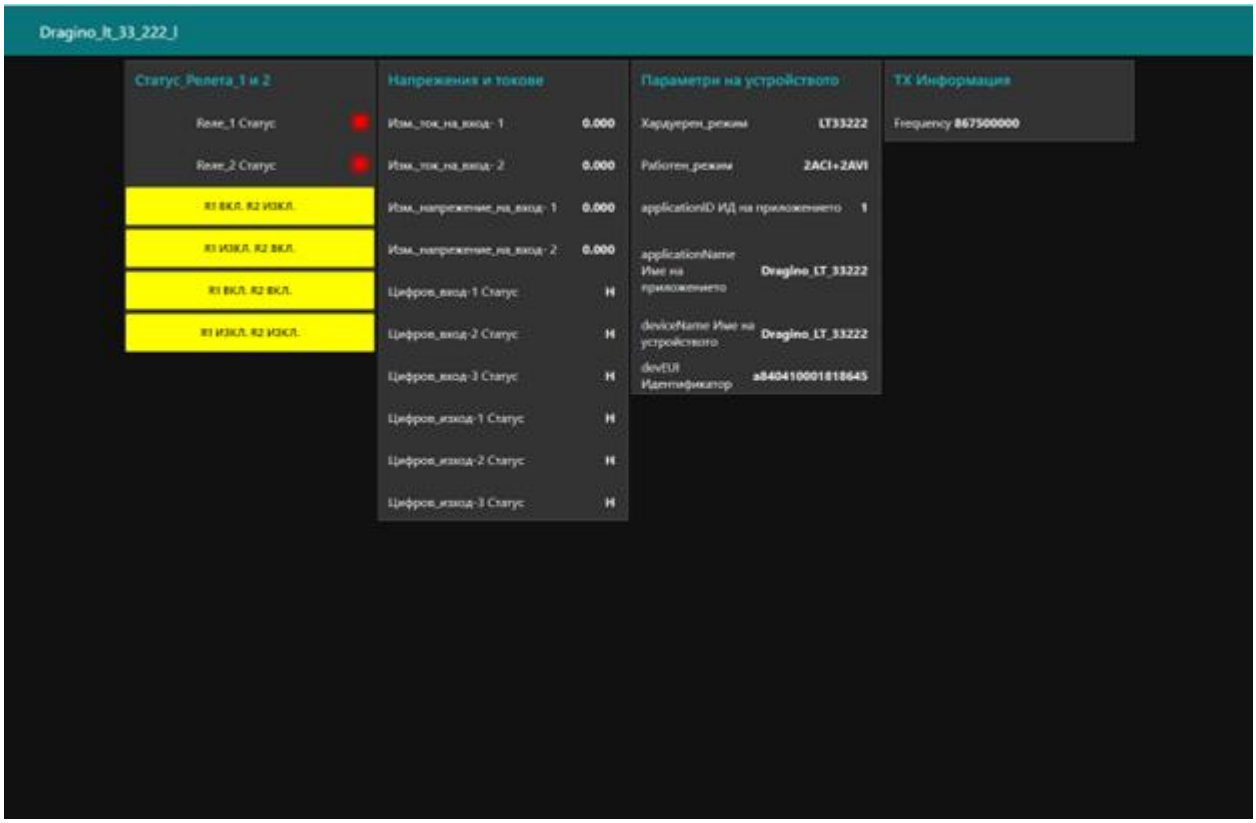
Фиг. 4.1. LoRaWAN базиран модул за управление и мониторинг.

Модула е поместен в електрическо табло заедно с релейните контакти, захранващ блок, и едноплатков компютър с дисплей, който служи за визуализация на web базирания интерфейс, стартиран от Node-Red. Всеки бутон и поле четат данни от устройството в реално време и се визуализират на интерфейса[A5]. Цялостния завършен вид на крайното устройство може да се види на Фиг. 4.2.



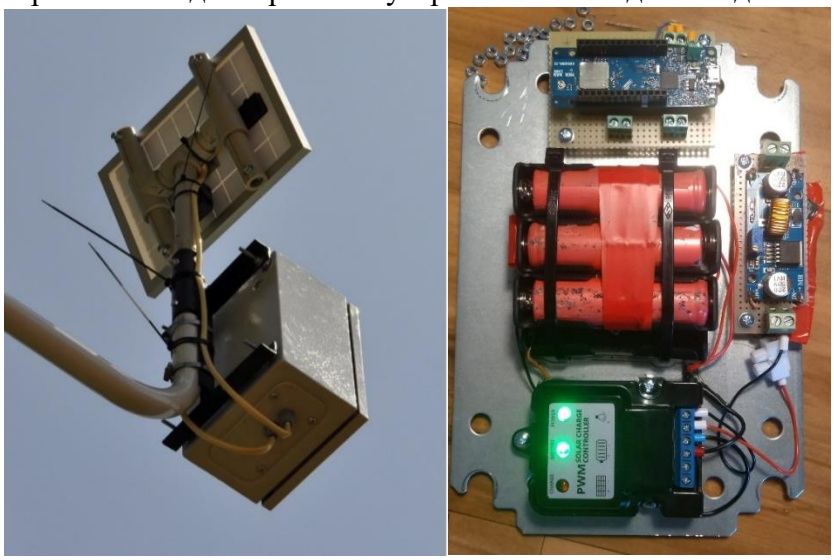
Фиг. 4.2. Крайно устройство 2 броя релейни комутатори

На Фиг. 4.3. може да се види web базирания интерфейс за контрол и мониторинг на данните от устройството.



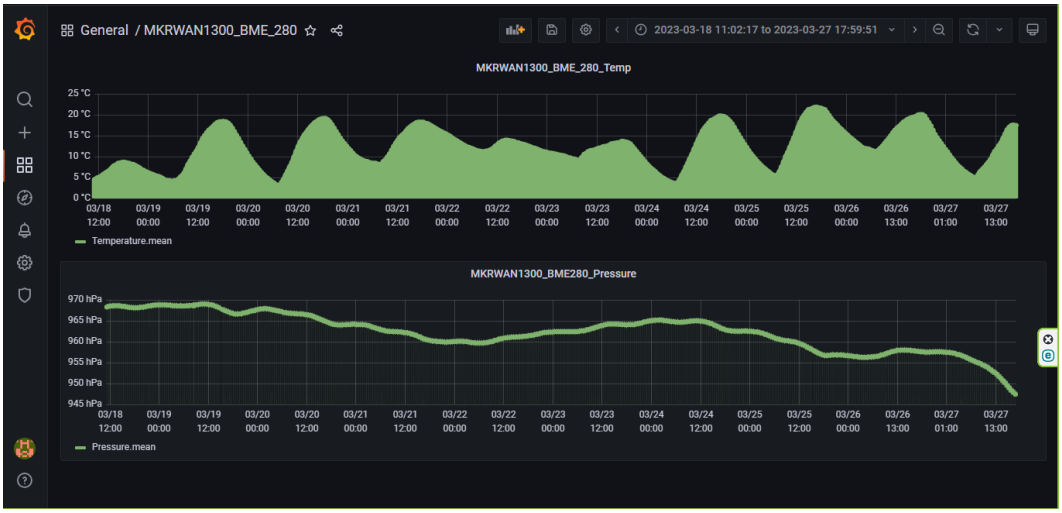
Фиг. 4.3. Web базиран интерфейс за управление и мониторинг на крайното устройство

Следващото крайно устройство е създадено отново за целите на дисертационната разработка с цел да се управлява автоматично и автономно вентилацията и проветрението в парникова инсталация. Устройството се захранва от батериен източник, а батерийните клетки се зареждат от соларен панел, който може да се изнесе извън парника. Комуникационното безжично устройство е MKRWAN1300[49] притежаващо комуникационен интерфейс LoRaWAN, то разполага и с редица възможности за свързване към него на различни по вид сензори и измерване на различни величини, които да послужат за автоматизация на определен процес в случая на автоматизирано отваряне и затваряне на капандурите на парника при определена температура и влажност. Към същия контролер може да бъде свързан и сензор за измерване на влагата в почвата, а чрез тази информация да се управлява и напоителна инсталация. Завършеният вид на крайното устройство може да се види на Фиг. 4.4.



Фиг. 4.4. Крайно устройство със соларен панел измерващо температурата и влажността на въздуха.

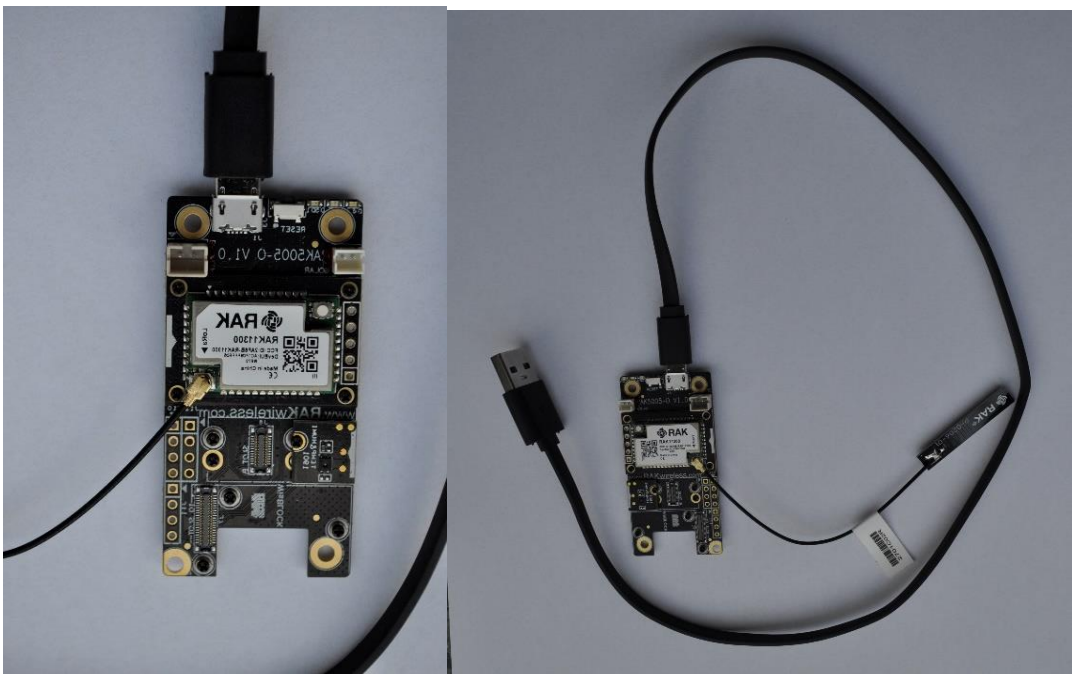
Данните от това устройство се визуализират в софтуерната среда Grafana, като те могат да се визуализират за голям период от време с цел статистика и предсказване на случващи се събития. На Фиг. 4.5. може да се види период на визуализация на данни от устройството.



Фиг. 4.5. Визуализирани данни от крайното устройство със соларно захранване

Ефективността на устройството се изразява в това, че то се захранва автономно от соларен източник на енергия, като батерийните клетки са предвидени с по-голям капацитет, заради възможно променливо или облачно време, с цел непрекъсваемост на измерването на температурата и влажността. Консумацията му на ток в режим когато не се предава съобщение е 1.6mA при 3,3V DC захранване. По груби сметки това е мощност със стойност 5,28mW. Този резултат е постигнат с използването на софтуерни библиотеки за „приспиване“ на хардуерни компоненти от контролера, на определени времеви интервали устройството се събужда прави измерване и след това изпраща данните, този момент се случва за около 25 ms[53], и след това отново хардуера се изключва за определено време. За тестово натоварване на устройството е заложен времеви интервал на пауза между изпращанията от 15 минути, т.е. устройството изпраща информация през 15 минути с цел да консумира повече енергия за 24 часов период и да се определи дали батерийните клетки са оптимално пресметнати.

Последното крайно устройство използвано в безжичната нискоенергийна платформа е предвидено за сградна автоматизация, а именно контрол на климатична инсталация и автоматизирано движение на щори. Отново измерва температурата и влажността, но в закрито помещение. Устройството е изградено от няколко модула свързани заедно, а те са: RAK5005[50] е основна платка върху която се включват и допълнителни модулни измервателни или комутиращи модули, RAK11300[51] е комуникационен модул съвместим с комуникационен протокол LoRaWAN, и модула за измерване на температура и влажност RAK1901[52]. Използваната LoRaWAN антена е от типа Patch антена (антена с нисък профил) и е подключена с конектор IPX чрез тънък коаксиален кабел към основната платка. Устройството може да се постави и в подходяща кутия, произведена конкретно за устройството, но за целите на дисертационната разработка такава не е закупена. Управлението на тези климатизацията и щорите се изпълнява от други устройства, които не са поместени в дисертационния труд. Логическите операции по следене на температурата, включването и изключването на климатика или изпращане на команди посредством инфрачервен модул се изпълняват в програмата среда Node-Red. На Фиг. 4.6. може да се види как изглежда крайното устройство с включените към основната платка модули.

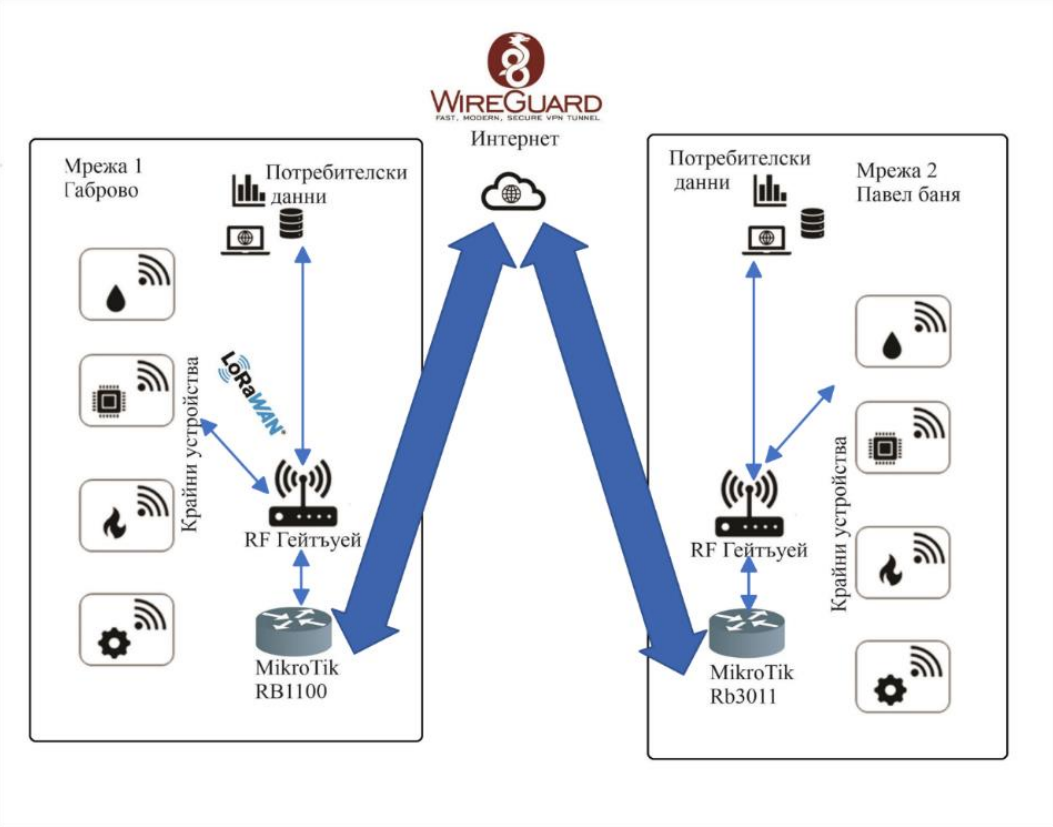


Фиг. 4.6. Крайно устройство RAK 5005 с комуникационен модул RAK 11300 и сензора за температура и влажност RAK 1901

Устройството е предвидено да се захранва от батериен източник на напрежение и ток, като има опция за свързване и на соларен панел за зареждане на батериите. Контролера за зареждане е интегриран и запоен на печатната платка. MicroUSB интерфейса е предвиден за конфигурация на устройството, както и за захранването му ако няма да се включват батерийни елементи. Устройството е модулно т.е. към основната платка могат да се включат различни по вид сензори или измервателни модули. Програмните среди с които се конфигурира устройството са Arduino IDE[54] и PlatformIO[55], като за всеки сензор или измервателен модул съществуват създадени софтуерни библиотеки от производителя.

4.3.Изследване на мрежовата свързаност между различни нискоенергийни безжични мрежи

Когато се изграждат няколко нискоенергийни безжични мрежи в различни сгради, райони, населени места или различни интернет мрежи данните генерирани от крайните устройства е добре да се съхраняват на едно основно място задължително с копиране на даните (backup). За тази възможност и за целите на дисертационния труд е изградена мрежова свързаност между различни интернет мрежи използвайки VPN тунелизация. За удобство е използван софтуерния продукт за тунелизация WireGuard[56], като той може да се инсталира ръчно на редица операционни системи, или както се използва в случая на дисертационната разработка, като софтуерен пакет от операционната система на маршрутизатор MiktorTik1100[57]. Концепцията на VPN тунела включва сървър и потребители, в случая описан в дисертационната разработка MikroTik1100 е конфигуриран да бъде сървър, а MikroTik3011[47] е конфигуриран да бъде клиент. За подробна информация как се конфигурират двата маршрутизатора виж [58]. След тази конфигурация между двата маршрутизатора, двете мрежи могат да обменят информация по между си. Единственото условие това да стане възможно е, и двата маршрутизатора да притежават публичен частен статичен IP адрес за да може да има достъп до тях и извън локалната мрежа. Двете мрежи се намират в два различни града в България- гр. Габрово и гр. Павел баня. На Фиг. 4.7. графично е показана интернет свързаността между двете нискоенергийни мрежи .



Фиг. 4.7. Мрежова свързаност между две нискоенергийни мрежи чрез WireGuard VPN

Общият сървър за запазване на данните от двете нискоенергийни мрежи се намира в Мрежа 2 с публичен статичен IP адрес с добавени защитни елементи за мрежова сигурност, като към нея е свързан маршрутизаторът RB1100 посредством VPN тунела виж. Фиг. 4.7.

4.2.1. Конфигурация на тунелната свързаност между маршрутизаторите

Конфигурация на интерфейса WireGuard

Първо, интерфейсите на WireGuard трябва да бъдат конфигурирани и на двата маршрутизатора, за да се позволяви автоматично генериране на частни и публични ключове. Командата е една и съща и за двата марврутизатора (въвежда се поотделно във всеки маршрутизатор):

```
/interface/wireguard
add listen-port=13231 name=wireguard1
```

Сега, когато се отпечатват подробностите за интерфейса, както частният, така и публичният ключ трябва да са видими, за да се позволи обмен на TCP/UDP пакети.

! Никой частен ключ никога няма да е необходим на отдалеченото устройство - оттук и името private.

Конфигурацията на маршрутизатор 1 RB1100:

```
/interface/wireguard print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=13231 private-
key="yKt9NJ4e5qlaSgh48WnPCDCEkDmq+VsBTt/DDEBWfEo="
      public-key="u7gYAg5tkioJDcm3hyS7pm79eADKPs/ZUGON6="
```

Конфигурацията на маршрутизатор 2 RB3011:

```
/interface/wireguard/print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=13231 private-
key="KMwxqe/iXAU8Jn9dd1o5pPdHep2blGxNWm9I944/I24="
      public-key="v/oIzPyFm1FPHrqhytZgsKjU7mUToQHLrW+="
```

За да могат да се достъпват трафици от информация от крайните устройства от едната мрежа към другата и обратно е необходимо да се конфигурират партньорски устройства с която се определя кой може да използва интерфейса на WireGuard и какъв вид трафик може да се изпраща през него. За да се идентифицира отдалеченият партньор, неговият публичен ключ трябва да бъде посочен заедно със създадения интерфейс WireGuard.

Конфигурацията на крайни устройство от мрежа 1 е:

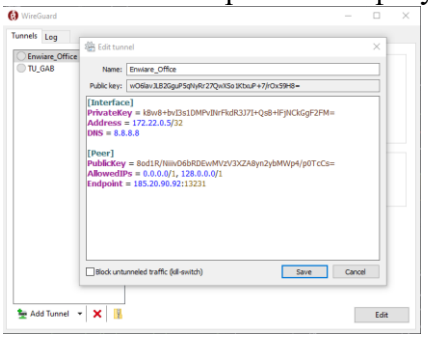
```
/interface/wireguard/peers
add allowed-address=192.168.14.100/24 endpoint-
address=37.143.223.xxx endpoint-port=13231 interface=wireguard1 \
public-key="v/oIzPyFm1FPHrqhytZgsKjU7mUToQHLrW+="
```

В мрежа 2 се намират всички останали крайни устройства и за момента не са необходими конфигурации за нея.

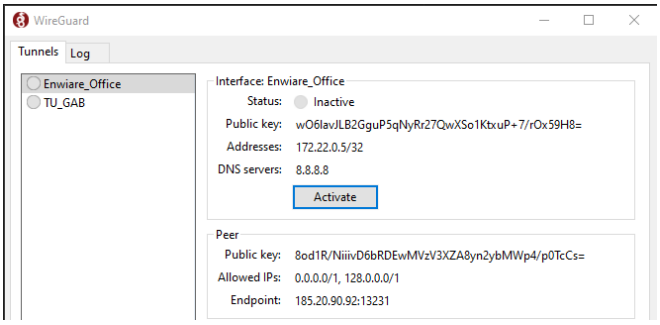
! Маршрутизаторите в двете мрежи трябва да имат осигурен реален публичен статичен IP адрес. В случая на дисертационната разработка единият маршрутизатор се намира в мрежата на доставчика на интернет услуги Bulsatcom, а другият в мрежата на доставчика Unics.

4.3.2. Тестване на тунелната комуникация между маршрутизаторите

За проверка на тунелната свързаност между маршрутизаторите се използва клиентското приложение Wireguard[56], инсталационния му пакет е разработен за различни операционни системи. След инсталацията му, е необходимо да се създаде или прикачи конфигурационен файл описващ, към коя мрежа да се свърже компютърната конфигурация и кои адреси да може да достъпва. Инсталирано и конфигурирано приложението може да се види на Фиг. 4.8.

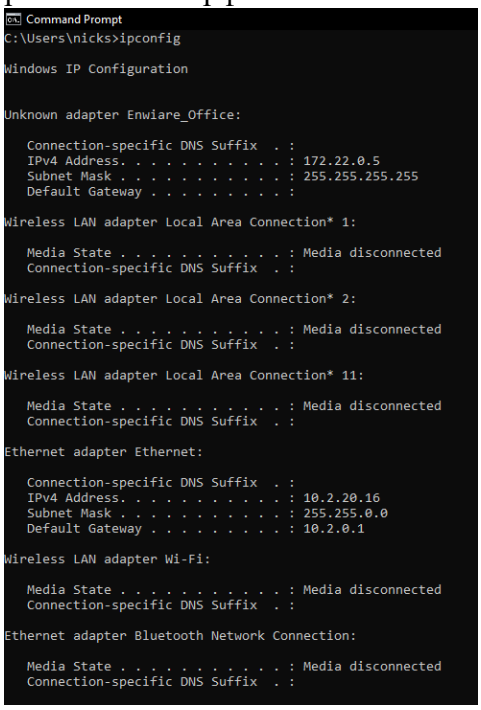


Фиг. 4.8. Конфигурационен файл за връзка с VPN сървъра



Фиг. 4.9. Активиране на VPN свързаността

След натискане на Save и след него бутона “Activate”, връзката се осъществява виж. Фиг. 4.9. Връзката може да се тества, като се изпълни в терминален прозорец командата „ipconfig” за проверка на комуникацията на мрежовите интерфейси на машината виж Фиг. 4.10.



Фиг. 4.10. Проверка на установена комуникация с VPN мрежата

III. ЗАКЛЮЧЕНИЕ

Обобщени изводи

Търсенето и експериментирането с нови нискоенергийни комуникационни протоколи и подобряване на кодирането на канала, използването на нови модулационни методи и разширяване на честотния спектър водят до интересни резултати свързани с подобряване на ефективността и обхвата на безжичното покритие. Избора на протокола LoRaWAN с висока енергийна ефективност би позволило да се следят важни параметри или да се управляват процеси на отдалечени места с цел подобряване качеството на живот. Това от своя страна води до увеличаване на трафиците от информация в комуникационните канали.

В дисертационния труд се разгледани възможности за пренос на данни на големи разстояния с помощта на нискоенергийни комуникационни протоколи. Изградена е софтуерна платформа за визуализация, нотификация и алармиране при промяна на параметър. Представената тематика води до създаване на методологии от процедури, свързани със създаването на нискоенергийна комуникационна платформа в контекста на концепцията IoT.

Публикации, свързани с дисертационния труд

По отношение на отразяване на резултатите по дисертационния труд са представени шест публикации на международни конференции и научни издания, напълно покриващи минималните изисквания относно разглеждания критерий. Три от трудовете са изнесени на Международна научна конференция „Унитех“ два в национална конференция „TechCo“ и един в рецензирано международно списание „JESTR”, като един от тях е самостоятелен, а останалите пет са изготвени в съавторство с научния ръководител и авторски колектив. Публикациите са издадени в сборници с научно рецензиране от международна научна конференция „Унитех“, национална конференция „TechCo“ и рецензирано международно

списание „JESTR” в периода на обучение 2019-2022 г. , като реално представят близо 2/3 от съдържанието на дисертационния труд.

IV. ПРИНОСИ КЪМ ДИСЕРТАЦИОННИЯ ТРУД

Научно-приложни приноси:

- Установени са и са изследвани доказали се алгоритми за криптиране на съобщенията при използването на нискоенергийния протокол LoRaWAN, които гарантират сигурността и надеждността на предаваните данни. Предложено е използването на метода с линейно променяща се честота (Chirp), който допринася за по-голямата защитеност на данните, като по този начин се използва по-тясна честотна лента, използвана при безжичните комуникации.
- Предложен е подход за определяне на ефективността на покритието при нискоенергийните безжични мрежи в градска среда, базиращ се на определени показатели, разделени в три групи - надеждност, забавяне и достоверност.
- Предложен е алгоритъм, представящ практически подход за реализация на RF шлюз и последователност при провеждането на експерименталните изследвания в закрита и открита зона.
- Изследвано е влиянието на отношението сигнал/шум върху качеството на безжичното покритие в конкретна открита зона. Направена е сравнителна оценка между практически получените резултати със симулационните в една и съща зона на радиопокритие, като обект на изследвания са параметрите на крайното устройство, на RF шлюза, затихването в коаксиалната линия и др.

Приложни приноси:

- За целите на дисертационния труд практически е реализирано крайно устройство на комуникационна система с използването на нискоенергийния протокол LoRaWAN за безжични комуникации с отдалечен контрол на електрически контакти с обратна връзка на състоянието на контактите.
- Практически е реализирано крайно устройство със соларно захранване, което е тествано в период от 3 години при различни метеорологични условия. Икономичността му е постигната чрез новосъздадената софтуерна библиотека за оптимизация на консумацията на крайното устройство по време на непредаването на данни.
- Предложена и е реализирана възможност за VPN свързаност на няколко маршрутизатора с реализираната нискоенергийна комуникационна система, използваща LoRaWAN протокола, с цел съхраняване на данните на определено място. В такъв случай отпада необходимостта от закупуването на допълнителен хардуер за запазване на данните като се предоставят и възможности за обработка, анализ, визуализация и изследване на данните от един централизиран пункт.

V. СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИЯТА

A1. Angelov K., **N. Manchev**, P. Kogias and S. Sadinov, Design and Development of a Platform for Test Applications in LoRa/LoRaWAN, Journal of Engineering Science and Technology Review (JESTR), Kavala Institute of Technology ISSN: 1791-9320, E-ISSN:1791-2377, 2019, pp. 17-21 (Scopus, SJR 0,189)

A2. Ангелов К., **Манчев Н**., Садинов С., Иванов Т., Планиране и изследване на зона на радиопокритие в LoRaWAN комуникационна мрежа, Международна научна конференция UNITECH 2020, 20-21 ноември 2020, Габрово, Том I,стр. I-263-268, 2020, ISSN: 1313-230X.

A3. Ташев П., К. Ангелов, **Н. Манчев**, Изследване и анализ на производителността на IoT комуникационни протоколи, Сборник доклади от научна конференция TechCo– Lovech 2021, стр. 71 – 76, 2021 (ISSN: 2535-079X).

A4. Ташев П., К. Ангелов, **Н. Манчев**, Сравнителен анализ на производителността на LoRa модулация за приложения в IoT. Международна научна конференция UNITECH 2021, 19 ноември 2021, Габрово, България, том. 1, стр. I-163-168, 2021 (ISSN: 1313-230X).

A5. П. Ташев, **Н. Манчев**, К. Ангелов, Изследване и сравнителен анализ на производителността на LoRa крайни устройства за мониторинг на улично осветление, TechCo 2022,стр. 47 – 52 (ISSN 2535-079X).

A6. **Н. Манчев**, Планиране и изследване на зона с безжично покритие в LoRaWAN комуникационна мрежа. Международна научна конференция UNITECH 2022, 18-19 ноември 2022, Габрово, България, том 1, стр. I-196-201, 2022 (ISSN: 2603-378X)

TITLE: „DEVELOPMENT AND RESEARCH OF A LOW ENERGY WIRELESS COMMUNICATION PLATFORM FOR THE INTERNET OF THINGS“

Author: M. Eng. Nikolay Petkov Manchev

ABSTRACT:

The dissertation deals with simulation models for low-power communications based on an analytical mathematical model describing the LoRaWAN communication protocol are presented, research is carried out and contributions related to the efficient use of the frequency spectrum, modulation type and channel coding are defined in order to achieve higher quality of service in low-power communication channels. Test setups have been implemented and experiments have been performed to evaluate the radio coverage and the success rate of the communication protocol in indoor and outdoor environments, and graphical relationships are presented giving information about the capabilities of the analytical model compared with results from the NS-3 simulation software.

Processes related to the processing, transmission and reception of low-energy signals in low-energy transmitters and receivers are studied - modulation, channel coding, multiplexing, synchronization, configuration, tuning and coordination of transceiving equipment. Different evaluation parameters and quality metrics such as equivalent isotropic radiated power (RSSI), field strength and signal-to-noise ratio are used as criteria to determine the quality of service, and the maximum allowable values of the SF spectrum broadening factors depending on the distance to the receiver are used in the criteria.

Keywords: Low Power, Wide Area Network, LoRa, LoRaWAN, FSK, DSSS, CSS, SNR, RSSI, , Dragino LT-33222, MKRWAN1300, Chirpstack, The Things Network