Moderní protokoly pro bezdrátové senzorové sítě

Bc. Andrej Osuský

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Andrej Osuský**
Osobní číslo:	**A15166**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**prezenční**
Téma práce:	**Moderní protokoly pro bezdrátové senzorové sítě**
Téma anglicky:	**Modern Protocols for Wireless Sensor Networks**

Zásady pro vypracování:

1. **Prostudujte vlastnosti protokolů využívaných v bezdrátových senzorických sítích.**
2. **Analyzujte rizika a zranitelnosti bezdrátových mesh sítí a k nim adekvátní obranné mechanismy.**
3. **Implementujte vybrané protokoly na platformách RE-Mote a CC2538EM a otestujte v reálném prostředí komplexu budov FAI UTB ve Zlíně.**
4. **Navrhněte testovací scénáře a vytvořte aplikaci pro ověření korektnosti chování sítě při komunikaci.**
5. **Změřte hodnoty propustnosti, latence, ztrátovosti packetů a energetické náročnosti.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MUKHERJEE, Nandini., Sarmistha. NEOGY a Sarbani. ROY. Building wireless sensor networks: theoretical & practical perspectives. ISBN 9781482230062.**
2. **XIAO, Yang, Hui CHEN a Frank Haizhon. LI. Handbook on sensor networks. London: World Scientific, c2010. ISBN 9812837302.**
3. **CHANG, Chip-Hong. Secure system design and trustable computing. ISBN 9783319149707.**
4. **MATOUŠEK, Petr. Síťové aplikace a jejich architektura. Brno: VUTIUM, 2014. ISBN 978-80-214-3766-1.**
5. **SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.**

Vedoucí diplomové práce: **Ing. Tomáš Dulík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **16. května 2017**

Ve Zlíně dne 3. února 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ..... Omsky

podpis autora

ABSTRAKT

Hlavným cieľom tejto práce je poskytnúť informácie o bezdrôtových senzorových sieťach. Teoretická časť pozostáva z analýzy tohto typu sietí, porovania rôznych techník smerovania, sietových bezpečnostných hrozieb a popisu štandardov IEEE 802.15.4, ZigBee a 6LoWPAN. Cieľom praktickej časti je otestovanie reálnej prevádzky siete a overenie jej funkcionalít. Sekcia taktiež obsahuje vyhodnotenie merania spotreby používaných zariadení počas rôznych simulovaných scenárov prevádzky.

Kľúčové slová: Senzorové siete, mesh siete, techniky smerovania, 6LoWPAN, Contiki

ABSTRACT

Main goal of this thesis is to provide informations about wireless sensor networks. Theoretical part consists of alaysis of this type of networks, comparsion of different routing techniques, network security vulnerabilities and description of standards IEEE 802.15.4, ZigBee and 6LoWPAN. Aim of practical part is testing a real network traffic and verification of network functionalities. This section also contains evaluation of device energy consumption measurements in different simulated traffic scenarios.

Keywords: Sensor networks, mesh networks, routing techniques, 6LoWPAN, Contiki

Chcel by som na tomto mieste poďakovať vedúcemu diplomovej práce pánovi Ing. Tomášovi Dulíkovi, Ph.D. za poskytnutie HW, bez ktorého by uskutočnenie tejto práce nebolo možné. Veľké ďakujem patrí taktiež mojej rodine a blízkym za ich pomoc a podporu počas celej doby štúdia na vysokej škole.

OBSAH

ÚVOD

Pokroky zaznamenané v oblasti bezdrôtovej komunikácie a neustále pokračujúcej miniaturizácie výpočtovej techniky, umožnili vznik drobných, energeticky nenáročných a cenovo dostupných komunikačných zariadení. Pripojenie senzorov k takýmto zariadeniam umožnilo vznik systému, v ktorom je celá fyzická infraštruktúra prepojená s komunikačnými a informačnými technológiami. V takýchto sofistikovaných systémoch, zariadenia vykonávajú senzorickú činnosť a jej výsledky kooperatívnym spôsobom zasielajú zvoleným zariadeniam. Predstavitelia takýchto systémov sú označovaní spoločným názvom ako bezdrôtové senzorické siete.

Bezdrôtové senzorické siete (BSS) pozostávajú obecne z množstva vzájomne spolupracujúcich zariadení, rozprestierajúcich sa často na veľké vzdialenosti. Výrazné odlišnosti oproti konvenčným sieťam, predstavujú vlastnosti ako samo-formovanie sieťovej štruktúry, fúzia zasielaných dát, možnosť mobility komunikujúcich zariadení a využívanie alternatívach trás v prípade poruchy zariadenia na používanej trase. Typicky sú zariadenia tohto typu sietí vybavené vlastným energetickým zdrojom. Využívané sieťové protokoly sú zamerané na maximálnu efektivitu komunikácie a minimálnu spotrebu energie pri jej vykonávaní. Svoje uplatnenie BSS nachádzajú v oblastiach od vojenskej, cez medicínsku až po dopravnú a civilnú.

Dôvodom výberu témy tejto diplomovej práce bol aktuálny rozmach v oblasti internetu vecí a BSS, ktorý je výrazne zastúpený v aktuálnych článkoch mnohých technických portálov. Táto oblasť predstavuje perspektívny trend a do budúcnosti sa predpokladá jej využitie v mnohých ďalších technických ale aj netechnických oblastiach.

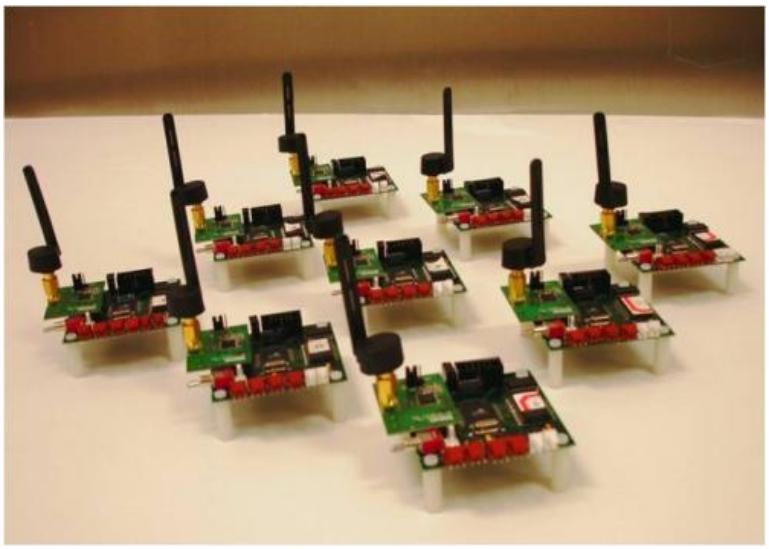
Cieľom tejto práce bola analýza BSS z pohľadu ich vnútorného fungovania, požadovaných vlastností a využívanej architektúry. Súčasťou teoretickej časti bolo popísanie smerovacích techník využívaných v BSS a zhodnotenie bezpečnostných rizík spojených s ich prevádzkou. Plánovanou činnosťou praktickej časti, bolo vykonanie testovania takejto siete v prostredí budovy FAI UTB v Zlíne. Účelom testovania bolo overiť a zhodnotiť správanie sa sieťových prvkov v rôznych situáciách. Súčasne bolo zámerom vykonať meranie energetickej náročnosti komunikácie pri simulovanej prevádzke.

I. TEORETICKÁ ČASŤ

1 Bezdrôtové senzorické siete

Bezdrôtové senzorické siete (BSS) boli podobne ako mnoho ďalších technických inovácii z počiatku vyvíjané pre využitie vo vojenskej sfére. Ich úlohou v tejto oblasti malo byť sledovanie a dohľad nad oblasťami vojnového konfliktu. Dnes siete pozostávajú z autonómnych zariadení, využívajúcich senzorov pre monitorovanie podmienok v priemyselnej sfére, zdravotníctve, doprave a mnohých ďalších oblastiach. [2]

Výskum v tejto oblasti, známy pod názvom distribuovaná senzorická sieť (DSN), začala agentúra DARPA v osemdesiatych rokoch minulého storočia. V tom čase agentúra už niekoľko rokov pracovala na projekte ARPANET pričom oba projekty boli vyvíjané na podnet americkej armády. Už vtedy sa u DSN predpokladalo využívanie veľkého množstva senzorických uzlov a ich vzájomnú kolaboráciu. Uzly mali fungovať autonómne bez nutnosti centrálneho riadenia a so schopnosťou smerovať informácie ku ktorémukoľvek uzlu. V tej dobe však technológia ešte nebola na dostatočnej úrovni. Existujúce senzory boli príliš rozmerné čo limitovalo množstvo potenciálnych aplikácii. K výraznej zmene vo vývoji BSS došlo vďaka pokrokom v mikro-elektromechanike a miniaturizácii senzorov. Takéto senzory už síce bolo možné umiestniť na potrebné stanoviská, no nastali problémy s ich inštaláciou. Nutnosť privádzať k senzorom kabeláž pre napájanie a prenos zaznamenaných údajov, predstavovala vynaloženie značných finančných prostriedkov. Keďže bezdrôtové senzorické siete predstavovali žiadanú alternatívu, spoločnosti z oblasti priemyselnej automatizácie investovali do ich vývoja značné prostriedky, čím priviedli túto oblasť do podoby v akej je dnes. [2]



Obr. 1.1 Uzly bezdrôtovej senzorickej siete [4]

1.1 Charakteristika

Bezdrôtové senzorické siete pozostávajú z množstva vzájomne spolupracujúcich zariadení. Sieť umožňuje riadiacemu systému získavanie informácii z prostredia do ktorého bola zavedená. BSS môže obsahovať množstvo senzorických zariadení, spoločne pokrývajúcich veľké vzdialenosti. Senzory využívané v sieti monitorujú fyzické podmienky prostredia, ako sú teplota, tlak, zvuk, vibrácie, pohyb a mnoho ďalších. Dáta získané senzormi sú zasielané cez sieť k analýze. Pri vytváraní topológie BSS je zásadnou schopnosť siete sa samo-formovať. Tá dovoľuje bezproblémové pridávanie nových komunikačných a senzorických uzlov, ako aj využívanie alternatívnych trás v prípade poruchy zariadenia na prenosovej trase. Fungovanie požadovaného sieťového správania umožňujú pre tieto účely vyvíjané komunikačné protokoly. [1, 2, 3]

Hardware ktorý tvorí jednotlivé uzly BSS je najčastejšie malých rozmerov, čo umožňuje umiestňovanie aj do ťažko dostupných miest. Tieto zariadenia je možné napájať privedenou kabelážou, avšak aby ich rozmiestňovanie bolo efektívne, jednotlivé zariadenia veľmi často disponujú vlastným energetickým zdrojom. Zariadenia sú spravidla vybavené jednoduchými mikrokontrolérmi (MCU). Obecne je možné definovať spoločné charakteristiky zariadení BSS nasledujúcimi vlastnosťami:

- Nízka pamäťová kapacita
- Limitované energetické zdroje
- Nízke výpočtové schopnosti [1]

1.2 Požiadavky

Počas niekoľkoročného vývoja došlo ku špecifikácii množstva návrhových faktorov, ovplyvňujúcich architektúru BSS a vlastnosti v nich používaných protokolov. Návrhové faktory sú ovplyvnené kombináciou implementačných požiadavkov na fungovanie siete a fyzikálnych princípov využívaných pri bezdrôtovej komunikácii. Jednotlivé návrhové faktory sú často objektom záujmu mnohých výskumníkov, či celých výskumných oddelení. Tieto požiadavky sú nasledujúce:

Spoľahlivosť - Označenie spoľahlivosť reprezentuje schopnosť sieťových uzlov udržiavať funkcionality a nepretržitú činnosť senzorickej siete aj v prípade výskytu poruchy na niektorom zariadení. Poruchy zariadenia môžu nastávať nepredvídateľne a je potrebné aby sieť bola schopná na takéto situácie adekvátne reagovať. Dôvodmi zlyhania zariadenia môže byť vyčerpanie energie, fyzické poškodenie, SW chyba či rušenie z prostredia brániace komunikácii. [9]

Sieťová topológia - Využívaná topológia svojím charakterom ovplyvňuje základné vlastnosti siete. Medzi tieto vlastnosti patria latencia, kapacita, priepustnosť alebo robustnosť. Topológiou je výraznou mierou ovplyvnená aj náročnosť smerovania pri zasielaní dát a s tým súvisiaca komplexnosť využívaného protokolu. Topológia priamo súvisí aj s fyzickým rozmiestňovaním uzlov do priestoru, kde je potrebné dbať na jej udržiavanie. Proces nasadzovania zariadení je preto často realizovaný v troch fázach:

1. Plánovanie pred nasadením
2. Nasadenie do prevádzky
3. Reorganizácia a pridávanie nových uzlov [9]

Škálovateľnosť - Vzhľadom na plánované využite môže sieť pozostávať z miliónov zariadení a z priestorového hľadiska zaberať rozsiahle územie. V takýchto rozľahlých sietiach je významným parametrom hustota rozmiestnenia uzlov. Tá v rámci siete, priamo úmerne ovplyvňuje stupeň pokrytia, ktorý je pre bezdrôtový prenos pozitívnym faktorom. Naopak so zväčšujúcou sa rozľahlosťou dochádza ku poklesu spoľahlivosti komunikácie a z dôvodu omeškania taktiež k zníženiu presnosti získavaných údajov. Škálovateľnosť siete označuje možnosť upravovať kombináciu jej hustoty a rozľahlosti. [9]

Bezpečnosť - Zabezpečenie siete, z pohľadu obrany voči možným útokom, je v senzorických sietiach zásadným požiadavkom. Útokov na sieť existuje viacero druhov, pričom môže ísť napríklad o pasívne odpočúvanie prebiehajúcej komunikácie, alebo o aktívne rušenie prenosu, zmeny v komunikačných trasách, podstrčenie nepravdivých informácii alebo špeciálne typy útokov zamerané na vyčerpanie energie uzlu a znižovanie jeho životnosti. Sieť by mala zabezpečovať ochranu dát a umožňovať detekciu narušiteľa. Pridávanie bezpečnostných postupov by malo byť aplikované so snahou o minimalizáciu ich negatívnych vplyvov na sieťovú komunikáciu. [9, 10]

Fúzia dát - Pojem fúziu dát označuje proces, pri ktorom dochádza ku redukcii veľkosti zasielaných dát, pomocou ich zoskupovania do nových zhlukov informácii. Tento proces je vykonávaný v priebehu zasielania dát prechádzajúcich sieťou. Pri množstve komunikujúcich senzorických uzlov, alebo veľkom objeme zasielaných dát, by v sieti mohlo dôjsť k záplave paketmi. Implementácia takejto funkcionality bráni nadmernému zaťaženiu siete ktorá by inak mohla spomaliť, alebo úplne znemožniť komunikáciu. [9]

Spotreba energie - Efektívne riadenie spotreby energie je kritickým faktorom. Príčinou je využívanie energeticky limitovaných zdrojov a častých prípadov, kedy výmena zdroju nie je možná. Kľúčovú úlohu pri predlžovaní životnosti batérie hrajú algoritmy riadiace aktivitu uzlu a používané komunikačné protokoly. Výskum v tejto oblasti protokolov je zameraný na minimalizáciu energetických výdajov pri komunikácii. Využívanými technikami sú kompresia dát, pre zníženie počtu zasielaných správ a zmeny v komunikačných trasách, pre balansovanie výdajov energie medzi ostatné uzly. [9, 10]

Samo-organizovanie - Schopnosť samo-organizovania je základnou vlastnosťou BSS. Umožňuje nasadenie nových senzorických uzlov schopných okamžite komunikovať a plniť pridelenú úlohu. Obzvlášť významnou sa táto funkcionalita stáva v prípadoch kedy dôjde na niektorom komunikačnom uzle k poruche. Okolité uzly dokážu detektovať nefunkčnosť zariadenia a zmeniť dovtedy používané trasy za alternatívne. Takýmto procesom dochádza k novému formovaniu komunikačnej štruktúry siete. V ideálnom prípade by nové formovanie siete malo byť vykonané s ohľadom na snahu o maximálnu úsporu energie. Novo vzniknuté trasy by mali využívať najefektnejšie spojenia a najmenší možný počet uzlov. [9]

Sieťová dynamika - Pod sieťovou dynamikou je označovaná schopnosť siete umožniť a vedieť reagovať na fyzické presuny uzlov v priestore. Toto je rozdiel oproti bežným sieťovým architektúram ktoré predpokladajú, že pozícia uzlov sa v sieti počas jej fungovania nemení. Možnosť takejto mobility uzlov je pozitívnou vlastnosťou, avšak jej zavedenie často negatívne ovplyvňuje stabilitu smerovania a spotreby energie. Uzol v tomto prípade musí vždy o svojej pozícii uvedomiť jeho nové okolie. [9]

Kvalita služieb - Pre aplikácie je nevyhnutné zasielanie aktuálnych informácii do stanoveného časového limitu. V opačnom prípade môže dôjsť k situácii, kedy sa dáta stávajú bezcennými. Pod pojmom kvalita služieb je v sieťovej terminológii označovaná úroveň schopnosti siete spoľahlivo a dostatočne rýchlo doručovať zasielané dáta. V aplikáciách je často so zvyšujúcou sa kvalitou služieb zvyšovaná aj energetická spotreba, preto je v tomto prípade potrebné hľadať akceptovateľný kompromis. [9, 10]

Pokrytie - Problematika pokrytia sa v tomto prípade zaoberá priamo senzorickými zariadeniami. Schopnosť uzlu sledovať svoje okolie je obmedzená z pohľadu vzdialenosti, ako aj presnosti zisťovaných údajov. Vzhľadom na zamýšľanú aplikáciu je potrebné uvedomenie si limitácii spojených so zvolenými senzormi. [9]

Konektivita - V BSS je nežiadúcim faktorom vytváranie podsietí, ktoré nie sú vzájomne prepojené. Pod pojmom konektivita je označovaná schopnosť dvoch ľubovoľných uzlov vzájomne nepretržite komunikovať. V reálnych aplikáciách je často využívané náhodné priestorové rozloženie, kde je konektivita kritickým faktorom. Túto vlastnosť môže ovplyvňovať aj využívaný protokol a spôsob voľby komunikačných trás. Dodržiavanie požiadavku na konektivitu by nemalo sieť obmedzovať z pohľadu variability topológie, fyzickej rozľahlosti ani z pohľadu samo-formovacej schopnosti siete. [9, 10]

1.3 Aplikácie

Vďaka svojím vlastnostiam sa BSS postupne presadili vo mnohých oblastiach. K ich zavedeniu dochádza do už existujúcich systémov, so zámerom vylepšiť ich vlastnosti, alebo rozšíriť ich funkcionality.

Svoje uplatnenie nachádzajú BSS najčastejšie v priemyselnej sfére. Vďaka jednoduchému nasadeniu BSS a poskytovaniu presných informácii v reálnom čase, sú zavádzané do výrobných a riadiacich procesov. V automatizovaných systémoch umožňujú sledovanie aktuálnej prevádzky a vzhľadom na získané informácie upravovať prebiehajúce procesy. BSS sú zavádzané na monitorovanie kritických systémov, v ktorých umožňujú včasné upozornenie ešte pred tým, ako dôjde ku krízovým stavom.

Doprava predstavuje ďalšiu oblasť využitia BSS. V mestách s rozľahlou dopravnou infraštruktúrou umožňujú siete sledovanie dopravnej prevádzky a podľa aktuálnych informácii upravovať spôsob jej riadenia. Dochádza k využitiu stacionárnych senzorov, monitorujúcich situáciu na konkrétnych miestach a taktiež mobilných senzorov, umožňujúci samotným vozidlám vykonávať senzorickú činnosť.

Inteligentné domácnosti taktiež predstavujú oblasť vhodnú pre BSS. Po zavedení a prepojení s riadiacim systémom umožňujú užívateľom špecifikovanie požadovaného správania (teplota, osvetlenie, atď.) v konkrétnych situáciách pre jednotlivé miestnosti. Napomáhajú taktiež ku znižovaniu spotreby v domácnosti.

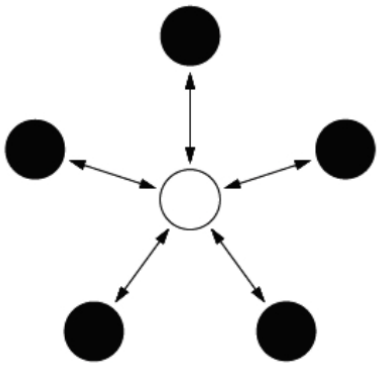
Ďalšou oblasťou využitia môže byť monitorovanie životného prostredia. Zavedenie umožnuje sledovanie znečistenia ovzdušia, získavanie meteorologických údajov a detekciu záplav alebo požiarov. Pre túto oblasť je významnou vlastnostnou siete schopnosť pokryť rozľahlé územia. [2]

1.4 Topológia

Pri bezdrôtovej komunikácii je z pohľadu efektivity kľúčovým prvkom využívaná topológia. Charakter topológie sa vzhľadom na požiadavky môže výrazne líšiť a ovplyvňovať parametre ako priestorový dosah, zaťaženie či celkovú priepustnosť siete.

1.4.1 Hviezdicová sieť

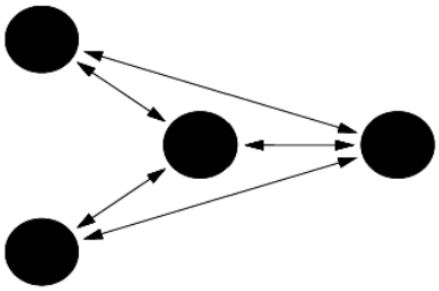
Hviezdicová sieť predstavuje topológiu pri ktorej jedna stanica zasiela a prijíma správy od ostatných uzlov. Týmto vzdialeným uzlom nie je dovolené komunikovať vzájomne medzi sebou, i keď niektoré z nich môžu byť vo vzájomnom dosahu. Medzi výhody takého typu siete patria jednoduchosť realizácie, možnosť udržať energetické zaťaženie vzdialených uzlov na minime a vykonávať rýchlu komunikáciu medzi uzlami a hlavnou stanicou. Výraznou nevýhodou takého riešenia je nutnosť vzdialených uzlov nachádzať sa v dosahu vysielania hlavnej stanice. Rizikom je taktiež fakt, že celá komunikácie je závislá na jedinom uzle, pričom pri jeho poruche sa celá sieť stáva nefunkčnou. [3]



Obr. 1.2 Hviezdicová topológia [3]

1.4.2 Mesh sieť

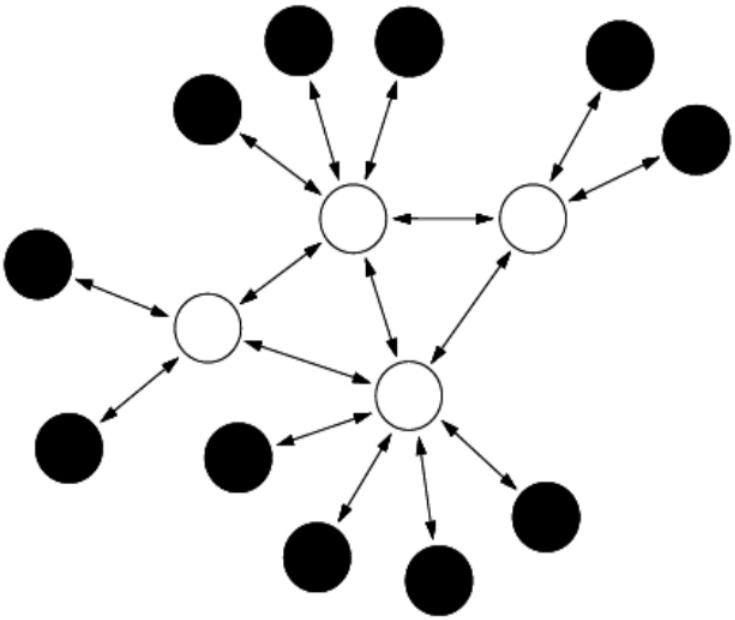
Mesh topológia siete umožňuje každému uzlu komunikovať so všetkými ďalšími uzlami v jeho dosahu. Takáto vlastnosť umožňuje v sieti tzv. viac skokovú komunikáciu. To v praxi znamená, že uzol ktorý chce komunikovať s uzlom mimo jeho vlastný dosah, môže pre doručenie správy využiť uzly medzi nimi. Výhodou topológie je škálovateľnosť a redundancia komunikačných trás. V prípade že jeden uzol siete prestane z akéhokoľvek dôvodu pracovať, komunikácia môže stále prebiehať pomocou ostatných uzlov v dosahu. Výhodou je taktiež vlastnosť tejto topológie, ktorá neobmedzuje priestorovú rozľahlosť na dosah jedného uzlu. Pridávaním ďalších uzlov umožňuje rozšírenie siete do priestoru, bez akýchkoľvek limitácií. Výrazným negatívom takého riešenia je vysoká spotreba energie a výrazné zníženie životnosti batérii uzlov zabezpečujúcich viac-skokovú komunikáciu. Typicky sú na uzly takýchto sietí kladené požiadavky na nízku energetickú spotrebu v čoho dôsledku pri viac skokovej komunikácii dvoch vzdialených uzlov, vzniká výrazné zvýšenie času potrebného pre doručenie správy. [3]



Obr. 1.3 Mesh topológia [3]

1.4.3 Hybridná mesh-hviezdicová sieť

Hybridná topológia vznikla spojením výhodných vlastnosti oboch predchádzajúcich topológii. Mesh-hviezdicová topológia poskytuje všestranné a robustné sieťové riešenie, zachovávajúc schopnosť senzorických uzlov udržovať spotrebu energie na minimálnej úrovni. V tejto topológii senzorické uzly nedisponujú schopnosťou preposielať správy. Modifikácia pôvodnej mesh topológie umožňuje udržanie minimálnych energetických nárokov. Nesenzorické uzly dovoľujúce skokovú komunikáciu a teda spotrebovávajúce väčšie množstvo energie sú často napájané priamo z elektrických rozvodov, alebo sú vybavené silnejším zdrojom energie. [3]



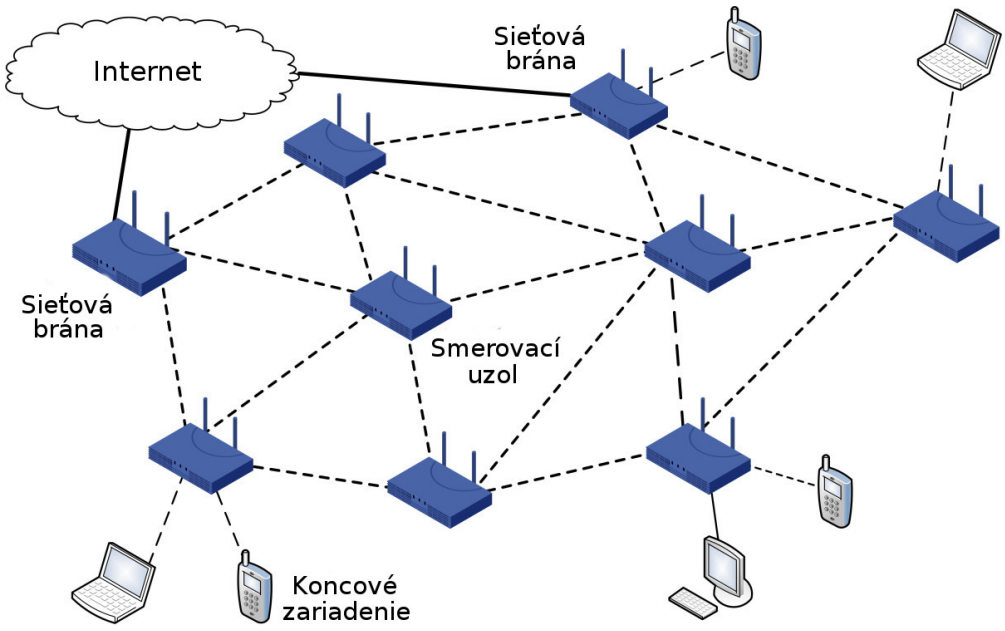
Obr. 1.4 Mesh-Hviezdicová topológia [3]

1.5 Architektúra

Využitie senzorických sietí v reálne prevádzke si z dôvodu požadovaných funkcionalít a vysokých nárokov na efektívnosť komunikácie, vyžiadalo vytvorenie sieťovej štruktúry. V nej je každému zariadeniu presne špecifikovaný jeho účel.

1.5.1 Senzorická sieť

Najobecnejšia akceptovaná architektúra vychádza zo spomínanej mesh-hviezdicovej topológie (1.4.3), kde sieť pozostáva z troch typov zariadení. Najpočetnejšie zastúpenými zariadeniami v sieti sú koncové uzly, nazývané tiež mesh klienti alebo senzorické uzly. Tento typ zariadení je typicky mobilný. Disponuje vlastným zdrojom energie, malou pamäťou a nižším výpočtovým výkonom. Typicky je jeho úlohou do siete vysielať senzorom zistené údaje, alebo v prípade ak slúži ako akčný člen, naopak zo siete príma preňho určené správy a vykonáva riadenie. Vzájomnú komunikáciu v sieti zabezpečuje zariadenie nazývané mesh smerovač alebo smerovací uzol. Tento typ zariadení tvorí strednú vrstvu architektúry a ich zoskupenie tvorí chrbticu site. Najvyššiu vrstvu architektúry tvoria zariadenia typu mesh gatesway, nazývanými tiež Internet gateway border router alebo obecne sieťová brána. Sieťová brána je drôtovo alebo bezdrôtovo prepojená s minimálne jedným smerovacím uzlom. Gateway disponuje pripojením do Internetu, čím umožňuje vzdialené riadenie procesov a monitorovanie senzormi zachytených údajov. [2, 3, 6, 7]



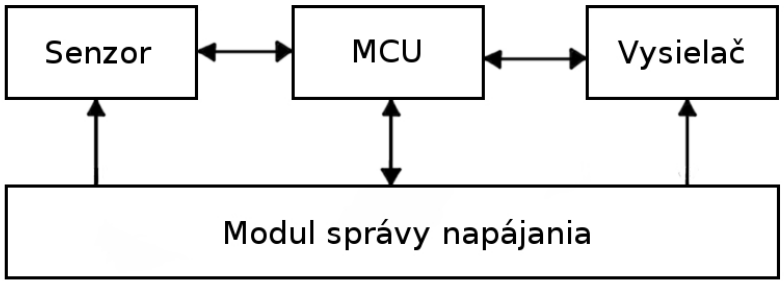
Obr. 1.5 Architektúra bezdrôtovej mesh siete [5]

1.5.2 Senzorický uzol

Senzorický uzol z pohľadu HW pozostáva zo štyroch základných častí:

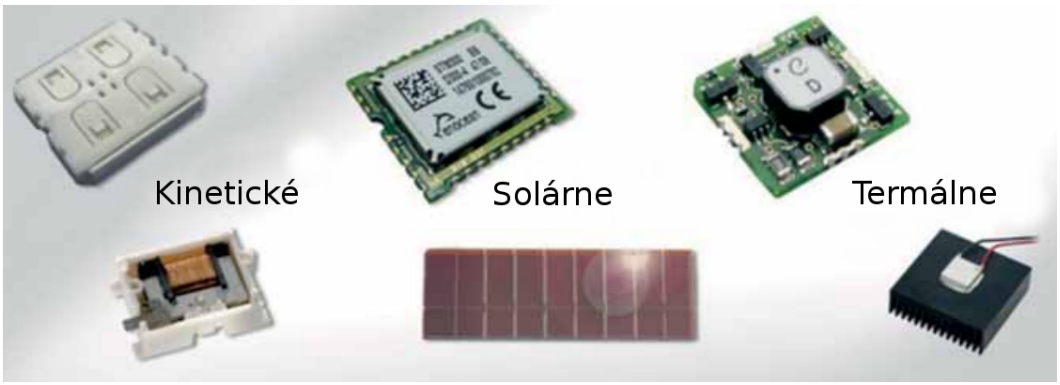
- Senzor pre monitorovanie sledovanej veličiny
- Mikrokontrolér riadiaci zariadenie
- Vysielač pre bezdrôtovú komunikáciu
- Zdroj energie a modul pre správu napájania

Každá z týchto častí je zodpovedná za vlastnú špecifickú činnosť. Senzor zodpovedá za sledovanie podmienok okolitého prostredia ako aj zisťovanie stavu zariadení. Činnosťou senzoru je zber a transformácia zo zdroja zachytených signálov, do formy elektrických signálov. Po transformácii sú pomocou A/D prevodníku signály konvertované do digitálnej podoby a v tomto stave sú sprostredkovávané mikrokontroléru. MCU po prijatí dát informácie uloží do vlastnej pamäte a v prípade potreby vykoná ich dodatočné spracovanie. MCU je riadiacou častou zariadenia a spolupracuje so všetkými ostatnými časťami. Dokáže podľa potreby fungovať v rôznych stavoch. V stave "spánku"sa nachádza v prípadoch kedy je jeho cieľom ušetriť maximum energie a ignoruje komunikáciu na sieti. V stave "nečinnosti"sa nachádza ak čaká na doručenie správ zo siete a v "aktívnom"stave je zariadenie v momente, kedy dochádza k prijímaniu alebo odosielaniu dát. Zasielanie zistených informácii, alebo prijímanie informácii zo siete je vykonávané za pomoci jednotky vysielača. Typicky ide od vysielače dosahujúce nízkych prenosových rýchlostí od 10 do 100 kb/s. Dosah vysielania sa pohybuje najviac do 100 metrov. Takéto parametre vysielača sú volené z dôvodu úspory energie, keďže bezdrôtová komunikácia u týchto zariadení predstavuje energeticky najnáročnejšiu úlohu. Modul pre správu napájania poskytuje zo zdroja energiu, potrebnú pre fungovanie celého systému. Zdroj často disponuje nízkou zásobou energie a preto je celé zariadenie, pre svoju bežnú prevádzku, uspôsobené na minimalizáciu energetických nárokov. [2, 7]



Obr. 1.6 Architektúra senzorického uzlu [8]

Z pohľadu HW a životnosti tvorí najkritickejší element senzorického uzlu jeho zdroj energie. Životnosť energetického zdroja, integrovaného do zariadenia, je závislá na jeho kapacite a na miere využívania prístroja. Aby mohla byť dosiahnutá vyššia alebo prípadne neobmedzená výdrž, ako alternatíva sú k zariadeniam pridávané technológie pre získavanie energie z okolitého prostredia. Požiadavkom na takéto systémy generujúce elektrickú energiu sú, podobne ako u samotného senzorického zariadenia, malé rozmery. Využívanými zdrojmi energie môžu byť svetlo, teplo, pohyb a vibrácie. Oproti dnes už konvenčným fotovoltaickým článkov sú využívané piezoelektrické kryštály, mikro oscilátory či termoelektrické generátory. [2]



Obr. 1.7 Alternatívne zdroje energie [2]

1.6 Komunikačný protokol

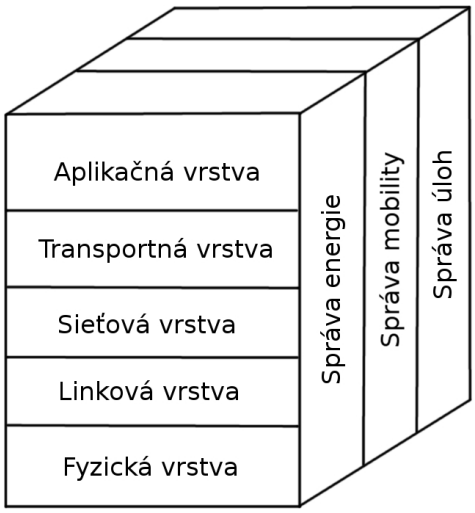
V BSS sa pri komunikácií všetky uzly riadia spoločnými protokolmi. Sada takýchto protokolov by mala umožňovať kooperáciu sieťových uzlov, efektívne vykonávanie bezdrôtovej komunikácie, vzájomne zoskupovanie zasielaných informácii a mala by byť schopná vykonávať smerovanie aj s vedomím o stave energie uzlov na využívaných trasách. Protokolová sada, ktorej štruktúra je zobrazená na obrázku 1.8, by mal vzájomne integrovať roviny riadenia ako sú správa spotreby energie, správa mobility, správa vykonávaných úloh a viaceré komunikačné vrstvy.

Správa spotreby energie zaobstaráva riadenie spôsobu, akým senzorický uzol využíva zásoby energie. Energia je rozdeľovaná trom základným aktivitám, ktorými sú: činnosť senzoru, výpočty MCU a bezdrôtová komunikácia. Príkladom spôsobu šetrenia energie môže byť obmedzenie prijímania opakujúcich sa správ, pri ktorom dochádza k dočasnému vypínaniu prijímača po prijatí správy. Ďalším prípadom je využívanie smerovacích funkcii výlučne smerovacími uzlami a využívať koncové uzly iba na odosielanie senzorom zistených údajov.

Správa mobility je zodpovedná za detekciu mobility senzorických uzlov a registráciu ich zmien v priestorovom rozložení. Primárnou úlohou je udržiavanie aktuálnych komunikačných ciest ku každému uzlu. Správa mobility uzlom umožňuje sledovať susedských uzlov v ich dosahu a taktiež susedstvo iných uzlov siete.
Správa úloh sa zaoberá snahou o kooperáciu sieťových uzlov. Cieľom tejto správy je plánovanie a balansovanie senzorickej a detekčnej činnosti uzlov. Veľké využitie nachádza správa úloh v prípadoch, kedy nie je potrebné aby všetky uzly v špecifikovanej oblasti vykonávali merania simultánne. Vzhľadom na energetickú zásobu môžu niektoré senzorické uzly vykonávať meranie častejšie ako iné. [3, 9]

Činnosť protokolovej sady zasahuje do nasledujúcich komunikačných vrstiev:

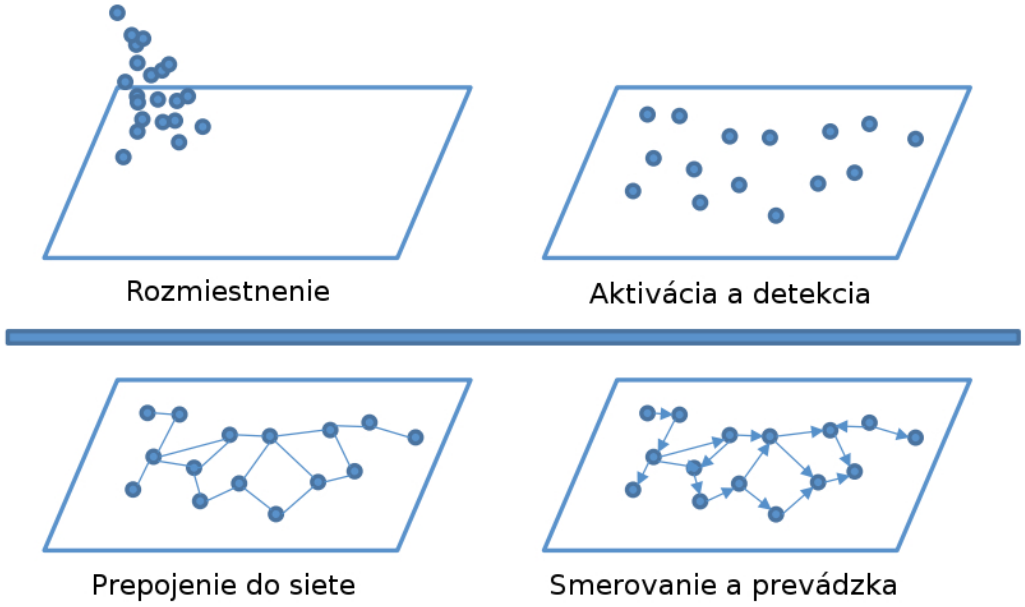
- **Fyzická vrstva** - venuje sa prenosu informácii z fyzikálneho pohľadu. Definuje spôsob modulácie signálu a techniky vysielania a príjmu.
- **Linková vrstva** - zodpovedá za multiplexovanie dátových prúdov, detekciu rámcov a kontrolu prípadných chýb.
- **Sieťová vrstva** - primárnou úlohou je smerovanie zasielaných dát.
- **Transportná vrstva** - ak to aplikácia BSS vyžaduje, pomáha táto vrstva udržiavať tok zasielaných dát.
- **Aplikačná vrstva** - podľa požadovanej funkcie umožňuje vrstva vytvorenie špecifického riadiaceho aplikačného SW.



Obr. 1.8 Protokolová sada [3]

2 Techniky smerovania

Smerovanie je jednou zo základných funkcii ktoré sú od uzlov BSS vyžadované. Spôsob akým je smerovanie vykonávané, zásadne ovplyvňuje fungovanie sieťovej infraštruktúry. So zvyšujúcim sa počtom zariadení v sieti sa správne smerovanie stáva náročnejším. Podľa rozlohy, hustoty a požadovaného zámeru je potrebné zvoliť adekvátny smerovací prístup. K smerovaniu resp. ku hľadaniu komunikačných trás by malo dochádzať okamžite po nasadení a aktivácii senzorických uzlov. [2]



Obr. 2.1 Nasadenie a aktivácia senzorickej siete [2]

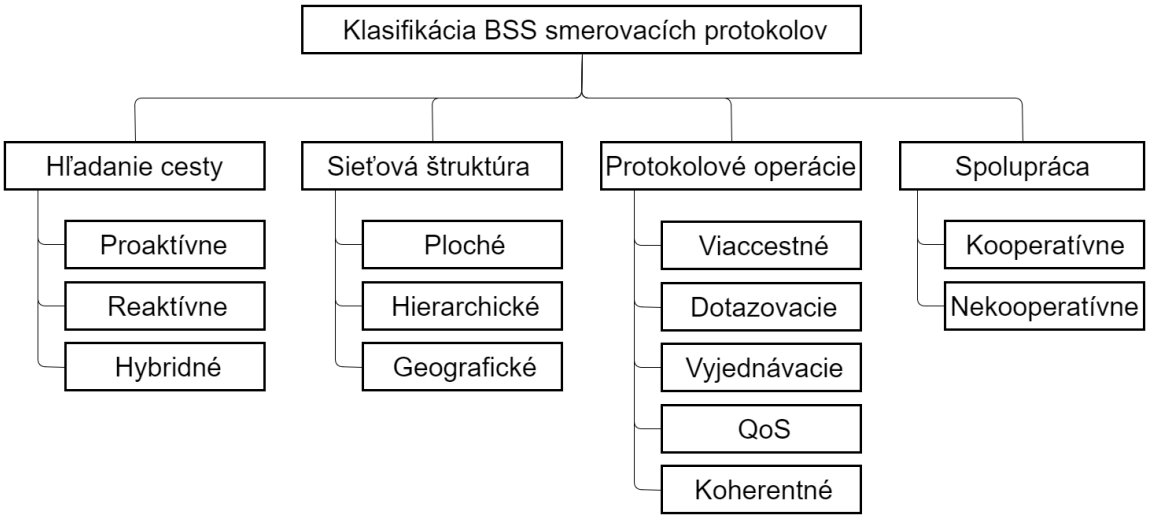
Za spôsob akým je smerovanie vykonávané je zodpovedný zvolený komunikačný protokol. Ten by mal v ideálnom prípade rešpektovať všetky už spomenuté požiadavky(1.2) kladené na BSS. Algoritmy aplikované v protokoloch môžu byť klasifikované podľa nasledujúcich parametrov:

1. **Hľadanie cesty** - Pri klasifikácii z pohľadu spôsobu akým zdrojový uzol hľadá cestu k cieľovému sú protokoly delené do kategórii proaktívnych, reaktívnych a hybridných. Pri proaktívnom prístupe sú všetky cesty vypočítané ešte predtým, ako sú pre komunikáciu potrebné. Prístup je vhodný ak sú senzorické uzly statické. Reaktívny prístup je presným opakom. Cesty sú stanovené na vyžiadanie, až v čase kedy sú reálne potrebné. Hybridný prístup predstavuje kombináciu výhodných vlastností oboch predchádzajúcich. Používané cesty sú uchovávané a v prípade nutnosti novej, je táto stanovená na vyžiadanie. [1]

2. **Sieťová štruktúra** - Pri klasifikácii z pohľadu sieťovej štruktúry je smerovanie hodnotené vzhľadom na spôsob vytvárania prepojení medzi senzorickými uzlami. V prípade že sú si v sieti všetky uzly rovné a vykonávajú rovnakú úlohu dochádza k tzv. plochému smerovaniu. Pokiaľ v sieti dochádza ku rozdeleniu úloh a niektoré uzly sú z pohľadu komunikácie nadradené nad inými, je tento spôsob smerovania klasifikovaný ako hierarchický. Poslednú kategóriu tvorí pozičné smerovanie ktoré je vykonávaná, s ohľadom na znalosť geografického rozmiestnenia uzlov v priestore. [1]

3. **Protokolové operácie** - Vzhľadom na toto kritérium dochádza k deleniu z pohľadu implementovaného spôsobu, akým protokol funguje. Z pohľadu vlastností môže protokol spadať do kategórie viaccestných, dotazovacích, vyjednávacích, koherentných alebo medzi protokoly zamerané na kvalitu poskytovaných služieb. Každý protokol môže spadať do viacerých kategórii zároveň. [1]

4. **Spolupráca** - Klasifikáciu je možné vykonať aj vzhľadom na fakt, či v sieti dochádza alebo nedochádza ku spolupráci uzlov. Pri kooperačnom smerovaní koncové uzly zasielajú dáta jednému centrálnemu uzlu kde sú spoločne agregované a až potom zasielané ďalej k cieľu. [1]



Obr. 2.2 Klasifikácia smerovacích protokolov v BSS [14]

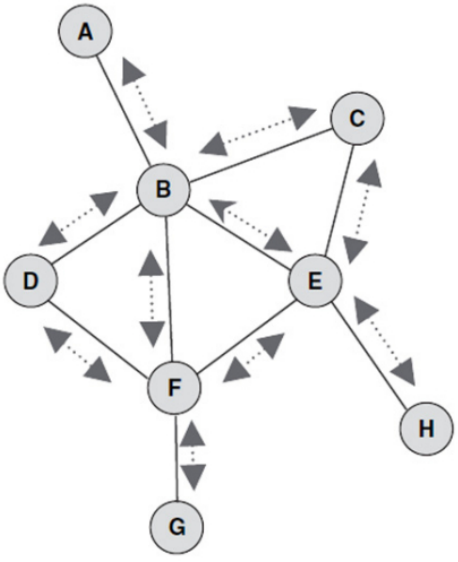
Z vyššie uvedených klasifikácii je najrozšírenejšia oblasť sústrediaca sa na sieťovú štruktúru. Nasledujúca sekcia je venovaná deleniu smerovacích techník podľa tohto kritéria a obsahuje popis vybraných protokolov.

2.1 Ploché smerovanie

V plochých sieťach všetky senzorické uzly spolupracujú a z pohľadu sieťovej štruktúry sú si vzájomne rovné. Takáto architektúra má niekoľko výhod ako minimálne nároky na udržiavanie sieťovej infraštruktúry a potenciálne veľké množstvo možných alternatívnych komunikačných ciest. [3]

2.1.1 Záplava

Záplava je jednou z najstarších techník pre objavovanie komunikačných ciest a rozširovanie informácii v rámci drôtových a bezdrôtových sietí. Stratégia smerovania je veľmi jednoduchá a nevyžaduje žiadnu údržbu sieťovej topológie. Pri záplave je využívaný reaktívny prístup. Každý uzol ktorý zachytí zasielanú správu ju ďalej pošle všetkým ostatným susediacim uzlom v dosahu. Odosielaný paket tak v sieti prejde všetky cesty, vďaka čomu vždy nájde cieľový uzol. Výhodnou je v tomto prípade schopnosť veľmi jednoducho reagovať na zmeny v topológii, či už ide o pridávanie alebo odoberanie uzlov. Takéto správanie však výrazne ovplyvňuje komunikáciu v sieti. Dochádza k nárastu redundancie, znižovaniu priepustnosti a z pohľadu spotreby energie uzlov pri preposielaní je takýto prístup najnevhodnejší. Obrázok 2.3 zobrazuje schému fungovania takéhoto typu sietí. [3]



Obr. 2.3 Záplava siete [3]

2.1.2 Roznášanie

Pod pojmami roznášanie alebo ohováranie je označovaný prístup odvodený od záplavy. Tento prístup vznikol za účelom vyhnutia sa niektorým jeho nevýhodám. Podobne ako pri záplave je využívané jednoduché pravidlo pre preposielanie správ. Oproti záplave kde je prijatá správa odoslaná všetkým z okolia, v tomto prípade dochádza ku odosielaniu správy náhodnému susedskému uzlu. Tento proces sa iteratívne opakuje až dokiaľ paket nedorazí do cieľa, alebo nie je vyčerpaný zadaný maximálny počet skokov zasielanej správy. Takýto prístup je menej energeticky náročný ako záplava avšak nie je zaručené doručenie správy. Komunikačná cesta sa neustále mení a taktiež je často volená cesta cez viac uzlov než je nevyhnutne potrebné. [3]

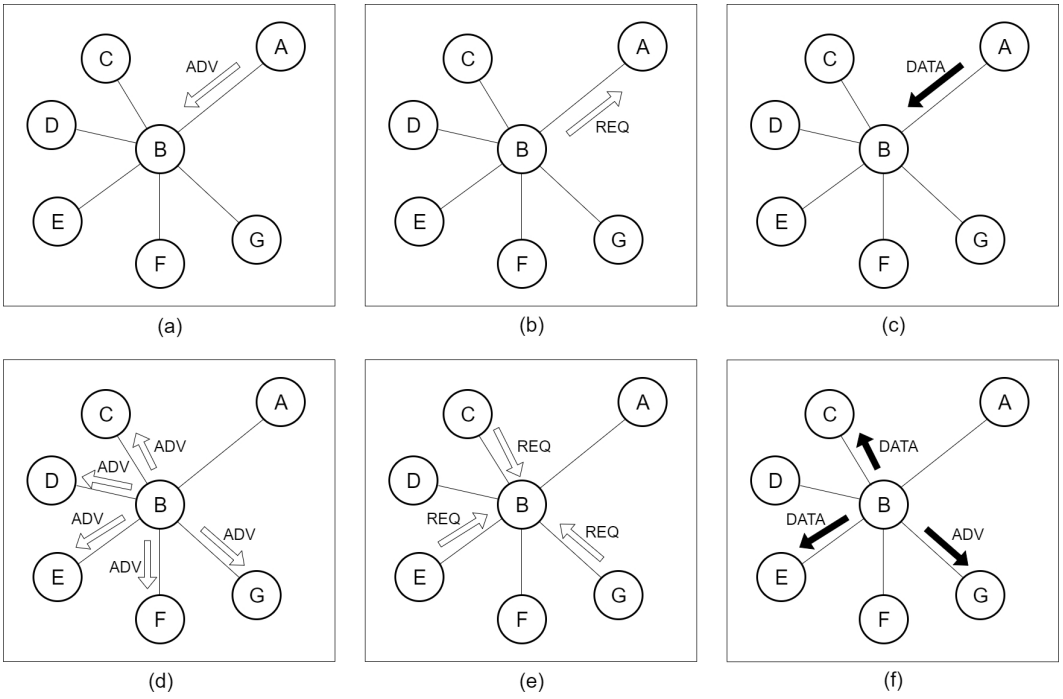
2.1.3 SPIN

Protokol SPIN (Sensor Protocols for Information via Negotiation) patrí do skupiny dátovo-centrických a vyjednávacích protokolov BSS. Hlavným cieľom je zasielanie získaných informácii ostatným uzlom v sieti. V tomto protokole je využívaný predpoklad, že uzly vo vzájomnej blízkosti disponujú podobnými dátami. Dochádza výlučne ku zasielaniu dát ktorými ostatné uzly nedisponujú.

Zariadenia využívajúce SPIN pridávajú k svojim dátam popisné metadáta. Pred vysielaním nameraných informácii dochádza medzi uzlami k vyjednávaniu s metadátami, za účelom eliminovania redundancie zasielaných dát. Sémantika týchto metadát nie je súčasnou protokolu SPIN a jej voľba je výlučne na užívateľovi.

V okamihu keď senzorický uzol získa nové informácie, je vyslaná správa typu ADV obsahujúca adekvátne metadáta. Ak má niektorý zo susediacich uzlov o tieto dáta záujem ,prejaví ho odoslaním správy typu REQ. Zdrojový uzol následne zašle všetkým susedom, ktorý prejavili záujem, správu typu DATA s požadovanou informáciou. Uzol ktorý dáta prijal následne zopakuje rovnaký postup, čoho výsledkom je doručenie kópie tejto správy do každej senzorickej oblasti.

Vyjednávanie je riešením klasického problému záplavového prístupu a dosahuje výrazne vyššiu efektivitu z pohľadu spotreby energie. Z pohľadu sieťovej prevádzky dochádza ku zníženiu redundancie takmer o polovicu. Výhodnou schopnosťou protokolu je malý vplyv zmien v topológii ovplyvňujúci len obmedzenú oblasť. Uzly potrebujú vedieť výlučne o svojich susedských uzloch vzdialených na jeden skok. Nevýhodou vyjednávacieho prístupu je nemožnosť zaručiť doručenie dát [11]

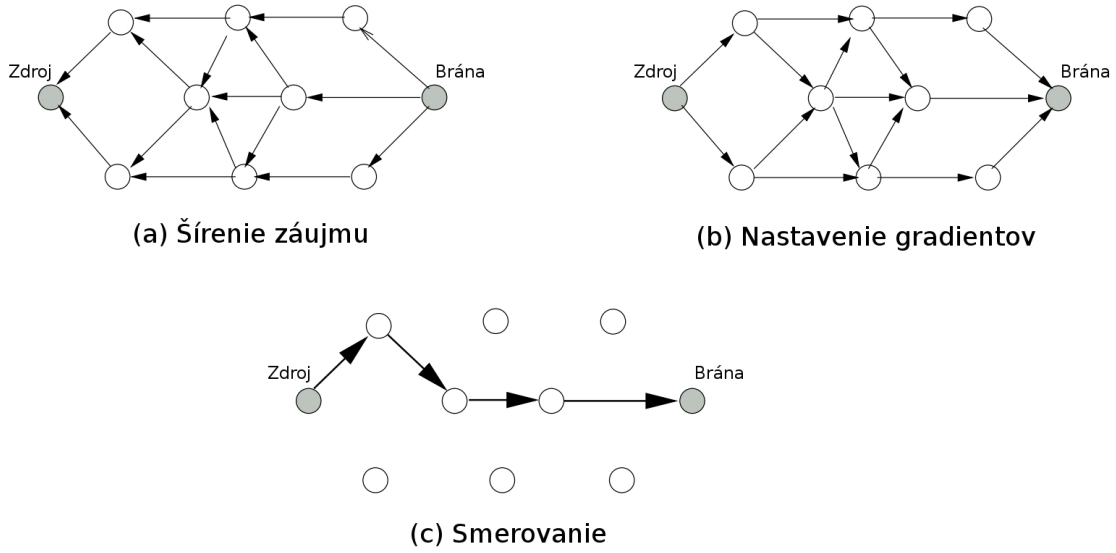


Obr. 2.4 SPIN [3]

2.1.4 Riadené šírenie

Riadené šírenie je ďalším dátovo-centrickým prístupom. Zasielané hodnoty sú vždy pomenované a dáta sú zasielané spoločne ako pár atribút a hodnota. V tomto prístupe senzorické uzly zaznamenávajú sieťové udalosti v ich bezprostrednom susedstve a vzhľadom na získané informácie si v pamäti vytvárajú tzv. gradienty. Obecne tieto gradienty špecifikujú názov atribútu a smer k uzlu ktorý má o tieto údaje záujem. V prípade že sieťová brána vyžaduje určité dáta, vyšle do siete správu o ich záujme. Takáto správa je šírená sieťou a preposielaná každým uzlom ktorým bola prijatá. Súčasne so šírením správy sieťou, sú nastavované gradienty cesty smerom ku zdrojovému uzlu. Tento proces pokračuje až kým sú nastavené všetky gradienty od zdroja až po cieľový uzol.

Spôsob akým prebieha voľba cesty je rozdelený do troch fáz a je znázornený na obrázku 2.5. Prvou fázou je zasielanie správy o záujme. Ako už bolo uvedené v tejto fáze správa postupne prechádza celou sieťou. Druhou fázou je tvorba gradientov. Tretiu fázu tvorí stanovenie cesty a zasielanie vyžiadaných dát. Po stanovení gradientov vzniknú mnohé alternatívne cesty toku informácii z ktorých je vybraná najvhodnejšia. V rámci poslednej fázy dochádza taktiež ku kontrole sieťového zacyklenia. Sieťová brána periodicky zasiela správu o záujme okamžite pri prijatí dát od zdroja. Takáto činnosť je nevyhnutná z dôvodu, že správy o záujme nie sú cez sieť šírené spoľahlivo. V prípade zasielania dát z viacerých zdrojov sú dáta po ceste agregované, čím je vytváraný tzv. agregačný strom. [3, 11]



Obr. 2.5 Vizualizácia riadeného šírenia [11]

2.1.5 Rozchyrovacie smerovanie

Rozchyrovací spôsob smerovania je úpravou riadeného šírenia, v ktorom pomocou záplavy dochádza ku rozšíreniu dotazov do celej siete. V určitých prípadoch kedy je potrebné zasielať len malý objem dát však nie je použitie záplavy nutné. Kľúčovou myšlienkou je smerovanie dotazov výlučne uzlom ktoré majú informácie o sledovanej udalosti, namiesto toho aby správa s dotazom cestovala celou sieťou. Algoritmus rozchyrovacieho smerovania využíva záplavu pre šírenie informácii o senzorických udalostiach. Tieto správy sú zasielané pomocou paketov s dlhou životnosťou nazývanými agenti. Ak uzol deteguje udalosť, vkladá si ju do vlastnej lokálnej tabuľky udalostí a vygeneruje agenta. Agenti následne cestujú sieťou aby podali informáciu o lokálnych udalostiach aj vzdialeným uzlom. Keď uzol vygeneruje dotaz na udalosť, uzly na ktoré tento dotaz dorazí môžu prehľadať vlastné tabuľky udalosti a zaslať odpoveď. Vďaka tomu nie je pri dotazovaní nutné zaplaviť celú sieť, čo redukuje nároky na sieťovú komunikáciu. Na druhej strane rozchyrovacie smerovanie udržuje iba jednu komunikačnú trasu, oproti riadenému šíreniu kde sú dáta zasielané mnohými cestami. Rozchyrovacie smerovanie nachádza uplatnenie v prípadoch, keď je v sieti generovaný malý počet udalostí a veľký počet dotazov. Pri veľkom počte udalostí a nedostatku požiadavkov sa cena využívania agentov a tabuliek udalostí stáva nevýhodnou. [11]

2.1.6 MCFA

Algoritmus MCFA využíva vlastnosť siete, ktorá vykonáva smerovanie oproti typicky statickej sieťovej bráne. Senzorické uzly nevyužívajú žiadny explicitný adresovací mechanizmus. Namiesto toho každý uzol udržuje najnižší odhad ceny cesty od seba k bráne. Každá uzlom prijatá správa je preposlaná všetkým jeho susediacim uzlom. Okamžite ako uzol prijme správu, skontroluje či sa nachádza na najmenej nákladnej trase medzi zdrojovým senzorickým uzlom a bránou. V takom prípade tento uzol vyšle prijatú správu svojim susedom. Tento proces sa iteratívne opakuje do momentu doručenia správy. Termín "cena"v tomto prípade označuje voliteľný hodnotiaci parameter, ktorým môže byť napr. počet skokov alebo energetická náročnosť.

Odhady ceny cesty od uzlov ku hlavnej stanici sú získavané v nastavovacej fáze. Brána najskôr vysiela všetkým uzlom naokolo správu s cenou nastavenou na hodnotu nula. Každý uzol má na začiatku nastavenú najnižšiu cenu cesty ku sieťovej bráne na nekonečno. Uzol po prijatí vysielanej správy skontroluje či odhad ceny ktorý prijal je menší ako aktuálny odhad. V prípade že je prijatá hodnota menšia, je lokálny odhad uzlu aktualizovaný. Hodnota odhadu v prijatej správe je taktiež adekvátne aktualizovaná a zaslaná ďalej. [11, 12]

2.1.7 ACQUIRE

Protokol ACQUIRE (ACtive QUery forwarding In sensoR nEtworks) pracuje so sieťou ako s distribuovaným databázovým systémom. Protokol umožňuje deliť zložité dotazy zasielané do siete na menšie poddotazy, riešiteľné jednotlivými uzlami. Brána zasiela dotaz, ktorý je následne preposielaný každým uzlom ktorý ho prijal. Počas toho sa každý uzol snaží zodpovedať aspoň časť dotazu a následne ho zaslať ďalšiemu uzlu. Ak požadovaná informácia ktorou uzol disponuje nie je aktuálna, uzol sa pokúsi získať informáciu od susedských uzlov vzdialených od neho na stanovený počet skokov. V momente úplného zodpovedaniu dotazu, dôjde k jeho spätnému zaslaniu bráne.

Protokol umožnuje upravovanie efektívnosti dokazovania. To je vykonané zmenou parametru maximálneho počtu skokov pre získanie aktualizovanej informácie. Ak je počet príliš veľký, dochádza v sieti k podobnému správnou ako pri záplave. Naopak pokiaľ je hodnota nízka, samotný dotaz musí cestovať sieťou na viac skokov. Pre nájdenie optimálneho nastavenia je využívané matematické modelovanie. Výber ďalšieho skoku pri preposielaní dotazu je volený náhodne, alebo na základe predpokladaného potenciálu s akým môže uzol uspokojiť zasielaný dotaz. [11]

2.2 Hierarchické smerovanie

Hierarchické smerovania je známou sieťovou technikou využívanou pôvodne už v pevných drôtových sieťach. Tento prístup poskytuje viaceré výhody týkajúce sa škálovateľnosti, efektivity komunikácie, energeticky efektívneho smerovania a možnosti uzlov sa zhlukovať. V zhlukoch môžu byť uzly s vyššou energetickou zásobou vybrané ako vedúce uzly nazývané hlavy klastrov. Úlohou vedúcich uzlov je spracovávanie, agregácia a zasielanie získaných informácii uzlov príslušného klastru. Cieľom hierarchického prístupu je zníženie počtu zasielaných správ a celkové zníženie spotreby energie. [1, 11]

2.2.1 LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) je protokol schopný organizovať sieť do sady klastrov. Náhodne vyberá niekoľko senzorických uzlov a volí ich za vodcovské uzly. Po stanovenom čase nastáva tzv. rotácia, pri ktorej dochádza k výberu nových hlavných uzlov. Výhodou tohto riešenia je rovnomerné zaťaženie všetkých zariadení v sieti. Zber dát je centralizovaný a je vykonávaný periodicky. Vďaka tomu je tento protokol vhodný v aplikáciách, kde je potrebné kontinuálne monitorovanie.

Fungovanie protokolu je rozdelené do dvoch fáz. V prvej fáze označenej ako nastavovacia, dochádza ku vytvoreniu klastrov a dochádza k výberu ich vedúcich uzlov. Stanovená percentuálna časť uzlov p sa sama navrhne za budúce hlavy klastrov. Voľba prebieha na základe vygenerovania náhodného čísla z intervalu od 0 do 1 a jej porovnaním s prahovou hodnotou $T(n)$ daného uzlu n. Výpočet prahovej hodnoty je vykonaný na základe rovnice ktorá zohľadňuje požadované množstvo vodcovských uzlov a informáciu o aktuálnom kole r. Voľba za vodcovský uzol prebieha výlučne u uzlov ktoré túto úlohu neplnili za posledných $1/p$ kôl.

$$T(n) = \frac{p}{1 - p\ (\ r \mod (1/p)\ )} \tag{2.1}$$

Každý zvolený vedúci uzol vyšle pre ostatné uzly upozorňujúcu správu o jeho novo získanej funkcii. Všetky ostatné uzly sa po prijatí takýchto správ rozhodnú, do ktorého klastru chcú byť zaradené. Rozhodnutie je založené na sile signálu prijatej správy. O tejto skutočnosti uzly zaslanou správou upovedomia vodcovský uzol. Ten následne vytvorí a rozpošle TDMA plán pre jednotlivé uzly ustanovujúci čas, kedy je im umožnené vysielanie. Vtedy nastáva prechod do druhej tzv ustálenej fázy, počas ktorej môžu uzly vykonávať senzorickú činnosť a zasielať získané dáta vedúcemu uzlu. Ten vykoná fúziu dát a agregované dáta zašle sieťovej bráne. Po určitom stanovenom čase sieť prechádza znova do nastavovacej fázy a celý cyklus sa opakuje. Doba trvania nastavovacej fáze oproti fáze ustálenej, je z dôvodu minimalizácie režijných nákladov výrazne kratšia.

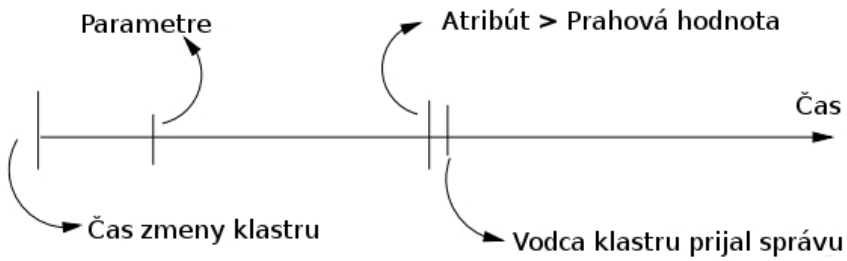
S protokolom LEACH sú spojené určité problémy. LEACH predpokladá že všetky uzly dokážu vysielať s dostatočným výkonom aby dosiahli na hlavnú stanicu jedným skokom. To znamená že prístup nie je použiteľný na priestorovo rozľahlé siete. Ďalšou nevýhodou je nemožnosť vopred odhadnúť akým spôsobom bude požadovaný počet klastrových hláv rozložený po sieti. Samotná vlastnosť dynamicky sa meniaceho zhlukovania prináša zvýšené režijne náklady. Protokol predpokladá že všetky uzly disponujú rovnakou zásobou energie a taktiež že činnosť všetkých vedúcich uzlov klastru je rovnako energeticky náročná, čo v reálnych aplikáciách nie je zaručené. [3, 11]

Tab. 2.1 Porovnanie vybraných protokolov [11]

	SPIN	Riadené šírenie	LEACH
Voliteľná cesta	Nie	Áno	Nie
Doba životnosti	Dobrá	Dobrá	Výborná
Vedomosť o spotrebe	Áno	Áno	Áno
Využitie metadát	Áno	Áno	Nie

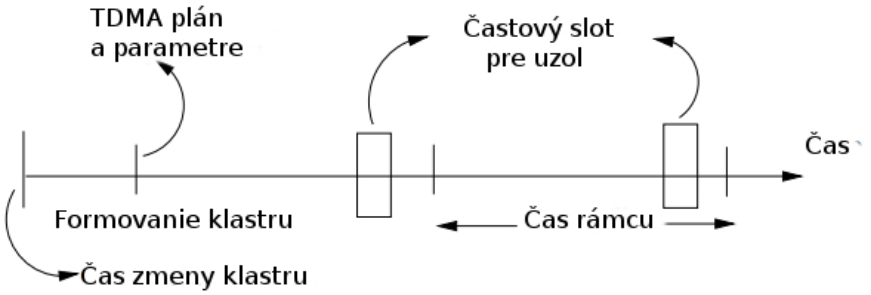
2.2.2 TEEN, APTEEN

Cieľom protokolov TEEN (Threshold-sensitive Energy Efficient sensor Network protocol) a APTEEN (Adaptive Periodic TEEN) je predĺženie aktívnej doby fungovania siete. Ide o vhodnú voľbu v aplikáciách kedy je rýchlosť získavania senzorických údajov kritickým faktorom. Na uzloch prebieha kontinuálna senzorická činnosť, no jej výsledky sú zasielané len pri splnení stanovených podmienok. Vodcovské uzly informujú členov klastru o atribútoch ktoré majú byť senzormi získavané a o dvoch prahových hodnotách. Prvou z nich je tzv. tvrdá prahová hodnota (TPH) ktorej prekročenie je nutnou podmienkou pre odosielanie senzorických dát. Druhou z nich je tzv. jemná prahová hodnota (JPH) ktorá je taktiež podmienkou vyvolania vysielanie a to v prípade prekročenia hodnoty prahu hodnotou rozdielu aktuálnej a predchádzajúcej nameranej hodnoty. Vysielanie nastáva jedine v prípade ak sú prekročené obe prahové hodnoty. Vhodným nastavením prahových hodnôt môže dôjsť ku výraznému zníženiu počtu vysielaných správ. Z pohľadu spotreby energie je takýto prístup výhodný, no dochádza ku kompromisu z pohľadu presnosti hodnôt sledovaného deja. Tieto popísané vlastnosti sú spoločné pre oba protokoly. [3, 11, 12]



Obr. 2.6 Operácie protokolu TEEN [11]

V protokole APTEEN sú vodcovské uzly volené podobným spôsobom akou u TEEN. V tomto prípade však hlavy odosielajú členom dva dalšie parametre, TDMA vysielací rozvrh a dobu časového odpočtu. Vďaka tomu môžu uzly vysielať výlučne počas stanoveného času. Pre kontrolu aktivity môže byť vynútené odoslanie dát po uplynutí stanovenej doby odpočtu. Protokol tak poskytuje viac flexibility a väčšiu kontrolu nad spotrebou energie. [3, 11, 12]



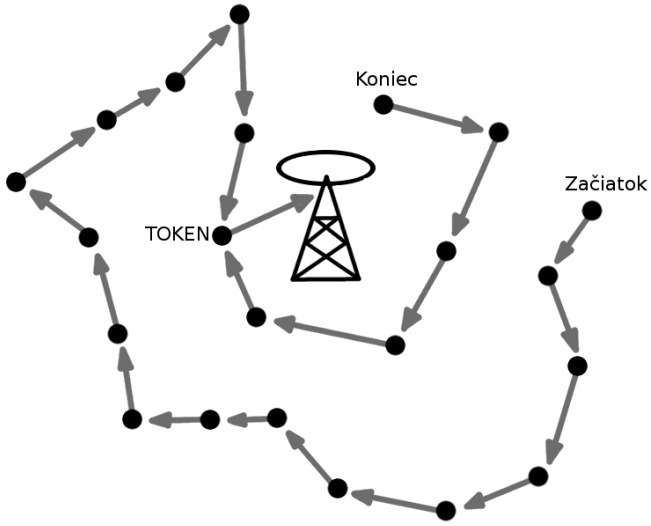
Obr. 2.7 Operácie protokolu APTEEN [11]

2.2.3 PEGASIS

Protokol PEGASIS (Power-Efficient Gathering in Sensor Information Systems) vznikol ako odpoveď na niektoré nedostatky protokolu LEACH (2.2.1). Hlavými cieľmi sú:

- Minimalizovať dosah každého uzlu
- Minimalizovať režijné náklady
- Minimalizovať počet správ zasielaných hlavnej stanici
- Rovnomerne rozložiť spotrebu energie naprieč sieťou

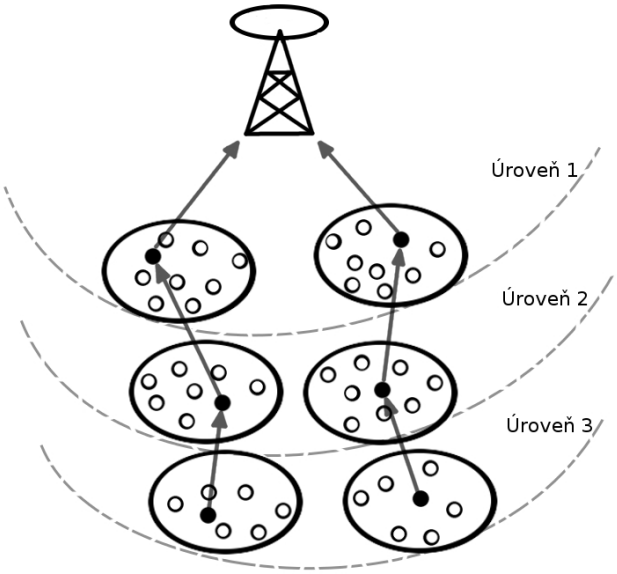
Protokol dovoľuje uzlom komunikovať iba s ich najbližšími susedmi. Na detekciu najbližších susedských uzlov a odhad ich vzdialenosti, protokol využíva informácie o sile signálu. Komunikácia so sieťovou bránou prebieha periodickým striedaním sa uzlov pri vysielaní. Všetky uzly siete sú pri komunikácii formované do zreťazenej štruktúry (obr. 2.8). Každý uzol po získaní dát od susedského uzlu vykoná fúziu s jeho vlastnými senzorickými dátami a jej výsledok zašle ďalšiemu uzlu. Proces sa opakuje až po dosiahnutie sieťovej brány. Pri reťazovitej komunikácii je využívaný riadiaci token, ktorý je od koncového uzlu postupne preposielaný po uzloch siete. Jeho úlohou je špecifikovať ktorý uzol je aktuálny vodca a teda ktorý je zodpovedný za komunikáciu s hlavnou stanicou. [11, 13]



Obr. 2.8 Ilustrácia protokolu PEGASIS [13]

PEGASIS umožňuje predĺženie doby životnosti siete, vďaka použitiu kooperatívnych techník spolupráce medzi uzlami. Pri použití protokolu dochádza ku redukcii šírky pásma keďže je uzlom povolená výlučne komunikácia v ich blízkosti. Dochádza k upravovaniu silu signálu aby bolo možné v ideálnom prípade vysielať a zachytávať signály len z jedného uzlu. Narozdiel od LEACH, protokol PEGASIS nevyužíva klastrovanie siete čo výrazne znižuje režijne náklady.

Nástupca protokolu označovaný ako hierarchický viac-skokový PEGASIS bol vyvinutý s cieľom znížiť omeškanie paketov počas prenosu. Využíva v sebe zhlukovací mechanizmus v kombinácii s viac-skokovým smerovaním cez hlavy jednotlivých klastrov. Takáto metóda umožňuje paralelné odosielanie dát a výrazným spôsobom urýchľuje komunikáciu. [11, 13]



Obr. 2.9 Hierarchický viac-skokový PEGASIS [13]

2.2.4 SOP

Protokol SOP (Self Organizing Protocol) popisuje prístup podporujúci v sieti heterogénne senzorické uzly a definuje ich architektúru. Protokol pracuje s uzlami ktoré môžu byť statické alebo mobilné. V architektúre sú definované tri typy zariadení:

- **Senzorický uzol** - môže byť stacionárny alebo mobilný
- **Smerovací uzol** - výlučne stacionárny, formujú štruktúru siete
- **Sieťová brána** - uzol zhromažďujúci získané dáta

Takéto rozdelenie funkcii sieťovým uzlom je už uvedenou najobecnejšou štruktúrou BSS (1.5.1). Každý senzorický uzol musí byť v dosahu smerovacieho uzlu aby mohol odovzdať získané dáta. Zozbierané dáta sú pomocou smerovacích uzlov preposielané hlavnej stanici. Priraďovanie adries senzorickým uzlom prebieha pomocou smerovacieho uzlu, ku ktorému je uzol pripojený. Vďaka tomuto procesu dochádza k vytvoreniu hierarchickej štruktúry. Oproti protokolu LEACH (2.2.1) takáto štruktúra umožnuje pri komunikácii nižšiu spotrebu energie. Vďaka prideľovaniu adries je tento prístup vhodne využiteľný v aplikáciách, v ktorých je vyžadovaná komunikácia s konkrétnym uzlom. Výhodou prístupu je nenáročná údržba smerovacích tabuliek a udržiavanie štruktúry pomocou periodického overovania výpadkov uzlov. Nevýhodou sú režijné náklady spojené s reštrukturalizáciou siete, ktorá nie je vykonávaná na vyžiadanie, ale prebieha neustále. [11, 12]

2.2.5 TTDD

Prístup protokolu TTDD (Two-Tier Data Dissemination) sa nespolieha na jeden centrálny statický uzol zhromaždujúci dáta, ale podporuje využívanie väčšieho počtu mobilných sieťových brán. Statickými sú v tomto prípade práve senzorické uzly. Každý zdrojový uzol si z okolitých uzlov proaktívne vytvára mriežkovú štruktúru, ktorú využíva pri šírení informácii.

Zdrojový uzol pre vytvorenie sieťovej mriežky najskôr volí seba samého ako prvý stred tejto štruktúry (prekríženie v mriežke) a zasiela oznámenie o dátach každému uzlu z jeho štyroch priľahlých priechodov. Celý proces sa u uzlov ktoré prijali správu zopakuje. Šírenie skončí v momente keď správa dorazí na uzol vzdialený jeden skok od cieľu špecifikovaného v správe alebo ak správa dorazí na hranicu siete. Po dokončení tohto procesu je vytvorená komunikačná a smerovacia štruktúra v tvare mriežky.

Obecne je dĺžka cesty v TTDD väčšia ako je najkratšia možná. Táto neoptimálnosť cesty je kompenzovaná prínosom vo forme škálovateľnosti siete. Komplikácie môže zapríčiniť spôsob, akým sú získané informácie o rozmiestnení pre korektné vytvorenie sieťovej mriežky. V porovnaní s riadeným šírením protokol dosahuje dlhšiu životnosť siete ale taktiež väčšie omeškanie pri komunikácii.[11]

2.3 Pozičné smerovanie

Pozičné smerovanie využíva adresovanie uzlov vzhľadom na ich umiestnenie v priestore. Vzdialenosť medzi susedskými uzlami môže byť odhadovaná na základe sily prichádzajúceho signálu. Pokiaľ je uzol vybavený satelitným prijímačom, je možné určiť presné umiestnenie uzlu pomocou GPS systému. Tento prístup umožňuje získavať údaje z vybranej oblasti, bez špecifikovania konkrétneho uzlu ako zdroja. Informácie o pozícii sú využité pre zvýšenie efektivity smerovania. [11, 12]

2.3.1 GAF

GAF (Geographic Adaptive Fidelity) je protokol pracujúci s informáciami o pozíciách a taktiež o aktuálnej zásobe energie. Pri tomto prístupe je sieť rozdelená do fixných symetrických zón formujúcich mriežku. Protokol definuje tri stavy v ktorých sa môže uzol nachádzať. Týmito stavmi sú:

- **objavný** - určenie umiestnenia v mriežke
- **aktívny** - účasť na komunikácii
- **uspaný** - vypnutie vysielača

Uzly priradené do rovnakej oblasti sú, z pohľadu smerovania a spotreby energie pri jej vykonávaní, považované za ekvivalentné. Vrámci každej oblasti uzly vzájomne spolupracujú. V zóne dochádza ku zvoleniu jedného uzlu, ktorý zostáva aktívny. Ostatné uzly v zóne môžu pre šetrenie energie prejsť do režimu spánku. Aktívny uzol následne komunikuje s hlavnou stanicou ktorej odovzdáva získané údaje za celú zónu. Protokol GAF teda predlžuje životnosť siete tým, že využíva len minimálny možný počet komunikujúcich uzlov. Predlžovanie životnosti sa výrazne zvyšuje so zvyšujúcim sa počtom uzlov v oblasti. V rámci protokolu nie je nad dátami vykonávaná žiadna agregácia.

Aby protokol umožňoval mobilitu, každý uzol v mriežke odhadne čas kedy danú oblasť opustí. Túto odhadovanú dobu rozpošle susedným uzlom v zóne. Uzly v oblasti následne upravia svoju dobu spánku podľa prijatej informácie. Pred vypršaním odhadnutého času odchodu sa spiace uzly zobudia a jeden z nich sa stane novým aktívnym uzlom. Voľba veľkosti štvorcov z ktorých sa mriežka skladá je vykonávaná podľa požadovaného vysielacieho výkonu. Problematickým je v tomto prístupe spôsob, akým plánovať pridelenie úloh jednotlivým uzlom. [3, 11, 12]

2.3.2 GEAR

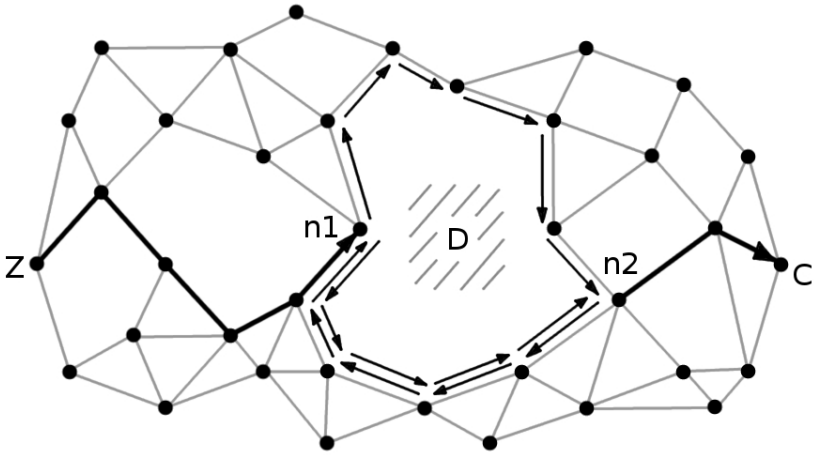
Pod označením GEAR (Geographic and Energy Aware Routing) je protokol využívajúci informácie o pozícii uzlov a ich energetických dispozíciách. Smerovanie správ prebieha pomocou heuristických techník, využívajúcich informácie o pozíciách uzlov. Protokol pracuje podobne ako riadené šírenie s tým rozdielom, že namiesto šírenia po celej sieti, propagovanie správ záujmu o dáta prebieha výlučne v stanovenej oblasti.

Každý uzol protokolu GEAR si uchováva odhadovanú a naučenú cenu prenosu správy cez jeho susedné uzly. Odhadovanie ceny je vykonávané vzhľadom na zostávajúcu energiu a vzdialenosť k cieľovému uzlu. V prípade že uzol nemá bližšie k cieľovej oblasti žiadneho zo svojich susedných uzlov ako je on sám, v sieti došlo k objaveniu tzv. diery. Naučené ceny sú zdokonalením odhadovaných cien, ktoré vyplynuli zo smerovania okolo týchto dier. Ak nie sú nájdené žiadne diery naučená cena je zhodná s odhadovanou.

Algoritmus je vykonávaný v dvoch fázach. Prvou je preposielanie paketov smerom ku cieľovej oblasti. Po prijatí paketu uzol overí či sa niektorý z jeho susedských uzlov nachádza bližšie k cieľovej oblasti ako je on sám a zvolí uzol ktorý je k oblasti najbližšie. Druhou fázou je šírenie paketov vo vnútri cieľovej oblasti. To môže prebiehať metódou záplavy obmedzenou na danú oblasť alebo pomocou rekurzívneho geografického preposielania. Pri rekurzívnom preposielaní je oblasť rozdelená na štyri podoblasti a do každej z nich je zaslaná kópia správy. Takýto spôsob sa nad každou zónou môže opakovať až do momentu kedy sa v oblasti nachádza len jeden uzol. [11, 12]

2.3.3 GOAFR

Princípom protokolu GOAFR (Greedy Other Adaptive Face Routing) je kombinácia tzv. hladového algoritmu a algoritmu OAFR (Other Adaptive Face Routing). Protokol využíva pre smerovanie ako prvý vždy hladový algoritmus. Tento protokol funguje dobre v sieťach s husto a rovnomerne rozloženými uzlami. Bežne takéto vlastnosti siete nie sú zaručené a tento prístup umožňuje nechcený stav kedy algoritmus uviazne v lokálnom minime. Vtedy prichádza na rad OAFR. Celý proces smerovania je zobrazený na nasledujúcom obrázku.



Obr. 2.10 Schéma smerovania protokolu GOAFR [15]

Smerovanie začína z uzlu Z a pomocou hladového smerovanie prechádza sieťou až k uzlu *n1* predstavujúci lokálne minimum. V takomto momente dochádza ku zmene smerovacieho režimu. Algoritmus začne prehľadávať hranice oblasti D až pokiaľ objaví uzol *n2* ktorý je najbližšie umiestneným uzlom k cieľovému uzlu C. Vtedy smerovanie prechádza znova do hladového režimu a dôjde k objaveniu cesty k cieľovému uzlu.

U tohto protokolu vznikajú viaceré nevýhody. Protokol negarantuje 100% úspešnosť doručenia dát a výrazne negatívnou je taktiež energetická cena využívania adaptívneho smerovania pre prekonanie prázdnej oblasti. [15]

3 Bezpečnosť mesh sietí

Požiadavky kladené na fungovanie BSS ako aj samotná podstata bezdrôtovej komunikácie vedú k viacerým zraniteľnostiam. Útoky využívajúce týchto bezpečnostných medzier by mohli ovplyvniť fungovanie jednotlivých uzlov, ale taktiež prevádzku celej siete. Mnohé protokoly predpokladajú pri komunikácii medzi uzlami s výlučne preddefinovaným správaním bez anomálii. Predpoklad korektného správania otvára priestor pre zraniteľnosti na viacerých vrstvách. Identifikácia a obrana proti útokom je základným predpokladom pre zabezpečenie spoľahlivých sieťových služieb. V tejto sekcii sú popísané konkrétne zraniteľnosti ako aj adekvátne obranné mechanizmy.

3.1 Zraniteľnosti na fyzickej vrstve

Úlohou fyzickej vrstvy je generovanie vysielaného signálu, voľba frekvencie, modulácie a detekcia prijímaného signálu. Útokom na túto najnižšiu komunikačnú vrstvu je tzv. Jamming. Cieľom Jammingu je rušenie rádiových frekvencii pomocou ktorých dochádza ku komunikácii. Výsledkom je teda úplné zamedzenie komunikácie alebo jej výrazné spomalenie. Takýto útok má často len lokálny charakter a preto sa útočníci snažia voliť najzraniteľnejšie uzly. V prípade existencie spojovacieho uzlu dvoch subsietí je takýto uzol ideálnym cieľom útoku, keďže jeho vyradením je sieť rozdelená do vzájomne nekomunikujúcich segmentov. [17]

3.2 Zraniteľnosti na linkovej vrstve

Na tejto vrstve je možné vykonávať viac typov útokov ako na fyzickej. Medzi tieto útoky patrí napríklad odpočúvanie, spoofing či cielená kolízia rámcov. Tieto a ďalšie sú opísané v nasledujúcich odrážkach.

3.2.1 Odpočúvanie

Ide o útok ktorý vychádza zo samotnej podstaty bezdrôtových sietí. Každé vysielanie je dostupné všetkým zariadeniam v dosahu a teda aj potencionálnym útočníkom. Tí sa snažia získavať informácie z po sieti prebiehajúcej komunikácie. Útočník sa musí fyzicky nachádzať v dosahu aspoň jedného komunikujúceho uzlu a uchovávať si prijímané a odosielané dáta. Pri tomto útoku nedochádza k priamemu ovplyvňovaniu alebo narúšaniu site. Nebezpečenstvo spočíva v získavaní informácii neoprávnenou osobou. Pre zabránenie takýmto útokom sa v sieťach využíva šifrovanej komunikácie. [17, 24]

3.2.2 Jamming

Naproti tomuto už spomínanému útoku na fyzickej vrstve pri ktorom dochádzalo k neustálemu vysielaniu náhodných hodnôt, v tomto prípade dochádza k vysielaniu cielených informácii. Ide o prázdne rámce iba s vyplnenou hlavičkou obsahujúcou cieľovú MAC adresu. Vďaka takémuto nepretržitému vysielaniu sa uzlom môže javiť komunikačný kanál ako zaneprázdnený a zariadenie často čakajú na jeho uvoľnenie. To vedie ku DoS (denial of service) a taktiež zvýšenej spotrebe energie cieľového zariadenia, ktoré sa snaží prijaté rámce spracovať. Vysielanie v tomto prípade nie je kontinuálne. Využitie tu nachádzajú sofistikované senzory na detekciu sémantiky protokolov vyšších vrstiev. Takto môže byť útok cielený a spúšťaný v momente identifikácie určitého typu komunikácie. [17]

3.2.3 Kolízia rámcov

Za kolíziu je považovaná situácia kedy sa súčasne a na rovnakej frekvencii pokúšajú vysielať dva uzly. V prípade kolízii dochádza ku vyrušenou rámcov a je nutné ich opätovné zaslanie. Útočník tak môže pri neustálom generovaní kolízii spôsobiť cielené vyčerpanie energetických zdrojov a to zvýšením prevádzky v prípade opakovaného vyžiadania a zaslania poškodených správ. Pri tomto útoku môže taktiež dochádzať ku ovplyvňovaniu šírky pásma prenosu. [17]

3.2.4 MAC Spoofing

MAC adresy boli dlho považované za unikátne sieťové identifikátory druhej vrstvy a na ich základe boli zariadeniam prideľované práva. Ako MAC spoofing je označovaná zámerná zmena zdrojovej MAC adresy útočníka. Táto technika umožňuje útočníkovi vyhnúť sa detekcii jeho prítomnosti v sieti. Ďalším z využití je získanie prístupu, ktorý je v sieti dostupný iba administrátorom povoleným zariadeniam na základe ich fyzickej adresy. [17]

3.3 Zraniteľnosti na sieťovej vrstve

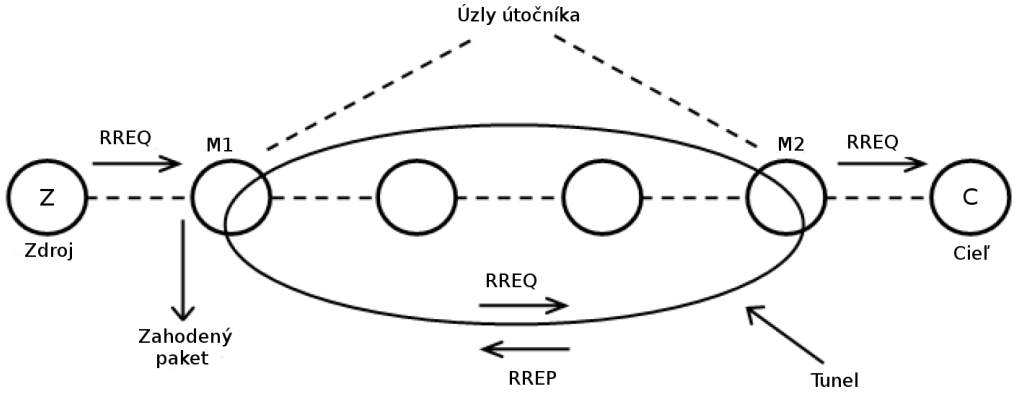
Útoky na tejto vrstve sa sústreďujú na kontrolné alebo na dátové pakety. Pri útoku na kontrolné pakety je zámerom znemožniť komunikáciu určitou trasou, alebo donútiť sieť používať inú trasu. Pri útoku na dátové pakety je snahou útočníka upraviť zasielané správy a vymeniť pôvodný obsah dáta útočníka.

3.3.1 Rushing

Tento útok napadá mechanizmus na objavovanie a voľbu komunikačnej cesty medzi uzlami. Príkladom protokolu napadnuteľného týmto útokom je protokol AODV. V protokole uzly pre nájdenie cesty využívajú tzv. RREQ (route reques) správu. Každý uzol ktorý prijal správu ju preposiela uzlom v okolí. Vzhľadom na predpoklad že rovnaká správa pri šírení môže na uzol doraziť naraz z viacerých zdrojov, je zavedená čakacia doba medzi prijatím a preposlaním prijatej správy. Výhodou zavedenia čakacej doby je minimalizácia redundancie správ, keďže aj po viacnásobnom prijatí správy dochádza k jej odoslaniu len raz. Nevýhodou prístupu je umožnenie úskočníkov ignorovať čakaciu dobu a zasielať správu skôr ako všetky ostatné uzly. Vďaka tomu si uzol útočníka zabezpečí jeho zvolenie za súčasť vytvorenej cesty medzi cieľom a zdrojom. Takýto uzol cez ktorý prechádza komunikácia je následne schopný ju kontrolovať, upravovať prijaté dáta alebo zasielané správy zahadzovať. [24]

3.3.2 Wormhole

Útok je veľmi podobný predchádzajúcemu. Využívajú sa minimálne dva útočiace uzly medzi ktorými je vytvorené vysokorýchlostné spojenie (tunel). Takto je prvou RREQ správou doručená práve tá, ktorá prešla tunelom medzi útočiacimi uzlami. Tiež sú tak podobne ako pri russhing útoku súčasťou komunikačnej cesty. [24]

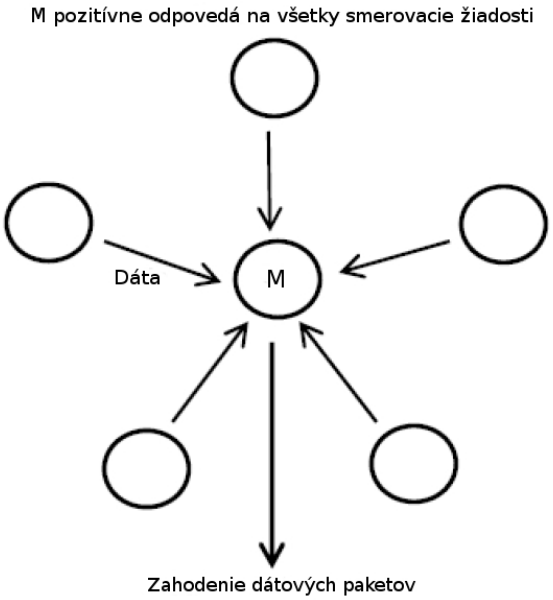


Obr. 3.1 Útok wormhole [17]

3.3.3 Blackhole

Útok blackhole je primárne zameraný na DoS. Škodiaci uzol pri tomto útoku vždy odosiela pozitívnu odpoveď na RREQ či už je alebo nie je súčasťou platnej cesty. Keďže tento uzol nečaká a nekontroluje či je naozaj súčasťou cesty bude jeho pozitívna odpoveď doručená ako prvá. Vďaka tomu takmer všetka komunikácia z okolitých zariadení bude smerovaná cez tento uzol. Všetka komunikácia prechádzajúca uzlom útočníka je

zhadzovaná a teda dochádza ku DoS. Modifikácia tohto útoku označovaná Grayhole, je náročnejšie detekovateľná. K vyhadzovaniu dochádza iba pri určitých správach a teda dochádza iba ku čiastočnému DoS [24]



Obr. 3.2 Útok blackhole [17]

3.3.4 Sibil

Ide o typ útoku kedy si uzol útočníka vytvára viacero identít v sieti pričom každá virtuálne reprezentuje samostatný uzol. Vďaka tomu môže v sieti dôjsť k narušeniu viacerých služieb spojených s preposielaním paketov, smerovaním a bezpečnostnými mechanizmami. Jednou zo základných výhod mesh sietí je schopnosť využívať pri komunikácii viacero uzlov a zabezpečiť väčšiu šírku pásma ako aj spoľahlivosť prenosu. Tieto schopnosti sú pri Sibil útoku značne ovplyvnené. Taktiež tu veľmi často dochádza ku komunikácii cez uzol útočníka, ktorý je následne schopný ju ovplyvňovať. [17]

3.3.5 Presmerovanie cesty

Útok sa zameriava na zmenu časti správ. Príkladom je pole správy udávajúce počet skokov. Útočiaci uzol v sieti jednoducho zmení tento počet na nulu, čím tvrdí zdrojovému uzlu že práve on je na najkratšej ceste k cieľovému uzlu a následná komunikácia bude prechádzať cez neho. V prípade že útočiaci uzol je v sieti nový a chce začať útok, je v mnohých protokoloch možné narušiť aktuálne smerovanie zaslaním chybovej správy, čím sa znova vyvolá inicializácia smerovania a znova dochádza ku hľadaniu cesty. To taktiež vedie ku energetickým stratám a zníženiu šírky prenosového pásma. [17]

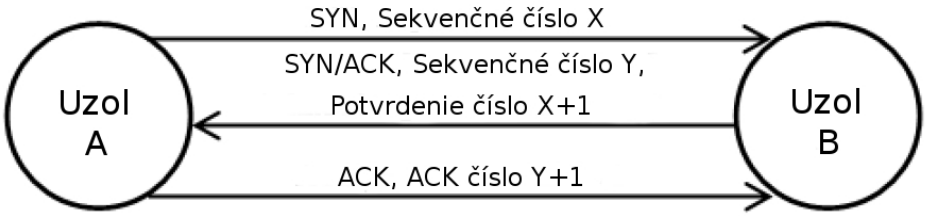
3.3.6 Útok na dátové pakety

V prípade útoku tohto typu dochádza ku modifikácii zasielaných dát vo vnútri paketu. Dáta môžu byť upravené a nahradené náhodným obsahom, aby cieľový uzol nedostal požadované informácie. Tento typ útoku je však veľmi ľahko detekovateľný a preto sa častejšie používa technika nazývaná paketová injektáž. V tomto prípade dochádza k preposlaniu dát užívateľovi avšak k vyžiadaným dátam sú pridané aj dáta útočníka. Príkladom môže byť dotaz na webstránku kde odpoveďou bude stránka s vloženým škodlivým skriptom ktorý sa na stránke reálne nevyskytuje. [19]

3.4 Zraniteľnosti na transportnej vrstve

3.4.1 SYN záplava

Tento typ útoku je veľmi jednoduché realizovať na protokole transportnej vrstvy ako je napríklad TCP. Ten pred začiatkom komunikácie potrebuje zistiť stav oboch komunikujúcich zariadení. Dochádza k tomu pomocou procesu výmeny troch správ nazývaného inicializačný handshake. Ako prvý je zaslaný paket SYN ktorého súčasťou je unikátne sekvenčné číslo. Spätne je z uzlu ktorý prijal správu odoslaná odpoveď SYN/ACK s rovnakým sekvenčným číslom. Na túto správu odpovedá uzol ktorý spojenie inicioval a to pomocou správy ACK. Útočník v tomto prípade opakuje zasielanie inicializačnej požiadavky bez zasielania odpovede. To na strane obete spôsobuje nechcené čerpanie zdrojov a postupné zaplnenie pamäte. Cieľový uzol si do momentu potvrdenia uchováva informáciu o uzle ktorý spojenie inicioval aj so zaslaným sekvenčným číslom. Vzhľadom na obmedzenú pamäť cieľového zariadenia sa po čase tabuľka s týmito informáciami zaplní. V takom prípade sú ostatné žiadosti o spojenie zo siete ignorované teda dochádza k DoS. [17]



Obr. 3.3 SYN inicializačný handshake [17]

3.4.2 Desynchronizácia

Desinchronizačný útok sa zameriava na narušenie existujúceho spojenia. Útočník môže opakovane zasielať cieľu klamlivé alebo porušené správy a tak ho donútiť vyžiadať ich opakované zaslanie. Pri správnom načasovaní takto môže útočník zabrániť výmene dát cieľovému uzlu a donúti ho míňať energiu pri spracovávaní umelo vytvorenej chyby komunikácie a následnom odosielaní žiadosti o korektné dáta. [17]

3.5 Zraniteľnosti aplikačnej vrstvy

Charakteristickým pre túto vrstvu je nutnosť útočníka mať znalosť a rozumieť aplikácií vykonávajúcej komunikáciu. Primárne sú tu útoky vykonávané pomocou vírusov, červov a škodlivého malware. Obzvlášť nebezpečným je tu samotné šírenie červov a vírusov po sieti, čím môže postupne dôjsť k infikovaniu všetkých uzlov. Bezpečnostné mechanizmy nižších vrstiev sú v tomto prípade neúčinné. Detekciu a obranu proti takýmto hrozbám je potrebné realizovať výlučne na aplikačnej vrstve. [17]

3.6 Bezpečnostné mechanizmy na fyzickej vrstve

Spomínanému útoku na fyzickej vrstve s názvom Jamming (3.1), ktorého cieľom je rušiť vysielanie a prijímanie signálu, možno predchádzať nasledujúcimi dvoma spôsobmi.

3.6.1 FHSS

Technika FHSS (Frequency Hopping Spread Spectrum) je mechanizmus pri ktorom dochádza ku rýchlemu prepínaniu frekvencie nosného signálu. Súčasne prebieha prepínanie na strane vysielajúceho uzlu ako aj pri detekcii na strane príjemcu. Je realizované na základe pseudo náhodnej postupnosti zmien známej obom uzlom. Pre útočníka je veľmi náročné zistiť práve používanú frekvenciu a vysielať na nej rušenie. Takýto mechanizmus je vhodný z dôvodu vyhnutia rušeniu od potencionálneho útočníka a taktiež akémukoľvek inému rušeniu z okolia. [17]

3.6.2 DSSS

Pri DSSS (Direct Sequence Spread Spectrum) dochádza ku rozšíreniu vysielacieho spektra a každý bit správy je reprezentovaný väčším počtom bitov pomocou prekódovania rozširujúcim kódom. Jednotlivé bity rozširujúceho kódu sú vysielané súčasne a to za pomoci adekvátne rozšíreného frekvenčného pásma. Príjemca následne použije rozširovací kód na dekódovanie a získanie pôvodných údajov. Pre ohrozenie prevádzky by prípadný útočník musel poznať zvolené rozšírené frekvenčné pásmo a taktiež používaný kód. [17]

3.7 Bezpečnostné mechanizmy linkovej vrstve

3.7.1 Obrana proti kolíziám

Bežnou obrannou stratégiou proti útoku zameranému na kolízie rámcov je používanie kódov schopných opravovania chýb. To si však vyžaduje pridanie spracovania kódov, čo zvyšuje energetické nároky na komunikáciu. Vďaka použitiu takýchto kódov je možné detegovať a opraviť prípadné vzniknuté chyby no v súčasnosti nie je známy spôsob ako útoku zameranému na kolízie predchádzať. [17]

3.7.2 Obrana proti vyčerpaniu energie

Obranou proti útoku zameranému na vyčerpanie energie je mechanizmus riadeného obmedzenie vstupov. Ten umožňuje v sieti ignorovať nadmerné požiadavky a šetriť tak zdroje. Ďalšiu efektívnou stratégiou je TDM (Time Division Multipelxing) pri ktorej je každému uzlu pridelený časový slot vysielania a ostatné vysielanie je ignorované. [17]

3.7.3 Obrana proti odpočúvaniu

Ide o spôsob obrany proti zachytávaniu a odpočúvaniu prevádzky v sieti. Jeho základom je vyžitie kryptografických techník na úpravu odosielaných dát. Útočník tak síce stále môže v sieti odpočúvať, avšak získané údaje bez dešifrovacieho kľúča sú preňho nečitateľne a ich vlastníctvom útočník nepredstavuje žiadnu hrozbu. [17]

3.8 Bezpečnostné mechanizmy sietovej vrstvy

Ako už bolo spomenuté s sekcii zraniteľností (3.3) na sietovej vrstve sú útoky delené podľa zamerania na proces voľby komunikačnej trasy alebo na doručovací proces dát. Proti týmto útokom je potrebná dostatočná obrana použitého protokolu. V nasledujúcej časti sú popísané vybrané komunikačné protokoly a ich bezpečnostné mechanizmy.

3.8.1 SRP

Bezpečnosť protokolu SRP (Secure Remote Password) je založená na používaní hesiel a výmene kľúčov. Hlavná stanica si uchováva verifikátor pre každý uzol a každý uzol si uchováva spoločné tajomstvo formou hesla. Kombinácia týchto dvoch údajov dovoľuje bezpečnú autentifikáciu uzlov. Vzájomná výmena uvedených údajov umožňuje bezpečnú šifrovanú komunikáciu. Útočník teda môže disponovať kompletnou znalosťou protokolu no bez znalosti špecifických informácii použitých na šifrovanie je obsah komunikácie pred ním chránený. [20]

3.8.2 ARAN

ARAN (Authenticated Routing for Ad-hoc Networks) využíva bezpečnostný prístup aplikovateľný na akýkoľvek smerovací protokol. Systém je postavený na využívaní digitálneho podpisu a to pri posielaní všetkých typov správ, vrátane správ o chybách. ARAN je takto schopný odhaliť prítomnosť neautorizovaného uzlu, detegovať zasielanie podozrivých správ a manipuláciu s ich obsahom. Protokol je náchylný na útoky brániace objaveniu cesty a útoky modifikujúce používané komunikačné cesty. [21]

3.8.3 SAODV

Protokol SAODV (Secure Ad hoc On-demand Distance Vector) reprezentuje modifikáciou protokolu AODV na ktorý boli aplikované bezpečnostné mechanizmy. Autenticita uzlov je zabezpečovaná vďaka hashovacím funkciám a algoritmu digitálneho podpisovania. SAODV využíva takzvané hashové zreťazenia a to pri overovaní počtu skokov uvedeného v zasielanej správe. Tak je možné na trase pri každom skoku zaručiť že počet skokov nebol znížený z dôvodu výskytu nového uzlu útočníka. Napriek využitiu asymetrickej kryptografie nedochádza oproti pôvodnému protokolu ku výraznému poklesu rýchlosti. Protokol je náchylný na útoky typu blackhole a wormhole. [21]

3.8.4 SODMRP

Protokol SODMRP (Stable On-Demand Multicast Routing Protocol) predstavuje odpoveď na nedostatky jeho predchodcu. Pôvodný protokol využíva pre stanovenie smerovacej cesty informácie o kvalite väzieb so susednými uzlami. Takýto prístup umožňoval uzlu útočníka zasielať umelo zvyšované ohodnotenie kvality jeho susedských vezieb, prípadne upravovať zachytené správy a umelo znižovať kvalitu ciest cez ostatné uzly. SODMRP bol vytvorený aby sa dokázal brániť voči týmto typom útokov. Každý uzol mesh siete má v tomto prípade verejný a súkromný kľúč zaisťujúci potrebnú autentifikáciu. Každý uzol taktiež vlastní certifikát zviazaný s v verejným kľúčom a jeho identitou. Každý paket je autentifikovaný, čim je zabezpečené, že nedôjde ku vloženiu žiadneho paketu z vonka. Súčasťou protokolu je detekčný mechanizmus založený na meraní prevádzky a výstražný obranný mechanizmus aktivovaný v prípade detekcie útoku. Stratégia detekcie útoku je založená na meraní pomeru predpokladanej a reálne zistenej prevádzky. V stratégii je implementovaná prahová hodnota, po ktorej prekročení, v prípade častejšej komunikácie ako bola predpokladaná, je aktivovaná výstraha. V prípade detekcie takéhoto správania, zaplaví uzol ktorý útok detegoval, sieť s upozorňujúcou správou s uvedením podozrivého a taktiež zdrojového uzlu správy. [17]

3.9 Bezpečnostné mechanizmy transportnej vrstvy

Najčastejšie používanými protokolmi pre zabezpečenie transportnej vrstvy, nie len v mesh sieťach, sú SSL (Secure Socket Layer), TLS (Transport Layer Security) a PCT (Private Communications Transport). Všetky sú postavené na využívaní asymetrickej kryptografie. TLS je považovaný za nástupcu SSL, navrhnutý aby poskytoval 3 základné služby v podobe šifrovania, umožnenia autentizácie a zabezpečenie integrity dát. Na vytvorenie bezpečného šifrovaného spojenia medzi účastníkmi je potrebné vykonať inicializačnú fázu. V tejto fáze dochádza k tzv. TLS handshaku. Ten predstavuje výmenu správ dohodnutým spôsobom. Pri nej sa účastníci dohodnú na type používanej šifry a dôjde ku výmene verejných kľúčov. Pomocou nich je následne umožnená bezpečná komunikácia. Pri výmene je na základe dostupných certifikátov možné vykonať autentifikáciu identity serveru klientom, ale taktiež klienta serverom. Integrita dát je overovaná pomocou podpisovania každej správy a zasielania vypočítaného výsledku hash funkcie. [17, 22]

3.10 Bezpečnostné mechanizmy aplikačnej vrstvy

Základnú obranu na úrovni aplikačnej vrstvy tvorí firewall. Ten poskytuje možnosti nastavenia povolení prístupu, autentizácie užívateľa, filtrovanie paketov, logovanie záznamov a ďalšie možnosti. Umožnená je taktiež detekcia a obrana proti niektorému malware a spyware. Nastavená konfigurácia povolení nazývaná prevádzková politika je statická. Nereaguje na novo zistené hrozby automaticky ale k jej zmene dochádza jedine zásahom užívateľa. Aplikačná vrstva obsahuje program schopný interagovať s užívateľom a podľa zvolených nastavení zasahovať do nižších vrstiev. [23]

Na detekciu viac sofistikovaných hrozieb slúžia systémy IDS(Intrusion Detection System), ktoré po firewalle predstavujú druhú líniu obrany. IDS sú pridaným komponentom sieťovej ochrany. Ich úlohou je kontrolovať zachytené pakety a správanie sieťových zariadení. Zameriavajú sa na detekciu paketov, ktoré nie sú vyžadované zariadeniami siete. Ako náhle je takáto udalosť detegovaná, bezpečnostný systém vyvolá adekvátnu reakciu pre ochranu systému. Najväčšie uplatnenie nachádza pri rýchlom odhaľovaní útočníka, ktorý tak po pripojení do siete nemá dostatok času vykonať útok. [24]

4 Štandardy

Tvorba a zavedenie štandardov je hlavným predpokladom umožnenia vzájomnej spolupráce. Z pohľadu BSS a internetu vecí je, pre umožnenie výmeny informácii medzi sieťovými zariadeniami, nevyhnutné využívanie spoločného komunikačného štandardu. Z pohľadu zariadení je podstatná možnosť vzájomne kombinovať rôzne druhy HW využívajúce rovnaký alebo kompatibilný štandard.

4.1 IEEE 802.15.4

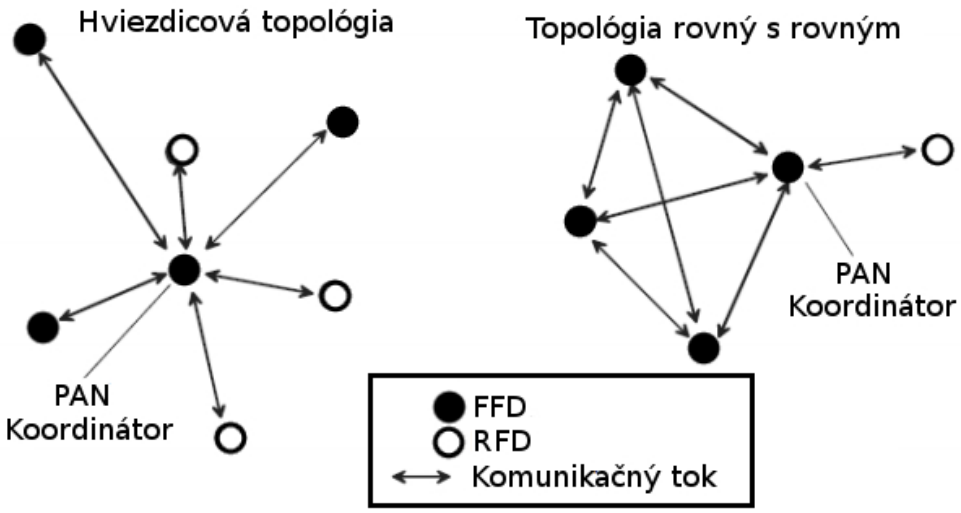
Nevýhodou často používaných štandardov IEEE 802.11(WiFi) a IEEE 802.15.1(Bluetooth) je na úkor dosiahnutia vyšších rýchlostí, podpora malého počtu prepojiteľných zariadení a vysoká spotreba energie. Akceptovateľnú alternatívu pre priemyselnú sféru tvorí štandard 802.15.4 vytvorený pre potreby požiadavkou bezdrôtových senzorických sietí. Cieľom bolo vytvorenie komunikačného štandardu zameraného na nízku spotrebu energie, dosahujúceho nízke prenosové rýchlosti, rádiové vysielanie na krátke vzdialenosti, prispôsobiteľný počet používaných zariadení, spoľahlivosť doručovania a výhody spojené s využívaním mesh sieťovej architektúry. Zámerom štandardu je jeho využiteľnosť na cenovo dostupných zriadeniach s nízkym výpočtovým výkonom a limitovaným zdrojom energie. Ideálna prenosová rýchlosť štandardu dosahuje 250 kb/s . [16]

Vybrané vlastnosti poskytované štandardom:

- Využívanie 64-bitovej rozšírenej adresy alebo skrátenej 16-bitovej adresy
- Voliteľná doba garantovaného časového slotu
- Vyhýbanie sa kolíziám pomocou CSMA-CA a ALOHOA prideľovania kanálov
- Potvrdzovanie prijatia správ pre spoľahlivosť komunikácie
- Nízka energetická náročnosť
- Detekcia zásoby energie
- Možnosť hodnotiť kvalitu spojenia

4.1.1 Podporované topológie

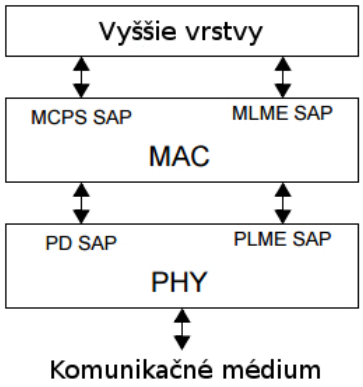
V závislosti na vyžadovanej aplikácii štandard dokáže prevádzkovať hviezdicovú topológiu alebo topológiiu rovný s rovným. V hviezdicovej topológii komunikácia nastáva medzi zariadeniami a centrálnym zariadením nazývaným PAN koordinátor. Zariadenia môžu využívať celú adresu alebo skrátenú adresu ktorá bola uzlu priradená koordinátorom. Topológia rovný s rovným taktiež využíva PAN koordinátora avšak odlišuje sa od hviezdicovej vďaka umožneniu všetkým zariadeniam komunikovať s ostatnými v dosahu. To umožňuje tvorbu mesh sieťových štruktúr. Štandard v topológii rozlišuje dva typy zariadení. Ak je zariadenie schopné vykonávať funkciu lokálneho koordinátora alebo koordinátora celej siete je označované ako FFD (Full-Function Device). Zariadenie bez tejto funkcie je označované ako RFD (Reduced-Function Device) [16]



Obr. 4.1 Topológie štandardu IEEE 802.15.4 [16]

4.1.2 Architektúra

Architektúra štandardu pozostáva z dvoch sieťových vrstiev. Každá z týchto vrstiev je zodpovedná za časť fungovania štandardu a pomocou pre každú vrstvu špecifických rozhraní, poskytuje svoje služby vyšším vrstvám. Týmito vrstvami sú fyzická (PHY) vrstva a media access control (MAC) vrstva. Definície vyšších vrstiev sú mimo rozsah tohto štandardu. [16]



Obr. 4.2 Vrstvy architektúry [16]

4.1.3 PHY vrstva

Obecne fyzická vrstva priamo pracuje s používaným komunikačným médiom. Vrstva poskytuje rozhranie medzi MAC vrstvou a fyzickým HW. V tomto štandarde vrstva priamo zodpovedá za nasledujúce funkcie:

- Aktiváciu a deaktiváciu rádiového vysielača
- Detekciu energie na aktuálnom kanále
- Indikovanie kvality spojenia
- Voľba frekvencie kanálu
- Odosielanie a prijímanie dát

4.1.4 MAC Vrstva

Primárnymi funkciami MAC vrstvy je overovanie platnosti rámcov, potvrdzovanie doručenia a správa beacon rámcov. Štandard definuje nasledujúce štruktúry:

- **beacon rámec** - využívaný koordinátorom na šírenie informácii o sieti
- **dátový rámec** - pre všetky prenášané dáta
- **potvrdzovací rámec** - použití na potvrdenie úspešného prijatia dát
- **príkazový rámec** - zasielanie žiadostí a upozornení

Štandard IEEE 802.15.4 zavádza viaceré postupy a mechanizmy pre zvýšenie pravdepodobnosti úspešného prenosu dát. Týmito mechanizmami sú:

CSMA-CA - Pre zníženie počtu kolízií je využívaný mechanizmus pre riadenie prístupu na komunikačný kanál. Sú používané dve verzie podľa toho či sú v sieti využívané beacon rámce. Ak nie sú využívané, každý uzol čaká náhodnú dobu a pred vysielaním overí či je komunikačný kanál volný. Ak nie je, znova čaká náhodnú dobu. Pri využívaní beacon rámcov dochádza k úprave čakacej doby tak, aby nekolidovala s opakujúcim sa zasielaním týchto rámcov.

ALOHA mechanizmus - Zariadenia vysielajú bez zisťovania stavu kanálu alebo čakania na konkrétne časové obdobie. Ochranou pred kolíziami je výlučne náhodná čakacia doba pred vysielaním. Takýto prístup je vhodný použiť v prípadoch kedy je v sieti predpokladaná malá prevádzka s malou pravdepodobnosťou výskytu rušenia v komunikačnom kanále.

Potvrdzovanie paketov - Úspešné prijímanie a validácia dát je oznamovaná zaslaným potvrdením. Ak po určitom čase nedôjde ku prijatiu potvrdenia, zdroj predpokladá že doručenie zlyhalo a zasiela rámce znova. Ak nie je potvrdenie vyžadované, po odoslaní sa automaticky predpokladá úspešné prijatie správ.

Verifikácia dát - Pri prenose môže nastať poškodenie zasielanej správy. Na detekciu chýb vyskytujúcich sa v rámcoch je zavádzaný overovací mechanizmus CRC. [16]

4.1.5 Bezpečnosť

Štandard z dôvodu bezpečnosti zavádza kryptografické mechanizmy založené na symetrickej kryptografii. Využívajú kľúč poskytnutý z procesov vyšších vrstiev. Údržba kľúčov je mimo rámec tohoto štandardu. Typy ochrany poskytované kryptografickými mechanizmami sú nasledovné:

- **Utajenie informácii** - zaručenie že prenášané informácie budú schopné prečítať výlučne zvolený príjemcovia.
- **Autenticita dát** - možnosť detektovať modifikácie zasielaných dát.
- **Ochrana preposielania** - zaručenie detekcie duplikovaných informácii. [16]

4.2 ZigBee

Štandard Zigbee predstavuje najčastejšie zavádzané riešenie v oblasti BSS a IoT. Zigbee bol postavený na štandarde IEEE 802.15.4 a využíva špecifikácie jeho vrstiev. Nad týmito vrstvami sám definuje vyššie vrstvy a v nich používané protokoly. Rovnako ako 802.15.4 je ZigBee štandardom pre energeticky nenáročné WPAN siete využívajúce nízke prenosové rýchlosti. Okrem bezlicenčného pásma 2,4 GHz je ZigBee prevádzkovateľné na rôznych ďalších frekvenciách, podľa povolení danej krajiny. Rovnako ako u štandardu IEEE 802.15.4 je maximálna prenosová rýchlosť 250 kb/s. [25, 26]

Zigbee prináša vylepšenie v podobe zavedeného šifrovania, autentifikácie platných sieťových uzlov a smerovacích schopností umožňujúcich využívať mesh sieťovú topológiu. Za vytvorením štandardu ZigBee stojí organizácia nazývaná ZigBee aliancia. Táto organizácia predstavuje spoločenstvo firiem, vyvíjajúcich štandardy pre bezdrôtovú komunikáciu s cieľom umožniť vzájomnú spoluprácu medzi rôznymi zariadeniami.[25]

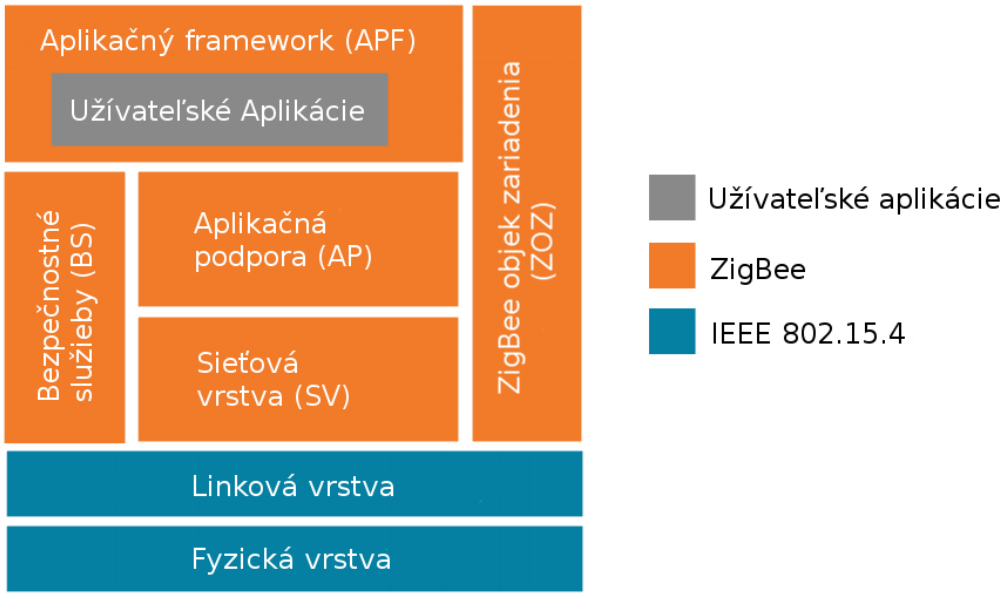
4.2.1 Charakteristiky

ZigBee je rozšíreným štandardom primárne v priemyselnej sfére. Dôvodom sú jeho mnohé charakteristické vlastnosti, vhodné pre priemyselné aplikácie. Ide o nasledujúce charakteristiky:

- Využívanie mesh sieťovej topológie
- Umožňuje v rámci jednej siete využívať 65 000 zariadení.
- Navrhnutý na prepojenie rôznych druhov zariadení do jednej siete.
- Umožňuje využívať bezlicenčné pásmo 2,4 GHz.
- Umožňuje využívať pásmo 915MHz (pre Ameriku) a pásme 868MHz (pre Európu)
- Definuje viacero voliteľných vysielacích možností
- Využíva šifrovanie AES-128 s bezpečným mechanizmom generovanie kľúčov.
- Podpora alianciou zavedených štandardov[25]

4.2.2 Architektúra

Štandard ZigBee využíva PHY a MAC vrstvu štandardu IEEE 802.15.4, ktorých funkcie boli uvedené v sekciách 4.1.3 a 4.1.4. Nad nimi definuje špecifikácie sieťovej a aplikačnej vrstvy, poskytuje framework pre tvorbu aplikácii a definuje služby pre zabezpečenie. Nasledujúci obrázok zobrazuje zjednodušenú schému architektúry. [25]



Obr. 4.3 ZigBee architektúra [26]

SV - Sieťová vrstva špecifikovaná štandardom ZigBee predstavuje rozhranie medzi aplikačnou a MAC vrstvou. Úlohou tejto vrstvy je formovanie sieťovej štruktúry a smerovanie zasielaných správ. Vrstva je primárne využívaná sieťovým koordinátorom pre pripájanie či odpájanie zariadení a pre priraďovanie adries novým uzlom. Podporovanými topológiami sú hviezdicová, stromová a meshová. Sieťová vrstva určuje správanie siete a u zariadení s obmedzenou zásobou energie, má zásadný vplyv na predlžovanie ich životnosti. [25, 26]

AP - Predstavuje podpornú aplikačnú vrstvu implementujúcu funkcie potrebné pre ZigBee aplikácie. AP reprezentuje rozhranie ku sieťovej vrstve. Vykonáva filtrovanie duplicitných paketov prijatých od sieťovej vrstvy a udržiava tabuľku uzlov v sieti. [26]

BS - poskytuje zabezpečovacie metódy pre sieťovú a aplikačnú vrstvu, vrátane postupov pre stanovenie šifrovacích kľúčov, prenos kľúčov a samotnú ochranu správ. [25]

ZOZ - je zodpovedný za celkovú správu ZigBee zariadenia. ZOZ inicializuje AP a SV, umožnuje objavenie zariadenia, spracováva požiadavky a definuje režim zariadenia (koordinátor, smerovač alebo koncové zariadenie). [26]

APF - predstavuje behové prostredie pre užívateľské aplikácie a zjednodušuje pre ne zasielanie a prijímanie dát. Táto funkcia je poskytovaná za pomoci tzv. *endpoint* hodnôt priraďovaných každej aplikácii. Hodnota 0 je rezervované pre ZOZ a číslo 255 pre zaslanie všetkým aplikáciám (broadcast). Vytvorené užívateľské aplikácie špecifikujú konkrétnu požadovanú činnosť zariadenia. [25, 26]

4.2.3 Typy zariadení

Štandard definuje zariadeniam presný spôsob ich sieťového správania. Rozdelenie a činnosti zariadení sú relevantné z pohľadu sieťovej topológie, smerovania a preposielania správ. Nezávisle na zvolenom type zariadenia môže každé vykonávať senzorickú činnosť. Podporované typy zariadení sú nasledovné:

- **Koordinátor** - Súčasťou každej siete musí byť minimálne jeden koordinátor. Tento uzol vykonáva inicializáciu siete, vyberá používanú frekvenciu a povoľuje pripojenie sa do siete novým uzlom. Uzol môže vykonávať smerovanie a často sú na ňom spustené bezpečnostné služby.
- **Smerovač** - Zariadenia typu smerovač nie sú nevyhnutne vyžadované vo všetkých topológiách ZigBee no často sú ich súčasťou. Smerovače sú zodpovedné za odovzdávanie správ ostatným uzlom. Uzly sa môžu pripájať do siete skrz smerovač, ktorý sa tak stáva ich rodičovským uzlom
- **Koncové zariadenie** - Úlohou koncového zariadenia je odosielanie vlastných správ a prijímanie správ zo siete. Zariadenia nevykonávajú žiadnu inú sieťovú činnosť. Sú jedinými zariadeniami ktoré môžu byť uspané. Rodičovský uzol v takej situácii zhromažďuje správy dokiaľ nedôjde ku prebudeniu uzlu.[26]

4.2.4 Adresovanie zariadení

Každé zariadenie v ZigBee sieti je identifikované dvoma adresami, MAC adresou špecifikovanou štandardom IEEE 802.15.4 a sieťovou adresou (NwkAddr) špecifikovanou štandardom ZigBee.

MAC adresa - je bežnou 64-bitovou, výrobcom zariadenia udanou, adresou ktorej hodnota by mala byť unikátna. V štandardne ZigBee je priame používanie tohto druhu adries veľmi zriedkavé. Využíva sa pri mapovaní a priraďovaní ku sieťovej adrese.

Sieťová adresa - označovaná ako *NwkAddr*, je skrátená 16-bitová adresa ktorá je unikátnou vrámci aktuálnej siete. Adresa je zariadeniu priradená v momente jeho pripojenia do siete. Podľa aktuálneho nastavenia môže byť prideľovanie adries vykonávané vzhľadom na pozíciu uzlu v topológii, alebo čisto náhodne. Adresa koordinátora je vždy 0x0000. [26]

4.2.5 Šírenie správ

V štandarde je podporovaných viacero spôsobov, ako špecifikovať adresáta správy. Adresátom môže byť jeden uzol, skupina uzlov prípadne všetky uzly siete.

Broadcast - je správou zasielanou všetkým uzlom siete. Ak je takáto správa zachytená koordinátorom alebo smerovačom je ďalej zaslaná všetkým uzlom v dosahu. V prípade tejto správy nie je vyžadované zasielanie potvrdenia o jej prijatí. Broadcast správa vzniká nastavením špecifickej hodnoty do atribútu adresáta správy. Tieto hodnoty môžu byť nasledovné:

- **0xFFFF** - vyslanie všetkým uzlom.
- **0xFFFD** - vyslanie uzlom s neustále aktívnym prijímačom.
- **0xFFFC** - vyslanie smerovačom a koordinátorom
- **0xFFFB** - vyslanie smerovačom s nízkou spotrebou

Multicast - definuje správu určenú skupine uzlov. Správa je zasielaná s adresou danej skupiny a vysielanie prebieha podobne ako pri broadcast správe. Rozdielom je, že každý uzol pred spracovaním správy overí či je súčasťou zvolenej skupiny.

Unicast - správy sú určené jednému uzlu. Pre doručenie je potrebné objaviť cestu k cieľu a až po zaslaní potvrdzovacej správy o objavení, dochádza k odoslaniu dát a ich postupnému smerovaniu k cieľovému uzlu. [26]

4.2.6 Šifrovanie

Pre zabezpečenie dát môže byť šifrovanie vykonané na úrovni troch vrstiev: MAC, sieťovej a podpornej aplikačnej. Vysielaný rámec v takomto prípade obsahuje zašifrované polia z každej vrstvy ktoré sú do seba postupne zapúzdrované. Šifrovanie je na všetkých vrstvách vykonávané algoritmom AES-128. Algoritmus využíva symetrickú kryptografiu, čoho dôsledkom je že každý uzol musí vlastniť potrebný kľúč. Spôsoby získavania kľúča sú nasledovné:

- **Preddefinovaním** - kľúč je priamo uložený v zariadení.
- **Prenosom** - kľúč je zaslaný sieťou po aktivácii zariadenia.
- **Vyjednávaním** - zasielaním vyjednávacích správ a stanovením kľúča bez jeho reálneho zasielania sieťou. [26]

4.3 6LowPAN

6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks) predstavuje otvorený štandard vytvorený organizáciou IETF. Hlavným prínosom štandardu je jeho schopnosť prepájať novšie a staršie webové služby, pričom umožnuje ich prepojenie so sférou IoT a BSS. Cieľom štandardu je adaptácia IPv6 paketov pre zefektívnenie prenos pomocou rámcov linkovej vrstvy definovaných IEEE 802.15.4 štandardom. [27, 28]

4.3.1 Charakteristiky

6LoWPAN umožnuje využívať výhody spojené s používaním IP protokolov a všetkým sieťovým zariadeniam umožňuje vykonávať ich auto-konfiguráciu. Je zameraný na použitie v sieťových riešeniach, v ktorých je zásadnou požiadavkou nízka spotreba energie. Znižovanie spotreby umožňuje štandardu minimalizácia objemu zasielaných dát. V sieti 6LoWPAN je možné využívať zasielanie unicast, multicast a broadcast. Podporovanou funkcionalitou je taktiež fragmentácia zasielaných dát. Štandard podporuje využívanie 64-bitového a skráteného 16-bitového adresovania. [28]

4.3.2 Typy zariadení

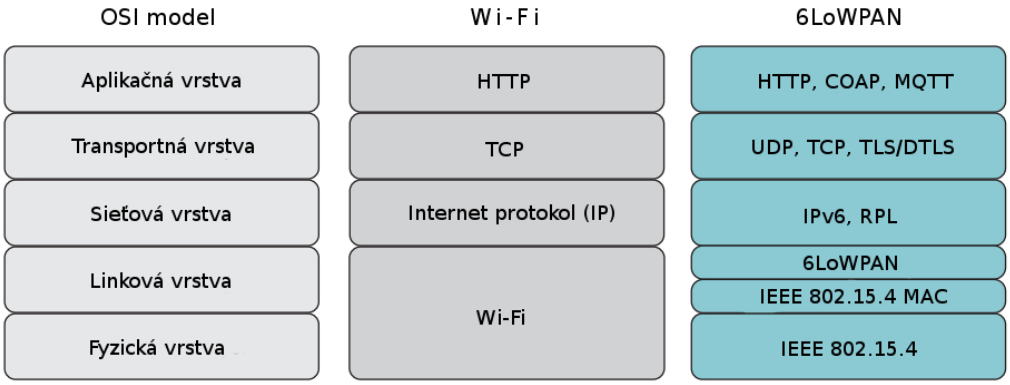
Podobne ako v štandarde ZigBee (4.2.3) sa v sieti nachádzajú koncové zariadenia a smerovače plniace rovnaké úlohy. Tretím typom zariadenia vyskytujúci sa v 6LoWPAN sieti je tzv. hraničný smerovač, ktorého úlohy sú nasledovné:

- Výmena dát medzi 6LoWPAN zariadeniami a Internetom.
- Lokálna výmena dát medzi zariadeniami 6LoWPAN siete.
- Vytváranie a udržovanie podsiete. [27]

Technológie ako ZigBee, Z-wave alebo Bluetooth na prepojeniie s IP sieťami musia v sieťových bránach implementovať špecifické aplikačné brány. Vďaka využívaniu IPv6 nie je v 6LoWPAN sieťach takáto aplikačná nadstavba potrebná. Vnútorné uzly sú priamo adaptovateľné aj z prostredia mimo 6LoWPAN siete. [27]

4.3.3 Architektúra

Z pohľadu architektúry predstavuje 6LoWPAN zavedenie adaptačnej vrstvy, medzi vrstvy linkovú a sieťovú. Zámerom vykonávanej adaptácie je umožnenie efektívneho prenosu IPv6 datagramov, pomocou rámcov štandardu IEEE 802.15.4. Nasledujúci obrázok obsahuje model architektúry so zavedenou 6LoWPAN vrstvou a jeho porovnanie s OSI a WiFi modelom. [27]

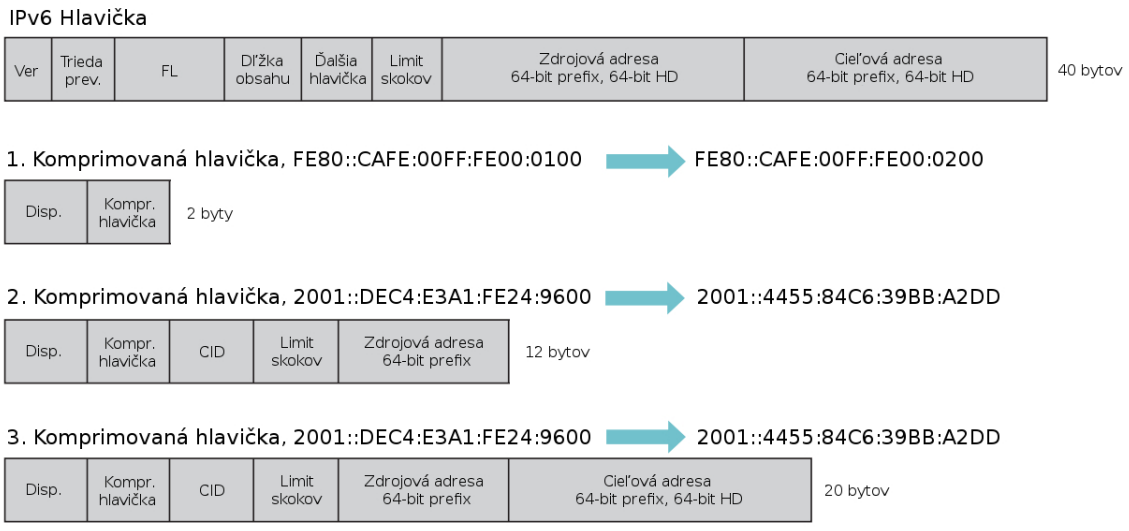


Obr. 4.4 Protokolový balík 6LoWPAN [27]

Maximálna definovaná veľkosť IPv6 paketu predstavuje 1280 bytov. Takúto správu musí byť možné zasielať pomocou 127 bytového rámca definovaného štandardom 802.15.4. Riešením tejto požiadavky je zavedená adaptačná vrstva ktorá vykonáva fragmentáciu správ a pre zvýšenie efektívnosti taktiež kompresiu IPv6 a UDP hlavičiek. [27]

4.3.4 Kompresia

Pre dynamicky sa meniace siete s veľkým počtom skokov a zriedkavým vysielaním akými sú 6LoWPAN siete, je nutné aplikovať tzv. bezstavovú metódu kompresie. 6LoWPAN využíva pri kompresii metódu zdieľaného obsahu. Táto metóda je postavená na predpoklade opakujúcich sa informácii pridávaných k správe na rôznych vrstvách. Jednotlivé polia hlavičiek sú ignorované ak môžu byť získané z inej vrstvy. Takáto kompresia je aplikovaná na 40-bytové IPv6 a 8-Bytové UDP hlavičky. [27, 28]



Obr. 4.5 Kompresia IPv6 hlavičky [27]

Na obrázku 4.5 sú zobrazené 3 komunikačné scenáre a k nim adekvátna úprava hlavičky.

1. Komunikácia medzi dvoma zariadeniami v rámci 6LowPAN siete za pomoci tzv. link-locak adries. Veľkosť hlavičky môže byť zredukovaná až na 2 byty.
2. Komunikácia zacielená na zariadenia mimo siete 6LoWPAN so známym prefixom externej siete. Veľkosť hlavičky dosahuje 12 bytov
3. Komunikácia so zariadením mimo siete bez známeho prefixu. Veľkosť IPv6 hlavičky 20 bytov. Aj tento najhorší možný výsledok dosahuje o 50% menší objem ako štandardná hlavička IPv6 správy.[27]

4.3.5 Fragmentácia

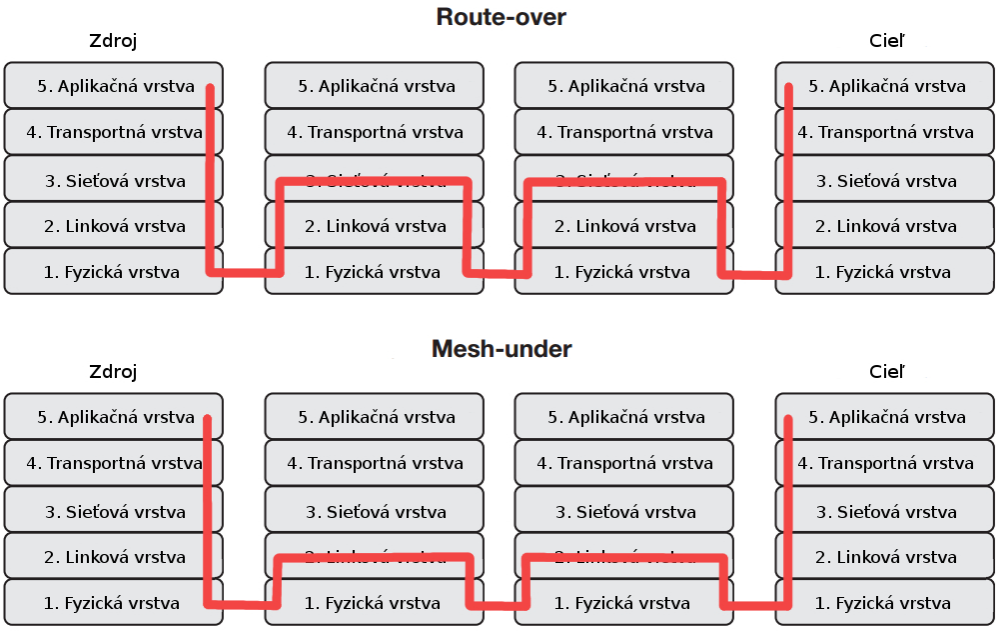
Pre prenos IPv6 správ pomocou rámcov štandardu 802.15.4, musia byť IPv6 pakety rozdelené na niekoľko menších segmentov. Za týmto účelom sú do hlavičiek pridávané informácie nutné pre správne poskladanie a zoradenie všetkých zasielaných paketov do pôvodného poradia. V momente zostavenia dochádza k odstráneniu pridaných dát a nastáva obnovenie pôvodnej IPv6 správy. Spôsob fragmentácie sa líši podľa použitého spôsobu smerovania. Využívaný spôsob smerovania určuje či bude dochádzať ku zostaveniu na každom uzle trasy alebo až na cieľovom uzle. [27]

4.3.6 Smerovanie

Vzhľadom na to na akej vrstve prebiehajú smerovacie mechanizmy, je smerovanie delené do dvoch kategórii:

Mesh-under - je prvým typom možného smerovania. Pre preposielanie správ sú v využívané adresy linkovej vrstvy. Smerovanie prebieha veľmi jednoducho keďže zasielané správy sú doručované všetkým uzlom v sieti. Tento typ smerovania spôsobuje veľké zaťaženie zariadení a z toho dôvodu nie je vhodné ho používať v rozsiahlych sietiach.

Route-over - je označenie druhého typu smerovania. Route-over je prístupom využívajúcim IP adresy sieťovej vrstvy, čo je vhodným riešením pre rozsiahlejšie siete. Najrozšírenejšie používaným smerovacím protokolom 6LoWPAN sietí je protokol RPL za ktorým taktiež stojí organizácia IETF. Protokol bol vyvinutý pre smerovanie v energeticky nenáročných sieťach. Poskytuje mechanizmy pre smerovanie a komunikáciu typu "jeden jednému", "jeden mnohým"a "mnohý jednému"čo je obzvlášť často využívaný princíp v BSS. [27]



Obr. 4.6 Smerovacie prístupy [27]

RPL podporuje dva odlišné smerovacie režimy: ukladací a ne ukladací. V ukladacom režime si všetky smerovače udržujú smerovacie a preposielacie tabuľky. V neukladacom režime je jediným zariadením využívajúcim smerovacie tabuľky hraničný uzol. V tomto prípade dochádza ku tzv. zdrojovému smerovaniu. Pri komunikácií medzi dvoma zariadeniami sú dáta najskôr zasielané hraničnému uzlu. Ten podľa informácii zo smerovacej tabuľky, pripojí k správe celú cestu k požadovanému cieľu a vyšle ho do siete. Ukladací spôsob je náročnejší pre smerovače ktoré si musia udržiavať smerovacie informácie. Neukladací režim zapríčiňuje doručovanie správ po dlhších trasách a zvyšuje zaťaženie hraničného uzlu. [27]

4.3.7 Auto-konfigurácia

Schopnosť Autokonfigurácie umožňuje zariadeniam samostatné generovanie IPv6 adries bez interakcie s DHCP serverom Za týmto účelom sú využívané 4 typy správ označované ako RS (Router Solicitation), RA (Router Advertisement), NS (Neighbor solicitation) a NA (Neighbor Advertisement).

Pokiaľ sa uzol chce stať súčasťou 6LoWPAN siete priradí si sám link-lokal adresu (FE80::IID) a vyšle túto informáciu do siete pomocou NS správy. Tak sa snaží zistiť či je zvolené adresa voľná. Uzol čaká na správu typu NA ktorú vysiela iný uzol vlastniaci zvolenú adresu z NS správy. Pokiaľ po uplynutí stanovenej doby takáto správa nedorazí, uzol považuje zvolenú adresu za unikátnu. Následne koncový uzol zasiela smerovaču správu RS, pre získanie korektného sieťového prefixu. [27]

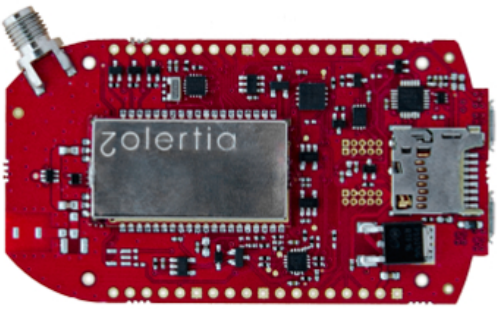
II. PRAKTICKÁ ČASŤ

5 Hardware

Pre testovanie funkcii senzorickej siete v reálnom prostredí bolo potrebné využiť viacerých zariadení umožňujúcich bezdrôtovú komunikáciu. Práca bola realizovaná z pomoci dvoch HW platforiem ktorými boli Zolertia RE-Mote a TI CC2538DK.

5.1 RE-Mote

Zariadenie RE-Mote je vývojovou platformou navrhnutou v rámci európskeho výskumného projektu RERUM (REliable, Resilient and secUre IoT for sMart city applications). Cieľom unverzít a priemyslených spoločnosťí ktoré sa na vývoji platformy podielali bolo vytvorenie zariadenia s extrémne nízkou spotrebou vhodného pre nasadenie do priemyslenej oblasti. [29]



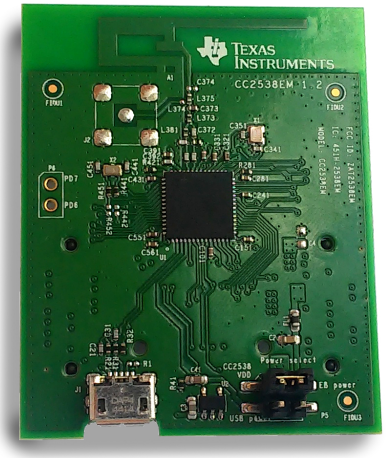
Obr. 5.1 Platforma RE-Mote [29]

RE-Mote využíva SoC (System on Chip) spoločnosti Texas Instruments označovaný názvom CC2538 ARM Cortex-M3 prevádzkovaný na frekvencii 32 MHz disponujúci 512 KB flash pamäte a 32 KB pamäte RAM. Tento systém umožnuje využívanie viacerých otvorených operačných systémov určených pre embedded zariadenia. Aktuálne podporovanými operačnými systémami sú Contiki, RIOT a Openthread. Súčasťou zariadenia sú dva vysielače umožňujúce komunikáciu na bezlicenčnej frekvencii 2,4 GHz a pre veľké vzdialenosti voliteľne 868 alebo 915 MHz. Vysielače umožňujú kompatibilitu s protokolmi Thread alebo SIGFOX a so štandardmi IEEE 802.15.4 a 6LoWPAN.

Platforma disponuje podporou pre rôzne bezpečnostné algoritmy. Podporovanými sú SHA2, AES-128/256, ECC-128/256 a RSA často využívané pre zabezpečenie komunikácie. Po HW stránke je platforma vybavená slotom pre pamätovú kartu, dvoma rozhraniami mikro USB, dvoma riadiacimi tlačidlami a konektorom RP-SMA pre pripojenie antény. [29]

5.2 CC2538EM

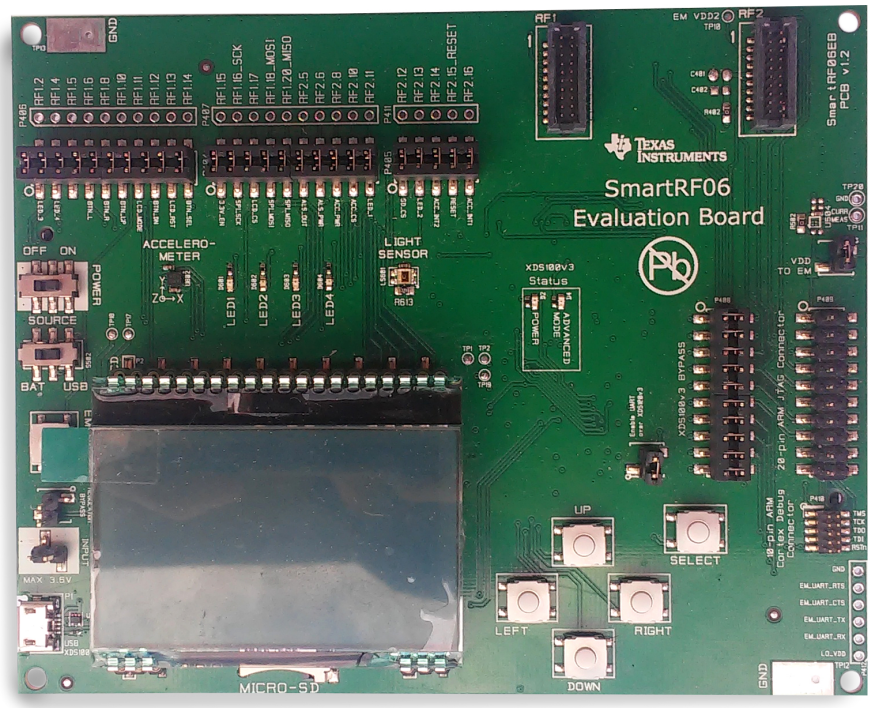
Druhou platformou využívanou v tejto práci bola CC2538EM od spoločnosti Texas Instruments. Tento modul je rovnako ako v prípade RE-Mote vybavený systémom CC2538 avšak disponuje iba jedným vysielačom a integrovanou anténou umožňujúcou komunikáciu výlučne pomocou frekvencie 2,4 GHz. Modul disponuje mikro USB konektorom a dvoma 20-pinovými konektormi pre pripojenie k vývojovej doske.



Obr. 5.2 Platforma CC2538EM

Vývojová doska SmartRF06EB je tretím typom využívaného zariadenia. Pomocou tejto dosky je možné programovať moduly CC2538EM s ktorými je prepojená spomínanou dvojice konektorov. Podstatný komponentom dosky je XDS100v3 umožňujúci nahrávanie a ladenie programov. Vývojová doska po pripojení modulu umožnuje využívať vlastné komponenty a periférie. Súčasťou vývojovej dosky sú:

- LCD panel (128 x 64 px)
- Snímač okolitého svetla SFH5711
- Akcelerometer BMA250
- Slot na MicroSD karty
- LED diody 4x
- Užívateľské tlačidlá 5x
- Sloty na AA batérie 1,5V 2x



Obr. 5.3 Vývojová doska SmartRF06EB

V porovnaní s platformou RE-Mote nastáva rozdiel v spôsobe programovania zariadení. Na nové nahrávanie programu nie je potrebné zariadenia RE-Mote vopred pripravovať. V prípade CC2538EM je vopred nutné manuálne prepnúť zariadenie do programovacieho režimu. Doska umožnuje vykonanie zmeny režimu pomocou kombinácie stlačenia tlačidiel *SELECT* a *RESET*.

Pre umožnenie práce so SmartRF06EB bolo do jadra linxového OS používaného pre kompiláciu a prácu s OS Contiki, nutné manuálne pridať modul potrebný pre prácu s XDS100v3. To bolo vykonávané pomocou nasledujúcich príkazov.

```
modprobe ftdi_sio
echo 0403 a6d1 > /sys/bus/usb-serial/drivers/ftdi_sio/new_id
```

Pri práci boli využívané všetky uvedené platformy a zariadenia. Dostupné boli v nasledujúcich množstvách.

Tab. 5.1 Použité zariadenia

Platforma	**Počet**
RE-Mote	2
CC2538EM	4
SmartRF06EB	1

6 Software

Pre umožnenie bezdrôtovej komunikácie medzi zariadeniami a docielenie požadovaného sieťového správania, bolo nutné zvoliť adekvátny komunikačný protokol. Vzhľadom na využívanie rôznych HW platforiem bolo taktiež výhodné zjednotiť ich spoločnú prácu pomocou využívania jednotného SW, aplikovateľného na každú z nich. Oba tieto ciele umožnil dohromady skombinovať zvolený operačný systém Contik.

OS Contiki je otvorený systém zameraný na využitie v oblasti IoT a aplikovateľný na výkonovo nenáročné zariadenia s obmedzenou zásobou energie. Okrem plnej podpory štandardou IPv4 a IPv6, Contiki umožnuje využívanie moderných protokolov zameraných na oblasť IoT. Vďaka podpore štandardov 6LoWPAN, RPL a CoAP, ako aj množstvu podporovaných zariadení, je systém vo veľkej miere využívaný v mnohých oblastiach. [7]

Systém Contiki, napísaný v jazku C, disponuje modulárnou architektúrou a jadrom využívajúcim správu udalostí. Disponuje plánovačom udalostí ktorého úlohou je vyvolávať spustenie procesov. Vyvolanie procesu v Contiki je vykonané ako odozva na zaslanú udalosť. Udalosti umožňujú taktiež medziprocesovú komunikáciu. Procesy v systéme pozostávajú z kontrolného bloku procesu a vlákna procesu. Kontrolný blok obsahuje behové informácie o procese a vlákno procesu obsahuje vykonávaný kód. Vlákna sú implementované formou tzv. protovlákien, ktoré v jazyku C umožňujú funkciám fungovať podobne ako vlákna avšak bez zvyšovania pamäťovej náročnosti ktoré sú s nimi bežne spojené. [31]

Tab. 6.1 Adresárová štruktúra OS Contiki [7]

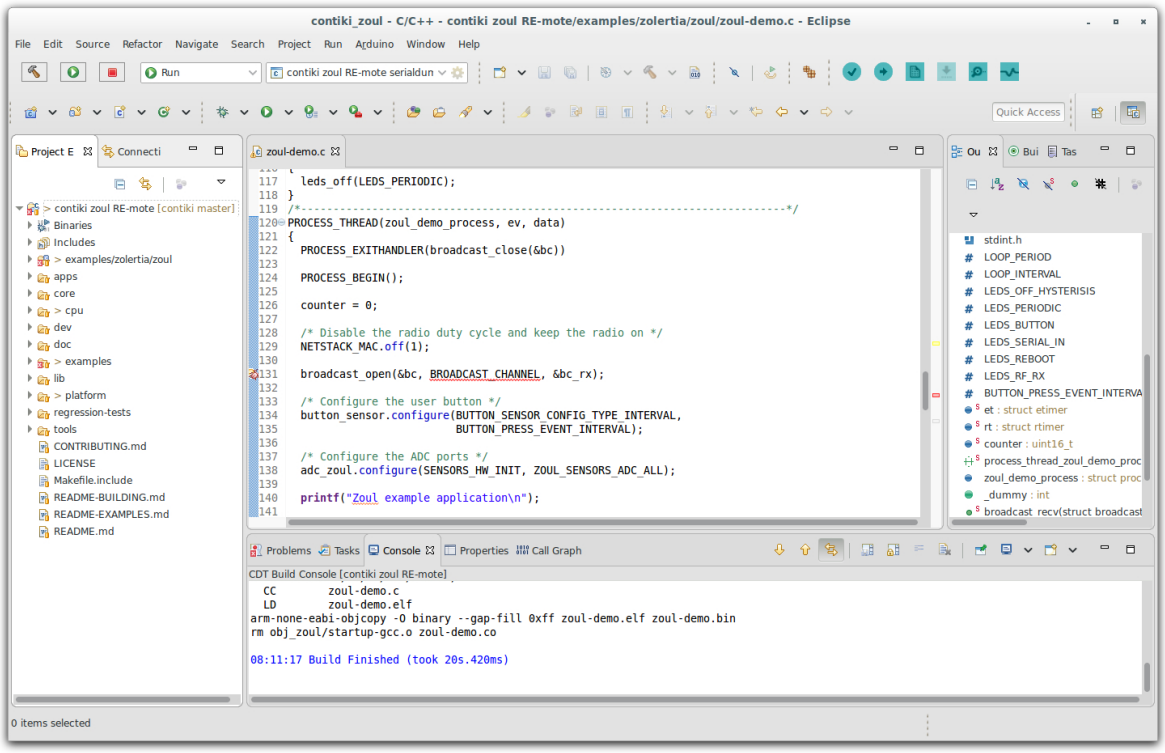
Adresár	**Popis**
examples	Predpripravené ukážky
app	Contiki aplikácie
cpu	MCU špecifikácie
dev	Externé čipi a zariadenia
platform	Konfiguračné súbory a ovládače platforiem
core	Knižnice kernelu
tools	Podporné nástroje
doc	Generovaná dokumentácia

Kompilácia vytvorených aplikácii prebieha za pomoci nástroja Cmake a kompilátoru pre procesory ARM. V tomto procese je vždy nutné špecifikovať názov konkrétnej platformy, aby mohli byť použité adekvátne nastavenia z adresára dev. Nasledujúca ukážka zobrazuje kompiláciu programu pre modul RE-Mote s nastavením adekvátneho identifikátora *zoul* .

```
make TARGET=zoul 01-hello-world
CC 01-hello-world.c
LD 01-hello-world.elf
arm-none-eabi-objcopy -O binary --gap-fill 0xff 01-hello-
world.elf 01-helloworld.bin
```

S kompiláciou vykonávanou špecificky pre zvolenú platformu sa pri práci vyskytli komplikácie. Dochádzalo k prípadom kedy bolo program možné zostaviť a nahrať na jednu platformu, no pri zostavení pre druhú platformu mal výsledný program prílišnú veľkosť a nebolo možné jeho nahranie na zariadenie.

Pre vývoj aplikácii bolo využívané IDE Eclipse, ktoré bolo nutné vopred nakonfigurovať. V prostredí bol pre zostavovanie programov, už uvedením spôsobom, využívaný nástroj Cmake. Vďaka prepojeniu s nástrojmi z adresára *dev*, bolo možné vykonávať nahrávanie zostavených programov do pripojených zariadení a taktiež vykonávať a zobrazovať sériovú komunikáciu priamo v IDE.



Obr. 6.1 Nakonfigurované IDE Eclipse

7 Sniffer

Pre sledovanie a zaznamenávanie prebiehajúcej bezdrôtovej komunikácie je potrebné využívať zariadenie nazývané sniffer. Pre tento účel bolo použité jedno z dostupných zariadení (tab. 6.1), do ktorého bol nahraný adekvátny firmware.

7.1 Realizácia

Aby bolo možné využívať niektorú z platforiem ako sniffer, bolo potrebné nahrať na na zariadene firmware umožňujúci promiskuitný režim prijímania bezdrôtovej komunikácie. Ten je súčasnou aktuálnej verzie operačného systému Contiki, ktorý je možné nájsť v adresári *examples/sensniff*. Program je možné nahrať na zariadenie príkazom

```
make clean && sudo make TARGET=zoul sensniff.upload
```

Takto pripravené zariadenie je schopné zachytávať sieťovú komunikáciu a zasielať získané pakety v hexadecimálnej forme pomocou sériovej linky. Pre spracovanie zachytených údajov bol využitý skript jazyku Python, ktorému boli ako parametre zadný zvolený komunikačný port a rýchlosť sériovej komunikácie.

```
python sensniff.py --non-interactive -d /dev/ttyUSB0 -b 460800
```

Úlohou tohto skriptu bolo vytvorenie rozhrania v použitom OS, ktoré by sprostredkovávalo získané údaje. Pre zobrazovanie zachytenej komunikácie bol využitý voľne dostupný program Wireshark. Ten umožnil zobrazenie komunikácie prehľadnou formou. Informácie o jednotlivých správach bolo možné prehľadávať pomocou vytvorenej stromovej štruktúry, zobrazujúcej význam získaných hexadecimálnych hodnôt. Súbor získaných správ bolo možné filtrovať podľa adresáta alebo zdroja správy a prípadne podľa používaného protokolu. Program Wireshark bolo potrebné spúšťať s uvedením adresy k vytvorenému rozhraniu.

```
sudo wireshark -i /tmp/sensniff
```

7.2 Mapovanie pokrytia

Zadaním tejto práce je vykonávať testovanie v reálnom prostredí budovy FAI UTB v Zlíne. Vďaka využitiu zariadenia pripraveného ako sniffer, bolo možné ešte pred testovaním prevádzky siete, v priestoroch budovy zmapovať pokrytie signálom. Získané informácie o dosahu vysielania boli využité pri návrhu testovacích scenárov. Obrázok 7.1 obsahuje výsledky merania.

Obr. 7.1 Pokrytie signálom (1. poschodie vľavo, 2. poschodie vpravo)

8 Testovanie funkcionalít

Hlavným cieľom tejto práce bolo testovanie funkcionalít protokolov využívaných v BSS. Využitím OS Contiki bolo možné testovať štandard 6LoWPAN, umožňujúci využívanie funkcionalít IPv6 a protokolu RPL využívaného na smerovanie v sieti. Vzhľadom na požadované správanie siete, bolo vytvorených 5 testovacích scenárov. Každý scenár bol zameraný na jednu konkrétnu situáciu. Pre sledovanie prevádzky v sieti mimo dosah sniffru, bolo využívané jedno zo zariadení slúžiace ako sietivá brána. Toto zariadenie bolo nakonfigurované a pripojené k PC, na ktorom bolo vytvorené sieťové rozhranie umožňujúce preosievanie správ medzi PC a 6LoWPAN sieťou. Pre komunikáciu zdrojového uzlu s bránou a následne aj s PC, bol využívaný protokol MQTT. Na PC bol nainštalovaný program Mosquitto, teda SW implementujúci MQTT prokolol, umožňujúci komunikáciu sieťovým zariadeniam. Zdrojový uzol v testovacích scenároch vždy periodicky odosiela správy, ktorých príjem bol kontrolovaný na cieľovom PC.

Na celkovo 6 zariadení boli nahrané programy definujúce ich sieťovú činnosť. Sieťové IPv6 adresy používané pre komunikáciu boli odvodené od MAC adries zariadení, vďaka čomu nedochádzalo pri testovaní k ich zmenám. Pre zvýšenie prehľadnosti popisovaných scenároch sú uvedené všetky typy zariadení s ich pridelenými adresami.

Zdroj MQTT správ:

fd00::212:4b00:60d:60bd

Cieľ, sieťová brána:

fd00::212:4b00:60d:60be

Smerovače:

fd00::212:4b00:62c:c4c0

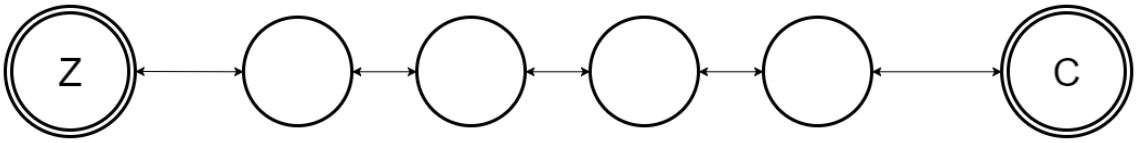
fd00::212:4b00:62c:c516

fd00::212:4b00:62c:c444

fd00::212:4b00:63a:4914

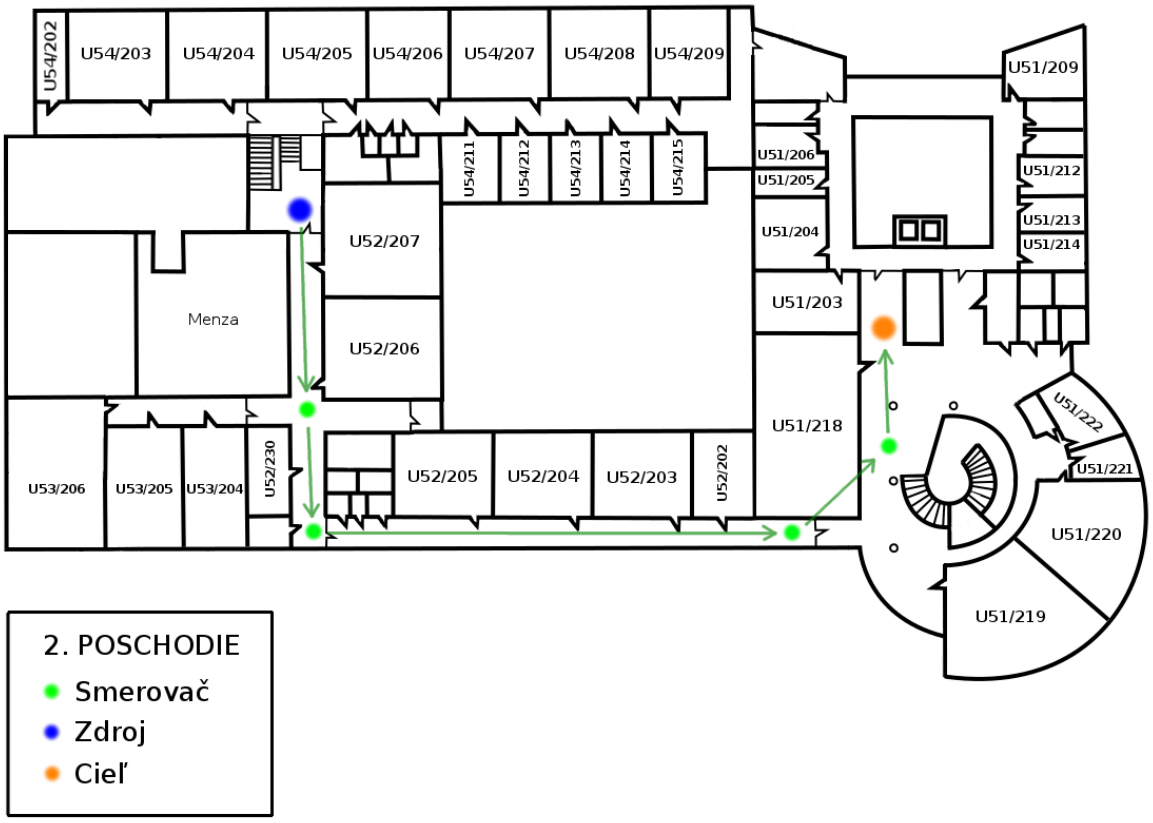
8.1 Expanzia

Základnou vlastnosťou BSS je schopnosť siete rozširovať sa pomocou pridávania nových uzlov. Prvý testovaný scenár je zameraný na skokovú komunikáciu zdroja s cieľom, za pomoci využívania medziľahlých smerovacích uzlov. Uzly by po zavedení mali umožňovať smerovanie medzi ľubovolnými zariadeniami. Predpokladané sieťové správanie je zobrazené pomocou diagramu na obrázku 8.1.



Obr. 8.1 Diagram - Expanzia

Test bol realizovaný postupným rozmiestňovaním uzlov tak, aby každý z nich bol v dosahu maximálne dvoch ďalších uzlov. Pri plánovaní rozloženia boli využité informácie získané pri zmapovaní pokrytia signálom (Obr. 7.1). Pri teste boli zo zdrojového uzlu vysielané správy, periodicky každých 10 sekúnd. Realizácia a reálne rozmiestnenie v budove je zobrazené na nasledujúcom obrázku.



Obr. 8.2 Nasadenie - Expanzia

Pri tomto teste bola zistená schopnosť uzlov samostatne sformovať komunikačnú trasu a tak umožniť komunikáciu dvom uzlom mimo ich vzájomného dosahu. Po aktivácii všetkých zariadení došlo približne po minúte k prvému doručeniu zasielaných správy. Vďaka implementovanému štandardu 6LoWPAN mohol byť správny prechod správ jednoducho overený. Pomocou príkaz *traceroute6* bolo vyvolané trasovanie komunikácie z PC pripojeného k sieťovej bráne až k poslednému uzlu v sieti. Zjednodušený výsledok overenia je zobrazený v nasledujúcej ukážke.

```
traceroute to fd00::212:4b00:60d:60bd, 30 hops max, 24 byte
1   fd00::212:4b00:60d:60be   18.593 ms   18.641 ms   18.722 ms
2   fd00::212:4b00:62c:c444   44.733 ms   115.678 ms   122.482 ms
3   fd00::212:4b00:63a:4914   257.001 ms   238.455 ms   249.595 ms
4   fd00::212:4b00:62c:c516   380.698 ms   367.39 ms   373.984 ms
5   fd00::212:4b00:62c:c4c0   624.187 ms   617.985 ms   620.24 ms
6   fd00::212:4b00:60d:60bd   752.386 ms   743.146 ms   751.053 ms
```

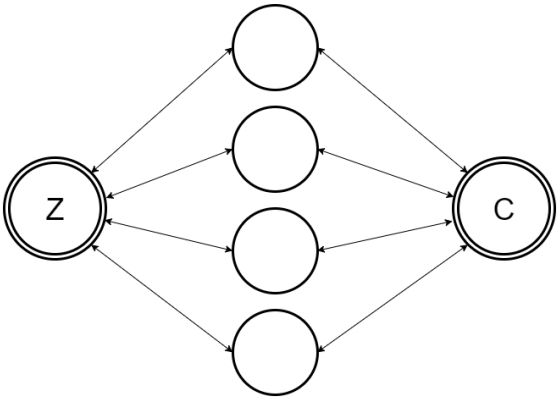
Takáto sieť bola podrobená testovaniu latencie pri komunikácii. Pre tieto účely bolo zdrojovému uzlu nastavené odosielanie správ každých 30 minút, vďaka čomu tieto správy neovplyvňovali výsledky testovania. Latencia bola s postupne redukovaným počtom zariadení v sieti testovaná v každej konfigurácii po dobu 15 min. Výsledky rýchlosti odozvy ako aj zistená stratovosť správ pri testovaní sú uvedené v tabuľke 8.1. V nej je možné sledovať zvyšujúcu sa hodnotu latencie a stratovosti spoločne so zvyšujúcim sa počtom testovaných uzlov. Od zistených hodnôt bola odpočítaná priemerná doba odozvy medzi PC a sieťovou bránou, ktorá dlhodobo dosahovala čas 20 ms.

Tab. 8.1 Testovanie rýchlosti odozvy

Počet	**Min [ms]**	**Max [ms]**	**St. hod. [ms]**	**Med [ms]**	**Stratovosť [%]**
2	19,156	846,145	85,045	44,260	1
3	125,809	6472,972	542,443	963.702	14
4	254,009	6180,627	589,402	710,867	17
5	376.839	12468.682	2603.523	2936.605	31
6	793.727	15561.494	5625.367	4255.882	32

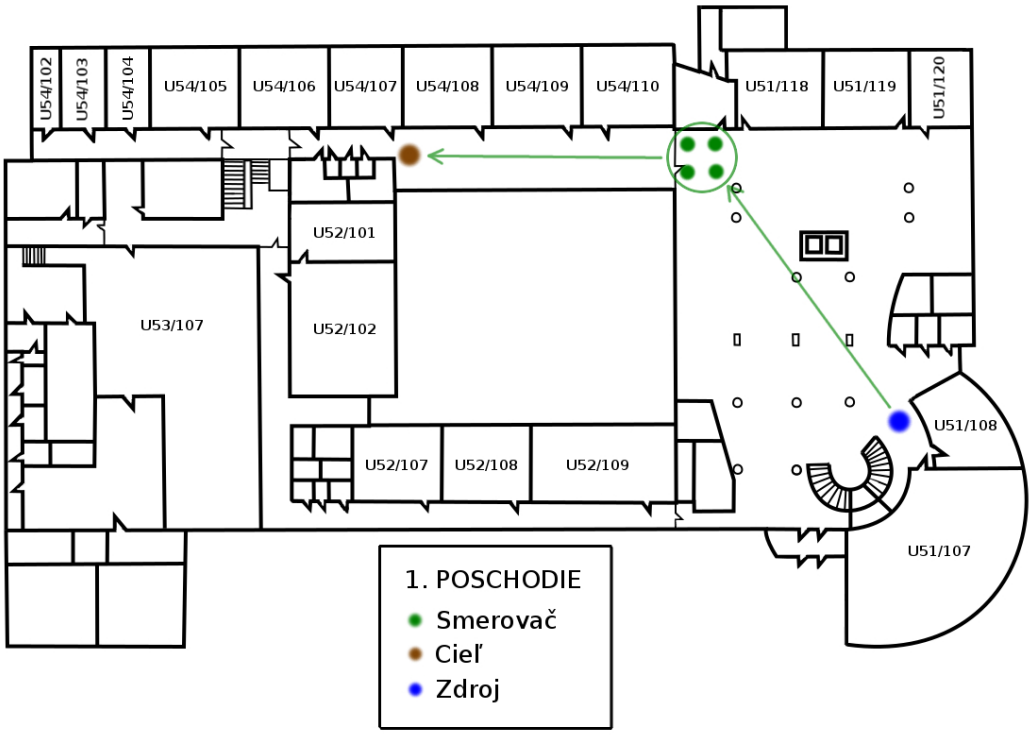
8.2 Alternatívne trasy

Druhý testovací scenár je zameraný na reakciu siete pri poruche niektorého z uzlov a taktiež na schopnosť protokolu zvoliť vhodnú cestu pre ďalšiu komunikáciu. Schopnosť adekvátne reagovať na vyradenie z prevádzky niektorého z uzlov, je pre sieť kritickým faktorom. Následne pri formovaní novej smerovacej štruktúry je nutná efektívna voľba nových ciest. Na obrázku 8.3 je zobrazená ideálna konfigurácia uzlov pre testovanie uvedených vlastností.



Obr. 8.3 Diagram - Alternatívne trasy

Uzly boli rozmiestnené tak, aby komunikácia medzi zdrojom a cieľom mohla byť vykonávaná pomocou skoku cez jeden smerovací uzol. Smerovacie uzly boli umiestnené vo vzájomnom dosahu, aby tak ponúkali možnosť využívania 4 alternatívnych trás. Pri simulovaných poruchách uzlov bola sledovaná reakcia siete a upravenie ciest.



Obr. 8.4 Nasadenie - Alternatívne trasy

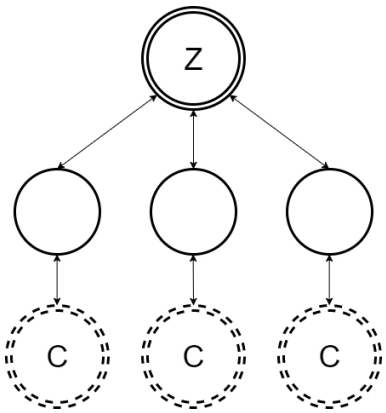
Pri opakovanej aktivácii a deaktivácii zariadení došlo vždy ku vytvoreniu trasy s použitím výlučne jedného smerovacieho uzlu. To poukazuje na inteligentný návrh protokolu využívajúceho najmenší možný počet uzlov. Pri simulovanej chybe aktuálne používaného smerovača došlo v sieti k veľmi rýchlej adaptácii. Dlhodobejším testovaním bolo overené, že ku zmenám využívaných trás za bezporuchovej prevádzky nedochádza.

Overenie využívanej trasy bolo v tomto prípade možné vykonať pomocou informácii zo sieťovej brány. Tá poskytuje webové rozhranie dostupne po zadaní jej IPv6 adresy do ľubovolného prehliadača. Stránka obsahuje informácie o susedských uzloch brány a uložených cestách. V druhom riadku nasledujúcej ukážky je možné vidieť že cesta k zdrojovému uzlu vedie cez jeden zo smerovačov.

```
Routes
fd00::212:4b00:60d:60bd/128  (via  fe80::212:4b00:62c:c516)
fd00::212:4b00:62c:c4c0/128  (via  fe80::212:4b00:62c:c4c0)
fd00::212:4b00:62c:c516/128  (via  fe80::212:4b00:62c:c516)
fd00::212:4b00:63a:4914/128  (via  fe80::212:4b00:63a:4914)
fd00::212:4b00:62c:c444/128  (via  fe80::212:4b00:62c:c444)
```

8.3 Mobilita

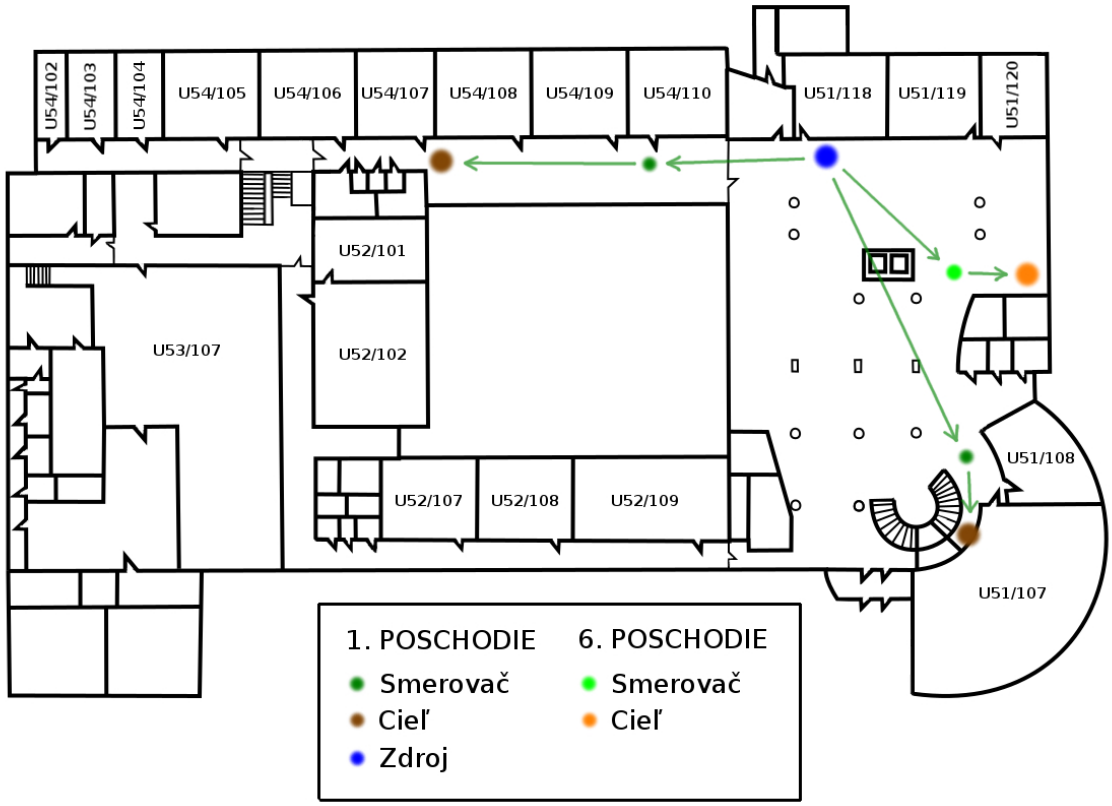
Tretí scenár bol zameraný na mobilitu sieťových uzlov. Možnosť meniť počas prevádzky pozíciu ktoréhokoľvek uzlu umožnuje využívanie BSS aj v dynamicky sa meniacom prostredí. V rámci testu bola zisťovaná reakcia na mobilitu zdroja správ a taktiež cieľovej sieťovej brány.



Obr. 8.5 Diagram - Mobilita

Realizácia bola vytvorená tak, aby bol zdrojový uzol v dosahu troch smerovacích uzlov, ktoré sa vo vzájomnom dosahu nenachádzajú. Rozmiestnenie bolo naplánované za pomoci informácii o pokrytí signálom. Overenie že sa uzol nachádza výlučne v dosahu jedného smerovača bolo možné overiť vo webovom rozhraní sieťovej brány.

```
Routes
fd00::212:4b00:60d:60bd/128  (via  fe80::212:4b00:62c:c444)
fd00::212:4b00:62c:c444/128  (via  fe80::212:4b00:62c:c444)
```



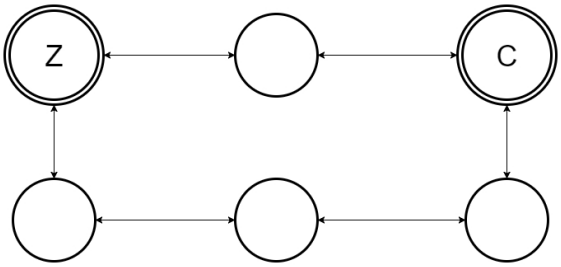
Obr. 8.6 Nasadenie - Mobilita

K pokračovaniu v komunikácií po presunutí uzlu došlo úspešne vo všetkých testovaných prípadoch. K adaptácii na presunutie cieľového uzlu došlo pri testovaní najneskôr do dvoch minút. To bolo zapríčinené nastavením sieťových zariadení, ktoré svoju aktivitu ohlasujú okolitým uzlom periodicky každú minútu. V tomto prípade došlo k úspešnému prijatiu až druhej ohlasovacej správy. Cieľové zariadenie bolo napájané z prenosného zdroja a teda jeho činnosť bola kontinuálna. Pri presunoch zdrojového uzlu dochádzalo k reštartom zariadenia a adaptácia prebehla do niekoľkých sekúnd. Príčinou bolo zasielanie ohlasovacej správy, vykonávané pri aktivácii zariadenia.

8.4 Výber efektívnejšej cesty

Ako už bolo zistené v teste 8.2, ku zmenám v rovnocenných cestách nedochádza. Tento štvrtý test bol zameraný na schopnosť siete zmeniť svoju štruktúru a zvoliť výhodnejšiu trasu. V tomto prípade nedochádzalo k simulovaným poruchám uzlov. Diagram 8.7 zobrazuje návrh realizácie tohto scenáru.

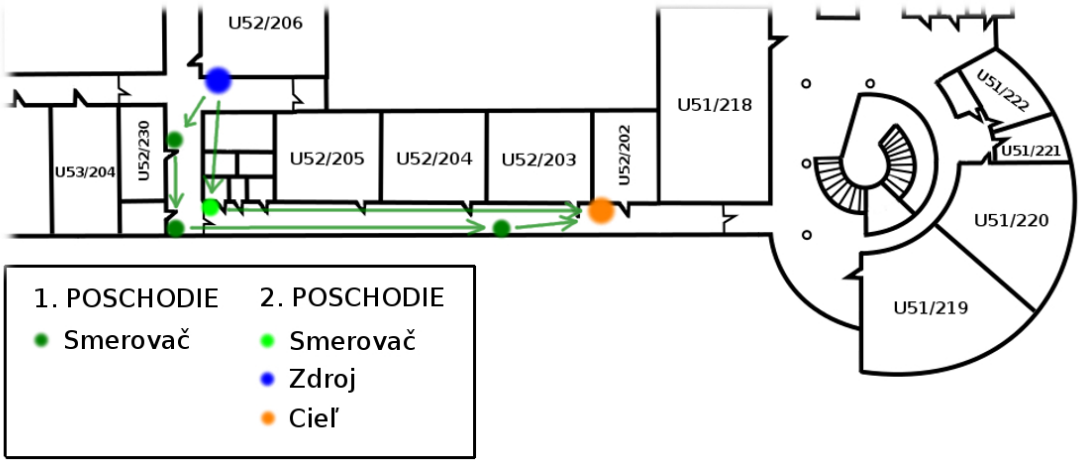
Pri realizácii boli ako prvé rozmiestnené zdrojový a cieľový uzol. Medzi uzlami boli vytvorené dve komunikačné cesty s využitím rôzneho počtu zariadení. Prvá trasa pozostávala celkovo z 3 smerovacích uzlov. Druhá efektívnejšia trasa, umožňovala prepojenie s využitím iba jedného medziľahlého zariadenia.



Obr. 8.7 Diagram - Efektívnosť cesty

Medzi zdrojovým a cieľovým uzlom boli ako prvé aktivované zariadenia na dlhšej komunikačnej trase. Funkčnosť trasy bola potvrdená prijímaním správ na PC pripojenom k sieťovej bráne. Po aktivácii uzlu umožňujúceho využitie kratšej trasy, sa sieť pri opakovaných testoch vždy dokázala úspešne preformovať. K výberu kratšej trasy došlo pri testovaní najneskôr do 29 minút. Táto doba poukazuje na vhodný návrh správania siete, keďže jej príliš častá zmena by mohla zvyšovať spotrebu energie a tak znižovať životnosť zariadení. Zmena smerovania bola overená trasovaním.

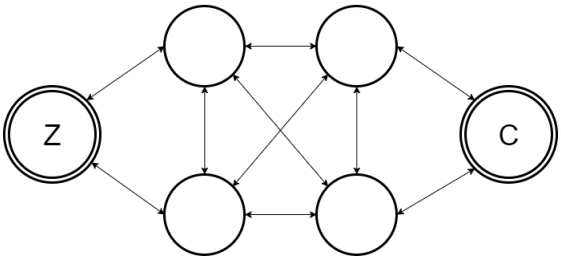
```
traceroute to fd00::212:4b00:60d:60bd, 30 hops max, 24 byte
1   fd00::212:4b00:60d:60be   18.548 ms   18.486 ms   18.368 ms
2   fd00::212:4b00:63a:4914   58.679 ms   122.647 ms   122.905 ms
3   fd00::212:4b00:60d:60bd   382.49 ms   865.814 ms   1619.47 ms
```



Obr. 8.8 Nasadenie - Efektívnosť cesty

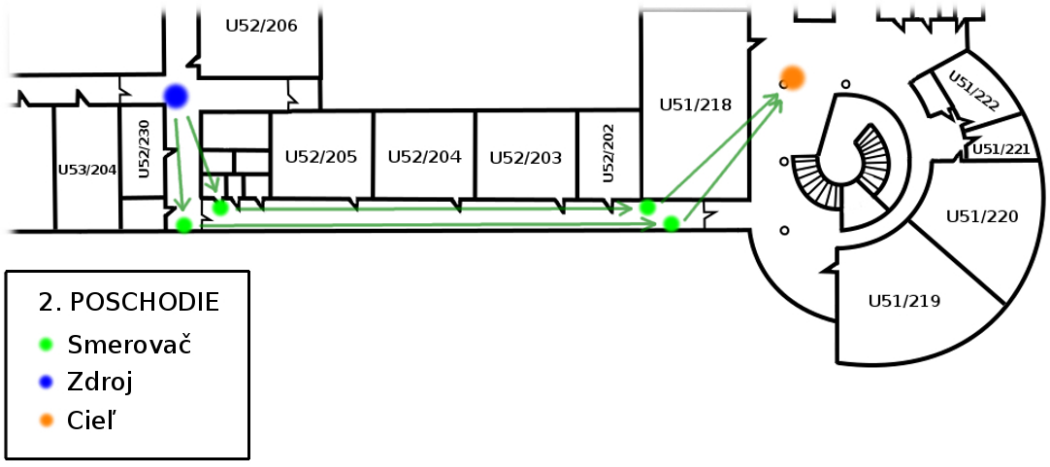
8.5 Rýchlosť adaptácie

Posledný testovací scenár bol zameraný na zisťovanie rýchlosti adaptácie siete po deaktivácii uzlu, používaného na komunikačnej trase. Komunikácia medzi zdrojovým a cieľovým uzlom musela prechádzať minimálne dvoma ďalšími uzlami.



Obr. 8.9 Diagram - Rýchlosť adaptácie

Po rozmiestnení uzlov (obr. 8.10) prebehlo meranie rýchlosti zmeny smerovacích ciest. Správy odosielané zo zdrojového uzlu boli upravené tak, aby obsahovali sekvenčné číslo správy a celkový čas od momentu aktivácie zariadenia. Zasielanie správ bolo vykonávané opakovane s periódou 1 sekundy, čo umožnilo záznam doby nutnej pre adaptáciu. Porovnávané boli situácie kedy bol aktívny výlučne jeden z dvojice pri sebe umiestnených smerovacích uzlov (v momente deaktivácie jedného zariadenia došlo k aktivácii druhého), so situáciou pri ktorej boli aktívne a teda už pre okolité zariadenia známe oba uzly.



Obr. 8.10 Nasadenie - Rýchlosť adaptácie

Pri testovaní bolo zistené že adaptácia prebieha rovnako rýchlo v oboch testovaných prípadoch. Vzdialenosť od sieťovej brány taktiež z časového hľadiska neovplyvňovala rýchlosť zmeny. Tabuľka 8.2 obsahuje vyhodnotené výsledky

Tab. 8.2 Testovanie rýchlosti adaptácie

Min [s]	Max [s]	St. hod. [s]	Med [s]
53	108	87,667	92

9 Meranie

9.1 Spotreba

Ďalšou zo zadaných úloh práce bolo vykonanie meranie spotreby elektrickej energie. Pre tento účel bol sledovaný a zaznamenávaný prúd odoberaný zariadením. Pri meraní boli upravované a porovnávané parametre vysielania a samotná činnosť zariadenia.

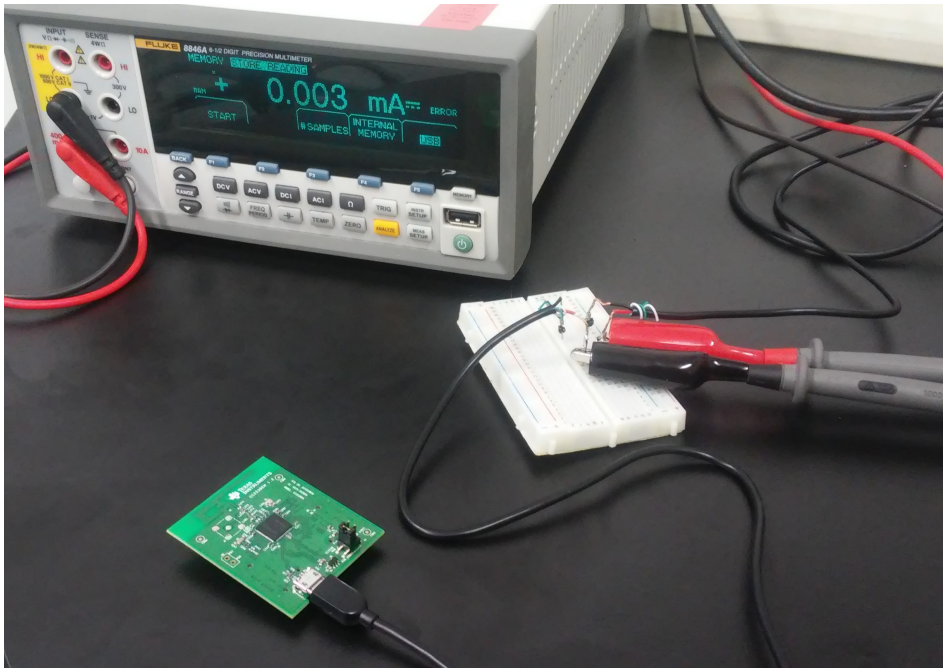
9.1.1 Meracie zariadenie

Pre meranie bolo potrebné zvoliť vhodné zariadenie schopné snímania s dostatočnou presnosťou a frekvenciou. Zvoleným meracím zariadením sa stal multimeter Fluke 8846A umožňujúci nastavenie presnosti a frekvencie snímania. Pri meraní bola využitá schopnosť multimetru zaznamenávať a ukladať zadaný počet meraní. Tabuľka 9.1 obsahuje relevantné parametre zariadenia

Tab. 9.1 Fluke 8846A

Parameter	**Hodnota**
Rozsah merania prúdu DC	100p...100μ/1m/100m/400m/1/3/10A
Presnosť merania prúdu DC	$\pm$(0,05% zmeranej hodnoty + 0,005% rozsahu)
Vzorkovanie	1000x/s

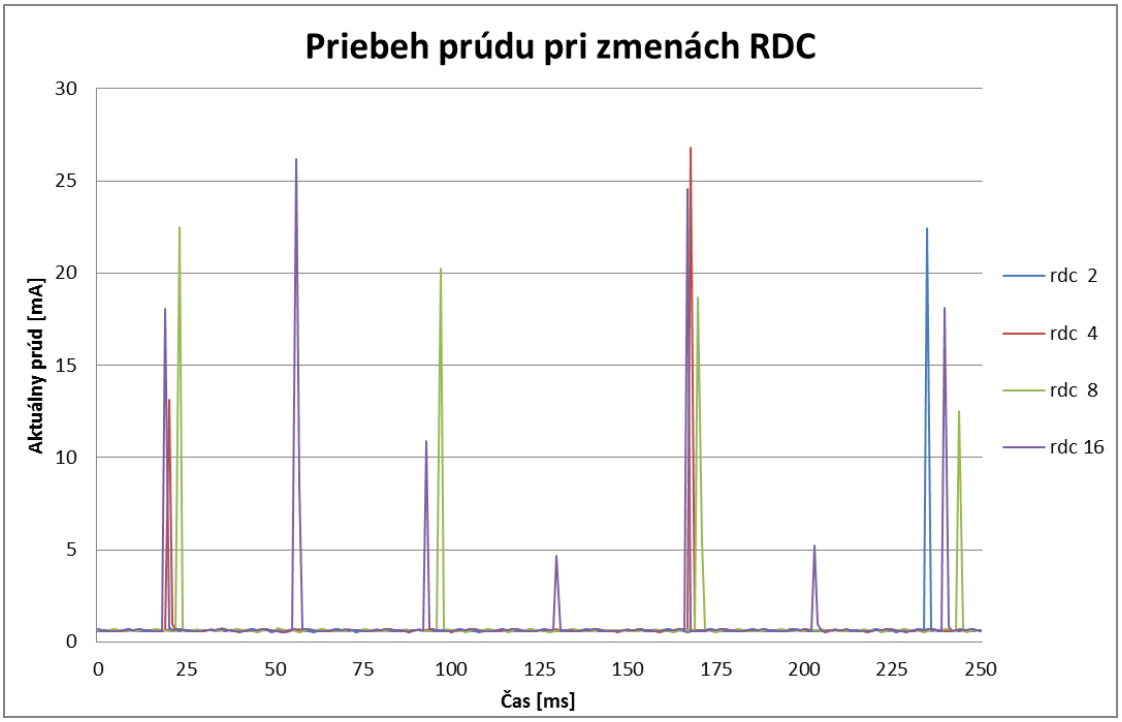
Nakonfigurovaný multimeter bol sériovo zapojený do elektrického obvodu pred testované zariadenie. Takýmto spôsobom prebehli všetky nasledujúce merania.



Obr. 9.1 Meranie spotreby

9.1.2 Výsledky merania

Meranie bolo vykonávané s modulom CC2538EM naprogramovaným pre činnosť smerovača. V prvom meraní bol modul postupne preprogramovávaný, so zmeneným nastavením parametru RDC (Radio duty cycle).



Obr. 9.2 Prúdový odber pri zmenách RDC

Z obrázku 9.2 je zrejmé, že zmena parametru RDC vyvolala adekvátne frekventované zapínanie vysielača, čo sa odzrkadlilo na zaznamenanom prúdovom odbere. Taktiež je možné pozorovať výrazný rozdiel medzi kľudovým stavom s odberom rádovo v stovkách µA a aktívnym stavom s odberom viac ako 26 mA. Tabuľka 9.2 obsahuje štatistické vyhodnotenie vykonaného merania. Informácie boli získavané po dobu 10 sekúnd so vzorkovacou frekvenciou 1 kHz.

Tab. 9.2 Prúdový odber bez okolitej prevádzky

RDC	Min [µA]	Max [mA]	St. hod. [µA]	Med [µA]	Rozp [µA]
2	519	26,443	689,390	626	1,129
4	514	26,811	738,536	626	1,896
8	514	26,783	844,547	628	3,583
16	521	26,869	1059,741	631	7,042

Z tabuľky je možné pozorovať priamo úmerné zvyšovanie strednej hodnoty a rozptylu s nastavovanou hodnotou RDC. Podľa očakávaní sú hodnoty zaznamenaných miním, maxím a spočítaného mediánu pre každú konfiguráciu veľmi podobné.

Rovnaké meranie bolo vykonané za simulovanej prevádzky. V dosahu smerovacieho uzlu boli rozmiestnené ďalšie 3 vysielacie zariadenia. Tie periodicky každých 500 ms odosielali do siete multicast správy, aby tak donútili smerovací uzol tieto správy spracovávať. Tabuľka 9.3 obsahuje spracované výsledky sledovaného prúdového odberu, v reakcii na túto uzlom vykonávanú činnosť.

Tab. 9.3 Prúdový odber počas simulovanej prevádzky

RDC	Min [µA]	Max [mA]	St. hod. [mA]	Med [mA]	Rozp [µA]
2	525	38,891	21,219	26,126	279,097
4	523	38,838	17,180	21,348	275,439
8	523	38,928	13,269	17,717	182,936
16	532	38,969	18,515	22,185	165,245

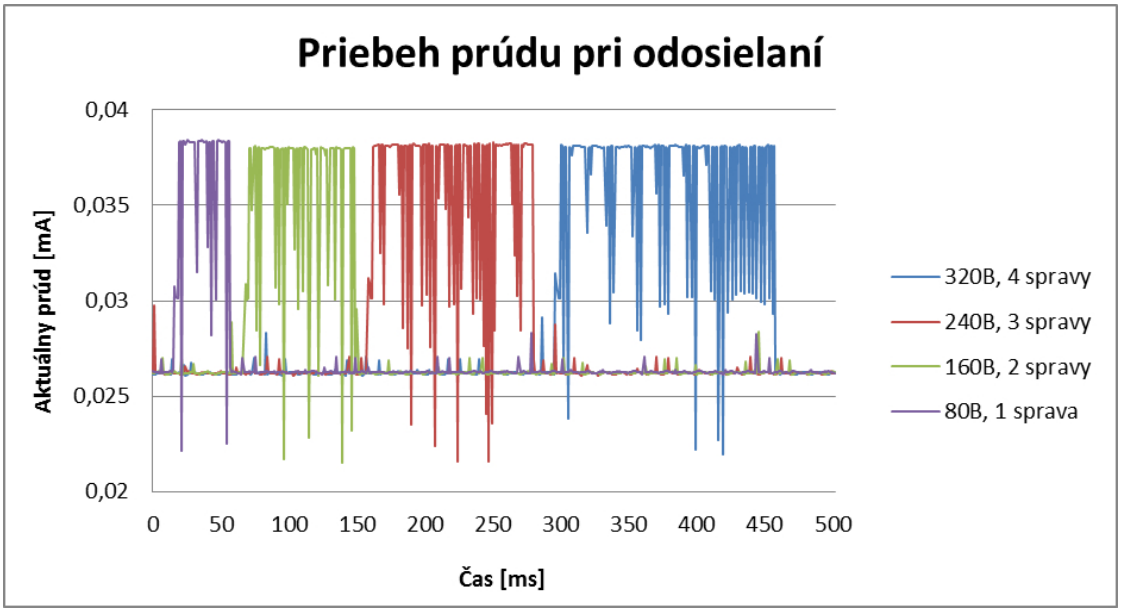
Oproti výsledkom z predchádzajúceho merania je možné pozorovať, okrem minima, zvýšenie všetkých vyhodnocovaných parametrov. Simulovaná prevádzka teda podľa očakávaní výrazne ovplyvnila množstvo zariadením odoberaného prúdu. Zistené informácie o strednej hodnote a mediáne nekorelujú s parametrom RDC a v prípade rozptylu došlo dokonca k nepriamej úmere. Tieto výsledky sú zapríčinené náhodným spúšťaním okolitých zariadení. Ich vysielanie nebolo realizovateľné s presne symetrickým časovým rozložením, čoho dôsledkom bol odlišný spôsob ovplyvnenia realizovaných testov.

Ďalšie meranie prebehlo s modulom vykonávajúcim odosielanie. V tomto prípade bolo vysielanie realizované postupne s rôznou veľkostnou dát a rôznym počtom zasielaných správ. K odosielaniu zo zariadenia dochádzalo každých 500 ms. Tabuľka 9.4 obsahuje vyhodnotenie získaných údajov.

Tab. 9.4 Prúdový odber pri odosielaní správ

Dáta [B]	Poč. správ	Max [mA]	St. hod. [mA]	Med [mA]	Rozp [µA]
80	1	38,493	27,0223	26,262	7,942
160	2	38,088	27,593	26,225	13,587
240	3	38,325	28,310	26,221	19,918
480	4	38,239	28,951	26,223	24,165

Zo získaných informácii vyplýva, že so zvyšujúcou sa veľkosťou zasielanej informácie, sa priamo úmerne zvyšovala stredná hodnota a zistený rozptyl. Maximálny prúdový odber dosahoval rovnakých hodnôt, ako v prípade simulovanej prevádzky (tab. 9.3). Vplyv množstva zasielaných dát ovplyvnil priemernú spotrebu zariadenia len minimálne. Rozdiel v stredných hodnotách odoberaného prúdu činil pri zvyšujúcom sa počte správ maximálne 717 µA.



Obr. 9.3 Priebeh odberu prúdu pri odosielaní

Obrázok 10.1 zobrazuje vybrané úseky priebehu prúdového odberu pri rôznych veľkostiach zasielanej informácie. Z grafu je očividné priamo úmerné predlžovanie doby nutnej ku kompletnému odoslaniu dát vzhľadom na ich množstvo. V prípade odosielania 4 správ táto doba dosahovala približne 170 ms.

9.2 Priepustnosť

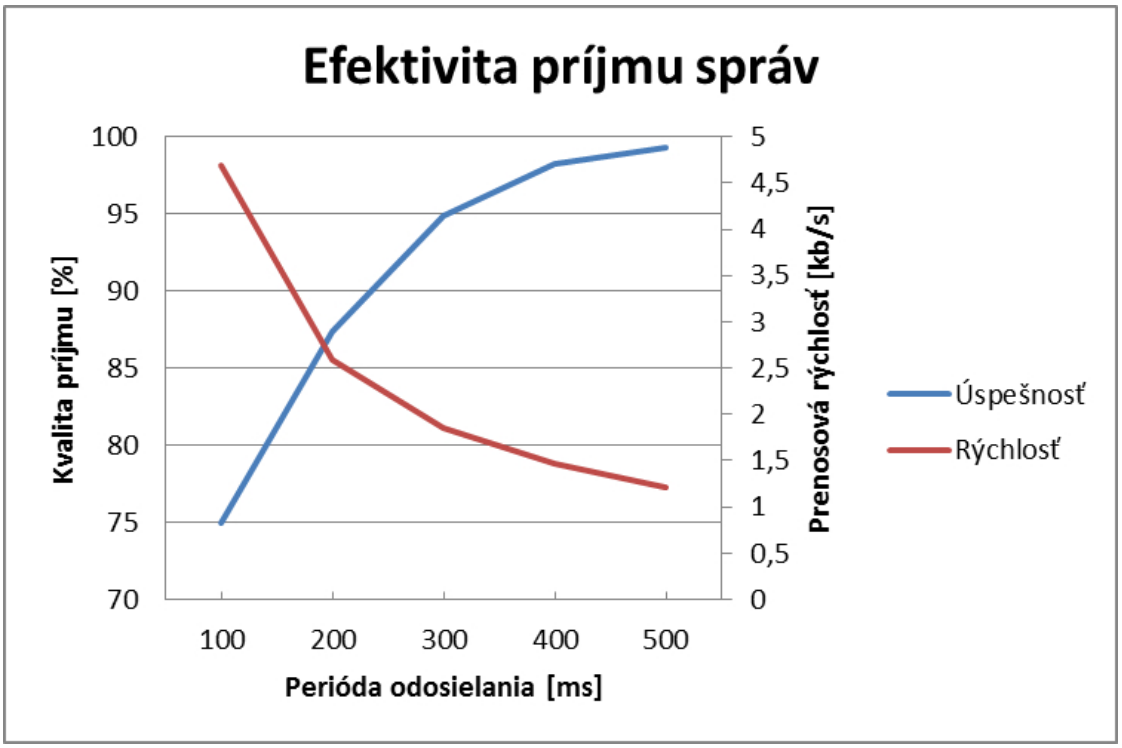
Súčasťou zadania práce bolo vykonanie merania priepustnosti. Prvým krokom procesu bolo zistenie maximálnej rýchlosti odosielania dát. Za týmto účelom bolo jedno zo zariadení naprogramované, aby odosielalo bez čakania stanovený počet správ. Veľkosť správy bola nastavená na hodnotu 80B, čo predstavuje maximálnu hodnotu ktorú bolo možné odoslať pomocou jednej správy. Vysielanie bolo zachytávané sniffrom a získané dáta prenášané do programu Wireshark. V programe bolo následne možné prezerať prijaté údaje a vďaka zaznamenávaniu času presne určiť dobu potrebnú pre vysielanie stanovených 500 správ. Vzhľadom na zistenú priemernú dobu vysielania 31,402 s, bolo zistené že pre odoslanie jednej správy potrebuje zariadenie minimálne 62,8 ms. Zistený údaj približne korešponduje s dobou zvýšeného odberu prúdu pri odosielaní jednej správy o veľkosti 80B (obr. 10.1).

Pre zistenie reálnej prenosovej rýchlosti bolo potrebné stanoviť, ako efektívne dokáže ďalšie zariadenie toto vysielanie prijímať. Za týmto účelom bolo pridané ďalšie zariadenie, upravené pre zaznamenávanie počtu prijatých správ. Vďaka tejto informácii mohla byť zistená reálna prenosová rýchlosť. Vzhľadom na známy počet odosielaných správ, bolo možné stanoviť ich percentuálnu úspešnosť. Tabuľka 9.5 obsahuje zistené informácie pre rôzne periódy odosielania.

Tab. 9.5 Výsledky merania priepustnosti

Perióda odosielania [ms]	Perióda prijímania [ms]	Kvalita príjmu [%]	Prenosová rýchlosť [kb/s]
50	112,727	66,8	5,677
100	136,363	75,1	4,693
200	247,337	87,4	2,587
300	344,815	94,9	1,856
400	435,115	98,3	1,470
500	525,609	99,3	1,217

V prvom riadku tabuľky je uvedený prípad nastavenia periódy odosielania na 50 ms, teda na hodnotu menšiu ako zistená maximálna rýchlosť. S týmto nastavením teda prebehlo odosielanie najrýchlejším možným spôsobom a zistenú prenosovú rýchlosť 5,667 kb/s je zároveň možné považovať za maximálnou priepustnosť.

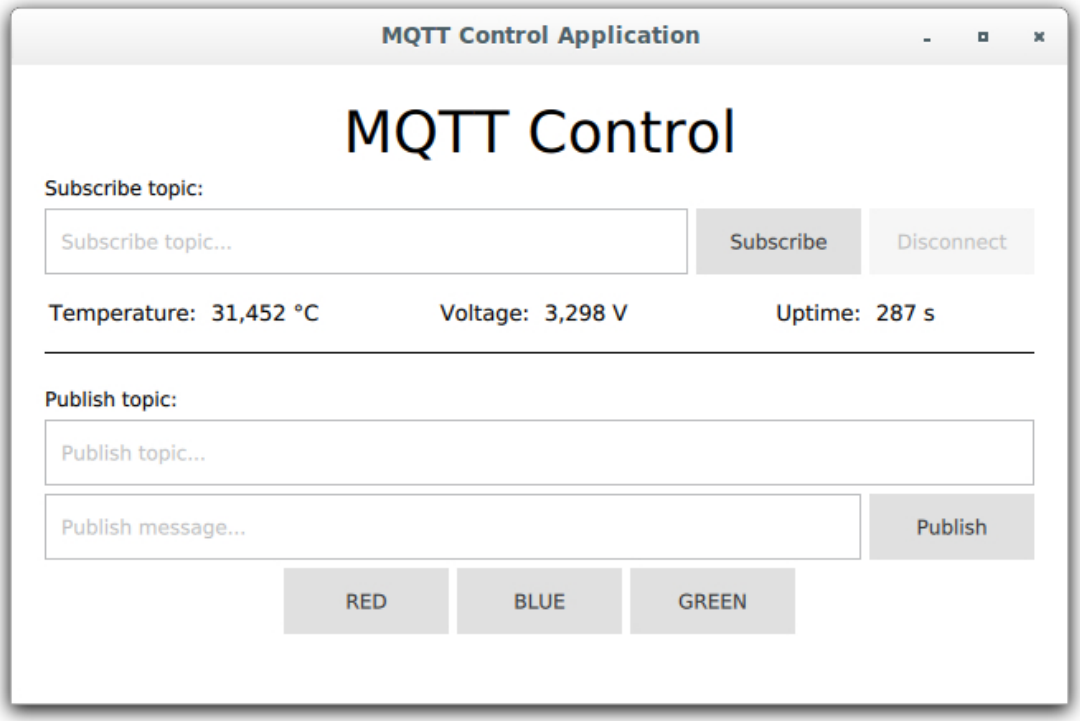


Obr. 9.4 Efektivita príjmu správ

Zo získaných dát vynesených do grafu je možné pozorovať, že so zvyšujúcou sa hodnotou periódy odosielania sa priamo úmerne zvyšuje úspešnosť a nepriamo úmerne rýchlosť prenosu dát.

10 Riadiaca aplikácia

Pre otestovanie funkcii komunikácie s uzlami bola vytvorená riadiaca aplikácia. Tá bola napísaná v jazyku C++ a QML za pomoci frameworku Qt. Jej účelom bolo umožniť príjem a zobrazovanie dát zasielaných od sieťových uzlov. Pre vzájomnú komunikáciu bol využitý už spomínaný program Mosquitto. Vďaka nemu bolo možné pomocou protokolu MQTT jednoducho prímať a odosielať požadované informácie. Pre umožnenie riadenia zariadenie bolo potrebné naprogramovať jeho odozvu na prijatú správu. Zo zariadenia boli odosielané informácie o zaznamenanej teplote, aktuálnej úrovni napätia a celkovom čase, počas ktorého je zariadenie aktívne.

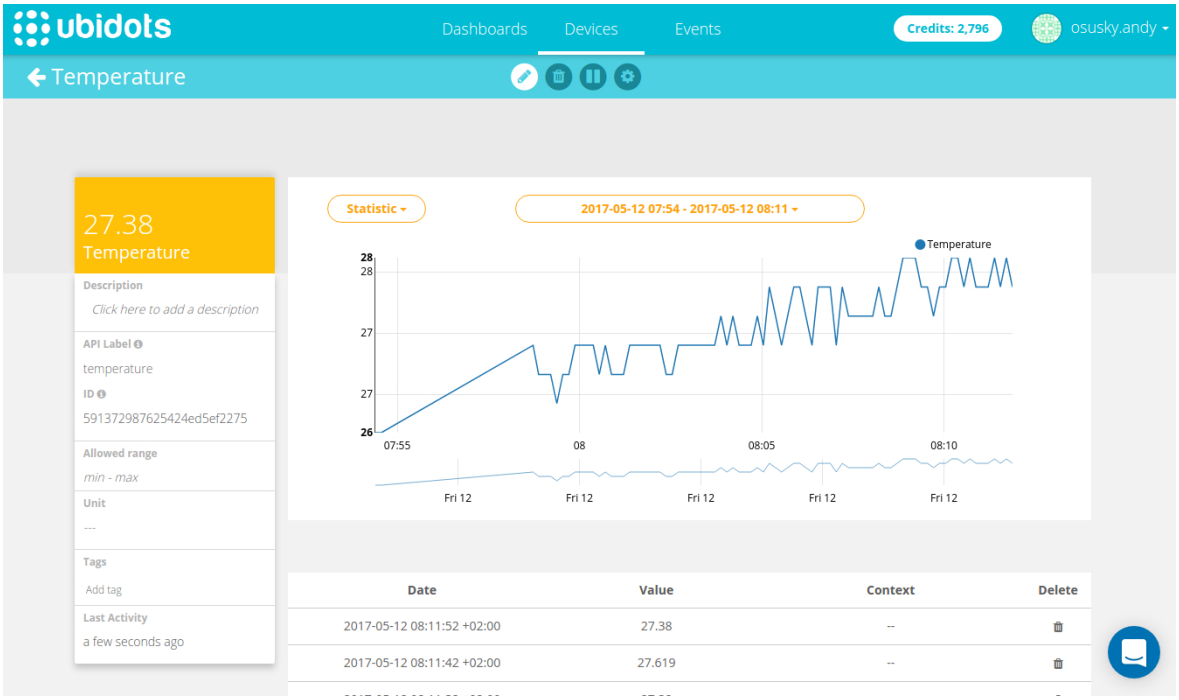


Obr. 10.1 MQTT riadiaca aplikácia

Aplikácia umožnuje pomocou prvého textového poľa nastaviť názov témy ktorej správy budú odoberané. Rovnaký názov témy bolo potrebné použiť pri odosielaní správ zo zariadenia. Po zadaní názvu a stlačení tlačidla *Subscribe* aplikácia po prijatí správ zobrazí získané informácie v príslušných poliach v hornej polovici rozhrania aplikácie. Ukončenie odberu je možné vykonať stlačením tlačidla *Disconnect*.

Ovládacie prvky pod touto čiarou sú určené pre odosielanie správ. V tomto prípade je potrebné nastaviť názov témy a obsah zasielanej správy. K odoslaniu dochádza v momente stlačenia tlačidla *Publish*. Pre demonštráciu riadenia zariadenia boli do rozhrania pridané tri spodné tlačidlá. V momente stlačenia tlačidiel dôjde k odoslaniu príkazov, na ktorých prijatie reaguje zariadenie rozsvietením adekvátnej farby.

Pridanou funkciou aplikácie bolo prepojenie s cloud službou Ubidost. Táto služba bola vytvorená priamo pre sféru IoT a umožnuje prehľadne graficky a v reálnom čase zobrazovať zaznamenané údaje. V rozhraní bolo potrebné vopred vytvoriť premenné, ktorých hodnoty mali byť zaznamenávané. Týmto hodnotám boli priradené špeciálne identifikátory, ktoré boli následne využité ako súčasť http dotazu pre zasielanie aplikáciou prijatých správ. Samotné dáta boli zasielané vo formáte JSON. K ich odoslaniu dochádza automaticky v momente ich prijatia zo 6LoWPAN siete. Aplikácia reprezentuje medzičlánok, v ktorom je možné prijaté informácie zo siete spracovať, ešte pred ich zverejnením pomocou služby Ubidots.



Obr. 10.2 Ubidots

ZÁVER

V rámci teoretickej časti tejto práce došlo k vypracovaniu viacerých okruhov. Prvým bola analýza BSS, popis ich charakteristických vlastností, využívanej topológie a kompletný zoznam požiadavkov, kladených na ich funkcionality. Ďalej boli analyzované vybrané princípy smerovania a popísané algoritmy klasifikované do skupín podľa ich spoločných vlastností. Tretia kapitola sa zaoberala sieťovou bezpečnosťou a popisom zraniteľností a obranných mechanizmov na jednotlivých sieťových vrstvách. Štvrtou a poslednou sekciou teoretickej časti boli aktuálne používané štandardy. Analyzovanými boli architektúry a vybrané funkcie štandardov IEEE 802.15.4, Zigbee a 6LoWPAN.

Účelom praktickej časti práce bolo vykonať testovanie reálnej prevádzky siete v prostredí budovy FAI UTB. Pre túto činnosť boli využité HW platformy Zolertia RE-Mote a TI CC2538EM. Pre riadenie uvedených zariadení bol využitý OS Contiki. Ten umožnil pri komunikácii využívať štandard 6LoWPAN a smerovací protokol RPL.

V rámci práce prebehlo testovanie požadovaných sieťových funkcionalít. Celkovo bolo vykonaných 5 testovacích scenárov. V scenári zameranom na expanziu sa podarilo úspešne overiť schopnosť siete, vytvoriť komunikačné trasy a skokovo zasielať správy cez všetkých 6 uzlov. Prebehlo taktiež meranie latencie(tab. 8.1) ktoré odhalilo výrazné zvyšovania sa stratovosti a odozvy so zvyšujúcim sa počtom uzlov. Druhým scenárom, zameraným na voľbu alternatívnych trás, bola overená schopnosť siete, adaptovať svoju štruktúru v prípade vyradenia zariadenia používaného na trase. Ďalší test potvrdil možnosť mobility zariadení, ktoré bolo možné počas prevádzky presúvať. Štvrtý test potvrdil schopnosť výberu efektívnejšej cesty. Pri opakovanom testovaní došlo ku adaptácii na trasu využívajúcu menší počet uzlov a to najneskôr do 29 min. To poukazuje na vhodný návrh protokolu, keďže príliš časté reorganizovanie by zapríčinilo nadmernú spotrebu energie. Posledný test zameraný na rýchlosť adaptácie umožnil vyhodnotiť rekčný čas siete, ktorej priemerná hodnota dosiahla necelých 88 sekúnd (tab. 8.2).

V sekcii merania bola vyhodnocovaná spotreba energie za rôznej sieťovej prevádzky. Meraním bola zistená adekvátna odozva na zmeny parametru RDC (obr. 9.2). Bola zistená najnižšia priemerná hodnota odoberaného prúdu činiaca 689 µA (tab. 9.2). Najvyššia priemerná hodnota odberu, pri simulovanej prevádzke, dosiahla úrovne necelých 21 mA (tab. 9.3). Pri odosielaní správ bol zistený vplyv veľkosti odosielanej správy na zvyšovanie spotreby zariadenia (tab. 9.4). V rámci merania bola vyhodnotená maximálna dosiahnutá priepustnosť, ktorej hodnota činí 5,7 kb/s (tab. 9.5).

Pre demonštráciu komunikácie a správu sieťových uzlov bola vytvorená riadiaca aplikácia. Tá za pomocou protokolu MQTT, umožnila riadiť sieťové zariadenia a prijímať zaznamenané senzorové informácie. Prijaté údaje boli zobrazované v aplikácii a taktiež zasielané na cloud a vizualizované pomocou služby Ubidost.

ZOZNAM POUŽITEJ LITERATÚRY

[1] RATHEE, Amit, Randeep SINGH a Abhishilpa NANDINI. Wireless Sensor Network- Challenges and Possibilities. *International Journal of Computer Applications* [online]. 2016, 140(2), 1 - 15 [cit. 2017-03-02]. Dostupné z: http://www.ijcaonline.org/research/volume140/number2/rathee-2016-ijca-909221.pdf

[2] *Internet of Things: Wireless Sensor Networks* [online]. Geneva, Switzerland: International Electrotechnical Commission, 2014 [cit. 2017-03-02]. ISBN 978-2-8322-1834-1. Dostupné z: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[3] MATIN, M.A. a M.M. ISLAM. Overview of Wireless Sensor Network. *Wireless Sensor Networks - Technology and Protocols* [online]. InTech, 2012 [cit. 2017-03-02]. DOI: 10.5772/49376. ISBN 978-953-51-0735-4. Dostupné z: http://www.intechopen.com/books/wireless-sensor-networks-technology-and-protocols/overview-of-wireless-sensor-network

[4] "Smart"Bridges Instrumented with Dense Networks of Wireless Sensors. *Civil and Environmental Engineering* [online]. Michigan: University of Michigan, 2013 [cit. 2017-03-02]. Dostupné z: http://cee.engin.umich.edu/Smart-Bridges

[5] LIU, Fang a Yong BAI. An Overview of Topology Control Mechanisms in Multi-Radio Multi-Channel Wireless Mesh Networks. *EURASIP Journal on Wireless Communications and Networking* [online]. 2012, 2012(1), 324- [cit. 2017-03-02]. DOI: 10.1186/1687-1499-2012-324. ISSN 1687-1499. Dostupné z: http://jwcn.eurasipjournals.springeropen.com/articles/10.1186/1687-1499-2012-324

[6] U. CHAUDHRY, Aizaz. Wireless Mesh Networks - Efficient Link Scheduling, Channel Assignment and Network Planning Strategies: *Channel Assignment Using Topology Control Based on Power Control in Wireless Mesh Networks* [online]. 1. Ottawa: InTech, Chapters, 2012 [cit. 2017-03-12]. ISBN 978-953-51-0672-2. Dostupné z: http://www.intechopen.com/books/wireless-mesh-networks-efficient-link-scheduling-channel-assignment-and-netw

[7] LINAN COLINA, Antonio, Alvaro VIVES, Antoine BAGULA, Marco ZENNARO a Ermanno PIETROSEMOLI. *IoT in five Days* [online]. Rev 1.1. Sweeden: E-Book, 2016 [cit. 2017-03-12]. Dostupné z: https://github.com/marcozennaro/IPv6-WSN-book/releases/

[8] SINGH, Santar Pal a S.C. SHARMA. A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks. *Procedia Computer Science* [online]. 2015, 45, 687-695 [cit. 2017-03-12]. DOI: 10.1016/j.procs.2015.03.133. ISSN 18770509. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1877050915003695

[9] On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management. In: *OPUS* [online]. Sydney: University of Technology Sydney, 2007 [cit. 2017-03-15]. Dostupné z: https://opus.lib.uts.edu.au/handle/10453/19594

[10] MAHGOUB, Imad a Mohammad ILYAS. *Sensor Network Protocols* [online]. 20141112. Boca Raton, Florida, U.S.A.: CRC Press, 2016 [cit. 2017-03-16]. ISBN 978-1-4200-0634-6. Dostupné z: https://books.google.cz/books?id=VT8qBgAAQBAJ

[11] AL-KARAKI, J.N. a A.E. KAMAL. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications* [online]. 2004, 11(6), 6-28 [cit. 2017-04-11]. DOI: 10.1109/MWC.2004.1368893. ISSN 1536-1284. Dostupné z: http://ieeexplore.ieee.org/document/1368893/

[12] MAHALIK, N. P. Sensor networks and configuration: fundamentals, standards, platforms, and applications. New York: Springer, c2007. ISBN 3-540-37364-0.

[13] RANA, Jigish, Sangeeta VHATKAR a Mohommad ATIQUE. Comparative Study of PEGASIS and PDCH Protocols in Wireless Sensor Network. *International Journal of Computer Applications* [online]. 2015, ICWET 2015(2), 13-18 [cit. 2017-04-27]. Dostupné z: http://research.ijcaonline.org/icwet2015/number2/icwet5023.pdf

[14] KUMAR, Prabhat, M.P. SINGH a U.S. TRIAR. A Review of Routing Protocols in Wireless Sensor Network. *International Journal of Engineering Research & Technology* [online]. 2012, 2012(1), 1 - 14 [cit. 2017-04-30]. ISSN 2278-0181. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.680.7855&rep=rep1&type=pdf

[15] SHYJITH, M.B a V.K. RESHMA. GOAFR: An Optimal Algorithm for Geographic Routing In Wireless Sensor Networks. *International Journal of Computer Networks and Wireless Communications* [online]. 2012, 2(2), 131 - 135 [cit. 2017-04-30]. ISSN 2250 - 3501. Dostupné z: http://www.ijcnwc.org/papers/vol2no22012/3vol2no2.pdf

[16] SPONSOR a LAN/MAN STANDARDS COMMITTEE OF THE IEEE COMPUTER SOCIETY. *IEEE standard for local and metropolitan area networks.* New York: Institute of Electrical and Electronics Engineers, 2011. ISBN 9780738166841.

[17] SEN, Jaydip. *Security and Privacy Issues in Wireless Mesh Networks: A Survey* [online]. s. 189-272 [cit. 2016-11-28]. DOI: 10.1007/978-3-642-36169-2_7. Dostupné z: http://link.springer.com/10.1007/978-3-642-36169-2_7

[18] PATHAN, Al-Sakib Khan. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET* [online]. 1. Boca Raton, Florida, USA: CRC Press, 2016 [cit. 2016-11-28]. ISBN 1439819203, 9781439819203. Dostupné z: https://books.google.cz/books?isbn=1439819203

[19] QIJUN GU, PENG LIU, SENCUN ZHU a CHAO-HSIEN CHU. Defending against packet injection attacks unreliable ad hoc networks. GLOBECOM '05. *IEEE Global Telecommunications Conference 2005* [online]. IEEE, 2005, , 5 pp.- [cit. 2016-11-27]. DOI: 10.1109/GLOCOM.2005.1577966. ISBN 0-7803-9414-3. Dostupné z: http://ieeexplore.ieee.org/document/1577966/

[20] SRP: What is it? *SRP: Industry standard strong password security* [online]. Stanford: Stanford University [cit. 2016-11-27]. Dostupné z: http://srp.stanford.edu/whatisit.html

[21] DR. CHEZHIAN, V.Umadevi, S. GEETHA a G. GEETHARAMANI. Survey on Secure Routing Protocols in MANET. *International Journal of Advanced Rese-arch in Computer and Communication Engineering* [online]. 2014, 2014(3), 7609 - 7615 [cit. 2016-11-27]. ISSN 2278-1021. Dostupné z: http://www.ijarcce.com/upload/2014/july/IJARCCE5B%20a%20kalyana%20Survey%20on%20Secure%20Routing%20Protocols%20in%20MANET.pdf

[22] Transport Layer Security (TLS). *High Performance Browser Networking* [online]. O'Reilly Media, 2013 [cit. 2016-11-28]. Dostupné z: https://hpbn.co/transport-layer-security-tls/

[23] INGHAM, KENNETH a STEPHANIE FORREST. A History and Survey of Network Firewalls. *University of New Mexico, Tech. Rep* [online]. 2012, 2012(2), 1 - 42 [cit. 2016-11-27]. Dostupné z: http://agl.cs.unm.edu/~treport/tr/02-12/firewall.pdf

[24] PATHAN, Al-Sakib Khan. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET* [online]. 1. Boca Raton, Florida, USA: CRC Press, 2016 [cit. 2016-11-28]. ISBN 1439819203, 9781439819203. Dostupné z: https://books.google.cz/books?isbn=1439819203

[25] KAUSHAL, Kanchan, Taranvir KAUR a Jaspinder KAUR. ZigBee based Wireless Sensor Networks. *International Journal of Computer Science and Information Technologies* [online]. 2014, 5(6), 7752 - 7755 [cit. 2017-05-05]. Dostupné z: `https://pdfs.semanticscholar.org/63f5/20df23db3979e362e0acd577881ca3db1c79.pdf`

[26] HILLMAN, Matt. An Overview of ZigBee Networks. In: *MWR InfoSecurity* [online]. United Kingdom, London [cit. 2017-05-05]. Dostupné z: `https://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf`

[27] OLSSON, Jonas. 6LoWPAN demystified. In: *Texas Instruments* [online]. [cit. 2017-05-06]. Dostupné z: `http://www.ti.com/lit/wp/swry013/swry013.pdf`

[28] DEVASENA, C. Lakshmi. IPv6 Low Power Wireless Personal Area Network (6LoWPAN) for Networking Internet of Things (IoT) – Analyzing its Suitability for IoT. *Indian Journal of Science and Technology* [online]. 2016, 9(30), 1 - 6 [cit. 2017-05-06]. ISSN 0974-5645. Dostupné z: `http://52.172.159.94/index.php/indjst/article/view/98730/72229`

[29] LIGNAN, Antonio. Zolertia RE-Mote platform. In: *Github* [online]. 2016 [cit. 2017-05-08]. Dostupné z: `https://github.com/Zolertia/Resources/wiki/RE-Mote`

[30] SmartRF06EB Board Support Package. In: *Texas Instruments* [online]. Texas Instruments Incorporated, 2013 [cit. 2017-05-08]. Dostupné z: `http://www.ti.com/lit/ug/swru327/swru327.pdf`

[31] SAKIRIS, Thanos. Contiki Processes. In: *Github* [online]. 2017 [cit. 2017-05-09]. Dostupné z: `https://github.com/contiki-os/contiki/wiki/Processes`

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

A/D	Analog to Digital
ACQUIRE	ACtive QUery forwarding In sensoR nEtworks
AP	Aplikačná podpora
APF	Aplikačný framework
APTEEN	Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol
ARAN	Authenticated Routing for Ad-hoc Networks
BS	Bezpečnostné služby
BSS	Bezdrôtové senzorické siete
CRC	Cyclic redundancy check
DoS	Denial of Service
DSN	Distribuovaná senzorická sieť
DSSS	Direct Sequence Spread Spectrum
FFD	Full-Function Device
FHSS	Frequency Hopping Spread Spectrum
GAF	Geographic Adaptive Fidelity
GEAR	Geographic and Energy Aware Routing
GOAFR	Greedy Other Adaptive Face Routing
HW	Hardware
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
JHP	Jemná prahová hodnota
LEACH	Low Energy Adaptive Clustering Hierarchy
MAC	Media Access Control
MCU	Microcontroller unit
NA	Neighbor Advertisement
NS	Neighbor solicitation
PAN	Personal area network
PCT	Private Communications Transport
PEGASIS	Power-Efficient Gathering in Sensor Information Systems
RA	Router Advertisement
RDC	Radio duty cycle
RERUM	REliable, Resilient and secUre IoT for sMart city applications

RFD	Reduced-Function Device
RREQ	Route request
RS	Router Solicitation
SAODV	Secure Ad hoc On-demand Distance Vector
SoC	System on Chip
SODMRP	Stable On-Demand Multicast Routing Protocol
SOP	Self Organizing Protocol
SPIN	Sensor Protocols for Information via Negotiation
SRP	Secure Remote Password
SSL	Secure Socket Layer
SV	Sieťová vrstva
SW	Software
TDM	Time Division Multipelxing
TEEN	Threshold-sensitive Energy Efficient sensor Network protocol
TI	Texas Instruments
TLS	Transport Layer Security
TPH	Tvrdá prahová hodnota
TTDD	Two-Tier Data Dissemination
WPAN	Wireless Personal Area Network
ZOZ	ZigBee objekt zariadenia

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I. POPIS SÚBOROV NA PRILOŽENOM DISKU

Text diplomovej práce:	*fulltext.pdf*
Zdrojové kódy aplikácie:	*prílohy/mqtt*
Zdrojové kódy Contiki:	*prílohy/contiki*