Západočeské univerzita v Plzni
Fakulta aplikovaných věd
Katedra informatiky a výpočetní techniky

Bakalářská práce

Síťové protokoly bezdrátových senzorických sítí

Plzeň, 2017 Marek Ľuptáčik

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a výhradně s citovaných pramenů.

V Plzni dne 28. 6. 2017

…….…….....

Marek Ľuptáčik

Místo této strany bude zadání práce.

Poděkování

Rád bych poděkoval svému vedoucímu balakářské práce panu Ing. Jiřímu Ledvinovi, CSc. za velkou trpělivost a odborné konzultace. Dále bych také rád poděkoval své ženě, rodině a přátelům za podporu při vypracování práce.

Abstract

Bachelor's thesis is focused on wireless sensor networks and their network layer.
The First part of the thesis describes network architecture and sensor node components. Furthermore, different network connection topologies commonly used in on wireless sensor networks, their limitations, properties and utilization are discussed.
Main emphasis on network protocols is being put in the second part of the thesis in which routing, various features, utilization and eventually advantages and disadvantages of specific network protocols are described. Finally, groups of protocols are evaluated based on their resistance against network attacks and their energy consumption.

Abstrakt

Bakalářská práce je zaměřena na bezdrátové senzorické sítě a jejich síťovou vrstvu. V první části práce je popsána architektura sítě a komponenta senzorického uzlu. Dále jsou rozebrány různé druhy topologií síťového připojení, obvykle využívané v bezdrátových senzorických sítích, jejich limitace, vlastnosti a využití.
Důraz na síťové protokoly je kladen ve druhé části práce, ve které jsou blíže popsány vlastnosti konkrétních síťových protokolů, jejich způsob směrování v síti, jejich výhody a nevýhody. Dále jsou skupiny protokolů zhodnoceny dle odolnosti proti síťovým útokům a porovnány dle spotřeby energie.

Obsah

1 Úvod

Bezdrátové senzorické sítě jsou sítě, které sledují svoje okolí a získávají cenné informace pro uživatele. Sítě mohou nejenom získávat data, ale i ovládat okolí pomocí externího zařízení. Využití těchto sítí je opravdu široké, od použití v zemědělství až po zdravotnictví nebo armádu.

Tato práce je zaměřena na architekturu uzlu a sítě, druhy topologií, popis síťových protokolů, jejich obranu proti útokům a spotřebu energie. V kapitole architektura budou stručně popsány komponenty uzlu a síťové vrstvy. Dále jsou popsány různé topologie, jejich výhody, nevýhody a využití.

V hlavní částí práce je popis síťové vrstvy se zaměřením na protokoly. Síťová vrstva zajišťuje směrování dat v síti. Tato vrstva navazuje na vrstvu linkovou a napojuje se na vrstvu transportní. V bezdrátových senzorických sítích se síťová vrstva musí vypořádat s novými problémy, které se liší od klasických bezdrátových sítí. Objevují se tak problémy jakými jsou omezené zdroje energie, časté změny v topologii nebo velký počet uzlů. Různé aplikace senzorických sítí vedou k různým řešením a potřebám (různé topologie, náročnost na energii, rychlost nebo odezvu). Na senzorické uzly je kladen také vysoký tlak. Některé uzly detekují důležité informace (např. o lesních požárech), jiné uzly detekují méně důležité informace (např. otevírání a zavírání dveří). Jejich odolnost vůči vnějším vlivům je pečlivě vyvíjena a zkoumána.

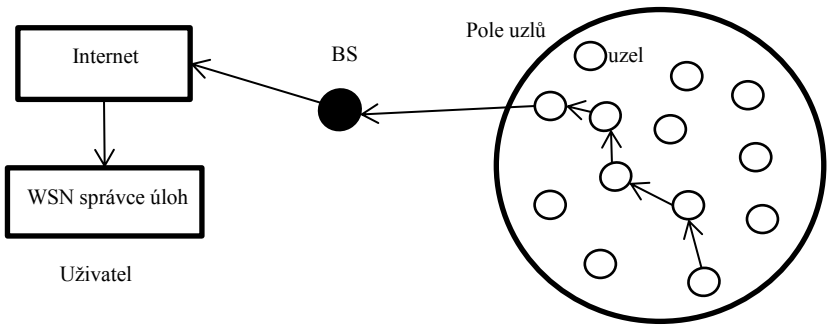
V kapitole o síťových protokolech budou popsány nejvíce citované a známé protokoly, způsob směrování těchto protokolů, výhody a nevýhody. Dále budou protokoly popsány z hlediska síťových útoků a jejich obrana proti nim. A také srovnání protokolů z hlediska spotřeby energie.

2 Úvod do bezdrátových senzorických sítí a obecné pojmy

Poznámka: V práci jsou pojmy data, paket a zpráva plynule zaměňovány kvůli podobnému významu. Pojem je vybrán tak, aby nejlépe vystihoval důraz na charakteristiku pojmu. Zpráva je složena z jednoho nebo více paketů. Paket je jeden přenášený blok složený ze řídících a uživatelských dat. Data se tedy vysílají pomocí paketů. Při použití pojmu data je kladen důraz na datovou složku paketů, kdežto při použití pojmu paket je důraz na řídící složku paketů. Pojem zpráva je použita v obecných případech, kdy není potřeba rozlišovat důležitost jedné nebo druhé složky paketů.

2.1 Základnová stanice a uzly

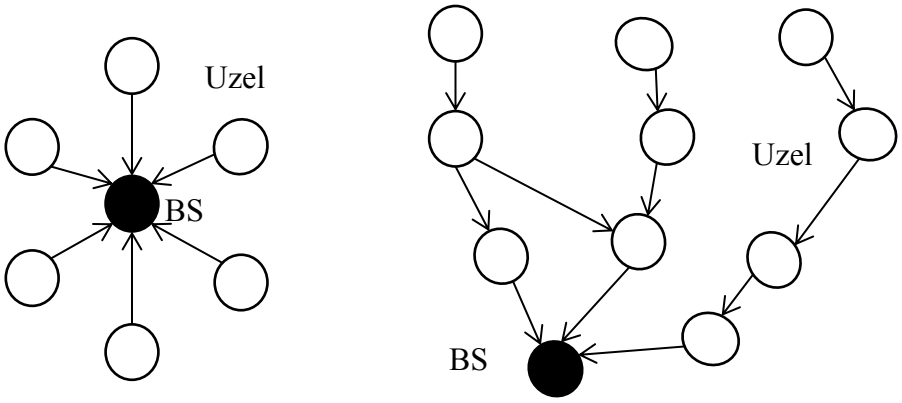
Bezdrátová senzorická síť (dále jen WSN, z anglické zkratky wireless sensor network) se skládá z uzlů a alespoň jedné základnové stanice (někdy také nazývané sink, sink node nebo base station, na obrázcích použita zkratka BS). Uzly jsou vybaveny kontrolerem, senzorem, baterií, případně akumulátorem. Zkoumají a sbírají data z prostředí a tato data mohou dále zpracovávat. Všechny uzly mohou mít stejný nebo různý hardware - výkonnější hardware pro důležitější pozice. Alespoň jeden z uzlů je základnovou stanicí (základnových stanic může být v síti i více, závisí při tom na aplikaci a funkci sítě), která je ve většině případech vybavena výkonnějším hardwarem, včetně kvalitnějšího zdroje energie než ostatní uzly. Funguje jako brána mezi uzly a koncovým uživatelem. Základnová stanice také zpracovává všechna data ze sítě a zpracovává uživatelské dotazy. Geografická pozice základnové stanice je velmi důležitá, protože nevhodné umístění stanice může vést k velkým ztrátám energie uzlů.



Obr. 2.1. – Model WSN sítě

Přeskok – hop

Přeskok je směrování paketu sousedním uzlem do cíle. Přeskoků může být i více. Směrování jednoho paketu se tak zúčastní více uzlů. Síťové protokoly se snaží najít cestu, která by ve výsledku měla nejnižší spotřebu energie pro přenos, tedy aby celková spotřeba energie všech uzlů byla co nejnižší. Ačkoli by se zdálo výhodné komunikovat přímo se základnovou stanicí, tento způsob je energeticky velmi náročný.



Obr. 2.2. – Vlevo jeden model s jedním skokem a vpravo model s více přeskoky

2.2 Základní problémy síťové vrstvy WSN

Energie

Největším problémem bezdrátových senzorických sítí jsou omezené zdroje energie. Každý uzel je vybaven zařízením pro uchování energie, baterií nebo akumulátorem. Některé uzly nepotřebují dlouhodobý přísun energie, pro jiné je třeba zajistit energii na několik dní, týdnů a někdy i déle. V některých případech je baterie možno vyměnit nebo dobíjet (např. senzory ve skleníku nebo senzory na otevřeném prostoru dobíjet pomocí solární energie). Pro jiné uzly není dobití baterie možné.

Škálovatelnost

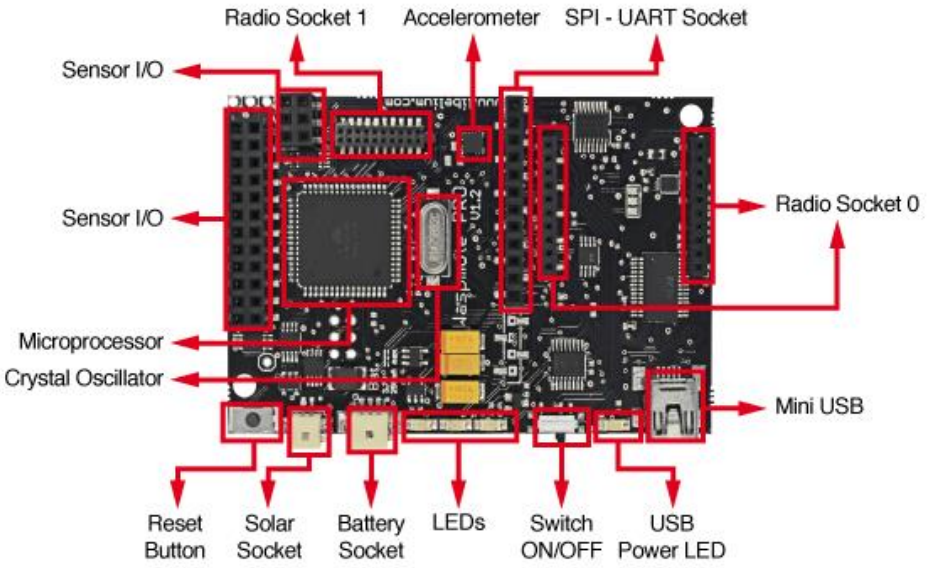
Některé aplikace potřebují velký počet uzlů v síti - stovky, tisíce i více. Směrování a zpráva sítě musí být navrženy tak, aby síť mohla fungovat i při větším počtu uzlů. Je pak obtížné efektivně využít protokol jako TDMA (Time Division Multiple Access) pro komunikaci celé sítě. Protokol přiřazuje stejná časová kvanta na vysílání na sdíleném kanálu.

Bezpečnost

Bezpečnost ve WSN může být velmi důležitá. Závisí při tom na důležitosti sítě a dat. Některé aplikace obsahují velmi citlivá data, jejichž zneužití by mohlo mít katastrofické následky, např. aplikace v armádě nebo zdravotnictví. Je třeba využívat bezpečnostní protokoly, bez kterých jsou WSN naprosto bezbranné proti útokům.

3 Architektura senzorického uzlu

Uzel je nejdůležitější součástí WSN. Skládá se z několika hardwarových komponentů. Mezi základní komponenty patří mikrokontroler, paměť, komunikační zařízení, zdroj energie a senzory. Uzly obsahují senzory, které monitorují okolí. Snímají tak veličiny jako teplotu, tlak nebo čas. Zařízení mohou být rozprostřena na velmi malé ploše, s hustotou rozdělení např. 20 uzlů na m^3. Uzly ve WSN mají dvě funkce: sběr dat z prostředí a komunikaci s ostatními uzly, tedy směrování paketů sítí. Níže je uveden příklad uzlu Waspmote.



Obr. 3.1. – Senzorový uzel Waspmote [35]

3.1 Kontroler

Nejdůležitější součástkou uzlu je mikrokontroler. Součástí mikrokontroleru je procesor, flash paměť programu, RAM paměť pro uložení dat, konvertor analogového signálu na digitální, časovače, jednotka pro obsluhu přerušení. Jeho úkolem je zpracovávat data a kontrolovat funkčnost ostatních komponentů uzlu. Na spotřebu energie mikrokontrolerů je ve WSN kladen velký důraz. Mikrokontrolery ve WSN mají přibližně 10 krát menší spotřebu energie než standardní mikrokontrolery [2,14].

3.2 Baterie

Napájení a spotřebu energie je potřeba vyvážit tak, aby uzlu vydržela zásoba energie potřebnou dobu (v extrémních případech i několik let). Proto je nutnost snížit spotřebu energie při operacích senzoru na minimum v kombinaci s velmi energicky nenáročným hardwarem. Pokud se senzor vyskytuje v odlehlých oblastech bez přístupu k senzorům, velmi důležité je nabíjení akumulátoru. Nejčastěji používané metody dobíjení jsou solární energie, teplotní rozdíly nebo vibrace. Nevýhodou akumulátoru je mnohem větší samovybíjení než u baterií. Baterie mají malý svodový proud. Některé baterie se dají i dobíjet, ale nejsou v tomto směru tak efektivní jako akumulátory.

Běžně se pro senzory využívají baterie nebo akumulátory alkalické, lithiové nebo nikl-metal hydriodové. Alkalické baterie jsou levné a mají vysokou kapacitou energie, ale se snižující se kapacitou už od počátku využívání baterie. Lithiové baterie mají v poměru s alkalickými větší kapacitu energie na m^3 a stálé napětí, které se snižuje až při konci životnosti baterie [13, 14]. Navíc mohou fungovat až do teplot okolo -40°C. Nikl-metal hydridové baterie jsou cenově přijatelné s vysokou kapacitou energie. Nevýhodou je vysoké samovybíjení při pokojových teplotách (15-30% za měsíc) [34]. Při nízkých teplotách začínají baterie ztrácet kapacitu. Lze využít také další baterie na bázi niklu.

3.3 Přenos

Pro přenos se nejčastěji využívají radiové vlny. Lze použít i jiné možnosti komunikace, avšak síť musí být k tomu dostatečně uzpůsobena (např. optická komunikace). Používají se zpravidla frekvence 433MHz, 868MHz nebo 2,4GHz v pásmu ISM. Závisí také na přenosové rychlosti zařízení - zpravidla čím větší přenosová rychlost, tím více je zařízení energeticky náročné. Čím vyšší frekvence, tím menší dosah při daném výkonu.

Uzel senzorické sítě se nachází v jednom ze čtyř stavů: odesílání, příjem, nečinnost a spánek. Odesílání je stav, kdy je vysílač aktivní – vysílá data. Příjem je stav, kdy je aktivní přijímač a přijímá zprávy. Nečinnost je stav kdy je radio připraveno přijímat zprávy, ale momentálně nic nepřijímá. Spánek je stav, kdy je rádio úplně vypnuto, není tedy možnost poslat uzlu data [2]. Přecházet mezi těmito stavy je důležité z hlediska spotřeby energie. Pokud by byl přenos nepřetržitě zapnut, došlo by ke zbytečně velké spotřebě energie. Rozdíl mezi stavy kdy radio přijímá

a kdy je ve stavu nečinnosti, není zanedbatelný z hlediska spotřeby energie, proto je mnohdy nejlepší varianta radio vypnout úplně.

Externí paměť a interní paměť

Interní paměť, která je součástí mikrokontroleru, je flash paměť. Interní paměť slouží k uložení programu a interních dat. Naměřená data se nejčastěji ukládají do RAM (Random-Access Memory) paměti procesoru. Pro dlouhodobé uložení dat nebo uložení velkého objemu dat se používá externí paměť typu EEPROM (Electrically Erasable Programmable Read-Only Memory) nebo FLASH. Existují i paměti typu FRAM (Ferroelectric Random Access Memory), které se chovají jako paměti typu RAM, ale uchovávají si informaci i po vypnutí napájení. [13]

3.4 Senzor

Senzory jsou součástky, které snímají data ze svého okolí (mohou využívat i technologii MEMS[1]-MicroElectroMechanical Systems). Měřenou neelektrickou veličinu převádí většinou na změnu odporu, změnu kapacity nebo využívají piezoelektrický jev. Moderní senzor je integrovaný obvod skládající se ze senzorické části a elektronické části. Senzor převádí naměřené hodnoty nebo události z reálného světa na signál, který může být měřen a dále analyzován. Převádí energii z fyzického světa na elektrickou energii, která může být předána do výpočetního systému. Elektrický signál je modifikován (např. filtrování, zesilování, izolace, atd.) pro lepší převod z analogového signálu na digitální[1]. Digitální signál je dále zpracováván. Součástí senzoru může být i digitální sběrnice. Ke sběrnici pak lze připojit více senzorů najednou.

Senzory se liší podle druhu snímané veličiny. Existuje mnoho různých druhů senzorů od měření teploty až po poslech zvuku. Analogový signál, který je vytvořen senzorem, se musí převést na digitální, avšak některé senzory mohou rovnou převést naměřené hodnoty na digitální signál (např. stupně Celsia). Senzory se dělí na pasivní a aktivní senzory.

Pasivní senzory negenerují energii a pouze měří energii z vnějšího světa, mění tak kapacitu, elektrický odpor nebo indukčnost. Příkladem pasivního senzoru je tenzometr. Tenzometr měří mechanické napětí na povrchu měřeného objektu prostřednictvím deformace a mění tak svůj odpor. Aktivní senzory generují energii

[1] Technologie společné integrace mechanických a elektronických struktur.

z vnějšího světa. Příkladem senzoru tohoto typu je piezoelektrický jev, při kterém krystal generuje elektrické napětí, pokud je vystaven působení tlaku. Dalším příkladem je indukční senzor, který využívá cívky a oscilátoru. Funguje na principu změny činitele jakosti jádra při přiblížení kovového materiálu.
Součástí uzlu může být také mechanismus, pomocí kterého uzel reaguje a ovlivňuje svoje okolí na základě naměřených hodnot. Musí mít připojen externí zdroj energie, pomocí které může vyvolávat např. světlo, zvuk nebo tlak pro otevírání dveří, různé průtokové senzory nebo řízení mechanických částí atd.

3.5 Čítače a časovače

Použití čítače a časovače se velmi liší od druhu a cíle WSN sítě. Používají se zejména pro algoritmy ve směrovacích nebo MAC protokolech, kde se počítá např. odezva nebo doba okna určená pro odesílání. Dále časovač může být využit pro snímání senzorem. Mnohdy je určitý prvek nutno zkoumat pouze jednou za delší časovou jednotku, např. 10 sekund. Čítač může počítat četnost naměřených událostí pro spolehlivá data.

3.6 Obecné výhody a nevýhody WSN

Výhody:

- Konfigurace lze provést bez pevné infrastruktury,
- vhodné pro špatně dostupné lokace,
- levná implementace.

Nevýhody:

- Složité zabezpečení proti útokům,
- nízký výpočetní výkon,
- více náročné na instalaci než kabelová síť,
- snadno ovlivněno prostředím (zdi, mikrovlny atd.) [1].

4 Architektura sítě

Uzly ve WSN mají dvě funkce: za prvé sběr dat z prostředí, případně jejich zpracování a za druhé komunikaci s ostatními uzly, tedy směrování paketů sítí. Každý senzor má vlastnosti na to, aby mohl posílat svoje data rovnou do základnové stanice, která se chová jako brána mezi WSN a sítí uživatele, ale ve většině případů je to neefektivní a nevhodné. Existuje mnoho možností implementace WSN, lze mít více základnových stanic pro více koncových uživatelů z různých sítí nebo připojit základnovou stanici rovnou koncovému uživateli (není třeba použít síť pro spojení základnové stanice a koncového uživatele). Pro efektivnější využití energie lze pakety směrovat do cíle pomocí sousedních uzlů.

4.1 Protokolový zásobník

Nejčastěji se ve WSN používá redukovaný ISO-OSI model. Model využívají všechny uzly sítě, včetně základnové stanice. Namísto sedmi vrstev je potřeba pouze pět - fyzická vrstva, linková vrstva (také označováno jako spojová vrstva), síťová vrstva, transportní vrstva a aplikační vrstva.

Dále WSN architektura obsahuje vrstvy, tzv. planes, což jsou vrstvy, které spravují síť a napomáhají efektivnějšímu běhu sítě.

Vrstva správy úloh (task management plane) plánuje úkoly pro danou oblast a rozlišuje, které uzly jsou zapnuté nebo vypnuté. Úkoly jsou rozdělovány podle kapacity energie uzlů.

Vrstva správy pohybu (mobility management plane) detekuje pohyb uzlů, umožňuje uzlům sledovat svoje sousední uzly a detekovat změny sousedních uzlů. Vrstva správy energie řídí spotřebu energie uzlů. Např. vypínání a zapínání vysílače nebo broadcast při malé energii (senzor se dále nezúčastňuje směrování a zbylou energii používá na snímání okolí) [6, 18].

4.2 Fyzická vrstva

Fyzická vrstva umožňuje uzlům přenášet zprávy přes bezdrátovou síť. Převádí proud bitů na signál, který vyhovuje bezdrátovému kanálu. Dále se stará o výběr frekvence, generování nosné frekvence, detekce signálu, modulace a šifrování.

Nejčastěji se používají radiové frekvence pro bezdrátový přenos. Další typy přenosu

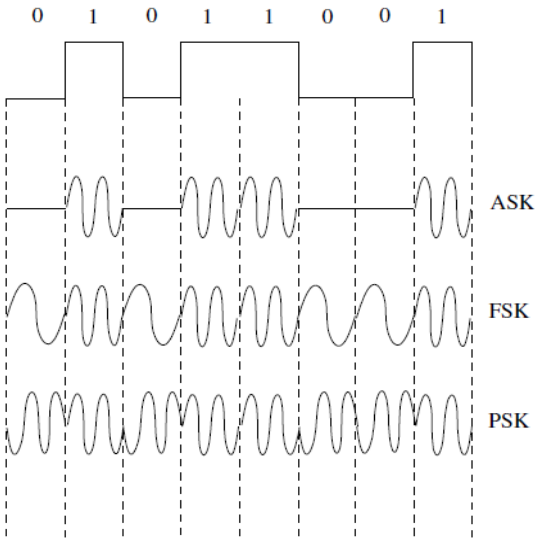
jsou optická komunikace, komunikace pomocí magnetické indukce nebo akustická komunikace.

Přenos mezi uzly (přenos mezi vysílačem a příjímačem)

Pro přenos se používají tři komponenty: kóder kanálu a modulátor, které jsou součástí vysílače, dekodér kanálu a demodulátor, které jsou součástí příjímače a komunikační kanál. Fyzická vrstva vykonává čtyři činnosti: kódování zdrojového signálu (komprese dat), kódování kanálu, prokládání a modulace, propagace bezdrátového signálu [4].

Senzor produkuje analogový signál. Signál musí být převeden na diskrétní signál (pro neztrátovost signálu je potřeba použít vzorkovací frekvenci vyšší než dvojnásobek nejvyšší harmonické složky vzorkovaného signálu). Po vzorkování je signál převeden na binární proud. Poté následuje kódování kanálu. Cílem je vytvořit signál dostatečně silný tak, aby nebyl ovlivňován rušením, případně umožnit opravu dat při poškození chyby v signálu.

obr 4.1 – Typy modulace ASK, FSK a PSK



Dále následuje modulace. Signál je přenášen analogově bezdrátovou komunikací, proto je třeba digitální signál modulovat na analogový. Základní signál je přetvářen pomocí nosného signálu na modulovaný signál. Používají se tři základní způsoby modulace: ASK (Amplitude shift keying – klíčování amplitudovým posuvem), FSK (Frequency Shift Keying - Klíčování frekvenčním posuvem), PSK (Phase Shift Keying - Klíčování fázovým posuvem) [6].

Nejčastěji využívanou formou ASK je tzv. OOK (on-off keying), kde logická jednička značí přítomnost nosného kmitočtu a logická nula nepřítomnost, viz. Obr. 4.1. V binární FSK je modulace založena na dvou různých frekvencích přiřazených binární nule

a jedničce, viz. Obr. 4.1. PSK je založena na změně fáze, která reprezentuje logickou nulu nebo jedničku, viz. Obr. 4.1.
WSN využívá pro komunikaci ISM pásmo, kde signál mohou rušit ostatní zařízení (WLAN, Bluetooth atd.). Dosah závisí na typu použité modulace, výkonu vysílače a citlivosti přijímače.

4.3 Linková vstva – MAC (media access control)

MAC je velmi důležitým prvkem ve WSN co se spotřeby energie týče. Spotřeba energie z přenosu dat (vysílání, příjímání, poslech) může být 80 až 90% z celé spotřeby energie uzlu [4]. Proto je potřeba minimalizovat plýtvání energie na kolizi a odposlech zpráv, poslech a režii protokolu.
Linková vrstva se stará o přenos v bezdrátové síti sdílené více zařízeními. Zařízení (v případě WSN vysílač) mohou vysílat najednou a došlo by tak k chybě. Řídí, který uzel bude mít možnost vysílat, na jak dlouho a na jaké frekvenci a také odstraňují vznik kolize přidělením časového slotu pouze danému uzlu. V linkové vrstvě existují dva druhy protokolů. Plánovací protokoly a protokoly náhodného přístupu.

Plánovací protokoly
Plánovací protokoly jsou typem protokolů zabezpečujících sdílený kanál. Každý uzel má slot, ve kterém je mu umožněno vysílat. Mimo tuto vysílací periodu může rádio přejít do režimu spánku. Nevýhodou těchto protokolů může být obtížnost synchronizace při větších počtech uzlů v síti, tedy nemožnost přesouvat vysílací okna mezi uzly. Tato nevýhoda se může dále prohlubovat se změnami v síti, např. topologii. Tyto nevýhody lze do určité míry vyřešit dynamickým přiřazováním oken. Přiřazování probíhá na základě algoritmu, např. podle algoritmu round robin.
Typické protokoly pro statické přiřazování jsou TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) a CDMA (Code Division Multiple Access).
V protokolu TDMA, každý uzel má vlastní časové slot, ve kterém může vysílat. Protokol FDMA umožňuje každému uzlu vysílat na jiné vysílací frekvenci a tím využívat sdílený kanál současně více uzly. Protokol CDMA funguje podobně jako FDMA. Narozdíl od FDMA rozlišuje zprávy pomocí kódování.

Protokoly náhodného přístupu

Protokoly tohoto typu nemají fixní přiřazování. Každý uzel se může pokusit vysílat nezávisle na ostatních uzlech. Protokoly poskytují algoritmy na redukování počtu kolizí a zotavení se z nich.

Jedním z nejvíce využívaných protokolů této skupiny je protokol CSMA. Prvky sítě při využívání protokolu CSMA musí nejprve zjistit, jestli je vysílací kanál volný, a až poté mohou vysílat. Po vysílání počkají na ACK paket (acknowledgement paket). Pokud paket přijde v nastaveném čase, vše proběhlo v pořádku. Pokud ACK paket nepřijde, nastala kolize. Uzel musí vyčkat náhodný čas z intervalu. Existují modifikace protokolu CSMA, jako např. CSMA/CA (CA - collision avoidance), které umožňují kolizím předcházet. Protokol ALOHA je velmi podobný protokolu CSMA. Uzly při použití protokolu ALOHA na rozdíl od protokolu CSMA nezjišťují, jestli je vysílací kanál volný nebo není.

4.4 Síťová vrstva

Síťová vrstva se stará o směrování paketů napříč sítí. Vytváří cesty mezi zdrojovým uzlem a cílovým. Kvůli charakteristikám ve WSN vznikají nové překážky a problémy pro síťovou vrstvu. Cílem síťové vrstvy je najít nejvhodnější cestu pro přenos paketů. Vhodná cesta může být rozdílná, závisí přitom na typu aplikace a použitých protokolech. Charakteristika vhodné cesty může být např. minimální spotřeba energie na přenos zpráv, nejrychlejší cesta nebo cesta, která využívá jen uzly s energií nad určitou hranicí.

Největší roli ve směrování hraje základnová stanice, do které směřují veškerá data. Výhodná pozice může velmi ulehčit směrování a snížit tak spotřebu energie nebo odezvu. Více o síťových protokolech a jejich rozdělení naleznete v kapitole 6. a 7.

4.5 Transportní vrstva

Pro úspěšný chod sítě je potřeba zajistit spolehlivý přenos mezi všemi prvky sítě. Pro WSN není vhodné použít standardní transportní protokoly jako v klasických bezdrátových sítích (UDP, TCP), a to zejména kvůli neefektivitě spojení konec-konec (přeloženo z anglického termínu end-to-end). Pro WSN je efektivnější využití přeskokového principu. Je potřeba použít jiné protokoly, které jsou více uzpůsobeny charakteristikám WSN.

Protokoly se dělí na dvě skupiny: upstream (uživatel-základnová stanice) a downstream (základní stanice-uživatel)[6]. Protokoly transportní vrstvy se starají o kontrolu zahlcení, spolehlivý přenos a multiplexování.

RMST (Reliable Multi-Segment Transport) je prvním transportním protokolem vyvinutým pro WSN. Protokol je vyvinut pouze pro protokol síťové vrstvy Directed Diffusion. Protokol zvládá pouze dvě ze tří výše popsaných funkcionalit, chybí kontrola zahlcení.

PSFQ (Pump Slowly, Fetch Quickly) je protokol zaměřený na komunikaci základnová stanice-uzel.Toto spojení se používá pro řízení sítě. Protokol vykonává tři funkce. Základnová stanice rozesílá pakety uzlům, každý uzel čeká určitou dobu před odesláním své odpovědi. Tato funkce se nazývá pumpa. Další funkcí je obnova dat, tzv. fetch (v českém jazyce přinést). Při ztrátě paketu uzly provedou obnovu ztraceného paketu od svých sousedních uzlů, kterým paket došel v pořádku. Jako třetí funkci PSFQ vykonává hlášení uživateli, pomocí kterého lze síť lépe řídit. Dalším protokolem je např. ESRT (Event-To-Sink Reliable Transport) [6,18].

4.6 Aplikační vrstva

Aplikační vrstva zajišťuje konverzi dat do podoby vhodné pro aplikaci a zajišťuje konverzi aplikačních dat do formátu vhodného pro přenos sítí.

Kódování zdrojového signálu (komprese dat)

Pokaždé, když chce uzel posílat paket, jako první krok se provede kódování zdrojového signálu (popsáno též v kapitole fyzická vrstva). Komprese může být bezeztrátová, při které se redukuje velikost paketu, ale data zůstanou neporušená. Druhý typ komprese je ztrátová komprese, při které jsou už data pozměněna, ale dochází k mnohem větší redukci velikosti paketu. Ve WSN se využívá bezeztrátový typ komprese, a to kvůli důležitosti naměřených dat senzory. Některá naměřená data potřebují naprostou přesnost a ztrátová komprese by mohla tuto přesnost poškodit. Ztrátová komprese je také náročnější na výpočet než bezeztrátová komprese. Protokoly spadající do této skupiny jsou např. Sensor LZW (Lempel-Ziv Welch) nebo DSC (Distributed Source Coding). Senzor LZW protokol je založen na slovníkové kompresi. Protokol vybírá řetězec a převádí ho na symbol ze slovníku [6].

Zpracování dotazu

Uživatel řídí síť pomocí dotazů na základnovou stanici, která slouží jako brána mezi uživatelem a uzly. Uzly vytvářejí nepřetržitě data, která reprezentují ve většině případech reálné události. Je potřeba k nim také přistupovat v reálném čase, a to nejen z důvodu přesnosti dat, ale také omezené kapacity disku základnové stanice. Existují různé způsoby dotazů: podle typu zpracování dotazu, podle času, podle vybrané skupiny.

Podle typu zpracování dotazu závisí jakým směrem proudí data. Při formě zpracování dotazu push uzly propagují svoje naměřená data, která mohou být uložená přímo v uzlech nebo na základnové stanici. Při formě zpracování dotazu pull začíná dotaz u základnové stanice, která vybírá určitý atribut nebo událost ke sledování. Při zpracování dotazu push-pull se podílejí na dotazování jak senzory, tak základnové stanice. Další dotazy umožňují např. nepřetržitý monitoring určité události, vybírání předešlých naměřených hodnot, data-centrické dotazy, dotazování jen na určitou oblast sítě nebo dotazy reálného času. Typické protokoly, které vykonávají tyto funkce, jsou např. COUGAR nebo SQTL (modifikace SQL) [6].

Správa sítě

Jako každou síť je potřeba monitorovat i WSN. Administrátorovi nebo uživateli by měly být dostupné informace o síti – pokrytí sítě, připojení, topologie a také informace o uzlech, stavu vysílače, kapacitě baterie, využití paměti, atd.

Existují tři různé způsoby řízení sítě: pasivní, reaktivní a proaktivní. Pasivní monitoring sítě znamená, že monitoring probíhá a data jsou zpracovávána na základnové stanici. Při reaktivním monitorování sítě závisí na zpracování dat přímo v uzlech. Monitorování sítě probíhá až v případě, že nastane nějaká důležitá událost. Proaktivní monitorování sítě znamená, že monitorování probíhá neustále a data jsou zpracovávána v reálném čase. Monitorování a správu sítě zajišťuje např. protokol MANNA (Management Architecture for Wireless Sensor Networks) [6].

4.7 Operační systémy WSN

Operační systém vytváří vrstvu mezi hardwarem a aplikací pro vzájemnou komunikaci, zajišťuje základní programovou vrstvu uzlu. Základní funkcemí operačního systému je plánování, které determinuje, jak budou procesy organizovány a priorizovány ve frontě.

WSN má dva způsoby plánování: round robin a plánování na základě fronty, které může být např. FCFS (First Come First Served) nebo SJF (Shortest Job First). Další důležitou funkcí je alokování paměti. Ve WSN je paměť velmi drahým zdrojem. Operační systém rozhoduje kolik a na jak dlouho bude paměť přidělena. Může jí přidělovat buď staticky (pevná velikost přidělené paměti) nebo dynamicky. Dynamické přidělení paměti se využívá, když není předem známa potřebná velikost paměti, může se během běhu programu zvětšovat. Mezi další důležité funkce patří správa datových typů, správa zásobníku, systémové volání, správa přerušení a správa vláken. Mezi nejvíce používané operační systémy patří TinyOS a Contiki [2, 32, 33].

4.7.1 TinyOS

TinyOS je monolitický operační systém, který umožňuje softwaru přímý přístup k hardwaru. Operační systém se skládá z komponent, nad kterými lze vykonávat tři operace - události, příkazy a úkoly. Komponenta mohou rozhraní poskytovat nebo využívat rozhraní jiných komponent. Komponenta jsou nakonfigurována tak, aby bylo jasné, jaké rozhraní komponent je využito ostatními komponentami. Lze pak konfiguraci komponent nastavit do hierarchického způsobu. Operace nad komponentami jsou plánovány podle plánovače FIFO (First In First Out). TinyOS využívá událostmi řízené jádro, které je vhodné pro aplikace vyžadující velkou responsivitu [32, 33].

4.7.2 Contiki

Contiki je modulární operační systém. Skládá se z jádra, knihoven, sady procesů. Komunikace mezi procesy a operačním systémem vždy prochází přes jádro. Oproti TinyOS, který je statickým systém, aplikace musí alokovat všechny zdroje před během programu. Contiki využívá dynamický systém. Aplikace mohou alokovat a dealokovat zdroje přímo za běhu. Contiki, stejně jako TinyOS, využívá událostmi řízené jádro, ale lze připojit různé knihovny pro podporu více vláknových procesů [32, 33].

5 Typy topologií

Topologie je důležitým aspektem WSN, protože cílená topologie zlepšuje spotřebu sítě a přispívá k správnému chodu sítě. WSN Topologie nepracuje pouze s pozicemi uzlů, ale i s jejich stavy (aktivní, spánek atd.) Protokoly napříč vrstvami jsou závislé na určité topologii (např. síťové protokoly, používající informaci o pozici uzlů). Různé topologie mohou být efektivní v různých situacích. Popsané topologie nejsou fyzickými topologiemi, ale pouze logickými topologiemi. To znamená, že topologie se takto jeví pouze pro uživatele. Reálně uzly komunikují pomocí broadcastu s nasteveným indentifikátorem pro uzel, kterému je zpráva určena.

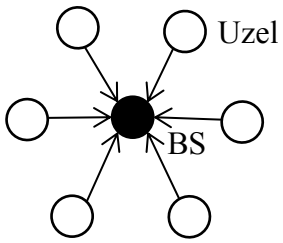
5.1 Typy jednoúrovňových topologií

V těchto topologiích mají všechny uzly stejnou roli v síti. Úkol uzlů je směrovat data do základnové stanice pomocí sousedních uzlů. Neexistují předem definované cesty. Směrovací protokoly musí tedy najít optimální cestu pomocí jednoho nebo více kritérií (např. kapacita baterie, počet skoků). Cesty se vytvářejí podle implementovaného směrovacího protokolu.

Nejjednodušší protokol je záplavový algoritmus, se kterým ale přichází řada problémů (např. imploze a překrývání). Dalšími typickými směrovacími protokoly pro jednoúrovňové topologie jsou: SPIN (Sensor Protocols for Information Via Negotiation), Directed Diffusion nebo Rumor Routing.

5.1.1 Topologie hvězdy

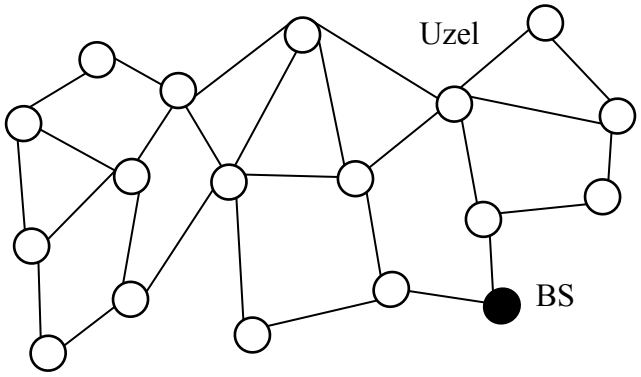
Obr 5.1. – Topologie hvězdy.



Topologie hvězdy je nejjednodušší topologií ve WSN. Jedná se o jedno-skokovou síť(single hop). Hvězda je strukturovaná tak, aby ve středu topologie byla základnová stanice, která slouží jako server. Uzly pak nemohou spolu navzájem komunikovat a fungují pouze jako klient. Tato topologie je efektivní pouze při malých vzdálenostech mezi uzly a základnovou stanicí (desítky metrů) a při malých počtech uzlů. Pokud tyto požadavky nejsou splněny, síť s touto topologií by mohla být velice neefektivní co se týče spolehlivosti přenosu, redundance dat, vysoké spotřeby energie, atd. [11, 30].

5.1.2 Smíšená topologie

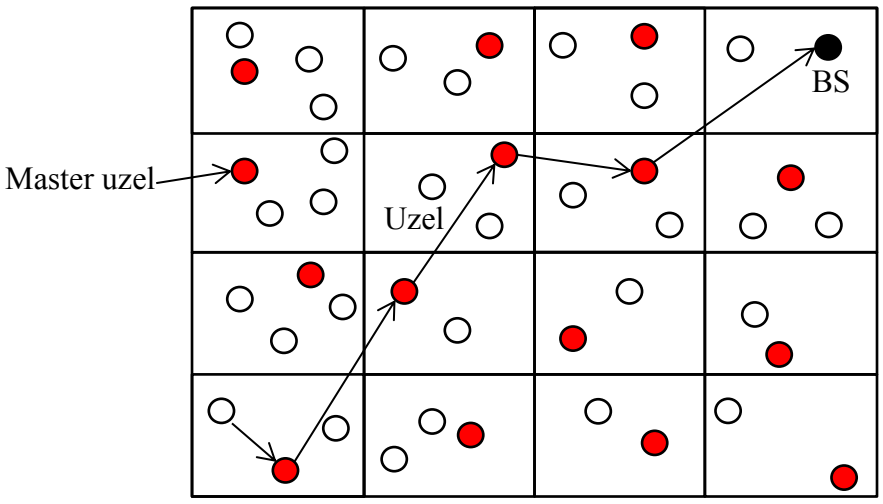
Obr 5.2. - Smíšená topologie



Smíšená topologie (někdy také nazývána obecný graf nebo mesh topologie) má uzly rozprostřené do nepravidelných pozic. Síť pak nemá podobu žádného z geometrických útvarů. Cílem této topologie je vytvořit alespoň dvě a nebo více cest, kterými se lze dostat do základnové stanice. Pokud existuje více cest, zpráva může být odeslána pouze jednou z nich. Způsoby hledání cesty a hledání cest závisí na použitém síťovém protokolu. Síťová topologie je efektivnější než topologie hvězdy. S vyšším počtem uzlů se rapidně neztrácí její efektivita [11, 30].

5.1.3 Buňková topologie

Obr 5.3. – Buňková topologie

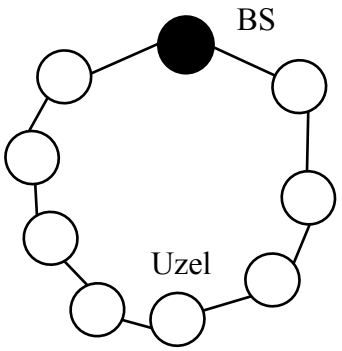


V buňkové topologii (někdy také nazývána mřížová topologie nebo grid topologie) se rozdělí celá síť na stejně velké čtverce, které se navzájem nepřekrývají. V každém čtverci je několik uzlů, jejich počet je strategicky vybrán tak aby v každém uzlu byl alespoň jeden aktivní uzel. Zprávy se směrují v síti přes nejbližší čtverce. Ve čtverci zprávy přeposílají master uzly, mezi kterými rotuje pověření z důvodu lepšího využití energie.

Efektivita této topologie je přibližně podobná jako smíšená topologie. Rozdíl je v lepším využití energie. V topologii buňky probíhá změna hlavního uzlu mříže.

5.1.4 Kruhová topologie

Obr. 5.4. Kruhová topologie



V kruhové topologii jsou uzly rozestavěny do kruhu (kruh nemusí být geometrický přesný). Postačí, když rozestavění uzlů bude alespoň vzdáleně připomínat kruh). Každý uzel má přesně dva sousední uzly. Všechny zprávy jsou směrovány pomocí sousedních uzlů po směru nebo proti směru hodinových ručiček. Tato topologie není příliš vhodná pro použití ve WSN, protože při výpadku jednoho nebo více uzlů může dojít k pádu celé sítě. Zároveň tuto topologii nelze využít ve velkých počtech uzlů. Cesty do cílového uzlu by pak byly velmi dlouhé a směrování by spotřebovalo velké množství energie [11, 30].

5.2 Typy hierarchických topologií

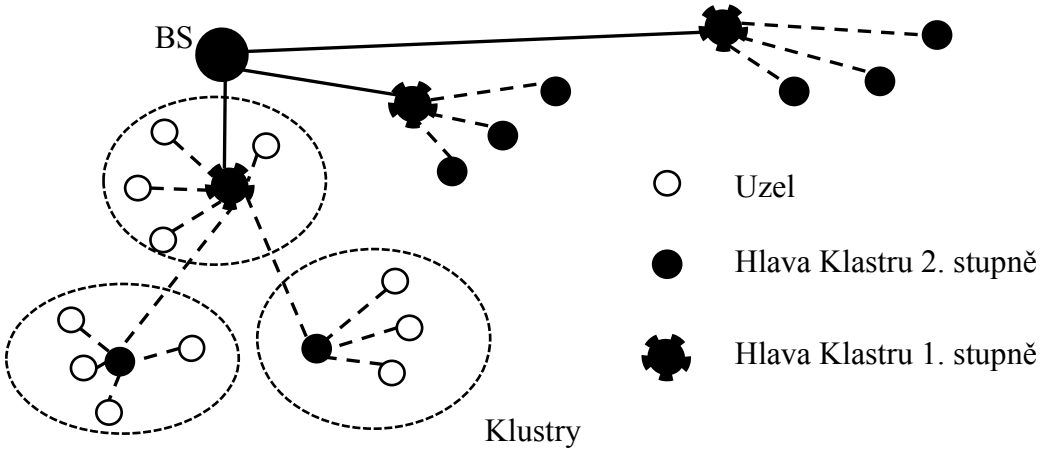
5.2.1 Klastrové topologie (cluster = shluk)

V klastrové topologii nemají všechny uzly stejnou funkci. Existují zde uzly a hlavy klastru. Uzly fungují jako základní uzly sítě, které snímají prostředí, zpracovávají a směrují data. Hlavy klastru jsou uzly, které slouží jako brána mezi uzly v klastru a základnovou stanicí nebo jako brána do nižších klastrů. V síti lze vytvořit více vnořených klastrů, záleží pouze na efektivitě dalšího vnoření. Agregace dat probíhá uvnitř klastru, tedy v hlavě klastru, která přijímá data z podřízených uzlů.

Existuje více druhů klastrových topologií: homogenní a heterogenní, statické a dynamické. V homogenní klastrové topologii mají všechny uzly stejný hardware. Homogenní uzly se většinou využívají s dynamickou topologií, kde se střídá pověření hlavy klastru. V heterogenní topologii už existují dva různé typy uzlů. Jeden typ uzlů má kvalitnější a výkonnější hardware, tvoří tak hlavy klastrů a pracuje pouze jako sběrnice dat. Statické topologie se většinou skládají z heterogenních uzlů, které si nepředávají pověření hlavy klastru. Všechny prvky sítě jsou vytvoření při vytváření sítě a nemění svoji pozici ani vlastnosti. Dynamická topologie lépe využívá hardware uzlů. Uzly mohou měnit klastry a svoje pověření. Dynamická topologie je výhodnější než statická topologie, při rozmístění uzlů ve špatně dostupných nebo odlehlých lokalitách [11, 29].

Klastrové topologie pracují mnohem lépe při větších počtech uzlů než nestrukturované

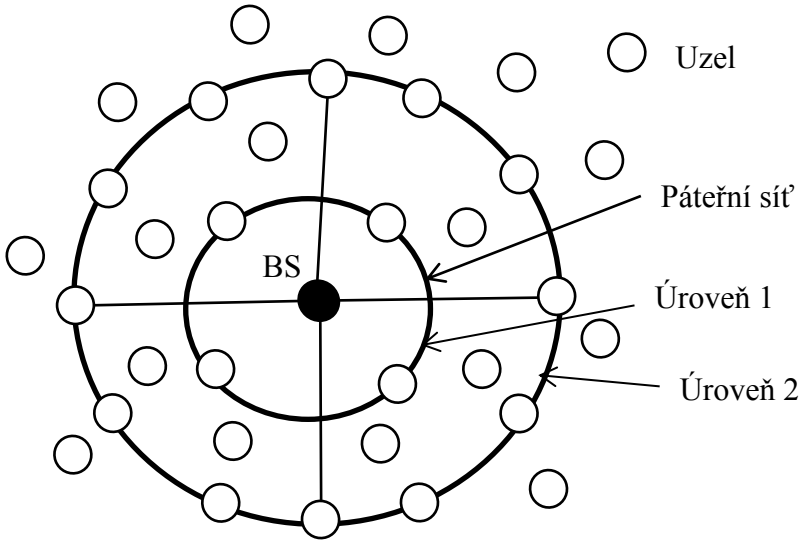
topologie. Zároveň se snižuje energetická náročnost sítě. Pokud má síť větší vzdálenosti mezi uzly a základnovou stanicí, je nevýhodou topologie je vyšší spotřeba energie při směrování dat.



Obr. 5.5. – Klastrová topologie

5.2.2 Topologie kruhové hierarchie

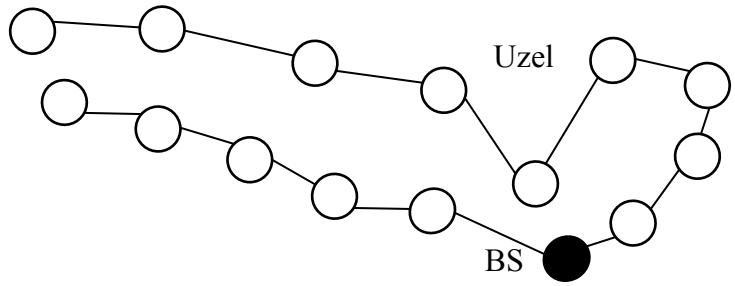
Topologie kruhové hierarchie se skládá z několika kruhů, které jsou složeny z uzlů. Některé uzly se mohou nacházet i mimo kruhy, ale jsou připojeny ke svým sousedům v páteřní kruhové topologii. Každý uzel směruje zprávy blíže ke středu, nejprve se zpráva dostane do kruhu, poté na uzel, který ho směruje na nižší třídy kruhů až do základnové stanice. Tuto topologii lze využít i při velkých počtech uzlů. Výhodou topologie je dobré udržování směrovacích cest. Nevýhodou je vyšší energetická náročnost uzlů blíže do středu, tedy do základnové stanice [30].



Obr. 5.6. – Topologie kruhové hierarchie

5.2.3 Topologie řetězu

Obr. 5.7. – Topologie řetězu

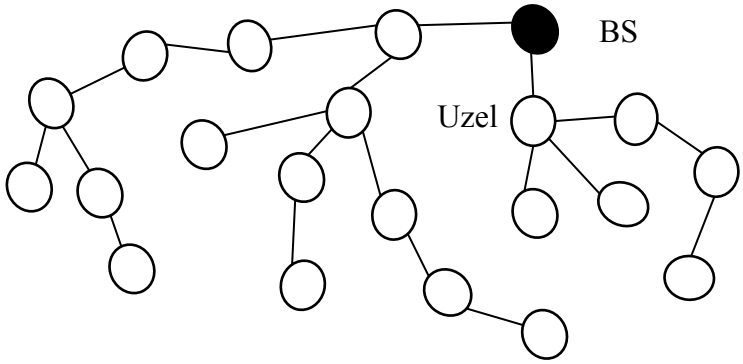


V této topologii jsou uzly propojeny mezi sebou a sestavují přenosový řetěz. Uzly v řetězu směrují svoje zprávy svým sousedům, ti pak agregují svá data s přijatými daty a směrují data dále do základnové stanice. Lze také vytvořit klastry, kdy každý klastr je jeden řetěz s hlavou klastru. Hlavy klastru pak směrují data dále do nižších vrstev.

Řetězová topologie, díky směrování svým blízkým sousedům namísto směrování na delší vzdálenosti, snižuje spotřebovanou energii na směrování. Protokol PEGASIS ušetří přibližně 50% více energie než protokol LEACH (Low-Energy Adaptive Clustering Hierarchy) [17]. Distribuce energie v síti je stejná napříč uzly. Nevýhodou topologie může být delší odezva při sběru dat a náročné řízení topologie. Topologie je nejvíce vhodná pro aplikaci do odlehlých a špatně dostupných lokalit.

5.2.4 Topologie stromu

Obr 5.8. Topologie stromu



V topologii stromu se sestaví logický strom z uzlů v síti. Vrchol stromu je základnová stanice, do kterého uzly směrují svoje data. Rodič agreguje data přijatá od svých listů. Struktura stromu (šířka a počet potomků) záleží na potřebě aplikace.

Topologie stromu je jen o málo lepší, co se týče spotřeby energie, a v ostatních chrakteristikách vykonává funkce stejně dobře nebo hůře jako topologie klastru. Nevýhody jsou: nerovnoměrná spotřeba energie napříč stromem, čím blíže k základnové stanici, tím má uzel větší energetickou náročnost. Při výpadku uzlu se odpojí celá větev stromu. Dlouhá odezva při směrování zpráv od konce stromu na jeho

kořen. Sestavování a udržování stromu je náročně jak časově, tak nákladově [11, 29, 30].

5.3 Správa topologie

Rozestavění uzlů

Pro správné rozestavění uzlů po oblasti je důležité určit správný počet uzlů a jejich vzdálenosti od sebe s ohledem na zkoumané prostředí. Je potřeba se také zamyslet nad charakteristikami prostředí, jeho dostupnost a vzdálenost. Rozestavění uzlů je první fáze implementace WSN. Aplikace sítě a pozice uzlů bude určovat topologii sítě, její limitace a vlastnosti. Zpravidla čím více uzlů v síti, tím méně energie je potřeba vynaložit na udržení připojení a pokrytí oblasti. Pro lepší rozestavění uzlů lze využít algoritmus VFA (Virtual Force Algorithm), který zlepšuje pokrytí uzly a jejich přesnost. Pro využití VFA se předpokládá klastrová topologie s mobilními uzly nebo manuální přerozdělení uzlů. [6, 12].

Řízení vysílacího výkonu

Topologie je z části vytvořena pomocí spojení mezi uzly. Pro efektivní spotřebu energie, nízkou odezvu a spolehlivost je třeba vytvořit co nejkratší cesty. Je třeba nalézt kompromis mezi snižováním rušení a zvyšováním životnosti sítě. Hlavními cíli protokolů na řízení vysílacího výkonu jsou: minimální energie potřebná na přenos pro uzly, hledání minimální kostry, distribuované operace, které jsou vhodné i pro větší sítě, diskrétní úroveň energie pro rozeznání proveditelné operace. Protokoly, které podporují řízení vysílacího výkonu jsou např. LMST (Local Minimum Spanning Tree), LMA (Local Mean Algorithm) [6].

Kontrola aktivních uzlů

Ve WSN muže být vysílač vypnut v určitých dobách, kdy se předpokládá nízký provoz sítě, nebo se může uzlu vybít zdroj energie. Uzel je tak úplně odpojen od sítě. Nijak se nepodílí na směrování v síti, ale pořád může pokračovat ve snímání prostředí, pokud mu to dovolují energetické zásoby.

Je potřeba monitorovat aktivní i neaktivní zařízení kvůli udržení propojení. V síti musí zůstat alespoň tolik aktivních uzlů, aby vytvořili páteřní cestu. Vypínání vysílače redundantních uzlů zvyšuje životnost sítě. Správné řízení aktivních a neaktivních uzlů

mají na starost protokoly na plánování aktivity. Mezi ně patří např. GAF (Geographical Adaptive Fidelity), ASCENT (Adaptive Self-Configuring Sensor Network Topologies), PEAS (Probing Environment And Adaptive Sleeping) [6].

GAF (Geographical Adaptive Fidelity) je algoritmus, který redukuje spotřebu energie vybíráním páteřních uzlů. Každý uzel musí tedy mít informaci o vlastní poloze. Algoritmus dělí síť na stejně velké pomyslné čtverce tak, aby se v každém čtverci nacházelo alespoň několik uzlů. Uzly ve čtverci pak mohou přejít do režimu spánku, ale alespoň jeden uzel musí být aktivní v každém čtverci, aby utvořil páteřní síť. Ostatní uzly potom mohou přejít do režimu spánku. Každý uzel musí tedy mít informaci o vlastní poloze [6].

6 Protokoly síťové vrstvy

Síťová vrstva ve WSN se potýká s mnoha problémy, jako např. omezenost energie, nespolehlivost síťového média, hardwarové limitace, změny topologie atd. Protokoly lze dělit do mnoha skupin. Pro rozdělení protokolů jsou vybrány tři nejvíce využívané skupiny rozdělení (také rozdělení podle Al-Karaki a Kamal 2004). Skupiny se navzájem prolínají, tudíž jeden protokol může patřit do více skupin najednou. Základním rozdělením je rozdělení dle organizace sítě, ve které jsou skupiny podle rozdělení a funkce uzlů. Další rozdělení je podle hledání cesty v síti a třetí rozdělení je podle podporovaných operací.
V práci je použito kritérium pro výběr protokolů podle počtu citací a také výběr různých způsobů směrová ve WSN. Pro jednotnost a charakterističtější význam jsou skupiny protokolů v kapitole 6.1 uvedeny anglicky.

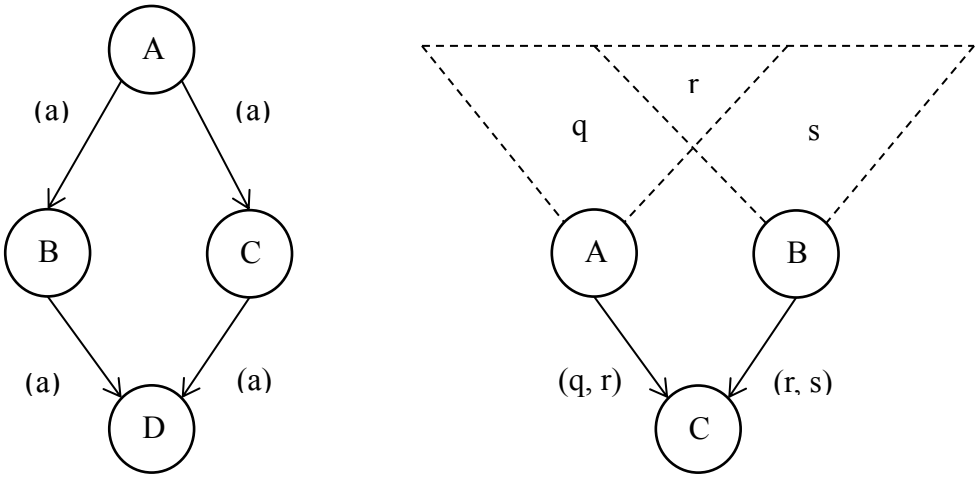
6.1 Základní protokoly a problémy síťové vrstvy

Záplavový algoritmus (flooding) – Každý uzel, který přijme datový paket, přeposílá paket všem sousedícím uzlům (broadcast). Tak se děje až do doby, kdy je vyčerpán počet skoků pro zprávu nebo pokud uzel přijme data, která již přeposlal. Počet skoků je nastaven tak, aby ke každému uzlu došla zpráva a aby se zpráva nepřeposílala dlouho v síti. Největší výhoda tohoto algoritmu je jednoduchost jeho implementace. Tato výhoda sebou nese i několik nevýhod – velký datový provoz a problémy zvané implosion, overlap a resourse blindness.

Klábosení (Gossiping) – V českém jazyce klábosení. Bohužel český překlad jen vzdáleně vystihuje pojem gossping, proto je v práci využit anglický název gossiping. Gossiping je vylepšená verze záplavového algoritmu. Každý uzel, který přijme datový paket, posílá datový paket pouze náhodně zvolenému sousedícímu uzlu. Tento uzel pak dále směruje zprávu k cíli. S tímto způsobem přichází větší zpoždění při šíření dat. Gossiping odstraňuje nevýhodu imploze kvůli vybrání náhodného uzlu pro odeslání dat, namísto broadcastu všem sousedům.[2, 7]

Imploze (implosion) - Uzel A pošle data svým sousedům B a C. Následně B a C posílají data svému sousedu D, který končí se dvěma kopiemi stejných dat [9].

Překrývání (overlap) – Při tomto problému uzel C přijímá data od uzlu A a B. Uzel A a B jsou uzly sousední a sledují prostory *q* a *s*. Protože se tyto prostory překrývají, mají uzly A i B část svých dat stejnou (měření z prostoru r na obrázku). Uzel C při směrování sousedních uzlů dostává data od uzlů A a B a vznikají redundantní data, tedy region *q* a *r* od uzlu A, *r* a *s* od uzlu B [9].



Obr. 6.1. – vlevo imploze a vpravo překrývání.

Bez ohledu na zdroje (resource blindness) – Tímto pojmem jsou nazývány uzly, které spotřebovávají velké množství energie, nehledě na svoje energetické zdroje, při směrování zpráv a dalších funkcích [2, 7].

6.2 Rozdělení protokolů

Rozdělení dle organizace sítě:

Flat (jednoúrovňové protokoly) – Všechny uzly mají stejnou funkci, žádný není nadřazený. To je jedním z řešení problému vysokého počtu uzlů v síti a tedy není možnost přiřadit všem uzlům globální identifikátory. Síťové protokoly tohoto typu používají reaktivní nebo proaktivní způsob směrování a efektivitita těchto protokolů je na tom závislá. Podmnožinou této skupiny jsou data-centrické protokoly, které směrují podle popisů dat. Nejzákladnějším protokolem je záplavový algoritmus, který spotřebovává velké množství energie a zároveň vytváří velké množství redundantních zpráv. Snižuje se i životnost sítě, nejen kvůli záplavovému algoritmu, ale také kvůli nerovnoměrnému zatížení uzlů. Senzory si nejsou vědomy nových nebo vypnutých uzlů. S výše uvedenými problémy také přichází vysoká nespolehlivost

a odezva [8].

Hierarchical (hierarchické protokoly) – Některé uzly jsou nadřazené ostatním. Síťové protokoly tvoří skupiny protokolů tzv. klastry (viz obr. 6.). V tomto klastru je jeden speciální uzel tzv. cluster head (česky hlava klastru, dále jen CH), který je nadřazen všem uzlům v tomto klastru a prochází přes něj veškerá komunikace, která směřuje vně klastru. Tyto CH se v každém kole mění tak, aby byla spotřeba energie co nejrovnoměrněji rozdělena uvnitř klastru. Tento způsob rozdělení redukuje počet zpráv a tedy i spotřebu energie uzlů a taktéž snižuje počet kolizí.

Geografical (Geografické protokoly) – Tyto protokoly pracují s informací polohy namísto topologické informace. Každý uzel musí znát svojí geografickou polohu. Pakety zasílají pouze do dané skupiny uzlů podle jejich polohy. Data jsou rozesílána pomocí unicast, broadcast nebo multicast. Multicast má výhodu oproti broadcast, že zprávy může zasílat pouze do potřebných uzlů, nikoli do všech.

Rozdělení podle hledání cesty: Vytváření směrovací tabulky (nebo podle způsobu hledání cesty)

Proactive (proaktivní protokoly) – Někdy také nazývány anglicky table driven protocols. Směrovací tabulky jsou již předem vytvořeny a jsou aktualizovány. Odezva u reaktivního hledání cesty je v tomto případě eliminována. Výhodou je efektivní funkce při velké zátěži sítě. S předem vytvořenými směrovacími tabulkami vznikají také problémy, jako je nutnost udržovat směrovací tabulky a provoz s tím spojený.

Reactive (reaktivní protokoly) – Hledání cesty na „požádání“ (anglicky se protokoly nazývají routing on demand nebo delay tolerant networks). Cesta se vytváří až těsně před odesláním dat. Pokaždé, když uzel potřebuje poslat zprávu dalšímu uzlu, posílá RREQ paket (route request – žádost o cestu) broadcastem svým sousedům. RREQ paket obsahuje: ID broadcastu, adresu zdroje a cíle, počet skoků a dvě sekvence čísel. Každý uzel, který přijme RREQ paket, aktualizuje informace o odesílateli broadcastu a pokud zná cestu do cílového uzlu, odpovídá PREP (route reply – odpověď ma žádost o cestu) paketem pomocí unicast. Pokud uzel cestu do cílového uzlu nezná, pokračuje rebrocastem svým sousedním uzlům a zvýší čítač skoků. Když zdrojový uzel dostane zpět PREP paket a pokud cestu ještě nemá ve svojí dočasné směrovací tabulce,

přidá ji. Pokud cestu již zná, aktualizuje ji podle čítače skoků, méně skoků rovná se rychlejší cesta. Největší nevýhoda je v delší odezvě, z toho také plyne název delayed-tolerant networks. Další nevýhodou je špatná efektivita při velké zátěži sítě [4].

Hybrid (hybridní protokoly) – Určitý způsob kombinace obou způsobů hledání cesty, proaktivního a reaktivního.

Rozdělení podle podporovaných operací:

Negotiation (protokoly s vyjednáváním) – Vylepšuje záplavový algoritmus vyjednávacím způsobem a přizpůsobení zdrojů v kombinaci s meta-daty. Vyjednávání je v podstatě nabízení svých dat před odesláním svým sousedním uzlům (zpráva ADV- advertisment). Data se posílají jen uzlům, které kladně odpoví REQ zprávu.

Multi-path (více-cestné protokoly) – Směrování, které umožňuje zřídit více možných cest mezi dvěma body sítě. Multi–path se využívá ze dvou důvodů: za prvé pro lepší energetické využití sítě, kde pomocí různých cest nezatěžuje jen jednu skupinu uzlů. Za druhé pro spolehlivé doručení dat. Data lze posílat vícekrát najednou pro zvýšení pravděpodobnosti správného doručení. Vhodné je využívat tuto metodu v síti s velkým šumem nebo častým selháváním uzlů. Při výběru cesty se preferuje primární cesta (většinou cesta, ve které jsou uzly s nejvíce energií k dispozici), která se využívá až do doby, kdy její kapacita energie neklesne pod určité množství energie nutné pro další pracování nebo záložní cestu.

Query (dotazové protokoly) – Komunikace v dotazových protokolech je založena na uživateli, který začíná komunikaci pomocí dotazu. Uzly, které mohou tento dotaz vykonat, posílají zpět odpověď do uzlu, do kterého si uživatel vyžádal data poslat. Ve většině případech se odpovědi na dotazy posílají do základnové stanice.

QoS (QoS protokoly) – Protokoly, které se snaží zajistit jednu nebo více metrik z QoS (Quality of service). Může to být např. rychlost, odezva, ztráta paketů, spotřeba energie atp.

Protokoly	Organizace sítě	Hledání cesty	Negotiation	Multi-path	Query
SPIN	Jednoúrovňová	Reaktivní	X	X	X
DD	Jednoúrovňová	Reaktivní	X	X	X
RR	Jednoúrovňová	Hybridní			X
COUGAR	Jednoúrovňová	Reaktivní			X
ACQUIRE	Jednoúrovňová	Proaktivní			X
DSDV	Jednoúrovňová	Proaktivní			
OLSR	Jednoúrovňová	Proaktivní			
AODV	Jednoúrovňová	Reaktivní			
DSR	Jednoúrovňová	Reaktivní			
LEACH	Hierarchická	Proaktivní			
PEGASIS	Hierarchická	Reaktivní			
TEEN	Hierarchická	Reaktivní			
APTEEN	Hierarchická	Hybridní			
HEED	Geografická	Proaktivní			
GAF	Geografická				
SPAN	Geografická		X		
GEAR	Geografická				
MECN a SMECN	Geografická				
GPSR	Geografická				
GFPG	Geografická				
SAR	QoS	Proaktivní	X	X	X
SPEED	QoS	Proaktivní			X
MMSPREAD	QoS	Proaktivní		X	

Tabulka 6.1. – Rozdělení a vlastnosti síťových protokolů WSN.

7 Příklady protokolů síťové vrstvy

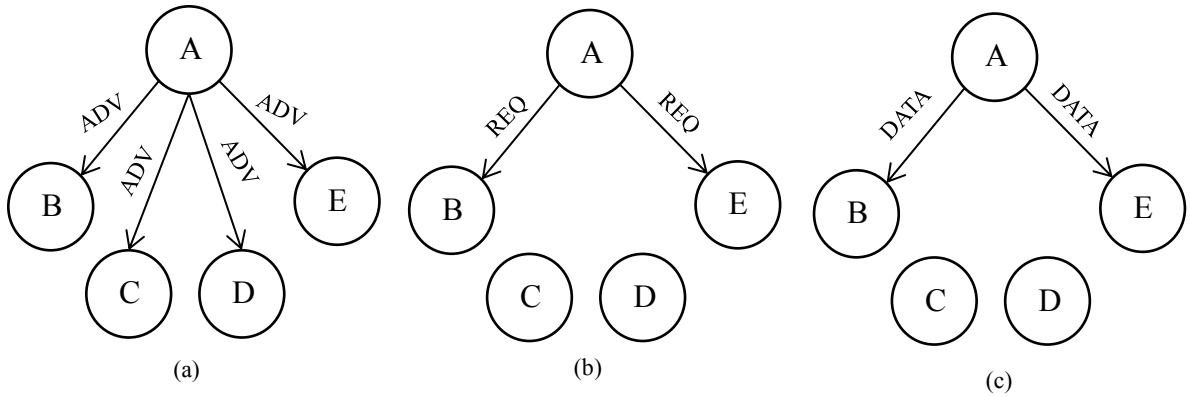
7.1 SPIN - Sensor Protocols For Information via Negotiation

Charakteristiky: Data-centric, reactive, negotiation, multipath, query

Skupina protokolů SPIN je vytvořena za účelem odstranění problémů, které přicházejí se záplavovým algoritmem. Používá se vyjednávání před každým směrováním dat pro odstranění problémů překrývání a imploze. Vyjednávání také odstraňuje redundantní komunikaci.

Pro odstranění problému „nehledění na energii uzlů“ se používají protokoly správce zdrojů na sledování jejich spotřeby energie. Umožňuje to protokolu na základě těchto informací měnit způsob směrování. Každý uzel zná jen své jedno-přeskokové sousedy.

SPIN používá meta-data pro úplné popsání dat nasbíraných senzory. Pro každá meta-data platí, že jejich velikost v bytech musí být menší než velikost dat, která popisují. Pokud mají dva uzly stejná data, potom se i jejich meta-data neliší. Příklad meta-dat může být geografická souřadnice nebo čas. Komunikace v protokolech typu SPIN probíhá pomocí trojcestného handshakingu ADV (advertisement message neboli nabízecí zpráva), REQ (request neboli žádost) a DATA (paket obsahující data). Nejprve uzel pošle ADV paket svým sousedním uzlům. Tento paket obsahuje popis nabízených dat, jejichž velikost je mnohem menší než velikost reálných dat. Pokud uzel, který přijme ADV paket a data nemá k dispozici, odpoví pomocí REQ paketu, následně obdrží kopii dat. Uzlů, které odpovídají na REQ, může být více. Po přijetí nových dat mohou uzly tato data agregovat a posílat je dále svým sousedům. Při ztracených ADV zprávách mohou uzly periodicky znovu nabízet svoje data okolním sousedům [1, 2, 7, 9].



Obr. 5. – Způsob směrování dat pomocí záplavového algoritmu a trojcestného handshakingu.

Dále jsou popsány modifikace protokolu SPIN.

SPIN-PP

SPIN optimalizovaný pro přenos z bodu do bodu (point-to-point). Dva uzly spolu komunikují bez přerušování od ostatních uzlů. V SPIN-PP jsou data směrována pomocí trojcestného handshakingu stejně je popsáno výše [1, 2, 7].

SPIN-EC

SPIN-EC je energeticky úspornější verze SPIN-PP protokolu. Pokud uzly mají dostatek energie, chovají se stejně jako u protokolu SPIN-PP, tedy používají trojcestný handshaking.

Uzly, které mají energie méně než určitou úroveň, vybírají, kdy se účastnit směrování-trojcestného handshakingu. Použijí ho jen v případě, pokud mají dostatek energie na dokončení všech kroků. Uzly ale stále přijímají ADV a REQ pakety, pouze na ně neodpovídají DATA paketem [2,7].

SPIN-BC

SPIN-BC je verze protokolu SPIN upravená pro broadcastové sítě (jedno-kanálová sdílená síť). Stejně jako předešlé protokoly SPIN-BC používá trojcestný handshaking, ale s určitými rozdíly: nabízení dat je nahrazeno broadcastem. Všechny uzly, které se nacházejí v dosahu přenosu, dostanou paket. Místo toho, aby uzly při přijetí ADV paketu rovnou odpověděli pomocí REQ paketu, čekají náhodný čas z přednastaveného intervalu, aby se snížila možnost kolize. Poté posílá REQ paket broadcastem. Když uzel odposlechne REQ paket stejný, jaký chce sám odeslat, zruší svůj naplánovaný REQ paket. Uzel, který nabízí data, posílá pouze jednou kopii dat a ignoruje tak duplikáty REQ paketů [2, 7, 17].

SPIN-RL

SPIN_RL vylepšuje SPIN-BC. Uzly udržují informace o ADV paketech poslaných uzly v přenosové vzdálenosti a pokud uzel nedostane kopii dat v určitém intervalu, posílá uzel paket znovu. Odstraňuje tak nevýhodu nezaručeného doručení zpráv [1, 7].

Výhody a nevýhody

Protokoly SPIN jsou lepší než základní směrovací algoritmy (záplavový algoritmus,

gossiping). Výhodou vyjednávání je redukce redundantních dat. Další výhodou je, že změny topologie jsou pouze lokální, protože uzly potřebují znát jen jedno-přeskokové sousedy. Nevýhodou protokolu je, že doručení dat není zaručeno [1, 17].

7.2 DD – Directed Diffusion

Charakteristiky: Data-centric, reactive, negotiation, multi-patch, query

DD je stejně jako protokol SPIN bez hierarchie. Největší rozdíl mezi protokoly je ve směru komunikace. V protokolu SPIN komunikace proudí směrem k základnové stanici, kdežto v DD komunikace proudí od uživatele-základnové stanice do uzlů. Uživatel tak může požadovat vybrané informace ze sítě. Další charakteristikou je, že všechny uzly jsou tzv. application-aware (uzly podporující aplikace).

Protokol má 4 fáze. V první fázi základnová stanice rozešle požadavek sítí pomocí záplavového algoritmu. V požadavku jsou jasně specifikovány atributy, která data je nutno poslat zpět do základnové stanice. V druhé fázi uzly vytvoří gradienty-zpětné cesty pro odeslání odpovědi na požadavek. Ve třetí fázi nastává výběr jedné nebo více cest určených ke směrování. Vybírat se může podle více kritérií, např. podle odezvy nebo spolehlivosti. V poslední čtvrté fázi probíhá odeslání pomocí jedné nebo více vybraných cest. V případě, že by se cesta z nějakého důvodu porušila, lze ji znovu obnovit vybráním jiné cesty [2, 22, 23].

Výhody a nevýhody:

Vhodný protokol pro monitorování mnoha různých typů dat a časté komunikace uživatelem a sítí. Není vhodné a někdy i nemožné, použít pro aplikace, které vyžadují nepřetržitý tok dat do základnové stanice.

7.3 LEACH - Low-Energy Adaptive Clustering Hierarchy

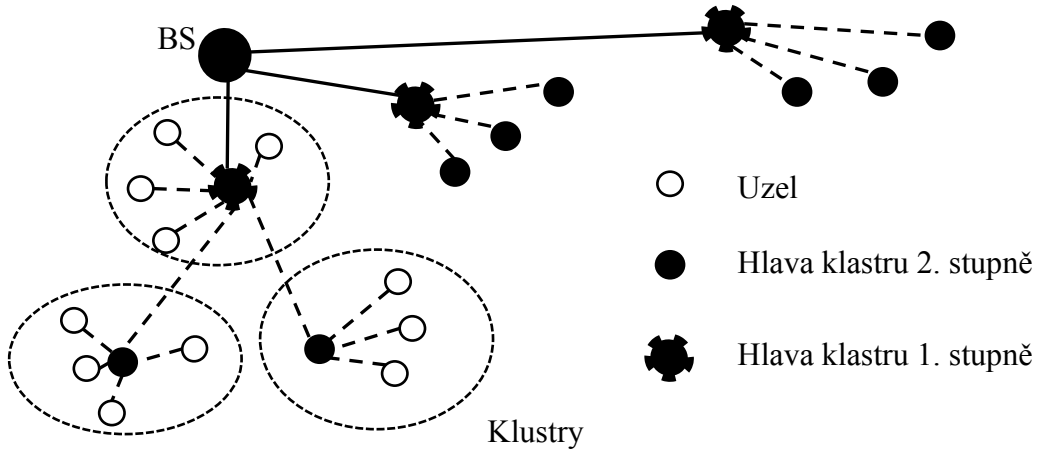
Charakteristiky: Hierarchical, proactive

LEACH (Low Energy Adaptive Clustering Hierarchy) je samo-organizační protokol. Využívá adaptivních klastrů a náhodnost pro distribuce energického zatížení pro senzory v síti. LEACH vytváří klastry uzlů podle síly přijímaného signálu. Jeden uzel je pověřen CH - hlavní uzel v klastru. CH se chová jako lokální základnová stanice. CH směrují data do CH nižších klastrů až do základnové stanice.

Tento systém snižuje náročnost na energii kvůli rovnoměrné spotřebě energie.

Uzly, které směrují data do základnové stanice, se střídají v pověření. Základnová stanice se může nacházet ve velké vzdálenosti od uzlů, to pak vede k velké spotřebě energie a neefektivitě protokolu. LEACH dále podporuje fúzi dat (komprese dat před odesláním do nižších vrstev. Snížení energie - zvýšení životnosti). Fúze dat a aggregace probíhá vždy uvnitř klastru [1, 7, 21].

Předpoklady protokolu:
Všechny uzly mají dostatečnou sílu pro dosah základnové stanice. Každý uzel má dostatečnou výpočetní sílu pro podporu různých MAC protokolů. Uzly nacházející se blízko sebe mají korelovaná data. Protokol LEACH má dvě fáze, fáze nastavení a fáze stabilní.



Obr. 7.1. – Větvení v protokolu LEACH.

Fáze nastavení
Během této fáze se nastavují CH, klastry a rozvrh pro protokol TDMA, který je využit při odesílání dat do CH. Protokol LEACH náhodně rotuje energicky náročné CH tak, aby aktivita a spotřeba energie byly rovnoměrně sdíleny mezi uzly. Každý uzel na začátku kola vybere náhodné číslo r v intervalu od 0 do 1. Pokud číslo je menší než hraniční hodnota *T(n)*, senzor se stane CH ve stabilní fázi na jedno kolo *r*. *P* je požadované procento nových CH v síti. G je skupina uzlů, které nebyly vybrány jako CH v posledních *1/P* kolech. Po vybrání všech CH v sítí, protokol LEACH využije protokolu založeného na CSMA pro inzerování nových CH. Na základě vybraných CH se vytvoří nové klastry na základě síly signálu inzerce.

$$T(n) = \begin{cases} \dfrac{P}{1 - P[r \bmod (1/P)]} & \text{if } n \in G \\ 0 & \text{Jinak} \end{cases}$$

Zdroj: [15]

Novým CH se mohou stát jen uzly, které nebyly vybrány v minulém kole. Tento přístup efektivně rotuje pozici CH v síti, ale nebere v potaz aktuální energii uzlu. Pro přístup vybrání CH podle aktuálního množství energie, může být zvolen tento vzorec:

$$P_i(t) = \min \left\{ \frac{E_i(t)}{E_{\text{total}}(t)} k, 1 \right\}$$

Zdroj: [2]

$E_i(t)$ - aktuální množství energie

$E_{total}(t)$ - suma množství všech uzlů v klastru

Fáze stabilní

CH musí být neustále aktivní kvůli přijímání dat od uzlů klastru a pro směrování dat do základnové stanice. V této fázi uzly posílají data na CH a to jen v čase, který je jim přidělen v rozvrhu.

Ačkoli uzly používají TDMA (umožňuje více uživatelům sdílet stejný frekvenční kanál dělením signálu do různých časových slotů), může se stát, že dojde ke kolizi s jiným klastrem. Proto uzly používají DSSS (Direct Sequence Spread Spectrum) pro rozšíření spektra při přenosu dat. Pokud tedy CH chce posílat data do základnové stanice, nejdříve zjistí, jestli někdo jiný posílá data ve stejném spektru. Nabízení dat a měnění hlavních uzlů může snížit efektivitu spotřeby energie [1, 7, 21].

Výhody a nevýhody:

Nízká spotřeba energie kvůli rovnoměrné distribuci energetické zátěže. Protokol může být velmi neefektivní, pokud je základnová stanice velké vzdálenosti od ostatních uzlů. Nevýhodou je také režie na vybírání hlavy klastru.

7.4 SAR - Sequential Assignment Routing

Charakteristiky: QoS, proactive, negotiation, query, multi-path

SAR je jedním z prvotních QoS protokolů v senzorických sítí. Protokol řeší QoS způsobem vytváření více možných cest mezi dvěma body sítě (multi-path). Jednoduše pro vybranou metriku QoS vybírá nejlepší možnou cestu. Každá cesta začíná

na rootovém uzlu, prochází síť směrem od základnové stanice a má dva parametry. První parametr je energetické zhodnocení cesty, popsané maximálním počtem paketů, které mohou být uzlem odeslány na této cestě. Druhý parametr je metrika QoS, která souvisí s energií a odezvou každého spojení. Čím více je jedna cesta využívána pro spojení, tím více se zvyšuje její druhý parametr a zároveň snižuje QoS [6, 10, 16].

Výhody a nevýhody

Výhodou je nízká spotřeba energie a udržování více směrovacích cest. Nevýhodou je režie udržování velkého počtu směrovacích cest.

7.5 GEAR - Geographic And Energy Aware Routing

Charakteristiky: Location,

GEAR stejně jako ostatní geografické protokoly potřebuje pro svojí funkci informaci o pozici všech uzlů v síti, pro vypočítání vzdálenosti mezi dvěma uzly. Informace o pozici se získává pomocí GPS nebo podobných lokalizačních systémů. Každý uzel udržuje informace o energetických nákladech směrování paketů do cílového uzlu. Směrovací algoritmus se rozlišuje na dvě fáze, směrování paketu do cílového regionu a vně cílového regionu.

Předpoklady pro síť:

- Každý paket má cílový region, kam posílat data.
- Každý paket zná: 1) svojí pozici 2) svojí aktuální kapacitu energie 3) pozici sousedních uzlů 4) aktuální kapacitu svých sousedů.
- Linky jsou obousměrné (např. point-to-point). Když uzel posílá pakety svému sousednímu uzlu, spojení lze navázat i v opačném směru.

Energetické možnosti dosažení cíle:

Odhadované náklady – je hodnota získaná kombinací aktuální energie uzlu a vzdálenosti do cíle. Normalizovaná rovnice rovnice pro výpočet odhadovaných nákladů, kde $c(N_i, R)$ je odhadovaná energie, N_i je sousední uzel a R cílový region.

Jako další parametry: α je volitelná váha, $d(N_i, R)$ je vzdálenost od sousedního uzlu N_i do centra D regionu R normalizovaného největší velikostí mezi sousedními uzly. $E(N_i)$ je spotřeba energie v uzlu N_i, normalizována o největší spotřebovanou energii

mezi všemi sousedními uzly [3, 31].

$$c(N_i, R) = \alpha d(N_i, R) + (1 - \alpha) e(N_i)$$

Zdroj: [3]

Naučené náklady – Naučené náklady je modifikovaná hodnota odhadovaných nákladů o tzv. díry. Díra se naskytne v síti tehdy, když cílový uzel nemá kolem sebe žádné přímé sousední uzly, přes které se lze spojit s cílovým uzlem. Pokud v cestě nebrání žádné díry, odhadované náklady a naučené náklady jsou stejné [3].

Fáze algoritmu:

První fáze

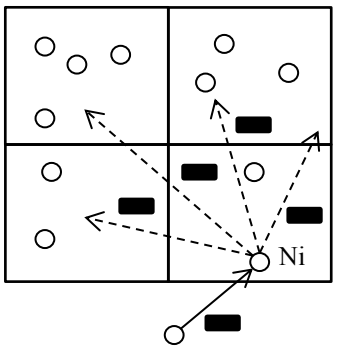
V první fázi algoritmu jsou pakety směrovány do cílového regionu. Při přijetí paketu uzel směruje paket dále pomocí hladového algoritmu. Vybírá sousední uzel tak, aby byl uzel co nejbližší cílovému uzlu. Pokud uzel nenajde uzel bližší cílovému uzlu než je on sám, znamená to, že v přímé cestě brání díra. Poté uzel vybere jeden ze sousední uzlů, přes který bude data směrovat. Ten pak směruje podle funkce naučených nákladů [3, 31].

Druhá fáze

Když paket dojde do daného regionu, je rozptýlen pomocí rekurzivního geografického směrování, pokud je v regionu větší hustota uzlů. Snižuje se tak efektivita spotřeby energie. Jinak při menší hustotě uzlů v síti je použit záplavový algoritmus omezený na region

Rekurzivní geografické směrování

Region *R* se rozdělí na několik subregionů. Uzel N_i, který je součástí regionu, vytvoří kopii paketu pro každý vytvořený subregion. Dělení a směrování pokračuje až do doby, kdy některý z uzlůje sám v subregionu [3, 31].



Obr. 7.2. – Rekurzivní geografické směrování.

Výhody a nevýhody:

Protokol GEAR se snaží rovnoměrně rozložit energetickou zátěž a tím i prodloužit životnost sítě. Uzly také znají svojí polohu a aktuální energii.

7.6 AODV - Ad Hoc On-Demand Distance Vector

Charakteristiky: Flat, reactive, multi-path

AODV je reaktivní protokol, což znamená, že neudržuje žádné informace o směrování, ani ve vyhledávání cest pro směrovací tabulky. Každá cesta je vytvářena, až když je potřeba přenést data. Cesty jsou udržovány tak dlouho, dokud jsou využívány, jinak zaniknou.

Tabulka má potom následující podobu:

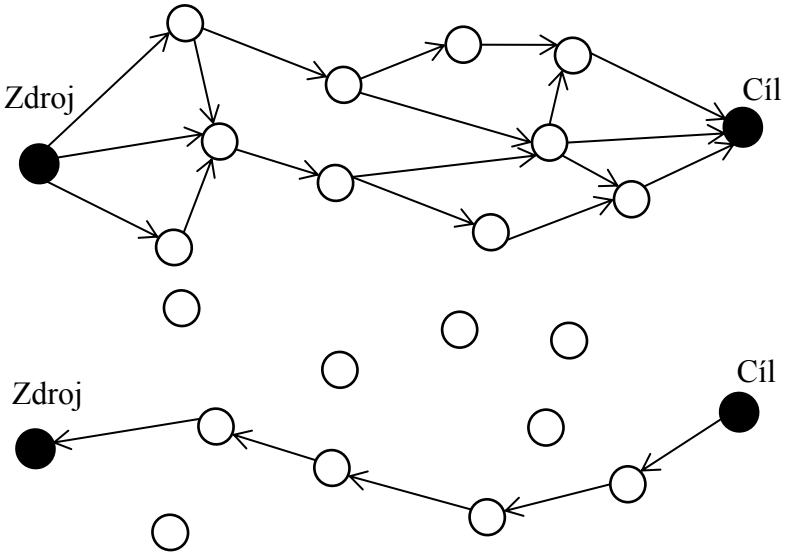
- IP adresa cíle – Pro každou IP adresu uzel ukládá seznam uzlů, přes které se dostane do cíle.
- IP adresa sousedního uzlu.
- Sekvenční číslo cíle - Sekvenční číslo se zvyšuje pokaždé, když uzel zjistí změnu v topologii okolí. Používá se pro zabránění používání starých nebo nepoužitelných cest a vytváření smyček.
- Časovač – Časovač je aktualizován pokaždé, když je cesta použita. Když časovač dojde na určitou hodnotu, cesta zanikne.

Proces vyhledávání cesty začíná, pokud uzel nemá ve své směrovací tabulce cestu k dispozici. Jako první krok uzel pošle broadcast pomocí záplavového algoritmu svým sousedům RREQ paket (route request – žádost o cestu), který obsahuje IP zdroje, ID cíle, ID broadcastu (ID broadcastu je zvýšeno o 1, pokaždé uzel použije broadcast), počítadlo skoků, sekvenční číslo zdroje a cíle. Když uzel přijme RREQ paket, vyhodnotí, jestli danou cestu zná či nikoli. Pokud cestu zná, odpovídá pomocí unicast RREP (route reply – odpověď na žádost). Pokud cestu nezná, použije rebroadcast RREQ paketu dalším sousedům a zároveň si zapíše pointer pro zpětnou cestu (IP zdrojového uzlu, sekvenční číslo zdrojového uzlu a počet skoků do zdrojového uzlu). Rebroadcast se opakuje až do doby, kdy se dostane k uzlu, který zná cestu k cílovému uzlu. Ten ve své směrovací tabulce musí mít záznam o cílovém uzlu a sekvenční číslo cíle musí být stejné nebo vyšší jako sekvenční číslo uvedené v RREQ paketu. Když jsou obě podmínky splněny, následuje zpětné hledání cesty posíláním PREP paketu.

PREP paket putuje sítí podle pointeru, který byl dříve nastaven.
PREP paket se odesílá jen v případě, když splňuje podmínky:

- PREP paket má jedinou kopii.
- PREP paket má větší sekvenční číslo než ostatní PREP pakety.
- Sekvenční číslo cílového uzlu je stejné jako v předchozím PREP paketu, ale počet skoků je menší.

V každé aktivní cestě si sousední uzly posílají HELLO zprávy pro zjištění stavu cest. Pokud některý uzel není již k dispozici (např. vybití baterie nebo změna pozice), sousední uzel blíže ke zdroji zprávy posílá RERR (route error) všem sousedním uzlům poznamenaným touto změnou směrem ke zdroji zprávy. Zdrojový uzel poté může znovu hledat vhodnou cestu [2, 5, 8].



Obr. 7.3. – Proces nalezení cesty v protokolu AODV.

Výhody a nevýhody

Režie tohoto protokolu není tak náročná jako u proaktivních protokolů. Exceluje při potřebě náhodných často nevyužívaných cest. Také není potřeba shromažďovat informace o uzlech. Největší nevýhoda je v delší odezvě, z toho také plyne název reaktivních sítí delayed-tolerant networks. Další nevýhodou je špatná efektivita při velké zátěži sítě.

7.7 PEGASIS - Power-Efficient Gathering In Sensor Information Systems

Charakteristiky: Hierarchical, reactive

Protokol PEGASIS je zástupcem topologie řetězu. Tento protokol byl vytvořen jako vylepšení protokolu LEACH. K největším změnám došlo ve spotřebě energie ve prospěch protokolu PEGASIS a odezvě ve prospěch protokolu LEACH. Uzly v této topologi vytvoří pomyslný řetěz nebo řetězy, pomocí hladového algoritmu. Směrování probíhá stejně jako u LEACH. Komunikace probíhá v klastru a CH pak dále směruje do nižších úrovní. Komunikace uvnitř klastru může proudit pouze ve dvou směrech, tedy mezi svými dvěma sousedy, jedním z každé strany. Základnovou stanici je nejlépe umístit do středu tohoto řetězu, aby nedocházelo k větším rozdílům spotřeby energie a odezvy, pokud je nějaký z uzlů vyřazen z provozu [6, 15, 23].

Výhody a nevýhody:

Velké snížení energie kvůli velkému počtu směrování na krátkou vzdálenost. Nevýhodou je dlouhá odezva sítě a redundantní přenos dat.

8 Porovnání síťových protokolů podle spotřeby energie

Spotřeba energie je důležitým aspektem WSN. Spotřebu energie je potřeba monitorovat a limitovat napříč celým systémem WSM, od hardwaru až po aplikace. Síťová vrstva není příliš významná, co se týče spotřeby energie. Největší spotřeba energie spadá na vrstvu linkovou, kde se spotřebuje přibližně 80 až 90% z celkové spotřeby energie.
Různé směrovací protokoly mohou být efektivní v jiných aplikacích (potřeby a charakteristika sítě). Stejně je to i se spotřebou energie, závisí při tom na rozdělení a počtu uzlů. Protokoly jsou efektivní za určité situace a pro určitý typ sítí.

8.1 Jednoúrovňové protokoly

Tyto prototokoly hledají cestu reaktivním nebo proaktivním způsobem. Proaktivní protokoly potřebují více směrovacích informací, spotřebují tedy více energie než reaktivní. Proaktivní protokoly zároveň nepotřebují zachovávat směrovací tabulky ani je aktualizovat při změně topologie, což vede k další redukci spotřebě energie. Reaktivní protokoly jsou lepší při nízkém provozu a při vysokém provozu mohou kolabovat, kdežto proaktivní protokoly pracují dobře i pod zátěží, ale při nízkém provozu mají zbytečně vysokou spotřebu na jeden poslaný paket. Základními protokoly jsou gossiping, záplavový algoritmus nebo RR (Rumor Routing) [9, 10, 15, 17].

8.2 Hierarchické protokoly

Hierarchické protokoly využívají sdružování uzlů do klastrů. Snižují tak velikosti směrovacích tabulek, protože veškerá komunikace musí projít hlavou klastru. Protokol LEACH je velmi efektivní ve spotřebě energie, snadné konfiguraci, a v rovnoměrné spotřebě napříč uzly. Tento protokol je jedno-přeskokový, uzly mohou komunikovat přímo s hlavou uzlu nebo základnovou stanicí. Protokol pracuje efektivně pouze v síti s menšími mezerami mezi uzly. Při větších mezerách dochází ve velké spotřebě energie na směrování. Vylepšení spotřeby energie přichází s modifikací protokolu LEACH pod názvem LEACH-C (C pro centralized). Rozdíl spočívá v správě klastrů. V LEACH klastry spravují sami uzly, kdežto v LEACH-C klastry spravuje základnová stanice.
PEGASIS (Power-Efficient Gathering in Sensor Information Systems) je protokol řetězové topologie a řeší problém děr protokolu LEACH. Každý uzel komunikuje pouze se svým nejbližším sousedem. Při výpadku uzlu je řetěz přestavěn tak, aby se mezera

zaplnila. Může se tak redukovat spotřeba energie i několikanásobně oproti LEACH, záleží přitom na velikosti děr mezi uzly.

TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol) je další protokol, který spotřebovává mnoho energie při velkých mezerách mezi uzly, ale s lepší spotřebou energie než LEACH i LEACH-C. Jeho výhoda je rychlá reakce na změnu snímaného prostředí, což je velmi důležité při aplikacích pracujících v reálném čase. Protokol APTEEN (Adaptive Threshold Sensitive Energy Efficient Sensor Network) je modifikací protokolu TEEN. Protokol zlepšuje spotřebu energie za cenu horší odezvy [15, 17, 20, 21].

8.3 Dotazové protokoly

Dotazové protokoly jsou založeny na dotazech, které přicházejí od uživatele a tedy z uzlu (většinou ze základnové stanice) do sítě, a na uzlech, které splňují podmínky, posílají svoje data zpět zadavateli. Příkladem dotazu může být dotaz o existenci regionu s teplotou vyšší než *c*. Základním protokolem této skupiny je DD, který může vybrat cesty podle předchozích experimentů a zpracovávat data pro lepší využití energie. Tento protokol je více efektivní co se spotřeby týče než základní jednoúrovňové protokoly. Dalším protokolem je COUGAR, který vidí síť jako jednu velkou databázi. Je efektivní při práci s objemnými daty, ale při méně objemných datech je režie zbytečně vysoká. Podobným protokolem je ACQUIRE (Active Query Forwarding In Sensor Networks), který má největší výhodu v komplexních dotazech. Při větších počtech možných odpovědí se směrování blíží záplavovému algoritmu [10, 15, 17, 21].

8.4 Vyjednávací protokoly

Hlavním představitelem této skupiny je protokol SPIN, podle kterého je založena většina data-centrických protokolů. Protokol využívá meta-dat pro vyjednávání, které redukuje redundantní data. Dalším protokolem této skupiny je SPIN-PP, který byl založen pro lepší optimalizaci komunikace point-to-point. Využívá trojcestný handshaking. Výhodou je jednoduchost, ale nedá se zaručit, že data budou doručena. SPIN-EC funguje dopobně jako SPIN-PP, ale využívá algoritmus na zachování energie [9, 10, 15, 17].

8.5 Geografické protokoly

Geografické protokoly jsou založeny na znalosti souřadnice každého uzlu. Sít tak může využívat unicast nebo multicast. Jedním z představitelům této skupiny je protokol GEAR. Jeho velká výhoda je, že uzly znají svoji aktuální zbývající energii a mohou podle toho měnit svoje cesty. Další výhoda je v lepším směrování okolo děr oproti geografickým protokolům používajícím hladový algoritmus pro směrování. Protokol MERR (Minimum energy relay routing) využívá pro směrování vzdálenost mezi uzly. Tato vzdálenost je spojována s energií potřebnou na uskutečnění směrovací cesty. Nejvýhodnější použití toho protokolu je pro lineární topologie, kde každý uzel spotřebuje stejně energie, ale pokud by byly uzly příliš blízko sebe, zbytečně by se spotřebovávala energie kvůli výběru sousedního uzlu, který se využije jako router [3, 10, 15, 17].

9 Zhodnocení síťových protokolů z hlediska odolnosti proti síťovým útokům

S rozvojem a rozšiřováním působnosti WSN se zvyšuje i počet útoků na tyto sítě. WSN sbírají data z reálného světa a v některých případech s objekty i manipulují. Tyto sítě trpí na některé typy útoku, které lze uplatnit na bezdrátové i kabelové sítě a zároveň trpí na útoky, které lze použít pouze na WSN. Jednou velkou nevýhodou WSN je fakt, že síť může být často na odlehlých místech bez jakéhokoli fyzického zabezpečení. Útočník pak může přijít a fyzicky působit na síť, vzít, přidat vlastní uzel, zničit prvky sítě nebo stáhnout, přehrát nebo smazat data ze sítě. Útoky mohou být provedeny z dálky nebo z větší blízkosti k síti za využití laptopu, tím je útok mnohem efektivnější, protože laptop může lépe komunikovat s uzly v síti. Útočník může také vložit svůj vlastní uzel, který bude imitovat uzly ze sítě a odposlouchávat komunikaci.
Bezpečnost ve WSN může být velmi důležitá. Závisí při tom na důležitosti sítě a dat, která touto sítí proudí. Některé aplikace nemá smysl zabezpečovat, a to z důvodu, že se nenajde nikdo, kdo by na tuto síť útočil. Např. útok na senzory, které monitorují vlhkost ve skleníku, nebudou útočníkovi nijak prospěšné. Na druhou stranu aplikace v armádě nebo zdravotnictví mohou být terčem útoků, které by při úspěšnosti mohly mít katastrofální dopad.

9.1 Útoky na síťovou vrstvu

Pro vytvoření falešného uzlu jsou třeba znát informace o síti a uzlu získané např. čtením paměti.

Červí díra (wormhole attack)
Útočník je vybaven alespoň dvěma uzly, pomocí kterých může oklamat zbytek sítě tím, že vlastní kanál s lepší šířkou pásma. Směrovací protokol má zájem využívat tento kanál kvůli jeho dobrým charakteristikám. Útočníci mohou poté vytvořit falešnou cestu, která je efektivní bránou do sítě. Tím přilákají velké množství provozu a umožní tak ostatní útoky na bázi černé díry. Tento útok je ve většině případech proveditelný pouze laptopem.

Černá díra a šedá díra (Blackhole attack, greyhole attack)

Při tomto útoku se útočník snaží dostat do pozice tak, aby skrze něj proudila jedna nebo více cest. Nabízí falešné výhodné směrovací cesty pro směrovací protokoly. Útočníkův uzel pak zahazuje veškerou komunikaci pocházející skrze něj.

Šedá díra je rozdílná v tom, že útočníkův uzel zahazuje jen určité procento paketů, a proto je také hůře detekovatelný než černá díra.

Výběrové směrování (Selective forwarding attack)

Tento typ útoku souvisí s útokem černá díra. Útočník nezahazuje veškerou komunikaci, ale vybírá pouze určité zprávy, které směruje dál, a ostatní zahazuje. Tento typ útoku se hůře detekuje kvůli normální ztrátovosti paketů, chybám kanálu nebo výpadku uzlů.

Útok na směrovací cesty (attack on routing path)

Útočník má k dispozici jeden nebo více uzlů sítě. Vytváří malé záškodnické útoky, které se běžně odehrávají v síti, a proto se špatně detekují. Může se jednat o zahazování vybraných paketů, vytváření smyček, vytváření méně výhodných cest, atd.

Imitace základové stanice (Sinkhole attack)

Další útok na základě útoku černé díry. Útočník se snaží zaujmout pozici, přes kterou proudí nejvíce cest. Snaží se vytvářet co nejvíce atraktivní cestu pro směrovací protokoly, nejlépe s imitací základnové stanice. Může pak významněji manipulovat se zprávami než při dvou výše uvedených útocích.

Útok na směrovací informace (Spoofed routing information)

Útočník poškozuje, pozměňuje, maže nebo znovu posílá směrovací informace a může tak vytvářet chybové zprávy, smyčky, pozměňovat nebo odstraňovat směrovací cesty, zvyšovat latenci, rozdělovat síť na části, atd.

Útok pomocí HELLO paketu (HELLO flood)

V některých směrovacích protokolech si uzly posílají pakety HELLO pro zjištění dostupnosti sousedních uzlů. Útočník může rozeslat HELLO pakety nebo odpovědi na ně. Uzly pak předpokládají, že útočník je sousední uzel. Útočník tak nabízí kratší a výhodnější cesty než ostatní sousední uzly. Uzly se pokouší odeslat pakety útočníkovi, ale nedisponují tak silným výkonem vysílače jako útočník.

Útok na reaktivní hledání cesty (Rushing attack)

Je způsob útoku na typ reaktivních směrovacích protokolů (AODV), kdy se využívá algoritmu hledání cesty. Útočníkův uzel směruje RREQ paket (paket na žádost o vytvoření cesty) bez ohledu na pravidla sítě (časové limity nebo fronty). Výsledkem je pak větší pravděpodobnost, že se útočník stane částí vytvářené cesty [19, 24].

Útok pomocí více identit najednou (Sybil attack)

Útočník se vydává za více identit najednou. Např. ve směrovacích protokolech na základě geografických informací se vydává za několik geografických souřadnic najednou. Zvyšuje tak pravděpodobnost směrování „sousedních uzlů“ přes svůj uzel.

Útok na uzel (attack on node)

Útočník se snaží oslabit nebo úplně vyřadit vybraný uzel sítě tím, že zaútočí např. na energii nebo výpočetní výkon uzlu. Útočník pak posílá uzlu úkoly nebo zprávy (např. neustálé směrování paketů sousedním uzlům), aby vyřadil jeden nebo více funkcí uzlu.

Červí díra (wormhole attack)

Útočník je vybaven uzly, které mají výkonnější hardware než typické uzly sítě. Dva spolupracující útočníci mohou oklamat zbytek sítě tím, že vlastní kanál s lepší šířkou pásma. Směrovací protokol má zájem využívat tento kanál kvůli jeho dobrým charakteristikám. Útočníci mohou poté vytvořit falešnou cestu, která je krátká a efektivní brána do sítě, tím přilákat velké množství provozu a umožnit tak ostatní útoky na bázi černé díry.

Stupnice a hodnocení

Vybráno bude několik skupin směrovacích protokolů ke srovnání podle odolnosti proti síťovým útokům. Protokoly budou srovnávány podle následujících parametrů:

- Počet proveditelných a zároveň relevantních útoků na protokoly bez použití zabezpečovacích protokolů.
- Způsob a obtížnost proveditelných útoků.
- Dopady proveditelných útoků.

9.2 Data centrické protokoly (DD, SPIN, RR)

Níže je popsán protokol RR (Rumor routing). Protokoly SPIN a DD se chovají podobně jako RR kvůli jejich společným charakteristikám, jako např. založení na data-centrickém směrování.

1) Počet proveditelných a zároveň relevantních útoků na protokoly bez použití zabezpečovacích protokolů.

Tyto směrovací data-centrické protokoly nemají žádnou základní ochranu proti útokům. Všech 10 popsaných útoků lze provést na protokoly. Proveditelné útoky: červí díra, černá díra a šedá díra, výběrové směrování, imitace základové stanice, útok na směrovací informace, útok na směrovací cesty, útok pomocí HELLO paketu (není relevantní útok na RR), útok na reaktivní hledání cesty, útok pomocí více identit, útok na uzel [24, 25, 26, 27, 28].

2) Způsob a obtížnost proveditelných útoků

V data-centrických protokolech záleží směrovací cesty na agentech (agent je paket, které proudí sítí a propaguje informace o události) se seznamem událostí. Přes tyto agenty lze vytvořit hned několik útoků. Útočník může odposlouchat agenty, směrovat více kopií sítí a vytvářet tím výběrové směrování. Může jím pokrýt větší část sítě a tím i vytvořit imitaci základové stanice. Lze také využít červí díru s využitím laptopu mezi základnovou stanici a sousední uzly. Odposlechnout agenty a využít více identit na zvýšení šance pro výběr prvního cíle pro agenta. Podobnými způsoby lze využít i další proveditelné útoky [24, 25, 26, 27, 28].

3) Dopady proveditelných útoků

Nezabezpečené sítě data-cetrických protokolů jsou naprosto bezbranné proti síťovým útokům. Lze využít nejsilnější a nejzávažnější útoky jako imitace základnové stanice, černá nebo šedá díra.

9.3 Geografické protokoly (GPSR, GEAR)

1) **Počet proveditelných a zároveň relevantních útoků na protokoly bez použití zabezpečovacích protokolů.**

Vybrané geografické protokoly mají lepší základní obranu proti útokům než data centrické protokoly, a to především z důvodu komplexnější topologie a využívání souřadnic uzlů. Využívání souřadnic ve směrování zabraňuje imitaci základnové stanice. Nelze ji napodobit, protože uzly již znají fyzickou pozici stanice a proto komunikace proudí tímto směrem. Ze stejného důvodu není efektivním útokem červí díra. Útok na reaktivní hledání cesty nelze provést z očividného důvodu – nevyužívání reaktivního typu hledání cest. Lze provést 7 z 10 vybraných útoků
Proveditelné útoky: černá díra a šedá díra, výběrové směrování, útok na směrovací informace, útok na směrovací cesty, útok pomocí HELLO paketu, útok pomocí více identit, útok na uzel [24, 25, 26, 27, 28].

2) **Způsob a obtížnost proveditelných útoků**

Velmi efektivním způsobem útoku je útok pomocí více identit. Útočník se vydává za několik uzlů najednou pomocí více souřadnic. Navrhuje ostatním uzlům „výhodnější cesty". K tomu může využít i kapacitu energie, podle které protokol GEAR směruje svoje data. Uzly útočníka budou mít pokaždé větší energii než ostatní sousední uzly. Tímto způsobem se dostane do směrovacích cest a může tak využívat dalších útoků jako výběrové směrování, černá nebo šedá díra [24, 25, 26, 27, 28].

3) **Dopady proveditelných útoků**

Dopady síťových útoků nejsou tak závažné jako u předchozí skupiny. Lze napadnout směrovací cesty geografických protokolů pomocí více identit a využít tak další útoky.

9.4 Klastrové protokoly (LEACH, TEEN, APTEEN, PEGASIS)

1) Počet proveditelných a zároveň relevantních útoků na protokoly bez použití zabezpečovacích protokolů.

Vybrané klastrové protokoly mají podobnou základní obranu proti útokům jako geografické protokoly. Největší rozdíl je v topologii a způsobu směrování. Ze stejného důvodu jsou útoky červí díry a imitace základnové stanice méně efektivní oproti protokolům tohoto typu [24, 25, 26, 27, 28].
Proveditelné útoky: černá díra a šedá díra, výběrové směrování, útok pomocí HELLO paketu, útok pomocí více identit, útok na uzel.

2) Způsob a obtížnost proveditelných útoků

Efektivním útokem na tyto typy protokolů je útok pomocí HELLO paketu a zároveň útočník musí využít laptop. Uzly vybírají hlavu klastru podle síly přijatého signálu, útočník tak může vyslat velmi silný signál do všech uzlů sítě a stát se tak hlavou klastru. Může pak využívat ostatních útoků jako výběrové směrování, černou nebo šedou díru. Aby útočník mohl zůstat delší dobu hlavou klastru, může využít útoku pomocí více identit a zastávat tak tuto pozici v každém výběrovém kole [24, 25, 26, 27, 28].

3) Dopady proveditelných útoků

Větší dopad na klastrové protokoly může mít útočník s laptopem v přístupných oblastech. Útoky do odlehlých a nepřístupných oblastí mohou být velmi náročné.

9.5 Zhodnocení

Síťové protokoly nejsou zabezpečeny proti útokům. Některé útoky nejsou efektivní z důvodu nevyužívání napadených algoritmů a funkcí. Data-centrické protokoly nemají žádnou základní obranu proti síťovým útokům a lze tak na ně uplatnit všechny možné útoky. Geografické a klastrové protokoly se dají stejně snadno napadnout, ale síť už nejde ovládat způsobem jako data-centrické, neboť jedny z nejvíce devastujících útoků jako červí díra a imitace základnové stanice nejsou tak efektivní. Protokoly je třeba zabezpečit algoritmy a bezpečnostními protokoly.

9.6 Obrana proti síťovým útokům

Směrovací protokoly nemají v základu žádnou obranu proti útokům. Některé protokoly jsou méně ovlivněny některými specifickými útoky nebo jsou dokonce imunní, protože nejsou založeny na funkcích, na které se útoky zaměřují. Je potřeba využít zabezpečovací protokoly, např. autentizační. Proti většině útoků na síťovou vrstvu se lze bránit šifrováním na linkové úrovni pomocí symetrické nebo asymetrické kryptografie. Zabraňuje se tak útokům „zvenčí" jako např. černá díra. Nezabraňuje útokům zevnitř sítě, útokům s využitím červí díry a útokům pomocí hello paketu.

Typicky se ve WSN využívá symetrická kryptografie, a to především z důvodu nižších nároků na výpočetní výkon uzlu a tím i nižší spotřebu energie. Typickými protokoly této skupiny jsou IDEA (International Data Encryption Algorithm), SHA (Secure Hash Algorithm), MD5 (Message-Digest Algorithm). Typickými protokoly asymetrické kryptografie použité ve WSN jsou RSA[2] nebo protokoly založené na ECC (Elliptic Curve Cryptography). Metoda ECC je založena na algebraických strukturách eliptických křivek nad konečnými tělesy [35].

Útoku pomocí více identit, útokuu na směrovací cesty nebo útoku na směrovací informace, může být zabráněno pomocí ověřování identit uzlů. Každý uzel má symetrický klíč sdílený s důvěryhodnou základovou stanicí, která může navzájem ověřovat identity. Základnová stanice může také limitovat počet sousedních uzlů, se kterými může jeden uzel komunikovat.

9.7 Obrana proti útokům zevnitř sítě

Útok „imitace základnové stanice" je složitější na obranu. Zvlášť obtížný je u protokolů, jež vytvářejí cesty na základě informací, které se těžko ověřují, např. zbývající energie uzlu. Cesty založené na počtu přeskoků zabraňují tomuto útoku, ale s využitím červí díry lze i tento způsob obejít. Imitace základnové stanice je neefektivní oproti protokolům založeným na geografickém směrování. Uzly směrují svoje data do základnové stanice a znají při tom její fyzickou polohu. Potom je obtížné přesunout provoz jinam pro vytvoření falešné základnové stanice.

Útoku na reaktivní hledání cesty se lze bránit pomocí ochranných opatření proti

[2] Zkratka vytvořena podle počátečních písmen zakladatelů. R – Ron Rivest, A – Adi Shamir, A – Leonard Adleman.

rozesílání paketů pro vytváření cesty, např. pokud by útočník vysílal zprávy z větších vzdáleností než je u WSN běžné. Uzly tak mohou tomuto útoku zabránit pomocí vzájemnému ověření, zda je uzel v běžném rozsahu přenosu.

Útoku pomocí HELLO paketu a útoku pomocí více identit lze zabránit pomocí symetrického sdíleného s základnovou stanicí. Dva uzly poté mohou využít některý z protokolů založený na Needham-Schroederově protokolu. Ten autentizuje komunikaci mezi dvěma uzly pomocí pěti zpráv s využitím dvou symetrických klíčů, každým z nich známým pouze základnové stanici a jednomu uzlu. Dále se využívají nonce (náhodné číslo vytvořené pro ověření komunikace) a symetrický klíč relace.

10 Závěr

Předmětem této práce je vytvořit úvod do bezdrátových senzorických sítí, představit architekturu sítě, architekturu bezdrátového uzlu, topologie sítě a síťové protokoly. Také srovnat síťové protokoly podle spotřeby energie a zhodnotit síťové protokoly z hlediska odolnosti proti síťovým útokům.

V kapitole architektura jsou představeny jednotlivé vrstvy síťové architektury, základní protokoly vrstvy a operační systém bezdrátových senzorických sítí. Dále jsou představeny jednotlivé typy topologií a je zde vysvětleno, jaké vlastnosti sítě jsou potřeba pro efektivní funkci topologii. Velmi při to záleží na aplikaci a počtu uzlů.

V kapitole o síťových protokolech je popsáno sedm od sebe odlišných protokolů. U každého protokolu je vysvětlen způsob směrování zpráv v síti a stručně nastíněny výhody a nevýhody protokolu. V další kapitole jsou srovnány některé protokoly z hlediska spotřeby energie. Byla zde snaha spíše srovnat protokoly, které spadají do stejné skupiny protokolů. Obecná spotřeba energie mezi síťovými protokoly je špatně měřitelná, protože každý protokol vyhovuje jiné topologii, jinému počtu uzlů v síti nebo jinému přístupu ke sběru dat. Nízká spotřeba energie sebou většinou nese i nevýhody, může se jednat například o delší odezvu.

V poslední části práce jsou představeny možné útoky na síťovou vrstvu a obrana protokolů proti útokům bez použití zabezpečovacích protokolů a dále popis možných bezpečnostních opatření na zabezpečení sítě.

V návaznosti na tuto práci je vhodné více se zaměřit na síťové protokoly bezdrátových senzorických sítí, zhodnotit a srovnat práci protokolů v různých podmínkách jako jsou například různé vzdálenosti mezi uzly, různé počty uzlů v síti nebo nehomogenní uzly.

Přehled zkratek

ADV – Avertisement (Nabízecí) Paket Protokolu SPIN

ASCENT - Adaptive Self-Configuring Sensor Network Topologies

ASK - Amplitude Shift Keying

BS – Base station

CDMA - Code Division Multiple Access

CSMA - Carrier Sense Multiple Access

CSMA/CA - Carrier Sense Multiple Access / Collision Avoidance

DSC - Distributed Source Coding

DSSS - Direct Sequence Spread Spectrum

EEPROM - Electrically Erasable Programmable Read-Only Memory

FCFS - First Come First Served

FDMA - Ffrequency Division Multiple Access

FRAM - Ferroelectric Random Access Memory

FSK - Frequency Shift Keying

GAF - Geographical Adaptive Fidelity

CH – Cluster head

ID – Identity - identita

ISO-OSI – International Standards Organization - Open Systen Interconnection,

LMA - Local Mean Algorithm

LMST - Local Minimum Spanning Tree

LZW - Lempel-Ziv Welch

MAC – Media Access Control

MANNA - Management Architecture For Wireless Sensor Networks

MEMS - Microelectromechanical Systems

OOK - On-Off Keying

PEAS - Probing Environment And Adaptive Sleeping

PREP – Route reply – Odpověď na paket RREQ

PSFQ - Pump Slowly, Fetch Quickly

PSK - Phase Shift Keying

Qos – Quality Of Service

RAM – Random-Access Memory

REQ – Request – Paket Na Žádost O Data

RMST - Reliable Multi-Segment Transport

RREQ - Route request – paket na žádost o cestu

SJF - Shortest Job First

SQTL - Modifikace SQL

TCP - Transmission Control Protocol

TDMA - Time Division Multiple Access

UDP - User Datagram Protocol

VFA - Virtual Force Algorithm

WLAN – Wireless Local Area Network

WSN – Wireless Sensor Network

Síťové Protokoly:

ACQUIRE - Active Query Forwarding In Sensor Networks

AODV - Ad Hoc On-Demand Distance Vector

APTEEN - Adaptive Threshold Sensitive Energy Efficient Sensor Network

APTEEN - Adaptive Threshold Sensitive Energy Efficient Sensor Network

DD - Directed Diffusion

DSDV – Destination Sequenced Distance Vector

DSR - Dynamic Source Routing

GAF - Geographic Adaptive Fidelity

GEAR - Geographic And Energy Aware Routing

GEAR - Geographic And Energy Aware Routing

GFPG – Geographic Forwarding Perimeter Geocast

GPSR - Greedy Perimeter Stateless Routing

HEED - Hybrid Energy Efficient Distributed Clustering

LEACH - Low-Energy Adaptive Clustering Hierarchy

LEACH-C - Low-Energy Adaptive Clustering Hierarchy-Centralized

MECN - Minimum Energy Communication Network

MERR - Minimum Energy Relay Routing

MMSPEED - Multipath Multi Speed

OLSR - Optimized Link Sstate Routing

PEGASIS - Power-Efficient Gathering in Sensor Information Systems

RR - Rumor Routing

SAR - Sequential Assignment Routing

SMECN - Small Minimum Energy Communication Network

SPIN - Sensor Protocols For Information via Negotiation

SPIN-BC - Sensor Protocols For Information via Negotiation -Broadcast

SPIN-EC - Sensor Protocols For Information via Negotiation – Energy Conservation

SPIN-PP - Sensor Protocols For Information via Negotiation -Point To Point)

SPIN-RL - Sensor Protocols For Information via Negotiation - Realiable

TEEN - Threshold Sensitive Energy Efficient Sensor Network Protocol

Literatura

[1] BHATTACHARYYA, Debnath, Tai-hoon KIM a Subhajit PAL. A Comparative Study of Wireless Sensor Networks and Their Routing Protocols. *Sensors* [online]. 2010, **10**(12), 10506-10523 [cit. 2016-12-01]. DOI: 10.3390/s101210506. ISSN 1424-8220. Dostupné z: http://www.mdpi.com/1424-8220/10/12/10506/

[2] DARGIE, Waltenegus. a Christian. POELLABAUER. *Fundamentals of wireless sensor networks: theory and practice*. Hoboken, NJ: Wiley, 2010.

[3] YU, Yan, Ramesh GOVINDAN a Deborah ESTRIN. *Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks* [online]. Los Angeles, USA, 2001. Dostupné z: http://webcache.googleusercontent.com-/search?q=cache:o6CJ4cgnSvoJ:citeseerx.ist.psu.edu/viewdoc/summary%3Fdoi%3D10.1.1.125.7826+&cd=2&hl=en&ct=clnk&gl=cz

[4] FISCHIONE, Carlo. *An Introduction to Wireless Sensor Networks* [online]. Version 1.8. 2014. Dostupné z: https:/www.kth.se/social/files/5431a388f276540a05ad2514/-An_Introduction_WSNS_V1.8.pdf

[5] AWERBUCH, Baruch a Amitabh MISHRA. *Ad hoc On Demand Distance Vector (AODV) Routing Protocol* [online]. Baltimore, USA, 2001. Dostupné z: http://www.cs.jhu.edu/~cs647/aodv.pdf

[6] AKYILDIZ, Ian Fuat a Mehmet Can VURAN. *Wireless sensor networks*. Hoboken, NJ: Wiley, 2010.

[7] AKKAYA, Kemal a Mohamed YOUNIS. *A survey on routing protocols for wireless sensor networks* [online]. University of Maryland, Baltimore, USA, 2003. Dostupné z: cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/RESA-M2/surveyRouting.pdf

[8] KAMAL, Ahmed a Jamal AL-KARAKI. *Routing Techniques in Wireless Sensor Networks: A Survey* [online]. Iowa, USA. Dostupné z: http://www.ics.uci.edu/~dsm/-ics280sensor/readings/networks/routing-survey.pdf

[9] KULIK, Joanna, Wendi HEINZELMAN a Hari BALAKRISHNAN. *Wireless Networks* [online]. **8**(2/3), 169-185. DOI: 10.1023/A:1013715909417. ISSN 10220038. Dostupné z: https://pdfs.semanticscholar.org/eb9a/a070103139be85868dc2de73148-ced300738.pdf

[10] GOYAL, Deepak a Malay Ranjan TRIPATHY. Routing Protocols in Wireless Sensor Networks: A Survey. In: *2012 Second International Conference on Advanced Computing & Communication Technologies* [online]. IEEE, 2012, s. 474-480. DOI: 10.1109/ACCT.2012.98. ISBN 978-1-4673-0471-9. Dostupné z: http://ieeexplore.ieee.-org/document/6168416/

[11] GURWINDER, Kaur a Garg Mohan RACHIT. *ENERGY EFFICIENT TOPOLOGIES FOR WIRELESS SENSOR NETWORKS* [online]. Indie, 2012. Dostupné z: airccse.org/journal/ijdps/papers/3512ijdps16.pdf

[12] GRILO, António. *WirelessSensor Networks Chapter 10: Topology control* [online]. Dostupné z: comp.ist.utl.pt/ece-wsn/doc/slides/sensys-ch10-topology.pdf

[13] GRILO, António. *WirelessSensor Networks Chapter2: Single node architecture* [online]. Dostupné z: comp.ist.utl.pt/ece-wsn/doc/slides/sensys-ch2-single-node.pdf

[14] HILL, Jason Lester. *System Architecture for Wireless Sensor Networks* [online]. USA, 2003 . Dostupné z: http://eps2009.dj-inod.com/docs/09-02-01/system_architecture_for_wireless_sensor_networks.pdf.

[15] 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. DOI: 10.1109/MWC.2004.1368893. ISSN 1536-1284. Dostupné z: http://ieeexplore.ieee.org/document/1368893/

[16] AKYILDIZ, I.F., W. SU, Y. SANKARASUBRAMANIAM a E. CAYIRCI. Wireless sensor networks: a survey. *Computer Networks* [online]. 2002, **38**(4), 393-422. DOI: 10.1016/S1389-1286(01)00302-4. ISSN 13891286. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1389128601003024

[17] PANTAZIS, Nikolaos A., Stefanos A. NIKOLIDAKIS a Dimitrios D. VERGADOS. Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey. *IEEE Communications Surveys & Tutorials* [online]. 2013, **15**(2), 551-591. DOI: 10.1109/SURV.2012.062612.00084. ISSN 1553-877x. Dostupné z: http://ieeexplore.ieee.org/document/6248647/

[18] ALKHATIB, Ahmad Abed Alhameed a Gurvinder Singh BAICHER. *Wireless Sensor Network Architecture* [online]. 2012. Dostupné z: www.ipcsit.com/vol35/003-CNCS2012-N010.pdf

[19] HONGMEI DENG, WEI LI a D.P. AGRAWAL. Routing security in wireless ad hoc networks. *IEEE Communications Magazine* [online]. 2002, **40**(10), 70-75. DOI: 10.1109/MCOM.2002.1039859. ISSN 0163-6804. Dostupné z: http://ieeexplore.ieee.org/document/1039859/

[20] DEHGHANI, Shahrzad, Mohammad POURZAFERANI a Behrang BAREKATAIN. Comparison on Energy-efficient Cluster Based Routing Algorithms in Wireless Sensor Network. *Procedia Computer Science* [online]. 2015, **72**, 535-542. DOI: 10.1016/j.procs.2015.12.161. ISSN 18770509. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1877050915036224

[21] ED. BY RALPH H. SPRAGUE. *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences: January 4 - 7, 2000, Maui, Hawaii ; abstracts and CD-ROM of full papers ; [HICSS-33]*. Los Alamitos, Calif. [u.a.]: IEEE Computer Soc, 2000. ISBN 0769504930.

[22] PERILLO, Mark A. a Wendi B. HEINZELMAN. *Wireless Sensor Network Protocols* [online]. Dostupné z: ww.ece.rochester.edu/courses/ECE586/readings/perillo.pdf

[23] IBBINI, Emad Mohammed, Kweh Yeah LUN, Homamad OTHMAN . *A SURVEY OF ROUTING MAC TECHNIQUES FOR WIRELESS SENSOR NETWORKS ROUTING PROTOCOL* [online]. 2015, **76**(3). Dostupné z: www.ece.rochester.edu/courses/ECE586/readings/perillo.pd

[24] DENER, Murat. Security Analysis in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks* [online]. 2014, **10**(10), 303501. DOI: 10.1155/2014/303501. ISSN 1550-1477. Dostupné z: http://journals.sagepub.com/doi/10.1155/2014/303501

[25] SADEGHI, Mohammad, Farshad KHOSRAVI, Kayvan ATEFI a Mehdi BARATI. *Security Analysis of Routing Protocols in Wireless Sensor Networks* [online]. 2012, **9**(3). Dostupné z: iauksh.ac.ir/content/users/user_iauksh/www.iauksh.ac.ir/admins/rezome%20asatid/khosravi-f/j1-2012-ijcsi.pdf

[26] JOHN, Celia a Charu WAHI. *Security Analysis of Routing Protocols for Wireless Sensor Networks* [online]. 2016, **11**(6). Dostupné z: Https://www.ripublication.com/ijaer16/ijaerv11n6_83.pdf

[27] KARLOF, Chris a David WAGNER. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks* [online]. 2003, **1**(2-3), 293-315 . DOI: 10.1016/S1570-8705(03)00008-8. ISSN 15708705. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1570870503000088

[28] KARLOF, C. a D. WAGNER. Secure routing in wireless sensor networks: attacks and countermeasures. In: *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003* [online]. IEEE, 2003, s. 113-127. DOI: 10.1109/SNPA.2003.1203362. ISBN 0-7803-7879-2. Dostupné z: http://ieeexplore.ieee.org/document/1203362/

[29] MAMUN, Quazi. A Qualitative Comparison of Different Logical Topologies for Wireless Sensor Networks. *Sensors* [online]. 2012, **12**(12), 14887-14913. DOI: 10.3390/s121114887. ISSN 1424-8220. Dostupné z: http://www.mdpi.com/1424-8220/12/11/14887/

[30] SHARMA, Divya, Sandeep VERMA a Kanika KANIKA. *Network Topologies in Wireless Sensor Networks: A Review* [online]. 2013, **4**(3). Dostupné z: www.iject.org/vol4/spl3/c0116.pdf

[31] ÁCS, Gergely a Levente BUTTY´AN. *A Taxonomy of Routing Protocols for Wireless Sensor Networks* [online]. 2007. Dostupné také z: https://www.crysys.hu/~acs/publications/AcsB06ht.pdf

[32] CHIEN, Thang Vu, Hung Nguyen CHAN a Thanh Nguyen HUU. *A comparative study on operating system for Wireless Sensor Networks* [online]. 2012. Dostupné také z: http://ieeexplore.ieee.org/document/6140770/

[33] REUSING, Tobias a Thanh Nguyen HUU. *A comparative study on operating system for Wireless Sensor Networks* [online]. 2012. Dostupné také z: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-2/NET-2012-08-2_02.pdf

[34] Nikl-metal hydridový akumulátor. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://cs.wikipedia.org/wiki/Nikl-metal_hydridov%C3%BD_akumul%C3%A1tor

[35] Kryptografie nad eliptickými křivkami. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://cs.wikipedia.org/wiki/Kryptografie_nad_eliptick%C3%BDmi_k%C5%99ivkami

[36] In: *Cooking hacks* [online]. Dostupné z: https://www.cooking-hacks.com/documentation/tutorials/waspmote/