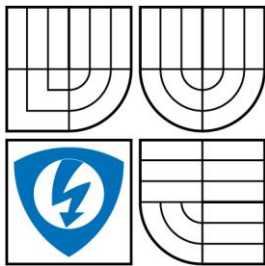


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

URČOVÁNÍ VAH SPOJŮ SMĚROVACÍCH PROTOKOLŮ V BEZDRÁTOVÝCH SENZOROVÝCH SÍTÍCH

ROUTING PROTOCOLS METRIC DETERMINATION IN WIRELESS SENSOR NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

MARTIN DUŠEK

VEDOUCÍ PRÁCE
SUPERVISOR

ING. PATRIK MORÁVEK

BRNO 2009



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Martin Dušek

ID: 73057

Ročník: 3

Akademický rok: 2008/2009

NÁZEV TÉMATU:

Určování vah spojů směrovacích protokolů v bezdrátových senzorových sítích

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou bezdrátových senzorových sítí, prostudujte směrovací protokoly používané v těchto sítích. Porovnejte určování metrik různými metodami, navrhnete a realizujete demonstrující aplikaci srovnávající výpočet trasy mezi uzly v síti podle těchto metod.

DOPORUČENÁ LITERATURA:

[1] HOLGER, Karl, ANDREAS, Willig. Protocols and Architectures for Wireless Se Networks . [s.l.] : John Wiley & Sons Inc., 2005. 481 s. ISBN 978-0-470-09510-2.

[2] FENG , Zhao, LEONIDAS, Guibas. Wireless Sensor Networks: An Information Processing Approach . [s.l.] : Morgan Kaufmann publishers Inc., 2004. 376 s. ISBN 1-55860-914-8.

Termín zadání: 9.2.2009

Termín odevzdání: 2.6.2009

Vedoucí práce: Ing. Patrik Morávek

prof. Ing. Kamil Vrba, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Abstrakt

Tato bakalářská práce se zabývá bezdrátovými sensorovými sítěmi z pohledu směrovacích protokolů a metriky. Je zde popsán obecný pohled na tyto sítě a jejich srovnání s IP sítěmi. Dále jsou popsány některé skupiny protokolů sensorových sítí a uvedeni zástupci používaných protokolů pro každou skupinu. Je zde taktéž rozebrán vliv metriky na výběr cesty a představeny dvě metody jejího výpočtu. Na závěr byla navržena aplikace, která simuluje použití jednotlivých druhů metriky pro vyhledávání cesty a zobrazuje rozdílně vyhodnocené cesty.

Klíčová slova

senzor, bezdrátové sensorové sítě, směrování, směrovací protokoly, metrika, váha spojů

Abstract

This bachelor's thesis deals with wireless sensor networks (WSNs) in terms of routing protocols and metrics. There is described common view on these networks and their comparison with IP networks. In addition, some types of protocols, used in WSNs, are described and representatives of each type are included. There is also considered influence of metrics on a route selection and presented two methods of calculation. In conclusion, an application, that simulates the use of each type of metrics for path search and displays the differently evaluated paths, is designed.

Key words

sensor, wireless sensor networks, routing, routing protocols metric

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Patriku Morávkovi za velmi věcnou metodickou pomoc, cenné rady při zpracování bakalářské práce a její odbornou konzultaci.

Martin Dušek

Bibliografická citace práce

DUŠEK, M. *Určování vah spojů směrovacích protokolů v bezdrátových senzorových sítích*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 45 s. Vedoucí bakalářské práce Ing. Patrik Morávek.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma “Určování vah spojů směrovacích protokolů v bezdrátových senzorových sítích,, jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení - § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 19. 5. 2009

Martin Dušek

Obsah

Úvod.....	9
1 Bezdrátové senzorové sítě.....	10
1.1 Srovnání s ostatními sítěmi	11
2 Směrování v IP síti	13
3 Směrování ve WSN.....	15
4 Datacentrické (datacentric) protokoly	19
4.1 SPIN	20
4.2 Directed Diffusion.....	21
5 Hierarchické protokoly.....	23
5.1 LEACH	23
5.2 PEGASIS.....	24
5.3 TEEN a APTEEN.....	25
6 Geografické protokoly.....	26
6.1 GAF.....	26
6.2 GEAR.....	27
7 Směrování s metrikou.....	29
7.1 ETX metrika.....	29
7.2 MOR/MER.....	30
8 Srovnání metrik směrovacích protokolů v navržené aplikaci.....	32
8.1 Generování sítě.....	36
8.2 Směrování	36
9 Závěr.....	42
Seznam použité literatury	43
Seznam zkratk.....	44
Médium	45

Seznam obrázků

Obr. 1 – Základní struktura bezdrátové sensorové sítě.....	11
Obr. 2 – Fáze rozesílání dat v protokolu SPIN	20
Obr. 3 – Jednotlivé fáze v protokolu Directed diffusion.....	22
Obr. 4 – Schéma směrování v hierarchickém PEGASISu.....	24
Obr. 5 – Schéma změny stavů senzoru v GAF	26
Obr. 6 – Schéma části sítě protokolu GAF	26
Obr. 7 – Schéma části sítě s jejím ohodnocením.....	30
Obr. 8 – Vývojový diagram navrhované aplikace – část 1.	33
Obr. 9 – Vývojový diagram navrhované aplikace – část 2.	34
Obr. 10 – Základní vzhled aplikace s vygenerovanou sítí bez typických situací	35
Obr. 11 – Vývojový diagram Dijkstrova algoritmu.....	37
Obr. 12 – Směrování shodnou cestou	38
Obr. 13 – Směrování rozdílnou cestou – lokální diference	39
Obr. 14 – Směrování rozdílnou cestou – samostatné cesty	40
Obr. 15 – Směrování rozdílnou cestou – delší samostatné cesty.....	40
Obr. 16 – Osamocené senzory.....	41

Úvod

Obecné komunikační sítě obsahují větší množství jednotlivých propojených bodů (základnových stanic, síťových prvků, routerů, senzorů) a vytváří tedy mnoho možných cest od jednoho bodu sítě k druhému. Právě kvůli existenci několika cest mezi dvěma vzdálenými body, je nutné mezi těmito cestami vybírat. Každý prvek může mít spojení s několika sousedními prvky a každé toto spojení je definováno určitým množstvím parametrů. Tyto parametry jsou různými způsoby vyhodnocovány a podle definovaných pravidel je jim přidělena váha (nebo také cena, metrika). Patří mezi ně například rychlost, chybovost a zpoždění spojení, ale i cena za použití tohoto spoje, pokud nejsme jeho vlastníky. Pravidla, podle kterých se jednotlivé parametry spojení vyhodnocují, určuje mimo jiné i typ sítě. V páteřní části počítačové sítě budou relevantní jiné parametry než v přístupové části, stejně tak v senzorové síti nás budou zajímat úplně jiné parametry než v síti telefonní.

V teoretické části se tato práce bude zabývat obecnými IP sítěmi a porovnávat je se sítěmi senzorovými. Dále se bude hlouběji věnovat několika konkrétním protokolům používaným v těchto senzorových sítích a i způsobům určení metriky.

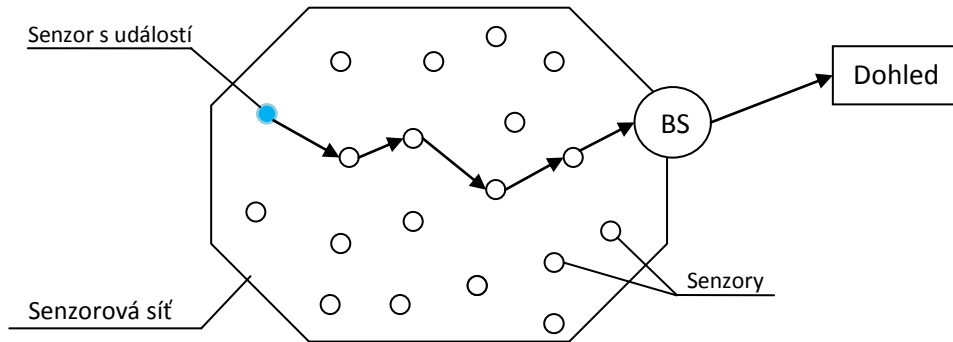
V praktické části pak bude vytvořena aplikace, pomocí níž bude demonstrován vliv různých typů metriky na výběr cesty.

1 Bezdrátové senzorové sítě

Bezdrátové senzorové sítě (Wireless Sensor Networks, WSNs) jsou velmi rozsáhlé sítě skládající se z velkého množství samostatných prvků (senzorů) a hlavní základnové přijímací stanice – BS (Base Station, někdy označována jako Gateway). Jednotlivé senzory, anglicky pojmenované nodes, jsou miniaturizovaná, nízkonákladová zařízení, která dle svého zaměření zaznamenávají vlastnosti svého okolí, převádí je na elektrický signál a předávají základnové stanici. Může se jednat například o sledování teploty, pohybu, tlaku, světla, zvuku, přítomnosti látek nebo různých polí a vlnění. Dále jsou vybavena bezdrátovým komunikačním rozhraním a zdrojem energie, nejčastěji baterií.

Běžným příkladem použití může být třeba sledování vzniku požáru v lese. Velké množství senzorů, řádově stovky až tisíce, jsou rozprostřeny po ploše, která má být sledována, například pomocí letadla. Na okraj lesa se umístí základnová stanice (BS), která je vybavena připojením k Internetu, případně mobilním nebo jiným komunikačním zařízením. Poté senzory sledují teplotu ve svém okolí. Pokud v některém místě dojde ke vzniku požáru, nejbližší senzory zaznamenají zvýšení teploty nad zadanou mez a tuto informaci odešlou směrem k BS. Topologie sítě, cesta k BS a další potřebné informace jsou zjištěny buď po rozmístění, nebo právě při vzniku události, záleží na použitých protokolech. Dále se daná informace o monitorované veličině dostane k BS, dojde k jejímu vyhodnocení, a pokud výsledek potvrdí skutečný vznik požárů, BS přes zmíněné komunikační rozhraní informuje příslušné operační středisko. Vyhodnocení skutečného vzniku události a rozlišení od planých poplachů lze provádět například podmíněním příchodu podobné informace od několika senzorů. Dalším příkladem může být přidávání senzorů do stavebních materiálů a sledování tlaku a vyhodnocování statiky budov. Původním záměrem, jak je u těchto technologií běžné, bylo vojenské využití na bitevním poli, kvůli sledování pohybu nepřátelských vojsk, přítomnosti bojových látek v ovzduší, nebo pátrání po přeživších po útoku.

Na Obr. 1 je uvedeno základní schéma bezdrátové senzorové sítě, kde je rozmístěno několik senzorů, vyhodnocená událost a posílání informace přes sousední senzory k základnové stanici a přes Internet nebo mobilní síť ke zpracování uživatelem v dohledovém centru.



Obr. 1 – Základní struktura bezdrátové senzorové sítě, včetně předávání informace o události

Největším omezením pro bezdrátové senzorové sítě je zdroj energie pro jednotlivé senzory. Celé zařízení je již od počátku koncipováno pro velmi omezenou kapacitu baterie a nadále jsou vyžadovány a vyvíjeny nové technologie, postupy a způsoby komunikace, přizpůsobené těmto limitům. Energetická náročnost je největší po vyhodnocení události při vysílání dat. Proto lze největší úsilí vložit právě do snižování nároků ve všech vrstvách aplikovaného komunikačního protokolu. Například na síťové vrstvě je velice žádoucí nalezení energeticky nejvýhodnější cesty k BS, posílání dat přes co nejméně senzorů a tím prodloužení životnosti celé sítě.

1.1 Srovnání s ostatními sítěmi

Ve srovnání s ostatními sítěmi se WSN liší v mnoha ohledech. Například množstvím prvků, které je mnohonásobně větší, a tedy je prakticky nemožné vytvoření obecného systematického adresového schématu. Nelze použít protokoly používané v IP sítích, zejména kvůli jejich nepřizpůsobenosti energetické náročnosti. Navíc, senzory jsou provozovány v režimu Ad-hoc a je nutné, aby samostatně budovaly spojení na základě aktuální situace ve svém okolí. Toto je nutné vzhledem k možnosti ztráty některých spojných bodů v důsledku například ztráty energie daného bodu.

Dalším rozdílem ve velké většině aplikací, využívajících senzorové sítě, je proti ostatním sítím tok dat od mnoha zdrojů k jediné BS, což vnáší nadbytečnost posílaných dat, které protokoly mohou omezit a tím ušetřit energii. Také je zde nebezpečí vzniku kritických míst (bottleneck), ve kterých vlivem příjmu velkého toku dat dojde k přetížení a také k rychlému vyčerpání energie. U senzorových sítích jsou rovněž omezené možnosti ukládání a zpracování dat, proto se musí těmto omezením přizpůsobovat jednak protokol a jednak samotná konstrukce zařízení.

Ve většině případů jsou senzory, až na několik výjimek¹ statické, nepohyblivé, na rozdíl od běžných bezdrátových sítí, kde jsou připojené body (notebooky, mobilní telefony atp.) pohyblivé. Dále na rozdíl od IP sítí je u sensorových pevně definováno jakým způsobem bude síť využívána a pokud dojde ke změně využití, dojde také k fyzické změně sítě. Například jiné vlastnosti bude mít síť pro taktické sledování bojiště a síť pro kontrolu počasí. Ve většině případů tedy nelze využít jednu síť pro několik aplikací.

Odlišností je také důležitost pozice zdroje informace. V již zmíněném příkladu sledování vzniku požáru, je nutné nejen vědět, že k němu došlo, ale také kde. V současnosti implementace GPS čipů do senzorů je stále ještě poměrně nákladná, přesto jsou již vyvíjeny nízkonapěťové snímače. Pro lokalizaci zdroje se také využívá například metoda triangulace. Tato metoda využívá měření velikosti signálu zdroje informace na několika senzorech se známou pozicí. Na okraj sledované oblasti se rozmístí pouze několik senzorů s GPS čipem, nebo se jejich pozice zaznamená při umístění.

¹ Některé aplikace používají senzory na vojácích nebo třeba na mobilních sledovacích jednotkách, které objíždějí sledovanou oblast

2 Směrování v IP síti

Podle [2] je směrování pojem, který zahrnuje všechny postupy, které se používají pro předávání datových paketů v síti. Směrování vždy řeší pouze jeden krok, kam předat paket dále a nezabývá se celou jeho cestou od adresáta k příjemci.

Základním elementem pro směrování je směrovací tabulka. Jedná se o soupis všech dostupných sítí na všech aktivních rozhraních, daného zařízení. Každý záznam obsahuje adresu sítě a rozhraní, na které se přijatý paket posílá. Každá tabulka by také měla obsahovat výchozí cestu, která je určena pro všechny pakety směřující do sítě, kterou dané směrovací zařízení nezná. Na druhém konci této cesty je většinou další síťový prvek, který již ví, kam daný paket zaslat, případně jej odešle dále po své výchozí cestě.

Směrovací tabulka musí být udržována aktuální a to se děje pomocí dvou typů směrovacího algoritmu - statického a dynamického. Statické (neadaptivní) směrování ponechává aktualizaci směrovací tabulky na ručním nastavení a je definováno například nastavením počítače. Toto řešení, ač se zdá nevhodné, se používá na většině směrovacích zařízení. Zejména je užito v koncových částech sítě (u koncových stanic), kde je situace tak jednoduchá, že použití dynamického směrování by bylo zbytečné. Většina těchto situací obsahuje jedinou cestu na odchozí směrovač. Naopak dynamické směrování se používá v hierarchicky vyšších vrstvách sítě, kde se topologie může častěji měnit, kde dochází k výpadkům spojů a je nutné automaticky udržovat tabulky aktuální.

Způsobů, jak se provádí aktualizace směrovacích tabulek je několik. Mezi nejčastěji používané patří směrování hierarchické a distribuované.

Distribuované algoritmy jsou založeny na postupném šíření informací o změnách směrovacích tabulek mezi sousedící směrovače. Toto řešení je dostatečně silné i pro rozsáhlé sítě a v podstatě je na něm založený Internet. Jednotlivé přístupy k šíření informací jsou velice rozdílné. Nejvýznamnějšími zástupci protokolů s distribučním algoritmem jsou RIP, OSPF nebo BGP.

Hierarchické algoritmy jsou vhodné pro rozsáhlé sítě, které rozdělují na několik samostatných oblastí, uvnitř kterých se informace o změnách šíří takzvaným zaplavováním (flooding). Příkladem může být opět OSPF protokol. Jde o princip, kdy se informace šíří od jednoho směrovače ke všem ostatním, kromě toho, od kterého informace přišla. Výměnu informace mezi oblastmi zajišťují tzv. hraniční směrovače, které si předávají pouze souhrnné informace o dané oblasti.

Mezi další příklady lze uvést:

- náhodné směrování – zahlcený směrovač místo zahození zašle paket do náhodné sítě a neprohledává směrovací tabulku,
- směrování přímo ke zdroji – směrovač nejprve zaplaví síť s požadavkem na cílový prvek, ten pokud je dostupný, odpoví, včetně té nejkratší cesty k němu,
- centralizované směrování – všechny záznamy o síti se zasílají do centrálního systému, který tak získává kompletní přehled o celé síti a pak záplavově šíří vyhodnocené směrovací tabulky,
- zpětné učení – směrovač se učí dostupné síť na základě příchozích paketů, které pak pokud nezná příjemce, rozesílá do všech směrů.

Pro většinu spojení v IP síti existuje více než jedna cesta. Může to být prostřednictvím záložní linky, nebo například přes jiné síť, jiné poskytovatele. V tomto případě je důležité vybírat tu nejvhodnější cestu. Jak již bylo zmíněno, pro popis cesty se používají různé parametry, které použitý protokol vyhodnocuje a přiděluje příslušnou metriku (váhu) spoje. Mezi tyto parametry patří rychlost spoje, zpoždění, počet skoků (hop count), spolehlivost spoje, zatíženost, šířka pásma, maximální velikost datového bloku a podobně. Podle [2] například **RIP** (Routing Information Protocol) jako metriku používá délku cesty do dané sítě. Pro její výpočet používá Bellman-Fordův algoritmus, jehož výsledkem je nejkratší počet skoků (počet směrovačů v cestě) včetně celé cesty. Do směrovací tabulky se pak zapíše adresa cílové sítě a daná metrika.

Dalším protokolem používajícím metriku je protokol **OSPF** (Open Shortest Path First). Také v tomto případě se hledá nejkratší cesta k danému cíli. Pro vyhledání nejkratší cesty se používá Dijkstrův algoritmus. Po jeho proběhnutí se vloží do směrovací tabulky cílová adresa, adresa nejbližšího směrovače ve vypočtené trase a rozhraní, na kterém je tento směrovač dostupný.

Dalším zástupcem protokolů používajících metriku je **BGP**. Směrovací tabulky v tomto případě obsahují stovky a tisíce záznamů současně s informací o ceně cesty. Tentokrát nezáleží pouze na vzdálenosti cíle, ale posuzují se také ostatní nastavitelné parametry zohledňující například cenu a dodatečná pravidla aplikovaná v závislosti na zdroji, cíli, seznamu tranzitních autonomních systémů a dalších atributech. Stejně jako u OSPF se používá diferenční aktualizace směrovacích tabulek, neposílají se tedy celé tabulky jako u RIP, ale rozesílají se pouze změny, ke kterým došlo.

3 Směrování ve WSN

Dle [1] je při vytváření protokolů pro bezdrátové sensorové sítě důležité brát v úvahu jejich vlastnosti, současně s ohledem na nároky aplikací a architektur, které chceme v těchto sítích použít. Z hlediska struktury sítě lze protokoly rozdělit na plošné, hierarchické a geografické. V plošných sítích mají všechny senzory stejnou úlohu. V hierarchických sítích se celý prostor dělí na oblasti, kde je vždy jeden senzor nadřízený ostatním a může shromažďovat a následně redukovat nadbytečná data a tím ušetřit energii. Volba nadřízeného senzoru je většinou řízena podle energetické úrovně a je jím stanoven senzor s nejvyšší energií. Geografické sítě využívají informace o pozici ke směrování do požadovaných oblastí, místo do celé sítě.

Základní otázky, kterými se návrh protokolu řídí, lze rozdělit na následující:

- *Rozmístění senzorů:* Rozmístění má velký vliv na chování protokolu, a proto je důležité vzít tento fakt při návrhu v potaz. Rozmístění může být náhodné nebo deterministické. Při deterministickém rozložení jsou senzory rozmístěny manuálně a směrování probíhá podle předem definovaných cest. Na rozdíl od náhodně rozmístěných senzorů, které vytvářejí síť typu Ad-hoc, kde vyvstává nutnost optimalizace shlukování senzorů pro vytvoření vhodných spojení a umožnění efektivního využívání energie.
- *Spotřeba energie bez ztráty přesnosti:* Během procesů vyhodnocování informací a jejich následného vysílání mohou senzory brzy vyčerpat své omezené zásoby energie, a je proto nutné nalézt postupy a metody, které budou touto energií šetřit. V sensorových sítích hraje každý senzor dvojí roli – vysílač vlastních a směrovač cizích dat. Právě neschopnost směrování v důsledku ztráty energie vede ke změně topologie a případnému nucenému vyhledávání nových cest a opakovanému směrování dat.
- *Způsob vysílání dat:* Každá aplikace využívající bezdrátové sensorové sítě může využívat jiný způsob získávání dat. Tyto způsoby lze rozdělit na řízené časem, událostí, žádostí a kombinované. Způsob řízený časem je vhodný pro aplikace, kde je třeba data získávat pravidelně, periodicky, například při sledování počasí nebo podmínek prostředí. Řízení událostí nebo žádostí je naopak vhodné v případě, že sledovaná veličina je stabilní a nás zajímá, pouze pokud dojde k její změně, nebo nás zajímá v nepravidelných časových intervalech, kdy žádost vysílá BS. Příkladem je výše zmíněné sledování

vzniku požáru v lese, nebo například zjištění aktuálních podmínek před vstupem osob do sledovaného prostoru. Kombinace těchto způsobů je rovněž často využívána, například při sledování několika veličin, kdy některé nás zajímají pravidelně a některé pouze při překročení definované meze.

- *Heterogenita senzorů:* Většina studií v tomto oboru pracuje se senzory jako s homogenní sítí, tzn., že všechny senzory mají shodnou kapacitu baterie, shodnou výpočetní a paměťovou výbavu. V praxi se však s homogenitou setkáme velice vzácně. V závislosti na aplikaci mají senzory různé role ve snímání dat. Některé mohou být určeny pouze pro sběr několika informací typu teploty nebo tlaku, jiné mohou být vybaveny zařízením pro detekci pohybu a snímání zvuku nebo obrazu, další mohou být kombinované. Odlišné parametry také bude mít senzor, který již od počátku bude vybrán jako nadřazený v určité oblasti.
- *Tolerance výpadků:* Během provozu sítě může dojít k výpadku funkce jednoho nebo několika senzorů z důsledku poklesu napětí, fyzického poškození nebo rušení prostředí. Tyto výpadky by neměly mít vliv na celkovou funkčnost sítě a protokol se musí umět postarat o změny cest dat do sběrné základnové stanice. Toto může znamenat změny vysílacích výkonů několika senzorů a přesměrování dat přes oblasti, kde je dostatek energie. V důsledku toho je větší požadavek na redundanci dat, kvůli opravě chyb v těchto sítích s tolerancí výpadků.
- *Dostupnost:* V takto rozsáhlých sítích je nutné, aby i protokoly byly přizpůsobeny k řízení velkého množství prvků. Ve většině času mohou být senzory ve stavu spánku a k aktivitě se probudí teprve ve chvíli příchodu události. Protokol musí být tedy schopen reagovat na posílání dat z jednoho a zároveň z opačného konce sítě.
- *Dynamika:* Většina sítí je statických, ale existují případy, kdy je nutné, aby se základnová stanice nebo některé senzory pohybovaly. Zasílání dat mezi pevným a pohyblivým bodem se takto stává velkou překážkou, protože stálost směrovací cesty je pro energetickou náročnost velice důležitá. Navíc i sledovaný jev může být statický (v případě požáru v lese) i dynamický (sledování pohyblivého cíle). Při statickém jevu stačí v případě jeho výskytu vygenerovat potřebná data, nalézt BS a data zaslat. V případě dynamického

jevu je žádoucí pravidelný nebo stálý datový tok s informacemi o sledovaném pohybu, kde změna polohy BS může vyvolat značné potíže.

- *Přenosové médium:* V bezdrátových sensorových sítích, jak z názvu vyplývá, je přenosovým médiem vzduch, přesněji elektromagnetické vlnění. U tohoto média se setkáváme s problémy vysoké chybovosti nebo četnosti úniku signálu, které také ovlivňují spotřebu energie sensorů. Vyžadovaná šířka pásma je nízká, v rozmezí 1 – 100kbps. V tomto ohledu je také důležité řízení přístupu k přenosovému mediu. Využívají se například protokoly založené na TDMA (Time Division Multiple Access – vícenásobný přístup k mediu pomocí dělení dat od více uživatelů do několika časových rámců), které jsou méně energeticky náročné než protokoly založené na CSMA (Carrier Sense Multiple Access – vícenásobný přístup k mediu, kterému předchází naslouchání na nosné frekvenci). Je možné také použít technologii Bluetooth.
- *Pokrytí:* Vzhledem k velkému množství sensorů v síti je velice nepravděpodobné, že jeden sensor zůstane osamocen. i přesto díky výpadkům sensorů se síť během své životnosti zmenšuje a řídne. Je vhodné brát také v úvahu, že každý sensor má určitou oblast pokrytí fyzického prostoru, omezenou jednak dosahem a jednak přesností.
- *Seskupování dat:* Vzhledem k velké četnosti sensorů mohou některé blízké detekovat stejnou událost, čímž dojde ke vzniku redundantních dat. Při jejich seskupování například u nadřazených sensorů lze tato data posuzovat a inteligentně je zpracovávat. Odstraňovat duplicitu, vyhodnocovat statistická data a tak omezit výsledný datový tok.
- *Quality of Service:* Řízení datových toků proti zahlcení sítě se používá i v sensorových sítích u aplikací, pro které je důležitá aktuálnost údajů. Pokud dojde ke značnému zpoždění informace od jejího vzniku do jejího doručení, může být informace pro nás již bezpředmětná. Přesto u některých typů sítí dojde při snížené hladině energie k upřednostnění efektivního využití zbylých zásob a k potlačení QoS.

Dalším parametrem směrovacího protokolu je chvíle, kdy se vypočítávají směrovací cesty. Rozdělit protokoly proto můžeme na proaktivní, reaktivní a hybridní (kombinované). Proaktivní protokoly vypočítávají směrovací cesty ještě před jejich upotřebením (například po rozmístění), zatímco reaktivní protokoly tyto cesty

vypočítávají až na vyžádání, těsně před vysláním. Jako další skupinu lze zařadit protokoly kooperativní. Jedná se o případ, kdy se data zasílají do centrálního senzoru, který je shromažďuje a vyhodnocuje, podobně jako v hierarchických protokolech, zde je však jen jeden centrální prvek.

Do této doby byl představen pouze obecný pohled na sensorové sítě a jejich srovnání s obecnými sítěmi, obecně bylo nastíněno směřování v IP síti a předloženo několik konkrétních příkladů směrovacích protokolů včetně využívané metriky. V další části této práce budou představeny konkrétní skupiny protokolů a jejich zástupců pro směřování v sensorových sítích.

Nejprve budou protokoly rozděleny podle [3] na „datacentrické“ (přejato z anglického datacentric), hierarchické a geografické. V každé kategorii pak budou podrobněji rozebrány funkce několika zástupců. Na závěr budou zmíněny protokoly využívající metricku.

4 Datacentrické (datacentric) protokoly

Jak již bylo zmíněno, v senzorových sítích nelze používat klasické adresování, které známe z IP sítí vzhledem k obrovskému počtu prvků sítě. Je proto velice obtížné například určit správné senzory, kterým chceme zaslat žádost na jejich aktuální stav a žádaná data proto odcházejí od senzorů ve značně nadbytečném počtu, s velikou redundancí. Toto je velice neefektivní vzhledem k požadavku na nízkou spotřebu energie. Proto byly vyvinuty protokoly, které jsou schopny zajistit agregaci (shromáždění) dat, jejich filtraci a odstranění nadbytečnosti a tím i efektivnější nakládání s omezenou energetickou zásobou. V datacentrických protokolech BS vyšle požadavek do oblastí se specifickými senzory a očekává jejich data. Protože jsou tyto žádosti vysílány neadresovaně, je nutné zavést jmenování vlastností, které identifikuje požadovaná data. Každý senzor, který tuto žádost přijme, vyhodnotí žádaná data a pokud jeho data těmto odpovídají, odešle odpověď.

Dva protokoly SPIN a Directed Diffusion jsou základními kameny pro většinu ostatních datacentrických protokolů. Jejich klíčové vlastnosti – popsané v [3] – jsou zaplavování a tzv. gossiping (náhodný výběr). Při zaplavování každý senzor posílá přijatá data na všechny strany, všem sousedním příjemcům, dokud paket nedorazí do místa určení, nebo nepřekročí počet povolených skoků. Gossiping funguje na podobném principu s tím rozdílem, že data nejsou vysílána všem sousedním senzorům, ale pouze jednomu, náhodně vybranému. Tento vybraný senzor postupuje shodně, tedy opět náhodně vybere svůj sousední senzor a jemu data zašle.

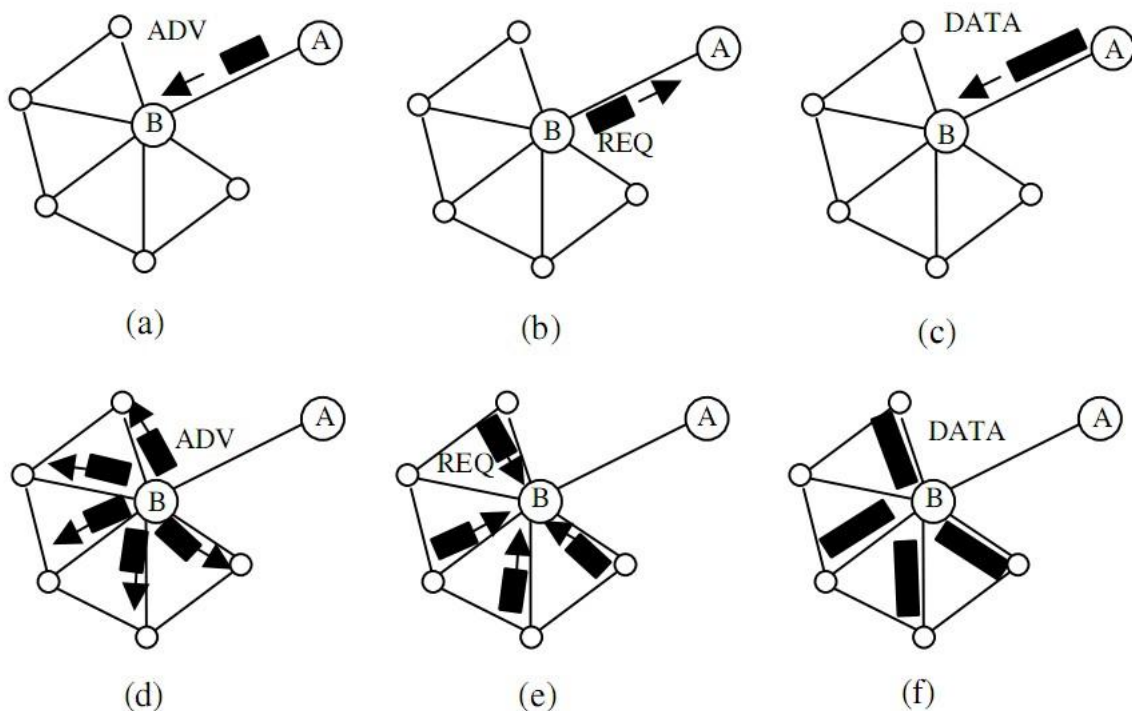
Implementace principu zaplavování je velice jednoduchá, ale přináší také nedostatky. Jedním z nich je zahlcení senzorů přijímáním identických informací od okolních sousedů a také přijímání podobných informací od několika senzorů pokrývajících stejnou oblast. Dalším problémem zejména při zaplavování je tzv. „oslepení“, kdy přijímač přijímá velké množství energie od několika sousedních senzorů, ale není schopen rozeznat jednotlivé datové toky. Gossiping eliminuje přijímání identických informací právě díky náhodnému výběru příjemce, nicméně tento princip vnáší velké zpoždění v doručení dat a nezaručuje dosažení všech senzorů.

4.1 SPIN

První protokol, který se v této oblasti objevil je **SPIN** (**S**ensor **P**rotocols for **I**nformation via **N**egotiation). Hlavní ideou tohoto protokolu je podle [3] definice dat na vyšších úrovních pomocí metadat. Metadata jsou před vysláním samotných informací rozeslána do okolí a očekává se příjem žádostí, na jejichž základě pak dojde k samotnému přenosu užitečných informací (dat). Poté senzor, který nová data přijal, opět tuto informaci zveřejní svému okolí, a kdo o ně projeví zájem, tomu je pošle. Tímto se dosahuje vysoké úrovně úspory energie. SPIN nijak nedefinuje metadata, která jsou závislá na využití senzorové sítě, a tedy nechává prostor pro přizpůsobení na míru aplikaci. V tomto protokolu se definují pouze zprávy zasílané mezi senzory a to:

- ADV – oznámení nově přichozích dat a vyjádření nabídky jejich zaslání
- REQ – zpráva pro vyžádání oznámených dat
- DATA – pro samotná užitečná a vyžádaná data.

Obr. 2, převzatý z [4] popisuje princip rozesílání dat.

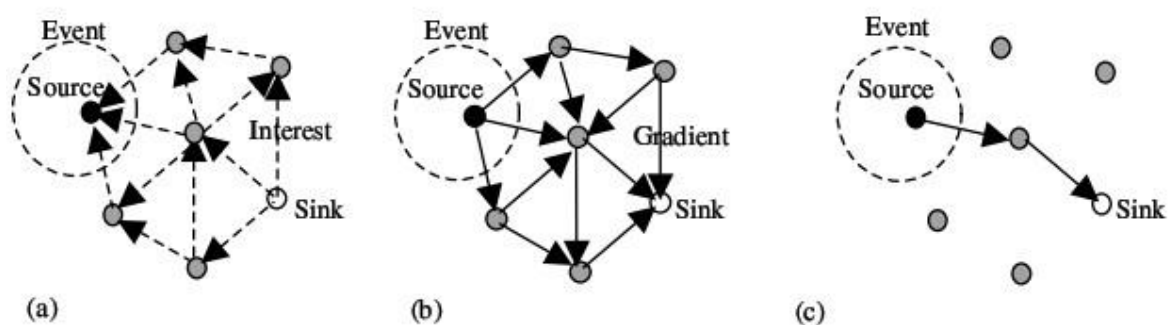


Obr. 2 – Fáze rozesílání dat v protokolu SPIN: (a) senzor A rozešle oznámení ADV o nově přijatých datech, (b) senzor B vyhodnotí metadata a projeví o oznámená data zájem zprávou REQ, (c) A reaguje na žádost a zasílá data, (d) stejně tak B oznamuje a šíří přijatá metadata (e,f) – ([4])

4.2 Directed Diffusion

Dalším významným protokolem je v [3] popsán **Directed Diffusion** (řízený rozptyl). Styčným bodem tohoto protokolu je využití dvojic atributů pro data a pro žádosti. Při vzniku žádosti o data je ze základnové stanice přes sousední senzory vyslána zpráva se zájmem o data (interest), která je definovaná právě uvedenými atributy. Atributy mohou být například jméno zdrojového objektu, geografická oblast, interval vysílání, trvání vysílání a podobně. Senzory při přeposílání zpráv se zájmem (interests) využívají uchovávání těchto zpráv pro jejich pozdější využití při příjmu užitečných dat. Z přijaté zprávy jsou v senzoru uchovávány také gradienty. Gradient je v podstatě informace o cestě, vedoucí zpět ke zdroji přijaté zprávy (interest). Je charakterizován datovým tokem, trváním nebo informací o expiraci zprávy, odvozené při jejím přijetí.

Využitím všech těchto informací vede k sestavení pevných cest mezi základnovou stanicí (zdrojem zpráv obsahujících zájem o určitá data) a jednotlivými senzory směřujícími k cílové oblasti. Těchto cest může být v senzoru uloženo několik a to nejen z důvodu úspory energie při výpadku sestavené cesty. Senzory tak nemusí znovu vysílat do svého okolí, aby zjistily další možné cesty k BS ale místo toho využijí záznamy již dávno uchované v paměti. Tyto náhradní cesty jsou průběžně využívány velmi nízkým datovým tokem, který sice spotřebovává energii senzoru, ale tato energie je v konečném důsledku mnohem nižší, než energie potřebná na kompletní nalezení nové cesty. Pro přeposílání zpráv základnovou stanicí je první sestavená cesta používána nejčastěji, čímž udržuje vysokou pozici vybudované cesty ve své směrovací tabulce. Ostatní cesty jsou pak udržovány s nižší hodnotou a tedy ponechávány jako záložní a pro přenos dat využívány méně často. Obr. 3 přejatý z [5] popisuje jednotlivé fáze z Directed diffusion protokolu.



Obr. 3 – Jednotlivé fáze v protokolu *Directed diffusion*: (a) zaplavování sítě zprávami obsahujícími zájem o specifikovaná data, (b) vyhodnocování gradient a sestavování cest, (c) výběr nejsilnější cesty a zaslání dat

Protokol *Directed diffusion* se od *SPIN* liší především ve způsobu žádání o data. Protokol řízeného rozptylu zaplavuje síť žádostmi o specifická data, kdežto *SPIN* naopak oznamuje dostupnost těchto dat a vyzývá k jejich vyžádání. *Directed diffusion* má několik klíčových výhod. Protože patří do skupiny datacentrických protokolů, veškerá komunikace probíhá pouze mezi sousedícími senzory bez nutnosti jakékoliv adresace známé z IP sítí. Každý ze senzorů je také schopen filtrovat přijímaná data a s pomocí uchování zmíněných informací o zprávách a cestách tak výrazně snižuje energetickou náročnost. To také podporuje jeho použití pro sítě, založené na zaslání dat pouze na vyžádání kde není potřeba udržovat síťovou topologii. Toto je však také nevýhodou v podobě nemožnosti využití tohoto protokolu pro všechny typy sensorových sítí.

Jako další zástupce způsobů směřování ze skupiny datacentrických protokolů, které jsou odvozeny ze dvou výše uvedených, lze uvést například „šíření zvěstí“, které spočívá ve využívání dlouho-žijících paketů, které obíhají sítí a oznamují výskyt události na daném senzoru společně i s cestou k němu. Základnová stanice, která pak vysílá žádost o tato data, brzy dostane odpověď s cestou k dané zaznamenané události. Dalšími zástupci jsou protokoly *GBR*, *CADR*, *COUGAR* nebo *ACQUIRE* – viz [3].

5 Hierarchické protokoly

Jako ve většině sítí je škálovatelnost jedním z nejvýznamnějších prvků návrhu i pro sítě sensorové. V případě použití jediného okrajového bodu pro aplikaci vyžadující větší datový tok, který celý prochází přes tento bod směrem k základnové stanici, dochází často k jeho přetížení a tedy ke zpoždění a případně k velice rychlému vyčerpání zásob energie. V takovémto případě může dojít po krátké době k „odstrižení“ základnové stanice od zbytku sítě, z důvodu výpadku nejbližších sensorů.

Hierarchické protokoly jsou využívány zejména u rozsáhlých sítí, kde není možné použití ani komunikace všech sensorů přímo se základnovou stanicí. Pro rozložení zátěže datového toku bez omezení funkčnosti sítě byly vyvinuty právě hierarchické protokoly. Ty jsou založeny na rozdělení sítě na několik oblastí (clusters). V každé oblasti je pak stanoven hlavní sensor (cluster-head), který je buď vybrán z běžných sensorů, nebo je například manuálně umístěn a vybaven větší hardwarovou výbavou, zejména větším zdrojem energie. Tento „nadřazený“ sensor je pak bránou pro ostatní senzory v dané oblasti a všechny směřují buď přímo, nebo přes ostatní senzory veškerý datový tok na něho. Nadřazený sensor data shromažďuje, odstraňuje redundanci a směřuje data dále přes další senzory stejné nebo vyšší úrovně, nebo přímo na základnovou stanici.

5.1 LEACH

Jako první hierarchický byl dle [3] vyvinut protokol **LEACH** (**L**ow-**E**nergy **A**daptive **C**lustering **H**ierarchy) a ten se stal později inspirací pro většinu ostatních protokolů. Optimální počet nadřazených sensorů byl stanoven na 5% všech sensorů v síti. Výběr nadřazeného sensoru se v čase mění. Rozhodování, kterému ze sensorů z oblasti bude tato role přiřazena je podle [3] řízena výběrem náhodného čísla mezi 0 a 1. Sensor se stane nadřazeným pro následující kolo, pokud je vybrané číslo je menší, než následující práh:

$$T(n) = \left\{ \begin{array}{ll} \frac{p}{1 - p \cdot (r \bmod \frac{1}{p})} & , \text{ pro } n \in G, \\ 0 & , \text{ jinak} \end{array} \right\}, \quad (5.1.1)$$

kde p je požadovaná procentuální část nadřazených sensorů (například zmíněných 0.05), r je aktuální kolo a G je množina sensorů, které nebyly nadřazenými v posledních $\frac{1}{p}$ kolech. Vybraný sensor se tedy na jedno kolo stane nadřazeným a shromažďuje data z celé „své“ oblasti. Díky tomuto postupu je zajištěno rovnoměrné energetické zatížení

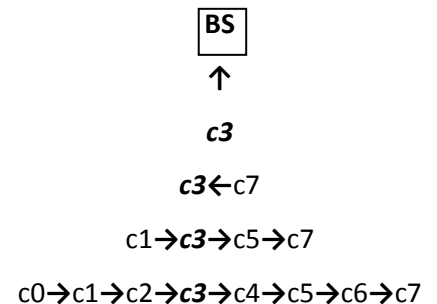
sítě. Navíc senzory vypadávají náhodně, ale celá síť zůstává, ač řídkší, v provozu a tento princip tedy napomáhá výrazně zvýšit životnost celé sítě.

Na druhou stranu tento protokol podporuje pouze jeden přeskok. Data putují od senzoru pouze přímo k nadřazenému a od něho rovnou do základnové stanice. Nelze jej tedy použít pro příliš rozsáhlé sítě. Navíc náhodné přidělování role nadřazenosti vyžaduje další prostředky na jeho řízení a zveřejnění, což snižuje energetickou úsporu.

5.2 PEGASIS

Vylepšením protokolu LEACH byl podle [3] vyvinut **PEGASIS** (**P**ower-**E**fficient **G**Athering in **S**ensor **I**nformation **S**ystems). Ten místo dělení sítě na oblasti vytváří ze senzorů řetěz, kde pouze jeden článek (senzor) vysílá k základnové stanici. V každém ze senzorů dochází k agregaci příchozích dat s vlastními a teprve po té jsou vysílána dalšímu článku řetězu. Jestliže se během průchodu dat řetězem prochází přes hlavní článek, tak ten vyšle pouze zprávu na druhý konec řetězu, ze kterého se začne „znovu“. Ve chvíli, kdy hlavní článek má data od obou sousedů, tak teprve provede jejich agregaci a pak je vysílá do základnové stanice. Tento princip vykazuje zlepšení úspory energie na různě velkých sítích o 100 – 300%, kterého je dosaženo odstraněním režie náhodného přidělování nadřazenosti. Nevýhodou tohoto principu je velmi výrazného zpoždění dat pro vzdálené senzory, a pokud je pouze jeden hlavní článek, stane se kritickým místem, „hrdlem láhve“.

Dalším vývojem došlo k vytvoření **hierarchické** verze protokolu **PEGASIS**, který redukuje zpoždění od vzdálených senzorů. Toho je docíleno souběžným zasláním dat. Aby nedocházelo ke kolizím a signálové interferenci, využívá se dvou postupů a to signálového kódování (např. CDMA), nebo principu, kdy pouze prostorově vzdálené senzory mají svolení vysílat současně. Schéma postupu posílání dat sítě s využitím signálového kódování je vykreslen na Obr. 4. Síť se rozdělí na několik menších řetězů a každému se stanoví jeden hlavní článek, v tomto případě c3. Celý řetěz je nyní na nulté úrovni hierarchie. V této úrovni se všechny články označí pozicí od nuly. Každý sudý článek v této úrovni zašle data následujícímu, který je spojí se svými daty. Každý článek, který data přijal, postupuje v hierarchii do vyšší úrovně. Nyní se tedy v první hierarchické úrovni vyskytují pouze původní liché články řetězu



Obr. 4 – Schéma směřování v hierarchickém PEGASISu

(c1, c3, c5, c7), které se znovu označí od nuly (v obrázku to není naznačeno) a opět všechny sudé zasílají již připravená data dalšímu článku. Opět senzory, které přijímaly data, postupují do vyšší úrovně v hierarchii a přijatá data agregují se svými. V tomto příkladě již zůstaly pouze senzory c3 a c7, a protože c3 byl stanoven jako hlavní, data se posílají opačně. Nakonec c3 opět spojí svá již připravená data s přijatými a zašle je základnové stanici.

Přestože se PEGASIS vyhýbá dělení sítě na oblasti a odpadá řízení určování nadřazeného senzoru, stále potřebuje jistou úroveň řízení a dynamické obměny topologie, a to kvůli rozptylu spotřeby energie.

5.3 TEEN a APTEEN

Dalšími zástupci ze skupiny hierarchických protokolů jsou protokoly **TEEN** (**T**hreshold sensitive **E**nergy **E**fficient sensor **N**etwork) a **APTEEN** (**A**da**P**tive**T**EE**N**). Tyto protokoly jsou po rozmístění řízeny ze základnové stanice, která nejprve rozdělí síť na několik oblastí a stanoví nadřazené prvky. Po tomto rozdělení nadřazené senzory rozešlou všem svým podřazeným sensorům dvě prahové úrovně A a B. První označuje minimální absolutní hodnotu parametru, který sledujeme, a druhá je pro velikost změny tohoto parametru. V případě, že sledovaná veličina nebo parametr okolí přesáhne prahovou hodnotu A, senzor toto oznámí nadřazenému, ale další vysílání se uskuteční až v případě, že dojde ke změně o hodnotu B nebo úroveň klesne pod hodnotu A. Takto je vysílání výrazně omezeno, pokud nás zajímá jen určitý rozsah sledované veličiny, jako například zvýšená teplota okolí před vznikem požáru. Tímto omezeným vysíláním je prakticky stálý dohled nad danou veličinou (víme, v jakém je stavu s tolerancí B), ale nedochází k vysílání dat, čímž se výrazně snižuje spotřeba energie a tím prodlužuje životnost sítě.

Rozdílem mezi TEEN a APTEEN je možnost vysílání požadavku na data, jenž TEEN nepodporuje. Tedy chceme-li například jednou za čas získat pohled na celou síť, nebo požadujeme pravidelné sběry dat, je možné tento jeden požadavek nebo časový rozvrh zaslat do nadřazených sensorů. Ty se pak okamžitě nebo v rozvržených časech postarají o získání dat ze sensorů pomocí zprávy s žádostí. Nevýhodou těchto protokolů je režie a komplexnost budování hierarchie v síti, rozesílání prahových hodnot a u APTEEN protokolu také složitost žádosti o data.

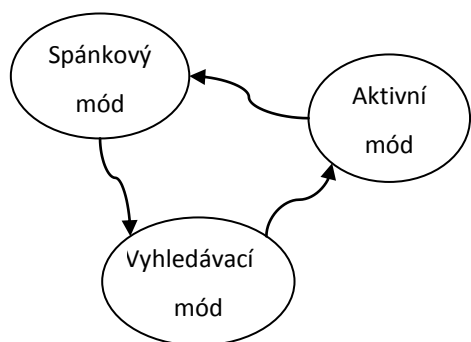
Jako dalšího zástupce je možné uvést GAF, který lze zařadit i do skupiny geografických protokolů.

6 Geografické protokoly

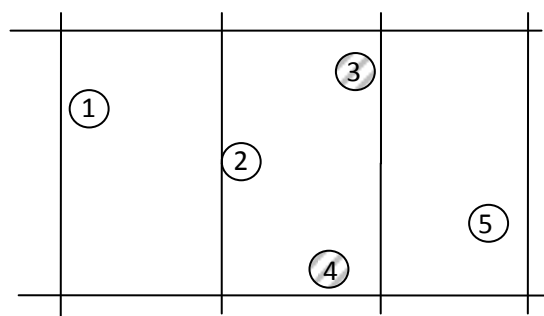
Většina protokolů pro senzorové sítě potřebuje informace o poloze jednotlivých senzorů pro výpočet jejich vzdálenosti a spotřebě energie pro vysílání mezi nimi. Dále lze informace o poloze využít při směřování do konkrétní oblasti zájmu. Například můžeme v celé síti sledovat jeden globální parametr, ale pouze v jeho určité části nás zajímá parametrů více, nebo jiný druh, který nás nezajímá neustále, ale pouze v námi určované okamžiky. Tehdy vysíláme pouze do konkrétní oblasti žádost o data, což mimo jiné šetří energii ve zbytku sítě. Obecně existují protokoly pro Ad-hoc sítě, ale tyto nelze použít v sítích senzorových, vzhledem k jejich energetické spotřebě. Informace o následujících informacích jsou čerpány z [3].

6.1 GAF

GAF (**G**eographic **A**daptive **F**idelity) je založen na myšlence vypínání nepotřebných senzorů. Protokol nejprve na síti vytvoří virtuální mřížku, podle které senzory rozdělí. Jednotlivé senzory identifikují svou pozici například pomocí nízkonapěťového GPS. Body přiřazené do stejné oblasti této virtuální mřížky jsou z hlediska metricky považovány za ekvivalentní, a tedy se některé mohou přepnout do režimu spánku. Ve stavu spánku senzor vypne bezdrátové rozhraní, tedy nepřijímá ani nevysílá a ve stavu aktivním se podílí na směřování paketů sítě.



5 – Schéma změny stavů senzoru v GAF



Obr. 6 – Schéma části sítě protokolu GAF – virtuální mřížka, uprostřed senzory, které se střídají ve stavu spánku a aktivním stavu

Názorným příkladem je Obr. 6, kde senzory 2, 3 a 4 mají spojení na všechny ostatní a je tedy možné aby se dva z nich uspali. Stav spánku, vyhledávací a aktivní stav se mění po předem definovaném čase, závislém na funkci sítě, aby se vyrovnalo využití energie všech senzorů. Na Obr. 5 je uvedeno schéma změny stavů senzoru. Před přechodem z aktivního stavu do spánku se ostatní spící senzory přepnou do vyhledávání, ve kterém zjišťují stav okolních senzorů a jeden z nich se pak přepne do aktivního stavu a tak nahradí stávající sensor, který se uspí.

Jak již bylo zmíněno protokol GAF je řazen i mezi hierarchické protokoly, kde aktivní senzory vystupují jako nadřazené. Nevýhodou tohoto protokolu je fakt, že aktivní senzory neprovádějí agregaci dat.

6.2 GEAR

Dalším zástupcem geografických protokolů je **GEAR** (**G**eographic and **E**nergy-**A**ware **R**outing). Tento protokol využívá informace o stavu energie a zasílání žádostí, stejně jako Directed diffusion, ale s tím rozdílem, že se žádost obsahující i lokalizační data zasílá do konkrétní geografické oblasti. V tomto také získává větší úsporu energie v porovnání s Directed diffusion, když žádostí nezatěžuje kompletně celou síť.

Každý senzor uchovává odhadovanou cenu (váhu) spoje do dané oblasti přes sousední senzory a také učením získává druhou cenu spoje. Odhadovaná cena se sestává ze zbytkové energie senzoru a vzdálenosti do cílového prostoru. Naučená cena se získává používáním daných spojů, reálných spojení, které obsahují mezery. Mezera vzniká, jestliže senzor nemá žádný v okolí bližší senzor pro cílovou oblast než je on sám. V případě, že zde nejsou mezery, naučená váha spoje je shodná s odhadovanou váhou.

Protokol GEAR má dvě fáze.

1. Přeposílání paketů do dané oblasti:

Po přijetí paketu senzor nejprve zjistí, zda v jeho okolí existuje alespoň jeden senzor, blíže k dané oblasti než je on sám (pokud neexistuje, vzniká mezera). Poté je vybrán nejbližší senzor směrem k destinaci jako další skok. Pokud je zde mezera, jeden z okolních senzorů je vybrán pro přeposlání paketu na základě naučení se nové váhy spoje. Tato nová naučená cena spoje je pak aktualizována ve směrovací tabulce senzoru.

2. Přeposílání paketu uvnitř cílového prostoru:

Jestliže paket dosáhl cílové oblasti, jsou dvě možnosti jak jej uvnitř rozšířit. Buď pomocí rekurzivního geografického přeposílání nebo omezeného zaplavování. V sítích s nízkou hustotou senzorů je vhodnější omezené zaplavování. V hustě osazených sítích je rekurzivní geografické přeposílání méně náročné na spotřebu energie. Pro tento způsob rozesílání pak následuje rozdělení oblasti na 4 podoblasti, do kterých se pošle kopie přijatého paketu. Takto se postupuje tak dlouho, dokud v takto vytvořené podoblasti nezůstane pouze jediný senzor.

GEAR podle [3] v porovnání s podobným protokolem bez užití stavů energie dosahuje mnohem lepších výsledků jak v oblasti úspory energie, tak při doručování paketů.

Dalšími zástupci geografických protokolů jsou MECN a SMECN a SPEED.

7 Směrování s metrikou

Jak již bylo dříve uvedeno, v sensorových sítích existuje vždy několik cest mezi dvěma body. Chceme-li zachovat energetickou obezřetnost, je vhodné vybírat vždy tu cestu, která z dlouhodobého hlediska spotřebovává nejméně energie. Proto je důležité každé cestě přiřadit vhodnou metriku. Za nejčastěji používanou metriku můžeme považovat chybovost spoje a vzdálenost bodů. Vzdálenost ovlivňuje vysílací výkon a chybovost počet nutných opakování vysílání paketu, kvůli jeho ztrátě při přenosu. Pokud budeme uvažovat zidealizovanou síť bez chyb přenosu a se stejně vzdálenými senzory, jedinou použitelnou metrikou zůstane „hop-count“, tedy počet skoků (směřujících senzorů) mezi dvěma body sítě.

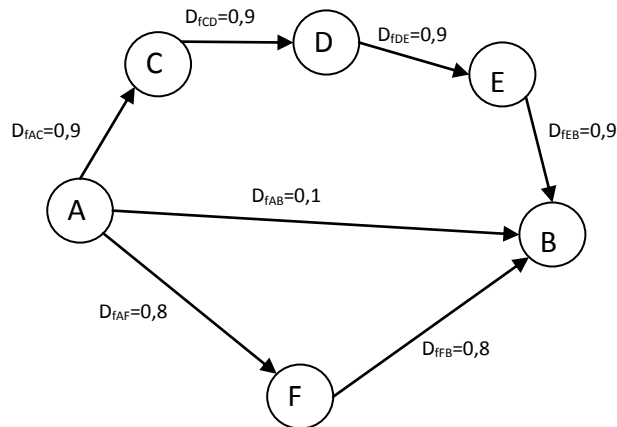
7.1 ETX metrika

V reálných sítích jsou spoje náchylné k chybám vlivem například okolního rušení nebo překážek v cestě mezi senzory. V tomto případě použití pouze principu nejkratší cesty nevede k nejlepším výsledkům. Proto byla představena metoda výpočtu metriky pro robustní síť, která minimalizuje očekávaný počet opakovaně vysílaných paketů na dané cestě. Nezávisle na metodě ETX byla představena téměř identická metoda zvaná „Minimum transmissions metric“.

Podle [7] metoda ETX předpokládá využití potvrzujících zpráv ACK (ACKnowledgement) po každém přijatém paketu. Označíme-li pravděpodobnost doručení paketu směrem dopředu k druhému senzoru d_f a pravděpodobnost doručení zprávy ACK směrem opačným d_r , předpokládaný počet vysílání jednoho paketu bude

$$EXT = \frac{1}{d_f \cdot d_r}. \quad (7.1.1)$$

Důležité je, že tuto metriku je možné začlenit do kteréhokoliv protokolu a tak více omezit spotřebu energie.



Obr. 7 – Schéma části sítě s jejím ohodnocením

Na Obr. 7 je naznačena část sítě včetně označení metrik. Přímá cesta mezi body A a B vyžaduje průměrně 10 opakování vysílání paketu. Cesta přes senzory C, D a E jich vyžaduje 1,11 pro každou cestu, celkem tedy 4,44 opakování. Poslední cesta přes sensor F obdobným způsobem přináší 2,5 opakování. Tento případ také demonstruje, že nejlepší cesta nemusí být vždy ta s mnoha spolehlivými skoky, ale ani přímá cesta, s nižší kvalitou spoje. Ta pravá cesta leží mezi těmito dvěma extrémy.

Tento způsob určení cesty přináší nejen úsporu energie, ale také pomocí měření chybovosti spoje pro určení metriky mapuje asymetričnost sítě.

7.2 MORMER

Metrika EXT je vhodná pro sítě bez pohyblivých objektů nebo senzorů. V případě pohybu totiž dochází k rapidním změnám v chybovosti jednotlivých cest, a tedy energetická úspora klesá. Pro tyto sítě E. Khandani a kolektiv v [6] odvodili metody s metrikou pro kolísavou kvalitu linky. Detailně modelovali bezdrátový kanál s vícecestným útlumem signálu a s kolísáním v čase podle Rayleighových statistik. Přístupují ke spolehlivosti linky jako k pravděpodobnosti výpadku. Definiuje se zde výpočet okamžité kapacity kanálu jako

$$C = \log \left(1 + \frac{|f|^2}{d^\eta} \cdot \text{SNR} \right), \quad (7.2.1)$$

kde d je vzdálenost dvou daných senzorů, η je útlum cesty, SNR je normalizovaný odstup signál – šum bez úniku a f stav úniku na kanálu.

Pak pravděpodobnost výpadku je definovaná jako pokles kapacity kanálu pod míru vysílání R

$$P_{\text{OUT}} = 1 - \exp\left(\frac{-d^n}{\mu \text{SNR}^*}\right), \quad (7.2.2)$$

kde

$$\text{SNR}^* = \frac{\text{SNR}}{2^R - 1} \quad (7.2.3)$$

je normalizovaný odstup signál-šum a

$$\mu = E[|f|^2] \quad (7.2.4)$$

je průměrný Rayleighův únik.

Na základě těchto formulací autoři vyvodili, že nejspolehlivější cesta mezi dvěma body sítě je taková, která minimalizuje metriku dané cesty podle

$$\sum_i d_i^n \quad (7.2.5)$$

kde d_i je vzdálenost i -tého skoku v cestě, za předpokladu spojů mezi senzory bez výpadků a se shodnými SNR. Tato metrika (d^n pro každý spoj vzdálenosti d) je označována jako Minimum Outage Route (MOR).

Také pro případ kontroly energie autoři vyvodili obdobně jako pro obecnou metriku, že nejspolehlivější spoj mezi dvěma body v síti je ten, který dosahuje minimální metriky dané

$$\sum_i \sqrt{d_i^n}, \quad (7.2.6)$$

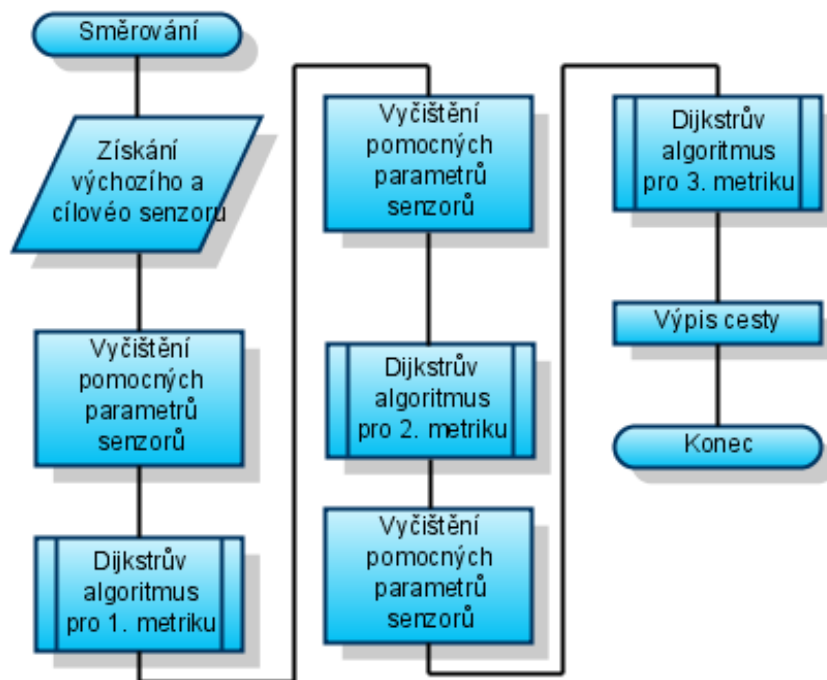
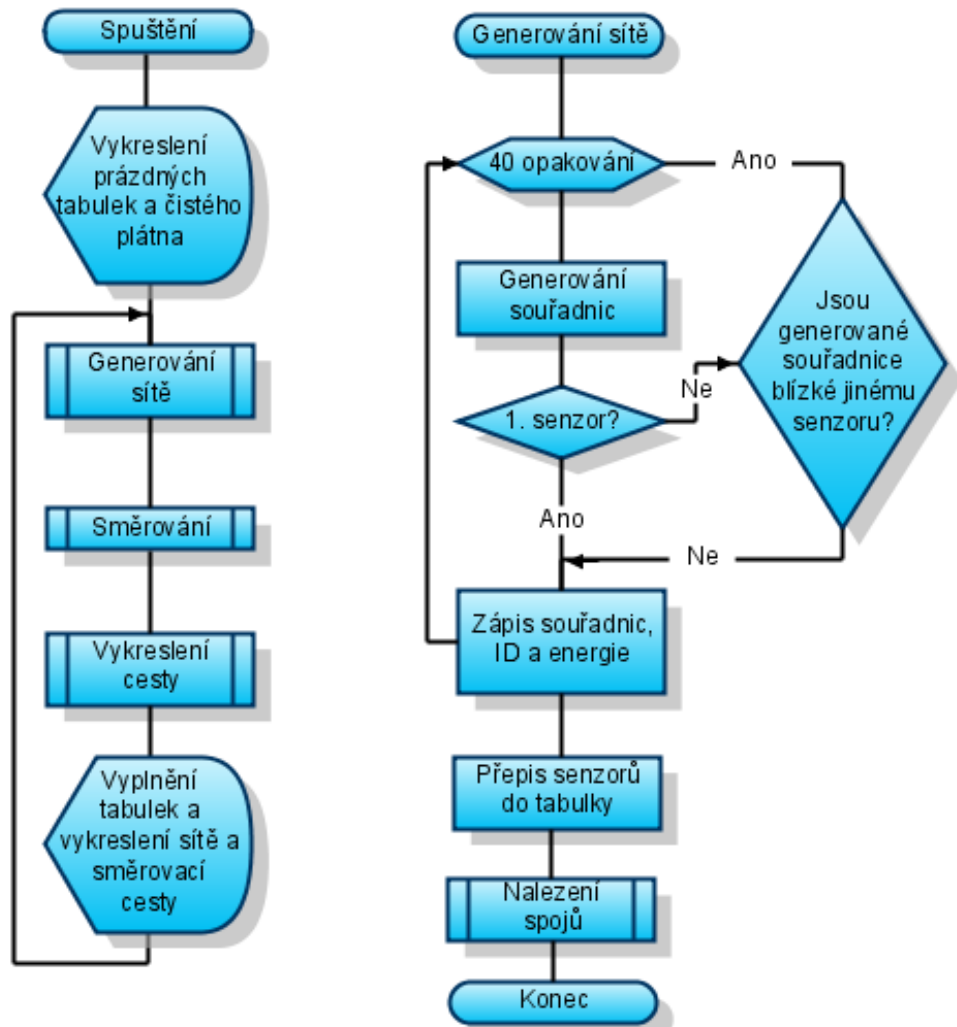
kde $\sqrt{d_i^n}$ je metrika pro každý skok mezi dvěma senzory na cestě, označovaný Minimum Energy Route (MER). Důležité v tomto bodě je, že minimalizovaná energie je energie vysílání závislá na vzdálenosti, nikoliv energie pro příjem nebo ostatní na vzdálenosti nezávislé operace.

Hlavním rozdílem mezi MOR/MER a ETX metrikou je, že první zmíněná neshromažďuje informace o kvalitě jednotlivých cest, které se mohou výrazně měnit. Na druhou stranu ETX pracuje s potvrzováním zpráv.

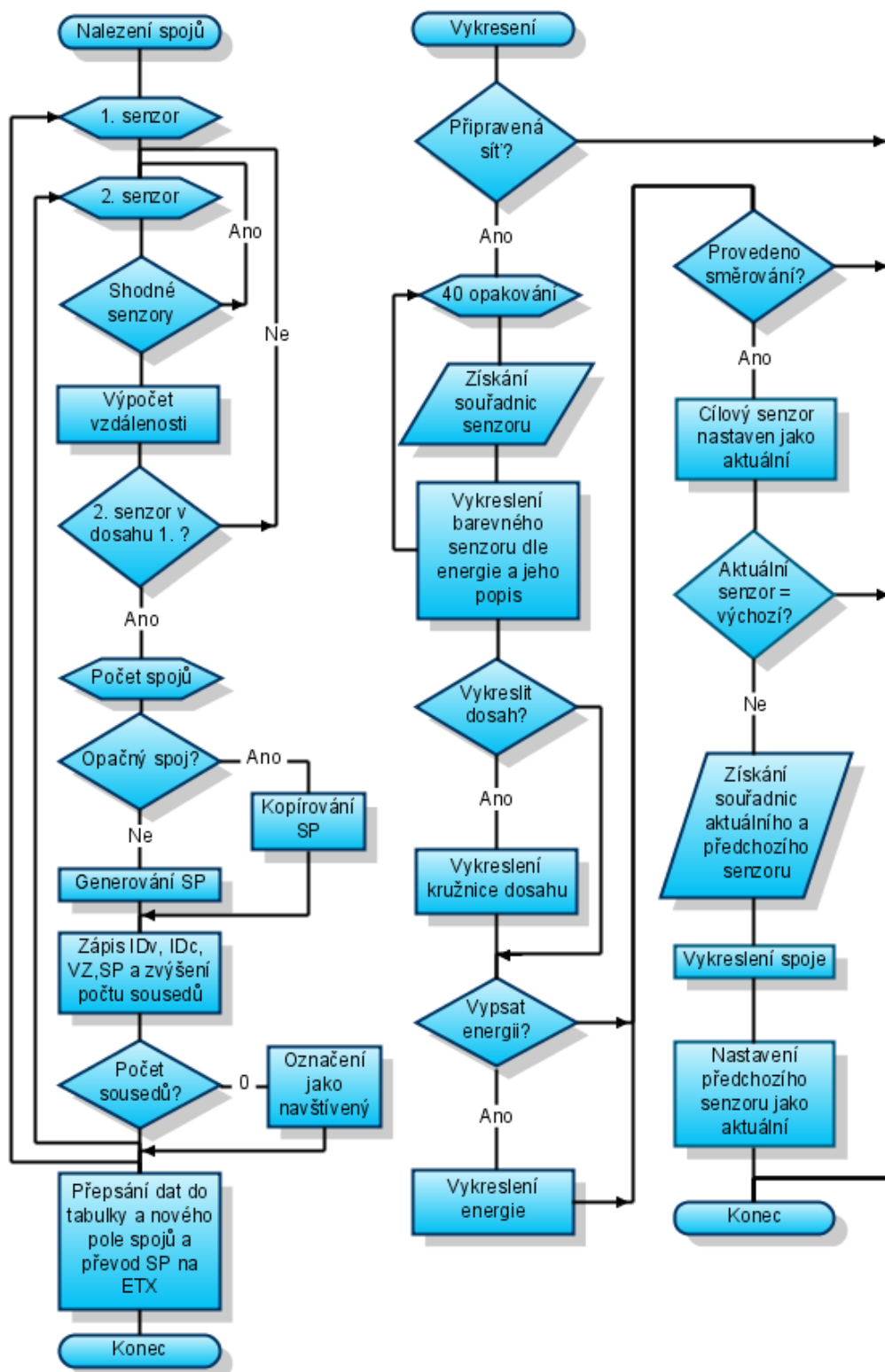
8 Srovnání metrik směrovacích protokolů v navržené aplikaci

Součástí této práce je také aplikace, která má za úkol znázornit vliv různých metrik na výběr cesty v síti mezi dvěma zvolenými senzory.

Aplikace byla vyvíjena v programovacím jazyku Java, který jsem zvolil kvůli jeho objektové orientaci, velmi kvalitní a rozsáhlé nápovědě a pomocným tutoriálům a v neposlední řadě kvůli široké základně uživatelů komunikujících a řešících konkrétní situace na fórech. Vývojové prostředí bylo použito NetBeans ve verzi 6.1 (dostupné z [8]), bez nutnosti použití speciálních knihoven. Pro grafiku by bylo možné použít rozsáhlejší knihovnu pro 3D grafiku (i pro 2D), ale její použití by bylo zbytečně složité a základní vybavení bylo dostačující. Aplikace je navržena tak, aby po spuštění znázornila čistý prostor pro síť a prázdné tabulky. Teprve po stisku tlačítka náhodně generuje rozložení sítě o 40 senzorech, včetně jejich vlastností. Po rozmístění proběhne analýza sítě z pohledu spojů mezi senzory. Každý senzor má spoje pouze k sousedním senzorům v blízkém okolí a každý spoj je definován několika vlastnostmi. Některé z vlastností jak spojů, tak i senzorů jsou pak vypsány do dvou přehledných tabulek. Nad sítí dále třikrát proběhne algoritmus pro určení nejlepší cesty z výchozího senzoru k cílovému podle předepsané metriky. Na závěr jsou vykresleny všechny tři cesty současně, pro každou cestu je vždy použita jiná barva pro větší přehlednost při jejich vyhodnocení. Vývojové diagramy celé aplikace jsou znázorněny na Obr. 8 a Obr. 9.

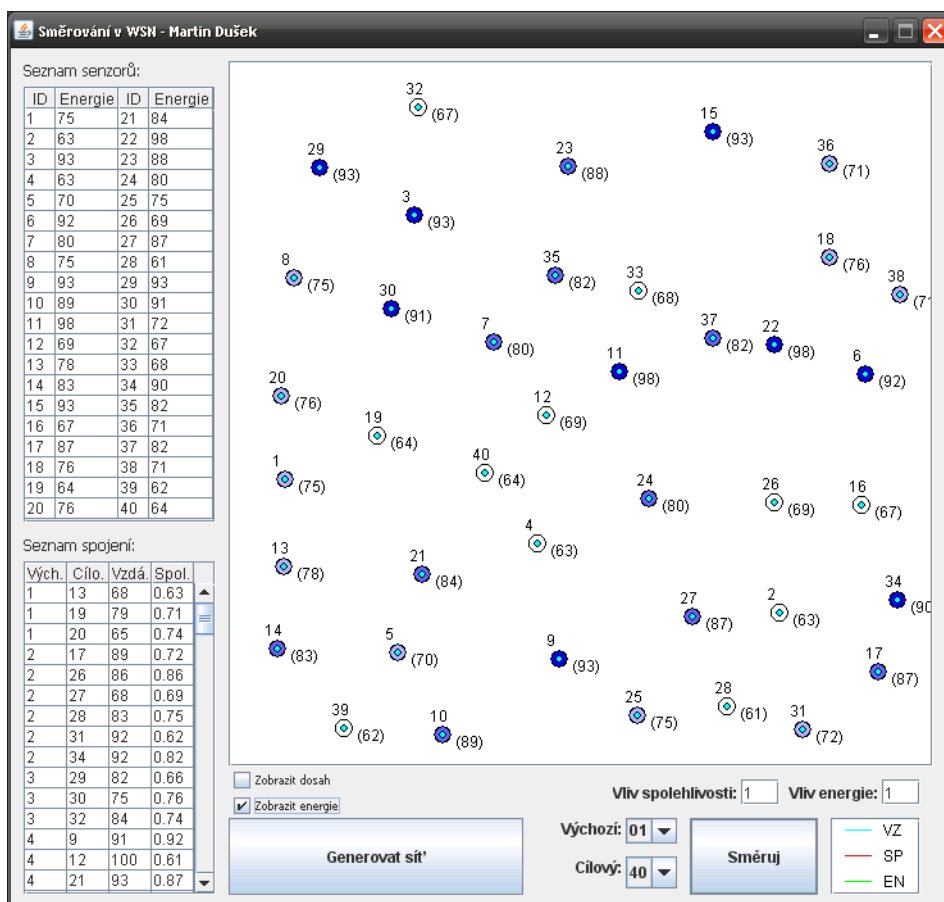


Obr. 8 – Vývojový diagram navrhované aplikace – část 1.



Obr. 9 – Vývojový diagram navrhované aplikace – část 2.

Základní vzhled po vygenerování běžné sítě bez typických případů je uveden na Obr. 10.



Obr. 10 – Základní vzhled aplikace s vygenerovanou sítí bez typických situací

Tabulka „Seznam senzorů“ obsahuje výpis senzorů a hodnotu jejich zbývající energie. Ta je generována náhodně v rozmezí 60-90 %. V druhé tabulce „Seznam spojení“ jsou pak uvedeny všechny existující spoje mezi senzory. Zleva je v tabulce vypsáno ID výchozího a cílového senzoru, jejich vzdálenost v metrech a pravděpodobnost doručení vyslaného paketu spojením, zmíněná v části práce zabývající se ETX metrikou.

Plátno, zabírající největší část aplikace, znázorňuje jednotlivé, barevně odlišené senzory a jejich popis. Barevné rozlišení spodního terčiku senzoru určuje úroveň hladiny zbývající energie (od sytě modré označující 90-99 %, až po bílou označující méně než 70 % energie). Číslo nad senzorem nese jeho označení (ID) a číslo v závorkách udává přesnou hodnotu energie a je možné ji skrýt. Pod zobrazenou sítí jsou ovládací prvky pro generování nové sítě, zobrazení pomocných údajů (dosah a energie), výběr senzorů pro směrování, tlačítko pro provedení směrování a také dvě pole, pro určení míry vlivu jednotlivých faktorů při směrování podle jedné z metrik. V pravém dolním rohu je legenda pro případnou vykreslenou cestu – tyrkysová barva

s popisem VZ označuje cestu s metrikou vzdálenosti, červená s SP je pro metriku ETX a zelená s EN pro společnou metriku zbytkové energie senzoru a ETX.

8.1 Generování sítě

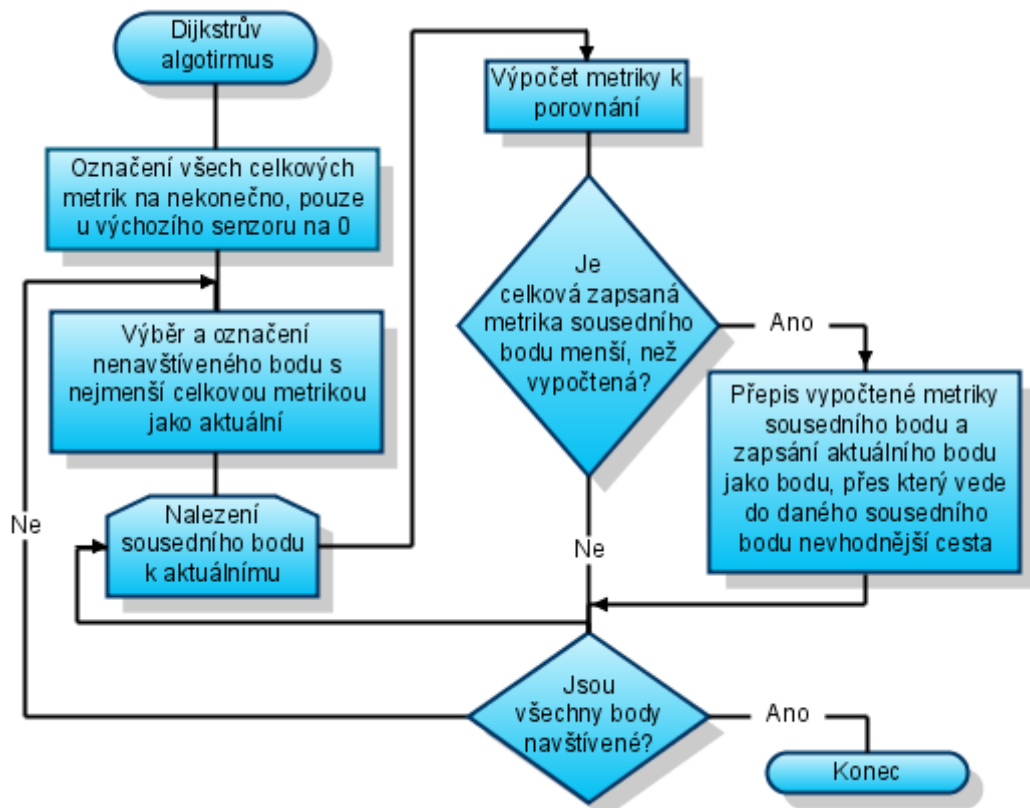
Obecně je rozmístění senzorů generováno náhodně ovšem za současného dodržení několika pravidel. Kvůli rovnoměrnosti sítě je nastavena podmínka, aby senzory nebyly příliš blízko u sebe, kvůli správnému vykreslení pak je nastaven okraj, aby se senzor nedostal ani svým popisem mimo pole. Samotný senzor má několik, již zmíněných vlastností. Kromě svého identifikačního čísla ID a úrovně energie si také uchovává své souřadnice v síti, počet sousedů (tedy senzorů v dosahu vysílače) a pak vždy dvojici atributů pro každý z algoritmů a to průběžnou celkovou hodnotu metriky od výchozího senzoru a předchozí senzor v cestě k cílovému. Při analýze sítě a vyhledávání spojů se kontroluje každý senzor s každým, a pokud je jejich vzdálenost kratší, než jejich dosah, jsou zapsány do tabulky spolu se zmíněnou vzdáleností. Navíc je každému spoji přiřazena spolehlivost, která se skládá z části z jejich upravené vzdálenosti a zbytek tvoří náhodné číslo, které reprezentuje vliv prostředí na daný spoj (rušení okolních senzorů, překážky apod.). Tato spolehlivost je vypsána v tabulce jako pravděpodobnost doručení, v databázi je již přepočítána na ETX, aby později uvnitř algoritmu nečinila kód nepřehledným.

8.2 Směrování

Pro směrování byl použit jednoduchý Dijkstrův algoritmus, který je zaměřen na hledání nejkratší cesty v grafu. Jednotlivé metriky byly pak upraveny, aby bylo možné na ně tento postup použít. Dijkstrův algoritmus prozkoumá celou síť, čímž dochází k delším výpočtům, než kdyby zpracovával pouze relevantní část sítě. Vývojový diagram Dijkstrova algoritmu je uveden na Obr. 11.

Nejprve je výchozí senzor označen jako *aktuální*. Do jeho celkové metriky je zapsána nula a ostatním senzorům maximální hodnota. Poté se pro daný *aktuální* senzor prohledají všechny ostatní, se kterými má spojení a porovnává se vypočtená a zapsaná metrika. Výpočet metriky spočívá v součtu zapsané metriky *aktuálního* senzoru a metriky mezi právě zkoumanými senzory. Pokud je vypočtená metrika menší, je zapsána se k senzoru a zároveň je *aktuální* zapsán jako *předchozí* – ten, přes který vede do zkoumaného senzoru nejlepší cesta z pohledu dané metriky. Po prohledání všech sousedních senzorů je *aktuální* označen jako navštívený a již nikdy nebude porovnáván. Ze všech již hodnocených senzorů je následně jako *aktuální* vybrán ten, který má

nejnižší celkovou metriku a zároveň nemá příznak, že již byl navštíven. Zde končí smyčka, která se opakuje do té doby, než jsou všechny senzory označeny jako navštívené. Po proběhnutí algoritmu se nejlepší cesta vypisuje a vykresluje opačným směrem, tedy od cílového senzoru přes zmíněný předchozí senzor až k výchozímu.



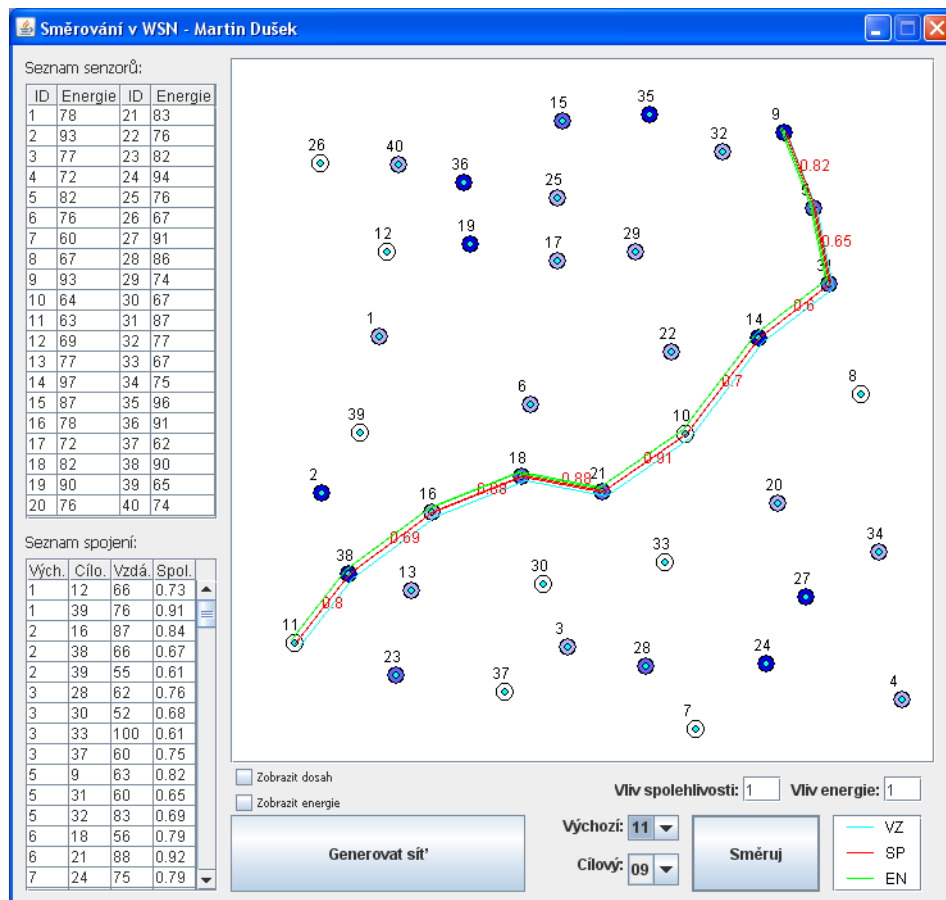
Obr. 11 – Vývojový diagram Dijkstrova algoritmu

Pro vzdálenost jako metriku není potřeba nic upravovat, stačí zaznamenané vzdálenosti použít přímo do algoritmu. Spolehlivost je díky výše zmíněnému přepočítání na ETX také možno použít bez dalších úprav. Jediné úpravy tak zůstávají u poslední, kombinované metriky. Jak již bylo řečeno, je složena z ETX a ze zbytkové energie senzoru. Energii oproti ETX je nutno upravit, protože zde platí, čím větší energie senzoru, tím výhodnější je jeho použití. U vzdálenosti a ETX je tomu naopak – čím nižší vzdálenost nebo ETX, tím výhodnější použití. Pro úpravu je tedy použita převrácená hodnota energie, a protože ETX vychází v řádech jednotek, je nutné pro srovnání úrovně vlivu energie a ETX použít vynásobení 100. Navíc je uživateli umožněna změna vlivu ETX nebo energie a to pomocí koeficientů z intervalu $\langle 0;1 \rangle$, zadávaných do označených polí. Těmito koeficienty je pak příslušná část metriky násobena:

$$ENSP = k_1 \cdot SP + k_2 \cdot \frac{1}{EN} \cdot 100, \quad (8.2.1)$$

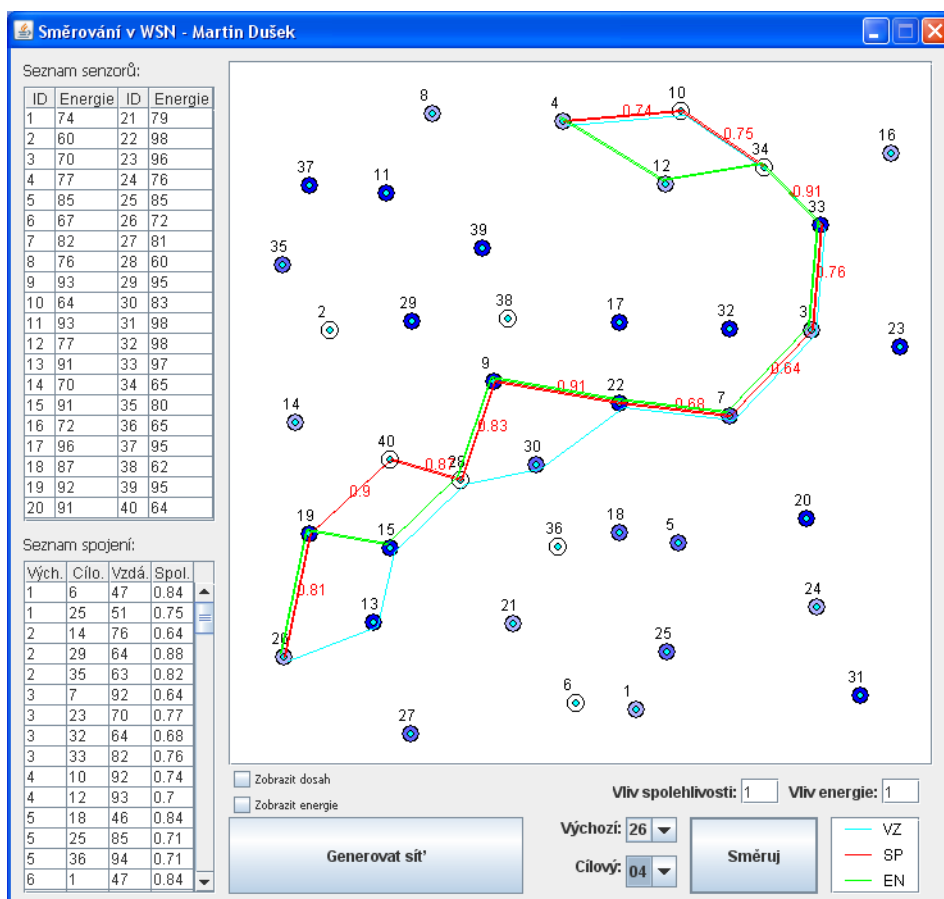
kde $ENSP$ je kombinovaná metrika, k_1 je koeficient vlivu spolehlivosti SP a k_2 je koeficient vlivu energie EN .

Další situace, které mohou nastat, jsou popsány na následujících obrázcích.



Obr. 12 – Směrování shodnou cestou

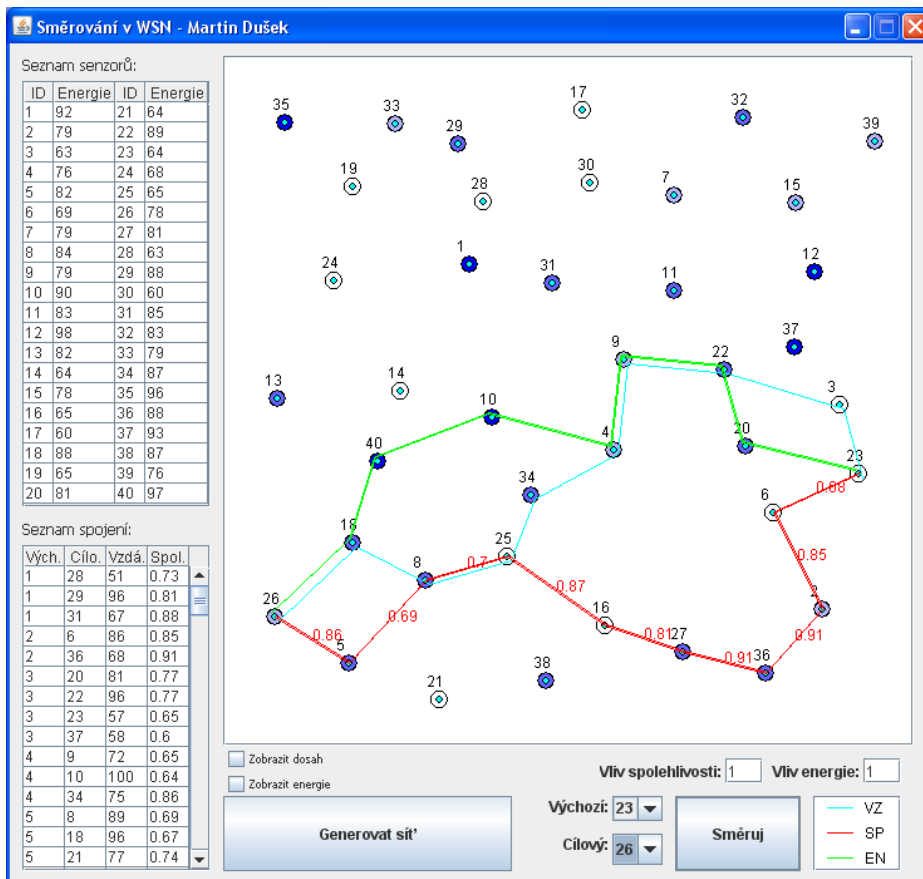
Na Obr. 12 je znázorněn nejběžnější výsledek směrování, kdy všechny tři cesty vedou shodnou trasou. Vzhledem k tomu, že spolehlivost je částečně závislá na vzdálenosti, je tento výsledek očekávatelný. Obdobně to je i s částečnou závislostí kombinované metriky, jejíž součástí je právě i spolehlivost. Barevné rozlišení je popsáno v legendě a červená čísla vyjadřují hodnoty pravděpodobností doručení paketů příslušným spojem.



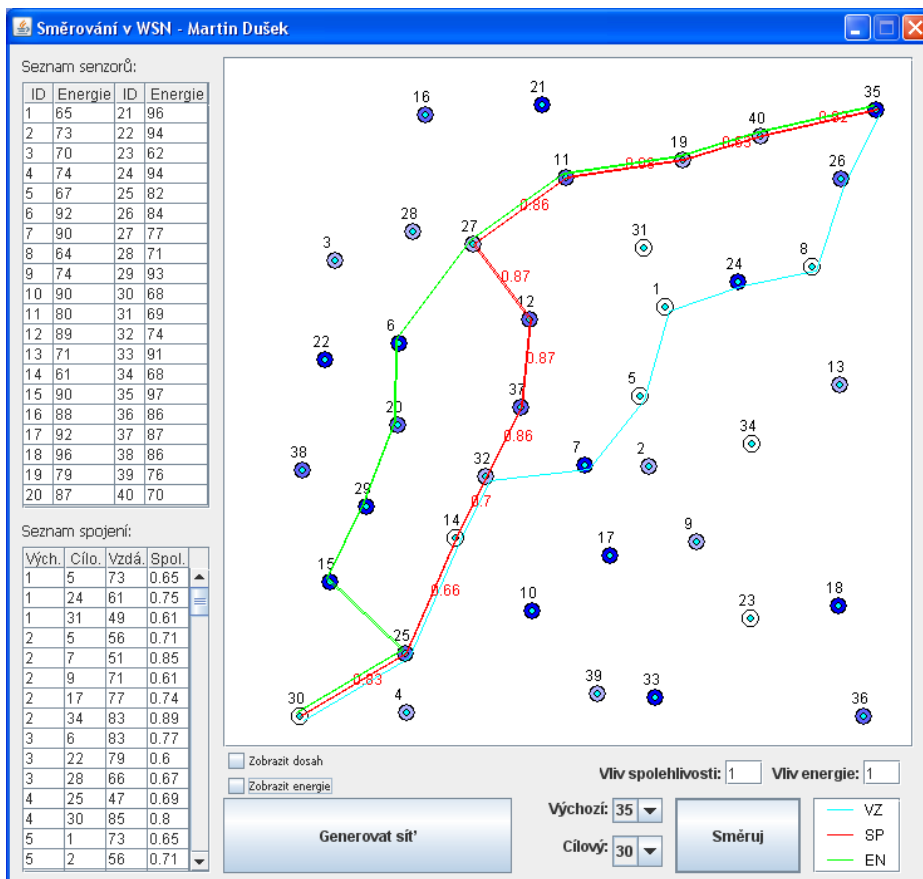
Obr. 13 – Směrování rozdílnou cestou – lokální diference

V situaci na Obr. 13 již dochází k drobným odlišnostem v cestách podle jednotlivých kvalit spojů. Vzdálenostní metriku je možné vysledovat pouhým pohledem, spolehlivost je možné ověřit nalezením hodnot ve spodní tabulce a porovnáním součtů hodnot ETX. Kombinovaná metrika je vysledovatelná podle barevně odlišených terčíků. Například u rozdělení hned za výchozím senzorem v levé dolní části sítě, kde senzory 19 a 13 mají shodnou úroveň energie, má vliv i spolehlivost, která je upřednostněna červenou cestou. Naopak u následujících senzorů 15 a 40 je jasně viditelný vliv výrazně rozdílné hladiny energie, kdy spolehlivost nemá vliv tak veliký.

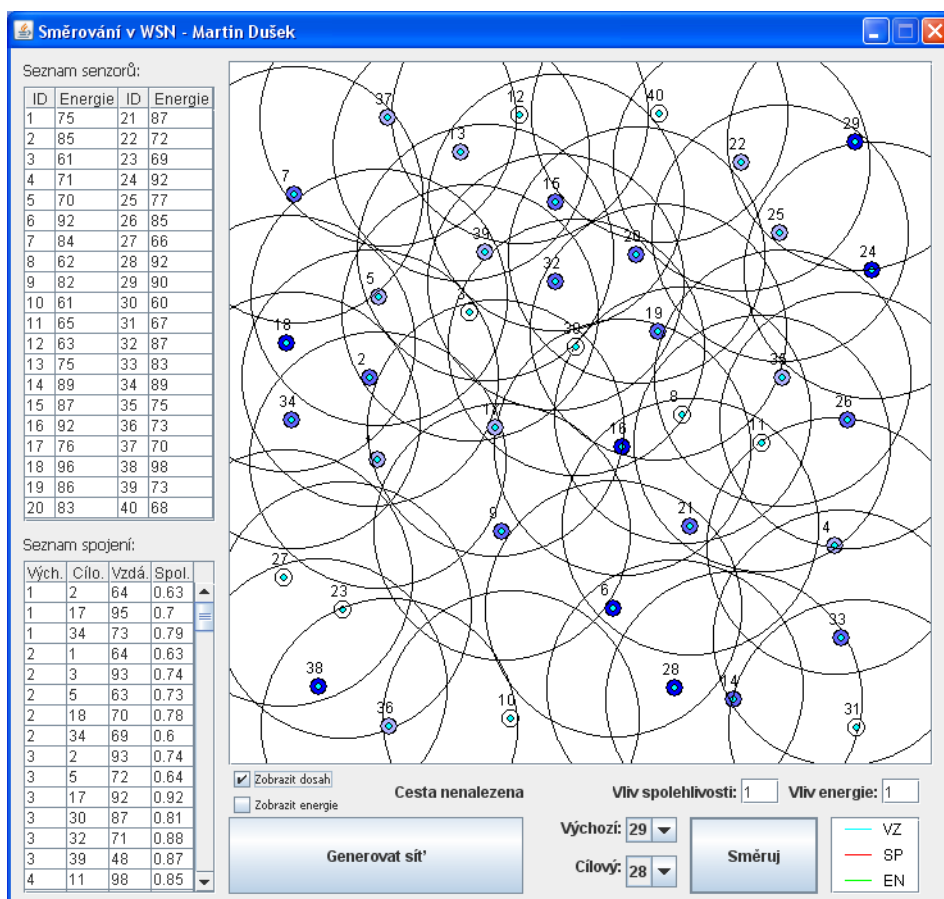
Obr. 14 ukazuje situaci, kdy se všechny tři cesty významně liší. Zde je velmi důležitý fakt, že ze senzorů 20 a 6 nevedou souběžné cesty, ale vzniká zde prostor, bez možnosti směrování. Cesty se rozdělí na základě parametrů pouhých třech spojů z výchozího senzoru. Rozdíl mezi pouze dvěma cestami tedy může být jen minimální. Na rozdíl od Obr. 15, kde jsou cesty rozděleny průběžně podle svých parametrů a je zde mnoho možností křížení a nuancí, jako tomu je na Obr. 13.



Obr. 14 – Směrování rozdílou cestou – samostatné cesty



Obr. 15 – Směrování rozdílou cestou – delší samostatné cesty



Obr. 16 – Osamocené senzory

Na závěr je na Obr. 16 znázorněna situace, ke které dochází díky dostatečně velké ploše pro rozptřeni senzorů a malé minimální vzdálenosti. Z praxe tato situace představuje oddělení senzoru, například když jej odnese zvíře, při rozptřirání po oblasti díky nerovnosti terénu se „odkutálí“ stranou nebo když některým senzorům dojde energie a takto „odříznu“ část síť. Obr. 16 pomocí kružnic zobrazí dosah každého senzoru – díky tomu se však síť stává nepřehlednou, a proto je tato funkce ve výchozím stavu vypnuta. Dosah je pouze teoretický a odvozený od výkonu vysílací části senzoru. Senzor je v dosahu, pouze pokud je jeho střední část (tyrkysový bod) uvnitř zmíněné kružnice. Lze tedy vypořozovat dvě extrémní místa, odříznutá od zbytku síť a to v levém dolním a pravém horním rohu (senzory 27, 23, 38, 36, 10 a 24, 25, 22, 40, 29). Uvnitř těchto tří separátních skupin je stále možné směřovat, ale mezi nimi to možné není. Jak je také znázorněno, při pokusu o směřování mezi vzájemně nedostupnými body je algoritmus přerušen a pod síť je vypsána zpráva, že cesta nebyla nalezena.

9 Závěr

V této bakalářské práci byla rozebrána problematika sensorových sítí, obecný pohled na ně a jejich srovnání s ostatními sítěmi. Hluběji byly prozkoumány metody směrování a rozděleny do několika skupin. V každé skupině pak vybrány důležité protokoly a bylo popsáno jejich chování a principy, na kterých jsou založeny. Z uvedených informací je zřejmé, že každá aplikace, která má být použita pro bezdrátové sensorové sítě, musí mít předem definované vlastnosti a požadavky a podle toho je nutné protokol vybrat. Některé aplikace však mají složitější nároky na směrování, zejména vyžadují kombinace několika zde představených principů. Pro tyto aplikace je pak nutné použít jiné protokoly, případně navrhnout vlastní, postavený na míru dané aplikaci.

V případě metriky v sensorových sítích jsou zde nepřehledné možnosti využití vzhledem k možnosti snadné implementace do téměř libovolného protokolu. Dva zde uvedené způsoby pokrývají pouze základní možnosti.

Vytvořená aplikace, pomocí programovacího jazyku Java, simuluje bezdrátovou sensorovou síť a směrování podle jednotlivých druhů metriky. Jako použité typy metriky byly vybrány: vzdálenost, spolehlivost spoje a kombinovaná metrika, složená ze zmíněné spolehlivosti a zbývající energie sensorů. Pro samotné směrování byl vybrán Dijkstrův algoritmus, který se bohužel ukázal jako nepříliš vhodný pro kombinovanou metriku, u které vyvstal problém s jejím přizpůsobením algoritmu a možnosti ovlivnění působení jejích částí byly značně variabilní a hůře kontrolovatelné. Na druhou stranu je tento algoritmus velmi jednoduchý na aplikaci a i přes zmíněné problémy je dostatečně názorný při vyhodnocování cest z pohledu různých vah spojů. Na navržené aplikaci lze snadno ukázat nevhodnost samostatného použití jednotlivých typů metriky bez ohledu na energii senzoru. Právě kombinovaná metrika ukazuje, jak lze ve většině případů jednoduše nalézt alternativní cesty vhodné pro úsporu energie jak z pohledu kvalitnějších, kratších cest, tak i z pohledu využití sensorů s větší zbytkovou kapacitou energie. Vždy se ale jedná o kompromisní řešení. Takovéto směrování zabraňuje nerovnoměrnému vytížení sítě, odpojení části sítě kvůli vyčerpaným sensorům a naopak pomáhá zvyšovat životnost celé sítě.

Seznam použité literatury

- [1]KARAKI, Jamal N.; KAMAL, Ahmed E. *Routing Techniques in Wireless Sensor Networks: A Survey*. [200?]. 37 s. Dostupný z WWW: <http://www.ece.iastate.edu/~kamal/Docs/kk04.pdf>.
- [2]LEDVINA, Jiří. *Úvod do počítačových sítí: Protokoly směrování* [online]. [2006] [cit. 2008-12-10]. Dostupný z WWW www.kiv.zcu.cz/~ledvina/Prednasky-UPS-2006/09-ups-2006-smerovani.ppt
- [3]KEMAL, Akkaya; YOUNIS, Mohamed. *A survey on routing protocols for wireless sensor networks*. 2003. 25 s. Dostupný z WWW: http://www.adms.ethz.ch/teaching/lectures/ss2007/hotdms/papers/routing_survey.pdf
- [4]HEINZELMAN, W.; KULIK, J.; BALAKRISHNAN, H. *Adaptive protocols for information dissemination in wireless sensor networks: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*. 1999. 20 s.
- [5]INTANAGONWIWAT, C.; GOVINDAN, R.; ESTRIN, D. *Directed diffusion: a scalable and robust communication paradigm for sensor networks: Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '00)*. 2000. 20 s.
- [6]KRISHNAMACHARI, Bhaskar. *Networking Wireless Sensors*. New York: Cambridge University Press, 2005. 202 s. ISBN 978-0-521-83847-4.
- [7]KHANDANI, E.; et al. *Reliability and route diversity in wireless networks: MIT LIDS Technical report Number 2634*. 2004. 50 s.
- [8]Oficiální stránky vývojového prostředí NetBeans [online]. 2009 [cit. 2009-05-25]. Dostupný z WWW: <http://www.netbeans.org/>

Seznam zkratek

ACK	ACKnowledgment	Potvrzení
ACQUIRE	ACTive QUery forwarding In sensoR nEtworks	
APTEEN	AdaPtive Threshold sensitive Energy Efficient sensor Network	
ARQ	Automatic Repeat reQuest	
BGP	Boarder Gateway Protocol	
BS	Base Station	Základnová stanice
CADR	Constrained anisotropic diffusion routing	
CDMA	Code Division Multiple Access	
CSMA	Carrier Sense Multiple Access	
GAF	Geographic Adaptive Fidelity	
GBR	Gradient-Based Routing	
GEAR	Geographic and Energy-Aware Routing	
GPS	Global Position System	Globální polohový systém
LEACH	Low-Energy Adaptive Clustering Hierarchy	
MECN	Minimum Energy Communication Network	
MER	Minimum Energy Route	
MOR	Minimum Outage route	
OSPF	Open Shortest Path First	
PEGASIS	Power-Efficient GATHERing in Sensor Information Systems	
RIP	Routing Information Protocol	
SMECN	Small Minimum energy communication network	
SPIN	Sensor protocols for information via negotiation	
TDMA	Time Division Multiple Access	
TEEN	Threshold sensitive Energy Efficient sensor Network	
WSN	Wireless Sensor Network	

Médium

- Smerovani_WSN – adresář, obsahující ukázkovou aplikaci
 - Lib – adresář se souborem AbsoluteLayout.jar, který obsahuje všechny nutné prostředky pro spuštění aplikace
 - SmerovaniWSN.jar – samotná aplikace – je nutné ji spouštět v Java prostředí a z tohoto místa, kvůli zmíněným prostředkům
- Dusek_Martin_BP.pdf – elektronická verze této bakalářské práce
- jre-6u13-windows-i586-p-s.exe – instalační soubor Java prostředí pro Windows XP/Vista, nutného pro spuštění aplikace