VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky

a komunikačních technologií

DIZERTAČNÍ PRÁCE

Brno, 2017 Ing. Bohumil Novotný

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

MULTIPLATFORMNÍ KOMUNIKACE V PŘÍSTUPOVÝCH SÍTÍCH

MULTIPLATFORM COMMUNICATION IN ACCESS NETWORKS

DIZERTAČNÍ PRÁCE
DOCTORAL THESIS

AUTOR PRÁCE — Ing. Bohumil Novotný
AUTHOR

ŠKOLITEL — doc. Ing. Vladislav Škorpil, CSc.
SUPERVISOR

BRNO 2017

ABSTRAKT

Dizertační práce se zabývá výzkumem zaměřeným na detekce poruchy v bezdrátové přístupové síti pomocí distribuovaných stochastických algoritmů. Byla navržena a simulována nová metoda detekce poruchy na základě algoritmu push-sum. V rámci plnění cílů práce byla komparována statistická kredibilita reprezentanta průměrné rychlosti konvergence protokolu push-sum a vliv ztráty zprávy během výpočtu na robustnost systému uvedený protokol využívající. Na základě získaných poznatků byla prokázána schopnost navržené metody matematicky odvodit odchylky od reálného průměru hodnot v zadané topologii, a tím byla prokázána či vyvrácena existence abnormality v síti.

KLÍČOVÁ SLOVA

Distribuovaný stochastický algoritmus, push-sum protokol, senzorová síť, interference, detekce poruchy, statistická kredibilita.

ABSTRACT

Doctoral thesis deals with failure detection methods in wireless access network using distributed stochastic algorithms. A new method of detecting a fault based on the push-sum algorithm has been designed and simulated. Within the scope of the work objectives, the statistical credibility of the average push-sum protocol convergence rate representative and the effect of message loss during the calculation on the robustness of the system using this protocol were compared. Based on the acquired knowledge, the ability of the protocol to mathematically derive deviations from the real average of the values in the specified topology was demonstrated and thereby the existence of an abnormality in the network has been proved or refuted.

KEYWORDS

Distributed stochastic algorithm, push-sum protocol, sensor network, interference, failure detection, statistical credibility.

NOVOTNÝ, Bohumil. Multiplatformní komunikace v přístupových sítích, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2017. 103 s. Dizertační práce. Vedoucí práce byl doc. Ing. Vladislav Škorpil, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou dizertační práci na téma multiplatformní komunikace v přístupových sítích jsem vypracoval samostatně pod vedením vedoucího dizertační 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 dizertační práce dále prohlašuji, že v souvislosti s vytvořením této dizertační práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a~jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu dizertační práce doc. Ing. Vladislavu Škorpilovi, CSc. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé dizertační práce.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

Obrázek 44: Charakter odhadu v plně propojené topologii pro p = 0, p = 0,5 a p = 0,9.86

SEZNAM TABULEK

ÚVOD

Vývoj komunikačních technologií je stále se zrychlující proces. Masový rozvoj bezdrátových technologií s sebou přináší nové výzvy, kterým je třeba čelit. Jednou z nich se stává komunikace mezi zdánlivě odlišnými platformami. Multiplatformní komunikaci v přístupových sítích tedy můžeme chápat jako kooperaci komunikačních mechanismů bez vzájemného narušování funkcí. Tato dizertační práce se zaměřuje primárně na koexistenci bezdrátových přenosových platforem LTE, DVB-T a družicového rádia SiriusXM. Právě skutečnost, že jsou tyto platformy integrované do sítě na blízkých frekvencích, s sebou přináší negativní dopad na její celkovou kvalitu a spolehlivost v podobě interferencí v přístupových sítích.

Vytyčeným cílem dizertační práce je návrh nové metody detekce poruchy v bezdrátové síti s pomocí distribuovaného stochastického algoritmu push-sum. Dizertační práce volně navazuje na výzkumné projekty LO1401 Národního programu udržitelnosti a grantu GAČR 14-25298, pro výzkum byla využita infrastruktura centra SIX.

Vytyčeného cíle je dosaženo využitím modelu bezdrátové sítě, ve které jsou vzájemně provázané senzory detekující interference z jednoho uzlu, který ruší okolní přístupové body. Detekce této uměle zavedené poruchy do již existující infrastruktury v modelu je prováděna pomocí distribuovaného stochastického algoritmu push-sum na základě odhadu průměru vnitřního stavu uzlu identifikovaného parametrem kvality signálu.

Výzkum probíhající v rámci řešení dizertační práce měl ambice navrhnout nový způsob detekce poruchy v síti, který by otevřel další možnosti prevence a eliminace interferencí mezi stávajícími přístupovými body v přístupových bezdrátových sítích.

Volba vhodného algoritmu pro využití k účelu práce byla provedena na základě komparace statistické kredibility reprezentanta průměrné rychlosti konvergence protokolu push-sum a vlivu ztráty zprávy na robustnost systému ve vybraných topologiích. Na základě uvedených předpokladů pro implementaci zvoleného algoritmu do sítě je v práci proveden výzkum nové metody detekce, která je úspěšně zavedena do

sítě a je prokázána a matematicky podložena správná funkce navržené metody.

Navržená metoda volně navazuje na snahu společností zabývajících se bezdrátovými přenosy pracujících s technologiemi využívajícími frekvence blízké LTE v různých zemích predikovat a detekovat interference v bezdrátových systémech. Stalo se tak především na základě upozornění místních autorit, které monitorovaly chování sítě a na základě hlášení uživatelů, společností a dalších subjektů koordinovaly nápravu.

Právě způsob predikce a detekce interferencí se ale lišil mezi společnostmi zabývajícími se řešením vzniklých problémů, a proto tyto společnosti vynakládaly velké úsilí, aby docílily nápravy. Pro Českou republiku byly pro implementaci centrálního dohledového systému zvoleny společnosti T-mobile v kooperaci s IBM, které mají za úkol zavést jednotný dohledový systém. Monitorovací platforma bude vybudována s ohledem na mezinárodní monitoring sítě.

Hlavní motivací dizertační práce je navázat na projekt implementace dohledového systému v síti a navrhnout a ověřit novou metodu detekce poruchy v síti. Metoda vychází z již známých distribuovaných stochastických algoritmů sloužících pro řešení jiných specifických problémů. Porucha v síti reprezentovaná interferencí mezi přístupovými body v síti je poté simulována pro scénáře s různou hustotou uzlů v síti a na základě analýzy výsledků je diskutován přínos zvoleného algoritmu a navržené metody detekce poruchy v síti.

1 CÍLE DIZERTAČNÍ PRÁCE

Hlavním cílem dizertační práce je navrhnout novou metodu pro detekci poruchy sítě s využitím distribuovaného stochastického algoritmu a ověřit její aplikovatelnost. Pro dosažení tohoto cíle je využito současných poznatků souvisejících s distribuovanými algoritmy, následně je v práci vysvětlena problematika stochastických distribuovaných algoritmů, které úzce souvisí s cílem práce. Teoretické poznatky problematiky jsou také rozšířeny o oblast kooperace senzorových uzlů, na které je primárně řešení práce zaměřeno.

Senzorový systém je využit pro získávání vstupních parametrů sítě, které jsou dále odesílány a zpracovávány distribuovaným systémem a doplňují tak stávající komplexní mechanismy zpracování vstupních dat. Účelem navržené metody je tedy poskytnutí možnosti rychlé konvergence k výsledku reprezentujícímu stav sítě.

V souvislosti s využitím metod distribuovaného výpočtu vyplývají další otázky, které jsou v práci řešeny. Mezi základní řešené otázky patří volba nejvhodnějšího kandidáta distribuovaného algoritmu k aplikaci ve vztahu ke složitosti propojení sítě. Součástí vytyčených cílů je definice typu dat, která jsou senzorovým systémem přenášena a jejich relevantnost vzhledem k časovému posunu od počátku vyslání dat až k finálnímu vypočtenému výsledku.

Výběr vhodného algoritmu pro detekci poruch v bezdrátové síti je jedním ze stěžejních bodů dizertační práce. Na základě jeho volby je navržena a simulována funkce metody detekce poruchy v síti. Porucha v síti je reprezentována interferujícím uzlem s okolím. Detekce interferujícího prvku je provedena metodou výpočtu odhadu průměru vnitřního stavu uzlu a váhy uzlu. Vnitřní stav uzlu je definován jako parametr kvality signálu. Při splnění předpokladu, že se v síti vyskytne porucha v podobě interference z neznámého uzlu, odhad průměru obou hodnot se změní a na základě této změny je chyba detekována.

Výsledky a výstupy v bodech

1. Analýza současného stavu zainteresovaných témat vedoucí k volbě vhodného distribuovaného stochastického algoritmu.
2. Komparace statistické kredibility reprezentanta průměrné rychlosti konvergence zvoleného protokolu.
3. Ověření vlivu ztráty zprávy na robustnost zvoleného protokolu a volba vhodné topologie pro model detekce poruchy.
4. Návrh nové metody detekce poruchy vedoucí k funkčnímu řešení a jeho prezentace.
5. Ověření funkčnosti nově navržené metody detekce a její diskuse.

2 SOUČASNÝ STAV PROBLEMATIKY

Kapitola reflektuje současný stav problematiky přístupových a senzorových sítí a na základě vhodné literatury poskytuje základní náhled na témata přímo související s navrhovaným řešením dizertační práce. Sumarizace všech dostupných řešení by byla z hlediska rozsahu práce příliš široká, a proto je další text věnován především protokolům, algoritmům a technologickým řešením, která jsou nebo mohou být využívána v souvislosti s řešením této práce.

Teoretická rovina práce je věnována distribuovaným algoritmům zaměřeným na zrychlení konvergence sítě. Z tohoto pohledu je rozebrán rozdíl mezi deterministickými a stochastickými algoritmy, které poskytují rozdílné možnosti předávání informace v senzorové síti. Senzorová síť je zvolena jako vhodný kandidát pro implementaci distribuovaných stochastických algoritmů.

Vzhledem k rozsáhlým možnostem využití senzorových systémů je další analýza věnována hlavně interferencím v bezdrátových sítích, které mohou vznikat mezi přístupovými body pracujícími na blízkých frekvencích. Senzory schopné měřit a zpracovávat výsledky aktuálního stavu bezdrátové sítě poskytnou hlavní podklad v podobě parametru kvality sítě pro analytickou části dizertační práce.

2.1 Distribuované systémy

V posledních letech byla evoluce počítačové konektivity směřována na systémy distribuovaného výpočtu. Centralizovaný způsob výpočtu cest, který byl dříve hojně využíván, byl nahrazen distribuovaným výpočtem. Systémy, jejichž funkcionalita je založena na distribuovaném výpočtu, jsou označovány jako distribuované systémy. Agenty, ze kterých jsou zmíněné systémy složeny, lze charakterizovat jako elementy limitované znalostí svého přímého okolí, stejně tak jako znalostí topologie jako celku. Distribuovanost je poté chápána jako rozprostření výpočetní zátěže mezi více entit zainteresovaných pro jeden úkol. Rozprostření výpočetní zátěže může být realizováno více procesory v jednom centralizovaném výpočetním centru, ale i více nezávislými zařízeními, která mohou být geograficky vzdálena. Nasazování a následné využití

distribuovaných systémů se stává odvětvím, které se dynamicky rozvíjí ve více oblastech našeho života. Jejich implementací je dosahováno výrazného zrychlení procesů, které vyžadují rychlou konvergenci. Za příklad lze vzít např. telekomunikační technologie, distribuované zpracování informací, vědecké výpočty nebo řízení procesů v reálném čase [1].

2.1.1 Nároky kladené na distribuovaný systém

Reálnou hnací silou využití distribuovaných systémů v centralizovaných systémech je ekonomická oblast. Jednoznačná definice distribuovaných systémů ovšem neexistuje. V mnoha literárních pramenech, jako jsou [1], [19] nebo [31], je definován distribuovaný systém různě. Pokud vyjdeme z faktu, že je distribuovaný systém složen z autonomních komponent a pro externího uživatele působí dojmem jediného systému, musí tedy distribuovaný systém splňovat následující podmínky.

Přístupnost zdrojů

Přístupnost zdrojů znamená jednoduchý přístup uživatelů nebo aplikací ke vzdáleným zdrojům a jejich efektivní sdílení skrze zvolenou cestu. Sdílení zdrojů dává nejvíce smysl v oblastech, ve kterých se vyplatí sdílet velmi drahé komponenty systému, jako jsou superpočítače, záložní systémy sloužící pro skladování dat a další velmi drahé periferie. Jako dobrý příklad poslouží např. rychle se rozvíjející Internet. Nejen, že slouží pro sdílení velkých objemů dat pro vysoký počet uživatelů, ale je využit pro telekomunikační spojení geograficky oddělených firem po celém světě. Firmy jej poté využívají k telekonferenčním hovorům, kooperaci při řešení složitých úkolů nebo finančním transakcím.

S přístupností zdrojů ale přicházejí otázky bezpečnosti sdílení dat po Internetu. Mezi důležité aspekty bezpečnosti se řadí zabezpečení nešifrovaného textu, ochrana proti odposlouchávání, odchycení důležitých hesel, podvržení identity nebo bezpečnostní problém související se sledováním komunikace a následném sestavení profilu specifického uživatele **Chyba! Nenalezen zdroj odkazů.**. Sledování uživatele ez jeho souhlasu může vyústit v nevyžádané cílení reklamy, spamování e-mailové schránky a dalších problémů spojených s odchycením informací o uživateli.

Transparentnost

Distribuované systémy rozkládají potřebu výpočetního výkonu mezi více entit systému. Pro koncového uživatele je ale důležité vidět tento systém jako jeden celek, popřípadě jako jedinou aplikaci. Takový systém je nazýván jako transparentní. Transparentnost v distribuovaných systémech má více významů. Ty jsou rozděleny podle způsobu skrývání rozložení výpočetního výkonu:

- Přístup – skrývá rozdíly v reprezentaci a přístupu k datům.
- Poloha – skrývá lokaci entit systému.
- Migrace – skrývá změnu polohy entity v rámci jiných geografických oblastí.
- Relokace – skrývá změnu polohy entity, i když je zrovna používána.
- Replikace – skrývá replikace zdrojů.
- Konkurence – skrývá sdílení zdrojů mezi konkurenčními entitami.
- Porucha – skrývá poruchy a obnovování zdroje.

Přístupová transparentnost pracuje se skrýváním rozdílů v reprezentaci dat a způsobu, kterým může ke zdrojům přistupovat uživatel. V první řadě je třeba skrýt rozdíly v architektuře využívaných zařízení a také v rozdílech operačních systémů. Právě rozdíly v typu operačního systému jsou nejvíce patrny u konvencí spojených s příponami souborů v systémech a způsobu přístupu k informacím v souborech obsažených.

Důležitou skupinou transparentnosti jsou geografické lokace zdrojů. Transparentnost lokace říká, že koncový uživatel nebude ovlivněn globálním umístěním fyzického zařízení, ale naopak nebude moci ani definovat, odkud byla požadovaná informace odeslána. K tomuto jevu přispívá také pojmenovávání logických uzlů. Jednoduchým příkladem může být jmenný systém DNS. IP adresy jsou skryty za jmenné významy. Bez překladu jmenného významu na IP adresu je jen velmi obtížné alokovat polohu serveru v síti. Díky způsobu přidělování doménových jmen a jejich překladu není koncový uživatel ani schopen rozeznat, jestli se lokace serveru, ze kterého uživatel čerpá data, nezměnila. Dalším příkladem migrační transparentnosti

může být pohyb uživatele v mobilní síti při probíhajícím hovoru. Uživatel nemusí být obeznámen, ke kterému přístupovému bodu je právě připojen, ale ve chvíli, kdy se vzdálenost od přístupového bodu blíží k hranici jeho dosahu je hovor pomocí některého z druhů handoverů přepnut na další přístupový bod s nejvhodnějšími parametry mobilní sítě.

Jak můžeme pozorovat v reálném životě, replikace zdrojů zlepšuje také dostupnost zdrojů a výkon celého systému pouhým kopírováním informace co nejblíže k místu, kde je vyžadována. Z uvedeného tedy vyplývá, že replikační transparentnost navazuje taktéž na transparentnost lokační, protože by jinak nebylo možné odkazovat na repliky umístěné na různých místech. S replikací zdrojů také souvisí schopnost systému sdílet informace mezi svými entitami. Aplikaci sdílení zdrojů dnes vidíme především v možnosti spolupráce více geograficky vzdálených uživatelů na jednom souboru, kdy každý z uživatelů může soubor v reálném čase modifikovat. Jiným příkladem potom může být přístup k médiu z různých lokalit více uživateli. Tento systém je úspěšně využíván pro cloudové služby. Tyto služby bývají zpravidla placeným úložným prostorem realizovaným jako server nebo více serverů propojených skrze kontinenty. Servery jsou řetězově propojeny z důvodu zálohy data a opět je dosahováno iluze jednotného systému. Uživatelé se vzájemně nemohou dozvědět, zda a kdy kdo upravuje svůj datový prostor na serveru. Tento mechanismus je nazýván transparentnost konkurence. Důležitou podmínkou je, aby byl obsah uživateli odeslán v konzistentní podobě. Konzistence je dosaženo pomocí uzamykacích mechanismů, které zaručí uživatelům exkluzivní přístup k požadovaným zdrojům.

Faktor, kterým se bude tato práce zabývat, je způsob pracování distribuovaného systému s chybami. Vytvoření distribuovaného systému transparentního vůči chybám znamená, že uživatel nepozná chybu v systému, popřípadě ani zotavování systému po výpadku. Maskování problémů v distribuovaném systému je složitým úkolem. Problém může vzniknout v systému většinou vypověděním služby některého zařízení. Tato chyba svým vznikem ovlivní správnou funkci některých částí systému, avšak ostatní součásti systému zůstanou chybou nedotčeny. V nedistribuovaném systému je situace diametrálně odlišná. Vzniklá chyba v jednom z komponent přeruší práci celého systému a tím ho úplně vyřadí.

Důležitým úkolem distribuovaného systému je sestavit takový funkční celek, který bude mít schopnost automatického obnovení po částečném výpadku bez narušení uživatelských procesů. Systém pracující tímto způsobem je poté odolný proti chybám a jeho stabilita je dána možností práce v přítomnosti chyb i za cenu zhoršené výkonnosti. Spolehlivost distribuovaného systému je často důležitá pro udržení procesů synchronizovaných. Schopnost tolerance k chybám zahrnuje tyto následující požadavky:

- Dostupnost.
- Spolehlivost.
- Bezpečnost.
- Udržitelnost.

Dostupnost definujeme jako možnost okamžitého přístupu k prostředkům. Řečeno jinak je to pravděpodobnost, že v daném časovém okamžiku pracuje systém správně. Spolehlivost odkazuje na prostředky, se kterými může systém neustále pracovat bez narušení výpočtu chybou. Hlavní rozdíl mezi těmito dvěmi vlastnostmi je způsob, jakým je přistupováno k časovému kontinuu. Zatímco dostupnost je definována pro krátký daný časový interval, spolehlivost systému vyjadřujeme pro celý jeho životní cyklus. Vysoce spolehlivý systém je potom takový, který dokáže pracovat po relativně dlouhou dobu bez přerušení. Toto je nepatrný, ale důležitý rozdíl mezi těmito vlastnostmi. Jako praktický příklad rozdílu mezi spolehlivostí a dostupností lze uvést následující. Systém je dostupný po 99,99% času své práce, ale je nedostupný každou hodinu na 1 ms. Vykazuje tedy vysokou dostupnost, ale je nespolehlivý [29].

Bezpečnost odráží situace, při kterých systém dočasně vypoví svou funkci, ale nedojde k enormnímu výpadku. Opačná situace nastane při procesech náchylných na krátké výpadky. Pokud dojde k situaci, při které probíhá kritický proces a zároveň se v systému vyskytne výpadek, je vysoce pravděpodobné, že se požadovaný proces úplně zhroutí. Jednoduchým příkladem může být stavba domečku z karet. Pokud se při jeho stavbě jedna z karet nečekaně vychýlí ze své polohy, celý domeček z karet velmi pravděpodobně spadne.

Posledním z výše uvedených požadavků na distribuovaný systém je udržitelnost.

Udržitelnost je parametr, který vyjadřuje schopnost distribuovaného systému být jednoduše opraven [29].

Úroveň transparentnosti distribuovaných systémů

I když je skrývání struktury distribuovaného systému preferovaným nástrojem k vytvoření iluze jednoho celistvého celku, často dochází k situacím, při kterých se může stát skrývání struktury systému nežádoucím. Jako příklad lze uvést potřebu uživatele zasáhnout do systému a upravit parametr, který by jinak uživateli přinášel zavádějící nebo zcela chybná data a tento parametr je stěžejním pro výsledný výpočet. Pod tímto příkladem si můžeme představit změnu časového pásma, pro které je nastavena synchronizace. Pokud budeme vyžadovat od systému průběžný výsledek výpočtu v přesném čase 12.00 CET a zařízení bude mezitím migrováno do jiného časového pásma, výsledky budou dodávány dříve, či později v závislosti na tom, kterým směrem se v časovém pásmu zařízení posunulo. V takové situaci je zásah uživatele nebo administrátora systému nevyhnutelný.

Z výše uvedených důvodů existují v systému kompromisy mezi vysokou měrou transparentnosti a výkonem systému. K situacím vyžadujícím úpravu transparentnosti dochází z pravidla v momentu, kdy se snaží více aplikací dotázat ve stejném momentu na informaci, ale dotazované zařízení není schopno tyto výsledky zpětně předat v požadované rychlosti, a proto maskuje tento nedostatek zpomalením své činnosti. Výsledek ale uživatelům zaslán není. Z tohoto důvodu musí mít dotazované zařízení možnost zrušit některé požadavky a jiné zpracovat přednostně.

V systémech využívajících skrývání distribuce mohou nastat i jiné situace. Distribuovaným systémem je i sdílené tiskárny pro jednu budovu. Pokud by uživatelé neměli možnost volby tiskárny, jejich dokumenty by byly odesílány do tiskárny s nejkratší frontou. Z matematického hlediska je výběr tiskárny na základě délky tiskové fronty vhodným, avšak z hlediska uživatele by bylo velmi nevhodné, kdyby si musel uživatel pro svůj dokument jít přes celou budovu místo pouhého počkání si na vytištění dokumentu ve své kanceláři, byť by před ním ve frontě bylo několik jiných tiskových úloh. Z hlediska uživatele je tedy zásah do řazení dokumentů žádoucím.

Pro shrnutí této kapitoly je nutné říci, že dosažení plného skrytí struktury distribuovaného systému může být vhodné, ale častěji se v praxi setkáváme s více

transparentními systémy umožňujícími externí zásahy do zpracování požadavků. Při implementaci distribuovaného systému je tedy třeba zvážit otázky výkonnosti a srozumitelnosti systému.

Otevřenost distribuovaného systému

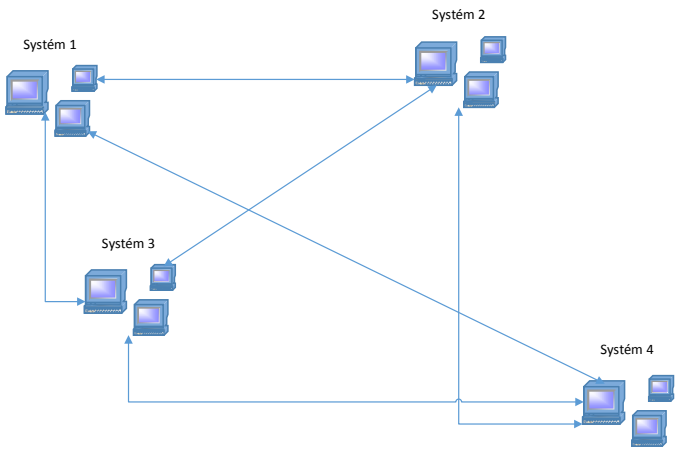
Otevřený distribuovaný systém je systém, který nabízí služby podle standardních pravidel, které popisují syntaxi a sémantiku těchto služeb. V praxi se s takovým systémem setkáváme v sítích využívajících internetových protokolů. Internetový protokol jako například TCP má jasně definovanou hlavičku, všechna svá povinná i nepovinná pole a datovou část. V distribuovaných systémech jsou služby obvykle specifikovány podle rozhraní, které je popsáno v IDL. Definice rozhraní v IDL je téměř vždy definována specifickou syntaxí. Nejtěžším úkolem definice je přesná specifikace služeb a jejich sémantika a význam rozhraní.

Pokud je rozraní správně specifikováno, dosahujeme bezchybné komunikace mezi procesy přistupujícími k rozhraní. To nám přináší možnosti sestavení dvou nezávislých implementací fungujících jako dva distribuované systémy fungující na stejném principu. Správné specifikace jsou úplné a neutrální. Úplnost specifikace je dána splněním všech nezbytných požadavků pro správnou funkci systému. Úplnost a schopnost systémů předávat si vzájemně data, poskytovat služby a efektivně spolupracovat jsou důležitým parametrem pro přenositelnost systému [31]. Uvedené vlastnosti charakterizují rozsah, v němž mohou dvě implementace systémů nebo komponent od různých výrobců existovat společně a spolupracovat tak, že spoléhají pouze na služby definované společným standardem. Přenositelnost algoritmu říká, do jaké míry může být použita aplikace vyvinutá pro distribuovaný systém A bez modifikace pro jiný systém B pracující se stejným rozhraním jako systém A [33].

2.1.2 Architektura distribuovaných systémů

Distribuované systémy jsou komplexním mechanismem spojujícím softwarové i hardwarové prostředky. Ke zvládnutí jejich komplexity je rozhodující jejich důkladná organizace. Nejvyššího stupně abstrakce je dosaženo cestou softwarového rozložení. Softwarové rozložení definuje způsob organizace v síti a také pravidla interakce, která jsou na komponenty sítě navázána. Jak bylo uvedeno v předchozí kapitole, jednou

z hlavních podmínek distribuovaného systému je jeho transparentnost. Transparentností distribuovaného systému je dosaženo abstrakce jednotného systému. Abstrakce systému vychází z jeho účelu nasazení a lze ji diverzifikovat na dvě úrovně. První úroveň je definována jako úroveň komunikace s uživateli a druhá úroveň je dána jako komunikace procesů s jádrem systému. Za distribuovaný systém lze považovat každý, který využívá ke zpracování dat více než jeden počítač či procesor, má rozdělen program na více kooperujících částí nebo jsou výpočty zpracovány na více různých procesorech. Jednoduchý náhled na princip diverzifikace zátěže mezi více entit je uveden na obrázku Obrázek 1. Jak je z nákresu patrno, jednotky pracující na zadaném úkolu mohou být vzdáleny geograficky a dalším úkolem je poté pouze synchronizace jejich úkolů a vzájemná konektivita. Podobným způsobem pracují tyto systémy na softwarové bázi. Uvedené systémy poté definujeme jako distribuované architektury.



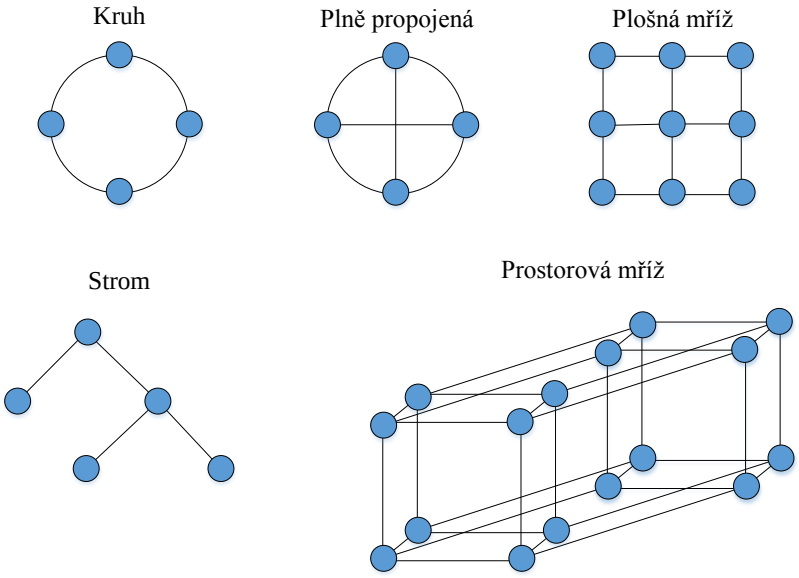
Obrázek 1: Zjednodušený náhled na hardwarově oddělený distribuovaný systém.

Distribuované architektury, které jsou založeny na sdílení společné paměti, označujeme jako systémy s velmi těsnou vazbou. Jsou určeny především k řešení diferenciálních rovnic nebo analýze a modelování přírodních jevů. Dalším typem distribuovaných struktur jsou takové, které jsou založeny na vzájemné komunikaci. Vzájemná komunikace je realizována pomocí komunikačních řadičů zajišťujících transportní služby. Soubor transportních služeb a procesorů, které se specializují na předávání zpráv v rozličných síťových topologiích, poté nazýváme komunikačním podsystémem. Tento podsystém je většinou vystavěn jako univerzální struktura sloužící v reálném nasazení pro směrování v rozlehlých sítích polygonálního rozložení [2].

2.1.3 Hardwarově definované topologie

V počítačových sítích, mobilních komunikacích a ve většině oborů vyžadujících spolupráci zařízení v síti jsou využívány topologie, které jsou svou povahou členěny na statické a dynamické. Za statické topologie jsou považovány takové, které udržují spojení mezi svými entitami konstantní. Naopak dynamické topologie se v čase mohou měnit a přizpůsobovat svá propojení požadavkům zadaným uživateli, správci nebo jejich entitami.

Statické topologie, nazývané též regulérní struktury, jsou převážně využívány pro aplikace výpočtů v menších sítích, kde nehraje roli počet spojů mezi jednotlivými uzly. Taková propojení sítě mohou být považována za žádoucí při aplikacích, které takovou topologii vyžadují. Pro kruhovou topologii platí, že je výhodná pro sítě s požadavkem na nízký počet spojů. Naopak stromovou strukturu lze využívat pro aplikace využívající hierarchického rozkladu. Mezi další struktury patří plošné a prostorové mříže vyznačující se vysokou měrou propojení. Příklady statických topologií jsou znázorněny na obrázku Obrázek 2. Jelikož se práce dynamickými druhy hardwarově definovaných sítí nezabývá, nebude tato tématika dále rozebírána.



Obrázek 2: Příklady statických topologií.

2.1.4 Softwarově definované topologie

Logické organizační struktury nebo také jinak řečeno softwarově definované topologie nasazují na fyzické spojení uzlů sítě logickou hladinu skrývající skutečné propojení sítě. Diskuse na témata týkající se architektonického stylu jsou důležité zejména z důvodu definice propojení komponent, druhu jejich propojení, typu dat, která jsou mezi nimi vyměňována a také způsobu implementace těchto jednotlivých elementů do systému. Soubor komponent specifikuje sady případů, které jsou užívány k definicím softwarových systémů libovolné velikosti a složitosti. Tento soubor komponent specifikuje v rámci svého prostředí nahraditelnou modulární jednotku. Koncept komponent se zabývá oblastí vývoje založeného na komponentách a strukturování systémů pro komponenty. Zde je každý jednotlivý komponent modelován po celou dobu vývojového životního cyklu a následně je vybrán ke spuštění a běhu. Důležitým aspektem komponentově založeného vývoje je opětovné využití předchozích komponent [34]. Pro distribuované systémy je důležité, že komponenta sítě může být nahrazena, pokud je zachováno její rozhraní. Složitějším případem pro implementaci je poté mechanismus navázání spojení, koordinace spojení nebo koordinace spolupráce komponent [35]. Spojení mohou být navázána vzdáleně pro probíhající procedury, průchod zpráv nebo posílání dat.

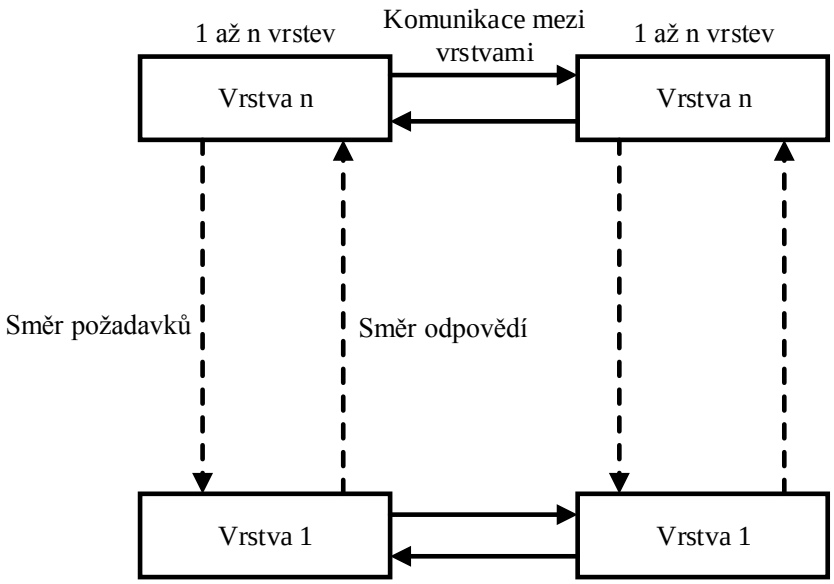
Používání komponent a jejich spojení můžeme dosáhnout rozličných konfigurací sítě. Tyto konfigurace poté nazýváme jako architektonické styly. Mezi nejvýznamnější architektonické styly sítí využívajících distribuované systémy patří:

- Vrstvové architektury.
- Objektově orientované architektury.
- Architektury založené na centralizaci datových přenosů.
- Architektury založené na centralizaci událostí.

Vrstvové architektury

Podobně jako u síťového modelu ISO/OSI vypracované organizací OSI jsou i výše uvedené vrstvové architektury organizovány tak, aby vzájemně komunikovaly pouze vrstvy stejného druhu. Každá vrstva poté volá pouze své komponenty [36]. Klíčovou vlastností vrstvového modelu je řízení toku řídících dat z vyšších vrstev na nižší.

Jednoduchý příklad je uveden na obrázku Obrázek 3.

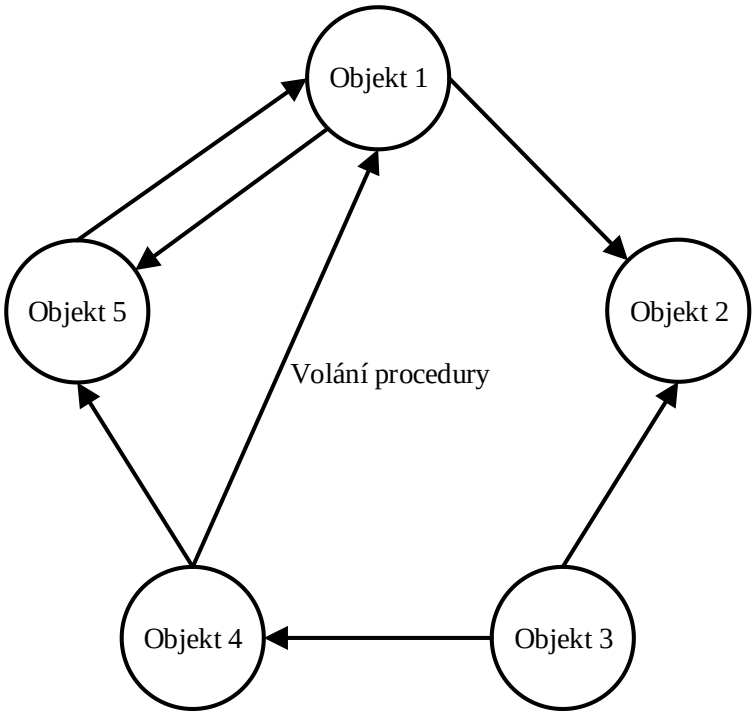


Obrázek 3: Vrstvová architektura.

Objektově orientované architektury

Méně vázanou organizační strukturou jsou objektově orientované architektury, které jsou zobrazeny na obrázku

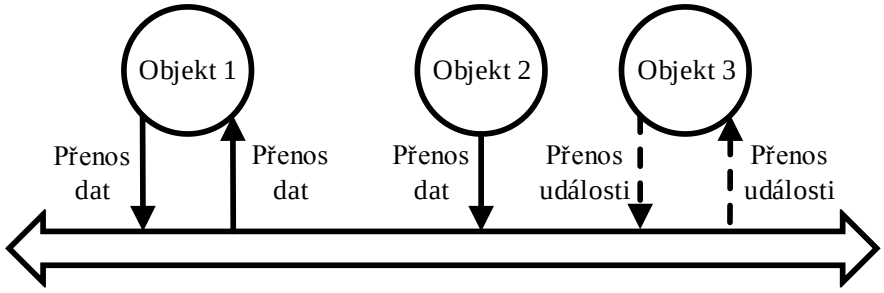
Obrázek 4Obrázek 1. Tyto struktury jsou složeny z komponent, které jsou předem definovány jako objekty. Komponenty spolu v rámci systému komunikují pomocí mechanismu vzdáleného volání procedur. Chování softwarové architektury tímto způsobem odpovídá chování systému klient – server. Vrstvové a objektově orientované softwarové struktury patří k nejvyužívnějším typům softwarově definovaných struktur [34].



Obrázek 4: Objektově orientovaná struktura.

Architektury založené na centralizaci datových přenosů a událostí

Architektury založené na centralizaci datových přenosů jsou často kombinovány s architekturami centralizující také přenosy událostí. Kooperace při sdílení média pro přenos obou typů informace v distribuovaném systému je nazývána sdílený datový prostor. Podstatou sdílení datového prostoru je časové oddělení obou rovin komunikace. To znamená, že nemusí být datový přenos a přenos události uskutečňován pomocí obou typů přenosů najednou, ale může docházet k nezávislé komunikaci na datové úrovni nebo na úrovni přenostu událostí, aniž by se oba přenosy vzájemně ovlinvnily. V mnoha případech je k přístupu ke sdílenému úložišti přistupováno pomocí popisu, než přímým odkazem jako u souborových systémů. Kooperace obou typů architektur je nastíněna na obrázku Obrázek 5.



Obrázek 5: Architektura založená na centralizaci datových přenosů a událostí.

2.1.5 Centralizované distribuované architektury

Komunikace v distribuovaných systémech probíhá většinou na bázi komunikace mezi klientem a serverem. Server poskytuje služby specifické pro implementaci procesu, například služby souborového systému nebo správy databází. Naproti tomu klient je ten, který služby od serveru požaduje a na svůj požadavek musí čekat. Interakce mezi klientem a serverem je nazývána také jako chování typu požadavek - odpověď.

Pokud dosáhneme vysoké spolehlivosti bezdrátové komunikace, spolupráce mezi klientem a serverem může být realizována pomocí jednoduchých protokolů bezdrátovou komunikací podporujících. V těchto případech bývá klientův požadavek zabalen do jednoduché zprávy pro server. Ve zprávě je obsažen identifikátor klienta a vstupní data. Server čekající na požadavek od klienta jej po jeho obdržení zpracuje a následně posílá klientu odpověď, či zpracovaná data podle požadavku.

Bezdrátová komunikace mezi klientem a serverem poskytuje řadu výhod, ale je úzce spjata i s nevýhodami plynoucími z povahy přenosu zpráv mezi entitami. Jedním z hlavních problémů v bezdrátových sítích je možnost porušení nebo úplné ztráty zprávy, která je přenášena volným prostředím. V případě detekce porušení nebo ztráty zprávy mezi klientem a serverem je nejčastější prevencí opětovné odeslání zprávy. Tato prevence ale s sebou přináší další případné problémy, jako je vyšší zahlcení sítě, zpomalení komunikace v síti a s tím související zvyšující se ekonomické i energetické nároky na obě komunikující entity. V případě senzorových systémů je právě zvýšená spotřeba elektrické energie kritickým faktorem pro plánovanou životnost akumulátorů. Dalším negativním faktorem je poté spolehlivost sítě při nedoručení zprávy. Ta může

být uměle zvýšena například opětovným zasíláním stavu entity po vykonání požadovaného úkolu. V aplikované sféře by toto opětovné potvrzení pracovalo jako v následujícím příkladu. Klient požaduje, aby bylo v databázi sníženo číslo na určitých souřadnicích z hodnoty 5 na hodnotu 4. Server požadavek obdrží, zpracuje a odesílá klientu potvrzení o snížení hodnoty čísla na 4. Klient ale odpověď serveru neobdrží. Opětovným odesláním zprávy směrem od serveru ke klientovi o stavu hodnoty nastavené na 4, by se předešlo dalším požadavkům od klienta k serveru a tím zefektivnění komunikace.

Alternativou jednoduchých komunikačních protokolů jsou spolehlivé spojově orientované protokoly. Jejich hlavní výhodou je vysoká spolehlivost, ovšem za cenu vyšších nároků na hardware implementovaných entit v síti. Tyto protokoly jsou často implementovány do sítí, které jsou ze své podstaty nespolehlivé. V případě praktické aplikace by se daly přirovnat k protokolům TCP, které nejprve vytvoří spojení mezi klientem a serverem, toto spojení poté pro komunikaci využívá klient i server pro přenos dat, zpráv i potvrzovacích údajů a po ukončení komunikace se vytvořená cesta opět rozpadá. Pro senzorové sítě je ale využití této formy komunikace velmi neefektivní hlavně v případech, kdy senzor odesílá pouze malé množství zpráv o délce několika bytů. Pro takové zprávy je každé sestavení komunikačního kanálu mnohem náročnější, než samotné odesílání zpráv.

2.1.6 Decentralizované distribuované architektury

Pro vysvětlení principu distribuovaných architektur je v této práci využito jejich analogie softwarové konfigurace, ze které vycházejí i aplikované důkazy v kapitole **Chyba! Nenalezen zdroj odkazů.**. Vícevrstvé architektury typu klient server jsou přímým následkem rozdělování aplikací na jejich vrstvy, kterými jsou úroveň datová, procesní a uživatelská. Různé úrovně dělení aplikací úzce korespondují s jejich logickou organizací. V distribuovaných systémech je tento typ úrovňového dělení nazýván vertikální distribuce. Charakteristickou vlastností vertikální distribuce je způsob logického umístění různých komponent na různé stroje. Pojem vertikální distribuce je často spojován také s koncepcí vertikální fragmentace využívané hlavně v distribuovaně orientovaných databázích. Zde je tato fragmentace vyjádřena užívána pro rozdělení tabulek na logické sekce a následně distribuována pomocí více fyzických

zařízení [37].

Z perspektivy správy systémů dopomáhá vertikální distribuce díky logickému a fyzickému rozdělení funkcí k následnému přiřazení funkce konkrétnímu stroji přizpůsobenému k jejímu vykonávání. Zjednodušeně řečeno každý stroj v síti pracuje pouze s jedním typem výpočtu, ke kterému je určen. Tím je dosaženo rychlejšího zpracování informace a samozřejmě jsou tak optimalizovány také náklady.

Oproti hojně využívané vertikální distribuci je při zpracování informace nebo dat v síti využívána také horizontální distribuce. Při horizontální distribuci, známé také jako systém peer to peer (P2P), nehraje roli druh funkce, která je právě vykonávána a celý proces není dělen podle typu informace, ale výpočetní prostor jednotek je rovnoměrně rozdělován mezi všechny entity stejně tak, aby byly zatíženy všechny stroje na podobnou úroveň. V důsledku toho je velká část interakce mezi procesy symetrická a každý proces navenek působí jako klient i server zároveň. Kvůli tomuto symetrickému chování procesů se P2P architektury potýkají s otázkou organizace procesů v překryvných sítích.

Překryvné sítě P2P jsou na základě svého přirozeného chování zařazeny mezi distribuované systémy bez centralizovaného řízení. P2P sítě nabízejí výhody jako je robustní směrovací architektura, efektivní vyhledávání datových položek, volbu nejbližšího uživatele, redundantní úložiště, stálost, hierarchickou strukturu názvů, věrohodnost, autentičnost, anonymitu, vysokou škálovatelnost a odolnost proti chybám. Na rozdíl od mřížových systémů ale P2P systémy nemohou vzniknout bez spolehlivých zdrojů dat a neustále připojených uživatelů. Tato dynamičnost sítě vyžaduje pro svou správnou funkci směrovací algoritmy pro optimalizaci [38].

Definice decentralizovaného distribuovaného systému vychází z myšlenky, že jsou všechny uzly v síti rovnocennými partnery z hlediska funkčnosti a úkolů, které vykonávají [39]. Do této definice ale nejsou zahrnuty částečně decentralizované systémy určené pro sdílení informací, které sice pracují na principu decentralizovaného systému, ale z pravidla je v jejich struktuře obsažen miniserver, který zajišťuje kooperaci a koordinaci zdrojů. Jedním z mnoha příkladů je projekt Edutella [40]. Referenční architekturu umožňující podrobnější porovnání decentralizovaných distribuovaných struktur poskytuje publikace Aberea a kolektivu v [41].

2.2 Stochastické distribuované systémy

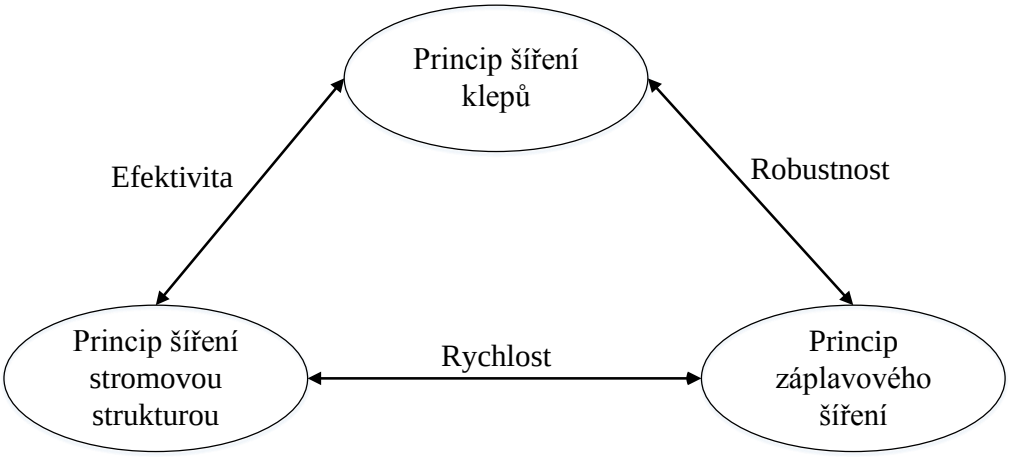
Stochastické optimalizační algoritmy lze definovat jako náhodné a tedy nedeterministické algoritmy, které mohou sloužit pro získávání informace. Většinu používaných algoritmů z kategorií výpočetní počítačové inteligence, metaheuristických nebo genetických lze pomocí stochastických algoritmů optimalizovat. Algoritmy využívající jisté náhodnosti v procesu mají ve skutečnosti daná pravidla chování a mohou se zaměřovat na oblasti vhodné pro jejich implementaci v síti a ostatní oblasti v rámci svých výpočtů ignorovat [42]. Skupiny technik zabývající se stochastickým vzorkováním jako například MCMC (Markov Chain Monte Carlo) selektují statistické vzorky do cílové hustoty pravděpodobnosti a jsou využívány především pro účely výpočtů ve fyzice.

2.2.1 Protokoly založené na vzájemném sdělování informace

Protokoly založené na vzájemném sdělování informace jsou velmi často využívány pro implementaci v ad-hoc sítích, ve kterých není určen žádný nadřazený prvek, peer to peer sítích označovaných také P2P pracujících na podobném principu jako ad-hoc a také senzorových sítích. Předávání informace v uvedených sítích mezi jednotlivými uzly je v odborné literatuře nazýváno též předávání drbů či pomluv. Takové označení nejlépe vystihuje podstatu procesu předávání drbů v sociální oblasti. Tyto protokoly jsou nasazovány nejčastěji k řešení problémů škálovatelnosti a spolehlivosti sítí. Jejich schéma je navrženo pro decentralizovaná zpracování agregačních funkcí v překryvných sítích [17].

Protokoly využívané pro šíření informací ve velmi rozsáhlých síťových systémech by měly splňovat základní podmínky, mezi které patří efektivita, robustnost, rychlost a škálovatelnost. Jak již bylo naznačeno v přecházející kapitole věnované využívaným topologiím, lze k sítím využívajícím alternativní postupy přistupovat na základě základních principů propojení jednotlivých uzlů a šíření informace skrz síť. Prvním z principů je stromově orientovaná topologie, která se vyznačuje vysokou efektivitou, složitou konfigurací a nepříliš vysokou robustností. Oproti tomu šíření informace principem záplavy sítě informací můžeme mluvit o vysoké robustnosti na úkor efektivity. Oba tyto příklady tedy vedou k principu šíření informace třetím způsobem.

Tím jsou právě protokoly vyžívající epidemického šíření informace založené na vzájemném sdělování informace mezi uzly v síti nazývané jako protokoly s principem šíření klepů. Jejich hlavními přednostmi je efektivita a robustnost na úkor latence. Na obrázku Obrázek 6 lze poté vidět vztah mezi všemi třemi principy.



Obrázek 6: Principy šíření informace v síti [23].

V reálném světě se princip rozprostření informace do populace šíří v podstatě stejným způsobem a lze ho popsat následovně. Nazvěme nositele klepu (informace) informovaným jedincem. Ostatní jedinci v jeho okolí, kteří jsou neinformováni, budou nazváni jako neznalí. Všichni neznalí chtějí mít informaci od znalého. Znalý jedinec si vybírá jednoho neznalého v okolí a informaci rozšíří. Tím se neznalý stává znalým a stejným způsobem informaci předá do svého okolí. Informace je předávána vždy po uplynutí času jednoho kola. Celá procedura předávání zprávy končí v momentě, kdy se všichni neznalí v určené oblasti stanou znalými. Minimální čas S_n potřebný k rozprostření informace lze vyjádřit jako:

$$S_n = \log n + \ln n + O(1) \qquad (1)$$

Tato rovnice ale platí pouze při předávání zprávy (push) s pravděpodobností n blížící se nekonečnu [25]. Při takovém rozeslání informace je počet všech zpráv definován jako $O(NlogN)$.

Předpokládejme, že máme populaci o velikosti n a v daném kole počet informovaných osob roven k. Můžeme tvrdit, že počet neinformovaných osob bude $n - k$. Poměr informovaných a neinformovaných osob tedy poté můžeme vyjádřit

proměnnou X při velikosti vzorku k. Tento případ je vyjádřen v rovnici (2).

$$P(X = x) = \frac{\binom{n-k}{x}\binom{k}{k-x}}{\binom{n}{k}} \quad (2)$$

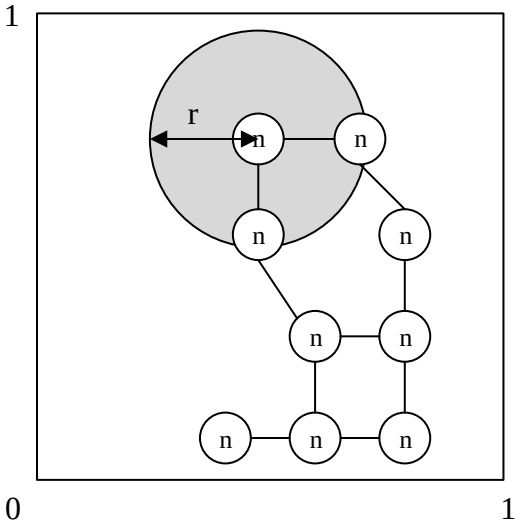
Pro $0 \leq x \leq \min(n - k, k)$. To je hypergeometrická distribuce s velikostí populace n, počtem informovaných osob v populaci $n - k$ a velikostí vzorku k, který je označován jako $HG(n, n - k, k)$. Z této rovnice poté dostaneme:

$$E(X) = \frac{k(n-k)}{n} = k - \frac{k^2}{n} \quad (3)$$

Z rovnice vyplývá, že zdvojnásobení počtu informovaných osob v populaci dosáhneme, když $E(X) > k$ nebo $k < \sqrt{\frac{n}{2}}$. Pro velikost populace s jednou informovanou osobou očekáváme 2^j osob informujících. Zde proměnná j definuje počet kol od začátku rozprostírání informace [26].

2.2.2 Geometrický náhodný graf

Geometrický náhodný graf je úspěšně využívaný k modelování senzorových sítí. V rámci modelování senzorové sítě budeme uzel označovat písmenem n, jeho poloměr dosahu bude označen r a dimenze grafu bude označována jako d. graf bude vyjádřen jako $G^d(n,r)$. Pokud bude mít graf dvě dimenze $[0,1]^2$, bude vyjádřen jako $G^2(n,r)$. Graf tedy znázorňuje model senzorové sítě a pracuje s předpokladem, že každé dva uzly, které jsou v dosahu r se mohou spojit a vzájemně komunikovat. Příklad dvoudimenzionálního grafu $G^2(n, r)$ je poté uveden na obrázku Obrázek 7.



Obrázek 7: Příklad náhodného dvoudimenzionálního grafu $G^2(n,r)$, ve kterém jsou jednotlivé uzly n propojeny s ostatními uzly n ve vzdálenosti r.

Následující příklad definuje matematický popis krajní meze dosahu signálu pro $G^d(n,r)$:

1. Nechť je konstanta $\alpha_d > 0$ pro všechna $\varepsilon > 0$,
2. pokud $(\frac{nr^d(n)}{\log n}) \geq \alpha_d + \varepsilon$,
3. pak $G^d(n, r(n))$ je propojeno s pravděpodobností $1 - o(1)$,
4. a pokud $\left(\frac{nr^d(n)}{\log n}\right) \leq \alpha_d - \varepsilon$,
5. pak $G^d(n, r(n))$ není propojeno s pravděpodobností $1 - o(1)$,
6. $d_{max} = (1 + o(1))d_{min}$.

To znamená, že $G^d(n, r(n))$je téměř regulérní. Proto můžeme definovat přirozeně náhodnou cestu pro $G^d(n, r(n))$ s přechodovou maticí P, kde:

$$P_{ij} = \begin{cases} \frac{1}{2}, & pokud\ i = j \\ \frac{1}{2d_i}, & pokud\ j \in N(i) \\ 0, & v\ opačném\ případě \end{cases} \quad (4)$$

Je zřejmé, že P je aperiodická díky zpětné smyčce a neredukovatelná kvůli

$G^d(n, r(n))$ s pravděpodobností $1 - o(1)$. Nechme π být stacionární distribucí náhodného průchodu maticí P. Pak tedy platí $\pi_i = (1 + o(1))/n$ s pravděpodobností $1 - o(1)$. Je tedy stanoveno, že smíšený čas náhodného průchodu bude:

$$\tau(\varepsilon, \mathrm{P}) = \Omega(\mathrm{r}(\mathrm{n})^{-2}) \qquad (5)$$

a

$$\tau(\varepsilon, \mathrm{P}) = \mathrm{O}\left(\frac{\mathrm{r}(n)^{-2} \log n}{\varepsilon}\right). \qquad (6)$$

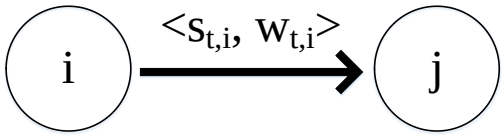
Dále bylo stanoveno, že nejrychlejší smíšený vratný náhodný průchod $G(n, r(n))$ s uniformní stacionární distribucí neměl smíšený čas větší, než $\mathrm{r}(n)^{-2}$. To znamená, že přirozený náhodný průchod přes G (n, r) má smíšený čas stejný jako náhodný průchod sítí s nejrychlejším smíšeným časem [19][21][22].

2.2.3 Druhy epidemicky se šířících algoritmů

Epidemicky se šířící algoritmy můžeme dělit na tři oblasti. Za stěžejní oblasti považujeme varianty šíření typu push (předej), pull (požaduj) a kombinaci push-pull (předej a požaduj).

Varianta šíření informace typu push

Každý jednotlivý uzel posílá svůj vnitřní stav a váhu jinému náhodně zvolenému uzlu ve svém okolí, se kterým má vytvořené spojení. Nejefektivnější fází této varianty šíření informace sítí je fáze počáteční. Jednostranné šíření informace zachycuje obrázek Obrázek 8.



Obrázek 8: Šíření informace v záplavových protokolech typu push.

Varianta šíření informace typu pull

Každý uzel žádá okolní uzly o jejich vnitřní stav a váhu. Stěžejní vlastností varianty šíření informace pomocí zadávání požadavků na informaci od okolních uzlů, je

pomalý start konvergence sítě, který ale vyústí v její rychlé dokončení.

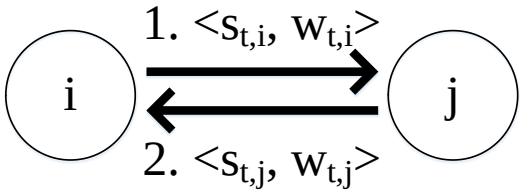
Varianta šíření typu First-Push-Then-Pull

Algoritmus First-Push-Then-Pull nazývaný zkráceně FPTF kombinuje výhody obou předchozích variant distribuce váhy a stavu uzlu v síti. U tohoto druhu algoritmu musí být nejprve zjištěna hranice, kdy je ještě výhodné používat variantu šíření push a následně pull z důvodu dosažení co nejlepší efektivnosti algoritmu. Princip výměny zpráv mezi uzly je poté prováděn náhodným výběrem okolních uzlů, kterým jsou odesílány informace o stavu a váze každého uzlu a následně jsou tyto zprávy od okolních bodů zase vyžadovány. Takto jsou párové výměny realizovány, dokud nedojde ke konvergenci sítě [24].

Podle obrázku Obrázek 9 bychom mohli matematicky vyjádřit výměny párů informací jako:

$$VRS = \begin{cases} S_{t+1,i} = \frac{1}{2}(S_{t,j} + S_{t,i}) \\ W_{t+1,i} = \frac{1}{2}(W_{t,j} + W_{t,i}) \end{cases} \quad (7)$$

Kde VRS vyjadřuje jeden krok protokolu, hodnota W vyjadřuje aktuální váhu uzlu v rozmezí 0 až 1 a hodnota S udává hodnotu stavu v rozmezí 0 až 1. Znaky i a j označují uzly lokálního páru, mezi kterými probíhá výměna těchto dvou informací[23].



Obrázek 9: Princip odesílání zprávy mezi dvěma uzly při použití protokolu FPTF [23].

Jak bylo publikováno v [24], optimální implementace algoritmu FPTP do plně propojené sítě, která je schopná vzájemné kooperace, může velmi výrazně snížit cenu komunikace. FTPF minimalizuje očekávanou normalizovanou cenu komunikace snížením počtu přenosů v protokolech využívajících záplavové šíření informace.

2.2.4 Protokol Push-Sum

Push-sum protokol je klasifikován jako multifunkční epidemicky se šířící algoritmus, jehož funkcionalita je založena na distribuci hodnot mezi páry agentů [19]. Je určen pro nahodilou komunikaci v rozsáhlých sítích, ve kterých garantuje jejich rychlost konvergence a přesnost. Mezi další přednosti protokolu push-sum patří robustnost, škálovatelnost, výpočetní a komunikační efektivita a vysoká stabilita při rušení. Díky nahodilosti procesu zpracování výsledků se výsledky mohou lišit navzdory zachování konstantních vstupních dat [18]. Jak již bylo zmíněno, push-sum protokol může po své modifikaci řešit více problémů. Charakter protokolu je inspirován sociálním chováním populace, ve které se informace šíří pomocí vzájemného sdělování informací mezi lidmi. V obecné rovině se jedná o pomluvy či drby definující epidemické sdělování faktů a názorů, jejichž důsledkem je rozprostření informace mezi členy populace. Z evolučního hlediska lze tento typ sítí nazývat jako překryvné [23].

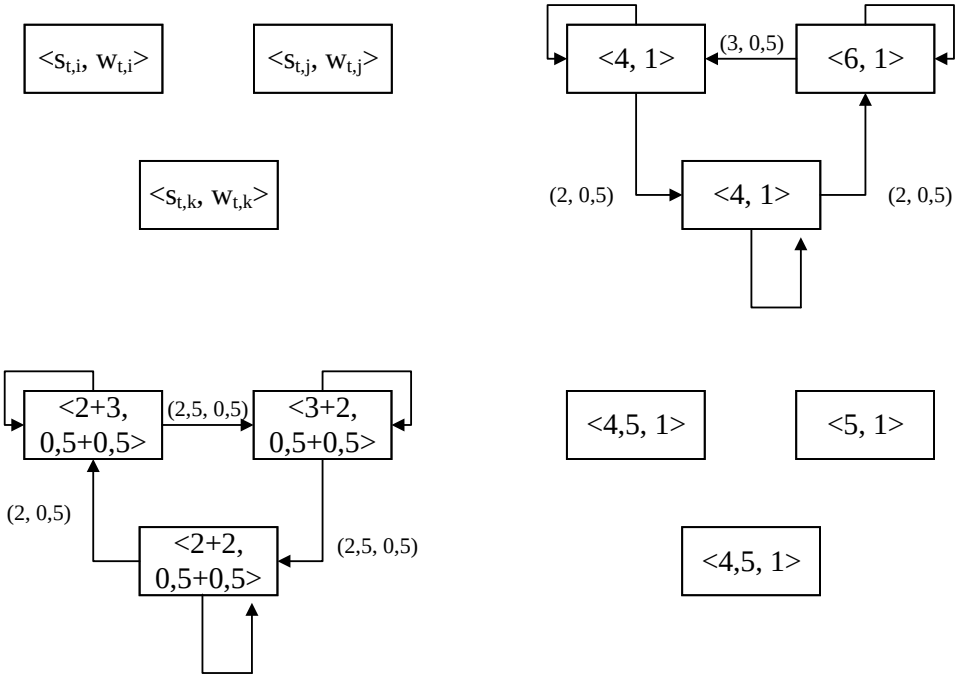
Základním principem protokolu bývají modifikace pro výpočet průměrných hodnot ze vstupních parametrů. Na začátku celého procesu je každému agentu přiřazen počáteční vnitřní stav roven jedné. Zároveň je určena váha každého agenta také pro hodnotu jedna. V následujícím kroku je náhodně vybrán jeden z jeho sousedů při každé iteraci. Zvolenému agentovi je poslána poloviční hodnota vnitřního stavu odesílatele a poloviční hodnota jeho váhy. Ty samé hodnoty jsou také uloženy ve vnitřní paměti odesílatele. Každý agent je poté schopen vypočítat poměr těchto hodnot. Tento postup je popsán následovně:

1. Nechť $\{(\widehat{s_r}, \widehat{w_r})\}$ jsou páry poslané i v $t-1$,
2. nechť $s_{t,i} := \sum_r \widehat{s_r}$, $w_{t,i} := \sum_r \widehat{w_r}$,
3. rovnoměrně náhodný výběr agenta $f_t(i)$,
4. odeslání páru $(\frac{1}{2}s_{t,i}, \frac{1}{2}\ w_{t,i})$ agentu $f_t(i)$ a i,
5. $\frac{s_{t,i}}{w_{t,i}}$ je odhad průměru v t.

Push-sum protokol může být implementován do distribuovaného systému proto, aby vypočítával průměr hodnot všech entit zúčastněných v systému. Při předpokladu implementace protokolu push-sum do systému ovšem nelze počítat s častými

dynamickými změnami v síti během výpočtu.

Protokol push-sum se chová podle následujících pravidel. Každý uzel i pracuje se sumou s_i.a váhou w_i. Počáteční stav s_i.= x_i a počáteční váha uzlu je w_i.=1. V každém kole je náhodně vybranému okolnímu uzlu označenému j a sobě samému zaslána polovina stavu uzlu $s_i/2$ a polovina váhy uzlu $w_i/2$. Poté jsou přičteny všechny obdržené hodnoty s_j a w_j. Na konci kola je vypočítán odhad jako poměru hodnot s_i/w_i. Aby bylo možné jasně určit princip fungování, je na obrázku Obrázek 10 znázorněn výpočet vah a stavů pro tři uzly v síti.



Obrázek 10: Princip výpočtu hodnot váhy a stavu u push-sum protokolu.

Součet všech vnitřních stavů musí být vždy rovem celkovému součtu. Oproti tomu součet všech vah uzlů w_i je roven n. Eventuálně může být každý agent vlastníkem frakce rovné 1/n ze všech hodnot počátečních stavů a eventuálně také frakce 1/n všech vah. Hodnota stavu s_i tedy bude průměrem a váha uzlu bude rovna hodnotě 1. Pokud by čistě teoreticky dosáhla váha jednoho uzlu hodnoty $w_i = 1$, váha všech ostatních uzlů by byla rovna hodnotě $w_i = 0$.

Hodnoty všech agentů v síti jsou protokolem push-sum rozptylovány do té doby,

dokud nejsou tyto hodnoty distribuovány v síti uniformně. Uniformní rozptýlení hodnot v síti lze považovat za ustálený stav. Rychlost výše zmíněné difúze hodnot v dané síti uzlů může být poté zkoumána společně s časovou náročností této difúze do některé téměř dokončené fáze výpočtu, která vyhovuje zadaným parametrům. Výše uvedené skutečnosti vedou k otázkám, které lze spolu s využitím protokolu push-sum řešit. Jedná se o rychlost konvergence a počet iterací nutných k nalezení požadovaného stavu uniformního rozdělení, popřípadě konečného stavu uniformního rozdělení hodnot.

Díky popsaným vlastnostem protokolu lze vlastnosti šíření informací využít i v rozsáhlých distribuovaných prostředích. Může se jednat především o všesměrové šíření informací, popřípadě šíření informací do vybraných sítí, pomocí protokolu push-sum lze detekovat chybu v síti, synchronizovat uzly, sbírat vzorky dat, udržovat replikované informace, monitorovat konkrétní hodnoty v síti nebo protokol využít pro správu sítě.

Epidemicky se šířící protokoly mohou být obecně využity k řešení problému s agregací dat plně decentralizovaným způsobem. Na základě těchto protokolů také mohou být sestaveny aplikace pro dolování dat ve velmi rozsáhlých a dynamických decentralizovaných distribuovaných systémech. Z výše uvedeného je patrné, že využití decentralizovaného distribuovaného počtu má velmi velký potenciál pro implementaci v širokém spektru technologií. Tato práce se ale úzce specializuje na detekci poruchy v síti, které bude dále věnována.

Rychlost difúze

Rychlost difúze, je pojem, který vyjadřuje rychlost šíření proměnné v síti do všech uzlů. Lze ji chápat jako počet iterací protokolu potřebných ke kompletnímu uniformnímu rozdělení informace v celé síti. Rychlost difúze je ovlivněna složitostí a velikostí sítě, maximální chybou a maximální pravděpodobností, že aproximace v uzlu je větší, než maximální chyba [23].

Rychlost konvergence

V každém cyklu každý uzel odhaduje globální agregační funkci. Globální agregační funkce je definována jako výpočet kombinací mnoha rozdílných hodnot. Tato odhadovaná hodnota konverguje exponenciální rychlostí. Faktor konvergence je poté rychlost, s jakou lokální aproximace konverguje k cílové hodnotě. Pokud budeme

uvažovat, že se faktor konvergence pohybuje mezi cykly t až $t+1$, dosáhneme variačního rozpětí rovné $E(\sigma_{t+1}^2)/E(\sigma_t^2)$. Čím nižšího faktoru konvergence dosáhneme, tím rychleji bude síť konvergovat.

Agregace dat

V síti tvořící seskupení uzlů drží každý uzel lokální hodnotu x_i. Cílem agregační funkce je získat hodnotu globální agregační funkce $f()$, vyjádřené jako $f(x_0, x_1, \dots, x_{n-1})$. Získání globální agregační funkce může být docíleno více způsoby. Mezi nejpoužívanější způsoby se řadí součet, průměr, maximum, minimum, náhodný výběr, kvantita nebo agregační databázové fronty. Jako příklad bude vybrán typ agregace součet (sum). Ten může být orientován na centralizovaný součet a všechny jeho přírůstky musí být serializovány. Složitost agregace typu centralizovaného součtu je $O(N)$. Serializace je obecně proces konverze libovolně složitého objektu na lineární sekvenci bytů. Serializace tedy ve svém důsledku umožňuje uložení stavů uzlů do paměti a kdykoliv data zpětně deserializovat.

Dalším způsobem agregace je strategie rozděl a panuj, která využívá vlastností topologie stromu k získání globální proměnné. Důsledkem využití topologie stromu je redukce počtu kroků potřebných ke konvergenci sítě z $O(N)$ na $O(log(N))$.

Odolnost proti chybám

Distribuované protokoly založené na epidemickém šíření informace jsou známy svou odolností proti chybám. Zprávy v sítích využívajících tyto protokoly jsou doručovány s vysokou spolehlivostí a stabilní propustností navzdory vysokým ztrátám datových jednotek a vysoké pravděpodobnosti selhání procesu [27]. Jak dále uvádí autoři uvedeného článku, robustnost epidemicky šířících se algoritmů vychází z náhodného šíření informace, který rovněž umožňuje směrování zpráv o procesních i komunikačních chybách. Šíření zpráv protokolem probíhá rychle, spolehlivě a s vysokou pravděpodobností, stejně jako viry mezi lidmi. Ve smyslu záplavově se šířících algoritmů je robustnost definována jako schopnost odolat velkému počtu chyb. Robustnost protokolu je ale v přímém rozporu se škálovatelností sítě [28].

2.2.5 Bernoulliho distribuce

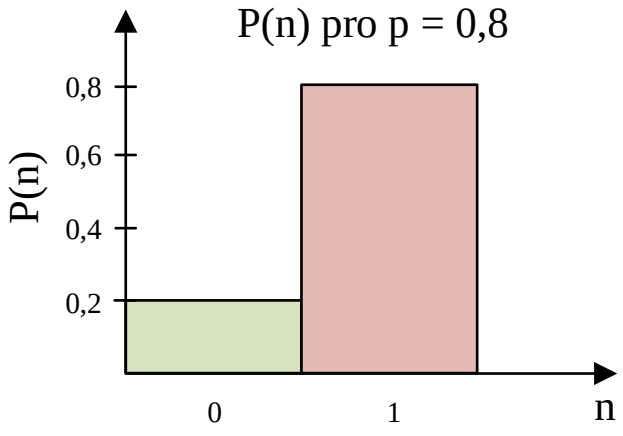
Bernoulliho distribuce je základním stavebním blokem ve statistice a může vyústit ve dva hraniční výsledky. Tyto výsledky lze klasifikovat jako úspěch definovaný proměnnou x = 1 a neúspěch definovaný proměnnou x = 0 [3]. Pravděpodobnost úspěchu je poté označována jako Bernoulliho parametr pravděpodobnosti p, který se pohybuje v rozmezí 0 < p < 1. Pravděpodobnost q je poté dána vztahem q = 1 - p. Bernoulliho náhodná proměnná X s pravděpodobností úspěchu p je dána funkcí:

$$f_{(x)} = p^x(1-p)^{1-x} \tag{8}$$

Odtud můžeme odvodit kumulativní distribuční funkci X(p):

$$F_{(x)} = P(X \leq x) = \begin{cases} 0 & pro\ x < 0 \\ 1-p & pro\ 0 \leq x < 1 \\ 1 & pro\ x \geq 1 \end{cases} \tag{9}$$

Podrobnějším matematickým důkazům jsou věnována publikace [4] a [5], kde je funkce pravděpodobnosti hustoty odvozena a popsána v kapitole 26. Názornou ukázku Bernoulliho rozdělení pravděpodobnosti lze vidět na obrázku Obrázek 11. Proměnná p zde byla zvolena jako hodnota o velikosti 0,8 a udává pravděpodobnost výskytu hodnoty 1 v systému.



Obrázek 11: Bernoulliho rozdělení pravděpodobnosti.

2.3 Senzorové sítě

Pokrok v konstrukci procesorů, pamětí a rádiových technologií umožnil zavádět do provozu malé a levné senzory, které jsou schopny komunikovat s okolím a provádět základní výpočetní operace. Sítě složené z takových zařízení mohou dosáhnout vzájemné spolupráce těchto senzorů a takto monitorovat své okolí [6]. Tato miniaturní zařízení sestavená z komponent určených k měření, zpracování dat a komunikačních rozhraní ovlivňují myšlenku realizace senzorových sítí [7]. Senzorové sítě spolupracující na měření nebo výpočtu určených parametrů jsou poté nazývány distribuovanými senzorovými sítěmi. Distribuované senzorové sítě se stávají dynamickými na základě možností průběžných změn topologie nebo nárůstu počtu zařízení v síti. Hlavní výhodou plynoucí z jednoduchosti senzorů je možnost jejich implementace v nehostinných částech prostředí, kde vyvstala potřeba měření některé z fyzikálních veličin. Vzhledem k jednoduchosti senzorů ale většinou vyplyne na povrch otázka zabezpečení sdílených dat především v senzorových sítích přenášejících citlivá data. Proto jsou v senzorové síti vyžadovány prvky kryptografické ochrany komunikace, detekce snímání senzorů, ochrany proti zachycení klíčů nebo deaktivaci senzorů [8].

Zařízení, která vzájemně v senzorové síti spolupracují, bývají označována jako uzly. Jsou určena k monitorování určité fyzikální jednotky. Bezdrátové senzorové sítě WSN jsou klasifikovány jako podmnožina typu sítí ad-hoc [9]. V této práci jich bude konkrétně využito pro monitorování hodnot určujících kvalitu příjmu signálu jejich a převodu na procentuální charakteristickou hodnou definující kvalitu příjmu signálu v souvislosti s interferencemi z okolí. Dalšími kritickými aspekty mnoha aplikací distribuovaných systémů v reálném životě jsou spotřebovaná energie a optimalizace [32].

2.3.1 Charakteristika bezdrátových senzorových sítí

Jelikož jsou sítě WSN (Wireless Sensor Networks) podmnožinou ad-hoc sítí, vlastnosti ad-hoc sítí přesně charakterizují i samotné WSN [9]. Základní charakteristiky WSN byly lehce předestřeny již v úvodu této kapitoly. V rámci WSN jsou uzly vždy elementárními zařízeními, která využívají pro komunikaci krátké zprávy sestávající

řádově z několika bajtů. Zprávy jsou zasílány na základě vnějšího podnětu, který můžeme definovat jako externí změnu událostí. Dalším podnětem pro zpracování informace mohou být požadavky sítě na odeslání informace mimo pravidelné časové intervaly, ve kterých jsou měřené hodnoty odesílány. WSN a sítě typu ad-hoc mohou mít společné protokoly, ale WSN jsou unikátní podskupinou ad-hoc sítí. V nasledujících podkapitolách se zaměříme na bližší charakteristiku základních vlastností WSN.

Odolnost vůči chybám

Chyby ve WSN většinou vznikají kvůli náročným podmínkám, do kterých jsou jejich jednotlivé uzly nasazovány. Mezi náročné podmínky lze zařadit vysoké či nízké teploty, klimatické změny, bouře, vlhko, elektromagnetické vlnění v případě nasazení ve zkušebnách a mnoho dalších specifických faktorů. Tyto negativní vlivy na zařízení mohou vést k poškozením hardwaru i softwaru a zvyšují nároky na jejich konstrukční robustnost. Vlivem některých z vyjmenovaných faktorů nebo jejich kombinací může být ovlivněna celková životnost nejen celého senzoru, ale i napájecích článků a komponent, ze kterých jsou sestaveny. Bezdrátové senzory navíc musí být vybaveny ochranou zabezpečující správné doručení dat skrze bezdrátové prostředí, přes které komunikují. Identifikace vzniklé chyby může být poté stěžejním faktorem při doručování dat do centrálního uzlu. Tato komplexita uzlů jde samozřejmě ruku v ruce s ekonomickou výhodností.

Cena zařízení

Cena zařízení je faktor ovlivňující především senzorové sítě sestávající z vysokého počtu uzlů. Vysoká hustota uzlů v síti vyžaduje co nejnižší pořizovací cenu každé jednotlivé komponenty. Jedním z cílů každého síťového architekta je snížení ceny každého implementovaného uzlu k hodnotám jednotek dolarů za kus.

Škálovatelnost

Bezdrátové senzorové sítě svou povahou vycházejí z požadavku na možnost rozšířit stávající síť o nové uzly ve svém blízkém či vzdálením okolí. Síť jako taková musí být schopná reagovat na náhlé změny topologie sítě nebo procesu v případě, že tato potřeba nastane.

Hardwarová konfigurace

Hardwarové vybavení uzlu musí splňovat kromě požadavků na správnost informace, její bezpečné přenesení a další vlastnosti také energetickou nenáročnost, maximální výpočetní kapacitu nebo možnosti komunikace ve více frekvenčních pásmech. Vzhledem k jejich konstrukční nenáročnosti se ale v drtivé většině volí kompromis mezi hardwarovými požadavky a cenou.

Přenosové médium

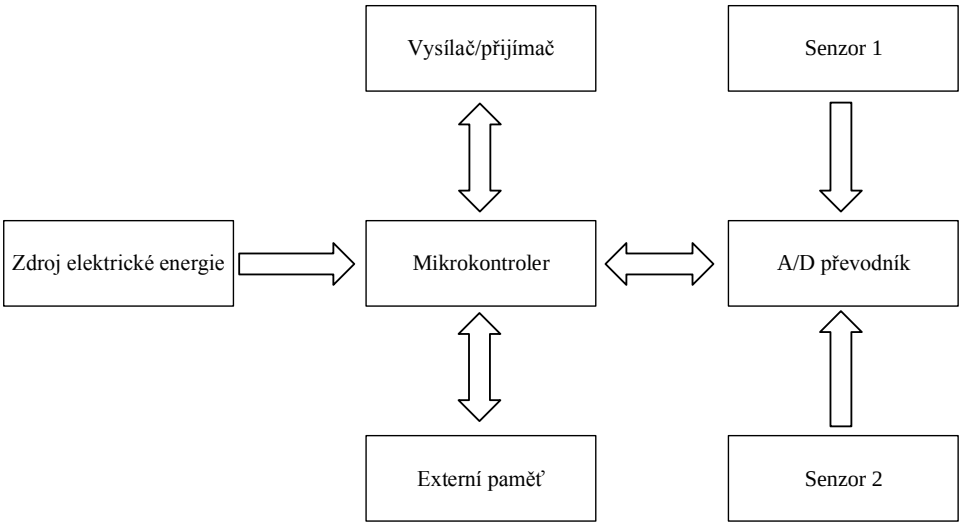
Již z názvu bezdrátová senzorová síť vyplývá požadavek na přenosové médium. Vzhledem k velkému počtu frekvencí určených ke specifickým účelům svázaných regulacemi příslušných úřadů jsou pro vzájemnou komunikaci jednotlivých uzlů voleny volné rádiové frekvence v rozsahu mezi 433 MHz až 2,4 GHz [9]. Méně často bývají přenosy informace uskutečněny pomocí infračerveného záření a jiných alternativ kvůli hardwarovým, ekonomickým i energetickým požadavkům.

Energetické požadavky

Spotřeba elektrické energie je velmi významným faktorem u WSN. V případě každého uzlu jsou definovány minimální energetické požadavky pro jeho správnou funkci. Tyto požadavky vycházejí často z lokace, ve které je senzor umístěn. Ne vždy může senzor dosáhnout na přímé napájení a bývá odkázán na kapacitu baterie. Z této kapacity musí být senzor schopen čerpat elektrickou energii co nejdéle. V nejlepším případě by měl úbytek elektrické energie jít ruku v ruce se životností článků baterie. Solární dobíjení nepřipadá v úvahu, pokud bychom chtěli splnit požadavek na nízkou cenu. Minimální spotřeba elektrické energie je tedy hlavní cestou, kterou se senzorové sítě ubírají.

2.3.2 Architektura senzorových sítí

Senzorové sítě mohou být složeny z více typů senzorů. Mezi nejčastěji využívané senzory patří tepelné, seismické, vlhkostní, pohybové, hlukové, světelné nebo například senzory měřící mechanické otřesy [10]. Za základní stavební prvek považujeme senzorový uzel sestavený z vysílače, přijímače, řídícího prvku, A/D převodníku, a zdroje energie, popřípadě také externí paměti, jak je znázorněno na obrázku Obrázek 12 [7].



Obrázek 12: Schéma senzorového uzlu

Mikrokontroler

Je základním stavebním prvkem a jádrem každého senzorového uzlu. Jeho úkolem je zejména zpracování vstupních dat přicházejících ze vstupů A/D převodníku, vysílače a přijímače a samozřejmě pokud je k tomu uzel přizpůsoben, tak ukládání dat do externí paměti. Každý mikrokontroler může být konstruován jinak, ale obecně vzato ho lze považovat za digitální prvek a jako takový zpracovává především digitální data. Častým požadavkem na jeho správné funkce je jeho programovatelnost. Mikrokontroler tedy bývá integrovaný obvod sestavený z výpočetní jednotky, vysokorychlostní sběrnice, RAM paměti, vstupně výstupního rozhraní, generátoru hodinového signálu, digitálních vstupů a výstupů a dalších sériových či paralelních rozhraní, která se mohou lišit dle výrobce. Správná volba tohoto zařízení může markantně ovlivnit nejen cenu, ale hlavně spotřebu celého senzorového uzlu.

A/D převodník

Slouží pro převod analogového signálu zachyceného senzorem na signál digitální pomocí vzorkování, kvantování a kódování. Základním požadavkem na převodník je tedy jeho schopnost transformace signálu spojitého v čase na signál diskrétní. Každý A/D převodník má ale svoje limity. Tím nejdůležitějším limitem je počet diskrétních hodnot, které je převodník schopen vzorkovat za jednotku času, tedy jeho vzorkovací frekvence, která musí splňovat Nyquistovu podmínku. Tato podmínka definuje pravidlo, které určuje vzorkovací frekvenci minimálně na dvojnásobek frekvence

vzorkované. Dalším limitním faktorem u senzorových sítí je poté rychlost kontroléru zpracovávajícího vstupní hodnoty z převodníku a také velikost paměti, do které jsou naměřená data ukládána [11].

Zdroj elektrické energie

Při vytváření architektury distribuovaných senzorových systémů se stává stále častěji diskutovaným tématem spotřeba elektrické energie jednotlivých senzorových uzlů. Limitovaná energetická zásoba s sebou přináší nutnost řešení spotřeby jednotlivých komponent uzlu, ale také požadavek na výměnu zásobárny elektrické energie, tedy baterií. Architekti senzorových sítí se v takových případech často potýkají s energetickou efektivností uzlů. Tento aspekt často proniká do roviny hardwarové i softwarové. Změna provedená na fyzické vrstvě senzoru tedy ovlivní spotřebu celého zařízení a návrh protokolů vyšších vrstev [12]. Energetická spotřeba mikrokontrolerů založených na procesorech CMOS E_{CMOS} je primárně složena z energie potřebné pro přepínání E_P a energie uniklé E_U [13]. Celý vzorec lze vyjádřit jako:

$$E_{CMOS} = E_P + E_U = C_{CK} \times V_{NAP}^2 + V_{NAP} \times I_{ZTR} \times \Delta_t \qquad (10)$$

Kde C_{CK} je součet přepínacích kapacit způsobených výpočtem, V_{NAP} je napájecí napětí, I_{ZTR} je uniklý proud a Δ_t je délka trvání výpočtu. Energie potřebná pro přepínání CMOS čipu je stále dominantní složkou celkové spotřeby energie procesoru. Do budoucna se však počítá s faktem, že se spotřebovaná úroveň energie spínání sníží na úroveň energie uniklé [14].

Externí paměť

Malá senzorová zařízení bývají velmi často omezena dostupnými úložnými a paměťovými kapacitami. Běžně dostupná zařízení mívají paměť RAM a ROM pouze v desítkách kilobytů a podobně je to i s flash pamětí zastoupenou nejčastěji EEPROM pamětí sloužící k ukládání programových instrukcí, dočasných naměřených dat a dalších informací. Tato hardwarová omezení vedou především k rozvoji a optimalizaci zabezpečovacích algoritmů, které jsou nenáročné na alokaci paměti sloužící pro jejich správnou funkci. V případě, že není alokován dostatečný prostor pro všechny procesy spojené se správnou funkcí senzoru, je implementace složitějších algoritmů do senzorového uzlu neuskutečnitelná. Maximální paměť se ale vždy odvíjí

od ceny, požadavků na fyzickou velikost a spotřebu každého jednotlivého typu senzorového uzlu.

Vysílač, přijímač a přenos komunikačním kanálem

Základním komponentem digitálního systému jsou vysílače a přijímače, které jsou úzce spjaty s komunikačním kanálem. Komunikační kanál je fyzické médium, které je použito k přenosu užitečného signálu z vysílače na přijímač. V případě bezdrátové komunikace je za komunikační kanál považováno volné prostředí. Během přenosu signálu volným prostředím je ale z pravidla signál deformován či narušen například jinými zařízeními produkujícími elektromagnetické vlnění, odrazy signálu a dalším nespočtem rušivých elementů, které nás obklopují. Z těchto důvodů jsou v přijímači a vysílači obsaženy další funkční bloky a implementovány procesy, které slouží k eliminaci ruchů deformujících užitečný signál [15][16].

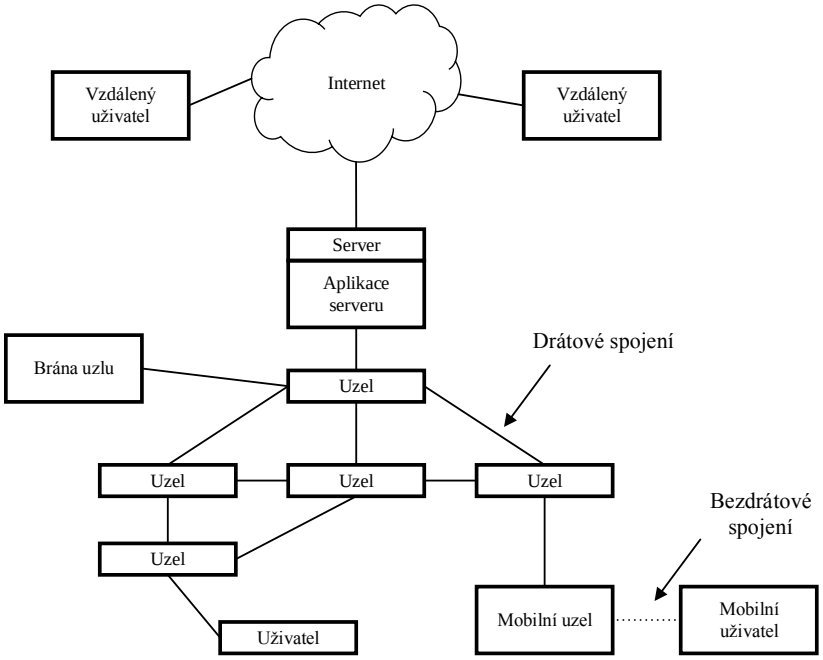
Senzor

Snímání je technika používaná pro získávání informací o fyzickém objektu, svém okolí nebo procesu měnícím hodnotu fyzikální veličiny. Za změnu hodnoty fyzikální veličiny můžeme považovat snížení či zvýšení atmosférického tlaku, teploty sluneční intenzity a mnoho dalších měřitelných faktorů. Předmět provádějící takové měření je poté nazýván senzorem. Z technického hlediska lze rozdělit senzory na dvě skupiny. Senzory určené pro dálkové měření a senzory určené k přímemu kontaktu s měřeným objektem. Oba typy měření mají za cíl převést fyzikální veličinu na signál, který je možné měřit a zpracovávat. Jiným názvem pro senzor je převodník. Pojem převodník je často užíván pro zařízení, která konvertují energii jednoho typu na jiný. Například tepelnou energii na elektrickou. Výstupy takto získané senzorem jsou následně zpracovávány dalšími bloky senzorového uzlu, kterými mohou být filtry použité pro odstranění nechtěného signálu, A/D převodníky sloužící pro převod spojitého signálu na diskrétní a další. Výsledná zpracovaná digitální data jsou předána procesoru a následně je s nimi nakládáno dle požadavků zadavatele.

2.3.3 Integrované bezdrátové senzorové uzly

Bezdrátové integrované senzorové uzly WINS poskytují senzorům možnosti využití distribuovaných sítí, přístupu k internetu a řízení a svým rozsahem využití pro

venkovní využití, implementaci v továrnách, či v jiném vybavení sítě jsou často pro tyto účely aplikovány. Jejich využitelnost spadá do oblastí transportu, výroby, zdravotní péče monitoringu prostředí nebo bezpečnostních technologií. WINS jsou kombinací mikrosenzorové technologie, nízkoenergetického výpočetního zařízení, s možností bezdrátového i drátového připojení při nízkých pořizovacích nákladech. Struktura sítě WINS je naznačena na obrázku Obrázek 13: Struktura sítě WINS [60].



Obrázek 13: Struktura sítě WINS

Jak je patrné z výše zveřejněných poznatků, sítě WINS jsou díky svým vlastnostem stále častěji implementovány do rozličných systémů, jako jsou aktuátory, identifikátory událostí nebo komunikační systémy s nízkou spotřebou elektrické energie. Podrobnější informace o senzorových sítích jsou uvedeny v [61] a [62].

2.4 Interference v bezdrátových sítích

Každý den v našem životě používáme komunikační technologie, které mohou využívat rozličné způsoby přenosu dat volným prostředím. Volné prostředí se již díky širokému spektru využití stalo jakýmsi typem obchodovatelné vyčerpatelné komodity regulované příslušnými regulačními orgány jednotlivých zemí. Regulační úřady všech zemí si skutečnost vyčerpatelnosti frekvenčních pásem uvědomují a jejich využívání

regulují, spravují a zajišťují výhradní využití společnostmi, které si tato frekvenční pásma zakoupí či si pronajímají licenci pro provozování komunikačních služeb v daném frekvenčním pásmu.

V systému přidělování frekvencí se ovšem mohou vyskytnout nestandardní situace. Jednou z nich jsou interference mezi přidělovanými pásmy. I když regulační úřad garantuje šířku přiděleného pásma frekvencí, interference v hraničních oblastech frekvenčních pásem vznikat mohou.

Problém interferencí v kmitočtovém spektru se nevyhnul České republice ani oststním státům. V České republice se při aplikaci sítí 4G LTE problém s interferencí projevil především u poskytování digitálního pozemního vysílání DVB-T, které je na území České republiky provozováno jako bezplatná služba.

Následující kapitoly proto budou věnovány analýze problému interference frekvenčních pásem na základě volně přístupných dat Českého telekomunikačního úřadu (ČTÚ), která jsou v rámci projektu Otevřená data (OpenData) dostupná pro laickou i odbornou veřejnost. Následující kapitoly rozšiřují povědomí o problému interferencí, které se dotýkají i ostatních zemí Evropy či některých států v USA. Důvod, proč jsou analyzovány podobné problémy v USA, je dán především podobnou povahou projevu interferencí vycházející z implementace nových sítí LTE do volného prostředí. Zde další koexistence bezdrátových systémů způsobuje útlum či úplné rušení přenosu informací mezi některými frekvenčními pásmy technologie LTE a satelitního rádia [57].

Způsob měření interferencí mezi vysílači DVB-t a LTE je v České je možné využít jako příklad pro další analýzy problému. V České republice je pro televizní digitální pozemní vysílání v současnosti používána varianta C2. Signifikantními parametry varianty C2 jsou počet nosných frekvencí OFDM stanovený na 8k, modulace 64QAM s kódovým poměrem 2/3, stupeň protichybové ochrany RS kód (188, 204, 8), ochranný interval ¼ sloužící především k eliminaci vícecestného šíření signálu a užitečný přenosový tok varianty C2 je 19,91 Mbit/s. Při měření úrovně užitečného signálu jsou v České republice sledovány parametry dané normou ČSN EN 60728-1. Pokud je ČTK doručen podnět k šetření kvůli rušení mezi blokem LTE a DVB-T, je tento podnět posuzován na základě parametrů uvedených níže.

Měřené parametry v LTE:

- Úroveň signálu - vztaženo k výkonu signálu v celém frekvenčním pásmu.
- Spektrum signálu - tvorba intermodulačních produktů a blokování.

Měřené parametry v DVB-T:

- Úroveň signálů jednotlivých přijímaných kanálů DVB-T.
- Subjektivní hodnocení kvality signálu DVB-T.
- CBER - chybovost měřená před dekodérem Viterbi.
- VBER - chybovost měřená před dekodérem Reed - Solomon.
- MER (Modulation Error Ratio).
- Odstup úrovní šumu nebo rušících signálů od úrovně užitečného signálu.
- Ochranný poměr (PR – Protection Ratio) - rozdíl mezi užitečným a rušícím signálem.
- Práh přebuzení (Oth – Overloading treshold).

Ochranný poměr a práh přebuzení jsou klíčovými parametry při měření interferencí mezi LTE a DVB-T. Oba měřené parametry jsou obvykle vyjadřovány v grafech vzhledem ke kmitočtovému vyvážení neboli ofsetu. Typické grafické vyjádření pro rok 2016 lze nalézt v dokumentaci pro ČTU v dokumentu [58], který vzniká na základě na hlášení poruch od uživatelů sítě.

2.4.1 Vznik interferencí

Digitální přenosy televizního signálu DVB-T se staly v mnoha zemích samozřejmostí. Místní autority alokují pro přenosy signálu určená pásma nazývaná též digitální dividendy. Frekvence vyčleněné pro přenosy určené pro mobilní komunikace se ve většině zemí pohybují mezi 790 MHz až 862 MHz [43]. Alokace zdrojů pro tyto frekvence začala již před rokem 2015. S vyhrazením zdrojů se objevil nový náhled na koexistenční problémy skrze sousední státy využívající toto spektrum. Mezi nové výzvy k řešení patří především tyto:

- Interference mezi kanály sousedících regionů či zemí využívajících stejné frekvence pro různé účely. Jeden region pro analogové přenosy, jiný pro digitální přenosy médií.
- Vzájemné rušení kanálů blízkých kmitočtu 790 MHz v rámci jedné geografické oblasti. Nejčastěji mobilní datová síť využívaná pod tímto frekvenčním limitem a pozemní televizní vysílání využívající frekvence nad tímto limitem.
- Mezikanálová interference v rámci dané geografické oblasti pro jednu digitální dividendu mezi DVB-C2 a mobilními systémy [44].

Teoretickým analýzám mezikanálových interferencí je věnováno několik publikací. Jako příklad lze uvést článek [45], ve kterém jsou tyto poruchy analyzovány pomocí adaptivní detekce a jsou zde diskutovány metody potlačení vlivu interferencí. Jak uvádí autoři v článku [46] a také autor habilitační práce v [47], standardy a požadavky na přenos napříč technologiemi GSM, LTE a DVB-T/H, se stále zvyšují. Kvůli postupnému překrývání frekvencí GSM, LTE a DVB- T/H je nutné využívat samoopravných kódů a dalších technik sloužících pro detekci chyb při přenosech užitečné informace. Autoři obou publikací prováděli simulace interferencí mezi výše uvedenými mechanismy přenosu s výsledky, které potvrzují teoretické předpoklady i pro technologii WiMAX pracující na frekvencích stejného rozsahu. Autoři zavedením bílého Gaussova šumu AWGN simulovali co nejvěrohodněji situaci pro SNR, ke které v praxi dochází nejčastěji.

Stejně tak jako v České republice a USA byly zaznamenány interference na frekvencích vyčleněných pro přenos DVB-T jiných částech Evropy. Autoři článku [48] uvádějí, že se zde například akvizice Chorvatsku pro frekvence 790MHz až 862 MHz dotkne kanálů 61 až 69. Okolní státy přitom stále využívají kanál 60 pro všesměrové šíření televizního signálu a je velmi pravděpodobné, že dojde k problémům s interferencemi. V USA se problém interferencí vyskytl mezi satelitním rádiem SiriusXM a sítí LTE. Zde stále probíhají modifikace sítě vedoucí k nápravě [59].

2.4.2 Ochrana kanálu DVB-T

Ochrana před rušením kanálů DVB-T vychází z předpokladu, že budou všechny

dotčené technologie maximálně přizpůsobovat své parametry tak, aby jejich vzájemná koexistence neznamenala omezení dodávaných služeb ani na jedné straně. Při nasazování technologií spojených s frekvencemi 790MHz až 862 MHz tedy musí dojít nejprve k plánování rozvoje sítě a simulacím ukazujícím co nejpřesnější údaje o možných rizicích vzájemného rušení. Pro plánování sítí jsou stěžejní dva parametry. Prvním z nich je minimální pole využití MUF dané jako $F_{k,min}$ (dB(μV/m)) a minimální odstup signálu od interference nazývaný též ochranný faktor PR udáván jako C/I (dB). Tyto parametry a jejich úrovně jsou blíže specifikovány v [49]. Tyto faktory jsou stěžejní pro správný příjem signálu od vysílače. Příjem signálu je možný, pokud je MUF nad úrovní interferencí. V případě nedodržení jedné z podmínek degraduje obraz na přijímači velmi rychle.

DVB-T technologie využívá pro přenosy signálu modulaci COFDM [50]. Pro tuto modulaci jsou stěžejní dva parametry. Prvním z nich je kódová rychlost a ochranný interval. Tyto dva parametry jsou souhrnně nazývány též systémové varianty [48].

Každá systémová varianta má svůj ochranný koeficient, minimální využitelnou sílu signálu a maximální datový limit. Aby bylo dosaženo robustnosti signálu při přenosu, nejsou využívány maximální hodnoty těchto proměnných. Ochranný koeficient potřebuje úroveň přijatého užitečného signálu vyšší, než 90% [51].

2.4.3 Koordinace interferencí v sítích LTE

V heterogenních sítích s expanzí dosahu je nutné, aby uživatelské zařízení využívající technologii LTE nebylo odpojeno od základnové stanice ani při nízkém odstupu užitečného signálu od součtu nežádoucích šumových složek signálů ostatních základnových stanic, či jiných technologií využívajících blízká frekvenční pásma. Bezdrátové buňkové sítě jsou obvykle tvořeny jako homogenní sítě využívající makrocentricky plánované procesy **Chyba! Nenalezen zdroj odkazů.**. Základnová tanice využitá pro komunikaci mezi uživatelským zařízením musí kooperovat s ostatními základnovými stanicemi tak, aby nedocházelo k interferencím s dominantními složkami spektra. Pro uživatelská zařízení, která jsou blízko k elementům vytvářejícím interferenční složky signálu je v takovém případě velmi složité sestavit spolehlivý komunikační kanál. Oproti homogenním sítím, ve kterých je

opětovné využití zdrojů možné, je ale v heterogenních sítích dobré přenosové schéma důležitým aspektem zvládnutí interferencí vznikajících mezi buňkami sítě.

Mezibuňková koordinace ICIC je tedy kritická pro sestavení heterogenní sítě a je využívána pro úpravu vysílacího výkonu nebo případně náklonu vysílacích antén. Dalším způsobem úpravy vysílacího signálu v síti složené z blízkých základnových stanic je úprava časové, frekvenční či prostorové domény. Rozprostření časové domény je v takovém případě nejčastějším jevem pro adaptaci spektra. Frekvenční rozprostření domény nenabízí tak jemné rozprostření, jako tomu je u časového rozprostření hlavně u asynchronních typů sítí. Prostorové rozprostření domény podporované standardem CoMP je v případě technologie LTE-A využíván jako prostředek k vylepšení přenosových kapacit sítě, propustnosti sítě na okrajích buněk nebo propustnosti při vysokém i nízkém provozu v síti [54][55].

Jiným způsobem koordinace interferencí v rámci sítě buněk LTE je pomalá adaptace řízení interferencí. Pomocí této metody jsou alokovány zdroje v časových intervalech. Cílem pomalu adaptivního algoritmu pro koordinaci zdrojů je najít optimální kombinaci vysílacích výkonů mezi základnovými stanicemi a uživatelskými terminály a tím maximalizovat celkovou využitelnost zdrojů sítě. Jeho prostředky pro adaptaci sítě jsou například úprava uživatelských rychlostí stahování i nahrávání, úprava toků dat QoS nebo úprava metriky. Uvedený algoritmus je většinou zpracováván v centrální jednotce, která má přístup ke všem afektovaným základnovým stanicím. Centrální jednotka ale nemusí být přístupná pro všechny základnové stanice v síti z důvodů omezení šířky pásma, výpočetní komplexity algoritmu nebo zpoždění. Výsledkem tohoto chování je, že distribuovaný algoritmus provádějící rozhodnutí o komunikaci mezi entitami sítě pracuje pouze s některými jejími podmnožinami. Koordinaci mezi jednotlivými podmnožinami je poté možné provádět s využitím páteřní sítě [56].

2.4.4 Parametr síly přijatého signálu

Při procesu plánování rozvinutí technologie DVB-T v geografické oblasti je stěžejní určit minimální sílu elektrického pole E (dBV/m). Množství elektromagnetického toku procházející jednotkou plochy zde definujeme jako B

[Wb/m^2]. Dostupný přijatý výkon označený jako P_r je poté produkt přijímací části antény A_{ef}. Dostupný přijatý výkon lze poté vyjádřit jako:

$$P_r = B \times A_{ef} = \left(\frac{E^2}{\eta}\right) \times \left(G_r \frac{\lambda^2}{4\pi}\right) = \frac{G_r c^2 E^2}{4\pi\eta f^2} \qquad (11)$$

Kde η je vnitřní impedance volného prostoru rovna 377Ω, G_r [dBi] je zisk přijímací antény, f [Hz] je frekvence signálu, c [m/s] je rychlost světla a λ [m] je vlnová délka. Aby bylo možné vyhnout se interferencím, musí být opět splněna podmínka, že odstup užitečného signálu od interferenční složky musí být větší nebo roven hodnotě P_r.

$$P_r \geq \frac{P_{r,DVB-T}}{P_{r,interference}} \qquad (12)$$

Kde $P_{r,DVB-T}$ [mW] je síla signálu obdržená televisním přijímačem a $P_{r,interference}$ [mW] je síla všech signálů obdržených na přijímací anténě, v našem případě i složky signálů LTE a GSM. P_r je tedy bezrozměrná jednotka [52]. Logaritmické vyjádření rovnice je dále publikováno v [53].

3 KOMPARACE STATISTICKÉ KREDIBILITY REPREZENTANTA PRŮMĚRNÉ RYCHLOSTI KONVERGENCE PROTOKOLU PUSH-SUM

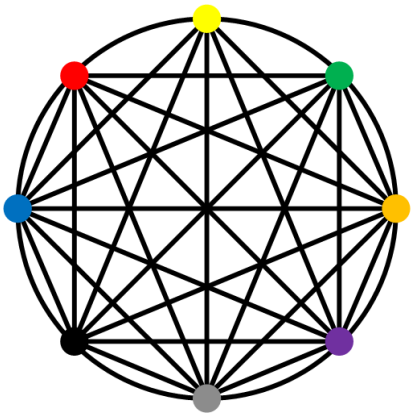
V rámci dizertační práce je vzájemně komparována statistická kredibilita reprezentanta průměrné rychlosti konvergence protokolu push-sum. Komparace je provedena z důvodu zjištění vhodnosti protokolu k vlastní implementaci a modelování navrženého řešení.

3.1 Analýza problému

Cílem analýzy je ukázat, jaký vliv má narůstající počet opakování provedení push-sum protokolu na statistickou kredibilitu reprezentanta rychlosti konvergence. Tato rychlost se mění pro různé běhy protokolu i při zachování stavu a váhy uzlů, topologie a dalších počátečních parametrů. Zmíněný jev je zapříčiněn stochastickými vlastnostmi push-sum protokolu. Proto byl tento protokol zvolen pro ověření statistické kredibility reprezentanta rychlosti konvergence. Nejprve je pro analýzu problému zvolena topologie linky představující velmi slabě propojenou síť uzlů. Nástin topologie je uveden na obrázku Obrázek 14.

Obrázek 14: Slabě propojená síť.

Silně propojenou síť v našem případě reprezentuje plně propojená síť, jak je znázorněno na obrázku Obrázek 15. Obě tyto sítě sestávají z osmi uzlů nazývaných též agenty. Počet osmi uzlů je zvolen pro simulaci z důvodu přehlednějšího modelu, ve kterém vynikne vzájemné propojení agentů.



Obrázek 15: Plně propojená síť.

U topologie se slabým propojením uzlů byla předpokládána její pomalejší konvergence oproti silně propojené topologii a to z důvodu horší dostupnosti uzlů. Ve struktuře sítě typu linka je rychlost šíření zprávy obecně vázána na skutečnost menšího počtu spojení. Silně propojená topologie je podle charakteru propojení uzlů volena jako varianta maximálního možného počtu spojení mezi uzly, tedy každý s každým. Zde je simulace orientována na předpoklad rychlého šíření informace a předpoklad rychlosti konvergence je opačný oproti slabě propojené topologii.

V obou topologiích je při stejném počtu opakování realizováno pět simulací průběhů. Z výsledků dosáhnutých v rámci jednoho průběhu je vypočítán průměr, tedy reprezentant rychlosti konvergence a porovnán s průměry získanými v rámci dalších průběhů. Statistická kredibilita je ověřena vypočítáním variačního rozpětí získaných průměrů. Vykonáno je pět scénářů – 10, 100, 1 000, 10 000 a 100 000 opakování pro oba typy topologií. Výsledky jsou porovnány v rámci jednotlivých scénářů a také mezi rozličnými typy topologií.

3.2 Model rychlosti konvergence ve slabě propojené topologii

V následující části jsou zobrazeny rychlosti konvergence ve slabě propojené topologii reprezentované topologií linky o rozměru osmi uzlů. Simulace byla provedena s pomocí protokolu push-sum. Pro větší přehlednost jsou výsledky uvedeny

v tabulce Tabulka 1. Následné grafické zpracování výsledků je uvedeno v příloze. Variační rozpětí bylo vypočteno jako rozdíl mezi největším a nejmenším prvkem z množiny naměřených hodnot. Z výsledků můžeme pozorovat skutečnost, že s narůstajícím počtem opakování se variační rozpětí opět zmenšuje.

Tabulka 1: Hodnoty variačního rozpětí pro slabě propojené topologie.

Počet opakování [-]	10	100	1 000	10 000	100 000
Běh 1 [-]	202,1	207,2	205,298	205,7752	205,6805
Běh 2 [-]	203,7	204,29	205,263	205,7373	205,619
Běh 3 [-]	204,1	207,34	205,165	205,5086	205,6778
Běh 4 [-]	200,5	204,1	205,646	205,711	205,6724
Běh 5 [-]	214,2	207,59	206,677	205,7225	205,6736
Variační rozpětí[-]	13,7	3,49	1,512	0,2666	0,0615

3.3 Model rychlosti konvergence v silně propojené topologii

V této části jsou zobrazeny rychlosti konvergence v silně propojené topologii reprezentované plně propojenou topologií o rozměru osmi uzlů. Testování uvedené topologie přineslo výsledky uvedené v tabulce Tabulka 2. Dle předchozích teoretických předpokladů bylo dokázáno, že čím více bude struktura sítě vzájemně provázána, tím lepší konvergence bude síť dosahovat. Rychlá konvergence je v případě následných metod využívaných v této práci stěžejním faktorem. Pokud by byla simulovaná síť uzlů velmi rozsáhlá, nebyl by zaručen správný odhad hodnoty průměru, protože by protokol push-sum ukončil v daném čase výpočet dříve, než se předpokládalo. Nebylo by tedy dosaženo dostatečného počtu iterací k dosažení přesnějšího výsledku.

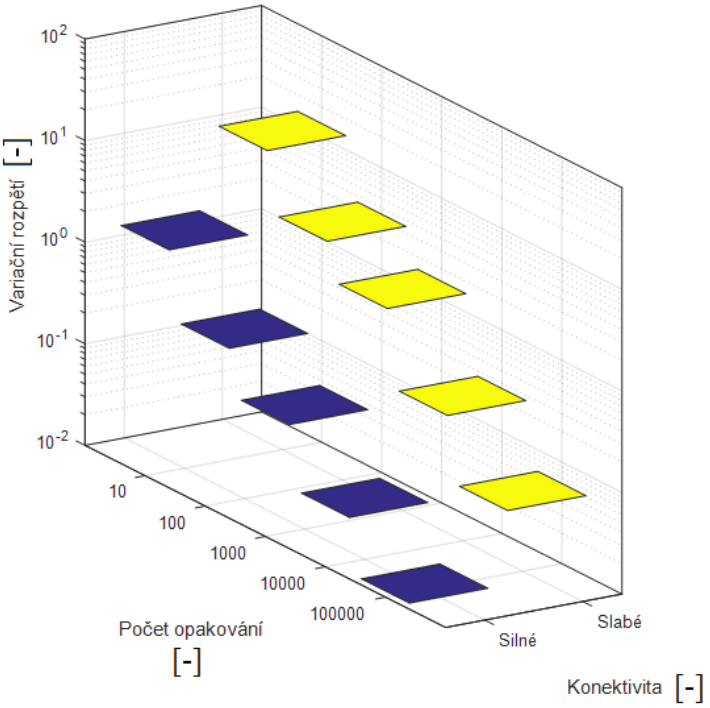
Tabulka 2: Hodnoty variačního rozpětí pro silně propojené topologie.

Počet opakování [-]	10	100	1 000	10 000	100 000
Běh 1 [-]	22,3	24,02	23,843	23,8121	23,816
Běh 2 [-]	24,2	24,11	23,765	23,8098	23,8098
Běh 3 [-]	24	23,81	23,797	23,8339	23,814
Běh 4 [-]	23,8	24,28	23,841	23,8021	23,8213
Běh 5 [-]	24,5	23,82	23,677	23,7936	23,8125
Variační rozpětí [-]	2,2	0,47	0,166	0,0403	0,0115

Variační rozpětí bylo opět vypočteno jako rozdíl mezi největším a nejmenším prvkem z množiny naměřených hodnot. Z výsledků můžeme opět pozorovat skutečnost, že s narůstajícím počtem opakování se variační rozpětí zmenšuje. Grafické znázornění situace je uvedeno v příloze A2.

3.4 Rozbor výsledů měření rychlosti konvergence v silně a slabě propojené topologii

Aby bylo dosaženo transparentního srovnání dosažených výsledků ze simulace obou topologií, je v následujícím textu a obrázku Obrázek 16 jejich komparace uvedena. Z výsledků můžeme vidět, že se variační rozpětí zmenšuje s narůstajícím počtem opakování v obou typech topologií. Z výsledků můžeme dále pozorovat, že v silně propojené topologii bylo zaznamenáno menší rozpětí pro stejný počet opakování. Z dosáhnutých výsledků vyplývá, že vyšší statistické kredibility reprezentanta rychlosti konvergence je možné dosáhnout větším počtem opakování.



Obrázek 16: Vzájemná komparace dosažených výsledků.

V rámci této analýzy byla ověřena vhodnost využití stochastického distribuovaného protokolu push-sum pro implementaci do senzorových sítí. Stochastičnost zmíněného protokolu spočívá v náhodném výběru přilehlého souseda podle rovnoměrného rozdělení, což má za následek, že se některé parametry i při zachování stejných podmínek liší při opakovaném zpracování tímto protokolem. Jedním z těchto parametrů byla rychlost konvergence. V rámci přípravy na návrh nové metody detekce poruchy v síti dále probíhá zkoumání vlivu počtu opakování protokolu push-sum na statistickou kredibilitu reprezentanta rychlostí konvergence. V našem případě byl jako reprezentant zvolen aritmetický průměr, jelikož má sledovaný fenomén normální rozdělení pravděpodobnosti. Simulace byly vykonány pro 5 různých scénářů, které se od sebe lišily v počtu opakování. Zkoumána byla statistická kredibilita reprezentanta pro velikosti 10, 100, 1000, 10 000 a 100 000 opakování. Tyto scénáře byly vykonány pro 5 rozličných běhů, ze kterých byla určena průměrná hodnota. Jako indikátor statistické kredibility byl zvolen parametr statistické rozpětí. Jeho nižší hodnota představuje vyšší statistickou kredibilitu. Simulace byly vykonány pro dva typy topologií: Silně a slabě konektovanou. Jako reprezentant silně konektované struktury byla zvolena plně

konektovaná mřížka a jako reprezentant slabě konektované topologie byl vybrána topologie linka. Obě tyto topologie měly stejné počáteční podmínky a velikost. Z dosáhnutých výsledků můžeme pozorovat, že větší počet opakování zabezpečí vyšší kredibilitu reprezentantů rychlostí konvergence. Charakter sledovaného fenoménu byl stejný pro oba typy sledovaných topologií.

4 VLIV ZTRÁTY ZPRÁVY NA ZVOLENÉ TOPOLOGIE V SÍTÍCH VYUŽÍVAJÍCÍCH PUSH-SUM PROTOKOL

Ztráta zprávy při konvergenci distribuovaného stochastického algoritmu může vést ke zkreslení celkového výsledku. Z povahy zvoleného algoritmu ale vyplývá, že by měl být dostatečně robustní a náhodné chyby vzniklé při prováděném výpočtu by neměly do jisté míry ovlivnit finální výsledek. Pokud by se předpoklad robustnosti zvoleného algoritmu push-sum nepotvrdil, nemohl by být dále využíván pro detekování poruchy v síti, protože by při ztrátě zprávy při jejím šíření mohl způsobit zkreslení výsledku a následně chybnou detekci v podsíti, ve které ve skutečnosti k žádné poruše ve smyslu obdrženého chybového hlášení ze senzoru nedochází.

4.1 Analýza problému

Tato kapitola má za cíl ukázat vliv ztráty zpráv v sítích využívajících push-sum protokol na jeho přirozenou robustnost. Analyticky je v ní ověřen následek vzniku chyby na charakter odhadu, odchylku od konečného odhadu od reálné hodnoty a dopad na změnu míry konvergence. Vycházeno je přitom z předpokladu, že je push-sum protokol uplatněn pro odhad průměrné hodnoty všech hodnot původních. Analýza vychází z teze, že každý uzel udržuje v paměti dva parametry:

- Aktuální hodnotu vnitřního stavu.
- Aktuální váhu uzlu.

Aktuální hodnotou vnitřního stavu uzlu může myšlena hodnota obdržená například měřením fyzikální veličiny. Fyzikální veličinou může být v této aplikaci výstup senzoru připojeného k vysílači v numerické hodnotě. Aktuální váha je pro tuto simulaci nastavována na hodnotu 1 pro počáteční stav všech uzlů.

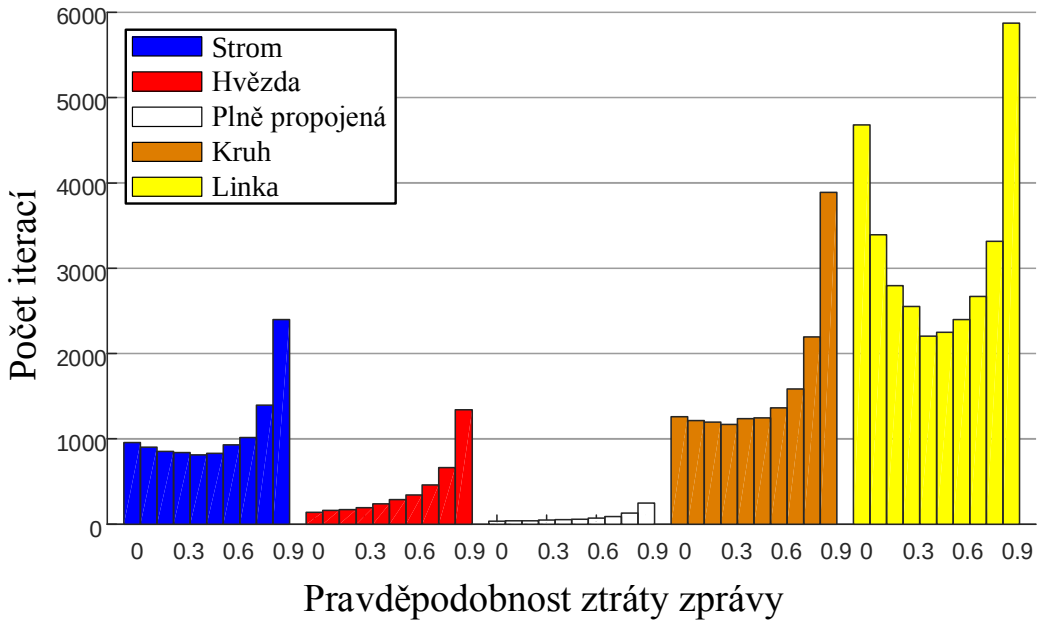
Jak již bylo zmíněno dříve, protokol push-sum pracuje iterativním způsobem. Každý uzel v síti si vybere jednoho ze svých sousedů a pošle mu poloviční hodnotu svého stavu a poloviční hodnotu své aktuální váhy v každé iteraci. Stejnou hodnotu si také uloží do své vnitřní paměti. Dalším krokem každého uzlu bude výpočet všech vnitřních stavů a vah a určení odhadu průměru iterace. Průměr iterace bude vypočten jako poměr hodnoty aktuálního vnitřního stavu a váhy entity. Tento postup bude aplikován na celou síť, dokud nebude dosaženo konsensu v systému.

4.2 Výsledky simulace

V této sekci práce jsou prezentovány výsledky získané během numerické simulace v programu Matlab. Hlavní pozornost byla věnována ověření robustnosti protokolu push-sum při ztrátě zpráv v některé z iterací. Simulací je ověřena odchylka konečného odhadu od reálné hodnoty průměru, změna charakteru odhadu způsobená odchýlením některé z hodnot a změna počtu iterací nezbytných pro dokončení výpočtu pomocí protokolu push-sum při vzniklých odchylkách. Simulace je vykonána v pěti známých statických topologiích popsaných v teoretické sekci. Jedná se o topologie stromu, hvězdy, plně propojenou topologii, kruh a linku. Všechny topologie jsou tvořeny 32 uzly. Ztráty zpráv jsou modelovány pomocí Bernoulliho distribuce. Bernoulliho distribuce určuje pravděpodobnost výskytu ztráty zprávy p. Pravděpodobnost ztráty zprávy je v simulaci udávána vzestupnými hodnotami od nuly po desetinách, tedy 0, 0,1, atd. až do hodnoty 0,9. Úplná ztráta informace daná hodnotou 1 není uvažována. Pravděpodobnost úspěchu doručení zprávy je poté dána jako $1 - p$. V první části pokusu je práce zaměřena na simulaci ukazující, jak ztráta zprávy ovlivní charakter odhadu. Výsledky simulace jsou znázorněny ve třech grafech pro každou ze zvolených topologií. Každá topologie byla simulována pro tři scénáře, a sice pro pravděpodobnost ztráty zprávy rovnu p = 0, p = 0,5 a p=0,9. Výsledky lze pozorovat na obrázcích Obrázek 40, Obrázek 41, Obrázek 42, Obrázek 43 a Obrázek 44 v příloze A.3.

Jak můžeme pozorovat z uvedených obrázků, zvyšující se hodnota pravděpodobnosti p je příčinou rostoucí doby většiny odhadů.

V dalším textu je zkoumán vliv ztráty zprávy na míru konvergence v jednotlivých topologiích. Protože je protokol push-sum stochastickým algoritmem, je každá simulace opakována 100 krát a jako výsledek je poté brán pouze průměr těchto hodnot. Na obrázku Obrázek 17 je znázorněn počet iterací nezbytných pro dokončení běhu protokolu push-sum po změně p. Výsledky dokazují, že plně propojená síť vyžaduje ke své konvergenci nejmenší počet iterací. Naopak nejhorších výsledků bylo dosaženo u reprezentanta slabě propojené sítě a to u topologie linky.

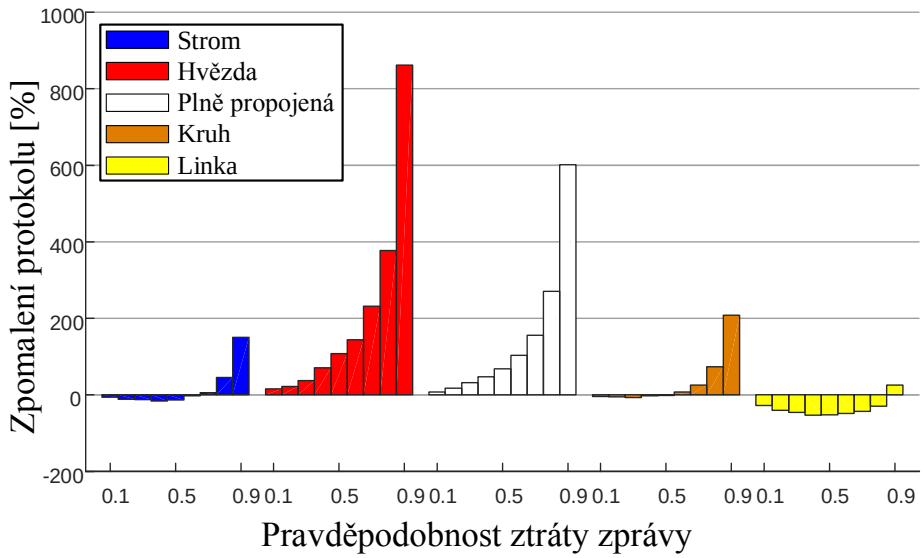


Obrázek 17: Vliv pravděpodobnosti ztráty zprávy na počet iterací.

Dalším výsledkem, který lze pozorovat z grafů je, že vyšší hodnota p má za následek vyšší počet iterací v plně propojené síti a také v topologii hvězdy. Oproti tomu v sítích zapojených do kruhu, stromu či linky jsou následky vyšší hodnoty p značně odlišné. V těchto slabě propojených sítích se na základě zvyšující se hodnoty p snižuje počet iterací. Pro p = 0,4 dosahuje graf minima a poté počet iterací zase stoupá. Z výsledků lze tedy odvodit, že u slabě propojených topologií ztráta zprávy urychlí výpočetní proces.

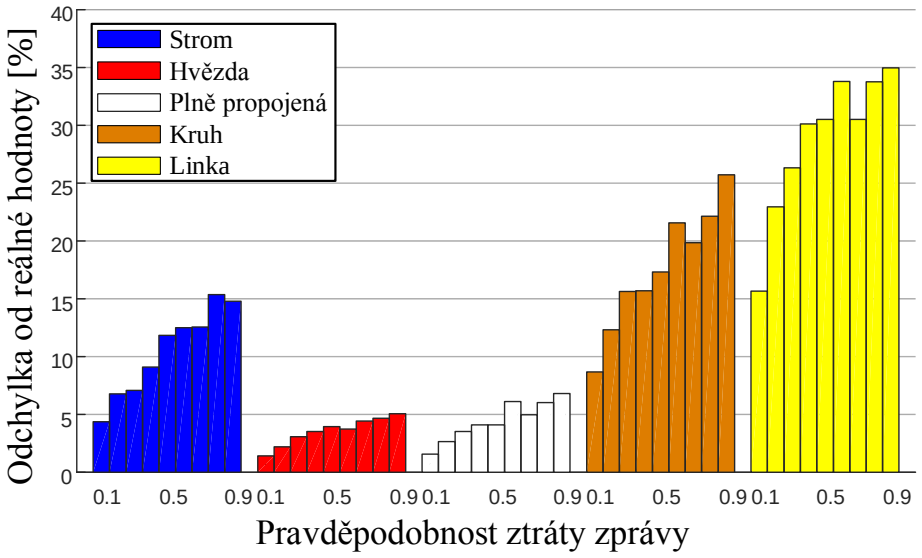
Obrázek 18 ukazuje relativní zpomalení procesu využitého protokolu push-sum.

Záporné hodnoty indikují jeho zrychlení. Jak je z grafu patrno, ztráta zprávy má nejmenší negativní dopad na topologie, které vyžadují vysoký počet iterací. Jedná se především o topologii linky, která sice konverguje nejpomaleji, ale je vůči tomuto aspektu selhání nejodolnější. Oproti tomu silně propojené topologie typu každý s každým nebo hvězdy, které konvergují oproti slabě propojeným topologiím velmi rychle, jsou ztrátou zprávy podstatně více ovlivněny. Pokud by se pokus zaměřil výhradně na relativní zpomalení protokolu, tak se topologie hvězdy a topologie plně propojené jako reprezentanti silně propojených topologií jeví jako výrazně rychlejší oproti topologii linky jako reprezentanta slabě propojené topologie.



Obrázek 18: Vliv pravděpodobnosti ztráty zprávy na zpomalení protokolu push-sum.

Další simulace byla zaměřena na odchylku konečného odhadu od reálného průměru, která může být způsobena ztrátou zpráv. Tak jako v předchozí simulaci byly hodnoty p voleny v rozmezí hodnot 0,1 až 0,9 a simulace byla opakován 100 krát, aby bylo dosaženo vyšší statistické kredibility. Výsledky analýzy pro všechny zvolené topologie jsou k nahlédnutí na obrázku Obrázek 19.



Obrázek 19: Vliv pravděpodobnosti ztráty zprávy na odchylku od reálné hodnoty.

Při porovnání výsledků s předchozí simulací lze vidět, že mají tyto poruchy signifikantní negativní dopad na topologie s nižší měrou konvergence. Topologie hvězdy je nejvíce odolná vůči poruše. Maximální odchylka od reálné hodnoty dosahuje pouze 5%. Simulace tedy prokazuje, že protokol push-sum dosahuje právě v této topologii největší robustnosti. Plně propojená topologie taktéž dosahuje velké odolnosti proti ztrátě zpráv. Maximální odchylka odhadu se pohybuje okolo 7%. Maximální odchylka odhadu zjištěná ve stromové topologii přesahovala hranici 15%. Odchylka odhadu v kruhové topologii dosáhla hodnoty vyšší než 25%. Vůbec nejhorší výsledky byly získány u linkové topologie. U této topologie se maximální odchylka pohybovala nad hodnotou 35%. Přitom bylo i u minimální hodnoty p = 0,1 v této topologii dosaženo minimální odchylky okolo 15%, což také představuje vysokou míru odchylky odhadu.

Každopádně, i když se míra konvergence v této topologii vlivem vložených poruch zvyšuje, konečné odchylky odhadu jsou nepřijatelné i pro nízké hodnoty p. Z pokusu lze vysledovat, že zvyšující se pravděpodobnost ztráty zprávy ovlivňuje odchylku odhadu bez ohledu na použitou topologii.

4.3 Diskuse výsledků

Tato část práce ukázala přirozenou odolnost protokolu push-sum modelovanou na základě Bernoulliho distribuce. Byly pozorovány změny charakteru odhadu, vliv chyb na zpomalení protokolu a také vliv pravděpodobnosti ztráty zprávy na odchylku od reálné hodnoty průměru. Vliv změny pravděpodobnosti chyby byl poté testován na zástupcích slabě propojených statických topologií, mezi které byly zařazeny linka, kruh a strom. Mezi silně propojené statické topologie byly zařazeny topologie sítě typu hvězda a plně propojená síť. Z výsledků lze pozorovat, že vložená chyba může znamenat pro silně propojené topologie zpomalení výpočetního procesu nebo naopak jeho zrychlení v topologiích slabě propojených. V topologiích, kde byl průběh protokolu push-sum rychlý a zároveň v něm nebyly vloženy chyby, byl pozorován rapidní nárůst počtu iterací. V přímém kontrastu s tímto zjištěním měla odchylka od konečného odhadu přesně opačný charakter. Dostatečná přirozená robustnost protokolu byla pozorována pouze v topologiích hvězdy a plně propojené. V linkové topologii dosáhla maximální odchylka výše 35%, což představuje velmi malou robustnost protokolu push-sum ke ztrátám zpráv. Tímto bylo prokázáno, že protokol nebyl přirozeně odolný ke ztrátám zpráv ve slabě propojených sítích.

5 NÁVRH NOVÉ METODY DETEKCE PORUCHY V SÍTI

V této kapitole je uveden návrh nové metody detekce poruchy v síti pomocí distribuovaného stochastického algoritmu push-sum. Model detekce poruchy je založen na výpočtu průměru hodnot získaných v reálném světě jako výstupy senzorů instalovaných na přístupovém bodě. V simulacích následujících návrzích modelu jsou tyto anomálie reprezentovány nižší hodnotou parametru kvality sítě.

5.1 Specifikace návrhu

Cílem simulace je ukázat, jakým způsobem lze využít distribuovaný stochastický

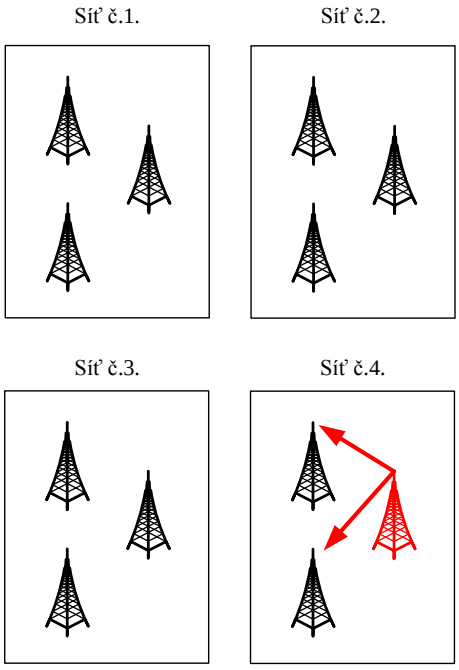
algoritmus push-sum pro detekci poruchy v síti. V případě protokolu push-sum se jedná o multifunkční algoritmus pro odhad agregační funkce. Tento model je v práci zaměřen na odhad průměru.

Každý uzel udržuje v paměti aktuální hodnotu vnitřního stavu reprezentující aktuální parametr kvality signálu uzlu a aktuální váhu uzlu. Oba dva tyto parametry budou aktualizovány na základě hodnot poslaných od uzlů z přilehlé oblasti, stejně jako hodnot z předešlých iterací. Jak už bylo řečeno dříve, testované topologie budou v rámci simulace vycházet z malých geograficky oddělených částí, jelikož nasazení robustní sítě uzlů pro velkou oblast by znamenalo výrazné zpomalení výpočtu a méně prokazatelné výsledky. Geografická oblast, ve které je detekován snížený vypočtený průměr parametru kvality signálu sítě, se poté stává sledovanou.

V první části simulace je nalezena topologie s hustotou uzlů, u které je nejvíce průkazný efekt vložené poruchy na parametr kvality příjmu signálu. V dalším kroku budou porovnány čtyři sítě o velikosti ploch 100x100, 200x200, 350x350 a 500x500, do kterých bude náhodně rozmístěno 200 uzlů s konstantním vysílacím rozsahem d = 50. Rozdílnou velikostí mřížky o stejném počtu uzlů bude zabezpečena různá hustota uzlů. Výstupní hodnoty prokážou, který typ sítě bude nejvhodnější pro další využití. Předpokládaným výsledkem je, že u sítí s velmi vysokou hustotou bude dosaženo nejvyššího vzájemného rušení mezi vloženým uzlem interferujícím s okolními uzly.

V druhé části simulace jsou simulovány scénáře pro čtyři sítě s velmi vysokou hustotou. Sítě budou opět sestaveny z 200 uzlů. Velikost plochy, na které budou uzly umístěny, je dána zvolenou konstantou d = 100, tedy ploše 100 x 100. Tato konstanta představuje jednotku reprezentující vzdálenost vzhledem k tomu, že v reálné situaci by za tuto konstantu mohly být dosazeny například jednotky km na základě dosahu uzlů. Dosah každého uzlu je zvolen jako d = 50.

Simulace je provedena pro všechny topologie s vysokou hustotou uzlů nejprve v prostředí odrážejícím fungování sítě bez interferenčních ruchů okolí. Předpokládaným výstupem simulace jsou numerické výsledky ukazující průměrnou procentuální hodnotu zisku signálu v určené síti se zvolenými parametry. Protokol push-sum proběhne v každé síti nezávisle.



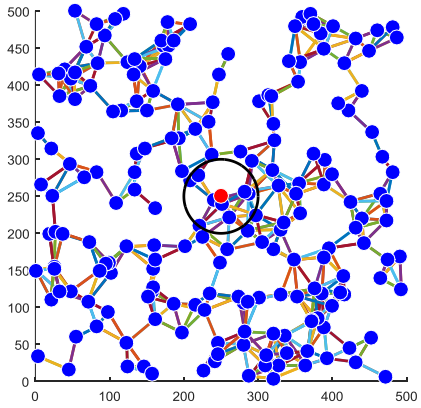
Obrázek 20: Porucha v síti č.4 způsobená implementací nového elementu

Jak je naznačeno na obrázku Obrázek 20, push-sum protokol je spuštěn na čtyřech nezávislých sítích. Každá síť bude testována nejprve bez jakýchkoliv poruch (naznačeno v sítích 1 až 3, obrázku Obrázek 20) a následně bude každá jednotlivá část sítě podrobena testu při poruše (naznačeno v síti 4, obrázku Obrázek 20). Výsledky budou následně prezentovány a diskutovány.

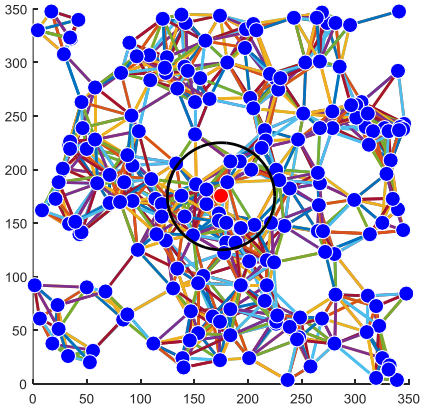
5.2 Nalezení vhodně konektované topologie

Simulace sítě, jejichž principy byly naznačeny v úvodním textu této kapitoly, jsou vyobrazeny níže na obrázcích Obrázek 21, Obrázek 22, Obrázek 23 a Obrázek 24. Modré body substituují jednotlivé přístupové body v síti, které jsou vzájemně propojeny barevnými spoji. Tyto spoje jsou barevné právě proto, aby bylo možné identifikovat, který uzel komunikuje se kterým. Jak lze z obrázků pozorovat, push-sum protokol je aplikován na topologie s různou hustotou uzlů bez jakéhokoliv rušivého elementu. Je vycházeno z předpokladu, že nerušené uzly jsou iniciovány hodnotami parametru kvality signálu v rozsahu 80% až 98%. V první simulaci modelu byla iniciační hodnota parametru kvality signálu pro nezarušené uzly zvolena jako konstanta o hodnotě 89,2763%, aby bylo možné prokazatelně určit nejvhodnější hustotu sítě pro další

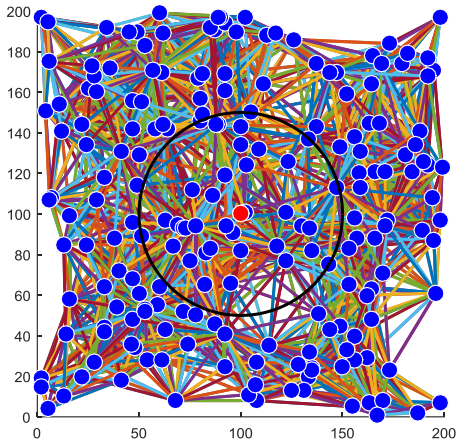
simulace. Uzly zasáhnuté interferencemi mají inicializační hodnotu parametru kvality signálu blízkou hodnotě 50%.



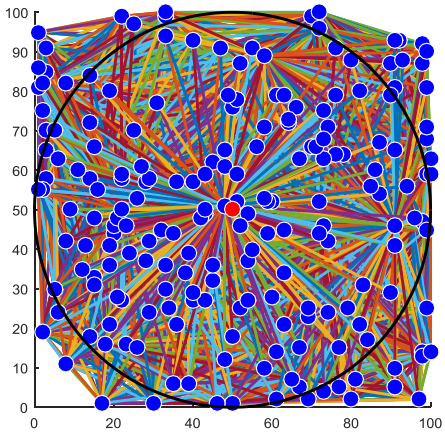
Obrázek 21: Topologie sítě s nízkou hustotou uzlů o velikosti d = 500.



Obrázek 22: Topologie sítě se střední hustotou uzlů o velikosti d = 350.



Obrázek 23: Topologie sítě s vysokou hustotou uzlů o velikosti d = 200.



Obrázek 24: Topologie sítě s velmi vysokou hustotou uzlů o velikosti d = 100.

Pro simulaci sítí s rušivým elementem byl zaveden do zdravé topologie jeden interferující uzel označený v obrázcích červeným bodem. Rušivý element v síti interferoval s okolními body do vzdálenosti d = 50. Jeho dosah je v obrázcích vyznačen černým kruhem. Jak je patrno z výše uvedených obrázků. V případě sítě s nízkou hustotou uzlů byl ovlivněn tímto rušivým elementem jen malý počet ostatních zdravých uzlů a tedy i numerická hodnota vyhodnocená simulací tomuto faktu odpovídá. I když je rozdíl mezi parametrem kvality signálu v takovéto síti nepatrný a odpovídá hodnotě 1,4228%, lze s jistou pravděpodobností říci, že se v oblasti rušivý prvek vyskytnul. V tabulce Tabulka 3 jsou znázorněny kompletní výsledky této simulace. Za nejprokazatelnější výsledky lze považovat hodnoty parametru kvality sítě u sítí s velmi

vysokou hustotou uzlů. Zde byla detekce poruchy nejzřetelnější. Předchozí teze tedy byly potvrzeny.

Tabulka 3: Výsledky detekce interferencí v zarušeném a nezarušeném prostředí ve zvolených topologiích.

Hustota uzlů v topologii	Parametr signálu [%]	
	Bez rušení	S rušením
Nízká	89,2763	87,8535
Střední	89,2763	85,7707
Vysoká	89,2763	82,2701
Velmi vysoká	89,2763	58,2632

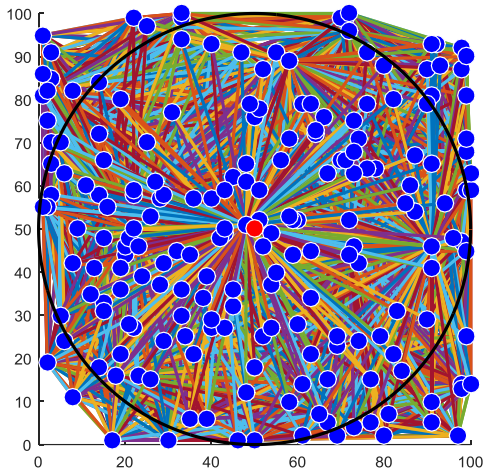
Ze simulací realizovaných na čtyřech rozdílných sítích je zřejmé, že nejvhodnější volbou pro další výzkum jsou sítě s velmi vysokou hustotou uzlů. Tento způsob propojení uzlů v senzorové síti zároveň reflektuje propojení senzorových sítí v praxi.

5.3 Detekce rušivého elementu v síti

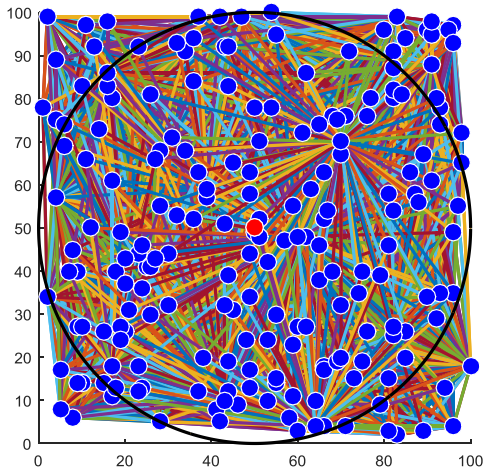
Simulace sítě, jejichž principy byly naznačeny v úvodním textu této kapitoly, jsou vyobrazeny níže na obrázcích Obrázek 25, Obrázek 26, Obrázek 27 a Obrázek 28. Čtyři uvedené topologie se liší vzájemným propojením uzlů i jejich rozmístěním proto, aby bylo možné tvrdit, že způsob propojení topologie při této hustotě uzlů markantně neovlivní výsledek. Výsledek by v případě těchto simulací ovlivněn mohl být, ale musel by být významně snížen počet vzájemných propojení mezi uzly.

Modré body, stejně jako v předchozím pokusu, definují jednotlivé přístupové body v síti, které jsou vzájemně propojeny barevnými spoji. Tyto spoje jsou barevné právě proto, aby bylo možné identifikovat, který uzel komunikuje se kterým. Jak lze z obrázků pozorovat, push sum protokol je aplikován na sítě s velmi vysokou hustotou uzlů. Nejprve byly simulovány tyto topologie jako nezarušené. Nezarušená síť neobsahovala červený bod uprostřed, ale simulované sítě zůstaly propojeny pro každý scénář stejně. Červený bod uprostřed obrázku představuje nově vložený neznámý přístupový bod interferující s okolními uzly. Černý kruh vyznačuje dosah červeného bodu. Následně je pro dané topologie simulován scénář s aktivním červeným bodem a

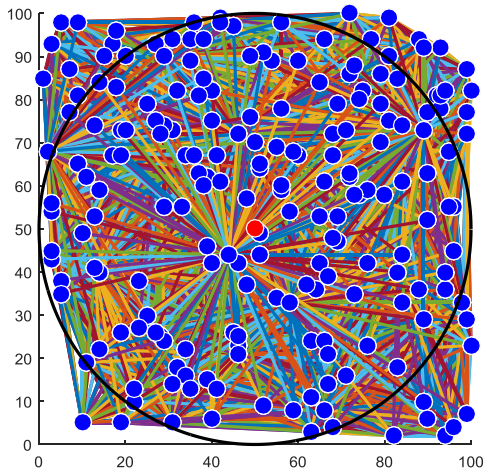
výsledky jsou vyhodnoceny v tabulce Tabulka 4. Je vycházeno z předpokladu, že nerušené uzly jsou iniciované hodnotami v rozsahu 80%-98%, zatímco uzly zasáhnuté interference mají inicializační hodnotu okolo 50%. V praxi bychom samozřejmě parametr určující sílu signálu mohli dosadit jako výstupní hodnotu senzoru přilehlého k uzlu, který identifikuje.



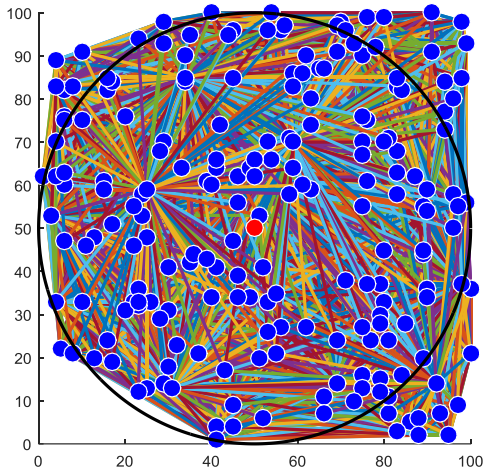
Obrázek 25: Topologie sítě 1 s velmi vysokou hustotou uzlů a jedním vloženým rušivým elementem.



Obrázek 26: Topologie sítě 2 s velmi vysokou hustotou uzlů a jedním vloženým rušivým elementem.



Obrázek 27: Topologie sítě 3 s velmi vysokou hustotou uzlů a jedním vloženým rušivým elementem.



Obrázek 28: Topologie sítě 4 s velmi vysokou hustotou uzlů a jedním vloženým rušivým elementem.

Jak lze pozorovat z výsledků v tabulce Tabulka 4, hodnoty parametru signálu určujícího kvalitu příjmu v nezarušené síti, jsou diametrálně odlišné od sítě zarušené. Zatímco nejlepšího výsledku s nejvyšší procentuální hodnotou zisku signálu bylo dosaženo v nezarušené topologii číslo 4, nejvyšší hodnota stejného parametru v zarušeném prostředí byla ve stejné topologii za stejných podmínek nižší o 31,837%. Lze tedy jasně určit, ve které části sítě dochází k rušení. Tímto způsobem je detekována

porucha v bezdrátové síti. Výzkum tedy prokazuje funkčnost nově navržené metody využití protokolu push-sum pro detekci poruchy příjmu signálu v silně propojených topologiích.

Tabulka 4: Výsledky detekce interferencí v zarušeném a nezarušeném prostředí.

Označení topologie	Parametr signálu [%]	
	Bez rušení	S rušením
Topologie č.1	89,2763	58,2632
Topologie č.2	89,1837	56,7127
Topologie č.3	88,561	56,4959
Topologie č.4	88,5806	56,7436

5.4 Diskuse výsledků

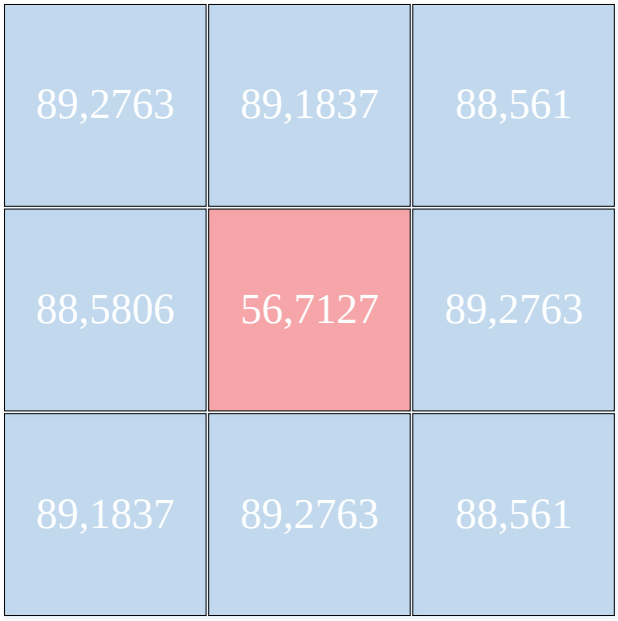
Pomocí tohoto návrhu bylo prokázáno, že je možné využít nově navrženou metodu detekce poruchy v síti s využitím protokol push-sum pro detekci poruchy v síti na základě odhadu průměru. Nejprve bylo experimentálně ověřeno, pro které sítě je aplikace tohoto postupu nejvhodnější. Z výsledných hodnot bylo zjištěno, že jsou nejvhodnějšími sítěmi k implementaci algoritmu push-sum pro detekci poruch nejvhodnější sítě s velmi vysokou hustotou uzlů. Na nich byly poté aplikovány další pokusy. Odhad průměru byl komparován nejprve pro sítě bez uzlu způsobujícího interference a následně byl ten samý pokus aplikován na sítě s přítomností tohoto rušivého elementu.

Na základě předchozích výsledků byla zvolena silně propojená topologie pro její vhodnost prokázanou v především v kapitole 3. Na základě dosažených výsledků je patrné, že porucha vložená do dříve neměnné topologie způsobuje snížení parametru určujícího kvalitu signálu okolních uzlů v síti vypočteného na základě odhadu průměru. Emitováním vlastních interferenčních vln na stejné frekvenci červený bod v každé simulované topologii způsobil menší, či větší zhoršení procentuálního vyjádření síly signálu. Ačkoli není protokol push-sum přímo určen pro výpočet odhadu průměru v dynamicky a často se měnících sítích, bylo prokázáno, že ho lze i přesto využít pro detekci poruch. U bezdrátových sítí totiž v drtivé většině neprobíhají změny topologie tak často, aby byl ovlivněn výpočet hodnot definujících kvalitu signálu. Změna

topologie je v tomto případě chápána jako přidání nebo naopak odebrání bezdrátového uzlu v síti.

Výsledný efekt metody detekce v přístupové síti

Pokud budeme uvažovat, že je telekomunikační přístupová síť rozdělena na kvadranty o určené velikosti, můžeme tyto oblasti softwarově definovat a v jednotlivých kvadrantech nechat ve zvoleném časovém intervalu pravidelně iterovat protokol push-sum. V každém kvadrantu dosáhneme jisté hodnoty parametru kvality sítě, která bude odrážet její aktuální stav. Jak lze vidět na obrázku Obrázek 29, modré kvadranty s hodnotami odpovídajícími předpokládanému průměru nevykazují výraznější odchylky od požadované kvality sítě. Červený kvadrant, který byl shledán vadným, vykazuje poruchu sítě vyjádřenou numericky.



Obrázek 29: Prezentace výsledku metody detekce poruchy v síti

Samotná lokalizace kvadrantu, ve kterém vzniká interference, již tedy bude pro dohledové centrum pouze formalitou. Síť se vyhne stížnostem od uživatelů na nefunkční služby, kterých bylo dle zdroje [63] za rok 2016 detekováno v České republice 3405 pro technologii LTE. Lokální autorita po detekci interferencí kontaktuje majitele nového zařízení, které se vyskytlo v přístupové síti a nařídí mu nápravu, aniž by koncový uživatel změny sítě pocítil. Tím se zároveň dosáhne vyšší úrovně transparentnosti přístupové sítě.

6 ZÁVĚR A DISKUSE DOSAŽENÝCH VÝSLEDKŮ

Stále se rozvíjející infrastruktura a technologická pokročilost komunikačních technologií s sebou přináší nové výzvy při implementaci či transformaci telekomunikačních systémů. Vzhledem k vyčerpatelnosti frekvenčních pásem se vývoj bezdrátového přenosového systému potýká s interferencemi mezi používanými pásmy především v jejich hraničních oblastech. Pro predikci a detekci hrozby tohoto druhu poruch v síti jsou již dnes implementovány dohledové systémy společnostmi, které orientují svoji obchodní strategii na datové či televizní přenosy volným prostředím.

Dohledové systémy pracují s velmi sofistikovanými metodami získávání, zpracování a reprodukcí získaných dat odrážejících aktuální stav celé bezdrátové sítě. Pro získávání dat jsou využívány senzorové systémy propojené do jedné rozsáhlé struktury, která centralizovaně zpracovává výsledky a na základě informace o stavu sítě vyhodnocuje a upravuje parametry sítě, případně po detekci chyby informuje operátora. Pro těžení z databází naplněných daty získanými analýzou sítě jsou veskrze využívány algoritmy k tomuto účelu určené. Celý systém ale v drtivé většině vyžaduje ekonomicky náročný hardware, který je rozprostřen po celé síti a tvoří centrální buňky schopné vytěžit důležité výsledky.

Tato dizertační práce využívá poznatků o dohledových systémech a pomocí nové metody detekce poruchy v síti ukazuje další možnou cestu transformace detekčních algoritmů, která by vedla nejen ke snížení výdajů na hardwarovou strukturu sítě, ale může také umožnit rychlejší odhad stavu sítě, díky rychlé konvergenci požadovaných dat. Pokud je totiž vycházeno z hlavní vlastnosti distribuovaných stochastických algoritmů využívajících principu push, že jsou schopny v počáteční fázi velmi rychle konvergovat, informace o aktuálním stavu sítě může být získána velmi rychle a s relativně nízkými náklady. Díky robustnosti těchto algoritmů dosahujeme vysoké pravděpodobnosti, že i když nám vypadne několik uzlů v síti kvůli poruše, jsme schopni obdržet informaci ze sítě v požadované kvalitě. Hlavním limitujícím faktorem algoritmů postaveným na principu push se ale může stát míra odhadu, které je potřeba dosáhnout.

Stávající systémy většinou nemusí využívat heuristiku k dokončení svého úkolu

a díky tomu je obdržená informace o stavu sítě vždy vypočtena do finální podoby. Právě jistá náhodnost v procesu získávání dat z rozsáhlých sítí vede ke zrychlení celého procesu. Z výše uvedených poznatků o chování senzorových sítích implementovaných do sítí poskytujících služby televizního přenosu a LTE technologií vychází výzkumná část dizertační práce, ve které je nejprve zvolen vhodný distribuovaný stochastický algoritmus, kterým se stal protokol push-sum a na jeho základě jsou prováděny další simulace.

Součástí první části navrhovaného řešení se stala komparace statistické kredibility reprezentanta v síti, která přinesla výsledky dokazující vliv nárůstu počtu opakování provedení iterací push-sum protokolu na statistickou kredibilitu reprezentanta rychlosti konvergence. Tato rychlost se měnila pro různé běhy protokolu v určených sítích při zachování stejných vstupních podmínek, jakými byla například neměnná topologie sítě nebo stejné počáteční stavy uzlů a jejich váhy, podle teoretických předpokladů. Měření rychlosti konvergence bylo provedeno nejprve pro slabě propojenou topologii, ve které dosahoval protokol pomalejší konvergence. Pomalejší konvergence v síti byla zapříčiněna horší dostupností uzlů a také na základě faktu, že všeobecné šíření informace ve slabě propojených sítích je pomalejší, než v silně propojených sítích. Silně propojené sítě byly v simulaci zastoupeny plně propojenou topologií, která poskytuje nejlepší možnou hustotu spojení mezi uzly. Zde byla simulace orientována především na velmi rychlé šíření informace. Aplikací mnohonásobného propojení sítě byla zvýšena schopnost její konvergence, jak bylo numericky ukázáno v tabulce a vyneseno ve srovnávacím grafu. Pro obě topologie bylo provedeno pět simulací pro různý počet iterací, aby byl důkaz předpokládaných výsledků co nejprůkaznější. Ze získaných dat byla poté ověřena statická kredibilita vypočítáním variačního rozpětí získaných průměrů.

Druhá část návrhu přinášející důkazy o využitelnosti protokolu push-sum u nové metody detekce poruchy v bezdrátové síti byla věnována ověření, nakolik je tento protokol robustní, tedy odolný vůči ztrátě zprávy při jeho běhu v síti. S využitím pravděpodobnosti ztráty zprávy při aplikaci Bernoulliho distribuce byly tyto ztráty zpráv substituovány. Postupně byla pro pět různých statických topologií ověřena odchylka konečného odhadu od reálné hodnoty průměru. Změna počtu iterací poté indikovala přizpůsobivost protokolu push-sum při ztrátách zpráv.

Samotný návrh nové metody pro detekci poruchy v bezdrátové síti obsažený v kapitole 5 byl věnován způsobu detekce chyby v síti na základě rušivého elementu vloženého do soustavy. Nejprve byly pomocí simulace potvrzeny předpoklady, že v silně propojené topologii s vysokou hustotou uzlů bude interference mezi rušivým elementem a ostatními uzly nejprůkaznější. Následně byly vytvořeny čtyři scénáře s náhodně rozmístěnými uzly v síti a na tyto uzly byl následně aplikován protokol push-sum, zatímco byly uzly ve vyznačeném kruhu rušeny interferujícím bodem. Analýza výsledků prokázala, že bylo ve všech případech rušení možné detekovat nově vložený interferující element s prokazatelnou pravděpodobností. Numerické výsledky byly poté vyneseny do tabulky a okomentovány. Prokázáním funkčnosti nově navržené metody detekce poruch v síti a následnou diskusí výsledků bylo dosaženo hlavních cílů dizertační práce.

V oblasti detekce poruch v bezdrátových systémech by bylo zajímavé sledovat, jakým směrem se detekční algoritmy budou dále ubírat. V současné době je trend vedoucí k integraci jednotlivých senzorů do uzlů sítě zároveň jistou úsporou v nákladech jednotlivých společností, ale zároveň zhoubou pro kooperaci sítě jako globálního celku. Vzhledem k tomu, že si společnosti své know how a detekční algoritmy pečlivě chrání, bude pravděpodobně nevyhnutelné instalovat senzory kontrolované nadřazenou entitou, které budou přinášet relevantní data o stavu sítě přímo nadřazené entitě.

LITERATURA

[1] LYNCH, N., A. *Distributed Algorithms, 2nd edition*. San Francisco, California: Morgan Kaufman, 1997, 904 s. ISBN: 978-1-55860-348-6.

[2] JANEČEK, J. *Distribuované systémy*. Praha: Vydavatelství ČVUT, 2001. ISBN 80-01-02307-9.

[3] ROSE, C. a SMITH, M.D. *Mathematical statistics with Mathematica*. New York: Springer, c2002. ISBN 978-038-7952-345.

[4] FORBES, C., EVANS, M., HASTINGS, N. a PEACOCK, B. *Statistical distributions*. 4. Oxford: Wiley-Blackwell, 2010. ISBN 9780470627242.

[5] ABRAMOWITZ, M. a STEGUN, I., A. *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. New York: Dover Publications, 1972. ISBN 978-048-6612-720.

[6] INTANAGONWIWAT, Ch., GOVINDAN, R. a ESTRIN, D. *Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks* [online]. [cit. 2017-06-27]. Dostupné z: https://www.isi.edu/division7/publication_files/directed_diffusion_scalable.pdf

[7] AKYILDIZ, I. K., SU, W., SANKARASUBRAMANIAM, Y., a CAYIRCI, E. *A survey on sensor networks* [online]. 2002, , 102 - 114 [cit. 2017-06-27]. ISSN 01636804. Dostupné z: http://ieeexplore.ieee.org/abstract/document/1024422/

[8] ESCHENAUER, L., GLIGOR, G. D., *A key-management scheme for distributed sensor networks.* Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002. New York, NY: ACM Press, 2002. ISBN 1581136129.

[9] RAMANATHAN, R. a REDI, J. *A brief overview of ad hoc networks: challenges and directions.* IEEE Communications Magazine [online]. 2002, 40(5), 20-22 [cit. 2017-06-27]. DOI: 10.1109/MCOM.2002.1006968. ISSN 0163-6804. Dostupné z: http://ieeexplore.ieee.org/document/1006968/

[10] ESTRIN, D., GOVINDAN, R., HEIDEMANN, J., a KUMAR, S. *Next century challenges: challenges and directions.* Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking - MobiCom '99 [online]. New York,

New York, USA: ACM Press, 1999, 40(5), 263-270 [cit. 2017-06-27]. DOI: 10.1145/313451.313556. ISBN 1581131429. ISSN 0163-6804. Dostupné z: http://portal.acm.org/citation.cfm?doid=313451.313556

[11] DARGIE, W. a POELLABAUER, Ch. *Fundamentals of wireless sensor networks: theory and practice*. Hoboken, NJ: Wiley, 2010.

[12] SHIH, E., BAHL, P., a SINCLAIR, M. J. *Wake on Wireless: An Event Driven Energy Saving Strategy for Battery Operated Devices.* MOBICOM [online]. 2002, [cit. 2017-06-28]. Dostupné z: https://www.cs.colorado.edu/~rhan/CSCI_7143_Fall_2007/Papers/p160-shih.pdf

[13] CALHOUN, B. H., DALY, D. C., VERMA, N., FINCHELSTEIN, D. F., WENTZLOFF, D. D., WANG, A., CHO, S. H., and CHANDRAKASAN, A.P. *Design considerations for ultralow energy wireless microsensor nodes.* IEEE. 2005, Transactions on Computers 54 (6), 727–749.

[14] DE, V. a BORKAR, S. *Technology and design challenges for low power and high performance [microprocessors]*. Proceedings. 1999 International Symposium on Low Power Electronics and Design (Cat. No.99TH8477) [online]. IEEE, 1999, s. 163-168 [cit. 2017-06-28]. DOI: 10.1109/LPE.1999.799433. ISBN 1-58113-133-X. Dostupné z: http://ieeexplore.ieee.org/document/799433/

[15] PROAKIS, J., G. *Digital communications*. 4th ed. Boston: McGraw-Hill, 2000. ISBN 0072321113.

[16] WILSON, S., G. *Digital modulation and coding*. Upper Saddle River, N.J.: Prentice Hall, c1996. ISBN 0132100711.

[17] KEMPE, D., DOBRA, A. a GEHRKE, J. *Gossip-based computation of aggregate information.* 44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings [online]. IEEE Computer. Soc, 2003, s. 482-491 [cit. 2017-07-11]. DOI: 10.1109/SFCS.2003.1238221. ISBN 0-7695-2040-5. Dostupné z: http://ieeexplore.ieee.org/document/1238221/

[18] KENYERES, M., KENYERES, J. a ŠKORPIL, V. *The Analysis Of The Push-sum Protocol In Various Distributed Systems.* European Scientific Journal [online]. 2016, **2016**(1), 64-80 [cit. 2017-07-11]. ISSN 1857 - 7431. Dostupné z: eujournal.org/index.php/esj/article/download/7287/7061

[19] STRAKOVA, H., NIEDERBRUCKER, G. a GANGSTERER, W., N. *Fault Tolerance*

Properties of Gossip-Based Distributed Orthogonal Iteration Methods. Procedia Computer Science [online]. 2013, **18**, 189-198 [cit. 2017-07-29]. DOI: 10.1016/j.procs.2013.05.182. ISSN 18770509. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1877050913003256

[20] EL GAMAL, A., MAMMEN, J., PRABHAKAR, B. a SHAH, D. *Optimal throughput-delay scaling in wireless networks - part I: the fluid model.* IEEE Transactions on Information Theory [online]. 2006, **52**(6), 2568-2592 [cit. 2017-07-12]. DOI: 10.1109/TIT.2006.874379. ISSN 0018-9448. Dostupné z: http://ieeexplore.ieee.org/document/1638544/

[21] GUPTA, P. a KUMAR, P.R. *The capacity of wireless networks*. IEEE Transactions on Information Theory [online]. **46**(2), 388-404 [cit. 2017-07-12]. DOI: 10.1109/18.825799. ISSN 00189448. Dostupné z: http://ieeexplore.ieee.org/document/825799/

[22] PENROSE, M. *Random geometric graphs*. New York: Oxford University Press, 2003. ISBN 0198506260.

[23] FATTA, G., D. *Epidemic Protocols in Peer-to-Peer Computing.* The Third International Conference on Advances in P2P Systems [online]. Lisabon, 2011 [cit. 2017-07-12]. ISBN 978-1-61208-173-1.

[24] SAIDI, A. a MOHTASHEMI, M. *Minimum-cost First-Push-Then-Pull gossip algorithm.* 2012. IEEE Wireless Communications and Networking Conference (WCNC) [online]. IEEE, 2012, s. 2554-2559 [cit. 2017-07-13]. DOI: 10.1109/WCNC.2012.6214229. ISBN 978-1-4673-0437-5. Dostupné z: http://ieeexplore.ieee.org/document/6214229/

[25] PITTEL, B. *On spreading a rumor*. SIAM Journal of Applied Mathematics, 47(1):213–223, 1987.

[26] FEDEWA, N., KRAUSE, E. a SISSON, A. *Spread of A Rumor* [online]. Department of Mathematics, Central Michigan University Mt. Pleasant, **2013** [cit. 2017-07-20]. Dostupné z: https://www.siam.org/students/siuro/vol6/S01182.pdf

[27] ALVISI, L., DOUMEN, J., GUERRAOUI, R., KOLDEHOFE, B., LI, H., VAN RENESSE, R. a TREDAN, G. *How robust are gossip-based communication protocols?* ACM SIGOPS Operating Systems Review [online]. 2007, **41**(5), 14- [cit. 2017-07-21]. DOI: 10.1145/1317379.1317383. ISSN 01635980. Dostupné z: http://portal.acm.org/citation.cfm?doid=1317379.1317383

[28] BIRMAN, K. P., HAYDEN, M., OZKASAP, O., XIAO, Z., BUDIU M. a MINSKY. Y.

Bimodal multicast. ACM Transactions on Computer Systems [online]. **17**(2), 41-88 [cit. 2017-07-21]. DOI: 10.1145/312203.312207. ISSN 07342071. Dostupné z: http://portal.acm.org/citation.cfm?doid=312203.312207

[29] KHANDEKAR, A., BHUSHAN, N., TINGFANG, J. a VANGHI, V. *LTE-Advanced: Heterogeneous networks*. In: 2010 European Wireless Conference (EW) [online]. IEEE, 2010, s. 978-982 [cit. 2017-07-26]. DOI: 10.1109/EW.2010.5483516. ISBN 978-1-4244-5999-5. Dostupné z: http://ieeexplore.ieee.org/document/5483516/

[30] KOPETZ, H. a P VERÍSSIMO. *Real time and dependability concepts*. 2. New York, NY, USA: ACM Press/Addison-Wesley Publishing Co., 1993. ISBN 201624273.

[31] BLAIR, G. a STEFANI, J. B. *Open distributed processing and multimedia*. Reading, Mass.: Addison-Wesley, c1998. ISBN 0201177943.

[32] SHELTAMI, T. *An enhanced energy saving approach for WSNs*. 2013. Procedia Computer Science, 21, 199-206.

[33] PASCHALIDIS, I., HUANG, F. a LAI, W. *A message-passing algorithm for wireless network scheduling.* IEEE/ACM Transactions on Networking [online]. 2015 [cit. 2017-07-31]. ISSN 1528-1541.

[34] BASS, L., CLEMENTS, P. a KAZMAN, R. *Software architecture in practice*. 3rd ed. Upper Saddle River, NJ: Addison-Wesley, c2013. ISBN 9780321815736.

[35] MEHTA, N.R., MEDVIDOVIC, N. a PHADKE, S. *Towards a taxonomy of software connectors.* Proceedings of the 2000 International Conference on Software Engineering. ICSE 2000 the New Millennium [online]. ACM, 2000, s. 155 [cit. 2017-07-31]. DOI: 10.1109/ICSE.2000.870409. ISBN 1-58113-206-9. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=870409

[36] SHAW, M. a CLEMENTS, P. *A field guide to boxology: preliminary classification of architectural styles for software systems.* Proceedings Twenty-First Annual International Computer Software and Applications Conference (COMPSAC'97) [online]. IEEE Comput. Soc, 1997, s. 6-13 [cit. 2017-07-31]. DOI: 10.1109/CMPSAC.1997.624691. ISBN 0-8186-8105-5. Dostupné z: http://ieeexplore.ieee.org/document/624691/

[37] ÖZSU, M. a VALDURIEZ, P. *Principles of Distributed Database Systems*. 3. New York: Springer, 2011. ISBN 9781441988348.

[38] LUA, E., K., CROWCROFT, J., PIAS, M., SHARMA, R. a LIM, S. *A survey and comparison of peer-to-peer overlay network schemes.* IEEE Communications Surveys &

Tutorials [online]. 2005, **7**(2), 72-93 [cit. 2017-08-21]. DOI: 10.1109/COMST.2005.1610546. ISSN 1553-877x. Dostupné z: http://ieeexplore.ieee.org/document/1610546/

[39] THEOTOKIS, A., S. a SPINELLIS, D. *A survey of peer-to-peer content distribution technologies*. ACM Computing Surveys [online]. 2004, 36(4), 335-371 [cit. 2017-08-21]. DOI: 10.1145/1041680.1041681. ISSN 03600300. Dostupné z: http://portal.acm.org/citation.cfm?doid=1041680.1041681

[40] NEJDL, W., WOLPERS, M., SIBERSKI, W., SCHMITZ, Ch., SCHLOSSER, M., BRUNKHORST, B. a LÖSER, A. *Super-peer-based routing strategies for RDF-based peer-to-peer networks*. Web Semantics: Science, Services and Agents on the World Wide Web [online]. 2004, 1(2), 177-186 [cit. 2017-08-21]. DOI: 10.1016/j.websem.2003.11.004. ISSN 15708268. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1570826803000271

[41] ABERER, K. a HAUSWIRTH, M. *Peer-to-Peer Systems. The Practical Handbook of Internet Computing*. Boca Raton, FL: eRC Press, 2005

[42] SPALL, J., C. *Introduction to Stochastic Search and Optimization* [online]. Hoboken, NJ, USA: John Wiley & Sons, 2003 [cit. 2017-08-21]. ISBN 9780471722137.

[43] ITU. *Final Acts of the World Radiocommunication Conference (WRC-15)*. World Radiocommunication Conference, Geneva (Switzerland), 2015. ISBN: 978-92-61-16561-1

[44] TEKOVIĆ, A. *LTE in Digital Dividend deployment challenges DVB-C2 case*. Proceedings of the 54th International Symposium ELMAR, Zadar, 2012, str. 251–254.

[45] KANG, D., ZHIDKOV, S. a CHOI, H. *An adaptive detection and suppression of co-channel interference in DVB-T/H system*. IEEE Transactions on Consumer Electronics [online]. 2010, 56(3), 1320-1327 [cit. 2017-08-22]. DOI: 10.1109/TCE.2010.5606265. ISSN 0098-3063. Dostupné z: http://ieeexplore.ieee.org/document/5606265/

[46] GUIDOTTI, A., GUIDUCCI, D., BARBIROLI, M. a kolektiv. *Coexistence and mutual interference between mobile and broadcasting systems.* Proceedings of the IEEE 73rd Vehicular Technology, Budapešť, 2011, p. 1–5. DOI: 10.1109/VETECS.2011.5956540

[47] KRATOCHVÍL, T. *Koexistence digitálních televizních vysílacích sítí se systémy mobilních komunikací*. Brno: VUTIUM, 2015. ISBN 978-80-214-5196-4.

[48] SAKIC, K., GRGIC, S. *The influence of the LTE system on DVBT reception.* Proceedings of the 52nd International Symposium ELMAR. Zadar, 2010, str. 235–238.

[49] ITU. *Recommendation ITU-R BT.1368-8, Planning criteria for digital terrestrial television services in the VHF/UHF bands*, 2009.

[50] STOTT, J., H. *The how and why of COFDM*, EBU technical Review, 1998, pp.1-14.

[51] ECC/TG4. *DRAFT ECC Report LTE - Measurements on the performance of DVB-T receivers in the presence of interference from the mobile service (especially from LTE)*, 15th ECC/TG4 meeting, Cork, 2010.

[52] TEKOVIC, A., BONEFACIC, D., SISUL, G. a NAD, R. *Interference Analysis between Mobile Radio and Digital Terrestrial Television in the Digital Dividend Spectrum.* Radioengineering, 2017, vol. 26, duben 2017.

[53] POLAK, L., KALLER, O., KLOZAR, L., a kol. *Mobile communication networks and digital television broadcasting systems in the same frequency bands: Advanced co-existence scenarios.* Radioengineering, 2014, vol. 23, no. 1, p. 375–386.

[54] 3GPP TR 36.814. *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects.* V9.0.0. 2010. Dostupné online z: http://www.qtc.jp/3GPP/Specs/36814-900.pdf

[55] HOLMA, H., TOSKALA, A. a REUNANEN, J. *LTE small cell optimization: 3GPP evolution to release 13*. ISBN 9781118912577.

[56] ETSI TR 136 912. LTE*: Feasibility study for Further Advancements for E-UTRA (LTE-Advanced).* V10.0.0. Dostupné online z: http://www.etsi.org/deliver/etsi_tr/136900_136999/136912/10.00.00_60/tr_136912v100000p.pdf

[57] ČTÚ. *Postup při šetření rušení rádiového příjmu provozem vysílacích rádiových zařízení širokopásmových mobilních radiokomunikačních sítí* [online]. Praha, 2014 [cit. 2017-01-24]. Dostupné z: https://www.ctu.cz/cs/download/radiove_ruseni/postup_setreni_ruseni_radioveho_prijmu_provozem_lte_24_03_2014_upraveny.pdf

[58] ČTÚ. *Základní informace o experimentu pro ověření dopadu provozu sítí LTE 800 MHz na příjem signálů DVB-T* [online]. 2012 [cit. 2017-01-23]. Dostupné z: http://www.ctu.cz/cs/download/experimentalni_vysilani/test_emc_dvb-t_lte_800_mhz_09_2012.pdf

[59] Federal Communications Commission. *Sirius XM Radio Inc - Nature of the Proposed*

Research and Experimentation. Dostupné online z: https://apps.fcc.gov/els/GetAtt.html?id=176132&x=

[60] DAVID, C., G. A KOL. *Method for collecting data using compact internetworked wireless integrated network sensors (WINS).* Patent US 6735630 B1. Říjen 2004. Dostupné online z: https://patentimages.storage.googleapis.com/pdfs/US6735630.pdf

[61] POTTIE, G., J. *Wireless Integrated Network Sensors (WINS): The Web gets Physical*. Electrical Engineering Department University of California. Dostupné online z: http://www.seas.ucla.edu/~pottie/papers/nae_01.pdf

[62] POTTIE, G.,J. a KAISER, W.,J. *Wireless Integrated Network Sensors (WINS): Principles and Practice*. Electrical Engineering Department University of California. Dostupné online z: http://www.seas.ucla.edu/~pottie/papers/smallWINS_ACM.pdf

[63] ČTÚ. *Výroční zpráva Českého telekomunikačního úřadu za rok 2016*. 2016. [cit. 2017-08-22] Dostupné online z: https://www.ctu.cz/sites/default/files/obsah/stranky/152584/soubory/vz-2016-web.pdf

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

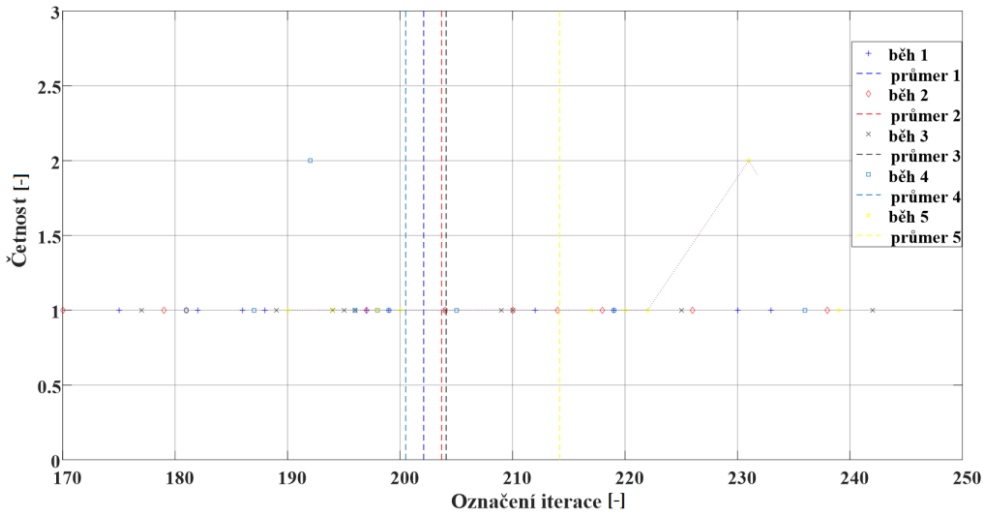
3GPP	Třetí generace partnerského projektu - 3rd Generation Partnership Project
4G	Čtvrtá generace – Fourth Generation
A/D	Analogově digitální - Analog to Digital
Ad-hoc	Z latinského překladu - k tomuto účelu
AWGN	Aditivní bílý Gaussův šum - Additive white Gaussian noise
CET	Středoevropský čas - Central Europien Time
CMOS	Doplňující se kov-oxid polovodič - Complementary Metal–Oxide–Semiconductor
COFDM	Kódovaný ortogonální frekvenčně dělený multiplex - Coded Orthogonal Frequency Division Multiplexing
CoMP	Koordinovaný mnohonásobný přenos a příjem - Coordinated multiple point Transmission and Reception
DNS	Doménový jmenný server - Domain Name server
DVB - C2	Digitální všesměrový videopřenos - Kabelový druhé generace - Digital Video Broadcasting - Cable second generation
DVB - T	Digitální všesměrový videopřenos - Pozemní - Digital Video Broadcasting – Terrestrial
DVB – H	Digitální všesměrový videopřenos – Ruční - Digital Video Broadcasting - Handhalds
EEPROM	Elektronicky vymazatelná paměť pouze pro čtení - Electrically Erasable Programmable Read-Only Memory
FEC	Samoopravný kód - Forward Error Correction
IDL	Jazyk definující rozhraní - Interface Definition Language
GSM	Globální Systém pro Mobilní komunikaci - Global System for Mobile

	Communication
ICIC	Mezibuňková koordinace interfererncí - Inter-cell Interference Coordination
IP	Internetový protokol - Internet Protocol
ISO/OSI	Mezinárodní standardizační organizace/propojení otevřených systémů International Standards Organization/Open Systen Interconnection
LTE	Dlouhodobá evoluce mobilní sítě- Long Term Evolution
LTE-A	Pokročilá dlouhodobá evoluce – Long-Term Evolution - Advanced
MCMC	Iniciály autorů - Markov Chain Monte Carlo
MUF	Minimální pole využití - Minimum Usage Field
P2P	Rovný s rovným - Peer to Peer
PR	Ochranný faktor – Protection Ratio
RAM	Paměť s náhodným přístupem - Random Access Memory
ROM	Paměť pouze pro čtení - Read Only Memory
SNR	Odstup signálu od šumu - Signal to Noise Ratio
TCP	Přenosový protokol - Transmission Control Protocol
VRS	Varianční redukční krok - Variance Reduction Step
WiMAX	Celosvětový standard pro mikrovlnnou interoperabilitu - **W**orldwide **I**nteroperability for **M**icrowave **A**ccess
WINS	Integrované senzory v bezdrátové síti - Wireless Integrated Network Sensors
WSN	Bezdrátová senzorová síť - Wireless Sensor Network

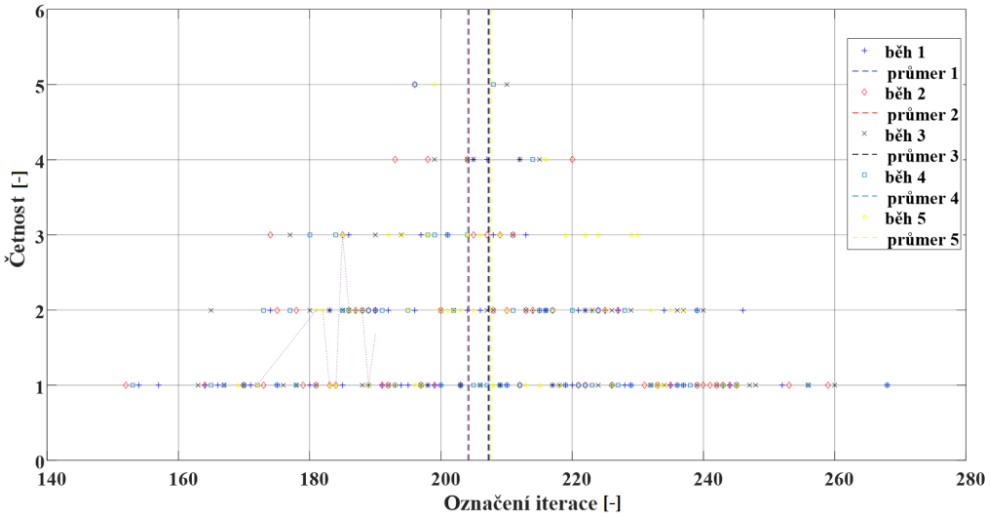
SEZNAM PŘÍLOH

A VÝSLEDKY SIMULACÍ

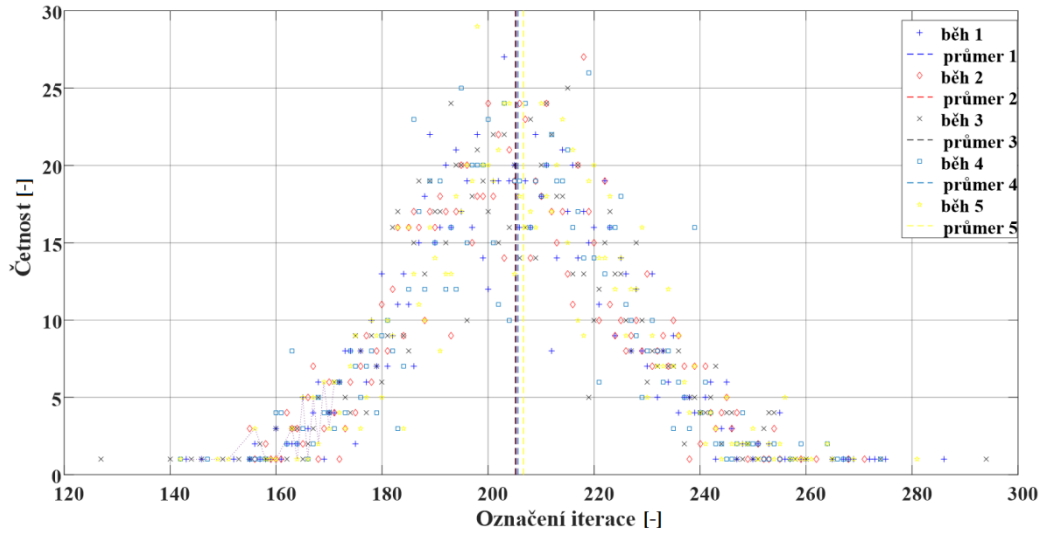
A.1 Výsledky simulace rychlosti konvergence pro slabě propojenou topologii sítě



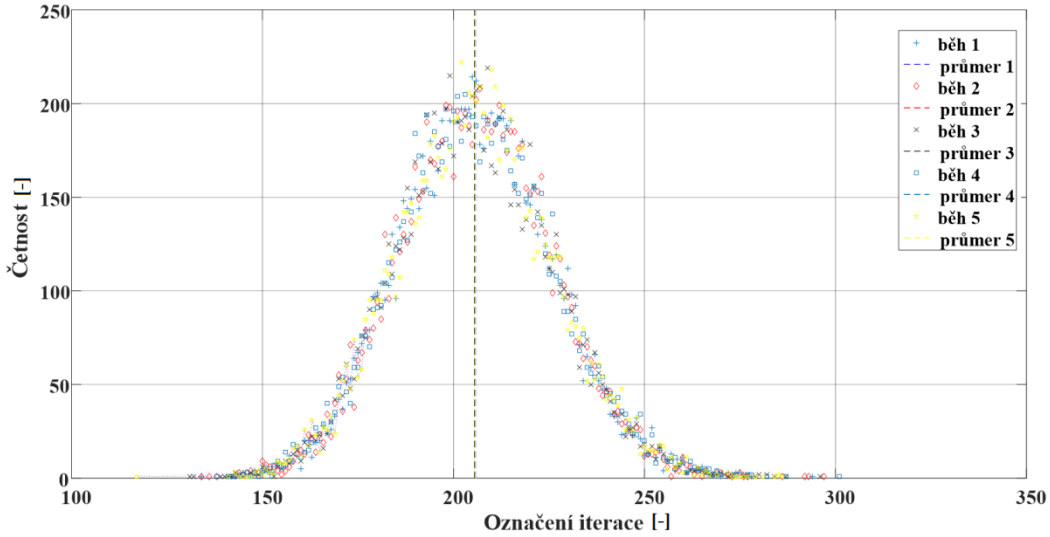
Obrázek 30: Výsledky pro scénář s 10 opakováními.



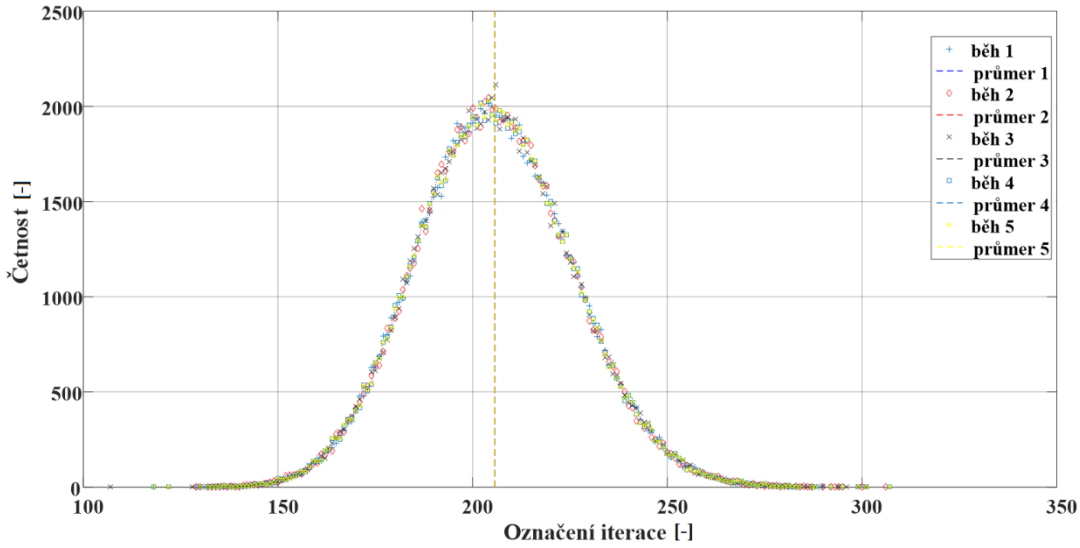
Obrázek 31: Výsledky pro scénář se 100 opakováními.



Obrázek 32: Výsledky pro scénář s 1000 opakováními.

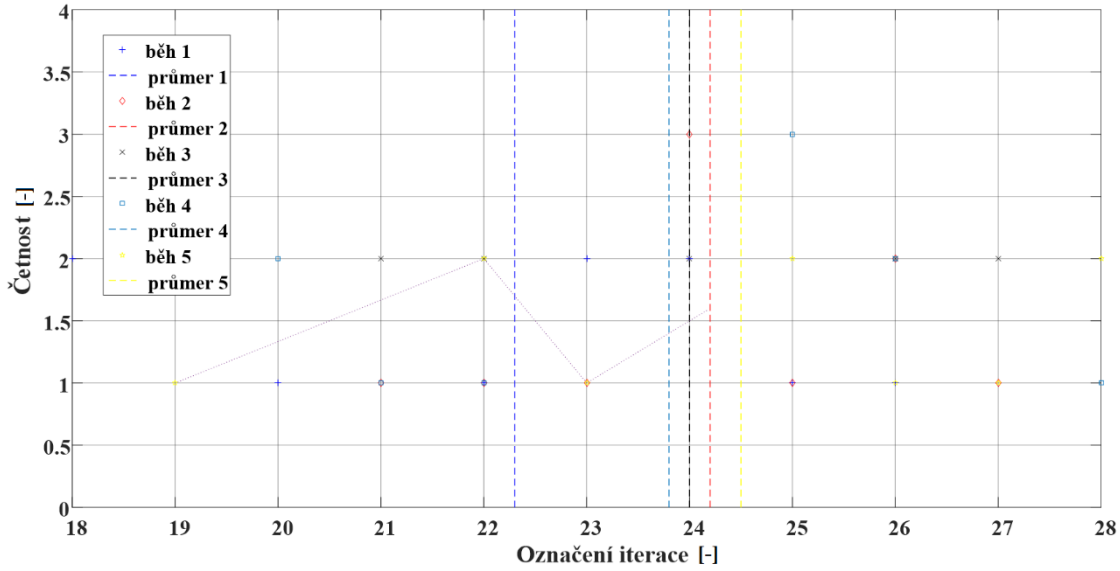


Obrázek 33: Výsledky pro scénář s 10 000 opakováními.

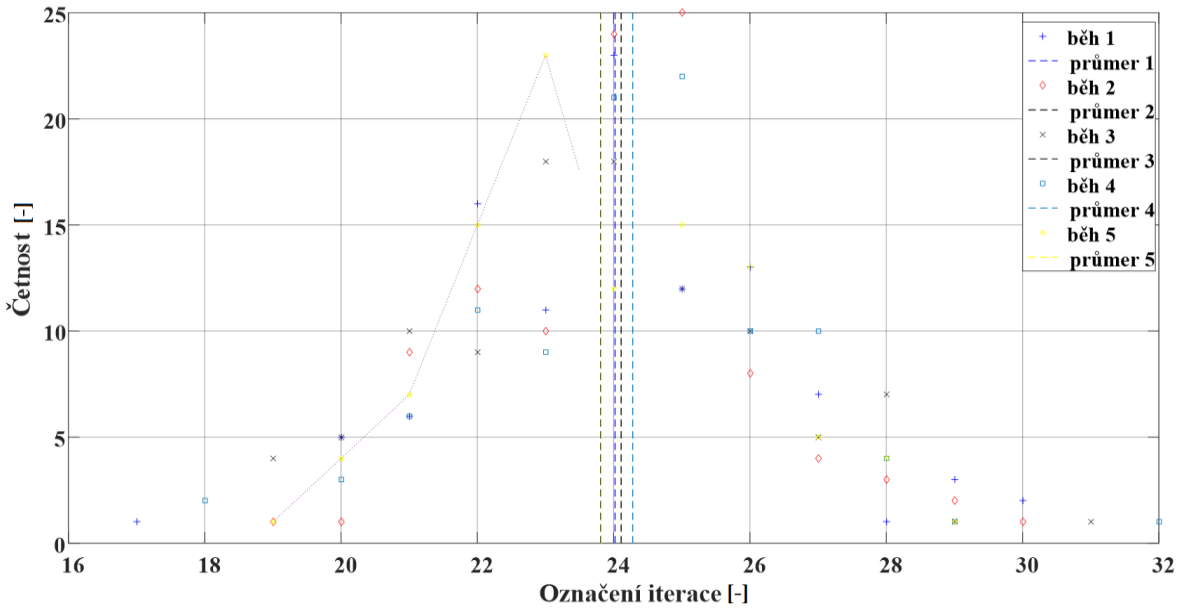


Obrázek 34: Výsledky pro scénář se 100 000 opakováními.

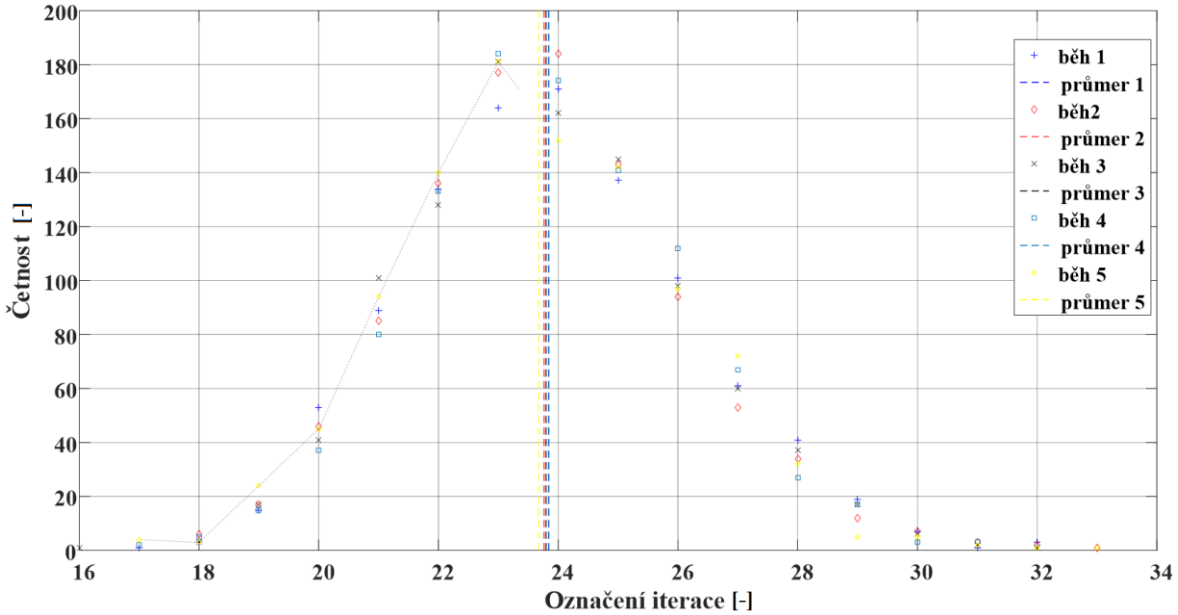
A.2 Výsledky simulace rychlosti konvergence pro silně propojenou topologii sítě



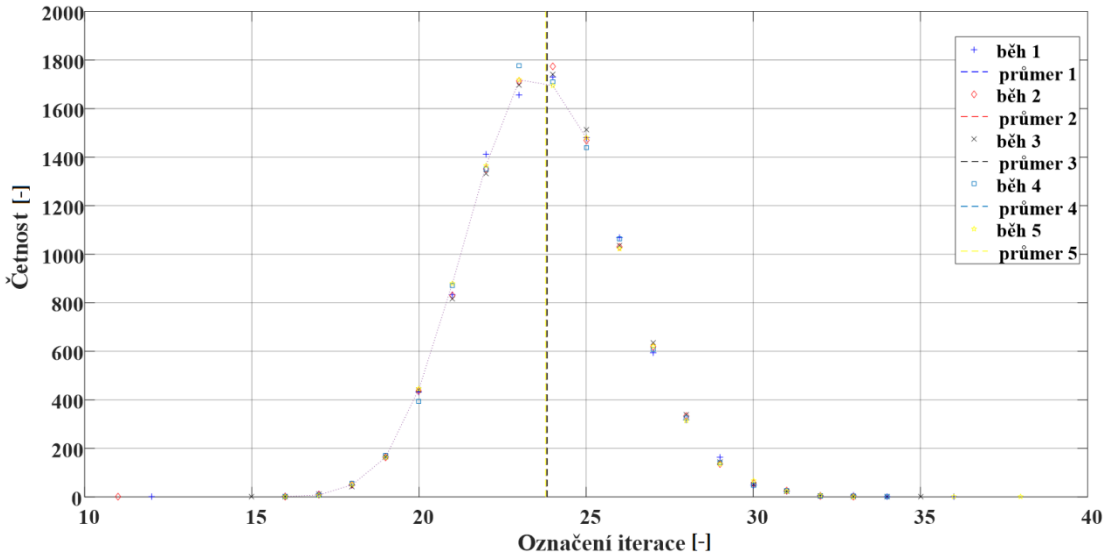
Obrázek 35: Výsledky pro scénář s 10 opakováními.



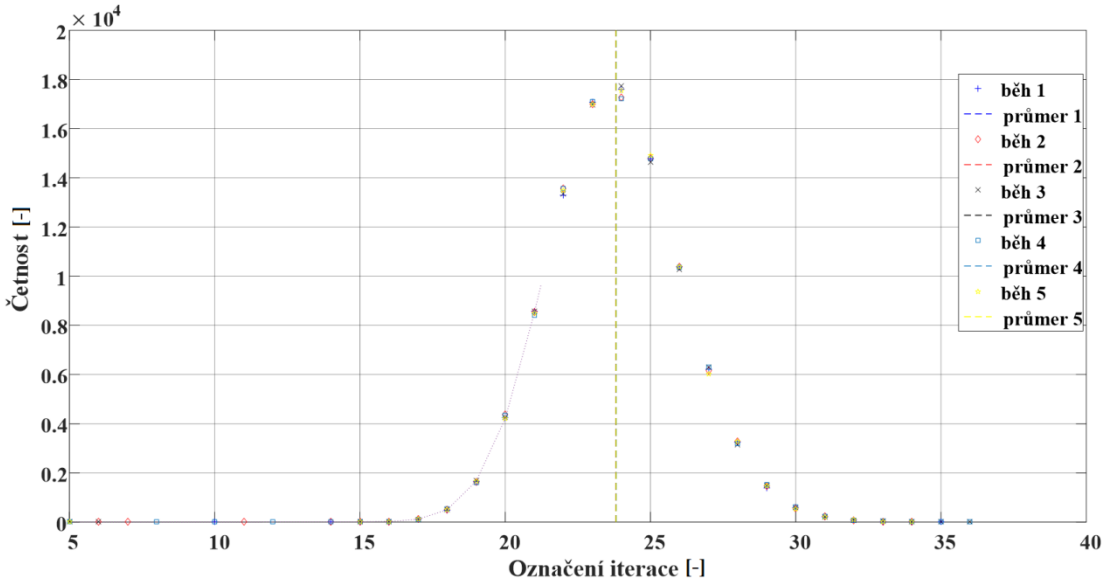
Obrázek 36: Výsledky pro scénář se 100 opakováními.



Obrázek 37: Výsledky pro scénář s 1000 opakováními.

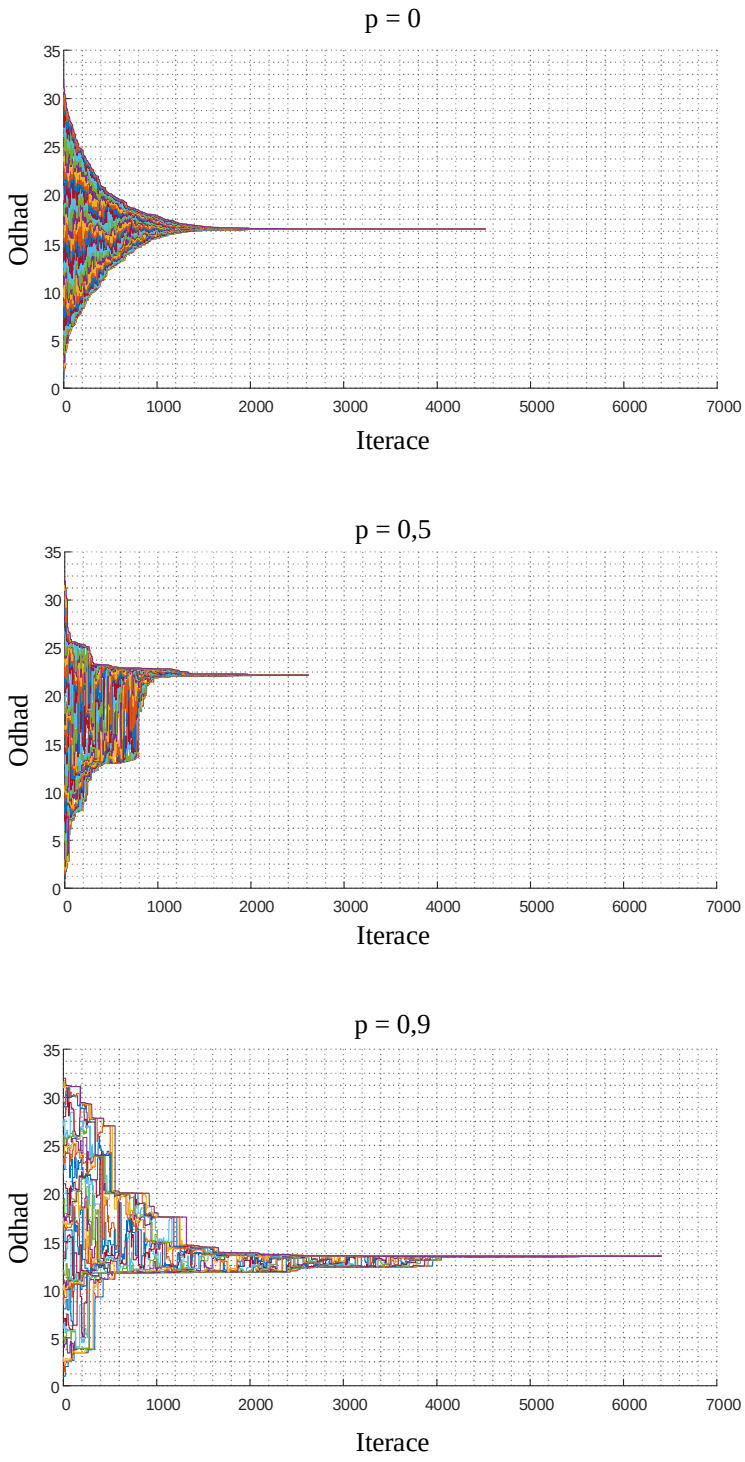


Obrázek 38: Výsledky pro scénář s 10 000 opakováními.

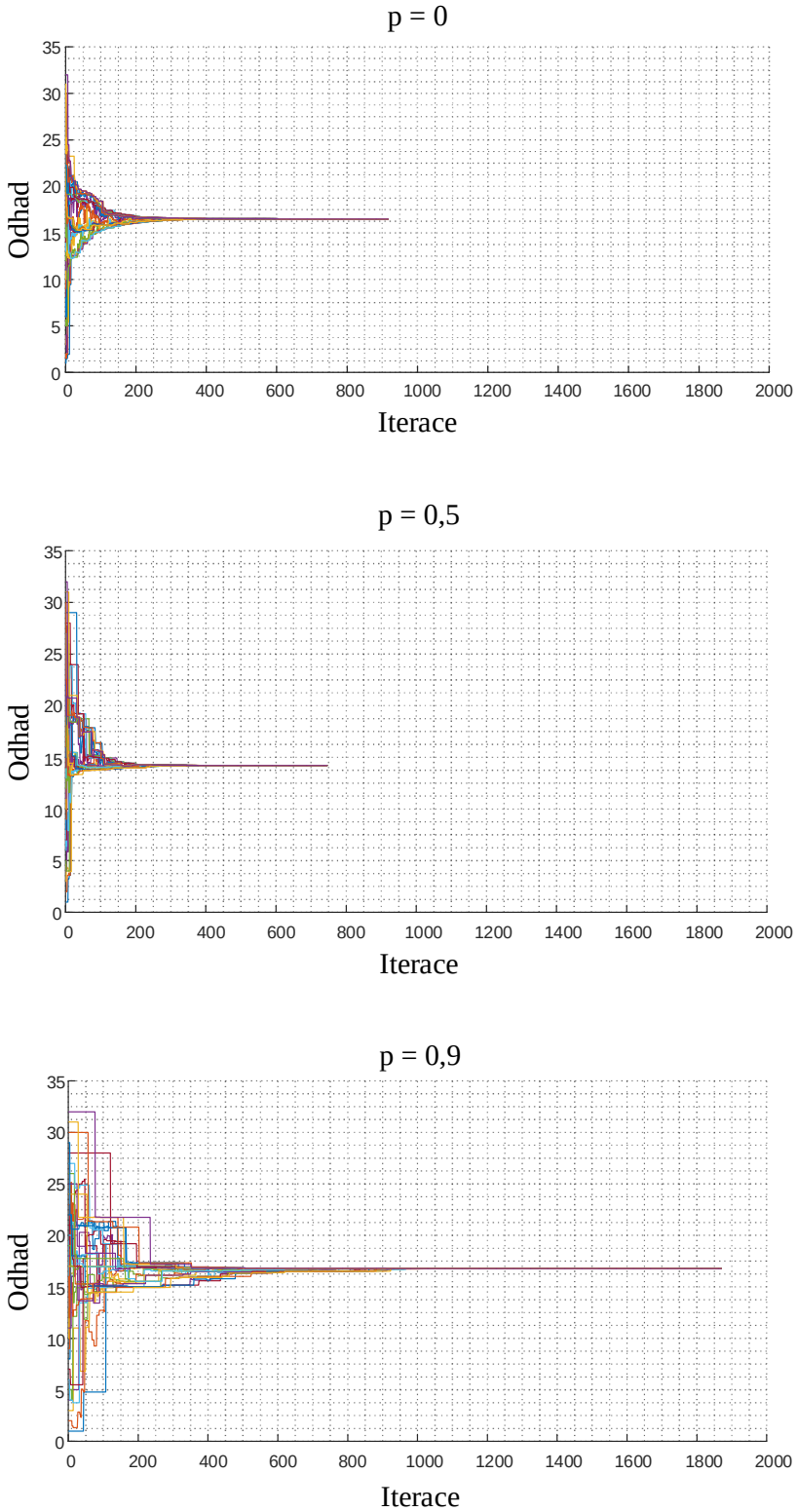


Obrázek 39: Výsledky pro scénář se 100 000 opakováními.

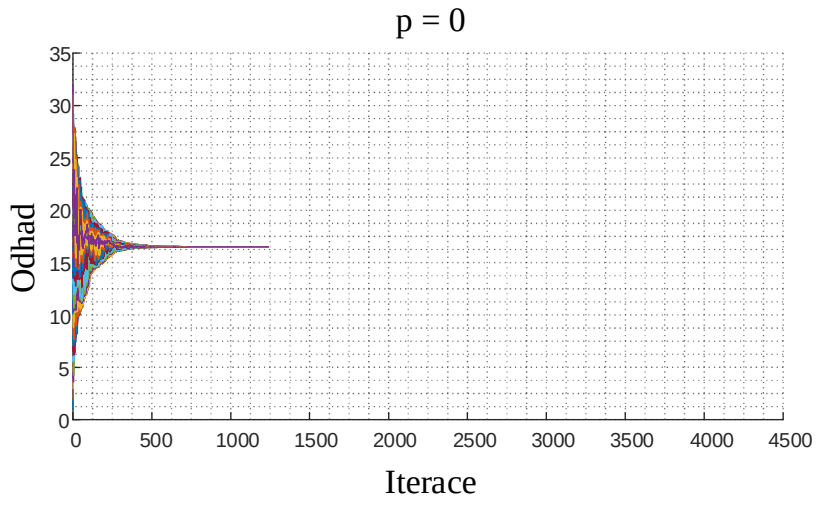
A.3 Výsledky simulace vlivu ztráty zprávy na zvolené topologie v sítích využívajících push-sum protokol

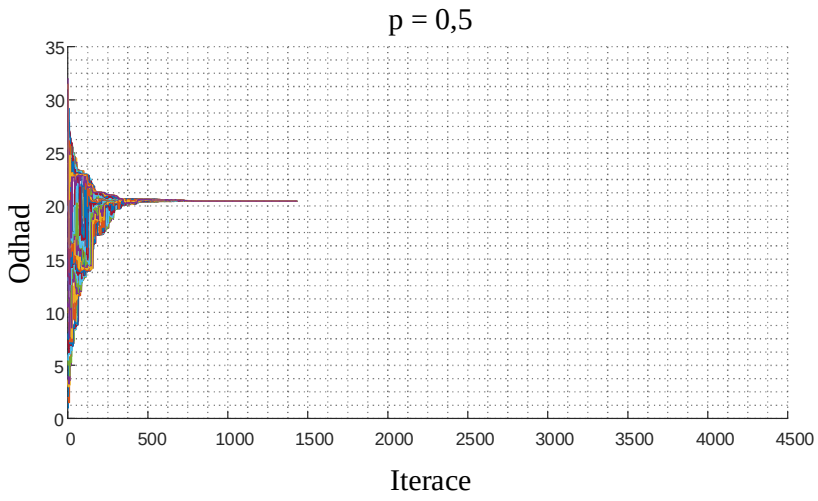


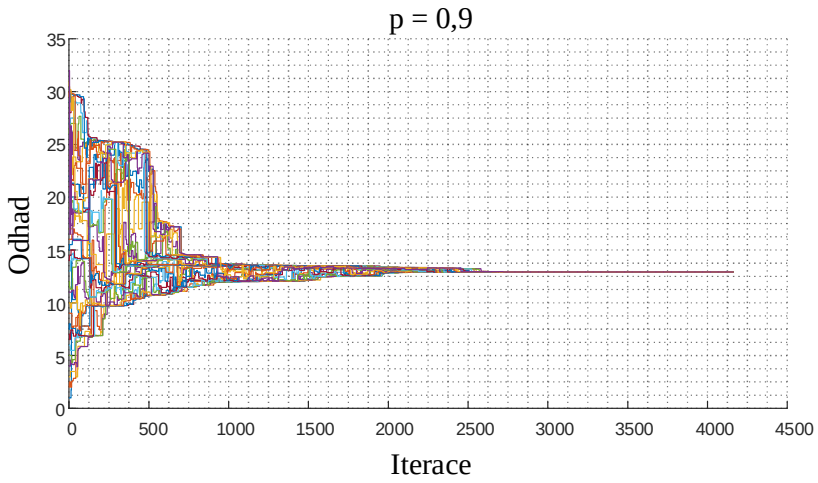
Obrázek 40: Charakter odhadu v linkové topologii pro p = 0, p = 0,5 a p = 0,9.



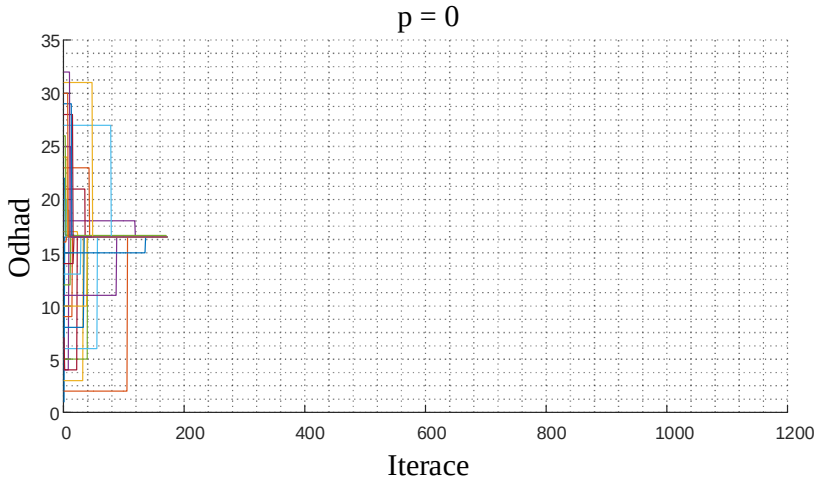
Obrázek 41: Charakter odhadu ve stromové topologii pro p = 0, p = 0,5 a p = 0,9.

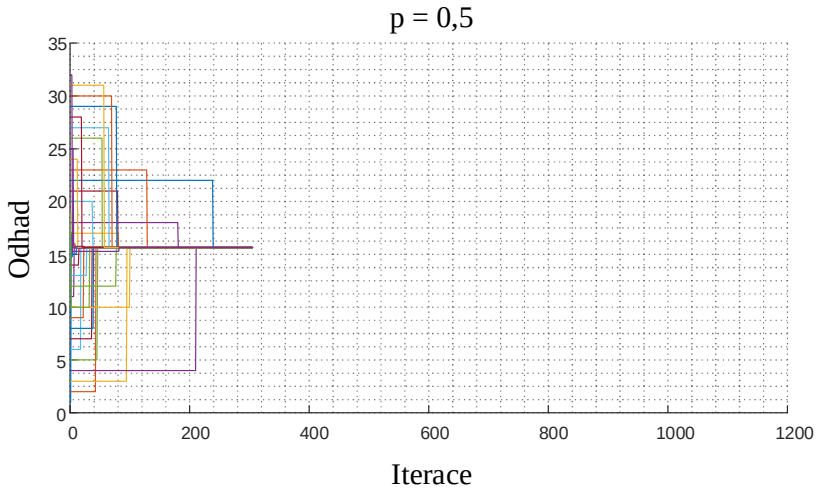


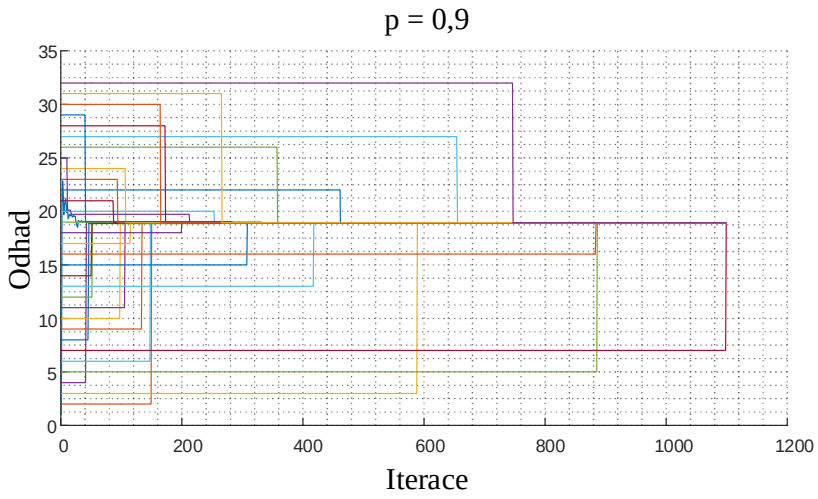




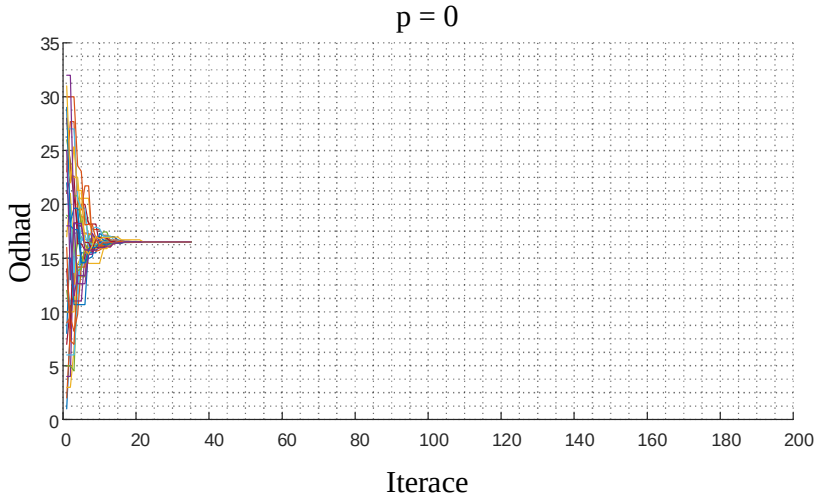
Obrázek 42: Charakter odhadu v kruhové topologii pro p = 0, p = 0,5 a p = 0,9.

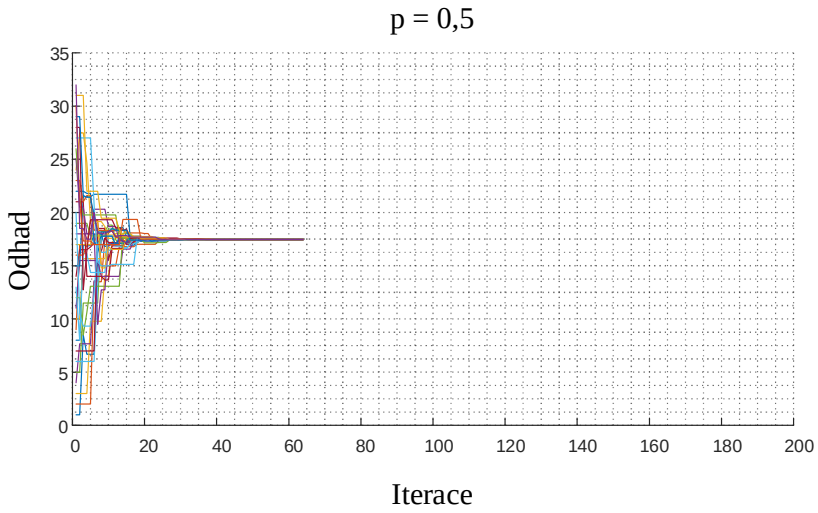


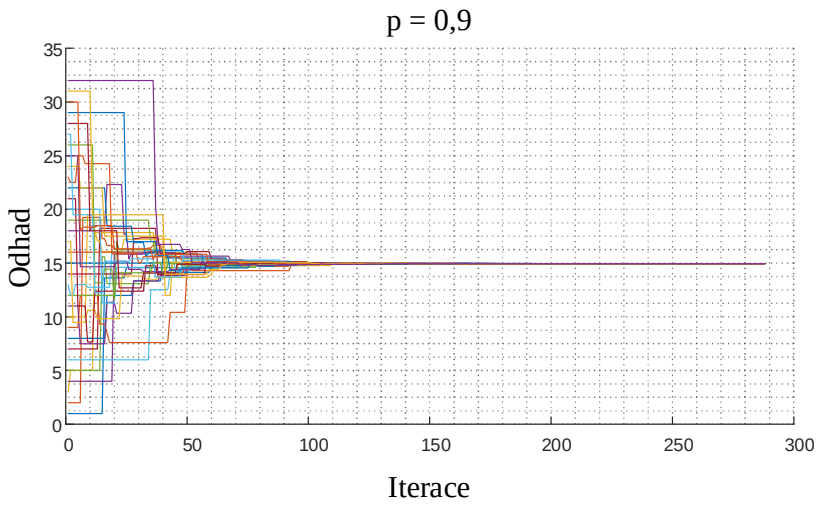




Obrázek 43: Charakter odhadu v topologii hvězdy pro p = 0, p = 0,5 a p = 0,9.







Obrázek 44: Charakter odhadu v plně propojené topologii pro p = 0, p = 0,5 a p = 0,9.

VYBRANÉ PUBLIKACE AUTORA

KENYERES, M., NOVOTNÝ, B. Impact of message losses on push-sum protocol in chosen topologies. *European Scientific Journal,* 2017, roč. 13, č. 7, s. 1-12. ISSN: 1857-7881.

NOVOTNÝ, B. Origin and elimination of interference resulting in coexistence of LTE, DVB-T and SDARS. In *STUDENT EEICT*. Brno: 2017. s. 400-404. ISBN: 978-80-214-5496- 5.

KENYERES, M., NOVOTNÝ, B. Dependency of the Convergence Rate Mean Extent of Variation on the Repetitions Number in Strongly Connected Topologies. In *STUDENT EEICT*. 2016. s. 569-574. ISBN: 978-80-214-5350- 0.

NOVOTNÝ, B., KENYERES, M. Komparace statistické kredibility reprezentanta průměrné rychlosti konvergence protokolu push- sum. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz),* 2016, roč. 18, č. 4, s. 1-4. ISSN: 1213-1539.

KENYERES, M., NOVOTNÝ, B. Dependency of the Convergence Rate Mean Extent of Variation on the Repetitions Number in Weakly Connected Topologies. In *STUDENT EEICT*. 2016. s. 564-568. ISBN: 978-80-214-5350- 0.

AKTIVITY SPOJENÉ SE STUDIEM

Vedené diplomové práce

2016/2017

Adaptace přístupové sítě pro moderní síťové technologie.

Analýza aplikace vysokorychlostní technologie VDSL2.

Simulace SDN sítě.

Využití distribuovaných a stochastických algoritmů v síti.

2015/2016

Vzdálené ovládání zařízení pomocí moderních komunikačních metod.

Analýza provozu bezdrátové sítě.

2014/2015

Multiplatformní brána pro hlasovou komunikaci v reálném čase.

Předcházení útokům na standard 802.11.

2013/2014

Analýza šifrovacích algoritmů ve standardu 802.11.

Útoky na standard 802.11.

Oponentury

2015/2016

Optimalizace síťového provozu pomocí OMNeT++

Vývoj aplikací pro softwarově definované sítě

Analýza konvergovaných sítí pomocí simulací

Návrh SW přepínače pro softwarově definované sítě

2014/2015

Analýza vysokorychlostních sítí zátěžovým testerem

Návrh přepínače využitelného v moderních komunikačních sítích

2013/2014

Návrh softwaru sloužícího k mapování topologie sítě

Bezpečnostní rizika přepínačů

Výuka laboratorních cvičení:

Vysokorychlostní komunikační technologie.

Přístupové a transportní sítě.

Služby transportních sítí.

Správa laboratoře vysokorychlostních komunikačních systémů.

DALŠÍ AKTIVITY

Recenze skript:

Analog Technology for joint teaching programme of BUT and VSB-TUO, Koton, J. a Herencsár, N. pro projekt č. CZ.1.07/2.2.00/28.0062

Tvroba multimediálních výukových materiálů pro předmět BPTS a KPTS, 2014. garant Doc. Ing. Vladislav Škorpil, CSc. (12 přednášek).