České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

OPTIMALIZACE VYUŽITÍ VÍCE CEST KE ZVÝŠENÍ ROBUSTNOSTI PŘENOSU DAT

Disertační práce

Ing. Petr Chlumský

Září 2014

Doktorský studijní program: Elektrotechnika a informatika
Studijní obor: Telekomunikační technika

Školitel: doc. Ing. Jiří Vodrážka, Ph.D.

Poděkování

Děkuji svému školiteli doc. Ing. Jiřímu Vodrážkovi, Ph.D. za jeho podnětné rady a celkové vedení v průběhu celého mého doktorského studia. Také děkuji Ing. Zbyňkovi Kocurovi, Ph.D. za jeho cenné rady a připomínky. Děkuji také své rodině a přítelkyni Pavlíně za podporu během mých studií.

Prohlášení

Prohlašuji, že jsem tuto disertační práci vypracoval samostatně, pouze za odborného vedení svého školitele doc. Ing. Jiřího Vodrážky, Ph.D. Dále prohlašuji, že veškeré podklady a zdroje, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Abstrakt

Tato disertační práce se zabývá optimalizací využití více přenosových cest za účelem navýšení robustnosti přenosu dat. Podstata práce je v navrženém schématu přenosu dat, které využívá principy z oblasti síťového kódování pro dosažení možnosti rekonstrukce chybných dat. Pomocí určitého způsobu kombinace dat a pomocí specifické logiky dekodéru je možné obnovit na přijímací straně jistou část chybně doručených dat bez použití retransmise. Navržené schéma pracuje mezi koncovými body komunikace a je plně transparentní, nezávislé na mezilehlých bodech komunikace. Navržené schéma bylo implementováno a otestováno pomocí simulačního nástroje OMNeT++. Součástí práce je vyhodnocení z pohledu robustnosti a zpoždění přenosu dat a také porovnání vůči dalším schématům přenosu, která využívají více přenosových cest.

Klíčová slova

schéma přenosu dat; vícecestný přenos dat; síťové kódování; robustnost přenosu

Abstrakt

This doctoral thesis deals with optimization of the use of multiple transmission paths in order to increase robustness of data transmission. The essence of the research is the transmission scheme proposal which uses principles from the network coding field to achieve the possibility of erroneous data reconstruction. With a particular method of data combining and using specific decoder logic, the proposed scheme is able to recover some erroneous data without any retransmissions. The scheme is designed as end-to-end and is fully transparent, independent on the intermediate communication nodes. The proposed scheme was implemented and tested by simulation framework OMNeT++. The evaluation of the scheme in terms of robustness and delay is part of the thesis as well as the comparison with other multipath data transmission schemes.

Keywords

transmission scheme; multipath transmission; network coding; robustness of transmission

Obsah

Zkratky

ACK	Acknowledgement
ARQ	Automatic Repeat reQuest
AWGN	Additive White Gaussian Noise
BCH	Bose, Chadhuri, Hocquenqham kód
BER	Bit Error Rate
CRC	Cyclic Redundancy Check
CWND	Congestion Window
EDGE	Enhanced Data rates for GSM Evolution
FEC	Forward Error Correction
FIFO	First In, First Out
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LLC	Logical Link Control
MIMO	Multiple-Input Multiple-Output
NAK	Negative Acknowledgement
NED	Network Description
OFDM	Orthogonal Frequency Division Multiplexing
PER	Packet Error Rate
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-shift Keying
RFC	Request for Comments
RM OSI	Reference Model Open Systems Interconnection
RSC	Recursive Systematic Coder
SNR	Signal-to-Noise Ratio
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over IP
XOR	Exkluzivní disjunkce
2G	Second Generation of Mobile Telecommunications Technology
3G	Third Generation of Mobile Telecommunications Technology

Symboly

z Hammingova vzdálenost
E_d počet chyb, které může kód detekovat
E_c počet chyb, které může kód opravit
k_c délka vstupního bloku
n_c délka zakódovaného bloku
R_c kódový poměr
$p_{A,B}$ pravděpodobnost chyby na cestě AB
$p_{B,C}$ pravděpodobnost chyby na cestě BC
R_{FEC}, R_{NC} propustnosti mezi koncovými body
v_t přenosová rychlost
f_n funkce pro kombinaci n paketů
X_n n vstupních toků
$\oplus$ exkluzivní disjunkce
l_{p_i} délka paketu
t_p interval mezi příchody paketů do kodéru
$Q_{c_{0,1}}$ fronty kodéru
$t_{Q_{c_{0,1}}}$ interval výběru paketů z front $Q_{c_{0,1}}$
$l_{Q_{c_{0,1}}}$ délky front kodéru
Q_{d_0} fronta dekodéru
$l_{Q_{d_0}}$ délka fronty dekodéru
k délka kódu schématu
N počet přenosových kanálů
D_i^N i-tý přímý, originální paket N-tého kanálu
X_j^N j-tý xorovaný, kombinovaný paket N-tého kanálu
m, n nezbytné počty paketů pro realizaci kódování
$M_{c_{0,1}}$ multiplikační blok kodéru
$M_{d_{0,1}}$ multiplikační blok dekodéru
$\alpha_{M_{c_{0,1}}}$ koeficient multiplikace bloku v kodéru
$\alpha_{M_{d_{0,1}}}$ koeficient multiplikace bloku v dekodéru
$R_{c_{0,1}}$ registry paketů kodéru
$R_{d_{0,1}}$ registry paketů dekodéru
d hloubka prokladače
$Q_{c_N}^{out}$ výstupní fronty kodéru
$t_{c_N}^{out}$ intervaly odesílání paketů z kodéru
P_N pravděpodobnost chyby paketu na N-tém kanálu
$Q_{d_N}^{in}$ vstupní fronty dekodéru

$t_{d_N}^{in}$ intervaly příchodu paketů z jednotlivých kanálů

Q_X dekódovací fronta

l_{Q_X} délka dekódovací fronty

t_e maximální čas mazání zastaralých paketů

t_s maximální čas čekání na doručení paketů

t_d^{out} interval odchodů paketů z dekodéru

P_d^{out} celková chybovost paketů

P_{se} pravděpodobnost chyby symbolu

M počet stavů modulace

R_s odstup signálu od šumu

b počet bitů na symbol

E_b střední energie signálu na bit

N_0 spektrální výkonová hustota šumu

P_{eb} bitová chybovost

P_{ep} paketová chybovost

P_b pravděpodobnost bitové chyby

P_p pravděpodobnost paketové chyby

m_e počet chybně přijatých bitů

t_m celková doba měření

p_i pravděpodobnost chyby paketu na kanálu i

p_m pravděpodobnost chyby u systému inverzního multiplexu

p_z pravděpodobnost chyby u systému zálohování

p_r pravděpodobnost doručení všech paketů u navrženého systému

r počet originálních paketů

t_μ střední hodnota zpoždění paketů navrženým kódováním

N_o celkový počet odeslaných paketů

γ_i pravděpodobnost, že nastane situace vhodná pro daný typ obnovy i

η_i počet korektně doručených paketů η_0 a paketů prošlých určitou variantou obnovy $\eta_{1,2,3}$

t_i zpoždění paketu pro daný typ obnovy i

t_a souhrn zpoždění při převodu informace na pakety

t_b zpoždění ve frontách

t_c procesní zpoždění při kódování podle schématu přenosu

t_x souhrn zpoždění v mezilehlých bodech komunikace

t_z celkové zpoždění

t_d serializační zpoždění

t_{tx} propagační zpoždění

$t_{pr_{0,1,2}}$ procesní zpoždění, index označuje počet XOR operací

v rychlost šíření signálu
s vzdálenost mezi odesílací a přijímací stranou
n_d index lomu
c rychlost světla ve vakuu
ε_r relativní permitivita
R_v procento paketů dané varianty obnovy
$\overline{t_z}$ průměrné celkové zpoždění paketů
t_r celkový čas přenosu souboru dat
t_f čas přenosu bez retransmisí
e_n počet chybných paketů
R_r poměr retransmisí
R_e procento chybných paketů
R_p procento přijatých paketů
ρ korelační koeficient
$K_{0,1,2}$ náhodné veličiny
ω účinnost korekce
N_x počet obnovených a korektně doručených paketů

1 Úvod

Optimalizace přenosu dat je důležitou součástí rozvoje informačních technologií i v dnešní době, kdy datová propustnost přenosových technologií dosahuje desítek gigabitů za sekundu. S rostoucí rychlostí přenosu dat se totiž zároveň zvyšují nároky samotných uživatelů a nelze proto plýtvat dostupnými fyzickými prostředky. V řadě situací navíc nejrychlejší přenosové technologie nejsou dostupné nebo využitelné a proto je důležité pokračovat v procesu optimalizace přenosu dat k získání efektivních řešení. Tato práce se zaměřuje na optimalizaci přenosu dat v systémech, kde je k dispozici více přenosových cest zároveň. Tyto přenosové cesty mohou být metalické, optické i bezdrátové. Práce se zabývá možnostmi využití těchto cest z pohledu maximalizace spolehlivosti přenosu při použití principů síťového kódování. Součástí je i využití přenosových cest s různými pravděpodobnostmi chyby přenosu dat pramenícími z použití různě odolných modulačních schémat.

Přenosové systémy s více přenosovými cestami nabízejí možnost specifického využití těchto cest s ohledem na nároky zajišťovaných služeb. Při práci na řešení projektu, který se zabýval přenosem dat po více přenosových cestách, jsme narazili na problém jak optimálně využít tyto cesty z pohledu odolnosti přenosu dat.

Předložená práce se zabývá optimalizací využití více přenosových cest ke zvýšení robustnosti přenosu dat. Navrhuje obecný systém přenosu, který umožňuje variabilní nastavení parametrů jednotlivých komponent systému tak, aby systém vyhovoval požadavkům služeb na něm provozovaných. Zaměřuje se pak na specifické schéma přenosu dat, s cílem zajistit vyšší spolehlivost přenosu. Navržený obecný systém se sestává z kodéru a dekodéru, jejichž jednotlivé součásti a logika funkce je v práci popsána. Při zvolení konkrétních parametrů je dosaženo přesného schématu přenosu, řídícího se určitými pravidly. Konkrétní specifikace schématu je součástí práce. Toto schéma je zaměřeno na dosažení vyšší spolehlivosti přenosu při využití dvou přenosových cest. Využívá jednoho ze základních principů síťového kódování - zásah do samotných přenášených dat, včetně uživatelské části dat. Pomocí vzájemného kombinování přenášených dat v kodéru na straně odesílatele a pomocí specifické logiky dekodéru na přijímací straně, je umožněno obnovit chybně doručená či chybějící data. Počet obnovitelných bloků

dat a způsob jejich obnovy je v práci podrobně popsán. Toto přenosové schéma je plně transparentní vůči systémům, které propojuje. Zabezpečuje spojení typu konec-konec, je tedy nezávislé na mezilehlých bodech komunikace.

Konkrétní navržené schéma přenosu dat je dále analyzováno z pohledu celkové chybovosti přenosu a je porovnáváno s obvykle používanými schématy přenosu dat po více cestách: zálohováním a inverzní multiplexací. Dále je analyzován vliv navržené obnovy dat z pohledu přidaného zpoždění přenosu. Diskutován je také vliv retransmisí na zpoždění přenosu při jejich využití u porovnávaných schémat, za účelem navýšení jejich robustnosti. Pro simulace ověřující robustnost navrženého schématu byla také využita data z měření v reálných provozních podmínkách českých mobilních sítí.

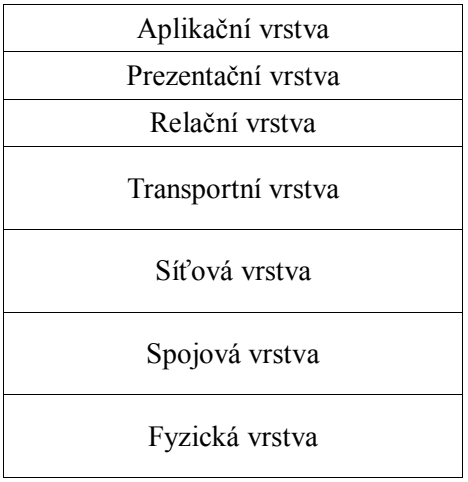
Jednotlivé kapitoly této disertační práce jsou řazeny následovně. Kapitola 2 popisuje současný stav řešené problematiky a témata související s obsahem práce. Kapitola 3 obsahuje cíle disertační práce. V kapitole 4 jsou shrnuty použité metody a nástroje použité při řešení této práce. Kapitola 5 popisuje nejprve navržený systém přenosu dat z obecného pohledu a následně je popsáno konkrétní přenosové schéma vycházející z obecného návrhu. Analýza navrženého schématu z pohledu celkové chobovosti přenosu dat a z pohledu zpoždění přenosu je obsahem kapitoly 6. Součástí této kapitoly je i porovnání s dalšími schématy přenosu dat po více cestách. Kapitola 7 se zabývá využitím naměřených dat v rámci simulací navrženého schématu a porovnáním se schématem zálohování. Závěr a diskuze splnění cílů práce je v kapitole 8.

2 Současný stav řešené problematiky

Existují různé způsoby jak přistupovat k problému minimalizace množství přenosových chyb, které lze v určitých případech i vhodně kombinovat. Hlavními skupinami kanálového kódování jsou systémy dopředné korekce chyb FEC (Forward Error Correction) a zpětnovazební systémy ARQ (Automatic Repeat reQuest). Skupina zpětnovazebních systémů je založena na opakovaném zasílání poškozených či nedoručených dat [1][2]. Systémy dopředné korekce, které lze dále dělit na blokové a konvoluční kódy, spoléhají na přidání redundance k přenášeným datům [3]. Cílem kanálového kódování je zabezpečit signál proti chybám vznikajícím při přenosu v komunikačním kanálu. Chyby při přenosu mohou být způsobeny šumem, různými druhy rušení, únikem signálu, odrazy, ale i přeplněním front v síťových prvcích. Zcela jiným způsobem, který spoléhá na zkvalitnění příjmu dat samotných, je technologie MIMO (Multiple-Input Multiple-Output), která využívá více antén na straně přijímače i vysílače za účelem možnosti využití vícecestného šíření [4]. Obecně je využití více paralelních přenosových kanálů další oblastí, kterou lze využít k dosažení vyšší celkové robustnosti přenosu.

K rozdělení jednotlivých technik zabezpečení přenosu dat proti chybám lze přistoupit z pohledu jednotlivých vrstev RM OSI (Reference Model Open Systems Interconnection) [5], které jsou zobrazeny na obrázku 1. Na fyzické vrstvě se využívají základní techniky níže více popsané, tedy dopředná korekce chyb, prokládání a další [6]. Do této vrstvy patří i diverzitní technologie MIMO (Multiple-Input Multiple-Output), která v případě využití rádiových přenosových cest využívá vícecestné šíření signálu pomocí dvou a více antén na vysílací i přijímací straně bezdrátové komunikace. Tato technologie využívá dva zásadní principy: prostorová diverzita (snižuje pravděpodobnost chyby přenosu) a prostorovou multiplexaci (zvyšuje přenosovou rychlost) [4][7]. Jako příklad optimalizačních technik mezi fyzickou a spojovou vrstvou lze zmínit dynamické přiřazování subnosných OFDM (Orthogonal Frequency Division Multiplexing) [8], či potlačení interferencí u bezdrátových sítí se smíšenou topologií [9].

Spojová vrstva, jakožto vrstva zaručující spolehlivé spojení mezi sousedními



Obrázek 1 Referenční model OSI

body, respektive její podvrstva LLC (Logical Link Control), je místem speciálně určeným pro kontrolu a případnou opravu chyb [10]. Aplikují se zde dále rozebírané způsoby zabezpečení, detekce i korekce chyb. Optimalizace na spojové vrstvě jsou obvykle založeny na určitém druhu přizpůsobení ve snaze upravit parametry použitého protokolu vzhledem k aktuálnímu stavu sítě [11], nebo na úpravě plánovacího mechanismu [12][13]. Objevují se také projekty přidávající funkcionalitu mezi vrstvy spojovou a síťovou, jako například zajímavý projekt COPE [14]. COPE architektura vylepšuje propustnost pomocí implementace nové podvrstvy mezi spojovou a síťovou vrstvu, která využívá všesměrové podstaty vysílání na bezdrátovém médiu. Ta umožňuje sousedním bodům komunikace zaslechnout paket, který je vysílán, což umožňuje dříve zkompletovat přenášený objem dat [15].

Síťová vrstva není běžně pro zabezpečení přenosu používána. Různé práce zaměřené na optimalizaci na síťové vrstvě zahrnují nové směrovací metody, jako je například rozprostřené směrování [16]. Na rozdíl od běžného směrování, které směruje zprávu po určité cestě mezi zdrojem a cílem, tento mechanismus rozdělí zprávu na menší díly a rozposílá je více cestami napříč sítí. Oproti fyzické a spojové vrstvě, které se orientují na spojení mezi sousedními body, je síťová vrstva zaměřena na spojení mezi koncovými body napříč sítí propojených bodů. Právě na tuto vrstvu se zaměřuje tato disertační práce, jakožto na místo s potenciálem přínosu vyšší odolnosti přenosu. Vzhledem k nezávislosti jednotlivých vrstev bude stále možné využívat i další bezpečnostní metody, tedy kanálové kódování nižších vrstev a opravné mechanismy vyšších vrstev.

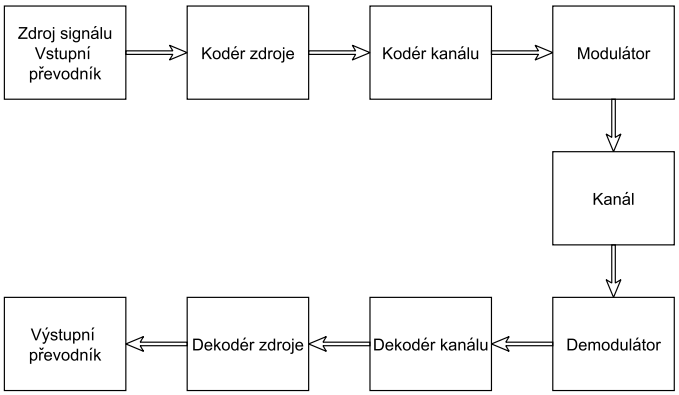
Transportní vrstva zajišťuje doručování celých bloků dat a zajišťuje kontrolu, opravu chyb i doručování dat ve správném pořadí. Jejím hlavním mechanismem je

opětovné zasílání dat. Spolehlivost doručování je závislá na použitém protokolu. UDP (User Datagram Protocol) [17] spolehlivé doručování nezajišťuje, odesílatel tedy neví, v jakém stavu a pokud vůbec byla data doručena. Pokud přijímací strana zjistí chybu pomocí kontrolního součtu, je datagram zahozen bez jakékoliv další akce [10]. Naproti tomu spolehlivý protokol TCP (Transmission Control Protocol) [18] udržuje spojení mezi koncovými body, potvrzuje korektně doručené segmenty dat a zajišťuje opětovné zaslání dat v případě chyby (využívá zpětnovazební systém, konkrétní podoba je nicméně závislá na dané variantě protokolu TCP).

Vyšší vrstvy RM OSI nejsou z pohledu robustnosti přenosu zásadní, možnosti pro realizace dalšího zabezpečení v aplikační vrstvě souvisí vždy s konkrétní aplikací a použité metody zabezpečení tedy nejsou obecně použitelné.

2.1 Bezpečnostní kódy

V následujících částech kapitoly 2 jsou popsány základní techniky, které ovlivňují odolnost přenosu dat. Z pohledu obecného schématu komunikačního kanálu, naznačeného na obrázku 2, se tato část zaměřuje na kódování kanálové. Následně jsou popsány techniky, které mají přímou souvislost s obsahem této práce a taktéž ovlivňují odolnost přenosu dat.



Obrázek 2 Obecné schéma komunikačního systému [19].

K zabezpečení dat za účelem dosažení snížení chybovosti, či ke sledování zda chyba nastala, se využívá přidání určité nadbytečné informace do přenášených dat. Tato informace je přidávána podle přesně definovaných zákonitostí a zvyšuje redundanci. Na přijímací straně se kontroluje splnění zmíněných závislostí a redundantní část je odstraněna [20].

Kanálové kódy lze dělit do dvou hlavních skupin [21]:

- *Detekční kódy*, které dokáží detekovat jednu, či více chyb (chybných bitů). Nedokáží ale zajistit jejich opravu ani určit jejich přesnou pozici v bloku dat.
- *Korekční kódy*, které umožňují určit pozici detekovaných chyb v bloku dat a část, případně všechny chyby i opravit.

2.1.1 Hammingova vzdálenost

Schopnost kódu detekovat, nebo opravit zabezpečený blok dat úzce souvisí s pojmem Hammingovy vzdálenosti. Což je počet symbolů (bitů) z v nichž se dva kódové bloky liší. Minimální Hammingova vzdálenost z_{min} kódu je nejmenší Hammingova vzdálenost mezi libovolnými dvěma kódovými bloky [21]. Poté pokud E_d je počet chyb, které může kód detekovat, E_c počet chyb, které může kód opravit, platí následující vztahy [20]:

Počet detekovatelných chyb:

$$E_d \leq z_{min} - 1. \tag{1}$$

Počet opravitelných chyb:

$$E_c \leq \frac{1}{2}(z_{min} - 1), pro\ z_{min}\ liché \tag{2}$$

$$E_c \leq \frac{1}{2}(z_{min} - 2), pro\ z_{min}\ sudé. \tag{3}$$

2.1.2 Blokové a konvoluční kódy

Korekční kódy lze dále dělit podle způsobu vkládání kontrolních prvků do zabezpečované zprávy na blokové a konvoluční.

- *Blokové kódy* rozdělují v kodéru sekvenci informací na jednotlivé bloky o délce k_c bitů. Každému bloku je pak přiřazen zakódovaný blok o n_c bitech, který se skládá ze vstupního bloku a paritní bitové skupiny (o délce $(n_c - k_c)$). Aktuální výstupní kódový blok je odvozen pouze od jediného jemu odpovídajícímu vstupnímu bloku, kodér tedy nemá paměť [21].
- *Konvoluční kódy* přijímají kódové sekvence o délce k_c bitů a produkují výstupní sekvence délky n_c. Zakódované bloky ale nezávisí pouze na odpovídající vstupní sekvenci, ale i na m_c předcházejících blocích dat. Kodér má tedy, narozdíl od předchozího případu, paměť o délce m [22].

S výše zmíněnými proměnnými se pojí důležitý parametr kódu a to kódový poměr definovaný vztahem $R_c = \frac{k_c}{n_c}$. Čím více se kódový poměr blíž k nule, tím k větší redundanci a ochraně dat v kodéru dochází.

Dalším možným dělením je systematičnost kódu. Systematické kódy se vyznačují možností ve výstupním kódovém bloku oddělit původní (informační) část od části kontrolní. U nesystematických kódů toto možné není.

K systematickým blokovým kódům patří například cyklické kódy, konkrétně často využívaná metoda k detekci chyb CRC (Cyclic Redundancy Check). Její zabezpečení lze realizovat zpětnovazebním posuvným registrem, jehož struktura zpětných vazeb je plně určena zvoleným generujícím mnohočlenem. Stupeň generujícího mnohočlenu ovlivňuje zabezpečující schopnost kódu. Dalšími často využívanými kódy jsou Reed-Solomonovy kódy, které jsou zvláštním případem BCH (Bose, Chadhuri, Hocquenqham) kódů. Nepracují s jednotlivými bity, ale s bitovými sekvencemi. Jejich důležitou vlastností je, že jsou vhodné pro korekci shluků chyb. Tyto kódy jsou využívány pro svou vysokou účinnost při nízké redundanci [6].

2.1.3 Prokládání

Pro řešení rozsáhlejších shluků chyb se používá kromě korekčních kódů také jejich kombinace s prokládáním. Posloupnost bitů je na vysílací straně vhodným způsobem přeskupena a v přijímači, pomocí inverzního prokladače, opět vrácena nazpět. Shluk chyb, který při přenosu ovlivnil souvislou část dat, je tak převeden na osamocené chyby, které korekční kódy dokáží lépe opravit. Existují dva základní typy prokládání: blokové a konvoluční. Při blokovém prokládání jsou bity ukládány do binární prokládací matice po řádcích. Po uložení se bity čtou a odesílají po sloupcích. Efektivnější konvoluční prokládání je založeno na vkládání přenášených bitů do matice po diagonálách a čtení probíhá po sloupcích [21]. Počet kódových slov v matici určuje hloubku prokladače, která udává schopnost rozprostřít data.

2.1.4 Turbo kódy

Významnými kódy, které byly objeveny v 90. letech 20. století a poprvé publikovány v [23], jsou turbo kódy. Jsou to kódy vykazující velký kódový zisk a to při relativně jednoduché realizaci. Díky svým vlastnostem mohou tyto kódy zajistit nízkou chybovost při nízkých hodnotách odstupu signálu od šumu. Základní princip je založen na využití dvou zřetězených konvolučních kodérech RSC (Recursive Systematic Coder) spojených prokladačem. Podrobnější popis lze nalézt například v [6].

2.1.5 Automatické opakování přenosu ARQ

Všechny zmíněné kódy patří do velké skupiny označované jako kódy s dopřednou korekcí chyb uváděné pod zkratkou FEC (Forward Error Correction). Podstatou všech těchto kódů je přidání určité redundantní informace k přenášeným datům na straně odesílatele. Na straně příjemce pak dochází k detekci, či k opravě chyb díky této přidané redundanci. Zcela jiným způsobem k oblasti zabezpečení přistupují metody založené na automatickém opakování přenosu na základě žádosti, tedy ARQ (Automatic Repeat reQuest). Při této metodě se při zjištění chyby systém nespoléhá na schopnosti opravného kódu, ale vyžádá si opakované zaslání chybných dat. Potřebuje k tomu tedy kanál pro možnost komunikace i v opačném směru. Samotná detekce chyb je ovšem méně složitá než korekce chyb.

Jednotlivých implementací ARQ je více druhů s různými vlastnostmi a nároky (obzvláště paměťové). Mezi hlavní varianty lze zařadit následující tři [6][10]:

- *Stop-and-Wait*, nejjednodušší varianta ARQ s jednotlivým potvrzováním. Odesílatel odešle data a čeká na odpověď příjemce. Ten v případě přijetí dat provede kontrolu pomocí CRC a v případě bezchybného přenosu potvrdí daný blok dat pomocí potvrzení ACK (Acknowledgement) a odesílatel může pokračovat dalším blokem dat. V případě chyby vyšle příjemce negativní potvrzení NAK (Negative Acknowledgement). Pokud ACK nedorazí v určitém čase, nebo přijde NAK, odesílatel posílá stejný blok dat znovu.

- *Go-Back-N*, je varianta efektivnějšího kontinuálního přenosu, konkrétně opakování s návratem, při kterém odesílatel plynule posílá bloky dat, bez čekání na potvrzení. Využívá takzvaného posuvného okénka, jehož velikost ("N"v názvu) musí být vybrána s ohledem na parametry daného systému. V případě chyby odešle příjemce NAK. Chybný blok dat, i všechny následující, jsou zahozeny a odesílatel zasílá od chybného bloku dat vše znovu.

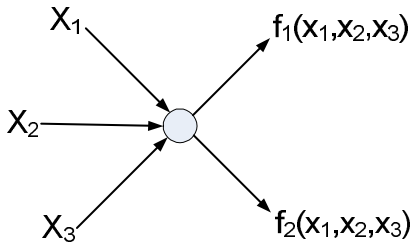
- *Selective Repeat*, tedy selektivní opakování, vylepšuje efektivitu využití přenosového kanálu oproti předchozí metodě. Činí tak pomocí opakování pouze chybně doručených dat. Informace, který blok je chybný, je součástí zprávy NAK.

Existují i varianty kombinující přístup dopředné korekce chyb s metodami ARQ, takzvané Hybrid ARQ. Princip je založen na opravě co největšího množství chyb tak, aby bylo nutné opakovat posílání co nejmenšího množství dat [24].

2.2 Síťové kódování

2.2.1 Úvod

Síťové kódování je nová technika představená na přelomu tisíciletí s potenciálem k zlepšení propustnosti dat, zvýšení robustnosti datového přenosu a k hospodárnějšímu nakládání s bezdrátovými prostředky. V běžných komunikačních sítích se předpokládá, že nezávislé datové toky mohou sdílet zdroje, ale informace jako taková je brána jako nedělitelný celek. Síťové kódování tento zažitý předpoklad narušuje tím, že síťové prvky mohou místo pouze obvyklého přeposílání dat zkombinovat funkcí f_n několik paketů z vstupních datových toků X_n do jednoho či několika odchozích paketů [25]. Obrázek 3 zobrazuje princip síťového kódování.



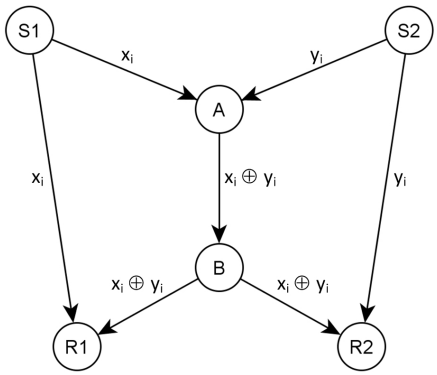
Obrázek 3 Princip síťového kódování.

2.2.2 Přínos síťového kódování

Následující odstavce stručně představují základní koncepty a výhody síťového kódování.

Maximalizace propustnosti Obrázek 4 ukazuje známou "motýlí"síť [26], která reprezentuje komunikační síť jako orientovaný graf. Hrany odpovídají přenosovým kanálům a body odpovídají terminálům, body bez vstupních hran jsou zdroji dat. Všechny hrany mají kapacitu jednoho bitu na jednu jednotku času, každý zdroj produkuje jeden bit informace za jednotku času. Nechť existuje skupinový přenos (multicast), při kterém zdroj dat $S1$ posílá tok bitů x_i do obou bodů $R1$ a $R2$, zatímco zdroj $S2$ posílá tok bitů y_i do stejných bodů $R1$ a $R2$. Při tradičním přístupu komunikace v síti by nastalo zahlcení na kanálu (A, B), jelikož každý kanál v této síti je schopen přenášet pouze jeden bit za jednotku času. Ahlswede v publikaci [26] ukázal, že lze umožnit mezilehlým bodům zpracovat a upravit vstupní datové toky a ne je pouze přeposílat tak, jak je obvyklé. Bod A může zpracovat bity z oddělených toků x_i, y_i a zkombinovat je pomocí operace

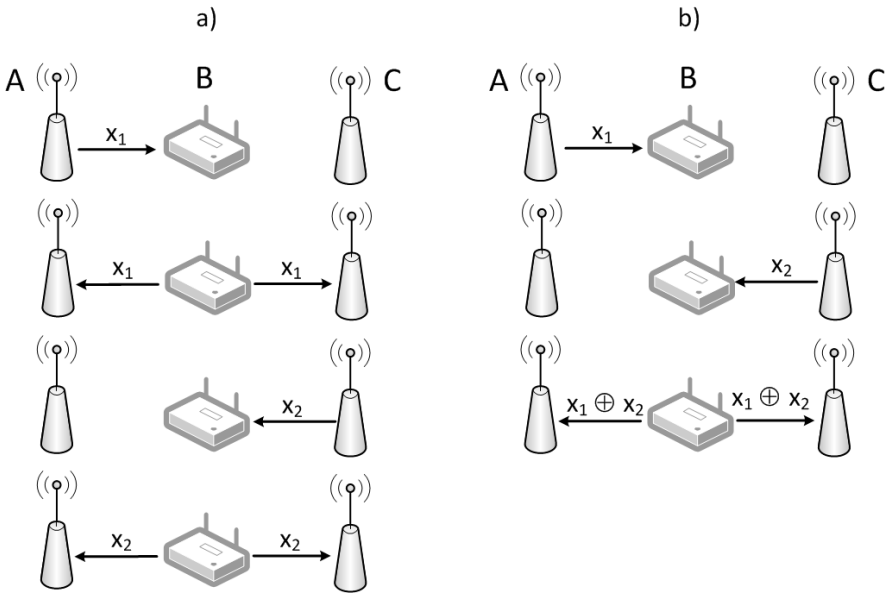
exkluzivní disjunkce (XOR) pro vytvoření nového toku $z_i = x_i \oplus y_i$. Bod $R1$ přijme bity $x_1, x_1 \oplus y_1$, pomocí operace XOR bod získá bity x_1 a y_1. $R2$ přijme $y_1, x_1 \oplus y_1$ a obdobným způsobem získá bity x_1 a y_1. Toto je způsob jak získat vyšší propustnost pomocí síťového kódování.



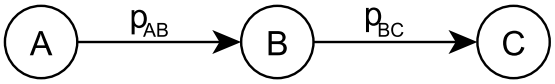
Obrázek 4 Skupinový přenos dat komunikační sítí.

Bezdrátové zdroje Síťové kódování umožňuje minimalizovat energii nutnou pro přenos dat, ušetřit bezdrátové zdroje a zredukovat celkové zpoždění přenosu. Mějme dvě sousední základnové stanice, A a C, komunikační sítě s retranslační stanicí B. Každé zařízení může vysílat, nebo přijímat data (poloviční duplex). Obě základnové stanice si přes bod B navzájem přenesou jeden bit během tří jednotek času. V prvních dvou jednotkách času přijme retranslační stanice po jednom bitu od každé ze stran. V třetí jednotce času vyšle bod B všesměrovým vysíláním XOR bit k oběma základnovým stanicím, které pak mohou bity vzájemně dekódovat [27]. Tato komunikace běžně vyžaduje čtyři jednotky času bez použití principů síťového kódování. Celkové zpoždění je tedy sníženo a bezdrátový kanál obsazen po kratší dobu. Navíc bod B vysílá pouze jednou (místo dvakrát), což přináší energetickou výhodu. Porovnání tohoto přístupu s tradičním přenosovým schématem je na obrázku 5.

Robustnost Závažným problémem v paketových sítích, obzvláště bezdrátových, je vysoká hodnota paketové chybovosti. Existuje několik způsobů, jak ji snížit. Jedním ze způsobů je využití protokolu TCP transportní vrstvy RM OSI. Tento protokol využívá pro spolehlivé doručování systém potvrzování, kdy korektně přijaté pakety jsou potvrzeny zprávou zaslanou zpět odesílateli. Pokud potvrzení určitého paketu není doručeno, pak je daný paket znovu odeslán. Jiným způsobem je například kanálové kódování, diskutované v části 2.1, které na odesílací straně přidává určité množství redundantních dat k paketům tak, aby pakety



Obrázek 5 Porovnání výměny informací bez (a) a se síťovým kódováním (b).



Obrázek 6 Jednoduchá síť s chybujícími přenosovými kanály.

bylo možné obnovit do původní podoby i v případě, že dojde k poškození části paketu [28]. Následující příklad publikovaný v [29][30] ukazuje možnost dosažení vyšší odolnosti přenosu při využití principu síťového kódování (umožnit také mezilehlým bodům provést kódování) oproti FEC schématu. U FEC schématu mezi koncovými body (end-to-end FEC) jsou totiž pakety zakódovány jen ve zdroji a dekódovány v cíli komunikace. Na obrázku 6 je zdroj dat A, který chce poslat data do cíle C. Na cestě z A do C existuje síťový bod B, který může vykonat operace síťového kódování. Pakety jsou ztraceny na cestě (A,B) s pravděpodobností p_{AB} a na cestě (B, C) s pravděpodobností p_{BC}. Použitím FEC schématu mezi dvěma koncovými body bude v bodě A propustnost komunikace na velikosti $R_{FEC} \leq (1 - p_{AB})(1 - p_{BC})$. Pokud ale bude povoleno na bodu B úplné dekódování a opětovné zakódování, bude dosaženo optimální kapacity minimálního řezu a tím propustnosti $R_{NC} \leq \min\{(1 - p_{AB}), (1 - p_{BC})\}$. V tomto případě jsou propustnosti R_{FEC}, R_{NC} dané pravděpodobností, že přenášený paket není ztracen ani na jedné z cest. Cenou zvýšené odolnosti je přidané zpoždění, je totiž nutné počkat na bod B, až přijme dostatečné množství zakódovaných dat tak, aby byl schopen dekódovat a znovu zakódovat paket.

2.2.3 Využití síťového kódování

Navzdory tomu, že síťové kódování je známo pouze velmi krátkou dobu, je využíváno, nebo alespoň intenzivně studováno, v celé řadě oblastí:

- V oblasti bezdrátových komunikací se uplatňuje jako prostředek pro dosažení vyšší propustnosti dat pomocí efektivnějšího využívání možností sdíleného média, ať už na fyzické vrstvě [31][32], či na spojové [14], síťové vrstvě [33] a transportní vrstvě [34] RM OSI.
- Pro distribuované ukládání dat nabízí efektivnější způsob zajištění opravy chyb v případě selhání určitého bodu [35].
- Efektivnější doručování dat v rozsáhlých klient-klient (peer-to-peer) sítích [36][37].
- Pro toky skupinového vysílání obsluhované v přepínačích se nabízí navýšení propustnosti [38].
- Možnosti využití síťového kódování pro oblast síťové bezpečnosti je diskutováno v [39].
- Rozvíjené je i použití v oblasti informační teorie [40][41][42].

2.3 Vícecestné šíření dat

Na vícecestné šíření dat lze nahlížet dvěma způsoby. Prvním je pohled bezdrátové komunikace s technikou diverzitního přenosu. Druhým pohledem lze nahlížet obecněji na jakýkoliv přenosový systém, který paralelně využívá více přenosových cest. A to ať už mezi dvěma sousedními síťovými body (například inverzní multiplexace [43]), nebo i širší přístup, který zahrnuje více cest napříč rozlehlejší sítí (multihoming s paralelním přenosem dat [44], či multimediální přenosy [45]). Využití těchto technik lze směrovat k navýšení přenosové rychlosti, či navýšení odolnosti systému vůči chybám.

2.3.1 Diverzitní rádiové systémy

Chyby přenosu dat bezdrátovými kanály mohou mít mnoho příčin, některé jsou dány trvalými podmínkami daného spoje (útlum způsobný šířením signálu prostorem, difrakční ztráty dané zastíněním spoje překážkou). Některé ale působí zcela náhodně, jako například kolísání útlumu šířením (takzvané úniky) [46]. Úniky vznikají šířením signálu od vysílače k přijímači po vícenásobných drahách (rychlý únik), či terénními překážkami mezi mobilní stanicí a pevnou základnovou stanicí

(pomalý únik). Účinným způsobem jak omezit vliv těchto jevů je právě diverzitní přenos, který je založený na využití více přenosových kanálů mezi přijímačem a vysílačem. Všechny signály přenášejí stejnou informaci, ale jsou z hlediska úniků co nejméně korelované [21]. Vhodným výběrem signálů na přijímací straně je poté složen výsledný signál, u kterého je vliv úniků do určité míry potlačen. Diverzitní systémy lze dělit podle toho, jakým způsobem jsou nezávislé přenosové kanály vytvářeny: prostorová, úhlová, polarizační, časová a frekvenční diverzita. Podrobnější popis lze nalézt v [21].

2.3.2 Obecný přístup k využití více přenosových cest

Dostupnost více nezávislých přenosových cest dává možnost variability jejich využití. Ať už pro využití všech cest pro přenos dat, nebo pro využití určité části pro zabezepečení přenosu. Využití více cest k přenosu dat umožňuje dva možné krajní případy využití, inverzní multiplexaci a zálohování. Jejich použití je závislé na požadavcích na přenos, zda je požadována co nejvyšší možná propustnost (inverzní multiplexace), nebo odolnost přenosu (zálohování).

Inverzní multiplexace Inverzní multiplexace rozděluje zasílaná data do N cest tak, aby byly rovnoměrně vytíženy. Výsledná přenosová rychlost je dána součtem přenosových rychlostí jednotlivých cest:

$$v_t = \sum_{i=0}^{N} v_{ti}. \tag{4}$$

Nevýhodou tohoto přístupu je chybovost přenosu. Množství nedoručených dat je totiž dáno součtem chyb ze všech použitých cest.

Zálohování Při zálohování dochází až k N násobnému navýšení odolnosti přenosu, v případě zasílání dat N nezávislými přenosovými cestami. V případě, že nastane chyba na jedné z cest, existuje pravděpodobnost, že na jedné z $N-1$ cest chyba nenastala. Díky této vlastnosti a díky skládání korektně doručených dat na přijímací straně, je výrazně navýšena odolnost přenosu. Celková přenosová rychlost je dána rychlostí nejpomalejší cesty:

$$v_t = \min_{i=0}^{N} v_{ti}. \tag{5}$$

Pro obě zmíněné metody je vhodné využití cest s podobnou přenosovou rychlostí. V případě velkých rozdílů se zvyšují nároky na velikost vyrovnávací paměti přijímače, který skládá jednotlivé toky dohromady a rekonstruuje původní posloupnost dat. To zároveň vede k nárustu zpoždění přenosu a k nárustu kolísání zpoždění.

3 Cíle disertační práce

Předložená práce se zabývá optimalizací využití více přenosových cest ke zvýšení spolehlivosti přenosu dat. Navrhuje obecný systém přenosu, který umožňuje variabilní nastavení parametrů jednotlivých komponent systému a vytvořit tak konkrétní, přesně definované schéma přenosu dat.

Stanovené cíle této disertační práce jsou následující:

1. Navržení obecného systému přenosu umožňujícího variabilní využití více přenosových cest. Návrh a detailní popis funkce konkrétního přenosového schématu schopného zvýšit odolnost přenosu proti chybám při přenosu.

2. Vytvoření modelu navrženého přenosového schématu v síťovém simulačním nástroji. Zvolit konkrétní simulační prostředí a provést úplnou implementaci přenosového schématu pro možnost jeho ověření.

3. Ověření navrženého schématu na simulacích z pohledu schopnosti obnovy chybných dat. Využít naměřená data pro možnost ověření při skutečných provozních podmínkách.

4. Ověření navrženého schématu na simulacích z pohledu z pohledu celkového zpoždění přenosu. Analyzovat vliv mechanismu obnovy dat na navýšení celkového zpoždění přenosu dat.

5. Porovnání navrženého schématu s obecně používanými schématy přenosu dat po více přenosových cestách.

4 Použité metody

Pro ověření teoretických předpokladů navrženého přenosového schématu bylo využito simulace jeho funkcionality. K vybudování dostatečně přesného modelu bylo potřeba implementovat samotnou funkci kodéru, dekodéru i další nezbytné bloky schématu, nastavit parametry, které jej definují, a také zvážit další vlivy, které mohou mít dopad na jeho provoz. Simulační nástroje jsou v tomto ohledu velmi dobrým pomocníkem, který umožňuje tvorbu modelu odpovídající teoretické funkci a zároveň jej dokáží prověřit z pohledu reálného využití.

Jedním z nejznámějších síťových simulátorů je NS-2 [47]. Je založen na zpracování diskrétních událostí (jako i ostatní zmíněné simulátory) a obsahuje modely mnoha síťových protokolů včetně podpory směrování či přístupových metod bezdrátových sítí. Pro zápis samotného chování prvků používá jazyk C++, pomocí skriptů v jazyce OTcl se v něm pak vytváří topologie sítě, konfiguruje a řídí simulace. Takzvaný Network Animator poskytuje možnost zobrazení simulace graficky, animací zobrazuje topologii sítě. Tento simulátor, přes svou popularitu, již není dále vyvíjen.

NS-3 [48] je přímý následník NS-2, jeho rozhraní je ale od základu přepracováno a není tedy zpětně kompatibilní. Jádro programu je modulární, modely se zapisují pouze v jazyce C++ (na rozdíl od použití OTcl u NS-2), případně v Pythonu. Jeho nevýhodou je nepříliš velká uživatelská přívětivost daná chybějícím grafickým rozhraním.

Dalším simulátorem je například OPNET Modeler [49], což je softwarové prostředí umožňující návrh a analýzu komunikačních sítí. Je hierarchicky a objektově orientován, nabízí grafické rozhraní, které umožňuje snadný návrh i analýzu výsledků. Obsahuje rozsáhlou databázi síťových protokolů založených na jazyce C. Zdrojové kódy simulačního jádra ale nejsou uživatelům dostupné a jako jediný ze zmíněných simulačních nástrojů není distribuován pod volnou licencí.

Simulační prostředí OMNeT++ [50] využívá pro funkční jádro simulací jazyk C++ a vlastní programovací jazyk NED (Network Description) pro topologii sítě. OMNeT++ je modulární, objektově orientovaný simulační nástroj primárně určený k tvorbě síťových simulací. Poskytuje grafické prostředí pro usnadnění návrhu a je pro něj k dispozici velké množství knihoven s hotovými modely ši-

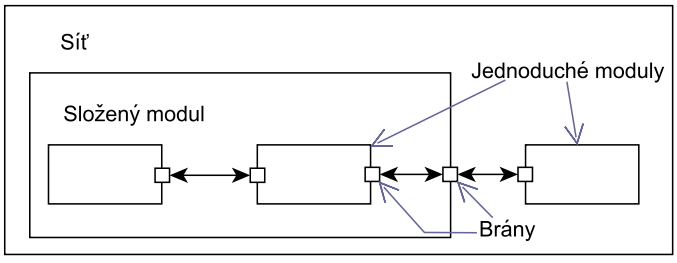
roké škály částí přenosového řetězce. Od modelů šíření signálu až k aplikacím generujícím provoz na síti. Jeho bližší popis je v následující sekci této kapitoly.

Z ostatních síťových simulátorů lze zmínit častěji využívané NetSim [51], JSim [52], či cnet [53].

Výběr vhodného nástroje je dán hlavně konkrétními potřebami uživatele. Existují však některé obecné vlastnosti, které by měl podle [54] každý simulační nástroj obsahovat: *flexibilitu* pro vytváření nových entit modelu. *Usnadnění vývoje* pomocí grafického rozhraní, aby se uživatel zaměřil na samotnou podstatu problému a ne jeho způsob realizace. Možnost *hierarchického členění* entit a možnost jejich opětovného využití. Umožnění *rychlého běhu simulace* s velkým množstvím simulačních událostí a entit modelu. A v neposlední řadě také *vhodný výstup dat* simulace, pro možnost jejich následné analýzy. To vše splňuje zvolený simulační nástroj OMNeT++, který je v posledních letech v akademickém prostředí hojně využívaný [50].

4.1 Simulační prostředí OMNeT++

OMNeT++ je vývojové prostředí, které umožňuje návrh simulací pro široké spektrum oblastí. Lze v něm nasimulovat libovolný systém, jehož funkce jsou zapsatelné pomocí diskrétních událostí a který může být rozložen do prvků komunikujících spolu pomocí zpráv [55]. Díky hierarchickému členění (naznačené na obrázku 7) a využití objektově orientovaného přístupu jsou vytvořené simulace velmi dobře škálovatelné a jejich rozsah je shora omezen pouze výkonností počítače, na kterém jsou spouštěné. Tvorba simulací je v tomto prostředí velmi pohodlná díky grafickému rozhraní, umožňujícímu snadný a přehledný zápis, a také množství dostupných knihoven již hotových modelů [56].



Obrázek 7 Hierarchické členění simulačního modelu.

Základním prvkem simulace vytvářené v prostředí OMNeT++ je tvorba takzvaných jednoduchých modulů. Jejich úkolem je samotné vykonávání požadované funkce, tvoří jádro simulovaného systému. Zapisují se pomocí jazyka C++ s vyu-

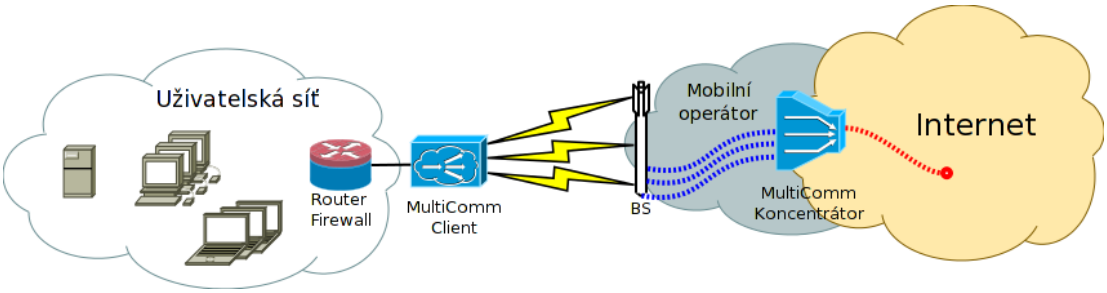
žitím knihovny simulačního jádra. Tyto základní prvky spolu mohou komunikovat pomocí zpráv, které mohou reprezentovat například rámce protokolu na 2. vrstvě RM OSI, či zákazníky obsluhového systému. Zprávy se zasílají mezi moduly buď přímo, nebo mnohem častěji pomocí takzvaných bran. Ty vytvářejí vstupní a výstupní rozhraní jednotlivých modulů a jejich propojením je tvořeno spojení. Každému spojení je možné nadefinovat různé parametry, jako například zpoždění či chybovost. Vzájemně propojené jednoduché moduly lze spojovat do složených modulů, který lze dále propojovat a vytvářet tak komplikovanější celky. Počet takovýchto vnoření není omezen [50]. Jednotlivé moduly, ať už jednoduché či složené, lze dále využívat i v rámci jiných simulací.

Vzájemné propojení modulů, tedy topologie simulovaného systému, se popisuje v jazyce NED (Network Description). Návrh struktury simulace je v systému OMNeT++ usnadněn možností využití grafického rozhraní, které pro zápis využívá právě jazyk NED. Tento simulační nástroj umožnil ověření funkce navrženého schématu s vysokou přesností díky možnosti generování velkého množství paketů a snadného opakování mnoha běhů simulací. Vysoké množství opakovaně zasílaných paketů (řádově 10^9) vyžaduje kvalitní generátor náhodných čísel. A i když v simulačním prostředí nelze nikdy získat opravdu náhodná čísla, tak generátor pseudonáhodných čísel, implementovaný v OMNeT++, je pro dané účely více než dostačující. Jedná se o kvalitní generátor Mersenne Twister, vyvinutý autory Matsumoto a Nishimura, s dlouhou periodou $2^{19937} - 1$. Více informací o tomto generátoru je v [57]. Simulační prostředí umožňuje nakonfigurovat automatické opakování simulace vždy s jiným počátečním stavem generátoru, což bylo při simulacích využíváno.

4.2 Další použité nástroje

Pro ověření funkce navrženého přenosového schématu bylo využito měření v mobilních sítích, při kterém bylo využito zařízení pro přenos dat po více paralelních cestách. Zařízení je pod jménem MultiComm vyvíjeno na katedře telekomunikační techniky FEL ČVUT ve spolupráci se společností Certicon [58][59]. MultiComm je zařízení specificky navržené pro navýšení přenosové rychlosti, stability a spolehlivosti datového přenosu prostřednictvím sítě GSM (Global System for Mobile Communications). Zmíněného efektu se dosahuje současným využitím několika přenosových cest nejlépe za využití více fyzických mobilních operátorů. MultiComm se skládá z klientské a serverové části, viz obrázek 8. Jedná se o koncové prvky multiplexovaného datového spoje. Klientská část je realizována jako integrované hardwarové zařízení s až čtyřmi GSM 2G/3G komunikačními jednotkami

a systémem GPS (Global Positioning System). Serverová část je softwarové řešení instalované na dedikovaný či virtuální server s připojením do sítě Internet.



Obrázek 8 Schéma komunikační sítě s využitím MultiCommu.

Generování požadovaného toku dat bylo realizováno pomocí softwarového nástroje FlowPing [60], který je také vyvíjen na FEL ČVUT. Tento nástroj umožňuje definovat parametry odesílaných dat a také jejich sběr pro následnou analýzu. Výstupní informace obsahují podrobný popis komunikace a lze z nich, například pomocí skriptů v jazyce Python, snadno připravit data pro analýzu.

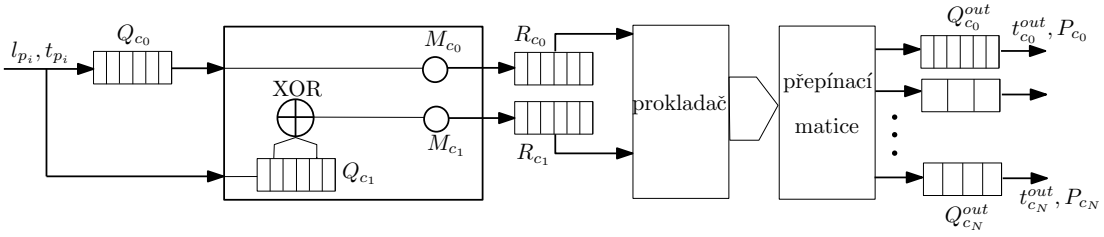
Při teoretické analýze bylo využíváno integrované prostředí MATLAB [61], které v sobě spojuje grafické vývojové prostředí, vlastní programovací jazyk, nebo možnosti vizualizace. Dále také obsahuje knihovnu matematických funkcí či prostředí pro psaní aplikačních programů.

5 Návrh systému přenosu

V této kapitole je nejdříve popsán navržený systém a součásti jeho dvou hlavních částí: kodéru a dekodéru. Systém je obecně definován tak, aby jej bylo možné pomocí parametrů jeho komponent upravit tak, aby odpovídal požadavkům služeb nad ním provozovaných. Na příklad podle toho, kolik přenosových cest je k dispozici, jak mohou být využity co do naplnění šířky pásma, ale i zda budou využívány pro redundantní či originální data. Pro systémy, kde je jednoduchost realizace zásadní součástí, je potřeba do úvahy vzít i maximální délky front a s tím související možnosti tvorby kódových variant paketů. Navržený systém pracuje na třetí vrstvě RM OSI a je plně transparentní, zdrojem dat tedy může být libovolný systém, neboť po dekódování budou data ve stejném formátu, ve kterém do kodéru vstupovala. Dále v kapitole následuje část, která popisuje jedno specifické schéma přenosu, které vychází z navrženého systému a je určeno pro zajištění vyšší redundance dat. V textu je termín kanál používán ve smyslu obecné datové přenosové cesty, která může procházet přes vícero síťových uzlů. Komunikace v rámci navrženého systému přenosu dat vytváří určité schéma přenosu, podle kterého se pak přenos dat řídí.

5.1 Kodér

Na obrázku 9 je zobrazen navržený princip funkce kodéru kanálu, který umožňuje využití více přenosových cest. Pomocí volby jeho parametrů je možné nastavit požadovaný stupeň redundance a optimalizovat jej pro konkrétní možnosti daného přenosového systému.



Obrázek 9 Navržený princip funkce kodéru.

Ze zdroje dat tedy do schématu vstupují pakety o délce l_{p_i} s intervalem t_p. Pakety jsou následně kopírovány do dvou First In, First Out (FIFO) front. Původní (originální) pakety D_i^N jsou ukládány do fronty Q_{c_0} o délce $l_{Q_{c_0}}$. Jejich kopie jsou ukládány do fronty Q_{c_1} o délce $l_{Q_{c_1}}$. Délky těchto front mají vliv na velikost možných kombinací prováděných s pakety za účelem dosažení určité redundance, tyto kombinace mají také vliv na možnosti obnovy ztracených paketů na straně dekodéru. Pro určitá schémata je možná i varianta s nulovými délkami těchto front, tedy přímý průchod paketů. Pro bitové délky front platí:

$$\begin{aligned} l_{Q_{c_0}} &\geq m \cdot l_{p_i} \\ l_{Q_{c_1}} &\geq n \cdot l_{p_i}, \end{aligned} \tag{6}$$

kde l_{p_i} je délka paketů ve frontě v bitech, m, n jsou nutné počty paketů pro realizaci daného kódování.

Originální pakety, tedy nijak nekombinované, jsou pak z fronty Q_{c_0} vybírány v intervalu $t_{Q_{c_0}}$, který je dán zvoleným schématem. Blok XOR si z fronty Q_{c_1} odebírá v intervalu $t_{Q_{c_1}}$ potřebný počet paketů, který je dán délkou k zvoleného kódu. Tyto pakety jsou vzájemně kombinovány operací exkluzivní disjunkce, případně jinou lineární funkcí. Pro možnost dekódování je důležité označení kombinovaných paketů X_j^N tak, aby bylo možné je jednoznačně identifikovat a určit, které pakety byly kombinovány. Tato problematika je diskutována níže. Pro správnou funkci schématu musí být kombinované pakety stejně dlouhé. V případě nestejné délky, lze situaci vyřešit doplněním kratšího/kratších paketu/ů nulami, což dekódování ostatních paketů neovlivní. Délku paketů je vhodné zvolit s ohledem na využití schématu. V případě, že je očekávatelné, že se budou vyskytovat převážně dvě výrazně odlišné délky paketů (typicky pakety s informacemi a potvrzovací pakety), je vhodné zařadit blok navíc, který zajistí kombinaci pouze stejných typů paketů.

Bloky M_{c_0} a M_{c_1} zajišťují multiplikaci paketů; celočíselné hodnoty $\alpha_{M_{c_0}}$ a $\alpha_{M_{c_1}}$ jsou dány navržením schématu a udávají kolikrát je určitý paket nakopírován; platí $\alpha_{M_{c_{0,1}}} > 0$. Tyto pakety jsou ukládány do registru R_{c_0} (originální pakety)

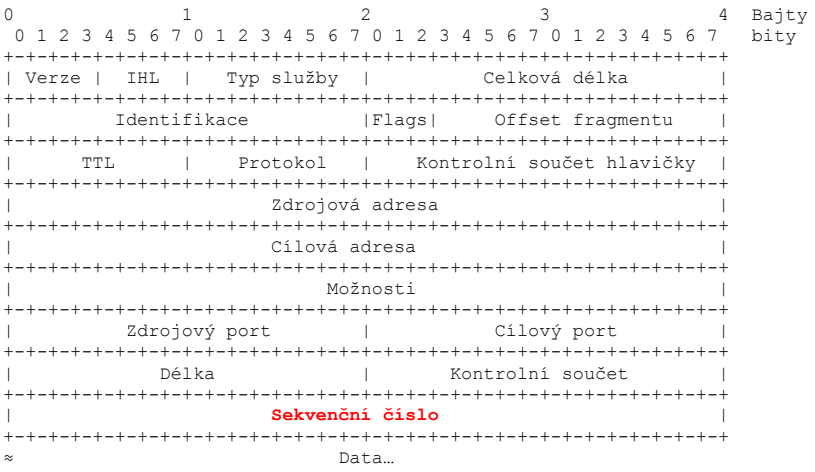
a do registru R_{c_1} (kombinované pakety). Registry jsou zde použity místo FIFO front z toho důvodu, že blok prokladače již může vybírat jednotlivé pakety nejen postupně, podle pořadí, ale podle logiky, dané použitým schématem. Například podle sekvenčních čísel střídavě vybírat každý x-tý paket z R_{c_0} a každý y-tý z R_{c_1} a podobně.

Následující blok zajišťuje prokládání jednotlivých paketů. Hloubka prokladače d je dána délkou shluků chyb, které má být zvolené schéma schopné opravit. Tato volba je také ovlivněna maximální požadovanou dobou zpoždění a také možnostmi technické realizace, jejíž náročnost se různými typy prokladačů liší. Způsob prokládání paketů vybraných z registrů je součástí logiky daného schématu.

Blok přepínací matice MxN zajišťuje rozdělení paketů z prokladače do front předřazeným N přenosovým cestám. Například může být prvních i cest využito pro posílání originálních paketů a $i + 1$ cesta pro zasílání redundantních dat ve tvaru kombinovaných XOR paketů. Variantou také může být střídavé využívání cest, tedy nikoliv konstantní zasílání určitého druhu paketů (originální, kombinované) po celou dobu přenosu. Tento přístup napomáhá vyšší odolnosti proti shlukům chyb vyskytujícím se na jedné z cest. Nevýhodou je pak složitější logika kodéru i dekodéru; zajištění detekce, o jaký typ paketů se na straně dekodéru jedná, je možné pomocí označování paketů speciálním příznakem v záhlaví. Navržené řešení je popsáno níže.

Pakety jsou z front $Q^{out}_{c_{0..N}}$ odesílány do N přenosových cest s intervaly $t^{out}_{c_{0..N}}$. Tyto intervaly mohou být shodné, ale mohou se i lišit. Každý přenosový kanál může mít jiné parametry propustnosti, stejně tak i technologie jednotlivých cest mohou být odlišné (metalické, rádiové, optické). Rozdílná četnost odesílání může vést i v rámci stejného typu cesty k využívání různé modulace a tím i k získání rozdílné pravděpodobnosti ztráty paketu $P_{0..N}$. To má vliv hlavně při přímo propojených stranách odesílatel příjemce, ale i v situaci, kdy odesílatel je spojen méně kvalitní přenosovou cestou do dalšího síťového bodu, který již má spojení s dalším bodem s lepšími parametry (ztrátovost, zpoždění, apod.). Při návrhu konkrétního schématu je nutné tyto parametry zohlednit.

Výše zmíněné označení paketů, které jsou kombinovány, je nutné z důvodu jejich detekce na straně dekodéru k získání informace o jaký typ paketu se jedná (originální, kombinovaný). Ze samotného obsahu paketu nelze totiž typ zpětně určit. Příklad řešení značení paketů může být následující: originální pakety, tedy ty, do jejichž těla není zasahováno, mají pole uvozeny nulou (0xxxxxx), následující bity již značí sekvenční číslo paketu. Kombinované pakety jsou uvozeny jedničkou (1xxxxxx) a následující bity označují, který paket byl využit pro kombinaci jako první. Tímto je vyřešena i situace nastávající u schémat, kde je počítáno



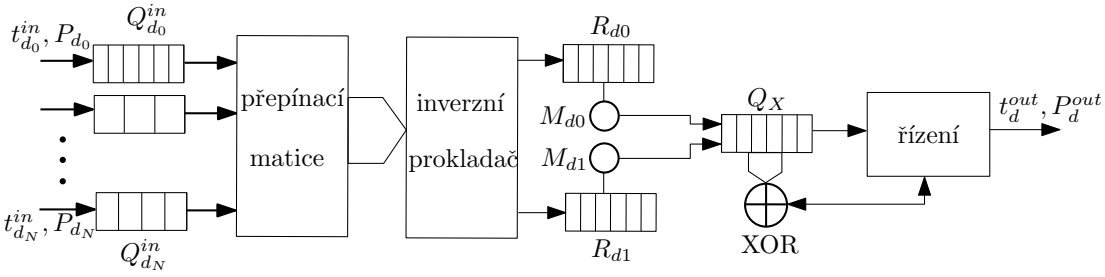
Obrázek 10 Příklad upravené hlavičky paketu.

s lineárními kombinacemi tří a více paketů. Jelikož všechna schémata počítají s kombinacemi po sobě jdoucích paketů, postačuje označení sekvenčního čísla prvního z kombinovaných paketů. Dekodér pro dané schéma se zvoleným počtem kombinovaných paketů počítá. Z důvodu zachování přínosné vlastnosti schématu, totiž jeho transparentnosti vůči síťovým uzlům v přenosové cestě, je potřeba, aby označování nenarušilo obvyklou strukturu hlaviček paketů. Byla zachována struktura hlavičky IP/UDP paketu [62] a [17], pakety jsou pouze rozšířeny o pole *Sekvenční číslo* tak, jak je červeně naznačeno na obrázku 10. Toto záhlaví síťové uzly považují za uživatelská data.

5.2 Dekodér

Jednotlivé kanály vstupující do dekodéru zobrazenému na obrázku 11 mohou doručovat pakety s rozdílnou přenosovou rychlostí, s různým zpožděním, ztrátovostí a v závislosti na návrhu schématu se mohou střídat typy doručovaných paketů (originální, kombinované). Jelikož je navržené přenosové schéma možné využívat nejen u přímo propojených koncových bodů, ale spojení může procházet přes více síťových bodů, je nutné počítat i s tím, že na vstupu dekodéru se mohou pakety objevit v jiném pořadí, než byly odeslány.

Z N kanálů vstupují pakety do dekodéru přes fronty $Q^{in}_{d_N}$, které jsou určeny na vyrovnávání rychlostí. Blok přepínací matice zajišťuje výběr z jednotlivých front podle zvoleného schématu. Výběr je ovlivněn i přenosovými rychlostmi jednotlivých cest a tedy intervaly příchodů paketů $t^{in}_{d_N}$ z jednotlivých kanálů; výběr paketů nemusí fungovat pouze systémem round-robin, ale například j paketů z první fronty, $j-1$ paketů z druhé atd. Blok inverzního prokladače následně zajiš-



Obrázek 11 Navržený princip funkce dekodéru.

ťuje zpětné poskládání paketů do původního pořadí. To vyžaduje, v případě nesynchronizovaného doručování paketů z jednotlivých cest, kontrolu sekvenčních čísel paketů. V případě větších odchylek od plánovaného pořadí paketů, které může nastat rozdílnými přenosovými dobami jednotlivých cest, rostou nároky na vnitřní paměť a roste zpoždění. Blok dále rozřazuje pakety podle typu (originální, kombinovaný) do dvou registrů $R_{d_{0,1}}$, které obsahují pakety pouze daného typu.

Z těchto registrů si řídicí blok vybírá pakety (do fronty Q_X s délkou l_{Q_X}) a případně je $\alpha_{M_{d_{0,1}}}$- násobně multiplikuje, podle potřeby dekódovacího mechanismu. Některé pakety mohou být pro dekódování využity vícenásobně, proto může schéma využít multiplikaci daného paketu. S touto funkcí souvisí mazání nepotřebných paketů z front. Podle zvoleného schématu k němu může docházet buď přímo logikou daného dekodéru (např. pokud originální paket dorazil, pak je jeho redundantní kopie smazána), nebo po určité zvolené době t_e. Tento čas má vliv na nutnou délku front a i na možnosti obnovy paketu, v případě jeho nedoručení. V případě, že nedochází ke ztrátám paketů, je celá tato část výrazně zjednodušena. Pokud nedochází k výpadkům paketů, pak větev k bloku XOR zůstává nepoužita a řídicí blok zajišťuje poskládání paketů do pořadí, v jakém byly odeslány. Pro určité protokoly vyšších vrstev, které si zajišťují správné pořadí samy (např. TCP), mohou být pakety zasílány i přímo. Skládáním paketů do pořadí má vliv na zpoždění doručení paketů, na kolísání zpoždění i na ztrátovost. V případě, že paket nebude doručen a ani se nepovede jeho obnova (do určité přednastavené doby čekání t_s), je nutné pokračovat v odesílání paketů dále. Tento časový limit je dán požadavkem služby (služeb), které budou přes přenosové schéma provozovány. V případě služeb citlivých na zpoždění (hlasové služby), bude mít tento limit hodnotu nižší, než u méně časově závislých služeb (datové služby). S vysokými požadavky na tento limit může docházet ke ztrátám paketů, které se zpozdily buď v přenosové cestě, nebo doba jejich obnovy (v případě ztráty paketu) překročila daný limit. Řídicí blok může pomocí vnitřní paměti zajišťovat vyrovnávání intervalů mezi doručovanými pakety a tím potlačovat kolísání

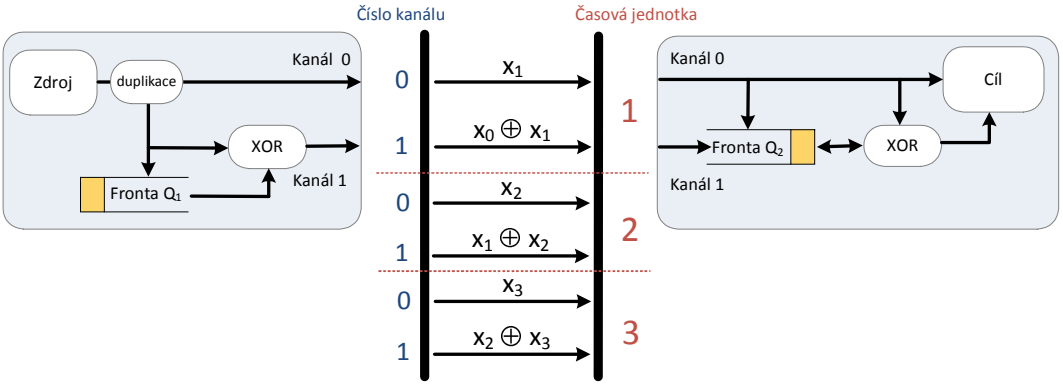
zpoždění způsobené přenosovými cestami i vnitřní logikou dekodéru. Výstupem z dekodéru jsou pakety odcházející v intervalech t_d^{out} s celkovou chybovostí přenosu mezi vstupem kodéru a výstupem dekodéru P_d^{out}. Pakety odcházejí v původní podobě v jaké vstupovaly do kodéru na vzdálené straně přenosu.

5.3 Specifický systém přenosu

Z obecného návrhu systému přenosu je dále odvozena jeho konkrétní realizace, její parametry jsou v tabulce 1. Vybraná varianta se vyznačuje schopností obnovy až dvou po sobě jdoucích originálních paketů (tj. nepozměněných), bez potřeby opětovného zaslání dat. Navržené schéma využívá techniky inverzní multiplexace - data jsou určitým, dále popsaným, způsobem zasílána po dvou nezávislých přenosových kanálech. Zároveň je využit přístup síťového kódování k paketům, kterým je pozměňována jejich uživatelská část. Navržené schéma využívá operaci exkluzivní disjunkce (XOR) pro manipulaci s daty paketů z různých přenosových cest.

Tabulka 1 Parametry zvoleného systému

Název parametru	**Symbol**	**Hodnota**	**Jednotka**
Počet přenosových kanálů	N	2	-
Délka fronty 0 kodéru	$l_{Q_{c_0}}$	≥ 1	paket
Délka fronty 1 kodéru	$l_{Q_{c_1}}$	≥ 2	paket
Intervaly výběrů paketů z front	$t_{Q_{c_{0,1}}}$	$t_{Q_{c_0}} = t_{Q_{c_1}}$	sekunda
Koeficienty multiplikace v kodéru	$\alpha_{M_{c_{0,1}}}$	1	-
Délka kódu	k	2	paket
Hloubka prokladače	d	1	paket
Intervaly odesílání paketů z kodéru	$t_{c_{0,1}}^{out}$	$t_{c_0}^{out} = t_{c_1}^{out}$	sekunda
Koeficienty multiplikace v dekodéru	$\alpha_{M_{d_{0,1}}}$	1	-
Délka dekódovací fronty	l_{Q_X}	3	paket
Délka paketu	l_p	variabilní	bit
Interval mezi příchody paketů do kodéru	t_p	variabilní	sekunda
Interval odchodů paketů z dekodéru	t_d^{out}	variabilní	sekunda
Maximální čas mazání zastaralých paketů	t_e	variabilní	sekunda
Maximální čas čekání na doručení paketů	t_s	variabilní	sekunda



Obrázek 12 Princip funkce navrženého schématu přenosu dat.

Na obrázku 12 je zobrazen princip funkce navrženého schématu přenosu dat. Na levé straně obrázku 12 je část zajišťující odeslání dat, na pravé pak část starající se o příjem dat. Paket doručený do systému s navrženým schématem je na vstupu zduplikován. Původní paket je odeslán pomocí přenosového kanálu 0, který je používán pouze pro odesílání originálních paketů. Duplikát paketu je nakombinován pomocí binární funkce XOR s paketem uloženým ve frontě Q_1, tato kombinace je odeslána druhým kanálem. Druhý kanál je navržen jako redundantní a je využíván pouze pro zasílání kombinace dvou po sobě jdoucích paketů. Paket ve frontě (duplikát z předchozí iterace) je nahrazen aktuálním. Tímto průběžným systémem je zaručena fronta o délce pouze dvou po sobě jdoucích paketů. V případě odesílání úvodního paketu komunikace, je paket kombinován s nulovým paketem (fronta je prázdná), což díky vlastnostem operace XOR znamená, že je oběma kanály posílán stejný paket. Princip funkce přijímací strany (pravá část obrázku 12) je vysvětlena níže.

Pokud paket z kanálu 0 není korektně doručen (přijímací strana nedokáže přečíst celý obsah přenášených dat paketu) je zde stále šance k obnovení daného paketu. Na rozdíl od schématu využívajícího obou kanálů pro posílání stejných dat (úplná redundance dat), je navržené schéma schopno obnovit původní nedoručený paket obnovit i v situaci, kdy není doručen ani redundantní paket z druhého kanálu a to bez opakování přenosu dat. Následující odstavce popisují princip obnovy nedoručených paketů v přijímací části rozdělené podle možných kombinací nedoručených paketů.

5.3.1 Varianta obnovy 1

Tato varianta obnovy zahrnuje situace kdy originální paket (z prvního kanálu) není doručen korektně, zatímco redundantní paket z druhého kanálu ano. Tento typ je řešen pomocí XOR operace doručeného redundantního paketu s paketem přijatým v předchozí komunikaci, který je uložen ve frontě Q_2. Výsledkem dané operace je získání původního (nedoručeného) paketu, jak naznačuje rovnice 7. Po obnově je paket zaslán do cíle a jeho duplikát je umístěn do fronty pro případ potřeby další obnovy. Tento typ obnovy nepřináší žádné zvýhodnění v porovnání s běžným schématem plné redundance, navíc v případě dvou a více po sobě jdoucích nedoručených originálních paketů nejsou xorované pakety v redundantním kanálu použitelné. V takové situaci je totiž nemožné je dekódovat. Tento typ obnovy je zmíněn pouze z důvodu úplnosti výčtu možností.

$$\begin{aligned} x_1 \ldots nedoručen \\ x_0 \oplus (x_0 \oplus x_1) \Rightarrow x_1 \end{aligned} \tag{7}$$

5.3.2 Varianta obnovy 2

Tato varianta popisuje situace kdy není doručen originální paket ani jeho odpovídající redundantní paket z druhého kanálu. Navržené schéma je schopné obnovy původního paketu, což by v případě použití plné redundance již nebylo možné. Pro tento typ je již navržené schéma robustnější než zasílání stejných dat oběma kanály při zachování stejného objemu redundantních dat. Rozdíl je ve využití vlastností xorovaného paketu v druhém kanálu. Vzhledem k tomu, že redundantní paket obsahuje informace o dvou sobě jdoucích paketech je možné obnovit nedoručený originální paket z dat získaných z následujícího přenosu. Na příklad, pokud je paket x_1 i paket $x_0 \oplus x_1$ nedoručený, pak paket x_2 xorovaný s paketem $x_1 \oplus x_2$ (tj. následující přenos) obnoví nedoručený paket x_1, viz 8.

$$\begin{aligned} x_1, (x_0 \oplus x_1) \ldots nedoručeny \\ x_2 \oplus (x_1 \oplus x_2) \Rightarrow x_1 \end{aligned} \tag{8}$$

5.3.3 Varianta obnovy 3

Třetí varianta nastává při nedoručení dvou originálních paketů a jednoho redundantního. Navržené schéma je schopné rekonstrukce obou nedoručených originálních paketů. Pro úspěšnou obnovu je potřeba přijmout jeden redundantní paket

k ztracenému originálu a úspěšně přijmout následující dvojici paketů (originální i redundantní). Princip funkce obnovy je v zachování informace z redundantního kanálu a vhodného použití operace XOR. Funkci lze demonstrovat při pohledu na obrázek 12 a rovnici 9, která naznačuje příklad použití.

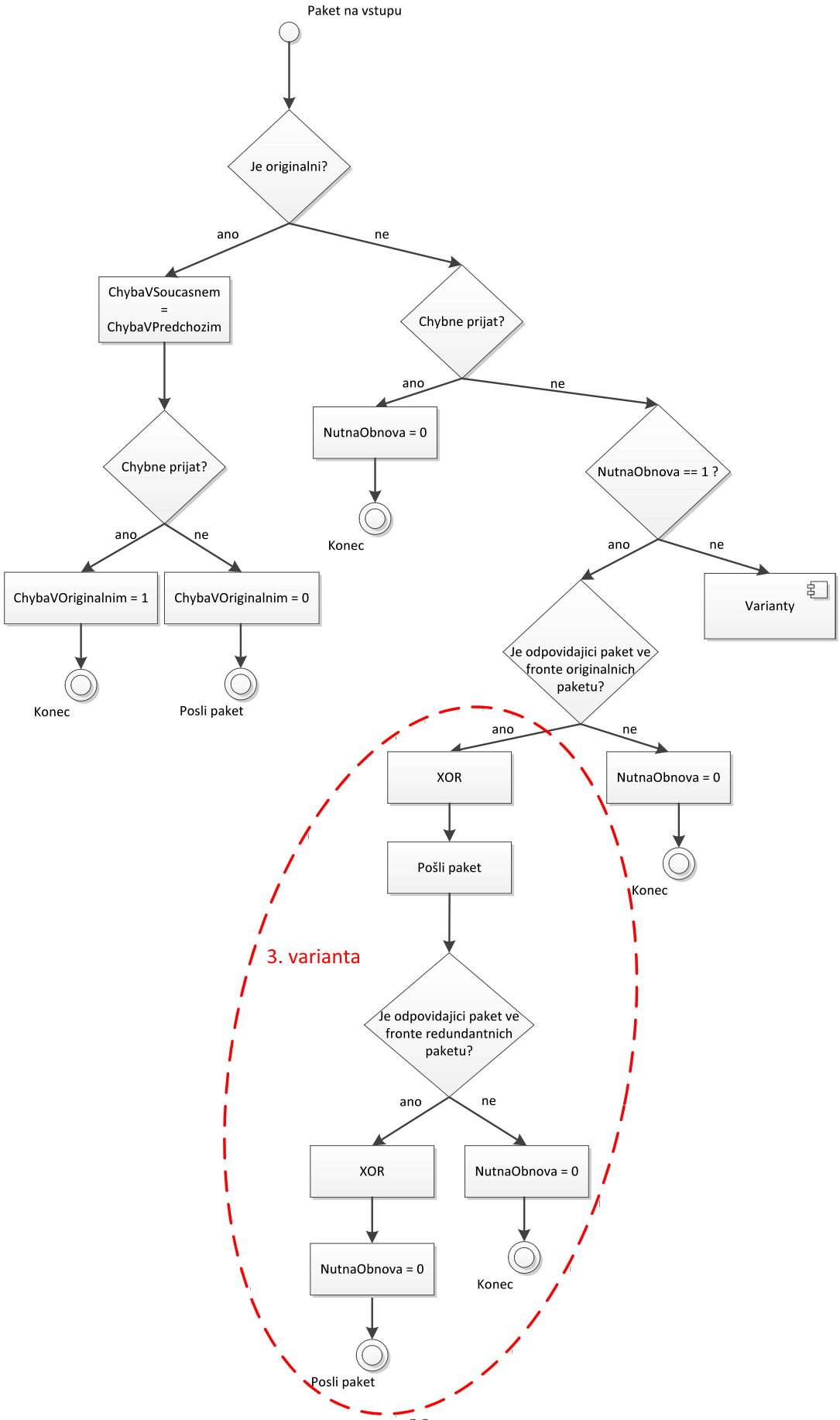
$$\begin{aligned} x_1, x_0 \oplus x_1, x_2 \ldots nedoručeny \\ x_3 \oplus (x_2 \oplus x_3) => x_2 \\ x_2 \oplus (x_1 \oplus x_2) => x_1 \end{aligned} \tag{9}$$

V případě ztráty paketů x_1, $x_0 \oplus x_1$ a x_2, jsou následující pakety $x_1 \oplus x_2$ a x_3 uloženy ve frontě Q_2. V momentě doručení paketu $x_2 \oplus x_3$ je možné začít s obnovou nedoručených originálních paketů. Z XOR operace paketu x_3 a jemu odpovídajícího redundantního paketu $x_2 \oplus x_3$ se získá nedoručený paket x_2. Ten je zaslán příjemci a jeho duplikát je použit pro další XOR operaci s paketem $x_1 \oplus x_2$ uloženým ve frontě. Tím je získán první nedoručený paket (x_1). Nedoručené redundantní pakety není potřeba obnovovat, jelikož originální pakety doručily kompletní informaci k příjemci.

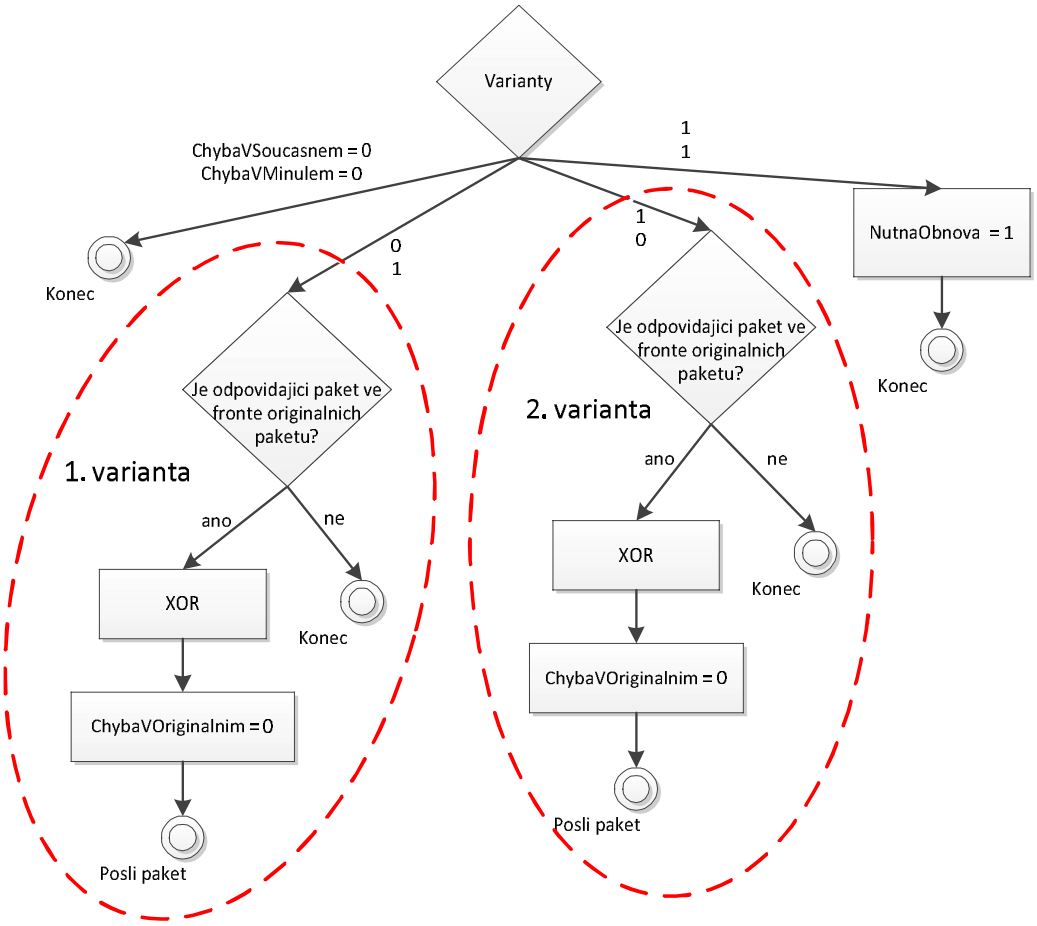
V průběhu přenosu dat dochází k různým výskytům zmíněných variant a jejich kombinací. Vnitřní logika schématu, reagující na konkrétní situaci, je naznačena na obrázcích 13 a 14.

V případě paketů nedoručených v pořadí odeslání (navržené schéma může pracovat napříč rozlehlou sítí s mnoha cestami různých parametrů) se zvyšují nároky na velikost fronty na přijímací straně schématu tak, aby mohlo dojít ke korektní obnově dat v případě její potřeby. V případě nestejné velikosti paketů určených ke xorování je nezbytné doplnit kratší paket nulami. Díky tomu a díky vlastnostem operace XOR bude informace z obou paketů zpětně získatelná. Možná je i varianta rozdělení paketů na stejnou délku (podle délky kratšího z paketů). V takovém případě je nutné následné spojení rozdělených dat na přijímací straně schématu tak, aby systém zůstal transparentní.

Navržené přenosové schéma je plně transparentní vůči systémům, které propojuje. Jedná se o spojení typu konec-konec, může tedy procházet přes mezilehlé body v přenosové cestě. Pracuje s pakety na třetí vrstvě referenčního modelu OSI [5], nicméně může být využito i na nižší vrstvě, kde se pak komunikace redukuje na spojení bod-bod. V takové variantě může díky své transparentnosti přenášet různé typy protokolů vyšší vrstvy modelu OSI.



Obrázek 13 Diagram vnitřní logiky schématu (část 1).



Obrázek 14 Diagram vnitřní logiky schématu (část 2).

6 Ověření navržené optimalizace přenosu dat simulací

6.1 Analýza z pohledu chybovosti dat

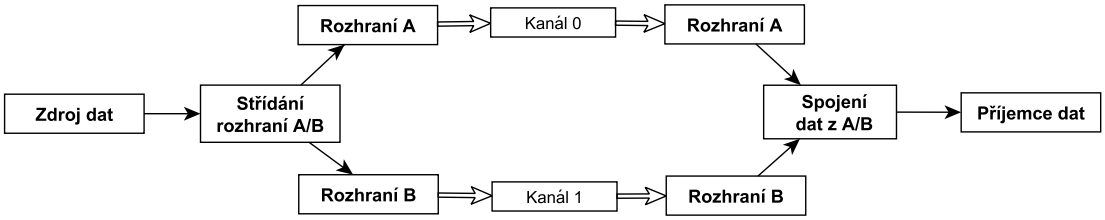
Následující část analyzuje dva pohledy na vliv chybovosti kanálu na celkovou chybovost dvou obecných přenosových schémat využívajících více přenosových kanálů - inverzní multiplexace a zálohování. Prvním je pohled použití bílého aditivního gaussovského šumu jako zdroje chyb, druhým je pak pohled vlivu chyb vznikajících interferencemi na celkovou chybovost přenosu. Specifický navržený systém přenosu dat z minulé kapitoly je následně porovnán s těmito obecnými schématy přenosu dat po více přenosových cestách. Ve všech případech jsou zvoleny dvě nezávislé bezdrátové přenosové cesty operující podle standardu IEEE 802.11g [63].

6.1.1 Popis obecných systémů přenosu

Pro možnost porovnání navrženého systému přenosu z pohledu ztrátovosti dat je potřeba zvolit referenční systémy, vůči kterým je možné vztahovat výsledky analýzy. Níže popsané metody jsou často využívané k využití více přenosových kanálů. Inverzní multiplexace, jako systém, který se snaží maximálně využít dostupné přenosové kapacity obou kanálů, stojí na opačné straně vůči systému zálohování. Ten je naopak navržen pro zachování vysoké robustnosti přenosu.

Přenosový systém inverzní multiplexace

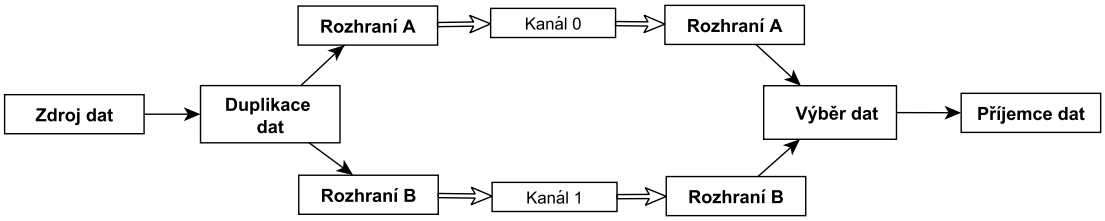
Přenosový systém, znázorněný na obrázku 15 rovnoměrně rozděluje přenášená data do dvou nezávislých kanálů. Princip je založen na předpokladu, že když každý z paralelních datových kanálů bude přenášet pouze polovinu z celkového objemu dat, tak bude možné použít pro jednotlivé kanály nižší přenosovou rychlost a tím i robustnější modulaci, která zajistí nižší chybovost přenosu dat. Celková přenosová rychlost bude v takovém případě přibližně stejná, jako u systému s jedním přenosovým kanálem.



Obrázek 15 Princip inverzní multiplexace.

Přenosový systém zálohování

Systém se zrcadlením dat na obrázku 16 využívá situaci, kdy oba paralelní přenosové kanály přenášejí zcela stejná data. Zde je nutné použít méně odolné modulační schéma v porovnání s předchozím systémem tak, aby celková propustnost dat byla stejná. Například u přenosového systému se dvěma kanály pracujícími podle standardu IEEE 802.11g a požadavkem na celkovou propustnost 24 Mbit/s bude u systému s inverzní multiplexací potřeba dvou QPSK (Quadrature Phase-shift Keying) kanálů (standard definuje přenosovou rychlost 12 Mbit/s). U systému zálohování bude nutné využít méně odolnou 16-QAM modulaci (Quadrature Amplitude Modulation), pro kterou standard definuje přenosovou rychlost 24 Mbit/s, viz tabulka 2. Celková přenosová rychlost se nezvýší, kvůli výběru pouze původních (ne již přijatých) dat na přijímací straně, ale vzhledem k paralelnímu přenosu stejných dat bude zachována vysoká odolnost přenosu a nízká celková paketová chybovost. A to přestože chybovost jednotlivých kanálů bude vyšší, z důvodu použití méně odolné modulace.



Obrázek 16 Zálohovací přenosový systém.

Toto vychází z faktu, že robustnost modulace se snižuje s větším počtem modulačních stavů [21].

$$P_{se} = \left(1 - \frac{1}{\sqrt{M}}\right) \operatorname{erfc} \sqrt{\frac{3}{2} \frac{R_s}{(M-1)}}, \tag{10}$$

kde je: P_{se} pravděpodobnost chyby symbolu [-],

M počet stavů modulace ($M = 2^b$, b je počet bitů na symbol),
R_s odstup signálu od šumu [dB].

Zmíněný odstup signálu od šumu R_s, v anglické literatuře Signal to Noise Ratio (SNR) [6], lze získat ze vztahu:

$$R_s \approx \frac{E_b}{N_0}. \tag{11}$$

E_b je střední energie signálu na bit [J/bit] a N_0 spektrální výkonová hustota šumu [W/Hz].

Rovnice 12 pak ukazuje dopad typu modulace na paketovou chybovost P_{ep} [-].

$$P_{ep} = 1 - \left[1 - \frac{2}{b}\left(1 - \frac{1}{2^{b/2}}\right) \operatorname{erfc} \sqrt{\frac{3b}{2^{b+1} - 2} R_s}\right]^{l_p}, \tag{12}$$

kde: b je počet bitů na symbol [bit],
$erfc(x)$ je Gaussova komplementární chybová funkce,
l_p je délka paketu [bit].

Za předpokladu mapování b bitových skupin do M symbolů pomocí Grayova kódu, lze bitovou chybovost vyjádřit takto:

$$P_{eb} \approx P_b \approx P_{se} \frac{2}{\log_2 M}, \tag{13}$$

kde P_{eb} [-] je bitová chybovost a P_b [-] pravděpodobnost bitové chyby.

K zjišťování bitové chybovosti z měření, lze využít následující vztah:

$$P_{eb} = \frac{m_e}{v_t \cdot t_m}, \tag{14}$$

kde m_e je počet chybně přijatých bitů, v_t je přenosová rychlost [bit/s] a t_m je celková doba měření [s].

Jelikož je většina práce zaměřena na operace s pakety, je vhodné zmínit vztah mezi bitovou a paketovou chybovostí pro pakety o délce l_p za předpokladu exponenciálního rozložení chyb:

$$P_{ep} = 1 - (1 - P_{eb})^{l_p} \tag{15}$$

Modulace a kódové poměry, které určují poměr počtu bitů uživatelské informace k celkovému počtu bitů (včetně přidané redundance) definované standardem IEEE 802.11g [63] jsou spolu s přenosovými rychlostmi ukázány v tabulce 2.

Tabulka 2 Modulace a odpovídající přenosové rychlosti podle standardu IEEE 802.11g

Modulace	**Kódový poměr**	**Přenosová rychlost**
BPSK	1/2	6 Mbit/s
BPSK	3/4	9 Mbit/s
QPSK	1/2	12 Mbit/s
QPSK	3/4	18 Mbit/s
16-QAM	1/2	24 Mbit/s
16-QAM	3/4	36 Mbit/s
64-QAM	2/3	48 Mbit/s
64-QAM	3/4	54 Mbit/s

6.1.2 Paketová chybovost pro aditivní bílý gaussovský šum

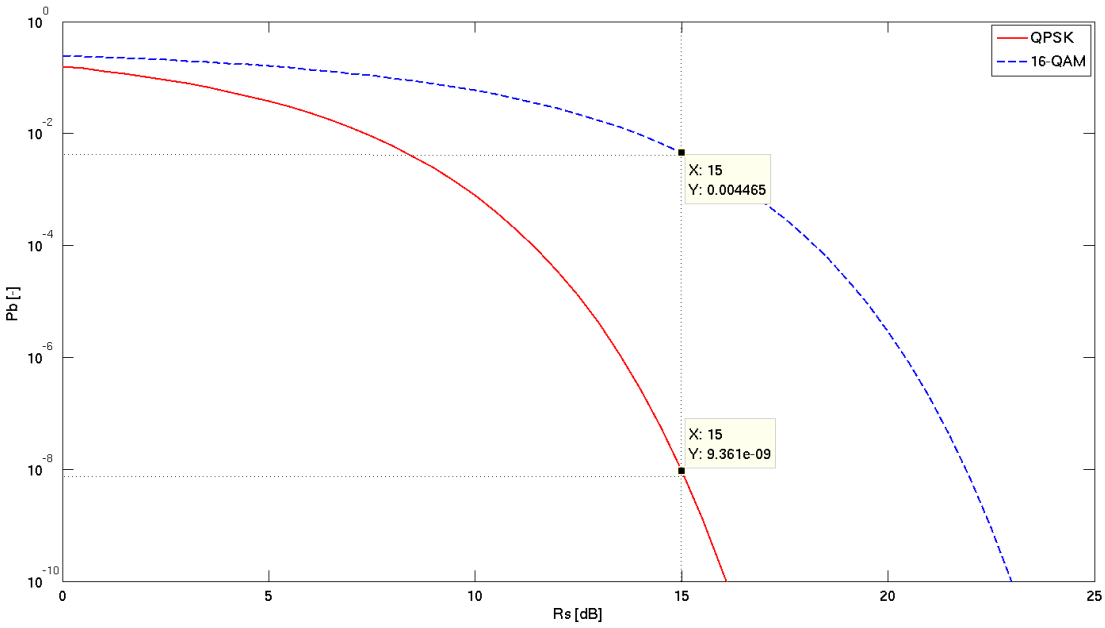
V případě, že je brán do úvahy pouze aditivní bílý gaussovský šum je rozdíl v chybovosti systému inverzního multiplexu a zálohování přibližně čtyři řády ve prospěch inverzního multiplexu. To je dáno tím, že systémy využívají modulace s různým počtem stavů, z čehož vyplývá jiná chybovost.

Pro danou modulaci jsou vzorce pro výpočet bitové chybovosti známé a jsou popsané v literatuře, například v [21]. Pro toto porovnání byla vybrána modulace 16-QAM pro zálohovací systém a QPSK modulace pro inverzní multiplex. Odpovídající bitové chybovosti pro 15 dB odstup signálu od šumu jsou ukázány na obrázku 17.

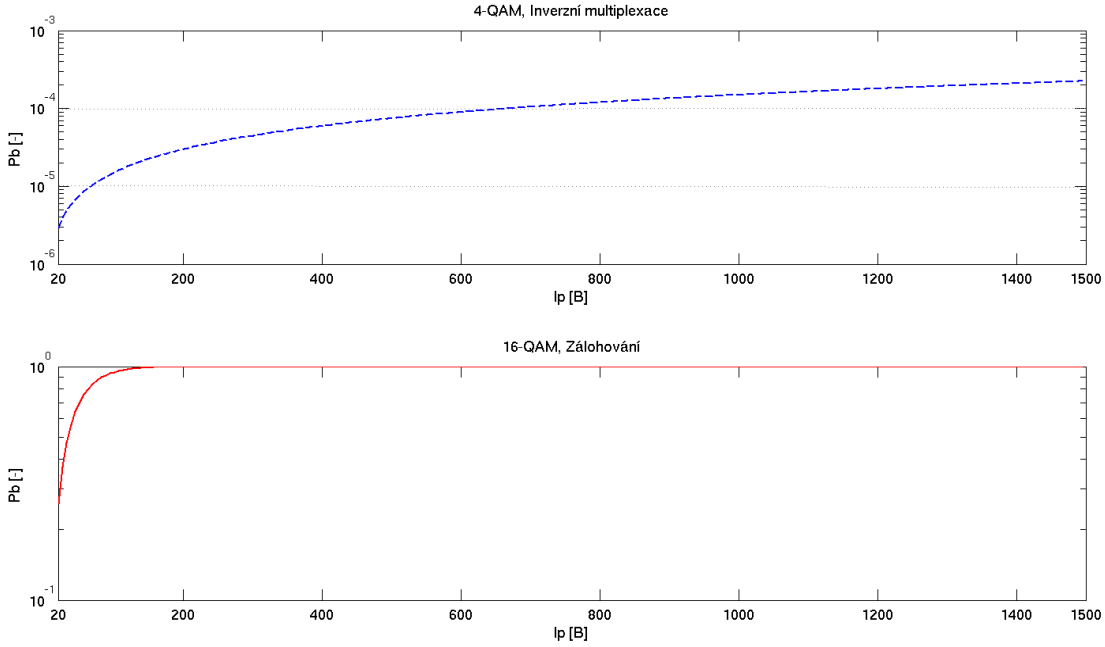
Obrázek 18 ukazuje, jak vypadají simulace zmíněných dvou systémů při použití daných modulací. Systém inverzního multiplexu vykazuje výrazně vyšší odolnost proti bitovým chybám na přenosových kanálech. To je způsobeno právě rozdílnými pravděpodobnostmi chyby pro QPSK a 16-QAM modulaci. Pro názornější pohled je délka paketů l_p vynesena v bajtech.

6.1.3 Paketová chybovost pro chyby vznikající v souvislosti s interferencemi

Druhým přístupem je zjištění, které ze schémat je více odolné vůči chybám přenosových kanálů dané interferencemi signálu na médiu. Pravděpodobnost chyby paketu je vyšší u systému inverzního multiplexu, stačí totiž, aby chyba nastala na jednom z kanálů a paket nemůže být korektně doručen. Zajímá nás totiž celková



Obrázek 17 Pravděpodobnost bitové chyby paketu pro modulace QPSK a 16-QAM.



Obrázek 18 Porovnání systémů s rozdílným typem modulace.

chybovost systému. Naopak pokud dojde k chybě na jednom z kanálů u systému zálohování, je stále možné, že paket bude doručen druhým kanálem. Tento rozdílný přístup je možné popsat následujícími rovnicemi z pohledu pravděpodob-

nostního za předpokladu, že paket je považován za chybný, pokud chyba nastane i v jediném jeho bitu.

Pravděpodobnost, že chyba nastane v intervalu délky paketu l_p u systému inverzního multiplexu:

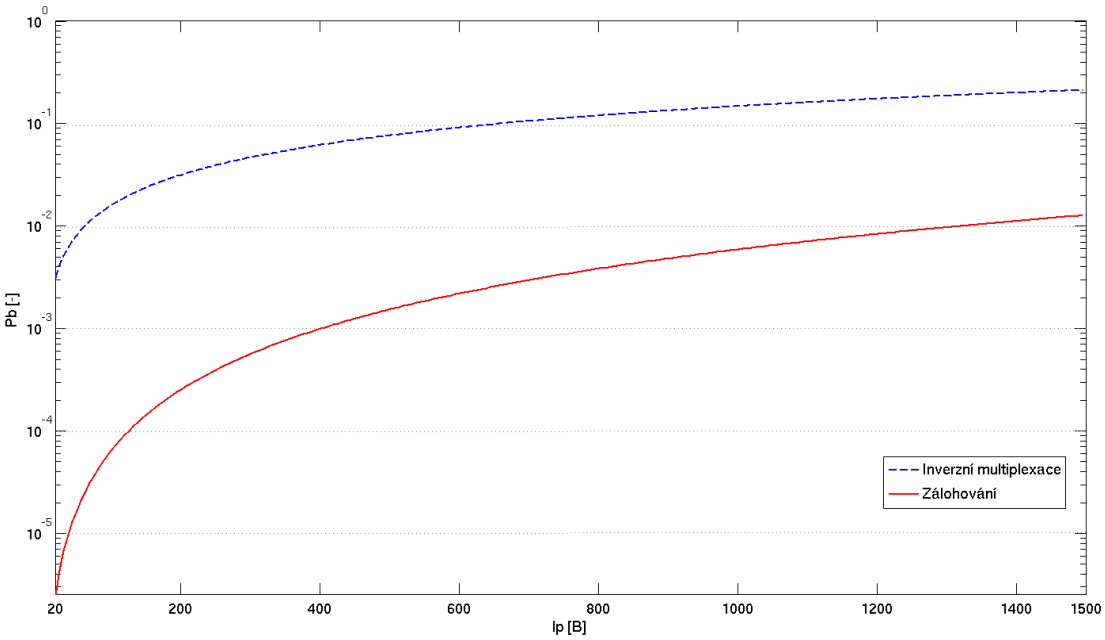
$$P_m = [1-(1-p_0)^{l_p}] + [1-(1-p_1)^{l_p}] - [1-(1-p_0)^{l_p}] \cdot [1-(1-p_1)^{l_p}]. \quad (16)$$

Pravděpodobnost, že chyba nastane v intervalu délky paketu l_p u systému zálohování:

$$P_z = [1-(1-p_0)^{l_p}] \cdot [1-(1-p_1)^{l_p}]. \quad (17)$$

Kde p_0 and p_1 jsou pravděpodobnosti chyby v jednom bitu.

Porovnání těchto pravděpodobností systému inverzního multiplexu a zálohování pro různé délky paketů, vždy pro stejnou bitovou chybovost na přenosovém médiu 10^{-5}, je pro oba systémy zobrazeno na obrázku 19. Rozdíl mezi inverzním multiplexem a zálohováním jsou přibližně tři řády ve prospěch zálohovacího přenosového systému. Z toho důvodu je například pro bezdrátové systémy ovlivněné úniky signálu či zastíněním antény vhodnější systém zálohování.



Obrázek 19 Porovnání přenosových systémů pro chyby dané interferencemi na kanálu.

6.1.4 Porovnání obecných metod s navrženým systémem přenosu

Navržený přenosový systém, znázorněný na obrázku 12 v minulé kapitole, je možné popsat pomocí pravděpodobnosti P_r, která udává, jak je pravděpodobné, že všechny originální (nekombinované) pakety dorazí do cíle bez chyby. Ať r značí počet originálních paketů a p_0, p_1 značí pravděpodobnost chyby paketu na kanálu 0 a 1, pak:

$$P_r = [(1 - p_0)(1 - p_1) + p_0(1 - p_1) + p_1(1 - p_0)]^r \tag{18}$$

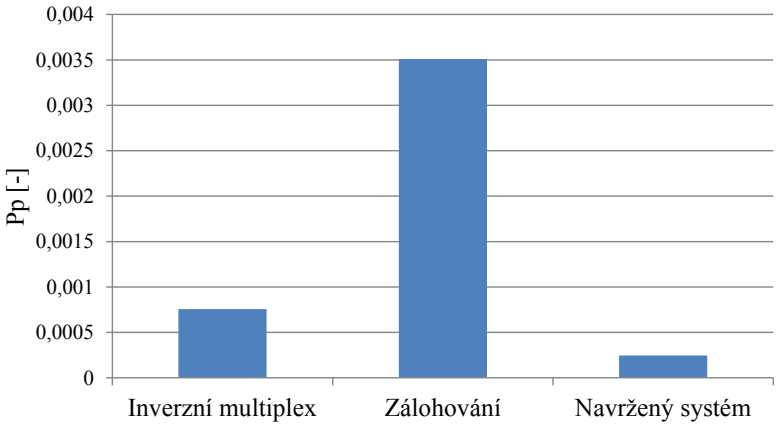
Jelikož navržený systém přenosu zasílá data v obou kanálech paralelně, je potřeba využít méně odolnou modulaci pro zachování stejné celkové přenosové rychlosti jako u systému inverzního multiplexu. Pro potřeby porovnání navrženého systému s výše popsanými systémy bude tedy využívat modulaci 16-QAM, stejně jako zálohovací systém. Pravděpodobnost chyby je pro oba kanály stejná: $p_0 = p_1 = 0,058987$. Toto číslo vychází z již zmiňovaného standardu IEEE 802.11g pro danou modulaci a z výpočtu podle rovnice 12. Pro systém inverzního multiplexu vychází díky modulaci QPSK chybovost kanálů $p_0 = p_1 = 0,0007827$. Využití jiného typu modulace je vysvětleno výše. Tabulka 3 shrnuje parametry kanálů pro jednotlivé systémy.

Tabulka 3 Výchozí chybovosti přenosových kanálů

Název systému	Inverzní multiplex	Zálohování	Navržený systém
Kanál 0	0,0007827	0,058987	0,058987
Kanál 1	0,0007827	0,058987	0,058987
Modulace	QPSK	16-QAM	16-QAM

Všechny tři systémy přenosu byly implementovány v jazyce C++ a NED a jejich funkce simulována v prostředí OMNeT++ [50]. Tento diskrétní síťový simulátor umožnil získat výsledky s vysokou přesností, díky možnosti generovat velké množství paketů (řádově 10^9) a simulace mnohokrát opakovat.

Obrázek 20 ukazuje výsledky simulace, jak je vidět, navržený systém dosáhl nejnižší celkové paketové pravděpodobnosti chyby. Přestože systém inverzního multiplexu měl pravděpodobnost chyby v jednotlivých kanálech 75,36 krát nižší, přesto je jeho výsledek třikrát horší oproti navrženému systému. To je dáno hlavně schopností opravy a redundancí obsaženou v druhém přenosovém kanálu systému. Zálohovací systém, přestože obsahuje plnou redundanci v druhém kanálu, vykázal



Obrázek 20 Výsledky celkové paketové pravděpodobnosti chyby systémů ze simulace.

kvůli nižší odolnosti modulace nejhorší výsledek. Detailně jsou výsledky ukázány v tabulce 4.

Tabulka 4 Výsledky simulace

Název systému	Inverzní multiplex	Zálohování	Navržený systém
Chybovost	0,000757	0,003509	0,000247
Konfidenční interval	8,478e-7	8,059e-7	4,100e-7

6.2 Analýza z pohledu zpoždění přenosu

Tato část se zabývá vlivem navrženého přenosového schématu na zpoždění přenosu dat. Jsou zde popsány jednotlivé součásti celkového zpoždění přenosu a také analyzován vliv přidaného zpoždění daného dekódováním podle navrženého schématu v případě korektně nedoručeného paketu. Dále je navržené schéma z pohledu přidaného zpoždění porovnáno s technikou využívající retransmise pro dosažení vyšší odolnosti přenosu.

6.2.1 Zdroje zpoždění

Jedním z nejdůležitějších parametrů v komunikačních sítích je zpoždění přenosu dat. Jeho hodnoty mají vliv na rozhodování o vhodnosti nasazení dané technologie, na možnost využití určitých služeb, nebo například i na rozhodování směrovacích algoritmů. Zpoždění, jakožto čas, který je potřebný k přenesení informace od zdroje k příjemci, je možné rozdělit do několika druhů [64][65], které různou měrou prodlužují celkový čas přenosu. Některé druhy lze, vzhledem k jejich malé hodnotě, považovat pro určité služby za zanedbatelné, jiné zásadně ovlivňují celý přenos. Zpoždění lze dále dělit podle místa vzniku, zda jsou zdrojem koncové body komunikace, mezilehlé body komunikace, či přenosové cesty [66].

Zpoždění v koncových bodech komunikace Zpoždění v koncových bodech vzniká již při převodu informace na pakety. V závislosti na použité technologii se jedná hlavně o zpoždění kodéru či dekodéru (převod hovorového signálu na elektrický signál) a paketizéru či depaketizéru (zapouzdření datových bloků do paketů podle požadavků síťové vrstvy). Dále pak nezbytné algoritmické a kompresní zpoždění, více lze nalézt například v [67]. V závislosti na vytížení daného koncového bodu se může různou měrou projevit vliv odchozích, respektive příchozích front. U služeb vyžadujících plynulý tok dat v pravidelných intervalech se může projevit další druh zpoždění daný vyrovnáváním kolísání velikosti zpoždění. U navrženého schématu přenosu dat jsou koncové body navíc zodpovědné za procesní zpoždění dané kódováním a dekódováním. Délka nutná pro tyto operace je závislá na konkrétním nastavení daného schématu.

Zpoždění v mezilehlých bodech komunikace Každý mezilehlý bod komunikace vloží do spojení určité procesní zpoždění. Velikost tohoto zpoždění je dána vytížením, množstvím a složitostí operací, které s daným paketem konkrétní bod provádí. Další významnou roli v celkovém přenosovém zpoždění hrají priority pro určité druhy služeb, které zasahují do rychlosti zpracování dat v mezilehlých, ale

i koncových bodech komunikace. Vliv vytížení front příchozích i odchozích hraje roli také v mezilehlých bodech.

Zpoždění na přenosových cestách Zpoždění dané dobou šíření informace (tzv. propagační zpoždění) závisí na délce přenosové linky, tedy fyzické délce přenosového kanálu, který obecně může používat i více druhů přenosových prostředí. Jedná se o nevyhnutelnou součást danou fyzikální podstatou přenosu dat. Rychlost šíření elektromagnetických vln se liší podle přenosového prostředí, jak je níže v textu naznačeno v tabulce 6. Přenosová rychlost a velikost posílaných bloků dat určuje velikost serializačního zpoždění, tedy doby od začátku do konce odeslání bloku dat z paměti komunikačního bodu na přenosovou linku. V případě přenosu dat u technologií se sdíleným médiem (například Ethernet, bezdrátové technologie) se může významně zvýšit zpoždění čekáním na uvolnění přístupu k médiu, více o této problematice například v [68].

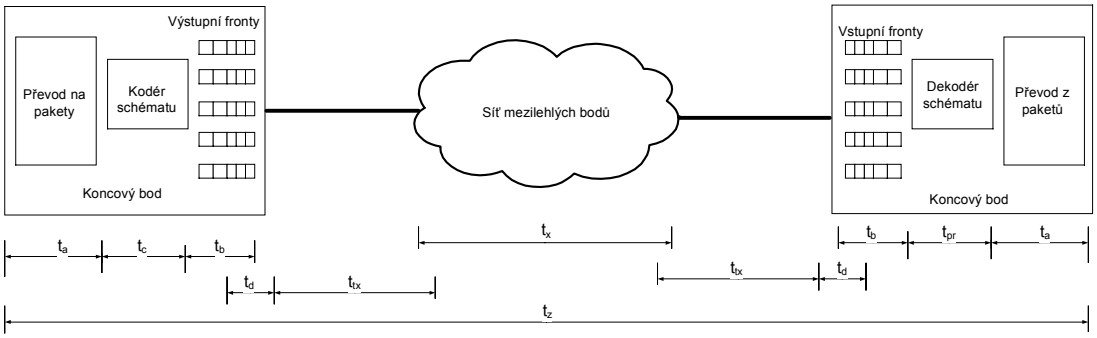
Různé druhy služeb vyžadují udržení celkového zpoždění a jeho kolísání do určité meze, dané příslušným standardem. Například pro služby založené na protokolu IP platí podle standardu ITU-T Y.1541 [69] hodnoty pro třídy Quality of Service (QoS) vypsané v tabulce 5. Do třídy 0 a 1 spadají služby pracující s daty v reálném čase, citlivé na kolísáním velikosti zpoždění (např. VoIP), do třídy 2 a 3 spadá signalizace, interaktivní data. Třída 4 zahrnuje služby vyžadující pouze krátké výpadky (video přenosy) a třída 5 pak běžný provoz bez zvláštních nároků. Přenosové zpoždění je důležitý parametr i vzhledem k jeho dopadu na výsledný počet chyb paketů. Paket je považován za ztracený pokud jeho hodnota zpoždění překročí určitý limit. Tento limit závisí na požadovaném standardu či třídě (viz například tabulka 5).

Tabulka 5 Horní limit střední hodnoty zpoždění a kolísání zpoždění IP paketu podle ITU-T Y.1541 (U - nespecifikováno)

	Třídy QoS				
	1	2	3	4	5
Zpoždění paketu	100 ms	400 ms	100 ms	1 s	U
Kolísání zpoždění	50 ms	50 ms	U	U	U

Na obrázku 21 je zobrazen přehled zmiňovaných zpoždění (jednotkou pro všechna zmiňovaná zpoždění je sekunda). Obrázek spojení se sestává ze dvou koncových bodů a sítě mezilehlých bodů komunikace. t_a souhrnně označuje zpoždění na koncových bodech vzniklé procesem převodu mezi informací a pakety, t_b označuje zpoždění ve frontách a zpoždění t_c je dané kódováním zvoleným přenosovým

schématem. t_d označuje serializační zpoždění a t_{tx} propagační zpoždění. Zpoždění dané mezilehlými body komunikace t_x se skládá z výše zmiňovaných součástí a to pro každý z bodů, přes který komunikace probíhá. Každé spojení mezi body přidává i propagační zpoždění. Procesní zpoždění dané dekódováním podle zvoleného přenosového schématu je označeno jako t_{pr} a t_z značí celkové zpoždění komunikace.



Obrázek 21 Náhled součástí celkového přenosového zpoždění.

6.2.2 Zpoždění navrženého schématu

Důležitou charakteristikou přenosového schématu je průměrné přidané zpoždění paketů dané algoritmem korekce chybných dat. Hodnota zpoždění má zásadní dopad na možnost využití schématu pro konkrétní službu. Střední hodnota zpoždění paketů a rozptyl zpoždění jsou důležité hlavně pro služby pracující s daty v reálném čase, například pro VoIP [70].

Střední hodnota zpoždění paketů t_μ [s], ukázaná v rovnici 19, je dána součtem zpoždění ze všech paketů daného přenosu děleným počtem všech přijatých paketů. Pro vybrané konkrétní schéma z kapitoly 5.3 je z pohledu přidaného zpoždění důležité rozlišovat, která varianta procesu obnovy byla provedena během procesu dekódování. Velikost přidaného zpoždění je tedy závislá na množství chybně doručených či ztracených paketů a tím pádem na variantě obnovy.

$$t_\mu = \frac{\sum_{i=0}^{3} \eta_i t_i}{\sum_{i=0}^{3} \eta_i}, \tag{19}$$

kde t_i je zpoždění pro jeden paket (viz rovnice 22), spodním indexem je rozlišeno mezi jednotlivými variantami obnovy (varianta první $i = 1$, druhá $i = 2$, nebo

třetí $i = 3$). Index 0 odpovídá situaci, kdy rekonstrukce paketu není potřebná (tj. paket byl doručen korektně). Hodnoty počtu korektně doručených paketů η_0 a paketů prošlých určitou variantou obnovy $\eta_{1,2,3}$ vycházejí ze součinu počtu poslaných paketů N_o a pravděpodobnosti, že nastane situace vhodná pro daný typ obnovy $\gamma_{0,1,2,3}$. Toto je ukázáno v rovnicích 20. Součet $\sum_{i=0}^{3} \eta_i$ se pak rovná celkovému počtu doručených paketů.

$$\begin{aligned} \eta_0 &= \gamma_0 N_o \\ \eta_1 &= \gamma_1 N_o \\ \eta_2 &= \gamma_2 N_o \\ \eta_3 &= \gamma_3 N_o \end{aligned} \tag{20}$$

Pro pravděpodobnost, že nenastala chyba daného paketu (γ_0), dále pro pravděpodobnosti, že situace vhodná pro danou variantu obnovy nastala ($\gamma_1, \gamma_2, \gamma_3$) a pro pravděpodobnost, že paket nebyl doručen platí:

$$\gamma_0 + \gamma_1 + \gamma_2 + \gamma_3 = 1 - \gamma_4 \tag{21}$$

Pravděpodobnost toho, že paket nebude doručen ani obnoven je označena jako γ_4.

Proměnná t_i v rovnici 19 nabývá hodnot popsaných následovně:

$$\begin{aligned} t_0 &= t_d + t_{tx} + t_{pr_0} \\ t_1 &= t_d + t_{tx} + t_{pr_1} \\ t_2 &= 2t_d + t_{tx} + t_{pr_1} \\ t_3 &= 3t_d + t_{tx} + t_{pr_2}. \end{aligned} \tag{22}$$

t_d značí serializační zpoždění, t_{tx} propagační zpoždění a $t_{pr_{0,1,2}}$ procesní zpoždění. Hodnoty indexů u $t_{pr_{0,1,2}}$ odpovídají počtu nutných XOR operací na straně dekodéru. Zmíněné procesní zpoždění, odlišující se podle varianty dekódovacího procesu, nebude mít zásadní vliv na celkové zpoždění, neboť operace XOR, jakožto lineární operace, není výpočetně náročná. Další druhy zpoždění zmíněné v úvodu kapitoly jsou pro potřeby popisu schématu nepodstatné.

Serializační zpoždění t_d lze spočítat jako:

$$t_d = \frac{l_p}{v_t}, \tag{23}$$

kde l_p je délka paketu v bitech a v_t je bitová rychlost kanálu v bitech za sekundu [71]. Počet, kolikrát je serializační zpoždění zahrnuto v rovnicích 22, je dáno počtem paketů, nutných pro danou variantu obnovy. Podrobněji je toto chování vysvětleno v kapitole 5.3.

Propagační zpoždění t_{tx} [s] je možné odhadnout z fyzické délky spojení s mezi odesílací a přijímací stranou [m] a z rychlosti šíření signálu v $[ms^{-1}]$:

$$t_{tx} = \frac{s}{v}. \tag{24}$$

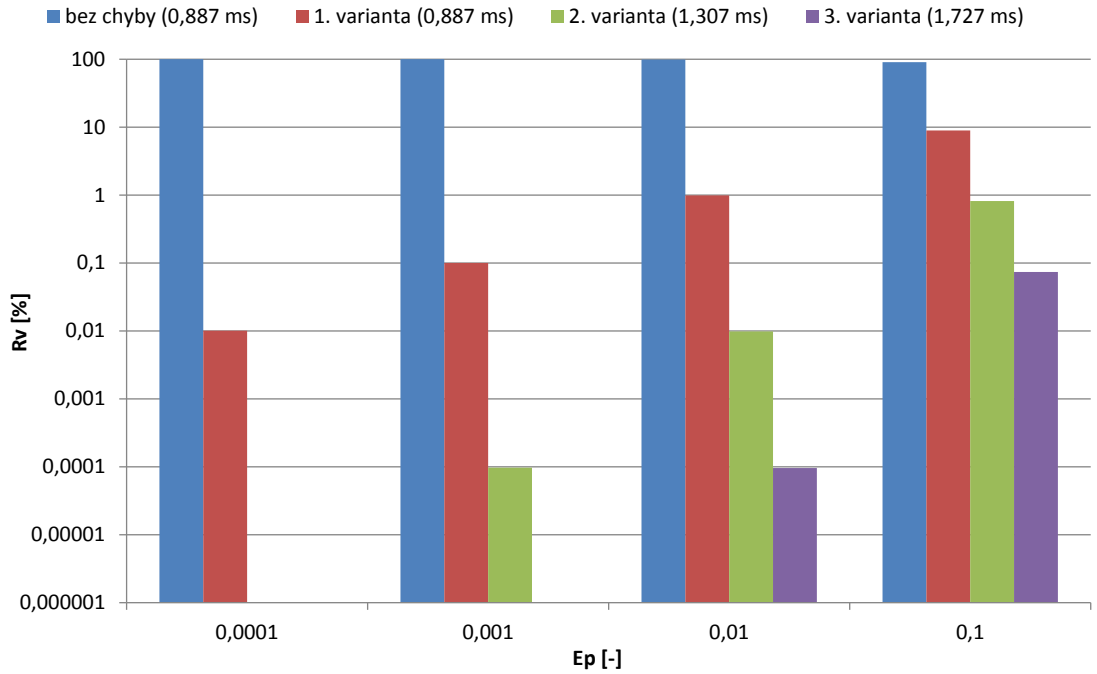
Hodnoty rychlosti šíření signálu v jednotlivých typech přenosových médií a jejich fyzikální vazby k rychlosti světla ve vakuu jsou zobrazeny v tabulce 6, kde c je rychlost šíření elektromagnetických vln ve vakuu $[ms^{-1}]$, ε_r je relativní permitivita izolace vodiče symetrického páru [-] a n_d je index lomu jádra optického vlákna [-].

Tabulka 6 Rychlosti šíření signálu [65][68]

Technologie přenosu	**Hodnota**	**Výpočet**
metalická	$\sim 1,80 \cdot 10^8 - 2,40 \cdot 10^8\ ms^{-1}$	$v = \frac{c}{\sqrt{\varepsilon_r}}$
optická	$\sim 2,05 \cdot 10^8\ ms^{-1}$	$v = \frac{c}{n_d}$
rádiová	$\sim 2,99 \cdot 10^8\ ms^{-1}$	$v \simeq c$

Pro zjištění dopadu navrženého přenosového schématu na zpoždění přenosu dat bylo navržené schéma naprogramováno a odsimulována jeho funkce v programu OMNeT++. Stejně tak byla naprogramována funkce schémat přenosu zálohování a inverzní multiplexace, a to ve variantě bez i s povolenou retransmisí nedoručených paketů.

Rozložení četnosti výskytu chybných paketů pro tři varianty obnovy navrženého schématu a četnost výskytu korektně doručených paketů je ukázána na obrázku 22. Graf zobrazuje výsledky čtyř simulací schématu, jednotlivé simulace se lišily nastavenou paketovou chybovostí přenosových kanálů $10^{-4}, 10^{-3}, 10^{-2}$ a 10^{-1}. Na svislé ose je vynesen procentuální poměr paketů spadajících do dané varianty obnovy vůči všem doručeným paketům R_v. V každé simulaci bylo odesláno 10^9 paketů délky 1250 B přenosovou rychlostí 24 Mbit/s, vzdálenost koncových stanic byla nastavena na 10 km. Část grafu pro chybovost 10^{-4} obsahuje pouze dva sloupce v důsledku nižší hodnoty chybovosti. A to sloupec pro pakety doručené bez chyby a pro první variantu obnovy. Situace pro druhou a třetí variantu (tedy více než jeden nedoručený paket v řadě) během simulace nenastala.



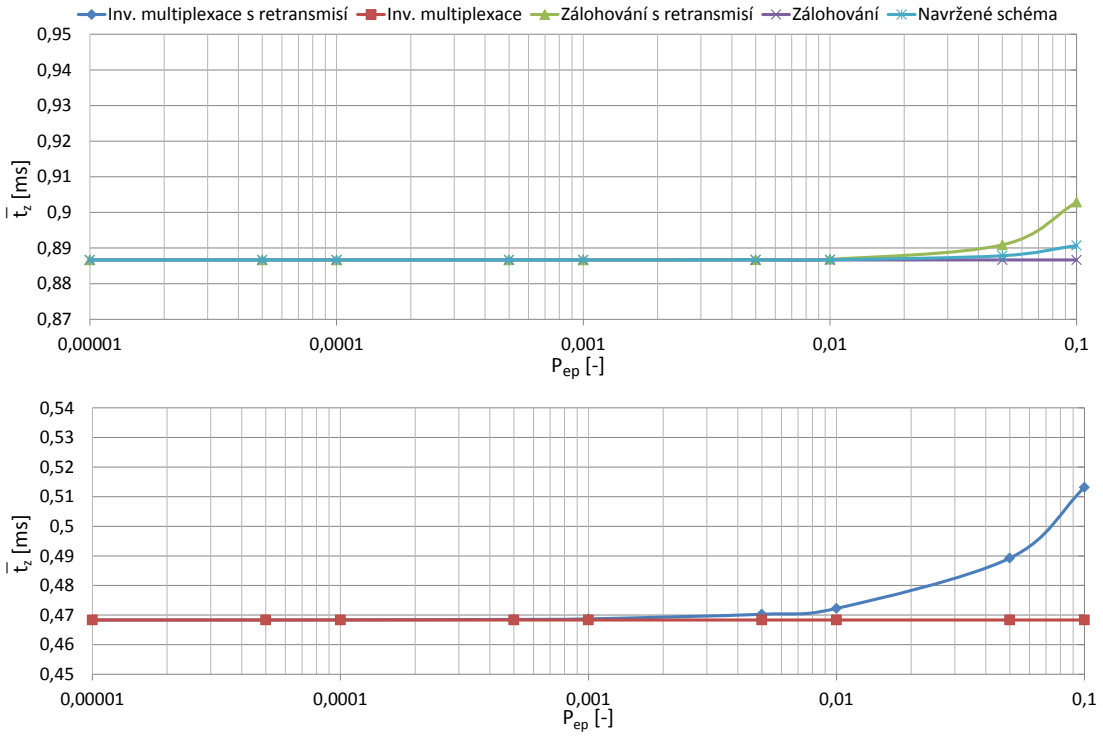
Obrázek 22 Průměrné hodnoty zpoždění přenosu a jeho rozložení u navrženého schématu pro různé paketové chybovosti přenosových kanálů.

Simulace pro vyšší chybovosti kanálů již ukazují, jak četné byly jednotlivé varianty obnovy. Navíc se s vyšší chybovostí přenosových kanálů zvyšuje průměrné zpoždění paketů. To je dáno častějším výskytem více časově náročných variant obnovy. Hodnoty průměrného zpoždění pro danou variantu obnovy jsou součástí legendy grafu. Procesní zpoždění XOR operace je zanedbatelné vůči ostatním složkám zpoždění paketu, z tohoto důvodu je hodnota zpoždění pro první variantu obnovy a situaci bez nutnosti obnovy stejná (což odpovídá rovnici 22). Rozptyl hodnot zpoždění je zanedbatelný z důvodu výrazně převažujícího počtu paketů korektně doručených, ty mají totiž vždy přibližně stejné zpoždění neovlivněné variantou obnovy, lišící se jen kolísáním zpoždění dané přenosovým řetězcem.

Tyto výsledky jsou užitečné k pochopení, pro jaké hodnoty chybovosti přenosových kanálů se hodí různé varianty obnovy navrženého schématu a pro jaké hodnoty chybovosti přenosových kanálů slouží navržené schéma k dosažení vyšší odolnosti přenosu dat.

Na obrázku 23 jsou dva grafy ukazující průběh průměrné hodnoty zpoždění v závislosti na paketové chybovosti přenosových kanálů pro porovnání různých schémat přenosu. V tomto případě bylo zpoždění na paket počítáno z celkového času přenosu. Navržené schéma vykazuje malé navýšení zpoždění o 0,5 % při nejvyšší simulované chybovosti kanálů vůči zpoždění při nízkých chybovostech. Toto na-

výšení je dáno vyšším počtem více komplexnějších (a časově náročnějších) variant obnovy paketů. Nicméně je toto navýšení nejmenší ze všech simulovaných schémat. Zálohovací schéma, stejně tak i inverzní multiplex, má konstantní hodnotu průměrného zpoždění paketů. To je logický důsledek toho, že daná schémata neprovádějí žádnou obnovu v případě nedoručení paketu ani neprovádějí opakování jeho přenosu. Zálohovací schéma s povoleným opakováním přenosu nedoručených paketů vykázalo téměř dvou procentní nárust průměrné doby zpoždění paketů při paketové chybovosti kanálů na hodnotě 0,1. Tento nárust, s počátkem při chybovosti kanálů 0,01, je způsoben delším časem, který je nutný v případě nedoručení paketu a čekání na jeho opětovné zaslání.



Obrázek 23 Porovnání průměrného přenosového zpoždění pro paketovou chybovost kanálů od 10^{-5} do 10^{-1}.

Zmíněný nárust, nicméně mnohem větší, je zobrazen na spodní části obrázku 23. Spodní graf je oddělen záměrně pro lepší zobrazení výsledků schématu inverzního multiplexu. Inverzní multiplex využívá výhody posílání různých dat oběma přenosovými kanály. Z toho důvodu je zde sice nižší redundance v porovnání s ostatními simulovanými schématy, ale doba přenosu je poloviční, protože každým kanálem je posílána pouze polovina z celkového počtu paketů. Tím i z doby přenosu dopočítané průměrné zpoždění je poloviční, i když je přenosová rychlost ka-

nálů nastavená pro všechna schémata stejně. Zato schéma inverzního multiplexu s povoleným znovuzasíláním nedoručených paketů vykazuje nejrychlejší nárust zpoždění jako důsledek nejnižší robustnosti mezi testovanými schématy přenosu. Průměrné zpoždění paketů bylo počítáno pouze z doručených paketů, v opačném případě by zpoždění rostlo do nekonečna.

6.2.3 Analýza vlivu retransmisí

Robustnost přenosu dat je důležitou součástí navrženého schématu přenosu, nicméně návrh záměrně neuvažuje použití retransmisí, tedy opětovného zasílání paketů v případě jejich nedoručení. Namísto toho umožňuje navržené schéma možnost dekódování nedoručených paketů z již doručených. Tento přístup byl zvolen jelikož retransmise mají, dále rozvedený, negativní vliv na celkovou bilanci přenosu dat.

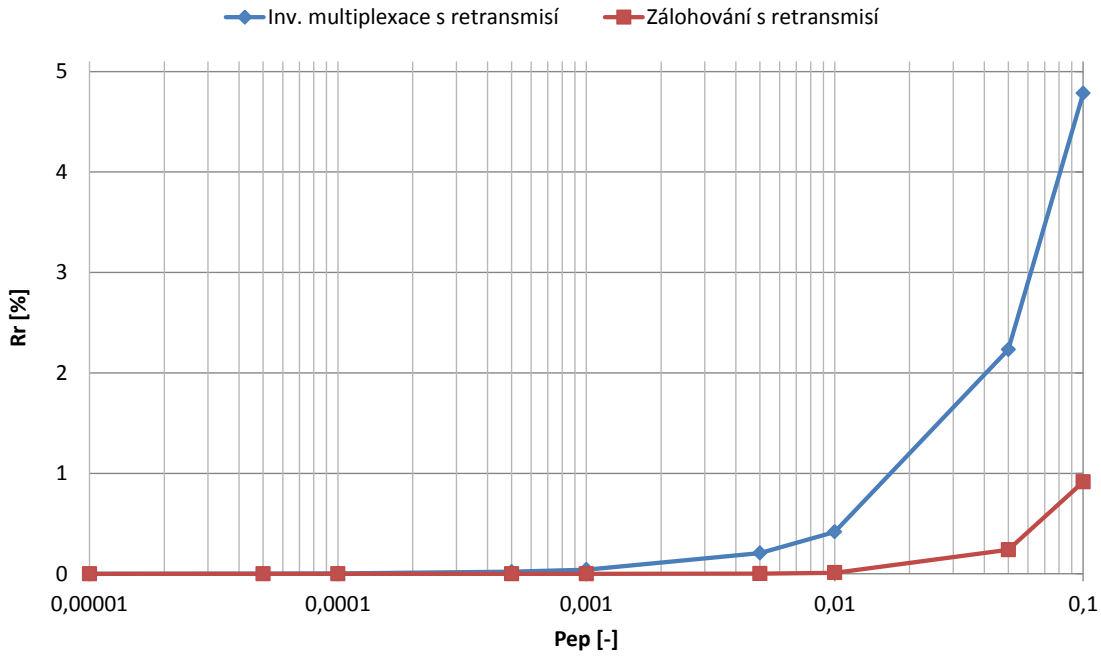
Nevýhody retransmisí jsou důsledkem více jevů. Například čím více retransmisí nastane během přenosu dat, tím delší je celkový čas přenosu a tím je i hodnota celkové propustnosti nižší. Tuto vlastnost lze popsat rovnicí 25.

$$t_r = t_f + 2e_n \left(\frac{t_f}{N_o} \right), \tag{25}$$

kde: t_r je celkový čas přenosu souboru dat [s], t_f je čas bez retransmisí [s], e_n je počet chybných paketů a N_o reprezentuje kompletní počet poslaných paketů.

Konkrétní demonstrace porovnání simulací běžných schémat přenosu dat po více cestách je na obrázku 24. Graf na obrázku ukazuje procentuální poměr retransmisí paketů vůči původnímu množství zasílaných paketů R_r v závislosti na paketové chybovosti přenosových kanálů (pro oba kanály je nastavena vždy stejná hodnota chybovosti). Zálohovací schéma těží výhodu vyšší redundance oproti inverznímu multiplexu. Čím je totiž méně paketů nedoručeno příjemci, tím méně retransmisí paketů je potřeba. Množství retransmisí v případě schématu inverzního multiplexu rychle roste od chybovosti kanálů 0,001, zatímco tempo růstu u zálohovacího schématu je výrazně nižší.

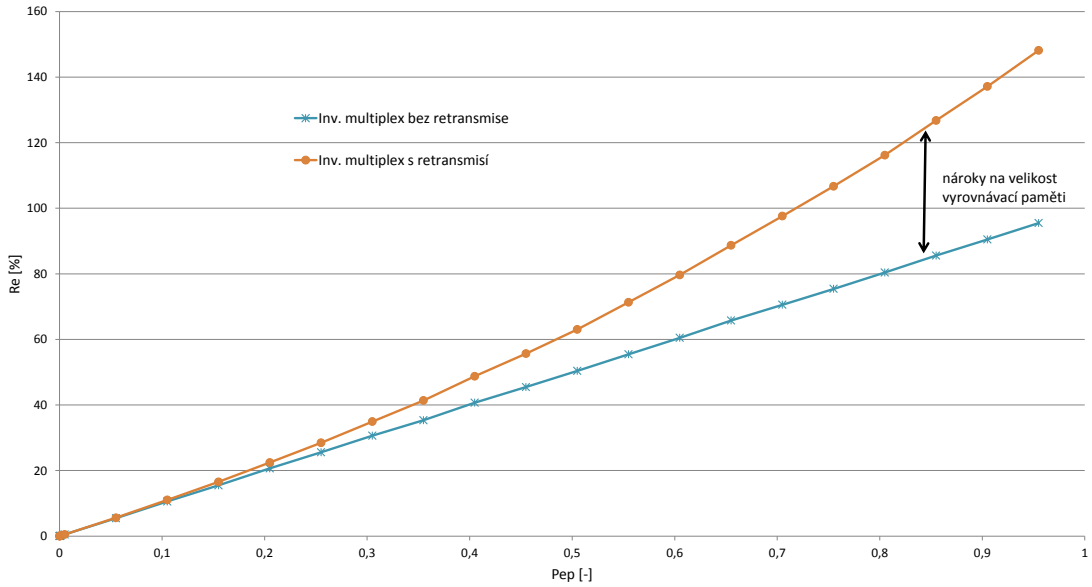
Dalším negativním jevem zvýšeného počtu přenášených paketů v důsledku retransmisí vede ke snížení propustnosti pro přenos dalších, nových dat. Při retransmisi dojde k vygenerování nejprve nového paketu s žádostí o zaslání ztraceného paketu. Ten je zaslán zpět k odesílateli a pak je teprve opětovně vyslán nedoručený paket. Dochází tedy k navýšení přenosu o dva pakety při ztrátě jednoho původního paketu. Toto chování je samozřejmě vázáno na použitém typu mechanismu ARQ.



Obrázek 24 Porovnání množství retransmisí pro schémata zálohování a inverzní multiplex.

Retransmise mají také negativní vliv na chování přenosového kanálu v případě přenosu dat po sdíleném médiu, obzvláště u bezdrátových přenosových technologií kde dochází k zahlcování sdíleného média. Tuto situaci demonstruje obrázek 25, na kterém jsou výsledky simulace schématu inverzní multiplexace bez a s povolenou retransmisí. Simulace byly provedeny pro jednotlivé paketové chybovosti kanálů s krokem 0,05. Na svislé ose je vyneseno procento chybných paketů R_e, vztažené k množství původně zasílaných dat (tedy k počtu paketů souboru dat, který měl být přenesen). Lze vidět, že křivka množství chybných paketů má zvyšující se tendenci s nárustem chybovosti přenosových kanálů, čímž zpoždění i nároky na paměť systému rostou. Dostatečně velké vyrovnávací paměti totiž opět souvisí s retransmisemi. Čím více paketů je opětovně zasíláno, tím větší musí být vyrovnávací paměť na obou koncích přenosu. Odesílatel musí dokázat zpětně vyhledat nedoručený paket a znovu jej zaslat. Příjemce musí udržovat v paměti, které pakety chybějí a v případě nutnosti dodržení pořadí paketů musí ještě udržovat v paměti i korektně doručené pakety, tak aby je pak bylo možné ve správném pořadí předat dále. Případný nedostatek místa ve vyrovnávací paměti navíc způsobí další ztráty a následné retransmise paketů.

Relativně malá procentuální ztráta paketů na nižší vrstvě může způsobit vysokou ztrátovost na vyšších vrstvách, například u TCP spojení dochází k zahození



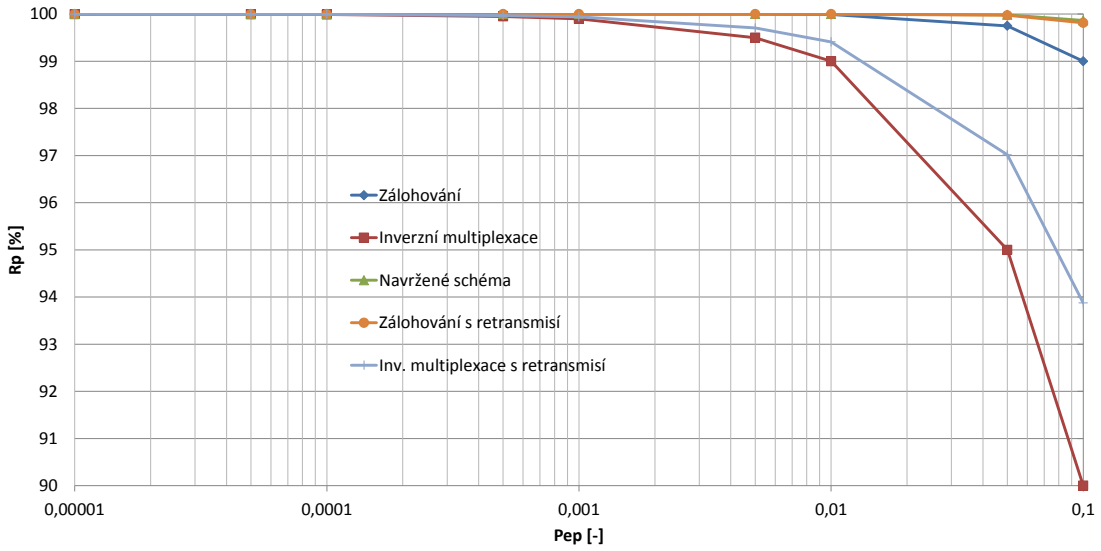
Obrázek 25 Ukázka nároků na velikost vyrovnávací paměti.

celého okna dat. Na vyšších vrstvách RM OSI mohou retransmise také způsobovat problémy. Například u TCP protokolu čtvrté vrstvy řeší congestion window (CWND) mechanismus případ ztráty potvrzovacího paketu tak, že v případě, že daný paket není doručen do určitého času je považován za ztracený a TCP congestion window je zmenšeno na polovinu (a tím také propustnost). Velikost okna se opět začne navyšovat, pokud potvrzovací pakety budou doručovány korektně (v časovém limitu). Ztráta paketu má dva efekty na propustnost přenosu: pakety jsou znovuzasílány (i v případě, že je ztracen pouze potvrzovací paket) a velikost TCP congestion window nedovolí optimální propustnost [72].

Při pohledu na situaci, jak ztráta dat ovlivňuje vyšší protokoly, je jasná závislost na konkrétní implementaci daného protokolu. Například u výše zmíněného protokolu TCP, který zajišťuje spolehlivou přenosovou službu, ztráta paketu způsobí opětovné zaslání všech do té doby vyslaných následujících dat. Při jiné, efektivnější implementaci tohoto protokolu podle RFC 2018 [73], která specifikuje využití tzv. výběrového potvrzování (selective acknowledgement), je potřeba zvýšit velikost vyrovnávací paměti pro provoz protokolu. Tato implementace umožňuje přijímači potvrzovat nespojité bloky korektně přijatých dat. Odesílatel tedy zasílá menší množství dat, pouze ty chybějící, nicméně přijímač mezitím musí udržovat zbylé pakety mezi chybějícími bloky v paměti. Pokud je přenosový systém provozován v prostředí s vyšší chybovostí, musí být obecně velikost vyrovnávací paměti větší. V opačném případě by totiž docházelo k snížení efektivní propustnosti z důvodu nedostatečné kapacity paměti a tím způsobenými častějšími opakováními

přenosu dat.

Mechanismu retransmisí ovšem přísluší i pozitivní vliv na celkovou odolnost přenosu. Pro znázornění, jak se různá schémata s či bez retransmisí dokáží vyrovnat s paketovými chybami během přenosu, byly provedeny simulace navrženého schématu i obou dalších porovnávaných schémat. Simulace byly provedeny pro paketovou chybovost přenosových kanálů v rozmezí od 10^{-5} do 10^{-1}, tato chybovost byla v simulaci nastavena stejně pro oba přenosové kanály. R_p na svislé ose označuje procento přijatých paketů, 100 % označuje všechna data určená k odeslání. Výsledky jsou na obrázku 26. Schéma inverzního multiplexu se ukázalo býti nejméně efektivním z důvodu jeho nulové redundance. V případě stejného schématu, ale již s povolenou retransmisí případného ztraceného paketu se zvýšil celkový počet doručených paketů, nicméně rozdíl vůči ostatním schématům je stále značný. Prudký pokles doručených paketů začíná o řád chybovosti kanálu dříve v porovnání se zálohovacím schématem.



Obrázek 26 Efektivita přenosu pro paketovou chybovost přenosových kanálů od 10^{-5} do 10^{-1}.

Zálohovací schéma využívá výhody plně redundantního přenosu dat, stejná data jsou na obou kanálech. Efektivnost přenosu zůstává na 99,9 % až do chybovosti kanálu 0,01. V případě varianty s retransmisí je 99,9 procentní efektivita prodloužena až do simulace s chybovostí kanálů 0,05.

Navržené schéma prokázalo být nejrobustnějším z porovnávaných přenosových schémat. Rozdíl oproti zálohovacímu schématu s povolenou retransmisí se může zdá zanedbatelný, ale je potřeba zmínit, že daná úroveň efektivnosti je u navr-

ženého schématu dosažena bez opakování přenosu jediného paketu, tj. s nižším celkovým zpožděním přenosu. V porovnání se zálohovacím schématem, ve variantě bez retransmisí, je navržené schéma výhodnější až o jedno procento pro chybovost kanálů 0,1.

6.3 Dílčí závěry

- Pro simulaci celkové chybovosti přenosu dat schématu inverzní multiplexace, zálohování a navrženého schématu, bylo využito rozdílných pravděpodobností pro kanály jednotlivých schémat. Tyto výchozí pravděpodobnosti chyby na přenosových kanálech byly dány principem fungování jednotlivých schémat, který jim umožňuje, při zachování stejné přenosové rychlosti, využít více či méně odolné modulace. Z následného porovnání výsledků simulace funkce těchto schémat vyplynul jednoznačný přínos navrženého schématu, jako nejrobustnějšího z testovaných.

- Při analýze zpoždění, způsobeného dekódovacím mechanismem navrženého schématu bylo zjištěno, že jeho velikost závisí na variantě obnovy dat, která nastala. Ta je dána počtem po sobě jdoucích chybných paketů. Další dvě porovnávaná schémata mají hodnotu zpoždění nezávislou na počtu chybných paketů. Velikost celkového zpoždění při jejich použití je tedy vždy nižší, nebo stejná, jako u navrhovaného schématu. Při využití retransmisí u schématu inverzní multiplexace a zálohování tak, aby se jejich robustnost zvětšila, se situace mění a navržené schéma dosahuje lepších hodnot celkového zpoždění.

7 Ověření navrženého schématu na naměřených datech

Pro další ověření chování navrženého přenosového schématu bylo provedeno měření pro získání parametrů zpoždění přenosu dat a paketové chybovosti v reálných podmínkách českých mobilních sítí. Simulační modely navrženého přenosového schématu a schématu zálohování pak bylo nutné koncipovat tak, aby byly schopné pracovat s datovými kanály, které vykazují časově závislé parametry získané z měření. Z důvodu možnosti porovnání z pohledu robustnosti přenosu bylo podobně koncipováno i schéma zálohování.

7.1 Měření parametrů mobilních sítí

Cílem měření bylo získání dat, které by umožnily zajistit v simulačním nástroji reálné chování kanálů v mobilních sítích. Pro získání parametrů paketové chybovosti a zpoždění přenosu bylo zvoleno přenosové prostředí mobilních bezdrátových sítí a technologie EDGE (Enhanced Data rates for GSM Evolution). Tato technologie je v současné době nejrozšířenější z nabídky služeb mobilních datových přenosů na území České republiky a pokrývá téměř 100 % území (podle [74]). V závislosti na kódovém a modulačním schématu a na využití časových slotů nabízí technologie přenosové rychlosti v řádech desítek až stovek kilobitů za sekundu (obvykle do 200 kbit/s v sestupném a 100 kbit/s ve vzestupném směru).

Měření probíhalo pomocí zařízení MultiComm, vyvíjeném na katedře telekomunikační techniky FEL ČVUT. Toto zařízení využívá více (až čtyři) paralelní bezdrátové kanály k přenosu dat mezi klientskou a serverovou částí. Více informací lze nalézt v kapitole 4. Pro potřeby toho měření byly využity dva kanály, jeden pro síť T-Mobile, druhý pro O2. Samotné měření probíhalo při pohybu testovacího vozu, na jehož střeše byla umístěna platforma s anténním systémem zobrazeným na obrázku 27. Spojení se základnovými stanicemi zajišťovaly dvoupásmové cloverleaf antény pro GSM frekvenční pásmo 900/1800 MHz. Více informací o použitých anténách je v [75].

Generování datového toku zajišťoval nástroj FlowPing, zmiňovaný v kapitole 4.

Obrázek 27 Anténní systém na střeše testovacího vozu.

Ten také zajistil i sběr dat pro následné využití v simulačním modelu. Nastavení tohoto generátoru a dalších parametrů pro měření je shrnuto v tabulce 7. Zvolená rychlost odesílání dat a délka paketů byla zvolena tak, aby spojení nebylo zbytečně zahlcováno. Měření probíhalo na území České republiky, rychlost pohybu vozidla nepřekročila 90 km/h.

Tabulka 7 Nastavení parametrů měření

Parametr	T-Mobile	O2
Číslo kanálu	0	1
Technologie	EDGE	EDGE
Generátor provozu	FlowPing	
Transportní protokol	UDP	
Rychlost odesílání dat	21,6 kbit/s	
Velikost paketů	500 B	
Doba měření	3600 s	

Při měření bylo sledováno zda odeslaný paket dorazil bezchybně z klientské části na serverovou a jaké bylo jeho zpoždění. Pro každý paket tak byl vytvořen konkrétní záznam včetně časového údaje v momentě jeho vygenerování. Celková informace pro další vyhodnocení pak byla složena z odpovídajících záznamů z obou částí systému MultiComm.

Tabulka 8 obsahuje souhrn výsledků měření. Hodnoty jsou průměrem za celou dobu měření, kdy například úseky s velmi nízkou propustností ovlivňují celkový výsledek. Vysoká hodnota zpoždění je dána průměrem celého měření, zde pro změnu velmi vysoké hodnoty, dané špatnými momentálními podmínkami spojení,

Tabulka 8 Výsledky měření

Parametr	T-Mobile	O2
Zpoždění	4904 ms	3946 ms
Propustnost	6,2 kbit/s	7,9 kbit/s
PER	0,135	0,119

ovlivňují celý výsledek. Vysoká paketová chybovost obou kanálů může mít mnoho příčin. Zmínit lze například vytížení konkrétní základnové stanice obsluhou jiných klientů, úniky signálu daného pohybem testovacího vozidla, přechodem mezi jednotlivými buňkami sítě či pohybem v oblasti s nízkou úrovní přijímaného signálu.

7.2 Úprava simulačního modelu

Naměřená data poskytují informaci o tom, jak se daný kanál choval v určitém čase. Nejedná se o informaci o fyzických parametrech kanálu, ale o vlastnosti datového kanálu na třetí vrstvě RM OSI. Z daných výsledků nelze rozklíčovat, zda je hodnota zpoždění dána aktuálním vytížením mobilní sítě, zaplněním vyrovnávací paměti zařízení na straně mobilního operátora nebo zařízení MultiComm. Takový rozbor však není předmětem této práce a naopak naměřené výsledky poskytují věrný obraz o chování přenosového řetězce z pohledu koncových stanic, na kterých bude probíhat příjem dat a tedy i případné dekódování podle navrženého schématu.

Simulační model bylo nutné upravit tak, aby v každý okamžik, kdy je paket odesílán na přenosový kanál, byl vyhodnocen aktuální čas a podle něj byly v záznamu z měření dohledány parametry pro přenos. Tedy zjistit zpoždění, s jakým byl paket doručen, a zda vůbec byl korektně doručen. Navržené přenosové schéma je testováno z pohledu chybovosti, nicméně hodnoty zpoždění byly také využity, jelikož mohou ovlivnit funkci obnovy nedoručených dat a tím i hodnotu celkové chybovosti přenosu pro dané přenosové schéma.

7.3 Porovnání a výsledky

Naměřené hodnoty byly využity pro ověření funkce navrženého schématu a pro možnost porovnání také pro schéma zálohování. Analýza je zaměřena na celkovou paketovou chybovost přenosu. Schéma inverzní multiplexace, které z předchozích porovnání vyšlo jako nejméně odolné, nebylo do porovnání zahrnuto. Z principu, jakým je v navrženém schématu dosahovaného navýšení robustnosti přenosu vy-

plývá, že jeho výhoda, oproti běžnému posílání stejných dat na obou kanálech, by se měla projevit u chyb, které zasáhnou oba kanály ve stejný čas. To může být dáno například impulsním rušením, či rychlým únikem signálu. V takový moment zálohovací schéma nemá jak získat ztracená data z obou kanálů, zatímco navržené schéma je dokáže z následující komunikace zpětně rekonstruovat.

7.3.1 Metodika porovnání

Pro zjištění do jaké míry jsou naměřené vzorky chyb paketů v čase vzájemně korelované, byl použit korelační koeficient ρ [76]:

$$\rho = \frac{cov(K_0, K_1)}{\sqrt{(varK_0)(varK_1)}}. \tag{26}$$

Náhodné veličiny K_0 a K_1 jsou v tomto případě vektory výskytu chyb paketů na přenosových kanálech 0 a 1 seřazené podle času. Koeficient ρ může nabývat hodnot v intervalu $\langle -1, 1 \rangle$. Čím je hodnota koeficientu blíže krajním hodnotám, tím těsnější je korelace mezi veličinami.

Je důležité zmínit, že charakter měřených dat má zásadní vliv na výslednou paketovou chybovost. Tento dopad je determinován na rozložení ztracených paketů v toku dat a na délce úseků chybných paketů. Dlouhé úseky chybných paketů, které nastávají na jednom z kanálů, dávají výhodu schématu zálohování, které je dokáže pomocí paketů z druhého kanálu nahradit. Jednotlivé chyby paketů mají podobný dopad na obě porovnávaná schémata v případě, že tyto výpadky neovlivňují druhý přenosový kanál. V případě, že jsou oba kanály zasaženy těmito chybami, je navržené schéma výrazně více odolné díky možnosti rekonstrukce chybných paketů z paketů následujících.

Pro demonstraci vlivu korelace chyb byly provedeny simulace s teoretickými vektory chyb paketů $K_0 = (1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$, $K_1 = (1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$ a $K_2 = (0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$. Hodnota 1 zde označuje korektně doručený paket, hodnota 0 značí chybný paket. Dvojice vektorů, použité pro jednotlivé kanály, byly vybrány do tří simulací tak, aby zachytily situaci vzájemně nekorelovaných, středně silně a úplně korelovaných chyb. Hodnoty korelačního koeficientu pro jednotlivé varianty jsou v tabulce 9. Poměr chybných paketů k celkovému počtu paketů (odpovídá hodnotě PER) pro K_0 je 0,2, pro K_1 0,4 a pro K_2 0,5. Navržené schéma dosáhlo výrazně lepšího výsledku paketové chybovosti pro středně silně a úplně korelované chyby oproti schématu zálohování. To je způsobeno jeho schopností obnovit ztracené pakety i v případě chyby na obou kanálech zároveň. Při nekorelovaných chybách se situace otáčí a projevuje se důsledek velkého množství chybných paketů, které již navržené schéma není schopno obnovit. Zatímco

Tabulka 9 Hodnoty pro porovnání vlivu korelace chyb na přenosová schémata

Vektory pro přenos. kanály	Korelační koeficient	PER navrženého sch.	PER zálohovacího sch.
K_0,K_0	1	0	0,2
K_1,K_0	0,612	0,002	0,2
K_2,K_0	0	0,223	0,109

zálohovací schéma těží z paralelního přenosu stejných dat po obou kanálech.

7.3.2 Výsledky simulací

Pro simulaci nekorelovaných chyb kanálů byly využity hodnoty z měření obou kanálů. Hodnota korelačního koeficientu ρ byla v tomto případě $0,067$. Hodnota tedy ukazuje na nezávislost výskytu chyb. Tabulka 10 ukazuje paketovou chybovost kanálů z měření použitých v simulaci a výslednou paketovou chybovost schématu v simulaci. Výhoda použití dvou kanálů pro dosažené vyšší robustnosti přenosu je zřejmá. Běžné zálohovací schéma dokázalo snížit chybovost z 0,127 (průměr kanálů) na 0,026, nicméně navržené schéma v tomto případě vykazuje výrazně lepší celkovou paketovou chybovost 0,003. To ukazuje na výskyt jednotlivých chyb.

Tabulka 10 Výsledky simulací pro nekorelované chyby kanálů

	PER kanálů		Výsledný PER
Navržené schéma	0,135	0,119	**0,003**
Schéma zálohování	0,135	0,119	**0,026**

Pro případ korelovaných chyb kanálů, byly naměřené hodnoty jednoho z nich (T-Mobile) využity pro nastavení průběhu chyb na obou kanálech zároveň. Hodnoty tedy byly úplně korelované ($\rho = 1$). Z výsledků simulací, ukázaných v tabulce 11, vyplývá zásadní dopad korelace chyb na jednotlivých kanálech na celkovou chybovost přenosu zajištěnou daných schématem. Mírné zhoršení navrženého schématu vyplývá z toho, že v obou kanálech nastávaly chyby na stejných místech. Jelikož pro svou funkci rekonstrukce chybných paketů využívá navržené schéma i pakety z druhého kanálu, nebylo v určitých případech (více chybných paketů v řadě) možné rekonstrukci provést. Na schéma zálohování měly zcela korelované chyby zásadní dopad. Celková paketová chybovost odpovídá chybovosti samotného kanálu, nebylo tedy vůbec využito přínosu paralelního přenosu dat. Schéma totiž spoléhá na obnovu chybného paketu pomocí odpovídajícího paketu

z druhého kanálu, na kterém ale došlo v tomto případě také k chybě.

Tabulka 11 Výsledky simulací pro vzájemně korelované chyby kanálů

	PER kanálů		**Výsledný PER**
Navržené schéma	0,135	0,135	**0,018**
Schéma zálohování	0,135	0,135	**0,135**

7.3.3 Rozbor výsledků v závislosti na míře korelace kanálů

Pro podrobnější rozbor vlivu korelace chyb jednotlivých kanálů byly provedeny simulace s pseudonáhodně generovanými hodnotami náhodných veličin. Tyto hodnoty byly získány pomocí výpočtu v prostředí MATLAB, podle zvolených korelačních koeficientů. Hodnoty byly následně použité pro simulaci rozložení chyb v jednotlivých kanálech. Pro zobrazení výsledků byla zavedena účinnost korekce ω [-], která je definována takto:

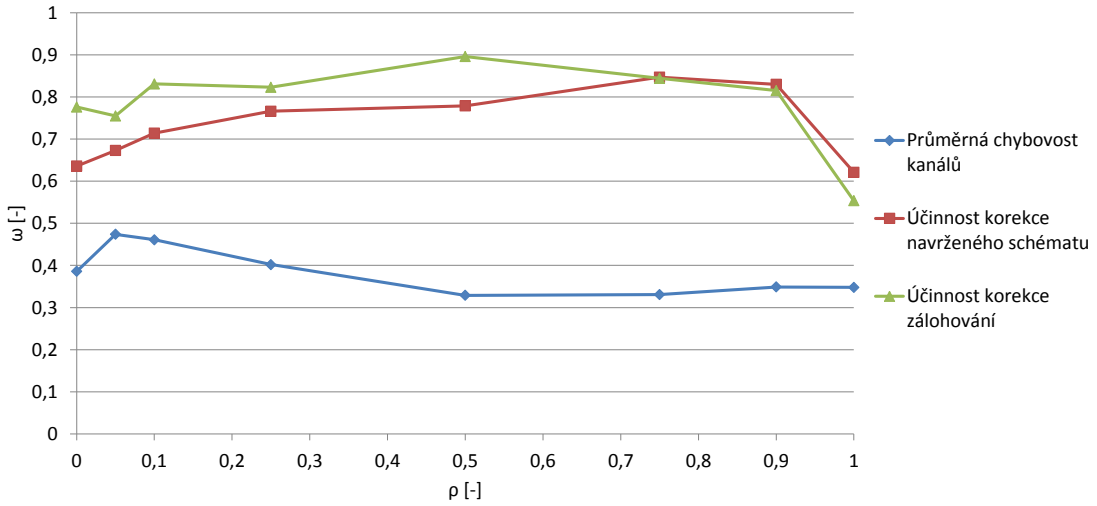
$$\omega = \frac{N_x}{N_o},$$

kde N_x je počet obnovených a korektně doručených paketů a N_o označuje celkový počet odeslaných paketů.

Výsledky ze simulací zálohovacího a navrženého schématu pro jednotlivé hodnoty korelačního koeficientu, jsou zobrazeny na obrázku 28.

Dále jsou v tabulce 12 vyneseny hodnoty paketové chybovosti pro jednotlivé simulace, seřazené podle hodnoty korelačního koeficientu chyb na jednotlivých přenosových kanálech.

Z výsledků vyplývá, že schopnost korekce obou přenosových schémat má závislost na korelaci chyb v jednotlivých kanálech. Oproti předchozím výsledkům, kde se celková chybovost při přenosu dat navrženým schématem pohybovala v nižších hodnotách, se tyto hodnoty nyní pohybují výše a zálohovací schéma vychází v části výsledků lépe. To je dáno vysokou hodnotou chybovosti kanálů, která dekódovacímu mechanismu navrženého schématu neumožňuje provést obnovu chybných paketů a také rozložením jednotlivých chyb paketů. Tento stav se mění u hodnoty korelačního koeficientu 0,75, kde se více projevuje vzájemná korelace chyb, které zvýhodňuje schopnost korekce dat navrženého schématu, oproti zálohovacímu schématu. Hodnota chybovosti pro $\rho = 1$ vykazuje nárust u obou schémat, který způsobilo využití sice úplně korelovaných, ale ne zcela identických hodnot jako u simulace v kapitole 7.3.1 a 7.3.2. Potvrzuje se tak vliv korelace chyb na schopnost korekce jednotlivých schémat přenosu.



Obrázek 28 Porovnání přenosových schémat z pohledu míry korelace přenosových kanálů.

Tabulka 12 Výsledky simulací pro teoretické hodnoty chybovosti kanálů

Korelační koeficient	Průměrná chybovost kanálů	PER navrženého sch.	PER zálohovacího sch.
0	0,386	0,364	0,224
0,05	0,474	0,327	0,245
0,1	0,461	0,286	0,169
0,25	0,402	0,234	0,177
0,5	0,329	0,221	0,104
0,75	0,331	0,153	0,156
0,9	0,349	0,170	0,185
1	0,348	0,399	0,446

8 Závěr

8.1 Závěrečné shrnutí

Předložená práce se zabývá optimalizací přenosu dat v systémech s více přenosovými cestami ve smyslu zajištění robustnosti přenosu. Toho je dosaženo pomocí navrženého schématu přenosu dat po dvou cestách. Toto schéma je navrženo pro použití na třetí vrstvě modelu OSI, kde zajišťuje spojení typu konec-konec a je nezávislé na mezilehlých bodech komunikace, ale může být využito i na druhé vrstvě (spojení se redukuje na typ bod-bod). Přenos dat pomocí něj je transparentní vůči službám, které jsou přes něj provozovány.

Navržené schéma využívá jednu z cest pro posílání lineární kombinace po sobě jdoucích paketů. Dekódovací část schématu obsahuje specifický algoritmus, pomocí kterého je dosažena možnost obnovy dvou chybně doručených či nedoručených paketů v řadě, a to i v případě chyby korespondujícího paketu v druhé přenosové cestě. Přínos práce spočívá ve způsobu obnovy chybných či vůbec nedoručených dat a v zajištění vyšší robustnosti přenosu. Navržené schéma bylo nejen teoreticky popsáno, ale i kompletně implementováno v simulačním nástroji OMNeT++ pomocí jazyka C++. Pro možnosti přímého porovnání byly implementovány i obecně používaná schématu přenosu dat po více cestách. I když existují projekty v oblasti síťového kódování pro zajištění vyšší spolehlivosti dat, nikde dosud nebylo při nejlepším vědomí autora publikováno podobné řešení. Schopnost obnovy chybných či nedoručených paketů a plná transparentnost navrženého schématu pro služby nad ním provozované jsou důležité součásti návrhu.

Součástí práce je i analýza navrženého schématu z pohledu spolehlivosti přenosu a porovnání s běžně používanými schématy přenosu dat po více cestách (inverzní multiplexace, zálohování). Z těchto částí vyplynul jednoznačný přínos navrženého schématu, jako nejrobustnějšího při zachování stejné celkové přenosové rychlosti. Při testování robustnosti přenosu navrženého schématu bylo využito i dat z měření v reálných podmínkách českých mobilních sítí. Byl také zjišťován vliv rozložení výskytu chybných paketů v toku dat na schopnost obnovy chybných paketů. Bylo zjištěno, že navržené schéma je lépe schopno obnovovat chybné pakety, jejichž výskyt na obou přenosových cestách je vzájemně korelovaný, v porovnání se

zálohovacím schématem, které využívá obě cesty pro posílání stejných dat.

Dále bylo navržené schéma analyzováno z pohledu přidaného zpoždění přenosu. Toto zpoždění je způsobeno rekonstrukcí chybných paketů a jeho velikost závisí na množství a rozložení v toku dat. U dalších porovnávaných schémat k podobnému nárustu zpoždění nedochází, velikost celkového zpoždění při jejich použití je tedy vždy nižší, nebo stejná, jako u navrhovaného schématu. V případě, že u schématu zálohování a u inverzní multiplexace je povolena retransmise chybných paketů tak, aby se spolehlivostí přenosu alespoň přiblížily k navrženému schématu, je situace opačná. Zpoždění u nich, vlivem nutnosti opakování přenosu v důsledku chyb, rychle narůstá při zvyšování chybovosti kanálů. Navržené schéma pak vůči nim dosahuje nižších hodnot celkového zpoždění.

8.2 Splnění cílů disertační práce

Zhodnocení cílů práce, které byly formulovány v kapitole 3, je provedeno v následujících bodech:

1. **Navržení obecného systému přenosu umožňujícího variabilní využití více přenosových cest. Návrh a detailní popis funkce konkrétního přenosového schématu schopného zvýšit odolnost přenosu proti chybám při přenosu.**

   Obecný systém byl navržen a je popsán v kapitole 5. Systém je definován tak, aby jej bylo možné pomocí parametrů jeho komponent upravit podle konkrétních požadavků. Jeho hlavními součástmi jsou kodér a dekodér, které jsou dále rozebrány v kapitolách 5.1 a 6.3. Návrh a detailní popis konkrétního přenosového schématu je proveden v kapitole 5.3. Navržené schéma využívá dvou přenosových kanálů, z nichž jeden je využíván pro přenos lineární kombinace paketů. Dekódovací strana zajišťuje detailně popsanou vnitřní logikou obnovu chybně doručených dat.

2. **Vytvoření modelu navrženého přenosového schématu v síťovém simulačním nástroji. Zvolit konkrétní simulační prostředí a provést úplnou implementaci přenosového schématu pro možnost jeho ověření.**

   Model navrženého přenosového schématu byl vytvořen v simulačním nástroji OMNeT++, který je popsán v kapitole 4.1. Implementace samotné funkce kodéru a dekodéru proběhla pomocí jazyka C++ ve spolupráci s navržením modelu pomocí jazyka NED.

3. **Ověření navrženého schématu na simulacích z pohledu schopnosti obnovy chybných dat. Využít naměřená data pro možnost ověření při skutečných provozních podmínkách.**

   Simulace potvrdily přínosnost schématu z pohledu obnovy chybných dat, což popisuje kapitola 6.1. Teoretické předpoklady se potvrdily a schéma je schopné obnovy až dvou nedoručených paketů v řadě, a to bez retransmisí dat. Využití naměřených dat a ověření navrženého schématu na těchto datech popisuje kapitola 7. Přínos se potvrdil i na naměřených datech.

4. **Ověření navrženého schématu na simulacích z pohledu z pohledu celkového zpoždění přenosu. Analyzovat vliv mechanismu obnovy dat na navýšení celkového zpoždění přenosu dat.**

   Kapitola 6.2 ukazuje výsledky simulací z pohledu zpoždění přenosu. Navržené schéma přidává zpoždění pouze v případě, že byla nutná obnova dat. Velikost tohoto zpoždění je dána množstvím chybných dat. Vliv retransmisí je v kapitole 6.2 také diskutován a jejich dopad byl analyzován i pomocí simulací.

5. **Porovnání navrženého schématu s obecně používanými schématy přenosu dat po více přenosových cestách.**

   Porovnání navrženého schématu bylo provedeno vůči schématům inverzního multiplexu a zálohování, které jsou popsány v kapitole 2.3.2. Porovnání bylo provedeno jak z pohledu schopnosti obnovy, tak z pohledu zpoždění přenosu dat.

Jak vyplývá z předloženého souhrnu, všechny vytyčené cíle byly splněny.

8.3 Závěry pro další rozvoj a praxi

Navržené konkrétní schéma přenosu dat počítá s využitím dvou přenosových cest, v následující práci by bylo zajímavé využít více přenosových cest a prověřit další možné varianty obecného schématu popsaného v kapitole 5, například v podobě dvou kanálů využitých pro přenos dat a jednoho pro redundantní data. To by mělo vést k navýšení propustnosti, ale zřejmě za cenu nižší robustnosti přenosu. Dalším námětem je zvážit jinou kombinaci paketů v kodéru, například zvětšit počet vzájemně kombinovaných paketů, s čímž by souvisela i změna dekódovacího algoritmu. Pro praktickou realizaci bude nutné zajišťovat vhodný způsob doplňování paketů tak, aby pro vzájemnou kombinaci byly stejně dlouhé, ale aby nedocházelo ke snížení efektivity přenosu užitečné informace. Navržené přenosové schéma je

plánováno pro využití v zařízení MultiComm, které zajišťuje přenos dat přes více přenosových kanálů. Zde budou vstupující pakety podle potřeby buď sdružovány, nebo naopak segmentovány a doplňovány pro získání segmentů stejné délky, které jsou pro funkci navrženého schématu nutné.

Literatura

Použitá literatura

[1] H.O. Burton a D.D. Sullivan. "Errors and error control". In: *Proceedings of the IEEE* sv. 60, č. 11 (1972), s. 1293–1301. ISSN: 0018-9219.

[2] G. Fairhurst a L. Wood. *Advice to link designers on link Automatic Repeat reQuest (ARQ)*. RFC 3366. Internet Engineering Task Force, 2002. URL: <http://www.ietf.org/rfc/rfc3366.txt>.

[3] J.R. Barry, E.A. Lee a D.G. Messerschmitt. *Digital Communication*. 3rd. Springer, 2004. ISBN: 978-0-7923-7548-7.

[4] D. Gesbert, M. Shafi, Da-shan Shiu, P.J. Smith a A. Naguib. "From theory to practice: an overview of MIMO space-time coded wireless systems". In: *IEEE Journal on Selected Areas in Communications* sv. 21 (2003), s. 281–302. ISSN: 0733-8716.

[5] *Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*. ISO/IEC 7498-1:1994. Geneva, Switzerland: ISO, 1994.

[6] I. Glover a P.M. Grant. *Digital Communications*. Prentice Hall, 2010. ISBN: 9780273718307.

[7] A. Lozano a N. Jindal. "Transmit diversity vs. spatial multiplexing in modern MIMO systems". In: *IEEE Transactions on Wireless Communications* sv. 9, č. 1 (2010), s. 186–197. ISSN: 1536-1276.

[8] G. Song a Y. Li. "Cross-layer Optimization for OFDM Wireless Networks-part I: Theoretical Framework". In: *IEEE Transactions on Wireless Communications* sv. 4, č. 2 (2005), s. 614–624. ISSN: 1536-1276.

[9] S. Shabdanov, P. Mitran a C. Rosenberg. "Cross-Layer Optimization Using Advanced Physical Layer Techniques in Wireless Mesh Networks". In: *IEEE Transactions on Wireless Communications* sv. 11, č. 4 (2012), s. 1622–1631. ISSN: 1536-1276.

[10] B.A. Forouzan. *Data Communications and Networking*. 3. vyd. New York, NY, USA: McGraw-Hill, Inc., 2003. ISBN: 0072923547.

[11] A. Farago, AD. Myers, V.R. Syrotiuk a G.V. Zaruba. "A new approach to MAC protocol optimization". In: *Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE*. Sv. 3. 2000, s. 1742–1746.

[12] E. Fasolo, M. Rossi, J. Widmer a M. Zorzi. "On MAC Scheduling and Packet Combination Strategies for Practical Random Network Coding". In: *ICC '07. IEEE International Conference on Communications*. 2007, s. 3582–3589. ISBN: 1-4244-0353-7.

[13] Q. Shi a C. Comaniciu. "Cross-layer MAC Optimization for Wireless Sensor Networks". In: *Sarnoff Symposium, IEEE* (2008), s. 1–5. ISSN: 978-1-4244-1843-5.

[14] S. Katti, H. Rahul, W. Hu, D. Katabi, Muriel Médard a Jon Crowcroft. "XORs in the Air: Practical Wireless Network Coding". In: *IEEE/ACM Transactions on Networking* sv. 16, č. 3 (2008), s. 497–510. ISSN: 1063-6692.

[15] S. Sengupta, S. Rayanchu a S. Banerjee. "An Analysis of Wireless Network Coding for Unicast Sessions: The Case for Coding-Aware Routing". In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. 2007, s. 1028–1036. ISBN: 0743-166X.

[16] N.F. Maxemchuk. "Dispersity Routing: Past and Present". In: *Military Communications Conference, MILCOM 2007. IEEE*. 2007, s. 1–7. ISBN: 978-1-4244-1513-7.

[17] J. Postel. *User Datagram Protocol*. RFC 768. Internet Engineering Task Force, 1980. URL: <http://www.ietf.org/rfc/rfc768.txt>.

[18] J. Postel. *Transmission Control Protocol*. RFC 793. Internet Engineering Task Force, 1981. URL: <http://www.ietf.org/rfc/rfc793.txt>.

[19] J.G. Proakis. *Digital Communications*. McGraw-Hill series in electrical and computer engineering : communications and signal processing. McGraw-Hill, 2001. ISBN: 9780071181839.

[20] B. Šimák, J. Vodrážka a J. Svoboda. *Digitální účastnické přípojky xDSL: Metody přenosu, popis přípojek HDSL, SHDSL, ADSL, VDSL*. Sdělovací technika, 2005. ISBN: 9788086645070.

[21] J. Dobeš a V. Žalud. *Moderní radiotechnika*. 1. vyd. Praha: BEN - technická literatura, 2006, s. 767. ISBN: 80-7300-132-2.

[22] S. Lin a D.J. Costello. *Error Control Coding*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2004. ISBN: 0130426725.

[23] C. Berrou, A Glavieux a P. Thitimajshima. "Near Shannon limit error-correcting coding and decoding: Turbo-codes". In: *IEEE International Conference on Communication, ICC '93 Geneva.* Sv. 2. 1993, s. 1064–1070. ISBN: 0-7803-0950-2.

[24] E. Dahlman, S. Parkvall, J. Skold a P. Beming. *3G Evolution: HSPA and LTE for Mobile Broadband*. Elsevier Science, 2010. 485 s. ISBN: 9780080549590.

[25] P. Chlumský. "Wireless Networks Optimization based on Network Coding". Dissertation Thesis Proposal. Czech Technical University in Prague, 2012.

[26] R. Ahlswede, Ning C., S.-Y.R. Li a R.W. Yeung. "Network information flow". In: *IEEE Transactions on Information Theory* sv. 46, č. 4 (2000), s. 1204–1216. ISSN: 0018-9448.

[27] R.W. Yeung, S. Li a N. Cai. *Network Coding Theory: Foundations and Trends in Communications and Information Theory*. Hanover, MA, USA: Now Publishers Inc., 2006. ISBN: 1933019247.

[28] T. Ho a D.S. Lu. *Network Coding: An Introduction*. Cambridge: Cambridge University Press, 2008. ISBN: ISBN: 978-0-511-39826-1.

[29] Ch. Fragouli, J. Le Boudec a J. Widmer. "Network Coding: An Instant Primer". In: *SIGCOMM Computer Communications* sv. 36, č. 1 (2006), s. 63–68. ISSN: 0146-4833.

[30] P. Pakzad, C. Fragouli a A. Shokrollahi. "Coding schemes for line networks". In: *International Symposium on Information Theory, ISIT 2005*. 2005, s. 1853–1857.

[31] H. Yang, W. Meng, B. Li a G. Wang. "Physical layer implementation of network coding in two-way relay networks". In: *IEEE International Conference on Communications (ICC)*. 2012, s. 671–675.

[32] B. Nazer a M. Gastpar. "Reliable Physical Layer Network Coding". In: *Proceedings of the IEEE* sv. 99 (2011), s. 438–460. ISSN: 0018-9219.

[33] S. Chachulski, M. Jennings, S. Katti a D. Katabi. "Trading Structure for Randomness in Wireless Opportunistic Routing". In: *SIGCOMM Computer Communications* sv. 37, č. 4 (2007), s. 169–180. ISSN: 0146-4833.

[34] J.K. Sundararajan, D. Shah, M. Medard, S. Jakubczak, M. Mitzenmacher a J. Barros. "Network Coding Meets TCP: Theory and Implementation". In: *Proceedings of the IEEE* sv. 99, č. 3 (2011), s. 490–512. ISSN: 0018-9219.

[35] A.G. Dimakis, P.B. Godfrey, Y. Wu, M.J. Wainwright a K. Ramchandran. "Network Coding for Distributed Storage Systems". In: *IEEE Transactions on Information Theory* sv. 56, č. 9 (2010), s. 4539–4551. ISSN: 0018-9448.

[36] C. Gkantsidis, J. Miller a P. Rodriguez. "Anatomy of a P2P Content Distribution system with Network Coding". In: *IPTPS'06* (2006).

[37] Y. Min a Y. Yuanyuan. "Applying Network Coding to Peer-to-Peer File Sharing". In: *IEEE Transactions on Computers* sv. 63, č. 8 (2014), s. 1938–1950. ISSN: 0018-9340.

[38] M. Kim, J.K. Sundararajan, M. Medard, A. Eryilmaz a R. Kotter. "Network Coding in a Multicast Switch". In: *IEEE Transactaions on Information Theory* sv. 57, č. 1 (2011), s. 436–460. ISSN: 0018-9448.

[39] K. Han, Tracey H., R. Koetter, M. Medard a Fang Z. "On network coding for security". In: *IEEE Military Communications Conference, MILCOM 2007.* 2007, s. 1–6. ISBN: 978-1-4244-1513-7.

[40] R. Dougherty, C. Freiling a K. Zeger. "Networks, Matroids, and Non-Shannon Information Inequalities". In: *IEEE Transactions on Information Theory* sv. 53, č. 6 (2007), s. 1949–1969. ISSN: 0018-9448.

[41] P. Sattari, Ch.Fragouli a A. Markopoulou. "Active topology inference using network coding". In: *Physical Communication* sv. 6 (2013), s. 142–163. ISSN: 1874-4907.

[42] B.K. Rai a B.K. Dey. "On Network Coding for Sum-Networks". In: *IEEE Transactions on Information Theory* sv. 58, č. 1 (2012), s. 50–63. ISSN: 0018-9448.

[43] J. Duncanson. "Inverse multiplexing". In: *IEEE Communications Magazine* sv. 32, č. 4 (1994), s. 34–41. ISSN: 0163-6804.

[44] P.A. Shah, M. Yousaf, A. Qayyum a H.B. Hasbullah. "Effectiveness of multihoming and parallel transmission during and after the vertical handover". In: *International Conference on Computer Information Science (ICCIS).* Sv. 2. 2012, s. 625–629. ISBN: 978-1-4673-1937-9.

[45] J.G. Apostolopoulos a M.D. Trott. "Path Diversity for Enhanced Media Streaming". In: *IEEE Communications Magazine* sv. 42, č. 8 (2004), s. 80–87. ISSN: 0163-6804.

[46] P. Pechač a S. Zvánovec. *Základy šíření vln pro plánování pozemních rádiových spojů.* BEN - technická literatura, 2007. ISBN: 9788073002237.

[47] *The Network Simulator NS-2*. [online] 2014 [cit. 2014-07-10]. Dostupné z: http://www.isi.edu/nsnam/ns/.

[48] *NS-3 Simulator*. [online] 2014 [cit. 2014-07-10]. Dostupné z: http://www.nsnam.org.

[49] *SteelCentral for Performance Management and Control*. [online] 2014 [cit. 2014-05-20]. Dostupné z: http://www.riverbed.com/products/performance-management-control/opnet.html.

[50] *OMNeT++ Network Simulation Framework*. [online] 2014 [cit. 2014-05-20]. Dostupné z: http://www.nsnam.org.

[51] *NetSim - Network Simulator*. [online] 2014 [cit. 2014-07-10]. Dostupné z: http://www.tetcos.com/netsim_gen.html.

[52] *J-Sim Official*. [online] 2014 [cit. 2014-07-10]. Dostupné z: http://sites.google.com/site/jsimofficial/.

[53] *The cnet network simulator*. [online] 2014 [cit. 2014-07-10]. Dostupné z: http://www.csse.uwa.edu.au/cnet/.

[54] A.M. Law a M.G. McComas. "Simulation software for communications networks: the state of the art". In: *IEEE Communications Magazine* sv. 32, č. 3 (1994), s. 44–50. ISSN: 0163-6804.

[55] P. Chlumský, Z. Kocur a J. Vodrážka. "The Use of Simulation Framework OMNeT++ in Telecommunications". In: *Knowledge in Telecommunication Technologies and Optics - KTTO 2010*. Ostrava: VŠB - TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2010, s. 87–91. ISBN: 978-80-248-2330-0.

[56] A. Varga a R. Hornig. "An Overview of the OMNeT++ Simulation Environment". In: *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*. Simutools '08. Marseille, France: ICST, 2008, s. 1–10. ISBN: 978-963-9799-20-2.

[57] M. Matsumoto a T. Nishimura. "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator". In: *ACM Transactions on Modeling and Computer Simulation* sv. 8, č. 1 (1998), s. 3–30. ISSN: 1049-3301.

[58] *Software developement and testing - Certicon*. [online] 2014 [cit. 2014-08-12]. Dostupné z: http://www.certicon.cz/.

[59] Z. Kocur, P. Macejko, P. Chlumský, J. Vodrážka a O. Vondrouš. "Adaptable System Increasing the Transmission Speed and Reliability in Packet Network by Optimizing Delay". In: *Advances in Electrical and Electronic Engineering* sv. 12, č. 1 (2014), s. 13–19. ISSN: 1804-3119.

[60] O. Vondrouš, Z. Kocur, P. Macejko a P. Jareš. *FlowPing - UDP based ping application*. [online] 2014 [cit. 2014-08-12]. Dostupné z: http://flowping.comtel.cz/.

[61] *Mathworks MATLAB*. [online] 2014 [cit. 2014-07-10]. Dostupné z: http://www.mathworks.com/products/matlab/.

[62] J. Postel. *Internet Protocol*. RFC 791. Updated by RFCs 1349, 2474, 6864. Internet Engineering Task Force, 1981. URL: <http://www.ietf.org/rfc/rfc791.txt>.

[63] *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 2007.

[64] S.B. Moon. "Measurement and Analysis of End-to-end Delay and Loss in the Internet". Dis. 2000. ISBN: 0-599-64586-5.

[65] R. Horak. *Telecommunications and Data Communications Handbook*. Wiley, 2007. ISBN: 9780470127223.

[66] J. Balej a D. Komosný. "Zdroje zpoždění při komunikaci v Internetu". In: *Elektrorevue* sv. 12, č. 3 (2010). ISSN: 1213-1539.

[67] P. Bezpalec. "Analýza zpoždění v IP telefonním systému I". In: *Access server* sv. 6. (2008), s. 1–6. ISSN: 1214-9675.

[68] A. Leon-Garcia a I. Widjaja. *Communication Networks: Fundamental Concepts and Key Architectures*. Second. McGraw Hill Higher Education, Boston, 2004, s. 900. ISBN: 0-07-119848-2.

[69] *Network performance objectives for IP-based services. Recommendation ITU-T Y.1541*. Tech. zpr. ITU-T, 2011, s. 66.

[70] B. Goode. "Voice over Internet protocol (VoIP)". In: *Proceedings of the IEEE* sv. 90, č. 9 (2002), s. 1495–1517. ISSN: 0018-9219.

[71] J. Vodrážka a P. Lafata. "Transmission Delay Modeling of Packet Communication over Digital Subscriber Line". In: *Advances in Electrical and Electronic Engineering* sv. 11, č. 4 (2013), s. 260–265. ISSN: 1336-1376.

[73] M. Mathis, J. Mahdavi, S. Floyd a A. Romanow. *TCP Selective Acknowledgment Options*. RFC 2018 (Proposed Standard). Internet Engineering Task Force, 1996. URL: <http://www.ietf.org/rfc/rfc2018.txt>.

[74] *Mapa pokrytí O2*. [online] 2014 [cit. 2014-05-20]. Dostupné z: http://www.o2.cz/osobni/199436-mapa_pokryti_a_prodejen/.

[76] J. Anděl. *Základy matematické statistiky*. 3. vyd. Matfyzpress, Praha, 2011. 358 s. ISBN: 978-80-7378-162-0.

Publikace autora týkající se náplně a tématu disertační práce

[A 1] P. Chlumský, Z. Kocur a V. Machula. "Simulation of the Data Transmission from the Aerobatic Plane". In: *Przeglad Elektrotechniczny* sv. 89, č. 2b/2013 (2013), s. 199–204. ISSN: 0033-2097 – podíl autora 33 %

[A 2] M. Rohlík, P. Chlumský a T. Vaněk. "Increasing Robustness of Multi-homed Systems in Heterogeneous Environment". In: *Advances in Electrical and Electronic Engineering* sv. 12, č. 4 (2014). ISSN: 1336-1376 – podíl autora 33 %

[A 3] P. Chlumský, Z. Kocur, J. Vodrážka a T. Kořínek. "Reduction of Packet Loss by Optimizing the Antenna System and Layer 3 Coding". In: *Advances in Electrical and Electronic Engineering* sv. 12, č. 4 (2014). ISSN: 1336-1376 – podíl autora 25 %

[A 4] Z. Kocur, P. Macejko, P. Chlumský, J. Vodrážka a O. Vondrouš. "Adaptable System Increasing the Transmission Speed and Reliability in Packet Network by Optimizing Delay". In: *Advances in Electrical and Electronic Engineering* sv. 12, č. 1 (2014), s. 13–19. ISSN: 1804-3119 – podíl autora 20 %

[A 5] P. Chlumský, Z. Kocur a J. Vodrážka. "Comparison Methodology of the Simulation Models Based on the IEEE 802.11 Standard". In: *Elektrorevue* sv. 3, č. 1 (2012), s. 32–38. ISSN: 1213-1539 – podíl autora 33 %

[A 6] P. Chlumský, Z. Kocur a J. Vodrážka. "Comparison of Different Scenarios for Path Diversity Packet Wireless Networks". In: *Advances in Electrical and Electronic Engineering* sv. 10, č. 4 (2012), s. 199–203. ISSN: 1336-1376 – podíl autora 33 %

[A 7] P. Chlumský a J. Vodrážka. "Delay Analysis of Data Transmission System with Channel Coding". In: *Proceedings of 10th Internetional Conference ELEKTRO*

2014. Žilinská univerzita, Fakulta elektrotechnická, 2014, s. 31–35. ISBN: 978-1-4799-3720-2 – podíl autora 50 %

[A 8] Z. Kocur, P. Chlumský, P. Macejko, M. Kozák, L. Vojtěch a M. Neruda. "Measurement of Mobile Communication Devices on the Testing Railway Ring". In: *15th International Conference on Research in Telecommunication Technologies*. Bratislava: Slovak University of Technology in Bratislava, 2013, s. 34–37. ISBN: 978-80-227-4026-5 – podíl autora 16 %

[A 9] P. Chlumský, Z. Kocur a V. Machula. "Simulation of Data Transfer from the Aerobatic Plane". In: *Proceedings of the 11th International Conference Knowledge in Telecommunication Technologies and Optics*. Ostrava: VŠB - TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2011, s. 113–116. ISBN: 978-80-248-2399-7 – podíl autora 33 %

[A 10] P. Chlumský, Z. Kocur a J. Vodrážka. "Comparison Methodology of the Simulation Models in Wireless Networks". In: *13th International Conference on Research in Telecommunication Technologies 2011*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011, s. 10–14. ISBN: 978-80-214-4283-2 – podíl autora 33 %

[A 11] P. Chlumský, Z. Kocur a J. Vodrážka. "The Use of Simulation Framework OMNeT++ in Telecommunications". In: *Knowledge in Telecommunication Technologies and Optics - KTTO 2010*. Ostrava: VŠB - TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2010, s. 87–91. ISBN: 978-80-248-2330-0 – podíl autora 33 %

[A 12] Z. Kocur, P. Chlumský a M. Kozák. *Vícekanálový paketový procesor*. Funkční vzorek. 2012 – podíl autora 33 %

Ostatní publikace

[B 1] T. Hégr, L. Boháč, Z. Kocur, M. Vozňák a P. Chlumský. "Methodology of the Direct Measurement of the Switching Latency". In: *Przeglad Elektrotechniczny* sv. 89, č. 7 (2013), s. 59–63. ISSN: 0033-2097 – podíl autora 20 %

[B 2] T. Hégr, L. Boháč, V. Uhlíř a P. Chlumský. "OpenFlow Deployment and Concept Analysis". In: *Advances in Electrical and Electronic Engineering* sv. 11, č. 5 (2013), s. 327–335. ISSN: 1804-3119 – podíl autora 25 %

[B 3] V. Machula, Z. Kocur a P. Chlumský. “Filtering Methods of the Inertial Position Measuring System”. In: *Proceedings of the 2011 International Conference on Telecommunication Systems Management*. Dallas, TX: American Telecommunications Systems Management Association Inc., 2011, s. 35–38. ISBN: 978-0-9820958-4-3 – podíl autora 33 %