# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

**FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ**

**ÚSTAV TELEKOMUNIKACÍ**

**Ing. Vladimír Schindler**


# PROBLEMATIKA OPTIMÁLNÍ ŠÍŘKY PŘENOSOVÉHO PÁSMA PRO PŘENOS MEDICÍNSKÝCH OBRAZOVÝCH DAT

CHALLENGES IN OPTIMAL BANDWIDTH FOR MEDICAL IMAGE TRANSFER

*ZKRÁCENÁ VERZE PH.D. THESIS*

Obor: Teleinformatika

Školitel: doc. Ing. Otto Dostál, CSc.

Oponenti:

Datum obhajoby: x. 3. 2014

**KLÍČOVÁ SLOVA**
MeDiMed, DICOM, PACS, PKI, IPSec, modalita, medicínské obrazové informace

**KEYWORDS**
MeDiMed, DICOM, PACS, PKI, IPSec, medical images, telemedicine




ISBN 80-214-
ISSN 213-4198

# OBSAH

OBSAH ..... 3
ÚVOD ..... 5
1 CÍLE DISERTACE ..... 7
2 STANOVENÍ OPTIMÁLNÍ ŠÍŘKY PŘENOSOVÉHO PÁSMA ..... 8
2.1 Analýza provozu sítě ..... 8
2.2 Analýza datového provozu modalit ve vybraných nemocnicích ..... 10
2.2.1 Analýza provozu mimobrněnské nemocnice ..... 10
2.2.2 Analýza provozu městské nemocnice ..... 11
3 ZABEZPEČENÍ PŘENOSU DAT PRACOVNÍCH STANIC ..... 13
3.1 Využití jednodeskových počítačů pro zabezpečení přenosu medicínských dat ..... 14
3.1.1 Realizace počítače ..... 14
3.1.2 Diskuze výsledku vyvinutého zařízení ..... 15
3.2 Simulace vlivů nastavení TCP paketu a šifrování na rychlost přenosu dat ..... 16
3.2.1 MSS ..... 16
3.2.2 Měřící sestava a schéma zapojení ..... 17
3.2.3 Aplikace použité při měření přenosu ..... 17
3.2.4 Porovnání rychlosti přenosu souboru při různých kombinacích šifer a hešovacích funkcí ..... 18
3.2.5 Porovnání rychlosti přenosu souboru při různé velikosti window size ..... 19
3.2.6 Porovnání rychlosti přenosu souboru při různé velikosti bufferu ..... 19
3.2.7 Vliv velikosti MSS na rychlost přenosu ..... 20
4 ZÁVĚR ..... 22
5 LITERATURA ..... 23

# ÚVOD

V lednu 2002 byl zahájen rutinní provoz brněnského metropolitního centra pro podporu zpracování medicínských obrazových informací. Naprosto klíčovou podmínkou realizace tohoto systému byla existence spolehlivé vysokorychlostní počítačové sítě propojující lokality všech spolupracujících zdravotnických zařízení. Zdravotnickým zařízením je dnes zpřístupněno prostředí usnadňující vzájemnou spolupráci a nabízena řada služeb v oblasti zpracování medicínských obrazových informací. Metropolitní centrum se tak stále více stává komplexním integrovaným systémem, který nabízí nejenom prostředky pro spolehlivou dlouhodobou archivaci obrazové informace, ale i podporu přenosů obrazových informací mezi jednotlivými pracovišti (nemocnicemi), která pacient v průběhu léčby navštíví. Rovněž se v posledních letech do tohoto systému zapojuje stále více lékařských specialistů, a proto využití tohoto řešení ve svém důsledku jednoznačně vede k usnadnění a urychlení formulace správné diagnózy, vyloučení opakovaných vyšetření, úspoře času pacienta i lékaře a tím i k úspoře finančních prostředků. [1]

U menších zdravotnických zařízení, která nejsou připojena vyhrazenými optickými spoji a zejména u privátních ordinací, je také důležité sledovat šířku přenosového pásma z důvodu požadavku na okamžitý přístup k obrazovým studiím v jednotkách sekund. Tato podmínka je však přímo v opozici s nutností míry zabezpečení přenášených dat. Správně dimenzované spojení mezi zdravotnickým zařízením a centrálním úložištěm je základem pro komfortní práci s obrazovými daty. Zároveň optimalizace připojení přináší nemalé finanční úspory spojené s náklady za pořízení či pronájem datových okruhů.

Zabezpečení přenosu medicínských dat je nutné řešit jak u stávajících velkých nemocnic, které využívaly systému mezi prvními a byly připojeny pomocí vyhrazených optických vláken, tak i u malých zdravotnických zařízení, privátních ordinací a klinik. Aby bylo možné připojit do výše uvedeného systému co nejširší spektrum uživatelů, je nutné podporovat různé typy datového připojení a zároveň se soustředit na maximální možnou míru zabezpečení přenosu citlivých medicínských dat. Ochrana před neoprávněnou manipulací s pracovní stanicí je mnohem vyšší nežli u medicínských modalit, neboť ty jsou většinou umístěny na pracovištích pod dohledem oprávněného personálu a jsou připojeny k izolovaným a zabezpečeným datovým sítím. Také pracovní stanice připojené do sítě v nemocničních zařízeních jsou chráněny před napadením škodlivým softwarem. Problémy mohou nastat u specialistů, jenž se připojují k databázím s medicínskými daty běžnými stolními počítači nebo notebooky. Z těchto důvodů je nutné stále zvyšovat zabezpečení přístupu do sítí s takto citlivými informacemi o pacientech. Úspěšná autentizace a autorizace oprávněné osoby je tedy podmínkou pro práci v tomto systému.

Systém se neustále rozvíjí a zdokonaluje, dokáže tak reflektovat nejnovější požadavky zdravotnických zařízení, uživatelů a používaných technologií. Využití nových metod zabezpečení přenosu dat, archivace pořízených studií a komunikace s uživateli drží krok s vývojem moderních technologií. Rozvoj systému je financován převážně z projektů a fondů českých a evropských dotačních agentur.

# 1 CÍLE DISERTACE

Hlavním cílem disertační práce s názvem „Problematika optimální šířky přenosového pásma pro přenos medicínských obrazových dat“ je analýza přenosového pásma určeného pro transport medicínských obrazových dat mezi zdravotnickými zařízeními a vzdálenými datovými úložišti. Jako reálná a plně funkční struktura, která bude v této práci analyzována, byl zvolen systém MeDiMed. Díky novým technologiím je třeba neustále sledovat možnosti zvyšování kapacity systému, neboť požadavky na zpracování medicínských dat a dostatečný prostor k jejich ukládání a archivaci se budou stále zvyšovat.

Důležitým kritériem při provozování a rozšiřování zdravotnických zařízení je optimalizace parametrů přenosové trasy pro transfer medicínských obrazových dat. Touto problematikou se bude zabývat první část disertační práce.

Druhá část disertační práce bude zaměřena na bezpečnostní požadavky pro přenos dat mezi pracovními stanicemi a vzdálenými datovými úložišti. Nejprve bude představeno řešení zabezpečení přístupu pracovních stanic k datovým úložištím, poté budou prezentovány vlivy šifrování přenášených dat na dobu přenosu.

# 2 STANOVENÍ OPTIMÁLNÍ ŠÍŘKY PŘENOSOVÉHO PÁSMA

## 2.1 ANALÝZA PROVOZU SÍTĚ

Před stanovováním optimální šířky pásma je nutné se nejprve seznámit s jednotlivými modalitami, které jsou používány ve zdravotnických zařízeních. Vzhledem k počtu různých druhů vyšetření, které může pacient absolvovat a širokému portfoliu lékařských přístrojů, není smyslem této práce se zabývat do hloubky jednotlivými přístroji a možnostmi jejich použití.

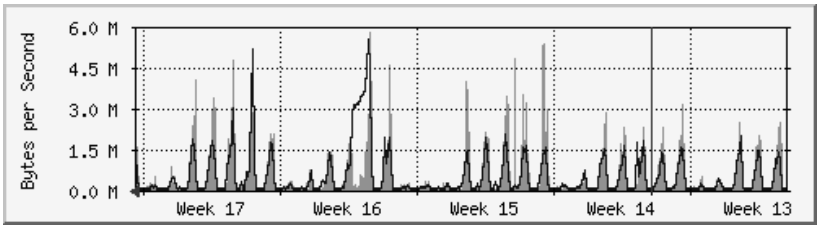
Některé metody vyšetření lidského těla produkují jednotky až desítky snímků, jiné mohou poskytnout až tisíce snímků během jednoho vyšetření. Vše záleží jak na složitosti a detailnosti prohlídky pacienta, tak i na použitém přístroji a jeho nastavení. V tab. 2.1 jsou proto uvedeny reálné změřené hodnoty některých metod vyšetření.

Tab. 2.1: Reálné hodnoty velikostí souborů vybraných metod vyšetření

| Metoda vyšetření | DICOM zkratka | Oblast vyšetření | Počet snímků | Velikost souboru |
|---|---|---|---|---|
| Počítačová tomografie | CT | hlava | 21 | 13,3 MB |
| Počítačová tomografie | CT | pánev | 91 | 48,6 MB |
| Mamografie | MG | prsa | 4 | 25,3 MB |
| Mamografie | MG | prsa | 2 | 17,6 MB |
| Digitální rentgen | DX | plíce | 1 | 8,4 MB |
| Digitální rentgen | DX | hrudník | 1 | 40,9 MB |
| Pozitronová emisní tomografie | PT | celé tělo | 1135 | 472,5 MB |
| Počítačová radiografie | CR | ruka | 1 | 8,6 MB |
| Angioskopie | AS | – | 19 | 20 MB |
| Endoskopie - polypektomie | ES | – | 5 | 6,7 MB |

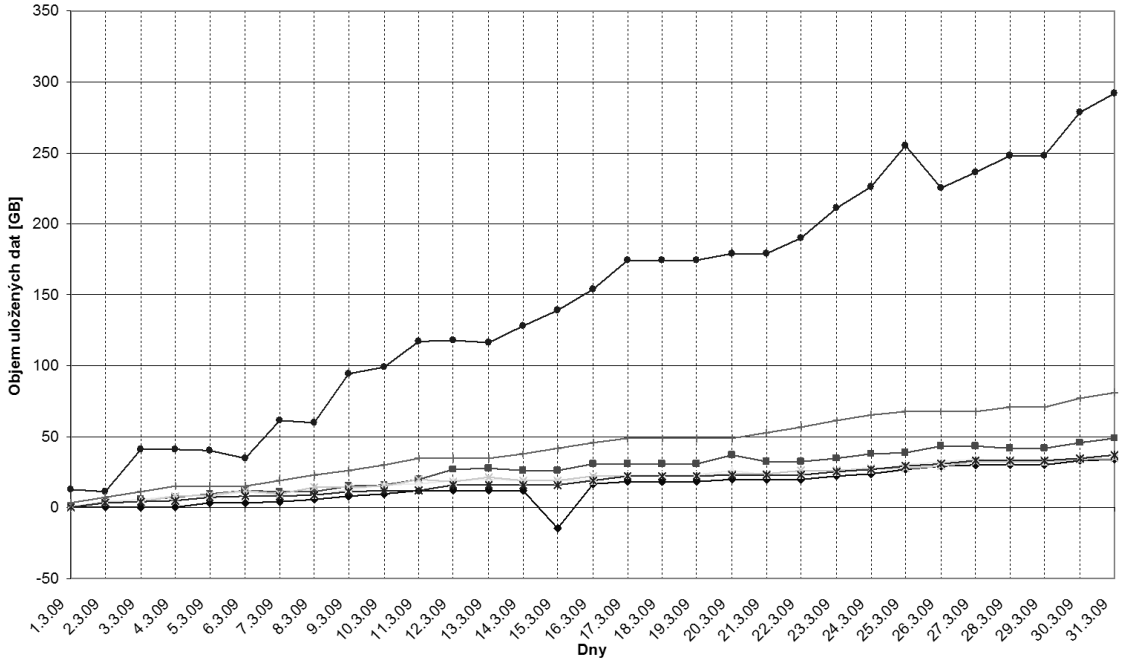
Z výše uvedených hodnot je zřejmé, že jsou velké rozdíly jednak ve velikostech souborů z jednotlivých modalit, tak i mezi soubory pocházejícími z téže modality.

O provozu mezi všemi zdravotnickými zařízeními a centrálním úložištěm také vypovídá měsíční graf provozu na obr. 2.1, kde jsou zachyceny přenosové rychlosti s dvouhodinovým průměrováním. Je z něj patrné, že přenosová rychlost se v pracovní dny pohybuje kolem 16 Mb/s, ve špičkách může dosáhnout až 43Mb/s. Výjimkou ovšem nejsou ani rychlosti blížící se 120 Mb/s.




Obr. 2.1: Měsíční graf celkového provozu přenosové sítě

Graf na obr. 2.2 znázorňuje denní přírůstky ukládaných dat z vybraných nemocnic na centrálním úložišti za měsíc březen 2009. Názvy zdravotnických zařízení zde nejsou úmyslně uvedeny, neboť se jedná o důvěrné informace. I tak je z grafu patrné, že průměrný denní přírůstek na datovém úložišti, který vyprodukuje jedna nemocnice je více než 1,2 GB dat a to včetně sobot a nedělí. Nelze si nevšimnout, že jedna z nemocnic dokázala během měsíce března uložit takřka 300 GB medicínských dat. Především díky ní tak diskové úložiště ukládá a archivuje měsíčně v průměru více než 900 GB dat.




Obr. 2.2: Měsíční nárůst objemu uložených dat v datových úložištích

## 2.2 ANALÝZA DATOVÉHO PROVOZU MODALIT VE VYBRANÝCH NEMOCNICÍCH

Pro získání profilu datového provozu byly vytipovány lokality a modality, na kterých bylo provedeno měření a sledování datového provozu v období od 26. 9. 2013 do 21. 10. 2013. Vzhledem k velkému množství získaných informací byla data rozdělena do skupin dle časového úseku, ve kterém byla přenášena. Časové úseky představují hodinové intervaly, které odpovídají času přenášených dat z dané lokality a modality. V těchto hodinových intervalech jsou také zpracovány grafy. Na základě získaných informací je dále možné určit základní statistické údaje.

### 2.2.1 Analýza provozu mimobrněnské nemocnice

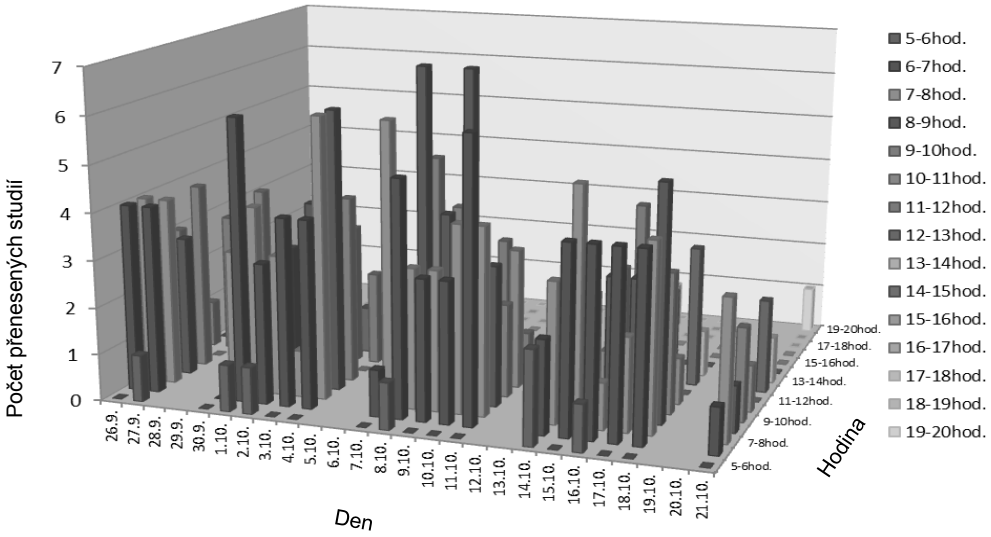
Mimobrněnská nemocnice se do systému MeDiMed připojila v roce 2005. Připojení je realizováno bezdrátovým radioreléovým spojem.

Pro analýzu provozu byla vybrána modalita ultrazvuk. Základní statistické údaje jsou uvedené v tab. 2.2. Graf na obr. 2.3 zobrazuje počet datových spojení v dané hodině a na obr. 2.4 je zobrazen objem dat přenesený mezi ultrazvukem a datovým centrem.

Tab. 2.2: Statistické údaje pro ultrazvuk v mimobrněnské nemocnici

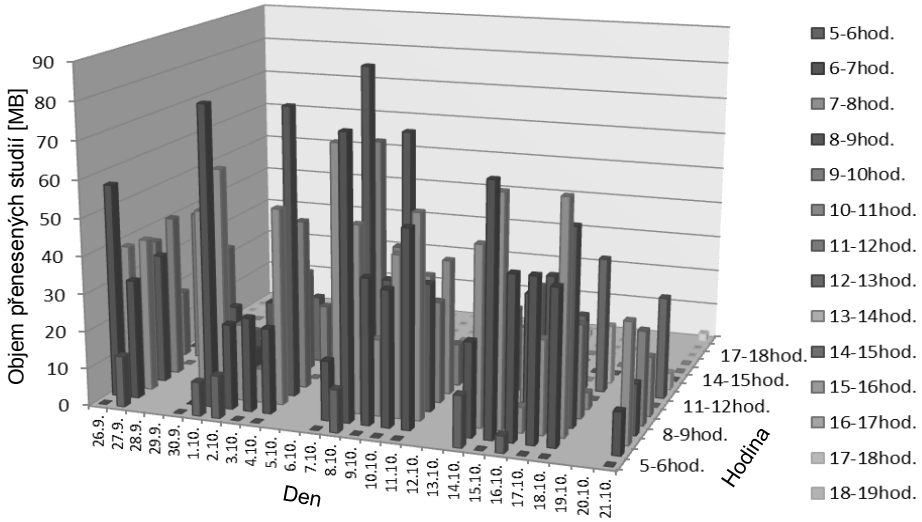
| | |
|---|---|
| Celkový počet přenesených studií | 296 |
| Maximální počet přenesených studií v hodině | 7 (8. 10. a 10. 10. mezi 8-9hod.) |
| Celkový objem přenesených studií | 3 228,4 MB |
| Maximální objem přenesených dat v hodině | 88,7 MB (8. 10. mezi 8-9hod.) |
| Maximální velikost studie | 27,3 MB |
| Minimální velikost studie | 2,3 MB |
| Průměrná velikost studie | 10,9 MB |
| Medián velikosti studie | 11,4 MB |

Z tabulky dále plyne, že za sledovaný časový úsek bylo průměrně přeneseno 16 studií za pracovní den. Objem přenesených studií za jeden pracovní den lze odhadnout na přibližně 180MB.




Obr. 2.3: Počet přenesených studií v hodinových intervalech v mimobrněnské nemocnici

Z výše uvedeného grafu je patrné, že v tomto zdravotnickém zařízení je ultrazvuk využíván pouze v pracovních dnech a to zejména dopoledne. Počet provedených vyšetření v dopoledních hodinách se většinou pohybuje mezi třemi až pěti za hodinu.




Obr. 2.4: Objem přenesených studií v hodinových intervalech v mimobrněnské nemocnici

### 2.2.2 Analýza provozu městské nemocnice

Městská nemocnice se do systému MeDiMed připojila již v roce 2002. Připojení je realizováno vyhrazeným optickým spojem.

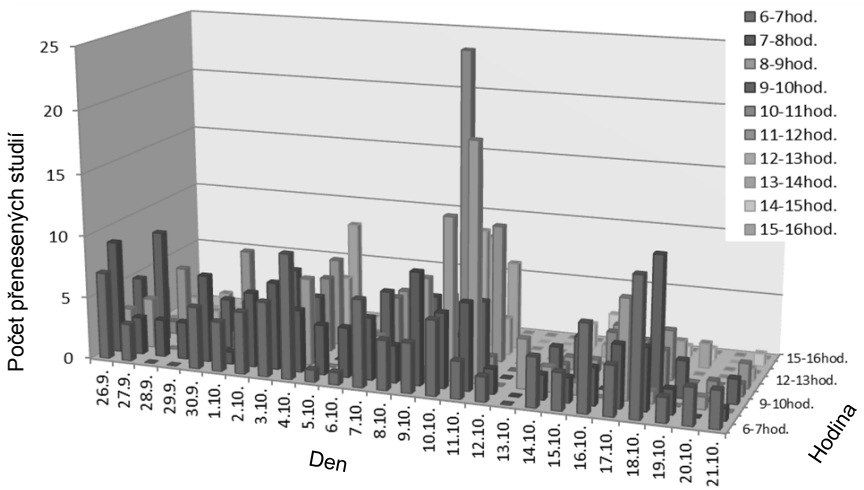
Pro analýzu provozu byl stejně jako u mimobrněnské nemocnice vybrán ultrazvuk. Graf na obr. 2.5 zobrazuje počet datových spojení v dané hodině a na obr. 2.6 je zobrazen objem dat přenesený mezi ultrazvukem a datovým centrem. Základní statistické údaje jsou uvedené v tab. 2.3.

Tab. 2.3: Statistické údaje pro ultrazvuk v městské nemocnici

| | |
|---|---|
| Celkový počet přenesených studií | 607 |
| Maximální počet přenesených studií v hodině | 25 (10. 10. mezi 10-11hod.) |
| Celkový objem přenesených studií | 53 290,4 MB |
| Maximální objem přenesených dat v hodině | 3 602,9 MB (10. 10. mezi 10-11hod.) |
| Maximální velikost studie | 1 519,3 MB |
| Minimální velikost studie | 2,3 MB |
| Průměrná velikost studie | 87,6 MB |
| Medián velikosti studie | 51,8 MB |

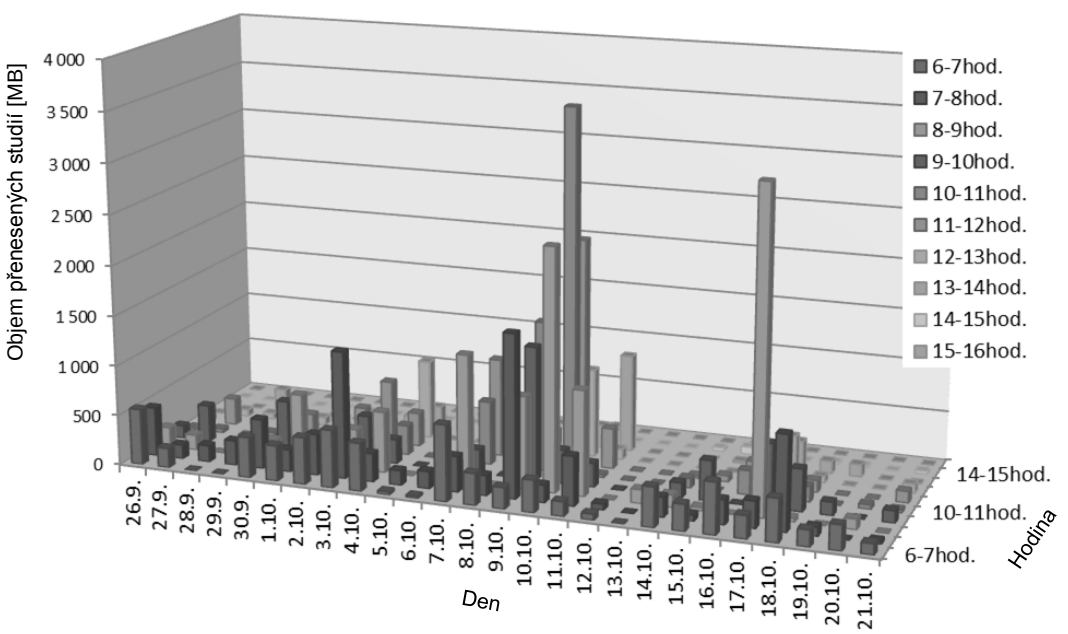
Z tabulky dále plyne, že za sledovaný časový úsek bylo průměrně přeneseno více než 23 studií za den, včetně víkendů. Objem přenesených studií za jeden den lze odhadnout na přibližně 2050 MB. Oproti mimobrněnské nemocnici je zřetelné, že ultrazvuk v městské nemocnici je mnohem vytíženější a produkuje mnohem více dat, která se ukládají do centrálního úložiště.

Na srovnání modalit těchto dvou nemocnic je názorně vidět, že i jednodušší přístroje jako jsou ultrazvuky, dokážou generovat odlišné datové toky. Tento fakt je nutné brát v úvahu při návrhu infrastruktury sítě.




Obr. 2.5: Počet přenesených studií v hodinových intervalech v městské nemocnici

Z grafu je patrné, že ultrazvuk je využíván každý den včetně sobot a nedělí. Na rozdíl od mimobrněnské nemocnice je ovšem doba jeho provozu během dne mnohem kratší.




Obr. 2.6: Objem přenesených studií v hodinových intervalech v městské nemocnici

V grafu jsou zřetelné dvě hodnoty, kde objem přenesených dat převyšuje 3GB za sledovanou hodinu. Pokud není optimalizována přenosová trasa, tak se tyto extrémy mohou velmi negativně projevit na dostupnosti služeb v daném časovém úseku.

# 3 ZABEZPEČENÍ PŘENOSU DAT PRACOVNÍCH STANIC

Zařízení rozličných výrobců v současnosti připojená k metropolitnímu PACS serveru (prohlížecí stanice, specializované stanice pro primární diagnostiku, archivační zařízení, terapeutická zařízení atd.) tvoří velmi heterogenní prostředí. Pro rozlišení pracovišť jednotlivých nemocnic je v současnosti rozhodující IP adresa pracovních stanic daného pracoviště resp. její transformace do unikátního adresného prostoru privátní sítě metropolitního PACSu. Toto řešení je dostačující pro zdroje obrazových dat případně pro prohlížecí stanice, které jsou využívány jediným uživatelem. Alternativa autentizovaného přístupu je zcela logickým požadavkem lékařů (služby v jiných nemocnicích, mobilní pracoviště, domácí pracovny lékařů atd.).

Původní uživatelé, kteří sdíleli pracoviště, používali pro komunikaci s PACS serverem IPSec tunel, kde jim byla na základě autentizace pomocí PKI (Private Key Infrastructure) přidělena „jejich“ privátní unikátní IP adresa IPSec tunelu.

Pro přenos a uchovávání PKI klíčů se používal USB klíč eToken PRO vyvinutý firmou Aladdin, který nepotřeboval žádný další hardware, ale stačil mu pouze USB port. Samotné řešení bylo postavené na přidělování privátní IP adresy IPSec

klientům na základě jejich autentizace. USB klíče byly úspěšně testovány a uvedeny do provozu na vybraných aktivních prvcích firmy Cisco.

## 3.1 VYUŽITÍ JEDNODESKOVÝCH POČÍTAČŮ PRO ZABEZPEČENÍ PŘENOSU MEDICÍNSKÝCH DAT

Následující kapitoly se zaměří na možnosti využití malých jednodeskových počítačů v medicínských aplikacích. Nejprve bude popsána realizace jednodeskového počítače, a poté budou uvedeny jeho možnosti při reálném použití v síťových instalacích. Výsledky výzkumu, jehož jsem byl spoluřešitelem, byly prezentovány v rámci projektu Fondu rozvoje CESNET, z.s.p.o. č. 311R1/2009 s názvem „Využití jednodeskových počítačů pro zabezpečení přenosu medicínských dat“.

Zabezpečená síť pro virtuální pracovní tým je tvořena soustavou IPsec tunelů ukončených ve dvou geograficky vzdálených lokalitách Masarykovy univerzity. Dvojice firewallů ASA5520 je konfigurována jako redundantní IPSec koncentrátor. Zařízení by proto mělo být složeno z cenově dostupných komponent a zajišťovat všechny služby potřebné pro bezpečný a spolehlivý přístup ke službám systému. Přemístěním služeb typu překlad adres, filtrování provozu a sestavení kryptograficky zabezpečeného tunelu postaveného na protokolu IPsec z klientské stanice do dedikovaného zařízení, se významně usnadní konfigurace a správa celého řešení. Hmotnost a rozměry použitého externího zařízení přitom musí být takové, aby toto řešení uživatele co nejméně omezovalo a obtěžovalo. Rovněž připojení tohoto zařízení ke klientskému počítači musí být co nejjednodušší.

### 3.1.1 Realizace počítače

Gumstix Verdex Pro 6LP má rozměry 80x20x6,3mm. K počítači je však nutné připojit desku síťového rozhraní o rozměrech 93x20mm. K této desce je možno volitelně připojit i desku rozhraní Wi-Fi 802.11b/g. Počítače Gumstix Verdex nabízí mimo jiné rozhraní USB typu OTG. Toto rozhraní je využito pro připojení k uživatelskému systému. Rozhraní USB OTG je však k dispozici pouze na konektoru pro rozšiřující moduly typ Hirose 60pin. Počítač může mít napájení přivedeno tímtéž konektorem. Externí napájení je připraveno např. na desce rozhraní ethernet. Napájení počítače bylo vyřešeno pomocí USB připojení k uživatelské stanici. Z těchto důvodů bylo nutné vyvinout a vyrobit hardwarový modul, který vyvede rozhraní USB OTG na standardní konektor - přivede napájení z externího USB portu

na napájecí sběrnici počítače - poskytne základní ochranné obvody napájení. Vývoj a výroba tohoto modulu byla řešena dodavatelsky.

Dále bylo třeba vyrobit vhodné pouzdro - chassis - pro uložení počítače. Vzhledem k tomu, že byl nakonec použit pouze jeden typ počítače namísto původně plánovaných dvou (Verdex a Overo, které bohužel nemá použitelnou kartu síťového rozhraní), bylo možno použít více finančních prostředků na vývoj chassis tohoto počítače. Zařízení tak oproti plánu navíc získalo i externí anténu pro připojení k Wi-Fi síti. Pouzdro počítače Gumstix Verdex je na obr. 3.1.

Obr. 3.1: Pouzdro počítače Gumstix Verdex vyvinuté na zakázku pro potřeby řešení projektu

Vývoj a výroba chassis byla svěřena specializované firmě. Prototyp zařízení je nakonec o 12 mm delší než deska ethernetového rozhraní. Důvodem k tomuto prodloužení je potřeba mechanického uchycení počítače v chassis a potřeba získat prostor pro ukotvení antény Wi-Fi. Původním záměrem bylo použití konektoru typu A-male přímo na příslušné desce plošných spojů pro připojení k USB portu uživatelské stanice. To by umožnilo připojit vyvíjené zařízení k počítači bez použití USB kabelu. Z důvodu velkého mechanického namáhání těchto konektorů bylo od tohoto záměru upuštěno. Zařízení proto používá konektor miniB-female a k počítači se připojuje kabelem.

### 3.1.2 Diskuze výsledku vyvinutého zařízení

Vyvíjené zařízení neslouží jako bezpečné úložiště privátních PKI klíčů, které by mohly být případně použity pro autentizaci nebo pro šifrování provozu. Rozšíření řešení tímto směrem je však v budoucnu možné. Výhodou tohoto řešení jsou velmi malé rozměry. Toto řešení však není otevřené, je koncipováno jako firewalová, antivirová a antispamová ochrana počítače a vyžaduje instalaci speciálních ovladačů do operačního systému tohoto počítače. Prototyp zařízení vyvinutý v rámci řešení projektu je složen z cenově dostupných komponent a zajišťuje všechny služby potřebné pro bezpečný a spolehlivý přístup ke službám systému MeDiMed.

## 3.2 SIMULACE VLIVŮ NASTAVENÍ TCP PAKETU A ŠIFROVÁNÍ NA RYCHLOST PŘENOSU DAT

Následující kapitoly budou zaměřeny na porovnání rychlosti přenosu 500MB souboru mezi serverem a klientem při nastavení různých kombinací šifer a hešovacích funkcí. Budou demonstrovány požadavky na rychlost přenosu při dostatečném zabezpečení přenášených informací v medicínských aplikacích. Ty jsou základními podmínkami pro návrh řešení, jenž má tyto specifické nároky splňovat. Zejména zajištění zabezpečeného přístupu z pracovních stanic s pomalejším připojením je nutná optimalizace a volba šifrování tak, aby uživatel nepociťoval přílišný diskomfort. Možností, jak optimalizovat nastavení parametrů přenášených dat je více a jejich vhodnou kombinací lze dosáhnout lepších výsledků, než při běžném nastavení aktivních síťových prvků. Taktéž je důležitý i výběr vhodného typu šifry tak, aby byly splněny nároky na zabezpečení přenosu citlivých medicínských informací a zároveň nebyl objem přenášených dat výrazně navyšován.

Z měření přenosu 500 MB souboru bude vybrána jedna kombinace šifry a hešovací funkce. S touto kombinací budou prováděna další měření. Nejprve bude ukázán vliv velikosti window size na délku přenosu a poté bude změřen účinek nastavení velikosti bufferu na délku přenosu. Poslední měření bude opět zkoumat délku přenosu ovlivněnou velikostí MSS (Maximum Segment Size) u TCP paketu. Velikost MSS má nezanedbatelný vliv na celkovou rychlost přenosu dat.

Parametry budou nastaveny na routerech umístěných mezi serverem a klientem. Klientské PC bude k serveru připojeno metalickou 10Mbps linkou. Mezi serverem a klientem budou umístěny switche Cisco Catalyst 3550, na které budou připojeny stanice. Firewally Cisco ASA 5505 se budou starat o šifrování. Provoz bude simulován pomocí programu Iperf a jeho grafické nástavby Jperf. Rychlost přenosu bude měřena na klientské stanici programem Wireshark.

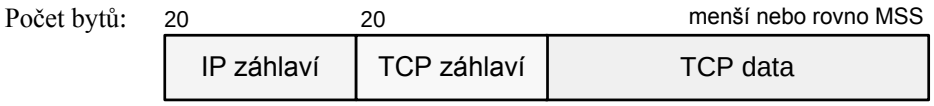
### 3.2.1 MSS

MSS (Maximum Segment Size) označuje největší objem TCP dat, která lze v rámci TCP poslat. Výsledný IP datagram je ještě o 40 oktetů delší (záhlaví IP a TCP). Teoreticky MSS může být 65.495, ale prakticky se používá hodnota MTU (Maximum Transmission Unit) odchozího rozhraní snížená o 40 oktetů (např. pro Ethernet by MSS bylo 1500 – 40 = 1460). Typická velikost MSS je právě 1460 bytů.

Při dlouhém segmentu TCP pak může docházet k další fragmentaci protokolem síťové vrstvy IP. MSS není hodnota, kterou by komunikující strany mezi sebou nějak dojednávaly při navazování spojení. Každá strana může použít volitelnou

možnost pro informování druhé strany o MSS, které očekává, ale nemusí. Pokud informace o MSS chybí, implicitně se použije hodnota 536 oktetů.

Výkonnost sítě přitom může degradovat při používání buď extrémně velkých segmentů, nebo extrémně krátkých segmentů. Každý segment obsahuje nejméně 40 oktetů záhlaví IP a TCP kromě samostatných dat. Pokud bychom tedy nastavili velikost MSS na 40 bytů, bylo by v každém segmentu obsaženo pouze maximálně 50% skutečných údajů a efektivita přenosu by byla velmi malá. Zapouzdření segmentu TCP do diagramu IP je znázorněno na obr. 3.2.

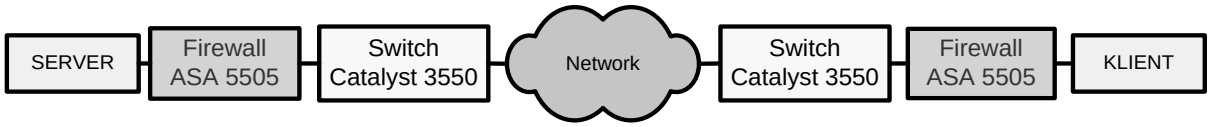



Obr. 3.2: Zapouzdření segmentu TCP do diagramu IP

### 3.2.2 Měřící sestava a schéma zapojení

Zapojení testovací sestavy je uvedeno na obr. 3.3. Skládá se z rackmount serveru, který je programem Iperf nakonfigurován jako server. K serveru je připojen firewall Cisco ASA 5505, na kterém bude nastavováno šifrování, hešovací funkce a také velikost MSS.

Dále jsou do měřící sestavy připojeny dva switche Cisco Catalyst 3550, které simulují koncová zařízení ISP (Internet Service Provider). Na nich je uměle omezena rychlost na 10Mbps, aby lépe odpovídala průměrné rychlosti poskytovatelů internetu. Na druhém konci pomyslné sítě je opět umístěn firewall Cisco ASA 5505, který šifruje provoz na straně klienta.




Obr. 3.3: Zapojení testovací sestavy

| | |
|---|---|
| SERVER – | Rackmount server; RedHat EL 5; Intel Xeon 2,8GHz; 4 GB RAM; 80GB SSD HDD; Iperf 2.0.5, rel. 1.el5 |
| Firewall ASA 5505 – | zajišťuje šifrování provozu na straně serveru a klienta |
| Switch Catalyst 3550 – | simuluje koncové zařízení ISP |
| KLIENT – | Notebook HP-6730b; Win7 Prof. SP1 v 2009 32b; Intel Core2 Duo CPU T9400@ 2,53GHz; 4GB RAM; 60GB HDD; Iperf 1.7.0, Jperf 2.0.2; Wireshark 1.6.7 (SVN Rev 41973 from/trunk-1.6) |

### 3.2.3 Aplikace použité při měření přenosu

Utilita Iperf je jednoduchou aplikací, která umožnuje testování propustnosti datového spoje. Nadstavba Jperf usnadňuje obsluhu a místo nastavování parametrů

pomocí textových příkazů lze kritéria jednoduše zadávat v grafickém rozhraní. Na serveru byla nainstalována verze Iperf 2.0.5, rel. 1.el5 a u klienta verze Iperf 1.7.0 a Jperf 2.0.2.

Program Wireshark je jedním z nejpoužívanějších protokolových analyzátorů používaných k analýze a ladění problémů v počítačových sítích. Aplikace byla nainstalována na klientském PC, kde monitorovala síťový provoz. Pomocí Wiresharku byl odečítán čas přenosu 500 MB souboru.

### 3.2.4 Porovnání rychlosti přenosu souboru při různých kombinacích šifer a hešovacích funkcí

Na obou firewallech Cisco ASA 5505 byly postupně nastavovány parametry pro šifrování a hešování přenosu 500MB souboru. Firewally bohužel neumožnily nastavit přenos dat bez šifrování a heše.

Výsledkem tohoto měření je tabulka 3.1, ve které je porovnáno pět typů šifrování, od nejjednoduššího a nespolehlivého DES, přes jeho vylepšenou verzi 3DES až po v současné době nejpoužívanější symetrickou blokovou šifru AES se 128, 192 a 256bitovými klíči.

Tab. 3.1: Porovnání rychlosti přenosu při různých kombinacích šifer a hešovacích funkcí

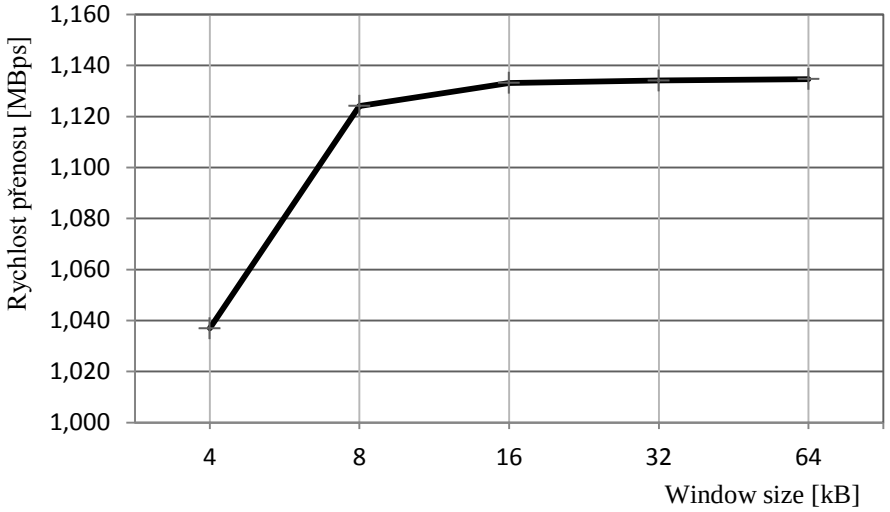
| Šifra | Hešovací funkce | Rychlost[MBps] |
|---|---|---|
| DES | MD5 | 1,13221 |
| 3DES | MD5 | 1,13264 |
| AES-128 | MD5 | 1,12542 |
| AES-192 | MD5 | 1,12357 |
| AES-256 | MD5 | 1,12345 |
| Bez šifry | MD5 | 1,13596 |
| DES | SHA | 1,12960 |
| 3DES | SHA | 1,12978 |
| AES-128 | SHA | 1,12335 |
| AES-192 | SHA | 1,12358 |
| AES-256 | SHA | 1,12256 |
| Bez šifry | SHA | 1,13575 |
| DES | Bez heše | 1,13930 |
| 3DES | Bez heše | 1,14154 |
| AES-128 | Bez heše | 1,13408 |
| AES-192 | Bez heše | 1,13438 |
| AES-256 | Bez heše | 1,14163 |
| Bez šifry | Bez heše | 0 |

Jako zástupci hešovacích funkcí byly zvoleny MD5, SHA a pro porovnání bylo provedeno měření i bez použité hešovací funkce. Rozdíly mezi nejnižšími a

nejvyššími hodnotami v rámci jedné použité hešovací funkce jsou velmi malé a pohybují se v řádech několika kBps. Rozdíl mezi nejpomalejší rychlostí přenosu u kombinace šifrování AES-256 s SHA a nejvyšší u kombinace šifrování AES-256 bez heše byl zhruba 19 kBps, což odpovídá 1,7%. Z tohoto důvodu byla pro další měření vybrána kombinace parametrů, která se při současném výpočetním výkonu používá při přenosu medicínských dat nejčastěji. Jedná se o šifru AES-256 s hešem SHA. Tato kombinace je současně nejsilnějším běžně používaným řešením při přenosu citlivých medicínských informací.

### 3.2.5 Porovnání rychlosti přenosu souboru při různé velikosti window size

V grafu na obr. 3.4 jsou zaznamenány rychlosti přenosu, které byly dosaženy při nastavování různé velikosti window size paketu TCP v programu Iperf. Byla nastavena šifra AES-256 a hešovací funkce SHA. Velikost bufferu byla 2MB.




Obr. 3.4: Graf rychlosti přenosu při různé velikosti window size

Z grafu je patrné, že nejvyšší rychlosti při přenosu 500MB souboru bylo dosaženo u window size 64kB, proto bude tato hodnota nastavena v následujících měřeních.

### 3.2.6 Porovnání rychlosti přenosu souboru při různé velikosti bufferu

V grafu na obr. 3.5 jsou uvedeny rychlosti přenosu, které byly dosaženy při nastavování různé velikosti bufferu paketu TCP v programu Iperf. Opět byla nastavena šifra AES-256 a hešovací funkce SHA. Window size bylo na základě minulého měření nastaveno na 64 kB.


Obr. 3.5: Graf rychlosti přenosu při různé velikosti bufferu

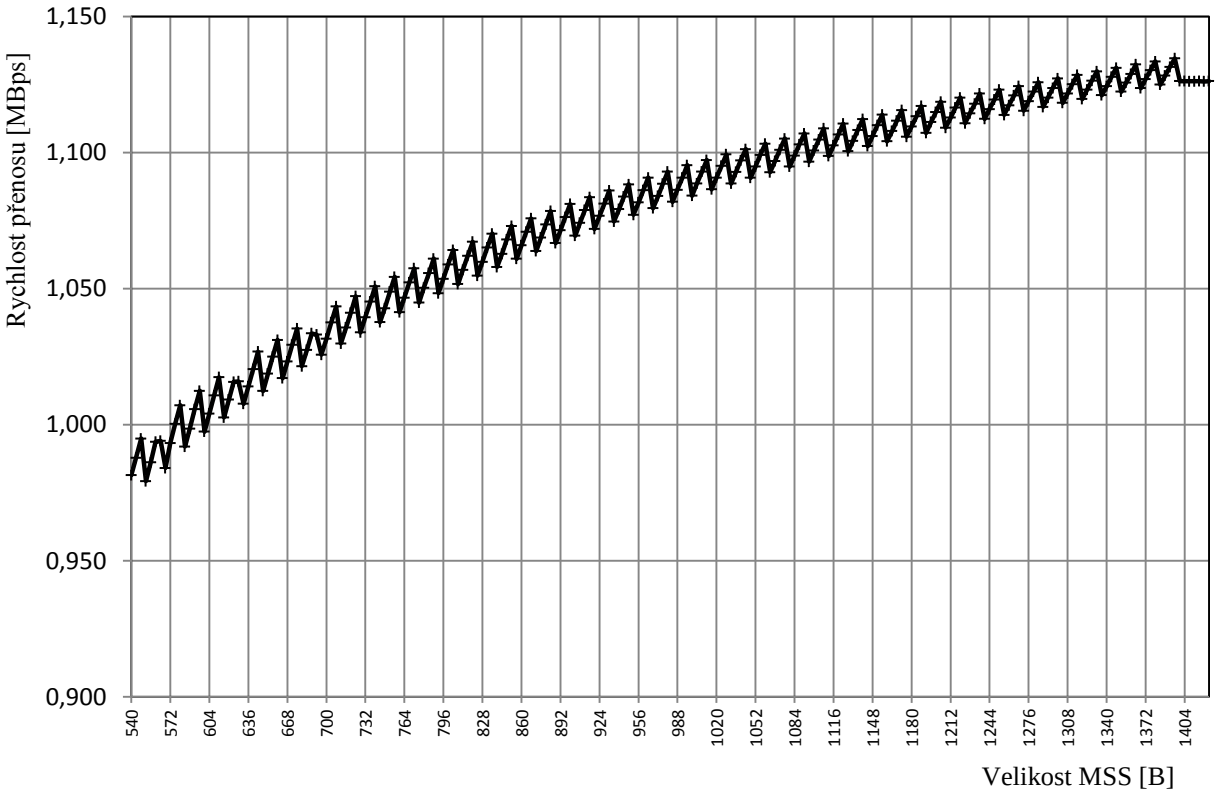
Nejvyšší rychlosti přenosu bylo dosaženo u velikosti bufferu 1MB. Vzhledem k tomu, že se v přenosových sítích běžně používá velikost bufferu 2MB a rozdíl mezi rychlostí přenosu s 1 MB a s 2 MB byl minimální, byl tento parametr v následujícím měření nastaven na 2 MB.

### 3.2.7 Vliv velikosti MSS na rychlost přenosu

Cílem tohoto měření bylo ukázat závislost nastavení velikosti MSS na rychlost přenášených dat. Na základě předchozích měření byly nastaveny následující vstupní parametry:

- Velikost bufferu 2MB
- Velikost window size 64kB
- Šifrovací algoritmus AES-256
- Hešovací funkce SHA

V následujícím grafu na obr. 3.6 je zobrazeno 222 hodnot nastavení MSS. Nejnižší hodnota, kterou umožnil firewall Cisco ASA 5505 nastavit je 540B. Hodnoty byly nastavovány po 4B krocích.




Nejvyšší rychlost přenosu 500 MB souboru byla naměřena při nastavení velikosti MSS 1396 B, a to 1,13456 MBps. Z grafu je patrné, že od hodnoty 1400 B se přenosová rychlost ustálila na konstantní hodnotě 1,126 MBps. Pilovitý průběh rychlosti přenosu je způsoben použitím šifrovacího algoritmu, který zpracovává data po blocích. Pokud velikost MSS odpovídá násobku délky zpracovávaného šifrovaného bloku, nastane lokální maximum.

# 4 ZÁVĚR

Disertační práce se zaměřila na analýzu přenosového pásma určeného pro transport medicínských obrazových dat mezi zdravotnickými zařízeními a vzdálenými datovými úložišti. Současně se věnovala bezpečnostním požadavkům pro přenos dat mezi pracovními stanicemi a vzdálenými datovými úložišti. Byly analyzovány datové toky jednotlivých modalit a prohlížecích stanic zapojených do systému MeDiMed.

S ohledem na očekávané masovější připojování menších zdravotnických zařízení jsem se zaměřil na analýzu datových toků modalit, které lze u tohoto typu uživatelů očekávat. U menších zdravotnických zařízení je důležité sledovat šířku přenosového pásma z důvodu požadavku na okamžitý přístup k obrazovým studiím v jednotkách sekund. Tato podmínka je však v protikladu s nutností dostatečné míry zabezpečení přenášených dat. Správně dimenzované spojení mezi zdravotnickým zařízením a centrálním úložištěm je základem pro komfortní práci s obrazovými daty.

Na srovnání ultrazvuků analyzovaných nemocnic je názorně vidět, že i jednodušší přístroje dokážou generovat odlišné datové toky. Tento fakt je nutné brát v úvahu při návrhu infrastruktury sítě. Požadavky na zpracování medicínských dat a dostatečný prostor k jejich ukládání a archivaci se budou stále zvyšovat současně se zlepšováním technických parametrů lékařských modalit a prohlížecích stanic.

Optimalizací parametrů přenosové trasy pro přenos medicínských obrazových dat lze dosáhnout zkrácení doby přenosu, což zvyšuje uživatelský komfort bez navyšování požadavků na šířku pásma a tím i nákladů na přenosové služby.

Analýzou bylo zjištěno, že datový provoz zkoumaných modalit se zpravidla koncentruje do běžné pracovní doby, na rozdíl od modalit obvyklých pro velké nemocnice (CT, magnetická rezonance), kde je takřka nepřetržitý provoz. Tato analýza umožní optimalizovat šířku pásma pro přenos dat menších zdravotnických zařízení a tím usnadní jejich zapojení do sdílených systémů pro zpracování medicínských obrazových dat, např. MeDiMed.

# 5 LITERATURA


[1] JAVORNÍK, M. Podpora komunikace virtuálních pracovních týmů v oblasti zpracování medicínských obrazových dat. *Závěrečná zpráva projektu 252/2007*, Cesnet, 2009

[2] DOSTÁL, O.; JAVORNÍK, M.; PETRENKO M.; SLAVÍČEK, K. Projekt MEDIMED – metropolitní PACS archiv v Brně. *Širokopásmové sítě a jejich aplikace*. Olomouc, 2005, s.138-143, ISBN: 80-244-1035-4

[3] DOSTÁL, O.; JAVORNÍK, M.; PETRENKO M.; ROČEK, A.; SLAVÍČEK, K. Projekt MEDIMED – regionální archiv medicínských obrazových dat. *Širokopásmové sítě a jejich aplikace*. Olomouc, 2007, s.110-114, ISBN: 978-80-244-1687-8

[4] JAVORNÍK, M. Dohledový systém metropolitního archivu medicínské obrazové informace, *Závěrečná zpráva projektu 143R1/2005*, Cesnet, 2007

[5] - eToken PRO - Portable USB Token With Advanced Smart Card Technology [online]. 2009, [cit. 2009-02-27]. Dostupné z: <http://www.aladdin.com/etoken/pro/usb.asp>.

[6] JAVORNÍK, M. Autentizovaný přístup k službám metropolitního archivu medicínské obrazové informace, *Závěrečná zpráva projektu 081/2004*, Cesnet, 2006

[7] SCHINDLER, V. Použití kryptografických metod v medicínských aplikacích. *Elektrorevue –internetový časopis (http://www.elektrorevue.cz)*, 2007. 2007(23). p. 1 – 5. ISSN 1213-1539.

[8] DOSTÁL, O.; JAVORNÍK, M.; SLAVÍČEK, K. Oportunity of Current ICT in the Processing of Medical Image Information. In *Proceedings of the IASTED International Conference on Advances in Computer Science and Technology*, Puerto Vallarta - Mexico, 2006, s.193-195, ISBN 088986-545-0, ISSN 1482-7905

[9] DOSTÁL, O.; JAVORNÍK, M.; SLAVÍČEK, K. Technology background of international colaboration on medicine multimedia klnowledgebase establishment. In *proceedings of the 2nd WSEAS International Conference on COMPUTER ENGINEERING and APPLICATIONS (CEA'08)* Acapulco - Mexico, 2008, s.137-142, ISBN 978-960-6766-33-6, ISSN 1790-5117

[10] BARTOŠEK, M. Dílčí zpráva o řešení výzkumného záměru za rok 2003 [online]. 2002, poslední revize 7. 1. 2003 [cit. 2009-03-26]. Dostupné z: <http://www.ics.muni.cz/toUTF8.cs/ research/VZ_zprava2003.html>.

[11] BARTOŠEK, M. Dílčí zpráva o řešení výzkumného záměru za rok 2004 [online]. 2005, poslední revize 8. 2. 2005 [cit. 2006-03-26]. Dostupné z: <http://www.ics.muni.cz/toUTF8.cs/ research/VZ_zprava2004.html>.

[12] SLAVÍČEK, K.; JAVORNÍK, M.; DOSTÁL, O. Extension of the Shared Regional PACS Center MeDiMed to Smaller Healthcare Institutions. In *The Eleventh International Conference on Networks.* Saint Gilles, Reunion Island: IARIA, 2012. ISBN 978-1-61208-183-0, s. 83-87. 2012, Saint Gilles, Reunion Island.

[13] JAVORNÍK, M.; DOSTÁL, O.; SLAVÍČEK, K. Regional Medical Imaging System. *World Academy of Science, Engineering and Technology*, France. ISSN: 2010-376X, 2011, vol. 7, no. 79, s. 389-393.

[14] SLAVÍČEK, K.; JAVORNÍK, M.; DOSTÁL, O. Redundancy in Processing of Medical Image Data. In *Fourth International Conference on Computer Sciences and Convergence Information Technology*. Seoul, Korea: IEEE Computer Society Conference Publishing Services, 2009. ISBN 978-1-4244-5244-6, s. 519-523.

[15] SLAVÍČEK, K.; NOVÁK, V. Introduction of Alien Wavelength into Cesnet DWDM Backbone. In: *Sixth International Conference on Information, Communications and Signal Processing.* Singapore : IEEE, 2007. ISBN: 978-1-4244-0982-2, s. 977-981. Singapore.

[16] SLAVÍČEK, K., Maximum Frame Size in Large Layer 2 Networks. *Lecture Notes in Computer Science,* Germany. ISSN: 0302-9743, 2007, vol. 4712, no. 1, s. 409-418.

[17] DOSTÁL, O.; SLAVÍČEK, K. Wireless Technology in Medicine Applications. In *Personal Wireless Communications*. Published. 2007. Praha: Springer Verlag, 2007. ISBN 978-0-387-74158-1, s. 316-324. 2007, Praha.

[18] DOSTÁL, O.; SLAVÍČEK, K.; JAVORNÍK, M. PKI Utilisation for PACS Users Authentication. In *ICN 2006*. Mauritius : IEEE Computer Society, 2006. ISBN: 0-7695-2552-0, s. 151-156. 2006, Mauritius.

[19] DOSTÁL, O.; JAVORNÍK, M.; SLAVÍČEK, K.; PETRENKO, M.; MEDIMED-Regional Centre for Archiving and Interhospital Exchange of Medicine Multimedia Data. In *Proceedings of the Second IASTED International Conference on Communications, Internet, and Information Technology*. Scottsdale, Arizona, USA : International Association of Science and Technology for Development- IASTED, 2003. ISBN: 0-88986-398-9, s. 609-614. 2003, Scottsdale Arizona USA.

[20] SLAVÍČEK, K.; DOSTÁL, O.; JAVORNÍK, M.; DRDLA, M. MEDIMED - Regional Centre for Medicine Image Data Processing. In *Knowledge Discovery and Data Mining*. Published. 2010. USA : IEEE Computer Society, 2010. ISBN 978-0-7695-3923-2, s. 310 - 313. 2010, Phuket, Thailand.

[21] PUŽMANOVÁ, R. TCP/IP v kostce. 2nd ed. České Budějovice: KOPP, 2009. ISBN: 978-80-7232-388-3

[22] Federal information processing standards publication (FIPS 197). Advanced Encryption Standard (AES), 2001.

*Curriculum Vitae*

**Vladimír Schindler**

---

**Osobní údaje:**

| | |
|---|---|
| Jméno a příjmení: | Vladimír Schindler |
| Datum narození: | 19. března 1981 |
| Rodinný stav: | ženatý, 2 děti |
| Bydliště: | Chrastová Lhota 38, Brněnec, 569 04 |
| Telefon: | +420 602 789 647 |
| Email: | v.schin@email.cz |

**Vzdělání:**

- **1995-1999 :** Střední průmyslová škola elektrotechnická v Brně, obor Telekomunikační technika, zakončena závěrečnou maturitní zkouškou.

- **2000-2004 : VUT FEKT v Brně,** magisterské studium, Fakulta elektrotechniky a komunikačních technologií, Obor: Elektronika a sdělovací technika. Zakončeno státní závěrečnou zkouškou na ústavu telekomunikací. (průměr 2,05)

  **Diplomová práce:** Systém dohledu optických vláken

  Diplomová práce získala 4. místo v soutěži České vědeckotechnické společnosti spojů o nejlepší diplomovou práci v oboru telekomunikací a teleinformatiky.

- **od 2006 : VUT FEKT v Brně,** doktorské kombinované studium

  Fakulta elektrotechniky a komunikačních technologií, Obor: Teleinformatika

  **Dizertační práce:** Problematika optimální šířky přenosového pásma pro přenos medicínských obrazových dat

**Zaměstnání:**

- **2004-2013 : Masarykova univerzita, Ústav výpočetní techniky**

  Technické oddělení, systémový analytik

- **od 2013 : Masarykova univerzita, Ústav výpočetní techniky**

  Oddělení nástrojů pro spolupráci – vedoucí pracoviště, systémový analytik

**Účast na vědeckých projektech:**

Spoluřešitel:

- **projekt CESNET/311R1/2009 (**7/2009-7/2010)**,** *Využití jednodeskových počítačů pro zabezpečení přenosu medicínských dat.*
  Řešitel Mgr. Karel Slavíček, Ph.D.

**Jazykové dovednosti**

- **Anglický jazyk** – konverzace na úrovni pokročilý, technická angličtina na dobré úrovni (pasivně)
- **Německý jazyk –** začátečník

**Další informace, záliby a dovednosti**

- Řidičský průkaz skupiny A (bez omezení), B, nekuřák.
- Cestování, informační technologie, film, hudba, rodina.

## Abstrakt

Disertační práce je zaměřena na optimalizaci parametrů přenosového pásma pro transport medicínských obrazových dat mezi zdravotnickými zařízeními a vzdálenými datovými úložišti. Jako reálná a plně funkční struktura, jež bude v této práci analyzována, byl zvolen systém MeDiMed (Metropolitan Digital Imaging System in Medicine).

Práce nejprve rozebírá provoz menších zdravotnických organizací a jejich modalit, které využívají tento systém pro vzdálenou archivaci dat. Analýza provozu je poté statisticky zpracována.

Disertační práce se dále zabývá analýzou zvýšení zabezpečení přístupu pracovních stanic do zdravotnického systému a posuzuje jeho vliv na přenášená data. Je zde porovnáván vliv nastavení přenosových parametrů a nejpoužívanějších typů šifer na rychlost přenosu.

## Abstract

This dissertation thesis is focused on the optimization of bandwidth parameters for the transport of medical image data between medical devices and remote data storage. As real and fully functional structure, which will be analyzed in this work. It was selected system MeDiMed (Metropolitan Digital Imaging System in Medicine).

The thesis examines the operation of the small health organizations and their modalities, which use this system for remote data archiving. Traffic analysis is then statistically processed.

The thesis also deals with the analysis of increasing the security during accessing health system, and assesses its impact on transmitted data. The effect of setting the transmission parameters and the most widely used types of ciphers on the transfer speed is also compared.