

# Využití šifrování v telekomunikačních prostředcích

The Use of Encryption in Telecommunications

Bc. Lukáš Marszalek

---

Diplomová práce  
2015



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

# **ZADÁNÍ DIPLOMOVÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lukáš Marszalek**  
Osobní číslo: **A13350**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **prezenční**

Téma práce: **Využití šifrování v telekomunikačních prostředcích**  
Téma anglicky: **The Use of Encryption in Telecommunications**

Zásady pro vypracování:

1. Specifikujte kryptografické algoritmy používané v současných aplikacích.
2. Charakterizujte problematiku přenosu signálu v telekomunikačních technologiích.
3. Zhodnoťte vybrané produkty, které jsou dostupné v komerčním sektoru.
4. Vyhodnoťte přínosy jednotlivých metod šifrování.
5. Vytvořte návrh vlastního řešení pro šifrování dat v telekomunikačních systémech.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.
2. BURDA, Karel. Aplikovaná kryptografie. 1. vyd. Brno: Vutium, 2013, 255 s. ISBN 978-80-214-4612-0.
3. LEK, Kamol a Naruemol RAJAPAKSE. Cryptography: protocols, design, and applications. New York: Nova Science Publishers, c2012, ix, 242 s. ISBN 978-1-62100-779-1.
4. JANSEN, Horst a Heinrich RÖTTER. Informační a telekomunikační technika. Vyd. 1. Praha: Europa – Sobotáles, 2004, 399 s. ISBN 8086706087.
5. VODRÁŽKA, Jiří a Ivan PRAVDA. Principy telekomunikačních systémů. Vyd. 1. Praha: Česká technika – nakladatelství ČVUT, 2006, 130 s. ISBN 800103366x.
6. STRNAD, Ladislav. Synchronizace sítí. 1. vyd. Praha: České vysoké učení technické v Praze, 2013, 166 s. ISBN 978-80-01-05196-2.
7. LAYON, Kristofer. Digital product management: design websites and mobile apps that exceed expectations. Berkeley, California: New Riders, c2014, xix, 168 s. ISBN 978-0-321-94797-0.
8. CASTLEDINE, Earle, Myles EFTOS a Max WHEELER. Vytváříme mobilní web a aplikace pro chytré telefony a tablety. 1. vyd. Brno: Computer Press, 2013, 288 s. ISBN 978-80-251-3763-5.

Vedoucí diplomové práce:

**Ing. David Malaník, Ph.D.**

Ústav informatiky a umělé inteligence


Datum zadání diplomové práce:

**12. ledna 2015**

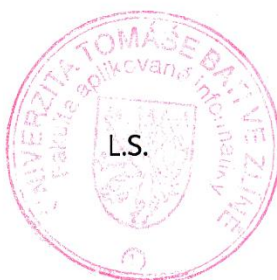
Termín odevzdání diplomové práce:

**15. května 2015**

Ve Zlíně dne 6. února 2015



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*

  
*ředitel ústavu*

doc. RNDr. Vojtěch Křesálek, CSc.

**Prohlašuji, že**

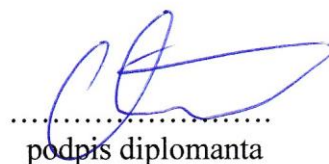
- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

dne 24.05.2015

  
.....  
podpis diplomanta

## ABSTRAKT

Práce se zabývá problematikou zabezpečení telekomunikační techniky proti odposlechu. Tedy moderním pojetím datové bezpečnosti. Prioritně je řešena problematika odposlouchávání a sledování citlivých údajů, a to prostřednictvím neznámého útočníka. Tato práce se proto zaměřuje na účinné způsoby jakými se tomuto narušení bránit z různých postavení. V praktické části je zejména řešena problematika běžného uživatele, soukromé osoby.

Klíčová slova: zabezpečení, telekomunikace, šifrování, mobilní zařízení

## ABSTRACT

This work covers the problem of secure telecommunication technology before listening. This means a modern way of look to data secure. With best priorities is seaking the look at listening and capturing of delicate informations, which is doing by unknown threat. This work is looking for working solutions how to defend ourselves from diferent possitions. In practical part is mainly solving the problems of common, private, users.

Keywords: security, telecommunication, encryption, mobile device

Ve své práci bych chtěl poděkovat svému vedoucímu Ing. Davidovi Malaníkovi PhD. za trpělivost, kterou věnoval mému úsilí, odborné vedení a rady, které mi věnoval již při studiu, ale i později s mou diplomovou prací aniž by se zaleknul mých nápadů i nedostatku času.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

**OBSAH**

<b>ÚVOD</b>	9
<b>I TEORETICKÁ ČÁST</b>	10
<b>1 KRYPTOGRAFIE</b>	11
1.1 HASH algoritmy	11
1.1.1 SHA	11
1.2 Symetrická kryptografie	11
1.2.1 Proudové šifry	11
1.2.2 Blokové šifry	12
1.2.3 AES	13
1.2.4 Twofish	13
1.2.5 Diffie-Hellman protokol	14
1.3 Asymetrická kryptografie	14
1.3.1 RSA	14
1.3.1.1 ZRTP	15
<b>2 TELEKOMUNIKAČNÍ TECHNOLOGIE</b>	16
2.1 VoIP telekomunikace	16
2.2 Mobilní telekomunikační technologie	17
2.2.1 GSM síť	17
2.2.2 UTRA	18
2.2.3 HSDPA	18
2.2.4 HSUPA	18
2.2.5 CDMA	19
2.2.6 W-CDMA	19
2.2.7 TDD	19
2.2.8 FDD	20
2.3 Satelitní telekomunikace	21
2.4 Převod zvukového signálu	22
2.5 Kódování	23
2.5.1 Skramblovací kódy	23
2.5.2 Kanálové kódy	24
2.5.3 Rozprostírací kódy	24
2.5.4 Symboly a čipy	24
<b>3 ŠIFROVACÍ TECHNOLOGIE PRO MOBILNÍ ZAŘÍZENÍ</b>	25
3.1 Zabezpečená infrastruktura	25
3.2 Šifrovací aplikace	25
3.2.1 Princip End-to-End v porovnání s Point-to-Point	25
3.2.2 Datový přenos v moderních sítích	26
3.3 VOIP telefonie	27
3.4 Speciální telefony	27
<b>II PRAKTICKÁ ČÁST</b>	28
<b>4 FUNKČNÍ APLIKACE NA TRHU</b>	29



4.1	Analyzátor paketů (sniffer) .....	29
4.2	Měřicí soustava .....	30
4.3	Hodnocené aplikace .....	31
4.3.1	BABEL .....	31
4.3.1.1	Hodnocení metodiky .....	32
4.3.2	PhoneX .....	33
4.3.2.1	Hodnocení metodiky .....	34
4.3.2.2	Výsledky měření.....	37
4.3.3	Open Whisper System .....	38
4.3.3.1	Hodnocení metodiky .....	38
4.3.3.2	Výsledky měření.....	40
<b>5</b>	<b>HODNOCENÍ FUNKČNÍCH MODELŮ NA TRHU .....</b>	<b>42</b>
5.1	Státní sektor .....	42
5.2	Zprostředkovatel na End-to-End komunikaci .....	43
5.3	Zabezpečení přenosu po GSM síti .....	44
5.4	Vyhodnocení .....	44
<b>6</b>	<b>NÁVRH ŘEŠENÍ ZABEZPEČENÍ KOMUNIKACE POMOCI ŠIFROVÁNÍ .....</b>	<b>45</b>
6.1	Způsob přenosu .....	45
6.2	Výběr vhodného algoritmu .....	47
6.2.1	Zahájení přenosové trasy .....	48
6.2.2	Příjem komunikace.....	49
6.2.3	Způsob ověření a distribuce klíčů .....	49
6.3	Tvorba rozhraní .....	51
6.4	Vyhodnocení .....	51
	<b>ZÁVĚR .....</b>	<b>53</b>
	<b>ZÁVĚR V ANGLIČTINĚ .....</b>	<b>54</b>
	<b>SEZNAM POUŽITÉ LITERATURY .....</b>	<b>55</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>57</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>59</b>
	<b>SEZNAM TABULEK .....</b>	<b>61</b>
	<b>SEZNAM PŘÍLOH .....</b>	<b>62</b>



## ÚVOD

Žijeme v době globální společnosti, kdy o sobě šíříme spoustu informací prostřednictvím technologií, jako jsou Internet a mobilní zařízení. Mnohdy si ani neuvědomujeme, kdo všechno může naše informace zobrazit a někdy nevíme, kdo by se mohl pokoušet do našich životů nahlížet bez našeho vědomí a svolení.

Zařízení, které používáme, jsou stále vyspělejší, inteligentnější, a proto bychom měli klást důraz na jejich zabezpečení. První možností je hlídat si informace, které těmito prostředky šíříme. Pokud však nemáme jiných možností, musíme se pohlédnout po technologiích, které nám umožní učinit takovou komunikaci co nejbezpečnější. Mezi takovéto prostředky patří právě kryptografie, kterou lze právě díky vyspělosti moderních zařízení aplikovat.

Abychom však mohly některé technologie aplikovat je zapotřebí vyspělého zázemí pro šíření informací. Tím máme především na mysli technologie mobilní komunikace, jakými jsou například vyspělé sítě, které umožňují datový přenos bezdrátovou formou na vysoké úrovni spolehlivosti a přenosové rychlosti. Zároveň však nesmíme zapomínat na konvenční formu připojení, pomocí drátových nebo optických technologií.

V otázkách zabezpečení komunikace se nám následně otevírá velké množství možností aplikace konkrétního řešení na různých rozhraních. V poslední době jsou zejména v rozvoji aplikace pro koncová zařízení. Tyto aplikace umožňují vytvářet zabezpečená spojení v rámci standardní sítě a to sice skrze vyhrazené linky nebo prostřednictvím zabezpečené infrastruktury. Je velmi důležité, položit si otázku vhodného řešení pro konkrétní potřeby uživatele. Zejména pak z pohledu užitého, ale i finančního.

Pro toto rozhodnutí je vhodné znát výhody nevýhody jednotlivých řešení stejně tak jako vhodnou metodiku a parametry systémů.

## **I. TEORETICKÁ ČÁST**

## 1 KRYPTOGRAFIE

Kryptografie je vědní obor, který se zabývá zabezpečením informací proti zneužití, změně obsahu nebo krádeži. V následujících podkapitolách si vysvětlíme základní členění, ve kterém jsou uvedeny souvztažné funkce používané k zabezpečení přenosu hlasových a textových zpráv.

### 1.1 HASH algoritmy

Hash algoritmus je jednocestná funkce, která vytváří digitální otisk souboru. Princip je založen na vytvoření souboru o pevné délce z libovolně dlouhého vstupu. Základem dobře navrženého algoritmu je bezkoliznost (dva soubory nemůžou mít stejný otisk) a skutečnost, že libovolně malá změna (například změna data úpravy/otevření v hlavičce souboru) vyvolá velký rozdíl ve výsledku. Postup vytváření hashe je založený na zarovnání zprávy do bloku. Tyto bloky musí mít konstantní délku, a proto jsou případně doplněny o vyrovnávací bity. Na konec řady se umístí požadovaná délka otisku, která se započítává do výpočetních bloku. Následně se definují stavy bloku závislé na operaci posunu bitů. Výsledná hodnota je poté právě funkcí těchto stavů.[1],[2]

#### 1.1.1 SHA

Byl vyvinut americkou vládou pro účely digitálního podpisu. Původní algoritmus byl, kvůli nedostačující délce kódu, prolomen. Základem byla délka hashe 160 bitu a zarovnání do bloků o 32 bitech. Je zde použita rotace bloku v pozicích. Modernější verze používají bloky o větších délkách (například 256).[1],[2]

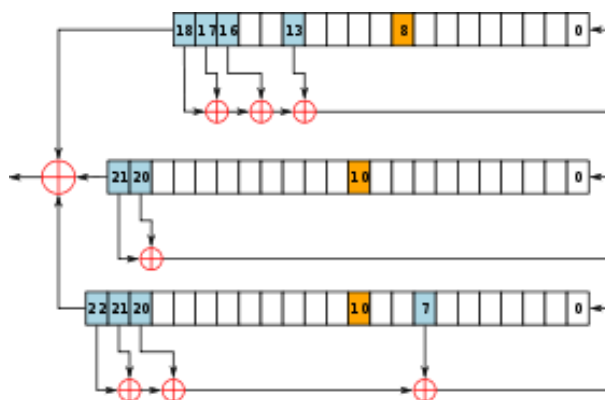
### 1.2 Symetrická kryptografie

Pro symetrickou kryptografii platí, že pro šifrování i dešifrování je použit stejný klíč. Proto je zde hrozba, že klíč bude odhalen při předávání nebo při archivaci. Pro tvorbu klíče se používají generátory pseudonáhodných klíčů. Platí však, že klíče jsou snadno odvoditelné při dostatečném množství vzorků a vstupních parametrů, případně ze znalosti klíče příjemce nebo adresáta. Tato metoda je výpočetně velmi rychlá.[1]

#### 1.2.1 Proudové šifry

Proudová šifra je tvořená šifrovacím klíčem a šifrovacím algoritmem, aby byla zachována nahodilost. Šifrovací algoritmus tvoří posloupnost funkcí XOR, tedy logického součtu.

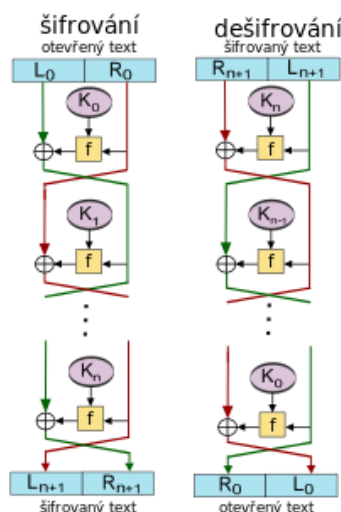
Zpráva se šifruje po jednotlivých bitech. Šifrovací posloupnost musí být vždy stejná na straně příjemce i odesílatele. Tato synchronizace může například probíhat pomocí klíče, který nastaví pseudonáhodný generátor do stejného stavu na obou stranách komunikačního kanálu.[1]



Obrázek 1: Proudová šifra[3]

### 1.2.2 Blokové šifry

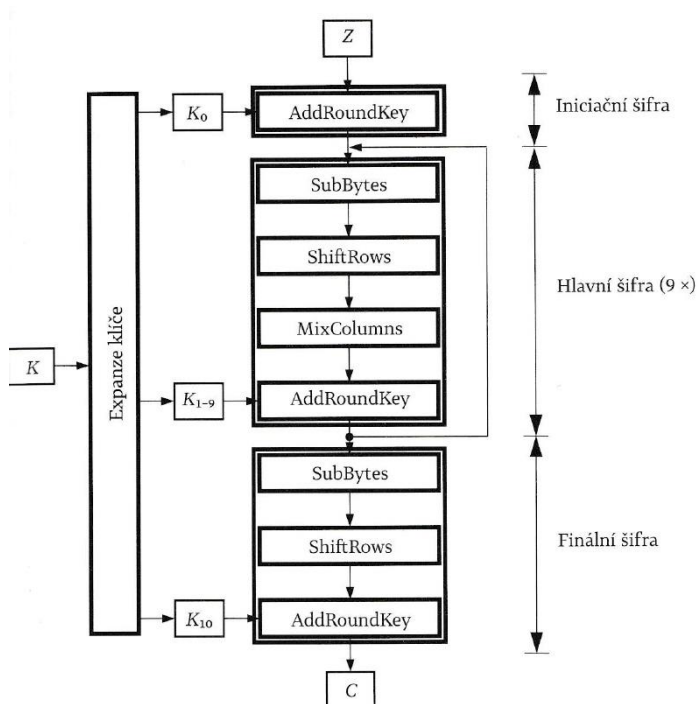
Blokovou šifru tvoří předem definované bloky o stejné velikosti, kdy poslední blok je pak vhodně doplněn na požadovanou velikost. Pro každý blok je pak použit jiný šifrovací klíč. Každý výstupní bit je přímo závislý na všech bitech v bloku vstupním. Velmi často se blok šifruje několikrát za sebou. Jinou variantou je možnost rozdělení klíče do subklíčů které jsou distribuovány v posloupnosti na jednotlivé procesní bloky, tomuto říkáme iterační proces.[1]



Obrázek 2: Bloková šifra[4]

### 1.2.3 AES

Jedná se o blokovou šifru, která byla původně navržena pro státní správu Spojených států amerických. Postupně se stala celosvětový standardem. Obsahuje bloky o délce 128 bitů, které šifruje pomocí klíčů o délce 128, 192 nebo 256 bitů. Používá maticového znázornění místo vektorového uspořádání bloků. To umožňuje rozšíření výpočetních a logických operací o transformace. Mezi ně patří posun v řádku, záměna řádků a substituce sloupců (pomocí transformace iteračním klíčem).[1]



Obrázek 3: Princip AES[1]

### 1.2.4 Twofish

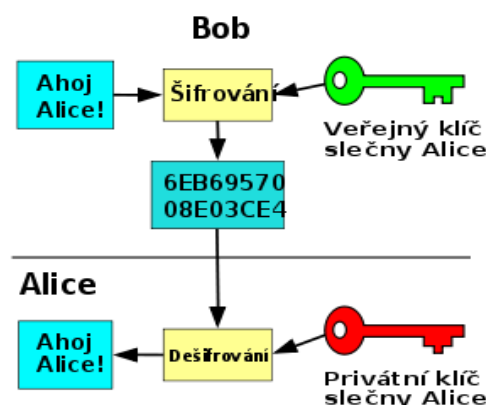
Jedná se o blokovou šifru, která byla vytvořena jako náhrada za prolomený DES algoritmus. Obsahuje bloky o 128 bitech a výsledný klíč má hodnotu až 256 bitů. Princip je založen na rozdělení bloku do dvou sérií bitů, první polovina je využita k šifrování zprávy a druhá k úpravě algoritmu (doplňuje šifrovací klíč bloků). Využívá s-boxy (předdefinované úseky šifrovacího klíče) v kombinaci s hashem MD5. Celou operaci opakuje 16-krát než vygeneruje zašifrovanou zprávu. [5]

### 1.2.5 Diffie-Hellman protokol

Slouží k vypočtení symetrického klíče komunikace. Nejprve se vhodně zvolí dvě velká prvočísla  $p$  a  $q$ , kdy  $p$  vždy dosadíme do funkce modulo a  $q$  umocníme náhodně zvoleným číslem, v rozsahu mezi 1 a  $p-1$ , konkrétního uživatele. Výsledný šifrovací klíč  $K$  je poté  $q$  umocněné na  $x*y$  v součinu s funkcí prvočísla (modulo  $p$ ). [2]

## 1.3 Asymetrická kryptografie

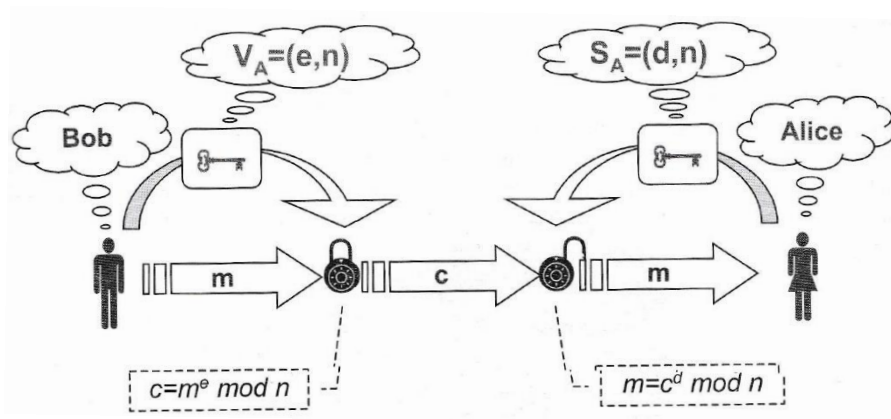
Asymetrická kryptografie je založená na principu veřejného a privátního klíče, kdy každý z nich má pouze jeden účel. Privátní klíč slouží k dešifrování zprávy a veřejný klíč slouží zašifrování zprávy. Není zapotřebí sdílet společný klíč, a tedy výrazně snižujeme možnost napadení chráněných dat. Podmínkou pro užití této metody je nemožnost spočítat hodnotu dešifrovacího klíče ze znalosti šifrovacího klíče. To prakticky znamená jeho dostatečnou délku a nahodilost. Tato metoda je však příliš výpočetně náročná pro použití na celém obsahu přenášené informace. [1]



Obrázek 4: Asymetrické šifrování[6]

### 1.3.1 RSA

RSA je ve své podstatě pouze úpravou protokolu Diffie-Hellman pro účely asymetrické komunikace. Tedy místo jednoho symetrického klíče, kdy je potřeba sdílet veškeré údaje potřebné k vytvoření, použijeme klíče veřejného a privátního. Řešený je především model distribuce. Pokud pomoci veřejného klíče zašifruji zprávu, lze ji dešifrovat pouze pomoci privátního klíče příjemce. Přitom vycházíme ze skutečnosti nemožnosti určit výsledek rozkladu dvou velkých prvočísel, faktorizace.[2]



Obrázek 5: Metoda RSA[2]

Z matematického hlediska se používá jednoduchého součinu dvou hodnot a použití funkce modulo.

$$\text{šifrování:} \quad C = M^E \cdot (\bmod N) \quad (1)$$

$$\text{dešifrování:} \quad M = C^D \cdot (\bmod N) \quad (2)$$

kde: C      zašifrovaný text  
M      je nezašifrovaný text  
E      šifrovací klíč, veřejný  
D      dešifrovací klíč, privátní  
N      součin náhodných prvočísel, veřejný  
Mod   funkce modulo

#### 1.3.1.1 ZRTP

Je protokol na principu RSA, který byl vytvořen Philem Zimmermannem. Jeho cílem bylo zjednodušit a zrychlit celou proceduru tak, aby byla použitelná pro běžné uživatele, to především kvůli výpočetní náročnosti. Výsledkem je koncept kombinace symetrické kryptografie pro zašifrování zprávy, kvůli rychlosti převodu, a asymetrické kryptografie, která je použita na šifrování symetrického klíče. ZRTP byl primárně vyvinut pro účely softwaru PGP. Na podobném principu dnes pracují funkce digitálního podpisu zprávy.[2]





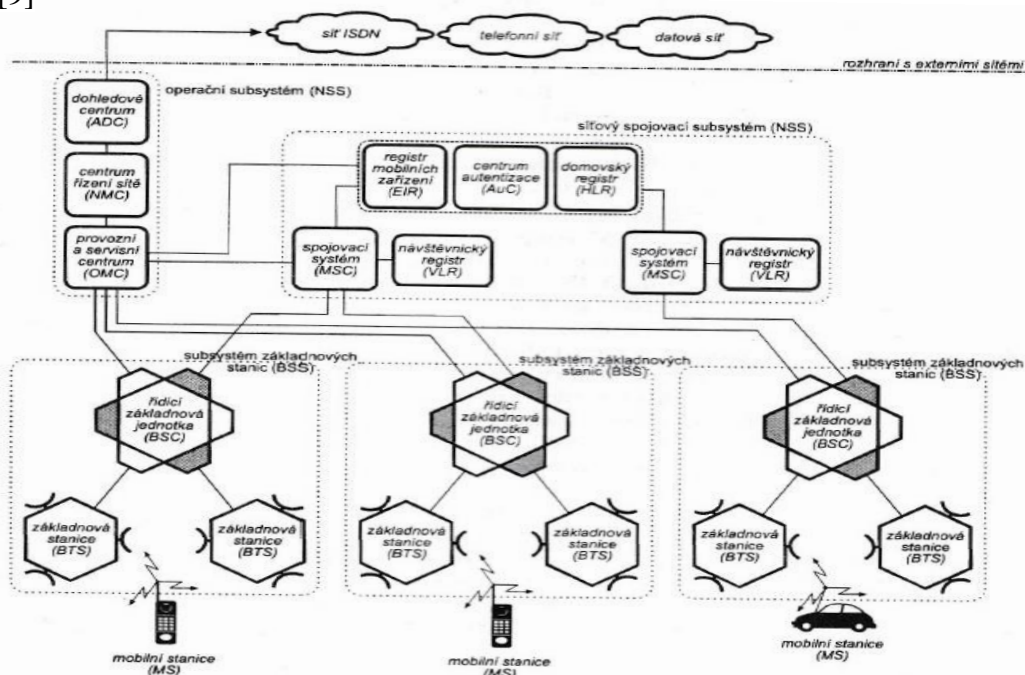
## 2.2 Mobilní telekomunikační technologie

### 2.2.1 GSM síť

GSM sítě jsou založeny na principu retranslačních buněk, které odkazují na infrastrukturu poskytovatele. Tato infrastruktura se skládá z páteřní sítě, síťového spojovacího subsystému (NSS), ta zahrnuje registry, spojovací systém a autorizační centrum. Dále je provoz přesměrován do konkrétní řídicí základnové jednotky (BSC), která obsahuje několik buněk koncových retranslačních jednotek, základnových stanic (BTS). [9],[10]

NSS slouží především jako telefonní ústředna s přepojováním a zprostředkovatel služeb, odtud PSTN (Public Switched Telephone Network), která obsahuje identifikační databáze účastníku a přehled subsystému. BSS přiděluje komunikační kanály a registruje účastníky na NSS. GSM pásmo se rozkládá pomocí kombinace frekvenčního (na 124 pásem po 200 kHz) a časového (na 8 kanálů) multiplexu. Jedna BSS tedy dokáže vytvořit pouze 992 telefonních okruhů. BTS pouze přenáší spojení. Pro identifikaci účastníků slouží SIM (modul identifikace účastníka) karta.[9]

Mobilní stanice účastníka se skládá ze čtyř hlavních částí, vysílače a přijímače, mikroprocesoru a SIM. A/D převodník použitý pro PCM modulaci používá frekvenci 8000 Hz a vzorek o velikosti 13 bitů při lineárním kvantování. Výsledná rychlost přenosového signálu, v této podobě, činí 104 kbit/s, ale pomocí kódování je uměle podhodnocena na výsledných 13 kbit/s. [9]



Obrázek 7:schéma GSM[9]

### 2.2.2 UTRA

UMTS Terrestrial Radio Access představuje doplněk do stávající sítě GSM, který zprostředkovává přístup do páteřní sítě skrze rozhraní rozprostřeného signálu. Dochází k záměnám funkčnosti původní struktury na spojovacích subsystémech. Především je pozměněna funkce síťového managementu mezi jednotlivými prvky. [11]

UTRA tvoří základní uživatelský terminál pro přístup do sítí UMTS. Skládá se ze subsystémů rádiových sítí, základnových stanic a páteřní sítě. Komunikace bez napojení na páteřní síť je zachována, ale pouze v dosahu do sousedního vysílače. [11]

### 2.2.3 HSDPA

K páté aktualizaci standardu UMTS došlo ke změnám, které vedly ke zvýšení Downlinkové rychlosti na 14,4 Mb/s. Vysokorychlostní downlink na paketovém přístupu je dostupný ve verzích pro frekvenční (FDD) i časový (TDD) duplex. Na jeden mobilní terminál došlo kna-  
výšení rychlosti na 1,8 Mb/s. [12]

Inovativně byly pozměněny některé přepojované služby v síťové architektuře, především pak na automatickém požadavku pro opakovaný přenos. Některé změny byly provedeny i přímo na rádiové části sítě kde se změnila značná část hardwaru na základnových stanicích. Dochází k odstranění zpoždění a rozptýlení signálu. [12]

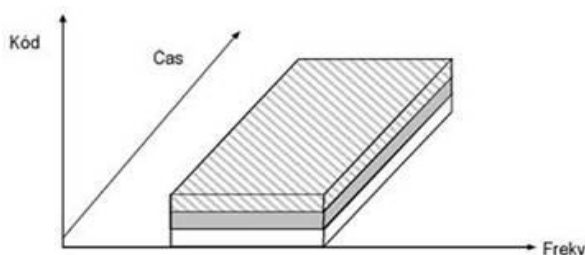
Většina informací se již přímo dekoduje na vnitřní struktuře UTRA a tedy nedochází k přetěžování na fyzické vrstvě koncových vysílačů. Zároveň se tak zkrátila přístupová trasa. Je používána adaptivní modulace i kódování, více kódové operace, rychlé plánování a opakované odesílání na fyzické vrstvě. [12]

### 2.2.4 HSUPA

Jedná se o nástavbu do protokolů UMTS, která náleží do rodiny vysokorychlostní přenosu paketů. Teoretická rychlost uploadu zde byla navýšena na teoretických 5,76 Mbit/s při maximálním vytížení jednoho kanálu. HSUPA není technicky správným pojmenováním pro univerzální technologii, protože byla patentována společností NOKIA, a proto je možné se v literatuře též setkat s pojmem EUL (Extended UpLink). Technickou realizací této metody pak značíme zejména zvýšení kapacity a propustnosti na kanálu při snížení délky odezvy. Tímto krokem je dosahováno výkonnostního nárůstu na přenosových kanálech. [12]

### 2.2.5 CDMA

Pro technologii CDMA je specifické, že multiplexu je dosahováno pomocí kódového dělení na přiděleném spektru ve stejný okamžik pro všechny uživatele. Rozlišování uživatelů je realizováno pomocí identifikačních binárních kódů v rozprostřeném spektru. Násobením binárního kódu z původních dat pak dochází ke vzniku širokopásmového signálu. Informace se rozprostřou do šířky uvolněného spektra. [12]



Obrázek 8: Podstata CDMA[11]

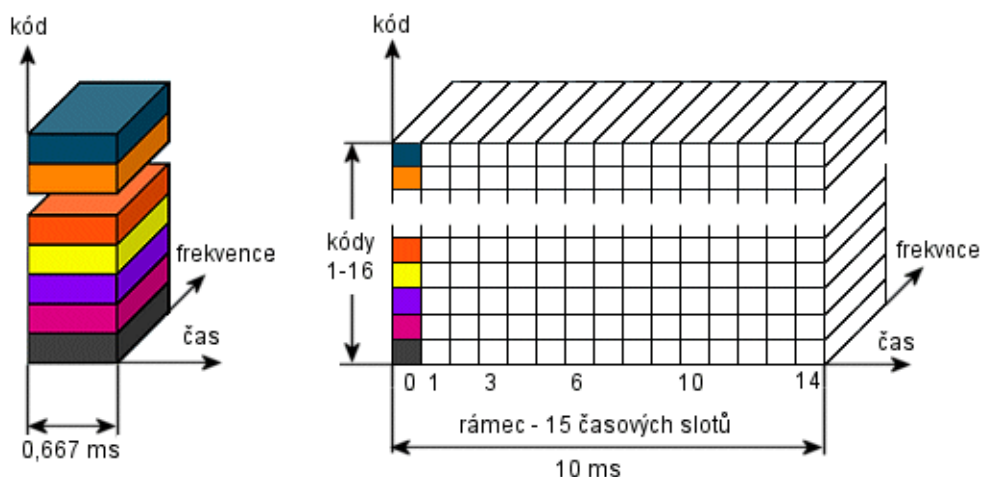
### 2.2.6 W-CDMA

Wideband Code Division Multiple Access je širokopásmovým přístupem s kódovým dělením. Tato technologie vznikla právě pro požadavky sítě UMTS. Jde o modulační technologii založenou na principu rozprostřeného spektra kdy je využíváno širší pásmo než je definováno přenosovou rychlostí. Na jednom kanálu je možné, vlivem kódování, přenášet více signálů ve stejný časový interval při stejné frekvenční modulaci. Pro zajištění obousměrné komunikace se používá frekvenční (FDD) nebo časové (TDD) oddělení informací. [12]

Pro tuto technologii se používá především pásma 1,9 a 2,2 GHz, protože UMTS je zpětně kompatibilní ke službám GSM. Šířka kanálu je 5 MHz. [12]

### 2.2.7 TDD

TDD využívá časového dělení pro přenos více signálů na jednom kanálu. Informace jsou rozděleny do rámců o délce 10 ms. V jednom rámci se pak skrývá 15 intervalů po 2/3 ms pro přidělení jednotlivým uživatelům. Mezi jednotlivými rámci jsou pak synchronizační signály. TDD je full-duplex metoda. Tedy v časovém intervalu na jednom kanálu můžeme do rámce umístit sestupné i vzestupné trasy. Dělení intervalů do směrů pak určuje požadavek ze synchronizačního signálu. [12]

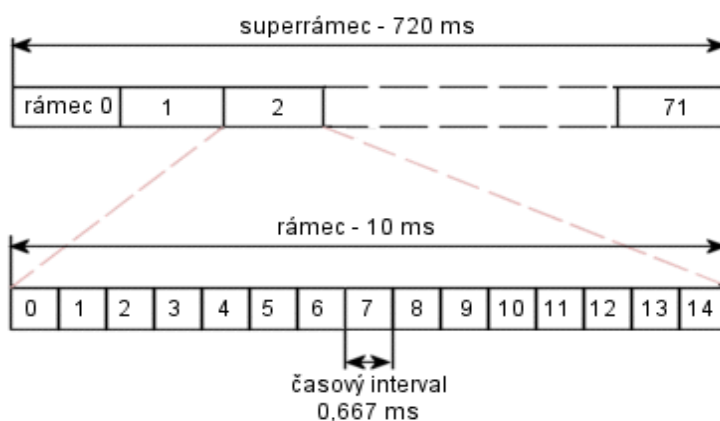


Obrázek 9: Struktura rámce TDD[11]

### 2.2.8 FDD

FDD poskytuje vysokou míru mobility, a proto se používá pro pokrytí větších oblastí, jako jsou městské nebo venkovské zástavby. Přenosová rychlost se odvíjí na základě potřeb uživatele a může dosahovat až rychlosti 384 kbit/s. Pro většinu spektra v síti UMTS se proto využívá právě technologie FDD. [12]

Informace se podobně jako u TDD ukládají do rámců o velikosti 10 ms a 15 intervalů o délce 2/3 ms. Tyto rámce se pak poskládají do superrámce o délce 720 ms, tedy 72 běžných rámců. Po jednom kanále pak může běžet ještě několik signálů o různých frekvencích. Stejně jako TDD i FDD funguje jako full-duplex komunikace. Tedy veškerá data mohou v různých potřebách na jednom rámci téct po vzestupné i sestupné trase. [12]

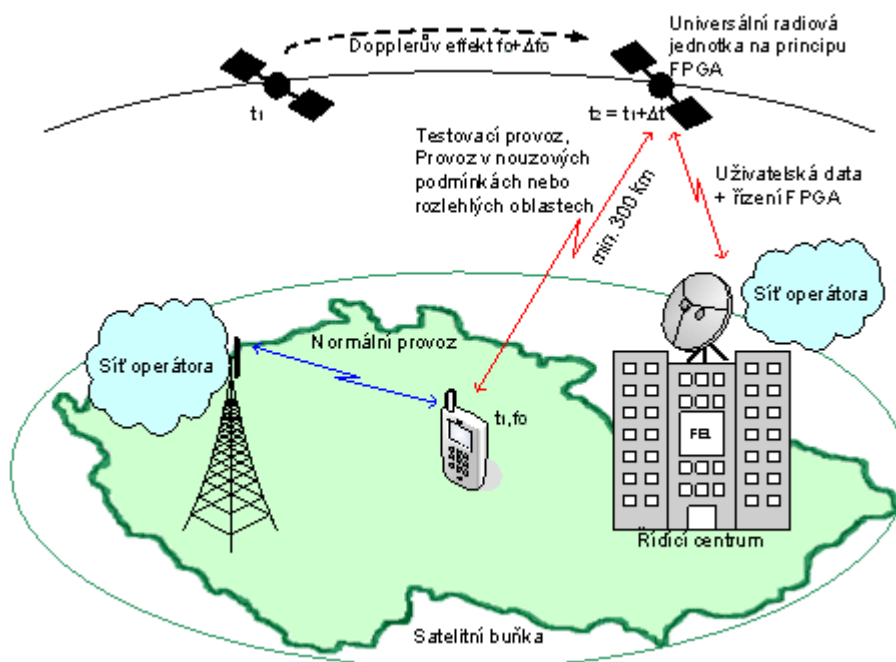


Obrázek 10: Struktura rámce FDD[11]

## 2.3 Satelitní telekomunikace

Samotný satelitní přenos má velice podobnou strukturu přenosu. Je používán přenos pomocí časového multiplexu v kombinaci s kanálovým multiplexem. Hlavní rozdíl je ve frekvenčních pásmech, která jsou v jednotkách až desítkách jednotek GHz. Proto lze i laicky, říct že nosné vlny mají podstatně vyšší energie. To má svůj účel především s ohledem na vzdálenosti, ve kterých komunikace probíhá.[13], [14]

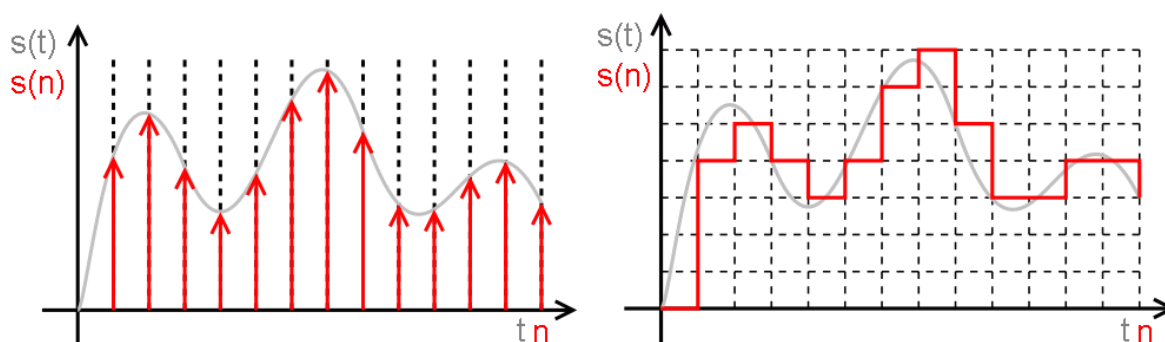
Pro civilní sféru komunikace je definováno frekvenční pásmo v rozsahu 1-2 GHz, v sektoru armádní (respektive státní) komunikace pak 8-12,5 GHz. Civilní pásmo je uzpůsobeno pro komunikaci s přenosovou rychlostí do 4 Mbit/s. Pro využití vyšší přenosové rychlosti se využívá multimediální pásmo pro zprostředkovatele internetových služeb (dále jen ISP), pásmo 11-18 GHz, ve kterém lze získat přenosovou rychlost až 60 Mbit/s. Největší telekomunikační společnost v této oblasti, Inmarsat, vynesla na oběžnou dráhu 9 komunikačních satelitu na vysoké orbitě (36000 km). Nízká orbita má nevýhodu nesynchronního pohybu s otáčením Země (původní koncept Iridium). Vysoká orbita oproti tomu má vzhledem k vzdálenost podstatně vyšší energetickou náročnost na přenos, vyšší latenci a s tím související nižší přenosovou rychlost.[14], [15]



Obrázek 11: Satelitní komunikace SPEROS[13]

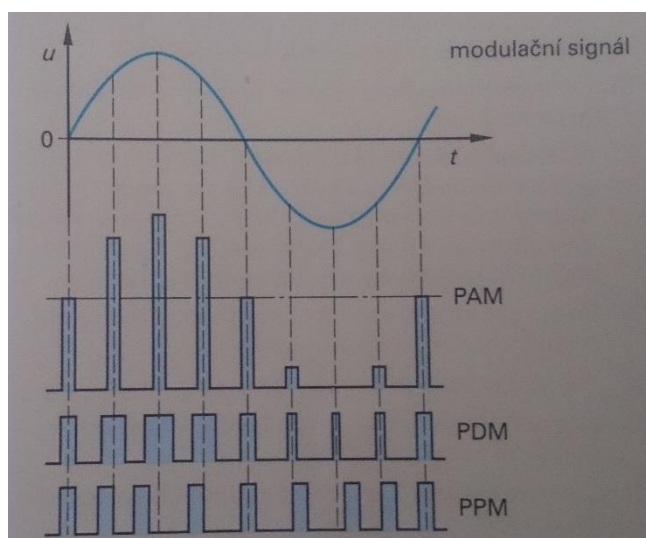
## 2.4 Převod zvukového signálu

Zvuk je analogová veličina, kterou pro potřeby přenosu musíme upravit do digitální podoby. Nejprve je nutné zvukový výstup vzorkovat, tedy definovat časové úseky záznamu a v těchto intervalech stanovit příslušnou hodnotu úrovně. Následně dochází ke kvantování. Kvantování je proces striktního začlenění hodnoty do kvantizační úrovně, tedy zaokrouhlení hodnoty do předdefinované hladiny. Princip je založen na rozdělení prostoru mezi kvantizačními hladinami na polovinu a hodnoty se následovně podle této poloviny přiřazují směrem nejbližší hladiny. Tímto způsobem jsou vytvořeny vzorky původního signálu, které musí být na straně přijímače zrekonstruovány. Výslednou zprávu je ještě nutno vhodným způsobem kódovat.[9],[10]



Obrázek 12: Převod signálu[16]

Pro přenos vytvořené zprávy se používá pulsně kódové modulace (PCM). Pulzní signál je nespojitá veličina. Signál je modulován amplitudou, délkou nebo posunem intervalu vysílání.[9],[10]



Obrázek 13: PCM typy[10]



Pro zkrácení délky kódového slova se používá vynechávání tichých míst hovoru, za předpokladu odrušení okolního šumu. Při využití sítě GSM jsme schopni ve frekvenčním pásmu přenášet zvukový záznam o rychlosti 13 kbit/s a to při pravidelném vybudení kanálu a využití dlouhé predikce k zajištění korektnosti přenosu. Při využití modernějších sítí vyšších generací, lze využít převodu hlasové zprávy do věrnější podoby a to sice až na úroveň studiové kvality, 24 bitů, zde je možné pomocí vhodné metody odrušit okolní šum diferenciální metodou. Problém je však náročnost na rychlost přenosu, která musí být nejméně 1152 kbit/s a kompatibilita zařízení, tím je především myšleno, že oba komunikační přístroje jsou uzpůsobeny na hlasový hovor v datových sítích a také předpoklad dostupnosti takové sítě. V opačném případě dochází k výpadkům nebo zkreslení.[9]

## 2.5 Kódování

Tabulka 1: Rozdělení kódování [11]

Typ kódu	Uplink	Downlink
Skramblovací	oddělení uživatelů	oddělení buněk
Kanálový	oddělení datových a kontrolních kanálů u jednoho terminálu	oddělení uživatelů v rámci jedné buňky
Rozprostírací	kanálové kódy x skramblovací kódy	kanálové kódy x skramblovací kódy

### 2.5.1 Skramblovací kódy

Jsou složeny z 512 kódových sad, proto nelze vždy využít veškerých kódů, kterých je dohromady  $262143=2^{18}-1$ . Každá sada se skládá primárního kódu a 15 sekundárních. Na každou buňku je vyhrazen jeden primární kód tedy jedna sada, jím určená. Skramblování je založeno na Reed-Solomonových kódech. [11]

### 2.5.2 Kanálové kódy

Jedná se o ortogonální kódy, které slouží k oddělení kanálů. Stejně jako u skramblovacích kódů, každá buňka obsahuje celou sadu kanálových kódů. Nejčastěji používanými kódy jsou Walsh-Hadamardovy kódy. [11]

### 2.5.3 Rozprostírací kódy

Při využití CDMA je předpoklad že uživatelé vysílají signály ve stejnou dobu na stejné frekvenci. Rozprostírací kódy pak slouží právě k oddělení signálů od jednotlivých uživatelů. Kód je unikátní a přiděluje ho síť před zahájením vlastní komunikace. [11]

### 2.5.4 Symboly a čipy

Při rozprostírání spektra dochází k vynásobení původního signálu, v základním pásmu, signálem o vyšší přenosové rychlosti. Jako symbolovou rychlost pak označujeme přenos signálu za pomoci konvolučního kódování, kdy jeden bit digitálního signálu v základním pásmu označujeme jako symbol. [11]

Čip je elementem rozprostírací sekvence. Do jednoho symbolu lze umístit čtyři čipy. Rychlost přenosu takového signálu po datovém toku pak označujeme jako čipovou rychlost. Pro síť využívající W-CDMA se používá čipová rychlost 3,84 Mcps/s. [11]

### 3 ŠIFROVACÍ TECHNOLOGIE PRO MOBILNÍ ZAŘÍZENÍ

#### 3.1 Zabezpečená infrastruktura

Požívá zabezpečených šifrovacích center umístěných do sítě Internet a pomocí datových hovorů pomocí aplikace v koncovém zařízení přesměruje hovor. Datové centrum je vybaveno speciální šifrovací technikou, která zajišťuje ochranu dat klienta. Pokud tedy někdo chce uskutečnit hovor, pak použije aplikace, která pomocí asymetrického klíče společnosti zašifruje hovor a informace je odeslána na server. Zde se informace dešifruje pomocí klíče společnosti, a znovu zašifruje klíčem klienta, kterému má být zpráva doručena. [17]

Tato metoda se používá jako služba, která je podstatně levnější než zřízení vlastní infrastruktury a současně při velkém množství uživatelů. Problematická je však otázka odezvy. Už z principu lze pochopit, že rychlost přenosu závisí na přenosové lince a celkovém vytížení střediska. Výhodou je využití různých přenosových technologií. [18]



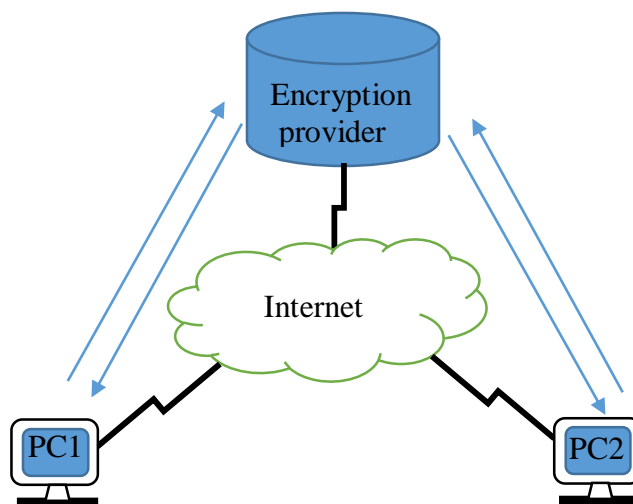
Obrázek 14: Zabezpečená infrastruktura[17]

#### 3.2 Šifrovací aplikace

Nejčastěji se používá aplikací end-to-end encryption, tedy šifrování probíhá na straně koncových uživatelů. Tato metoda je náročná na výpočetní schopnosti zařízení. Z tohoto důvodu ji lze uplatnit až u vyspělejších zařízení. [19]

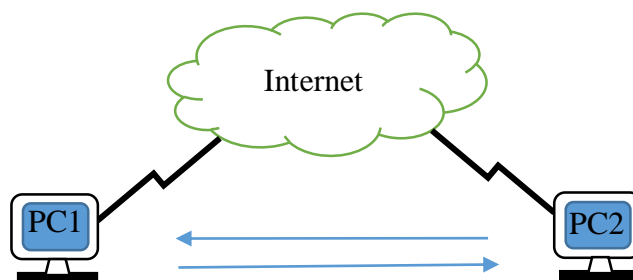
##### 3.2.1 Princip End-to-End v porovnání s Point-to-Point

End-to-End se zaměřuje na zpracování informací na straně uživatele a následný přenos po veřejné ne uzavřené síti za pomoci vytvoření přenosového kanálu mezi několika body. Vytváří tedy přestupné body na trase, kterou v realitě tvoří servery zprostředkovatele, jak lze znázornit na schématu.



Obrázek 15: End-to-End spojení přes server

Point-to-Point technologie je oproti tomu založena na přímém spojení pomocí protokolu PPTP (Point-to-Point Tunneling Protocol), vytvoření přímého komunikačního kanálu mezi dvěma uživateli.



Obrázek 16: Point-to-Point připojení

V konečném porovnání si lze povšimnout jisté podobnosti a to právě proto, že technologie End-to-End vychází právě z technologie Point-to-Point a to z hlediska zajištění bezpečného přenosového kanálu. Z hlediska zajištění velkého objemu dat, ale také zabezpečení a účtování poplatků za služby, do struktury vstupují právě datová centra. V některých open source aplikacích však vzniká čisté spojení Point-to-Point. To má velký dopad především na odezvu z přenosové sítě.

### 3.2.2 Datový přenos v moderních sítích

Pro každou komunikaci je vygenerován unikátní klíč, který je pomocí zprávy předán uživateli na druhé straně linky. Ten zprávu přijme a rozšifruje si klíč. Poté pošle ověřovací klíč zpět. Pokud vše proběhne v pořádku je zahájena komunikace pomocí právě daného šifrovaného klíče. Po ukončení komunikace je klíč smazán. [20]

### 3.3 VOIP telefonie

U VOIP telefonie je možné použít vlastní infrastruktury i již zmiňovaného datového centra. Vycházíme při tom ze znalosti koncových uživatelů, a jejich přesného umístění. Pro vytvoření vlastní infrastruktury existují šifrovací moduly, které používáme jako generátor klíče, a který obsahuje šifrovací algoritmus. Stejně tak lze aplikovat síťové prvky a to v případě pokud nechceme zajistit bezpečnost koncového prvku, který je například uvnitř zabezpečené oblasti, ale pouze celistvé struktury našeho objektu. [18]



Obrázek 17: Šifrovací síťové prvky[18]

### 3.4 Speciální telefony

Za speciální šifrovací telefony můžeme považovat přístroje, které obsahují šifrovací moduly nebo pouze speciální operační systém. Zpravidla se tyto produkty prodávají již přednastavené se službou provozovatele zabezpečeného datového centra. Pro účely státní bezpečnosti se pak používají tyto telefony připojené do sítě zřizovaných zvláště pro účely zabezpečené komunikace. Právě státní složky tuto metodu používají nejčastěji a to právě kvůli finanční náročnosti. Výhodou je však nesrovnatelné zabezpečení a rychlost přenosu po vyhrazených linkách. [18]



Obrázek 18: Šifrovaný telefon[18]

## **II. PRAKTICKÁ ČÁST**

## 4 FUNKČNÍ APLIKACE NA TRHU

Výběr aplikací je přizpůsobený modernímu trendu vývoje v oblasti komerčních telekomunikačních sítí, rozvoji zabezpečení hovoru proti odposlechu. Z tohoto důvodu lze definovat rozmanitost používaných zařízení, ale i konkrétní metodu použité kryptografie. Cílovou skupinou tedy bude komerční sféra, která v rámci úspor hledá řešení v podobě End-to-End aplikací. Z tohoto důvodu jsem způsob svého hodnocení zaměřil na metodiku odposlechu zasílání paketu skrze přístupové body. Prokazatelným údajem zde bude časová odezva na straně sprostředkovatele tedy vyvíjející společnosti. Ve skutečnosti se však jedná o jedinou reálně ověřitelnou a objektivní možnost jak tyto prostředky ohodnotit.

Další metodikou, na kterou je možné se zaměřit a to však pouze subjektivně je komfort užívání a složitost ovládání. Těžce ověřitelnou a značně zkreslenou metodou je poté analýza rychlosti zpracování samotného datového paketu v přístroji. Tato metoda je však zkreslená o funkce, které přístroj využívá při běžném provozu, nejedná se však o zanedbatelnou hodnotu. Rozsah operačního výkonu je přímo závislý nejen na výrobcí daného přístroje, zejména z hlediska podpůrných funkcí, ale i na samotném uživateli, který volí různé varianty služeb v konkrétním případě. Tato skutečnost má přímý dopad na rychlost přenosu i komfort užívání.

### 4.1 Analyzátor paketů (sniffer)

Sniffing, neboli metoda zachytávání paketu je především jedna z metod, která slouží k odhadování hesel při útoku hackeru. Základem je připojení na přístupový bod, který umožňuje sledování činnosti. To znamená, že je nezabezpečený proti přístupu třetích osob. V případě, že by se nejednalo o šifrovanou komunikaci, snadno by jsme mohli vyčíst přístupové údaje jednotlivých zařízení do systému zprostředkovatele. Toto by nemělo být z popisu společnosti, které šifrované telekomunikace provozují, možné. Dalším důležitým poznatkem, který nás bud zajímat, je časový údaj spjatý se záznamem. Z tohoto údaje budeme vycházet při srovnávání, protože pokud tyto pakety označíme jak na straně odesílatele, tak na straně příjemce, dostane odezvu systému. [1]

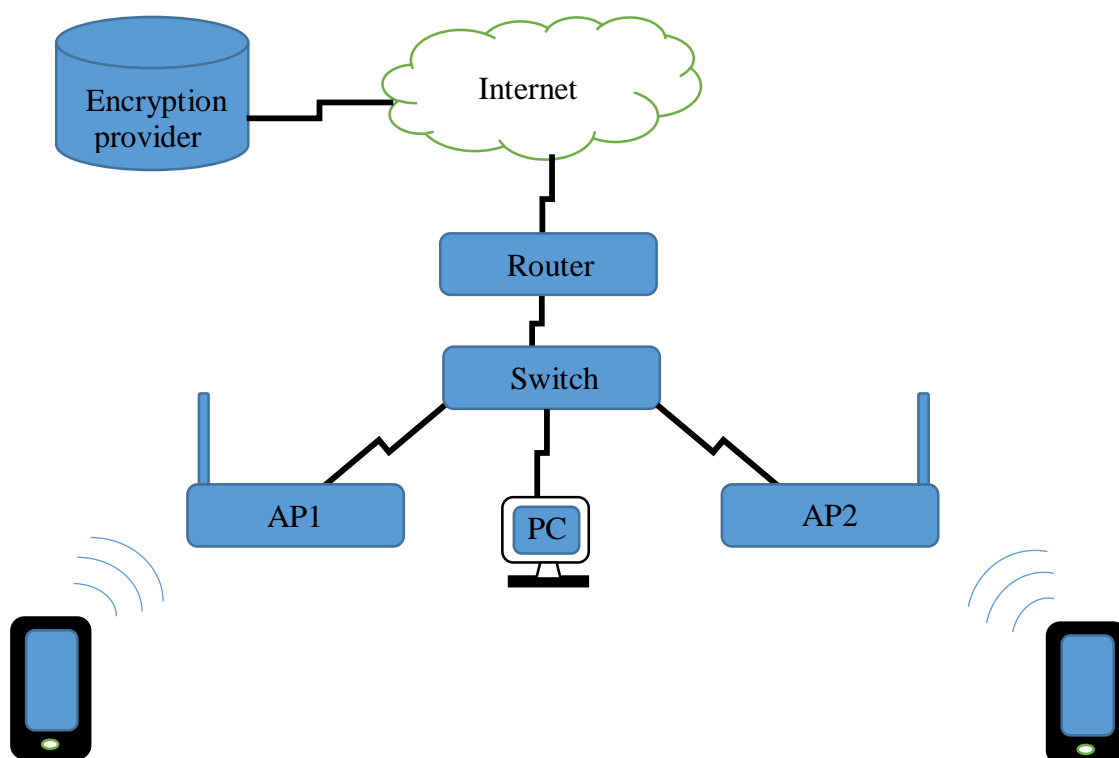


## 4.2 Měřicí soustava

Hodnotící soustava je uzpůsobena tak aby vytvářela dvě samostatné sítě z důvodu jednoznačného oddělení uživatelů. Vzhledem ke zvolené metodě lze zanedbat použité koncové přístroje, jedinou podmínkou zůstává použití telefonu, který obsahuje alespoň procesor se dvěma jádry a to z důvodu kompatibility zařízení.

Pro přístup do sítě Internet je využit jeden router značky Asus (technická dokumentace v Příloze P1), který je spojen gigabitovou linkou ke zprostředkovateli. Dále je pro odrušení vlivu zabezpečení routeru použit pěti-portový switch značky TP-link (technická dokumentace v příloze P2). Z tohoto bodu jsou vyvedeny dvě kroucené dvoulinky s přenosem 100 Mb/s na dvě stejná zařízení výrobce TP-link (technická dokumentace v Příloze P3) s bezdrátovým přenosem a nastavených do režimu přístupového bodu (AP). Tyto zařízení vytvářejí dvě oddělené sítě.

Pro zachytávání paketů jsem zvolil software WireShark, který je spuštěn na dvou počítačích připojených do stejné sítě jako koncová zařízení, a to pomocí metalického vedení kroucené dvoulinky s rychlostí přenosu 100 Mb/s. Toto zapojení může způsobovat krátkou prodlevu na samotném zachytu. V konkrétním schématu však neovlivní samotný výsledek měření vzhledem ke stejnému zapojení a zaměření na příchozí a odchozí zprávy z pohledu vnější infrastruktury.



Obrázek 19: Schéma zapojení

Při takovémto zapojení je zjevné, že i za použití různých variant operačních systémů nedáme moci sledovat celý provoz sítě. Toho bychom mohli docílit pomocí zrcadlení portů a tedy přenášení kopii souboru do našeho testovacího počítače. V této možnosti však riskujeme ztrátu dat nebo identifikačních údajů. Jinou variantou, kterou jsem nakonec uplatnil, je metoda přesměrování provozu pomocí ARP poisoning. ARP poisoning je metoda kdy uměle docílíme útoku man-in-the-middle. Tedy virtuálně vytvoříme prostředníka připojení mezi komunikačními kanály pozorovaných linek. Do hlavního operačního systému jsem nainstaloval virtuální počítač s operačním systémem Windows, který obsahuje software Caine & Abel. Tento software bude přesměrovávat veškerou komunikaci přes testovací počítač. Navíc je schopný analyzovat příchozí certifikáty a hodnotit zprostředkované služby. Nelze z něj však hodnotit nezabezpečené protokoly přenosových kanálů.

### 4.3 Hodnocené aplikace

Jako vzorové příklady dostupných možností jsem zvolil tři zprostředkovatele. Z toho u dvou případů se jedná o české společnosti, a to zejména z důvodů dosažitelnosti datových center, tedy přizpůsobení místnímu trhu z hlediska odezvy. Tyto aplikace budu hodnotit v časově omezené zkušební verzi. Poslední hodnocenou aplikaci je open source program, u kterého je použit protokol ZRTP tvůrce programu PGP a funguje na principu připojení VoIP. Tedy odezvy ve vlastní síti by měli být nezávisle na dosažitelnosti datového centra příslušného zprostředkovatele.

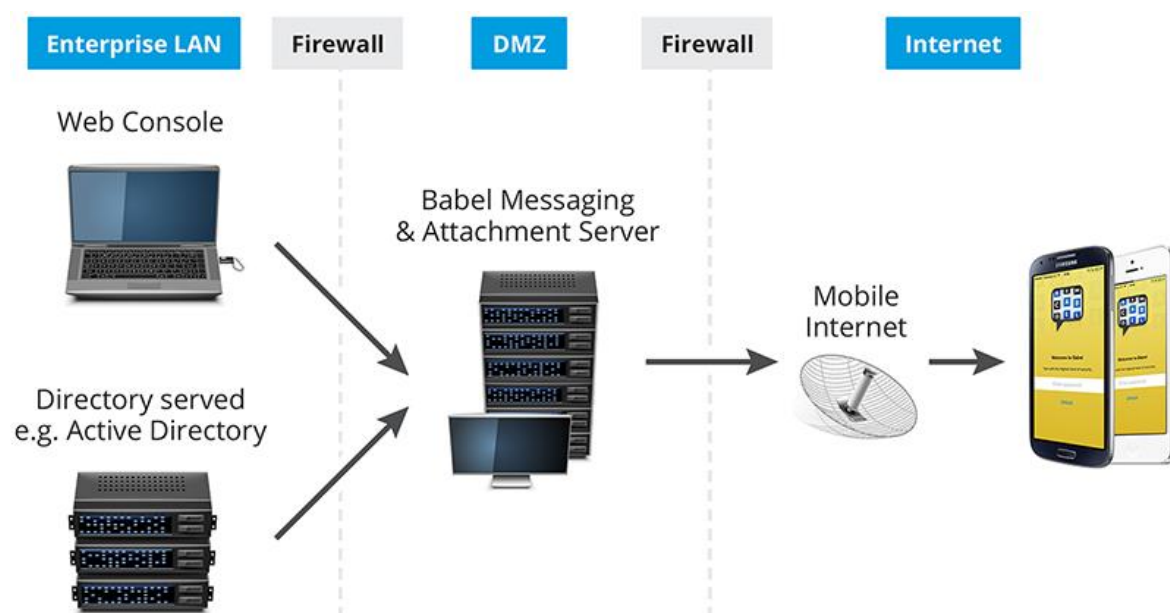
#### 4.3.1 BABEL

Používá kombinaci symetrické a asymetrické kryptografie. Pro komunikaci je vygenerován klíč pomocí algoritmu Diffie-Hellman. Konečná šifrování probíhá za pomocí algoritmu AES nebo Twofish. Pro ověření uživatelů pak slouží certifikát standardu X509v3, který používá i americká armáda. Pro textové zprávy je použit algoritmus RSA. Jedná se o End-To-End aplikaci. Pro inicializaci hovoru je používán server společnosti. Společnost v současné době zrušila poskytování hlasových služeb pomocí VoIP telefonie a zaměřila se výhradně na poskytování přenosu zabezpečených textových zpráv[21]



Obrázek 20: BABEL[21]

#### 4.3.1.1 Hodnocení metodiky



Obrázek 21: Schéma připojení do infrastruktury BABEL[21]

Podle schématu uváděného výrobcem lze odvodit oddělení inicializačního serveru a serveru pro přepojení od databázové struktury. Navíc jsou jednotlivé segmenty v úrovních zabezpečeny pomocí firewallů. Toto rozdělení umožňuje samostatnou činnost administrace uživatelské skupiny a funkčních procesů.

Vzhledem k nutnosti registrace zkušební verze na stránkách provozovatele nebylo možné měření uskutečnit. Provozovatel uvádí 30 denní zkušební licenci pro pět uživatelů na vyhrazeném kanálu po vyplnění registračního formuláře. Formulář obsahuje tři pole pro každého uživatele:

- Jméno
- Kontaktní e-mail
- Telefonní číslo

Po odeslání je obratem zaslán potvrzující e-mail zakládajícímu (prvnímu v seznamu) uživateli. Následně je uživatel na stránkách upozorněn o prodlevě v délce jednoho dne, která slouží ke zřízení komunikačního rozhraní pro danou skupinu.

Při prvním pokusu jsem skutečně obdržel informační e-mail od obchodního zástupce, který mě však informoval pouze o poděkování za projevenou důvěru a neobsazenosti pole telefonních čísel zkušebních účastníků. Telefonní číslo bylo po vzoru stránek vyplněno s českou předvolbou a bez mezer. Při opětovném pokusu o vytvoření (bez české předvolby) ani při kontaktování obchodního zástupce již nedošlo k žádné odezvě.

Z těchto důvodů již nebylo možné ověřit korektnost uváděných algoritmů systému ani formu komunikace.

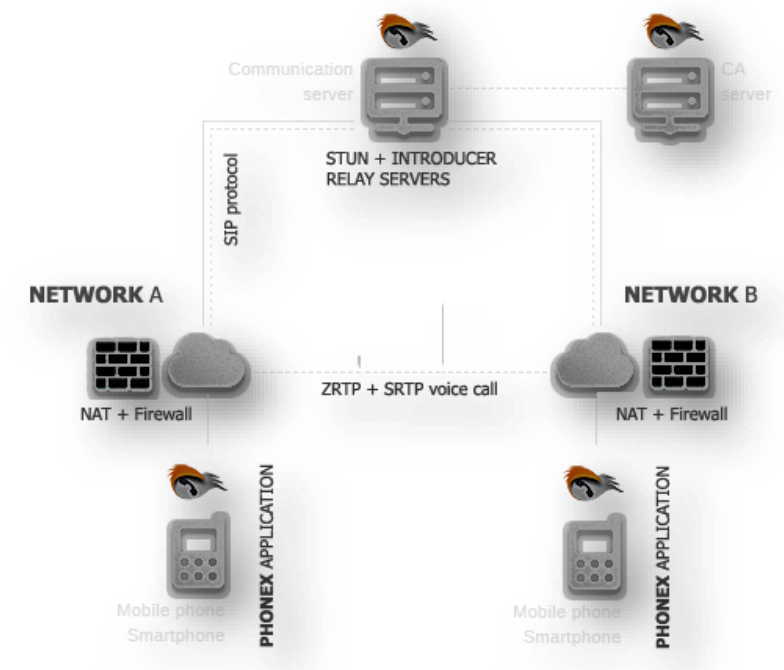
#### 4.3.2 PhoneX

Používá kombinaci symetrické a asymetrické kryptografie. Pro komunikaci je vygenerován unikátní klíč. Konečná šifrování probíhá za pomoci algoritmu AES nebo Twofish. Pro ověření uživatelů pak slouží certifikát standardu X509v3. Pro textové zprávy je použita metoda digitálního podpisu algoritmus AES. Jedná se o End-To-End aplikaci. Pro inicializaci hovoru je používán server společnosti, který lze použít pro ukládání citlivých dat a zálohování. [22]



Obrázek 22: PhoneX[22]

#### 4.3.2.1 Hodnocení metodiky



Obrázek 23: Schéma připojení do infrastruktury PhoneX[22]

Podle schématu výrobce by mělo docházet k přímému přepojení účastníků hlasového přenosu. Ve skutečnosti je však celý proces začleněný do vnitřní infrastruktury zprostředkovatele. Tedy hlasové i textové přenosy prochází skrze komunikační server společnosti, který služby přepojuje na virtuální rozhraní uvnitř serveru.

V tomto případě lze aplikaci stáhnout do telefonu z některých z dostupných serverů výrobců mobilních operačních systémů (například Google Play) a to bez poplatku a dalších licenčních požadavků. Po stažení je uživatel vyzván k založení účtu a to sice zadáním uživatelského jména a hesla. Následuje výzva k předložení licence, kterou uživatel může zamítnout. V takovém případě může uživatel využít sedmi denní zkušební verzi. Vše je velice rychlé a bezproblémové, uživatel je okamžitě dostupný v síti zprostředkovatele.

Pro korektní funkci je zapotřebí použít grafické rozhraní aplikace registrované do sítě zprostředkovatele. To obsahuje tři základní záložky:

- Seznam registrovaných účastníků
- Textové zprávy
- Upozornění (systémová upozornění, příchozí zprávy)

Tyto tři záložky jsou doplněny o menu, indikaci stavu přihlášení, volbu přidání uživatele a vyhledávání uživatelů. Synchronizace certifikátů a ověření šifrovacích klíčů probíhá při přihlášení do systému nebo při prvotním zadání nového účastníka.

Komunikace je plně závislá na registraci účastníku do sítě. Nedostupnost uživatele je sice indikována, ale neplatí s garancí aktuálnosti, pouze zrcadlí stav po přihlášení. Uživatel může požadovaného účastníka zavolat, v takovém případě je upozorněn obsazovacím tónem a textem upozorňujícím na aktuální stav. V případě chybné komunikace se serverem můžou dojít k cyklické chybě přihlášení, která generuje chybný požadavek na dostupnost a synchronizaci. V takovém případě je nutné celou aplikaci restartovat.

Údaje o uživateli, ve formě přihlašovaného účtu, jsou zasílány na server v nezašifrované podobě. Při přihlašovacím procesu je možné i zachytit údaje o uživateli v telefonním seznamu aplikace a to včetně uživatelského záznamu v databázi.

```
..Phoenix ltd1.0...U...PhoenixCA1.0...U...ca.phoenix.info!0...*.H..
....admin@phoenix.info.^0\1.0...U...CY1.0...U...Larnaca1.0...U.
..Phoenix ltd1.0...U...Server031.0...U...localhost.}0
{1.0...U...GI1.0...U...Gibraltar1.0
..U.
..Phonex1.0
..U...Server1.0...U...phone-x.net1 0...*.H..
....admin@phone-x.net.....0...0.....0
..*.H..
....0{1.0...U...GI1.0...U...Gibraltar1.0
..U.
..Phonex1.0
..U...Server1.0...U...phone-x.net1 0...*.H..
....admin@phone-x.net0..
150516144639Z.
170515144639Z0..1"0 ..*.H..
....lucie_m@phone-x.net1.0...U...lucie_m@phone-x.net1.0
..U...Phonex1.0
..U.
..Phonex1.0...U...Gibraltar1.0...U...Gibraltar1.0...U...GI0.. "0
..*.H..
.....0..
.....;.....>.....r..i..mG.Y9.....E.>Z...4....P..K.N..ON...enw..E..p..P..."...
[..._f...!.ngeK_bskkp0.....^&..0
.....\.....&?...E.O.I17.H.!H..0...5I.....*...j.BS.....6u.k.Y.I0..'
+..j...Y..#.hT...h..L...3..e...
\..)".....>Q.I.9.....}.....~..(".....PON0...U.....0.O...U.....:T.e2@.v9g.m
...S...0...U.#..0.....l.$b...;L.?...F.0
..*.H..
.....A..g2.q?.H...J.a..b..cv.
c8.A.X.X.&z...$vt..w.....*.SO.....Z.&U<e.....<M...8.}
```

Obrázek 24: Obnova telefonního seznamu při přihlášení

192.168.3.109	89.29.122.60	STUN	74 Binding Request
192.168.3.109	89.29.122.60	STUN	74 Binding Request
192.168.3.109	89.29.122.60	STUN	82 Allocate Request UDP
192.168.3.109	89.29.122.60	STUN	74 Binding Request
192.168.3.109	89.29.122.60	STUN	82 Allocate Request UDP
192.168.3.109	89.29.122.60	STUN	74 Binding Request
192.168.3.109	89.29.122.60	STUN	82 Allocate Request UDP
192.168.3.109	89.29.122.60	STUN	82 Allocate Request UDP
192.168.3.109	89.29.122.60	STUN	190 Allocate Request UDP user: lukas_m@phone-x.net realm: phone-x.net with nonce
192.168.3.109	89.29.122.60	STUN	190 Allocate Request UDP user: lukas_m@phone-x.net realm: phone-x.net with nonce
192.168.3.109	89.29.122.60	STUN	190 Allocate Request UDP user: lukas_m@phone-x.net realm: phone-x.net with nonce
192.168.3.109	89.29.122.60	STUN	190 Allocate Request UDP user: lukas_m@phone-x.net realm: phone-x.net with nonce
192.168.3.109	89.29.122.60	STUN	82 Allocate Request UDP
192.168.3.109	89.29.122.60	STUN	82 Allocate Request UDP
192.168.3.109	89.29.122.60	TLSv1	1514 Application Data
192.168.3.109	89.29.122.60	TCP	708 [TCP segment of a reassembled PDU]

Obrázek 25: Přenos požadavku

Síť zasílá pouze hlasovou stopu a vynechává tichá místa z důvodů úspory na datové komunikaci. Tedy vždy komunikuje pouze s aktivně působícím (mluvícím) uživatelem.

89.29.122.60	192.168.3.239	TLSv1	333 Application Data
89.29.122.60	192.168.3.239	TLSv1	333 [TCP Retransmission] Application Data
192.168.3.239	89.29.122.60	TLSv1	155 Application Data
192.168.3.239	89.29.122.60	TLSv1	155 [TCP Retransmission] Application Data
89.29.122.60	192.168.3.239	TLSv1	614 Application Data, Application Data
89.29.122.60	192.168.3.239	TLSv1	614 [TCP Retransmission] Application Data, Application Data
192.168.3.239	89.29.122.60	TCP	66 1577-5222 [ACK] Seq=3187 Ack=4251 Win=78208 Len=0 TSval=1191374 TSecr=2299535741
192.168.3.239	89.29.122.60	TCP	66 [TCP Dup ACK 2529#1] 1577-5222 [ACK] Seq=3187 Ack=4251 Win=78208 Len=0 TSval=1191374 TSecr=2299535741
89.29.122.60	192.168.3.239	TLSv1	163 Application Data
89.29.122.60	192.168.3.239	TLSv1	163 [TCP Retransmission] Application Data
192.168.3.239	89.29.122.60	TCP	66 1577-5222 [ACK] Seq=3187 Ack=4348 Win=78208 Len=0 TSval=1191377 TSecr=2299535807
192.168.3.239	89.29.122.60	TCP	66 [TCP Dup ACK 2533#1] 1577-5222 [ACK] Seq=3187 Ack=4348 Win=78208 Len=0 TSval=1191377 TSecr=2299535807
89.29.122.60	192.168.3.239	TLSv1	908 Application Data, Application Data
89.29.122.60	192.168.3.239	TLSv1	908 [TCP Retransmission] Application Data, Application Data
192.168.3.239	89.29.122.60	TCP	66 1577-5222 [ACK] Seq=3187 Ack=5190 Win=81088 Len=0 TSval=1191380 TSecr=2299535840
192.168.3.239	89.29.122.60	TCP	66 [TCP Dup ACK 2537#1] 1577-5222 [ACK] Seq=3187 Ack=5190 Win=81088 Len=0 TSval=1191380 TSecr=2299535840
192.168.3.239	89.29.122.60	TLSv1	143 Application Data
192.168.3.239	89.29.122.60	TLSv1	143 [TCP Retransmission] Application Data
89.29.122.60	192.168.3.239	TCP	66 5222-1577 [ACK] Seq=5190 Ack=3264 Win=33024 Len=0 TSval=2299535918 TSecr=1191381
89.29.122.60	192.168.3.239	TCP	66 [TCP Dup ACK 2545#1] 5222-1577 [ACK] Seq=5190 Ack=3264 Win=33024 Len=0 TSval=2299535918 TSecr=1191381
192.168.3.239	89.29.122.60	TLSv1	143 Application Data
192.168.3.239	89.29.122.60	TLSv1	143 [TCP Retransmission] Application Data
89.29.122.60	192.168.3.239	TCP	66 5222-1577 [ACK] Seq=5190 Ack=3341 Win=33024 Len=0 TSval=2299535951 TSecr=1191388

Obrázek 26: Přenos hlasu

Z paketu lze vyčíst hlavičku přenášených souboru, která obsahuje některé identifikátory. Dokonce je možné rozeznat použití technologie softwaru Jabber, která slouží jako komunikační aplikace s přidruženým VoIP, podobně jako například ICQ. Lze tedy odvodit, že se jedná pouze o nastavbový systém.

```
<stream:stream to="phone-x.net" xmlns="jabber:client" xmlns:stream="http://etherx.jabber.org/streams" version="1.0"><?xml version="1.0" encoding="UTF-8"?><stream:stream xmlns:stream="http://etherx.jabber.org/streams" xmlns="jabber:client" from="phone-x.net" id="c09a30f8" xml:lang="en" version="1.0"><stream:features><starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"><required/></starttls><mechanisms xmlns="urn:ietf:params:xml:ns:xmpp-sasl"><mechanism>PLAIN</mechanism></mechanisms></stream:features><starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"><proceed xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>.....UX.Se.y...pPRy...O...^...G.K.9En'G UX.....5/
=.....YT...dV...VC.F...../S.....
.....3.9.2.8.
...
.....@.....
.4.2.
.....
.....M..UX.T..w.fmw.....U]=^..F.....4
UX.T.HH.....^x.n.tun.....S.....".....0.....0.....0
..*.H..
.....O..1.0...U...GII.0...U...Gibraltar1.0...U...Gibraltar1.0
..U.
..PhoneX1.0...U...CA1.0...U...ca.phone-x.net1 0...*.H..
.....admin@phone-x.net0..
140517215559Z.
170516215559Z0..1.0...U...GII.0...U...Gibraltar1.0...U...Gibraltar1.0
..U.
..PhoneX1.0...U...IM Server1.0...U...phone-x.net1 0...*.H..
.....admin@phone-x.net0..0
..*.H..
.....0..
.....J...B.V.&X...!0...V.....v4.^X.0~.....#j...6...3...js.D'f...&.....'..F..C
{7p}.....8:Z^@.....(D.w.i...SPRD.....X...j...5...#.\.
.)|.2%b...;6'SGA...s}K..f..S&-<.h...U...[0B\>$.a.....Y."4..z.<.....]...w>e.3..R...kX.X....*.
\..u...Q1..6G...
..c91.....{0y0...U...0.0...H...B.
...OpenSSL Generated Certificate0...U.....$.2
.....F...=0...U.#..0...M..n.....O...G..O.k.0
..*.H..
.....%.....!..C...N...-R...k..N8$.4.....`g.....F.Bn...y.2..0.
%...}.e.r.....y.!.....!.....E...8..!..C..Z.....)5c).....L...2...[(P/N...y$....!
€..1..e..0..f...M...A...y
```

Obrázek 27: Výpis TCP streamu komunikace



#### 4.3.2.2 Výsledky měření

Při hodnocení odezvy systému je nutné připomenout, že se jedná o předem registrované uživatelské rozhraní. Komunikace probíhá na virtuálním připojení u zprostředkovatele, který drží veškeré údaje o pozicích uživatelů. Z těchto důvodů může docházet k prodlevám a výpadkům při přechodu mezi komunikačními buňkami. Server je totiž nucen přijmout změnu polohy a obnovit virtuální rozhraní.

Časové rozhraní je definováno od prvního požadavku na spojení až po dosažení odezvy formou přijetí požadavku na druhém zařízení.

199	7.58196200	89.29.122.60	192.168.3.109	STUN	178 Allocate Error Response error-code: 401 (Unauthorized) Unauthorized realm: phone-x.net with nonce
200	7.58243400	89.29.122.60	192.168.3.109	STUN	178 Allocate Error Response error-code: 401 (Unauthorized) Unauthorized realm: phone-x.net with nonce
203	7.71448900	89.29.122.60	192.168.3.109	STUN	154 Allocate Success Response XOR-RELAYED-ADDRESS: 89.29.122.60:54010 lifetime: 600 XOR-MAPPED-ADDRESS:
204	7.71495900	89.29.122.60	192.168.3.109	STUN	154 Allocate Success Response XOR-RELAYED-ADDRESS: 89.29.122.60:54010 lifetime: 600 XOR-MAPPED-ADDRESS:
254	11.5035910	89.29.122.60	192.168.3.109	STUN	122 CreatePermission Success Response
255	11.5041810	89.29.122.60	192.168.3.109	STUN	122 CreatePermission Success Response
256	11.5101900	89.29.122.60	192.168.3.109	STUN	122 CreatePermission Success Response
257	11.5107790	89.29.122.60	192.168.3.109	STUN	122 CreatePermission Success Response
258	11.6379810	89.29.122.60	192.168.3.109	STUN	122 CreatePermission Success Response
259	11.6383980	89.29.122.60	192.168.3.109	STUN	122 CreatePermission Success Response
262	11.6675410	89.29.122.60	192.168.3.109	TCP	66 5222-59591 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2299814980 TSecr=19316443
265	11.6681110	89.29.122.60	192.168.3.109	TCP	66 [TCP Dup ACK 262#1] Seq=1 Ack=1 Win=501 Len=0 TSval=2299814980 TSecr=19316443
266	11.7393170	89.29.122.60	192.168.3.109	ICMP	182 Destination unreachable (host administratively prohibited)
267	11.7399590	89.29.122.60	192.168.3.109	ICMP	182 Destination unreachable (host administratively prohibited)
268	11.7569240	89.29.122.60	192.168.3.109	STUN	142 Data Indication XOR-PEER-ADDRESS: 89.29.122.60:37374
269	11.7575160	89.29.122.60	192.168.3.109	STUN	142 Data Indication XOR-PEER-ADDRESS: 89.29.122.60:37374

Obrázek 28: Měření odezvy

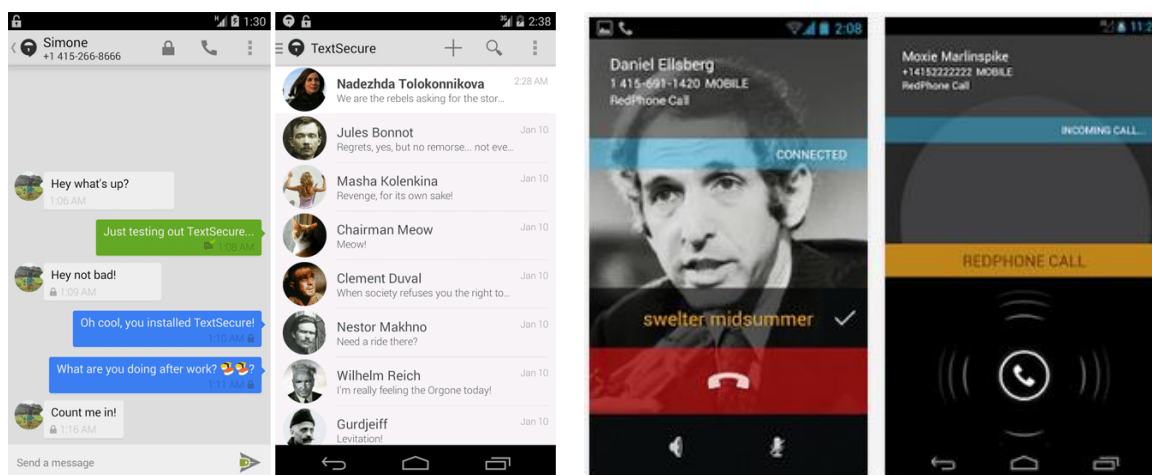
Tabulka 2: Měření odezvy PhoneX

Čas vysílání $t_1$ [s]	Čas příjmu $t_2$ [s]	Odezva $\Delta t$ [s]
60,700	70,988	10,288
20,702	24,324	3,622
8,198	14,720	6,522
7,714	11,756	4,042
5,295	13,097	7,802
6,662	11,113	4,451
6,148	10,998	4,850
6,292	10,503	4,211
6,912	12,327	5,415
Průměrná odezva [s]		$5,120 \pm 2,018$

Z výsledku měření lze vypožorovat schopnost serveru reagovat na požadavek klienta v poměrně dlouhé době, která odpovídá pomalému a zastaralému připojení mobilního internetu a to i přes připojení na rozhraní přístupového bodu. Velkým problémem je rovněž nestabilita serveru, která způsobila přílišnou odezvu u prvního měření. Obrovskou výhodou zůstává snížení výpočetní náročnosti u koncových uživatelů.

### 4.3.3 Open Whisper System

Jak již bylo zmíněno aplikace, kterou uvolnila skupina nezávislých vývojářů, pracuje na protokolu ZRTP, který byl vytvořený pro účely PGP, tedy kombinace asymetrické a symetrické šifry. Samotný systém je oddělený do dvou úrovní. Jedna aplikace, RedPhone, slouží čistě k potřebě hlasových hovorů a je doplněna protokolem AES. Druhou aplikací je TextSecure, která slouží k odesílání textových a multimediálních zpráv a je doplněna o protokoly Curve25519, AES-256 a HMAC-SHA256. [23]



Obrázek 29: Aplikace TextSecure a RedPhone[23]

#### 4.3.3.1 Hodnocení metodiky

Jedná se o volně šiřitelnou aplikaci, kterou si stačí stáhnout z dostupného serveru. K registraci poslouží označení státu a funkční telefonní číslo. Toto číslo poté slouží jako identifikátor v aplikaci. Nejsou zapotřebí žádné uživatelské účty. Aplikace je navíc kompatibilní s běžným rozhraním hovorů. Pro volbu zabezpečeného volání stačí potvrdit využití služby a dostupnost uživatele se stejnou aplikací. Její běh probíhá na pozadí operačního systému. To sebou přináší aktualizací procesy, o kterých uživatel nemusí mít ponětí.

Komunikace je nezávislá na registraci účastníku, tedy podprocesy na rozhraní uživatelského systému vždy předávají informace o stavu volaného účastníka na inicializační server.

176.58.114.110	192.168.3.109	TCP	74	31337-37153 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=186027806 TSecr=18915854 WS=128
176.58.114.110	192.168.3.109	TCP	74	[TCP Retransmission] 31337-37153 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=186027908 TSecr=18915854
176.58.114.110	192.168.3.109	TCP	74	[TCP Retransmission] 31337-37153 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=186027968 TSecr=18915854
192.168.3.109	176.58.114.110	TCP	74	37153-31337 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=18916555 TSecr=0 WS=64
192.168.3.109	176.58.114.110	TCP	74	[TCP out-of-order] 37153-31337 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=18916555 TSecr=0 WS=64
176.58.114.110	192.168.3.109	TCP	74	[TCP Retransmission] 31337-37153 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=186028010 TSecr=18915854
176.58.114.110	192.168.3.109	TCP	74	[TCP Retransmission] 31337-37153 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=186028010 TSecr=18915854
192.168.3.109	176.58.114.110	TCP	66	37153-31337 [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=18916561 TSecr=1860280810
192.168.3.109	176.58.114.110	TCP	66	[TCP Dup ACK 314#1] 37153-31337 [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=18916561 TSecr=1860280810
192.168.3.109	176.58.114.110	TLVSl	250	Client Hello
192.168.3.109	176.58.114.110	TLVSl	250	[TCP Retransmission] Client Hello
176.58.114.110	192.168.3.109	TCP	66	31337-37153 [ACK] Seq=1 Ack=185 Win=30080 Len=0 TSval=1860280833 TSecr=18916563
176.58.114.110	192.168.3.109	TCP	66	[TCP Dup ACK 326#1] 31337-37153 [ACK] Seq=1 Ack=185 Win=30080 Len=0 TSval=1860280833 TSecr=18916563
176.58.114.110	192.168.3.109	TLVSl	1202	Server Hello, Certificate, Server Hello Done
176.58.114.110	192.168.3.109	TLVSl	1202	[TCP Retransmission] Server Hello, Certificate, Server Hello Done
192.168.3.109	176.58.114.110	TCP	66	37153-31337 [ACK] Seq=185 Ack=1137 Win=16896 Len=0 TSval=18916568 TSecr=1860280833
192.168.3.109	176.58.114.110	TCP	66	[TCP Dup ACK 330#1] 37153-31337 [ACK] Seq=185 Ack=1137 Win=16896 Len=0 TSval=18916568 TSecr=1860280833
192.168.3.109	176.58.114.110	TLVSl	376	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.3.109	176.58.114.110	TLVSl	376	[TCP Retransmission] Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
176.58.114.110	192.168.3.109	TLVSl	109	Change Cipher Spec, Encrypted Handshake Message
176.58.114.110	192.168.3.109	TLVSl	109	[TCP Retransmission] Change Cipher Spec, Encrypted Handshake Message
192.168.3.109	176.58.114.110	TCP	66	37153-31337 [ACK] Seq=495 Ack=1180 Win=16896 Len=0 TSval=18916585 TSecr=186028085
192.168.3.109	176.58.114.110	TCP	66	[TCP Dup ACK 340#1] 37153-31337 [ACK] Seq=495 Ack=1180 Win=16896 Len=0 TSval=18916585 TSecr=186028085

Obrázek 30: Přenos stavu uživatele

Identifikátory se odesílají jako hodnota hash algoritmu SHA, které jsou zašifrovány pomocí RSA. Vlastní komunikace poté probíhá pomocí ZRTP protokolu, který šifruje i údaje účastníku. Jedinou čitelnou informací je sídlo vyvíjející společnosti (stát a provincie, označení společnosti). Dále následuje sled upozornění na ZRTP protokol a informace o přijetí komunikace. Identifikátory na inicializačním serveru jsou zašifrovány pomocí 256-bitového algoritmu AES.

```
GET /open/3915892978831840303 HTTP/1.0
GET /open/3915892978831840303 HTTP/1.0
HTTP/1.0 200 OK
Content-Length: 0
HTTP/1.0 200 OK
Content-Length: 0
...Z RTP...PZ.\Hello 1.10RedPhone 024 A.....X...V.rg.`....z.y.?.Up.;8.
A.....EC25.3;....KS.D...Z RTP...PZ.\Hello 1.10RedPhone 024
A.....x...v.rg.`....z.y.?.Up.;8.{...EC25.3;....KS.D...Z RTP...PZ.
.\Hello 1.10RedPhone 024 H...R.%
u...<.v...f...KVF.uq.....*.....EC25..9.Gs.D.9....Z RTP...PZ.\Hello
1.10RedPhone 024 H...R.%
u...<.v...f...KVF.uq.....*.....EC25..9.Gs.D.9....Z RTP...PZ.HelloAck...
...Z RTP...PZ.HelloAck...s...Z RTP...PZ.tCommit $HF...C:;u..Mf.?.u...G...\.%
IUq.....*S256AES1HS80EC25B256U.....4.....*L5.....VL
.9o...{.60.p...Z RTP...PZ.tCommit $HF...C:;u..Mf.?.u...G...\.%
IUq.....*S256AES1HS80EC25B256U.....4.....*L5.....VL
.9o...{.60.p...Z RTP...PZ.DHPart1.f./F.?i.$V..l6...#.N.K.ss...F.1~g3
(,).b.....sp%.....t...>..b.>..L.2@$..EC....4.q*.R.....G.8....[@
$.@.....Gno.T.v.....r.w.....Z RTP...PZ.DHPart1.f./F.?i.
$.V..l6...#.N.K.ss...F.1~g3(,).b.....sp%.....t...>..b.>..L.2@$..EC....
4.q*.R.....G.8....[@$.@.....Gno.T.v.....r.w.....Z RTP...PZ.DHPart1.f./F.?
i.$V..l6...#.N.K.ss...F.1~g3(,).b.....sp%.....t...>..b.>..L.2@$..EC....
4.q*.R.....G.8....[@$.@.....Gno.T.v.....r.w.qm.....Z RTP...PZ.DHPart2
C.R..7...3~d...q.....2.....r.B.....uG.R.....7.v..U..Gs.Hm5.....O..j...t.T
.3..U..|v..u..|.....w.....
^f>.._@;|.....<.*$w...Z RTP...PZ.DHPart2 C.R..7...3~d...
q.....2.....r.B.....uG.R.....7.v..U..Gs.Hm5.....O..j...t.T
.3..U..|v..u..|.....w.....
^f>.._@;|.....<.*$w...Z RTP...PZ.DHPart1.f./F.?i.$V..l6...#.N.K.ss...F.1~g3
(,).b.....sp%.....t...>..b.>..L.2@$..EC....4.q*.R.....G.8....[@
$.@.....Gno.T.v.....r.w{Fb...Z RTP...PZ.DHPart1.f./F.?i.
$.V..l6...#.N.K.ss...F.1~g3(,).b.....sp%.....t...>..b.>..L.2@$..EC....
4.q*.R.....G.8....[@$.@.....Gno.T.v.....r.w{Fb...Z RTP...PZ.DHPart2
C.R..7...3~d...q.....2.....r.B.....uG.R.....7.v..U..Gs.Hm5.....O..j...t.T
.3..U..|v..u..|.....w.....
^f>.._@;|.....<.*$w...Z RTP...PZ.DHPart2 C.R..7...3~d...
q.....2.....r.B.....uG.R.....7.v..U..Gs.Hm5.....O..j...t.T
.3..U..|v..u..|.....w.....
^f>.._@;|.....<.*$w...Z RTP...PZ.LConfirm1K
Y.v.....#,H...C.....\.....k1.g.C8..E..r.....
\F...i.i...Z RTP...PZ.LConfirm1K
```

Obrázek 31: Komunikace pomocí aplikace RedPhone

Při samotné komunikaci je vyslán nepřetržitý proud informací, který blokuje komunikační rozhraní koncových zařízení. Nedochází zde k přerušování komunikace v hluchých místech. Tedy nedochází k úsporám na datovém spojení. To má za důsledek i zhoršení kvality zvukové reprodukce a výskyt šumu.

#### 4.3.3.2 Výsledky měření

Při hodnocení odezvy je nutné přihlížet ke skutečnosti, že se jedná o nezaplatněnou aplikaci a služby. Nicméně je skutečností, že časté výpadky spojení s inicializačním serverem mohou spousty uživatelů odradit. Zejména pokud je uživatel nucen opakovaně vytáčet hovor. Při měření jsem dospěl ke zjištění, že úspěšné spojení probíhá nahodile s průměrným počtem pokusů dvou vytáčení. Tato skutečnost může signalizovat nadměrné využití nebo špatné zajištění komunikačních linek.

Časové rozhraní je definováno od prvního požadavku na spojení až po dosažení odezvy formou přijetí požadavku na druhém zařízení. Za první požadavek považováno je otevření komunikačního rozhraní a za přijetí požadavku je považováno přidělení komunikačních portů.

Toto měření v sobě nedokáže zachytit schopnost reakce samotné aplikace ale pouze přidělení komunikačního kanálu. Aplikace poté vytváří další prodlevu při zpracování.

192.168.3.109	176.58.114.110	TCP	66 [TCP Dup ACK 340#1] 37153-31337 [ACK] Seq=495 Ack=1180 win=16896 Len=0 TSval=18916585 TSecr=1860280885
176.58.114.110	192.168.3.109	TCP	66 31337-37153 [RST, ACK] Seq=1180 Ack=495 win=31104 Len=0 TSval=0 TSecr=18916585
176.58.114.110	192.168.3.109	TCP	66 31337-37153 [RST, ACK] Seq=1180 Ack=495 win=31104 Len=0 TSval=0 TSecr=18916585
192.168.3.109	176.58.114.110	TCP	74 37157-31337 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=18919931 TSecr=0 WS=64
192.168.3.109	176.58.114.110	TCP	74 [TCP out-of-order] 37157-31337 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=18919931 TSecr=0 WS=64
176.58.114.110	192.168.3.109	TCP	74 31337-37157 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1860290939 TSecr=18919931 WS=128
176.58.114.110	192.168.3.109	TCP	74 [TCP out-of-order] 31337-37157 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1860290939 TSecr=18919931 WS=128

Obrázek 32: Zahájení komunikace

176.58.114.110	192.168.3.109	TCP	66 [TCP Dup ACK 857#1] 31337-37157 [ACK] Seq=1180 Ack=638 win=32256 Len=0 TSval=1860291028 TSecr=18919957
176.58.114.110	192.168.3.109	TCP	229 31337-37157 [PSH, ACK] Seq=1180 Ack=638 win=32256 Len=163 TSval=1860291113 TSecr=18919957
176.58.114.110	192.168.3.109	TCP	229 [TCP Retransmission] 31337-37157 [PSH, ACK] Seq=1180 Ack=638 win=32256 Len=163 TSval=1860291113 TSecr=18919957
192.168.3.109	176.58.114.110	TCP	66 37157-31337 [ACK] Seq=638 Ack=1343 win=19200 Len=0 TSval=18920011 TSecr=1860291113
192.168.3.109	176.58.114.110	TCP	66 [TCP Dup ACK 865#1] 37157-31337 [ACK] Seq=638 Ack=1343 win=19200 Len=0 TSval=18920011 TSecr=1860291113
192.168.3.239	176.58.114.110	TCP	74 1067-31337 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=867612 TSecr=0 WS=64
192.168.3.239	176.58.114.110	TCP	74 [TCP Retransmission] 1067-31337 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=867612 TSecr=0 WS=64
192.168.3.109	176.58.114.110	UDP	84 Source port: 55574 Destination port: 50621
192.168.3.109	176.58.114.110	UDP	84 Source port: 55574 Destination port: 50621
176.58.114.110	192.168.3.239	TCP	74 31337-1067 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1860291241 TSecr=867612 WS=64
176.58.114.110	192.168.3.239	TCP	74 [TCP Out-of-order] 31337-1067 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1860291241 TSecr=867612 WS=64
192.168.3.239	176.58.114.110	TCP	66 1067-31337 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=867617 TSecr=1860291241
192.168.3.239	176.58.114.110	TCP	66 [TCP Dup ACK 886#1] 1067-31337 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=867617 TSecr=1860291241
192.168.3.239	176.58.114.110	TCP	250 1067-31337 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=184 TSval=867618 TSecr=1860291241

Obrázek 33: Přidělení komunikačních portů

Tabulka 3: Měření odezvy RedPhone

Čas vysílání $t_1$ [s]	Čas příjmu $t_2$ [s]	Odezva $\Delta t$ [s]
54,608	55,630	1,022
9,984	10,801	0,817
6,651	7,409	0,758
14,987	16,061	1,074
59,636	60,321	0,685
99,653	100,484	0,831
15,209	16,706	1,497
7,108	8,006	0,898
8,108	8,861	0,753
Průměrná odezva [s]		$0,834 \pm 0,239$

Při měření bylo zjištěno, že aplikace neskrývá účel komunikace. Dokonce je možné pořídit záznam šifrované komunikace, přestože se jedná pouze o sled tónu ve zdánlivě nahodilém rytmu. Příznivé odezvy je dosaženo především přenesením procesu přidělování komunikačního kanálu až na straně koncových uživatelů. Je tedy přímo úměrné výpočetní schopnosti zařízení. Inicializační server pak působí jen rolí prostředníka, který nevytváří komunikační rozhraní, ale pouze ho přepojuje bez dodatečného zabezpečení kanálu.

Příznivým výsledkem této metody je však dosažení relativně stabilní odezvy na straně zprostředkovatele.



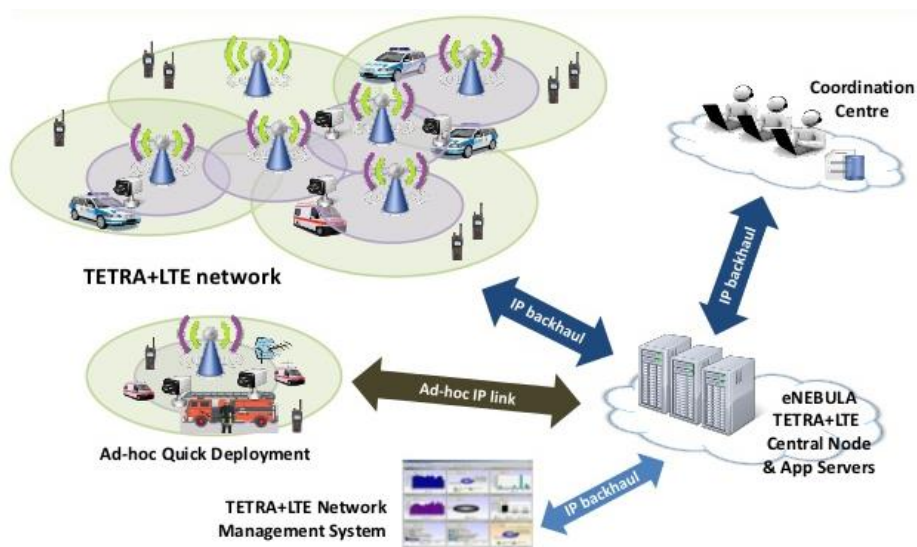
## 5 HODNOCENÍ FUNKČNÍCH MODELŮ NA TRHU

Modely kryptografického zabezpečení lze rozdělit podle účelnosti. První skupinu tvoří státní sektor, který vždy stojí v čele vývoje a má nejvyšší požadavky na bezpečnost. Z této skupiny přebírá technologie komerční sektor podnikatelských subjektů. Další skupinu tvoří soukromí jedinci nebo skupiny, kteří požadují tyto aplikace pro zvýšení míry pocitu jejich bezpečí. Modely zabezpečení pak lze definovat podle určení a stáří technologie, stejně tak jako finanční náročnosti.

### 5.1 Státní sektor

Státní sektor disponuje rozsáhlými investičními prostředky, a proto se zde setkáváme především s tvorbou vlastní komunikační sítě, popřípadě pronajaté. V důsledku toho vzniká zabezpečená infrastruktura. Zpravidla jsou použity nejmodernější prvky, které dosahují vysoké míry odolnosti a přenosových rychlostí. Stejně tak jako možností využitelnosti technologií pro komunikační účely a sdílení dat.

Lokální strukturu tvoří především centra zabezpečené infrastruktury objektu a vyhrazené komunikační kanály. V současné době je stále nejvyužívanější nezávislá základnová síť ve formátu přenosu X509. V tomto standardu je však omezený datový přenos v řádech kbit/s. V rámci zabezpečení interní komunikace po místní síti rozlehlých objektu jsou především používány šifrovací moduly síťové infrastruktury s konektivitou do vnější sítě přes rozhraní spojovací ústředny. Tyto koncepty jsou kompatibilní a operabilní v rámci evropského kontinentu a tvoří komunikační standard pro členské státy Evropské unie. [1], [17]



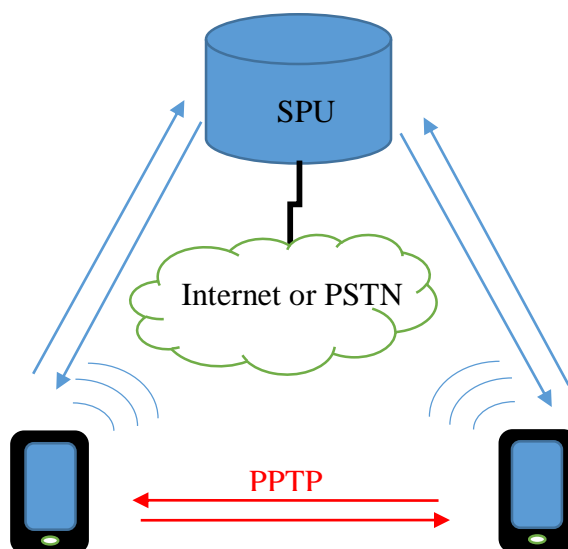
Obrázek 34: Architektura modernizované sítě Tetra[24]

V rámci globalizace komunikace je zapotřebí satelitní komunikace a to zejména v otázkách dosahu v odlehlých oblastech. Tuto část řeší především armádní složky. Obrovskou výhodou státního sektoru jsou smlouvy o spolupráci mezi jednotlivými strategickými partnery. Tyto smlouvy naší zemi umožňují například využívat vyhrazené komunikační sítě NATO nebo americké komunikační satelity. Pro komunikaci se využívá VoIP technologie a speciální telekomunikační prostředky ve formě zabezpečených a satelitních telefonů. [1], [17]

## 5.2 Zprostředkovatel na End-to-End komunikaci

End-to-End koncepce v současné době nabývá velké popularity a to zejména s ohledem na špionážní kauzy s posledních let. Vzhledem k dostupnosti na jakémkoliv operačním systému se zdá být vhodnou variantou pro většinu uživatelů. Velmi příznivým faktorem je také cena. V mnohých případech dnes již stáhnete volně šiřitelnou aplikaci pro nekomerční účely. U těchto aplikací je ale nutné zkontrolovat používané šifrovací protokoly a způsoby přenosů v systémové soustavě. Další nevýhodou pak bývá nespolehlivost, kde řešíme především časté výpadky komunikace s inicializačním serverem (SPU) nebo také v průběhu komunikace. Stejně tak zpravidla nedochází k dostatečně kvalitnímu přenosu, pokud tedy hovoříme o kvalitě zvukové reprodukce.

Druhou variantou v tomto segmentu jsou placené licenční služby, kdy zákazník platí za zprostředkování přenosového kanálu a zálohu dat na serverech společnosti. V takových případech společnost nabízí kvalitní reprodukci zvuku při přenosu a stabilní komunikační rozhraní, společně s garancí dostupnosti.

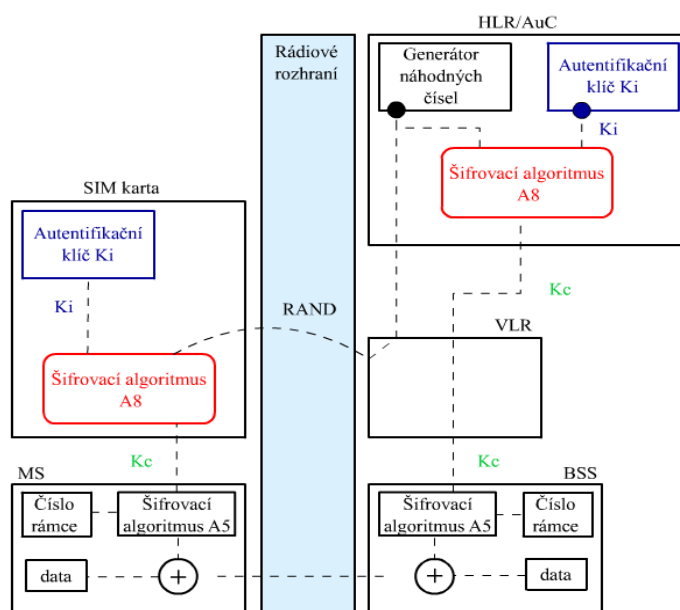


Obrázek 35: End-to-End připojení

### 5.3 Zabezpečení přenosu po GSM síti

Zabezpečení komunikačního rozhraní na GSM síti tvoří dnes již zastaralou technologii s vysokými prodlevami způsobené pomalými přenosovými rychlostmi sítě. Jedním z hlavních problémů je současně nutnost využití speciální techniky nebo operačního systému v telefonu. [1], [19]

Vše je založeno na postupném šifrování, pomocí proudové šifry, do komunikačního kanálu. Proces šifrování je posledním bodem před zahájením komunikace. Signál po síti GSM proudí pomocí pulsní modulace proto je výsledkem sled impulsních tónů, které je nutno před dekódováním dešifrovat. To má za důsledek značné zpoždění v rekonstrukci zvukové stopy. K autentizaci uživatelů dochází prostřednictvím mobilní sítě a identifikátoru na SIM kartě. [1], [19]



Obrázek 36: Princip šifrování v síti GSM[11]

### 5.4 Vyhodnocení

Lze říci, že nejbezpečnější realizaci uskutečňuje státní sektor a to především svým vlivem i finančními prostředky. V tomto segmentu lze docílit i nejrychlejšího přenosu. V soukromém sektoru však existuje spousta kvalitních zprostředkovatelů služeb, kteří jsou schopni dosahovat kvalitních výsledků při nesrovnatelně nižších finančních nákladech. Pokud se týče zastaralého přenosu v klasické síti GSM, jedná se o drahou a nekvalitní službu. Drahou zejména v kontextu s cenou pořizovaných speciálních zařízení a licencí.



## 6 NÁVRH ŘEŠENÍ ZABEZPEČENÍ KOMUNIKACE POMOCÍ ŠIFROVÁNÍ

Nejprve je nutné si definovat oblasti, ve kterých by mohl klient chtít komunikovat. Primární, jako v každém podnikatelském záměru, je určení segmentu trhu. V tomto případě máme tři základní skupiny uživatelů.

První skupinou je státní sektor, který má vysoké požadavky na kvalitu spojení a míru odolnosti. Dále zde hodnotí dosažitelnost v různých zeměpisných polohách, tedy globální pokrytí. Hodnocené jsou i nabízené služby a to zejména z pohledu konferenčních hovorů. Požadavky na cenu tvoří druhořadý faktor.

Druhou skupinou je komerční sféra podnikatelských subjektů. Zde je rovněž požadována kvalita spojení a míra odolnosti. Tyto parametry jsou srovnatelné se státním sektorem, pokud vynecháme armádní složky. Je požadováno širší spektrum nabízených služeb, včetně přenosu interních souborů. Důležitou roli hraje možnost přenosu obrazu a dosažitelnost v hustě zasedlených oblastech. Cenový faktor už je zde výraznější, ale závislý na velikosti podniku.

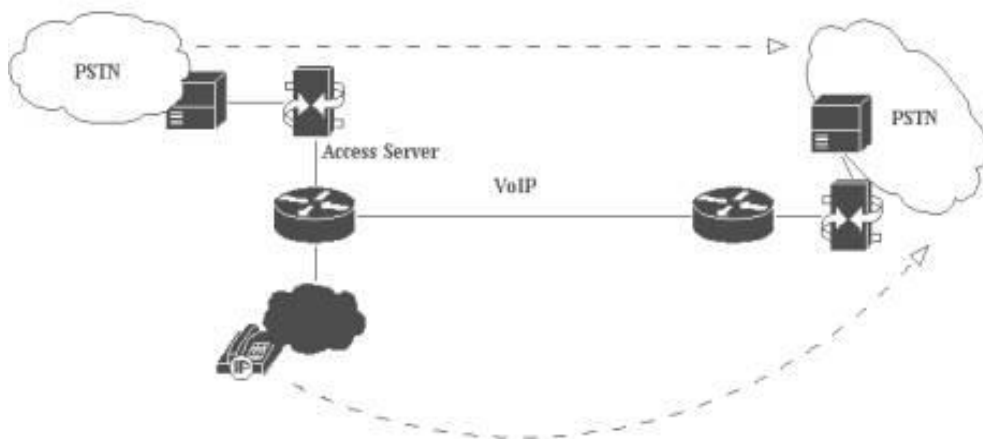
Poslední skupinou je běžný obyvatel. Má nejmenší nároky na kvalitu služeb i jejich šíři. Hlavním parametrem je cena a spolehlivost na lokálním území. Zpravidla nevznikají požadavky na přenos nadměrně velkých souborů, konferenčních hovorů nebo video-telefonie. Tuto službu si pořizuje jako doplněk zvyšující míru jistoty v sociálním zázemí. V tomto návrhu se prioritně zaměřím právě na tuto skupinu.

Pro návrh využiji poznatku získaných při hodnocení testovaných aplikací. Především z pohledu efektivnosti použitých metod.

### 6.1 Způsob přenosu

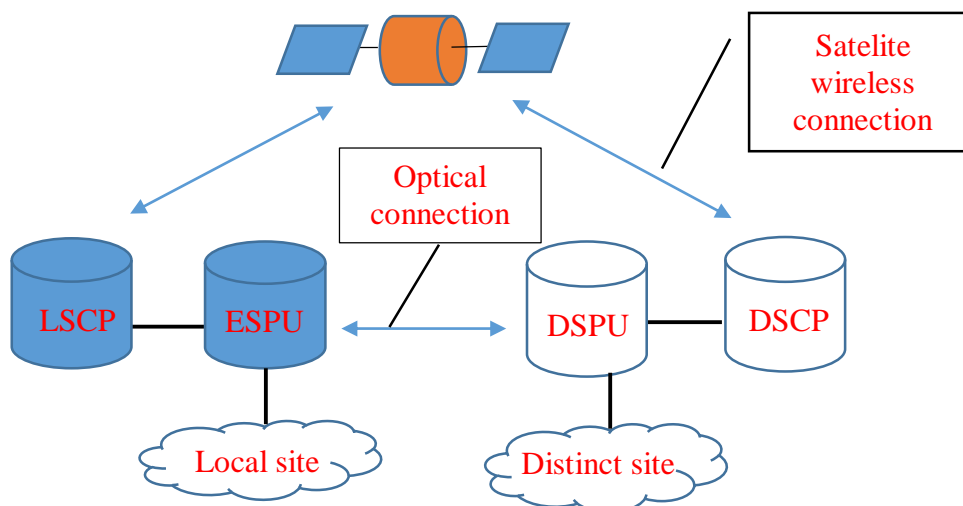
Přenosové trasy jsou přímo odvoditelné z požadavků uvedených v úvodu návrhu. Přímou souvisí s požadavkem na dosažitelnost a to především z pohledu přenosové latence. V základu lze odvodit dvě základní síťová uskupení přenosových tras. První variantou je zaměření na lokální okruh, kde řešíme především schopnost komunikace mezi poskytovateli datových služeb (mobilní operátoři a ISP). V druhé kategorii je zapotřebí zohlednit faktor vzdálenosti, a to sice z pohledu dosažitelnosti přes kabelové vedení s ohledem na ztráty latence. Popřípadě se nabízí možnost satelitního přenosu, která je ovšem cenově vysoce náročná.

Lokální přenosové trasy mohou tvořit ISP a mobilní operátoři v datových tarifech. Základem každého uskupení je vytvoření lokálního inicializačního centra, které je schopné operovat v obou z těchto přenosových tras, případně nabízet zprostředkování jejich kombinace. Je zapotřebí vytvořit dostatečně propustné kanály pro pokrytí všech přenosových služeb. Při současném stavu mobilních sítí na území našeho státu jsou v hustě osídlených oblastech tyto trasy rovnocenné, a to z pohledu na využití moderních přenosových standardů.



Obrázek 37: Schéma kombinace komunikačních rozhraní[7]

Při začlenění globálního pohledu šíření služeb je nutné definovat přenosové parametry na danou vzdálenost. Těžko lze získat stejnou stabilitu přenosu po kabelovém vedení na vzdálenosti srovnatelné s lokální sítí (například okolní státy) v porovnání s opačným koncem zeměkoule. V případě okolních států plně postačí optické linky hlavních zprostředkovatelů internetového připojení mezi státy, spojení mezi zabezpečenou infrastrukturou (ESPU) a vzdáleným poskytovatelem služeb (DSPU). Tyto linky poskytují stále ještě dostačující latenci. V případě vzdálenějšího připojení je však nutné začlenit do infrastruktury satelitní připojení přes vyhrazené kanály mezi místním zprostředkovatelem (LSCP) a vzdáleným zprostředkovatelem (DSCP). Cena pronájmu satelitního pásma se však pohybuje v řádech tisíců za poskytnutí hodinového přenosu.

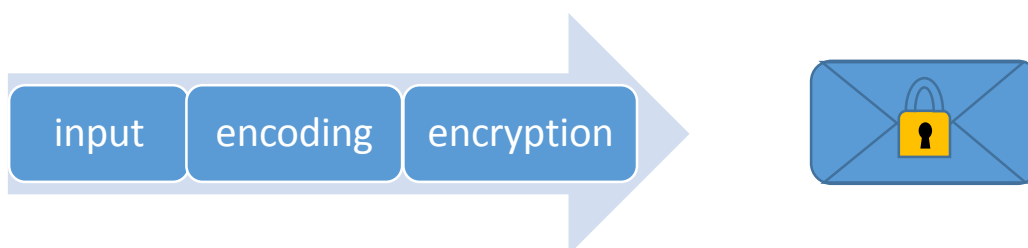


Obrázek 38: Schéma kombinace globálního spojení

Pro účely uživatelské aplikace je nejvhodnějším řešením varianta bez satelitního spojení, která by neúměrně zvyšovala cenu poskytovaných služeb s ohledem na požadavky většiny uživatelů. V tomto smyslu fungují i veškeré open source aplikace. Zde se nehledí na latenci a spolehlivost přenosu. Hlavním posuzovaným parametrem je odolnost vůči odposlechu a neoprávněným změnám přenosové zprávy. Menší důraz je kladen na ochranu identity.

## 6.2 Výběr vhodného algoritmu

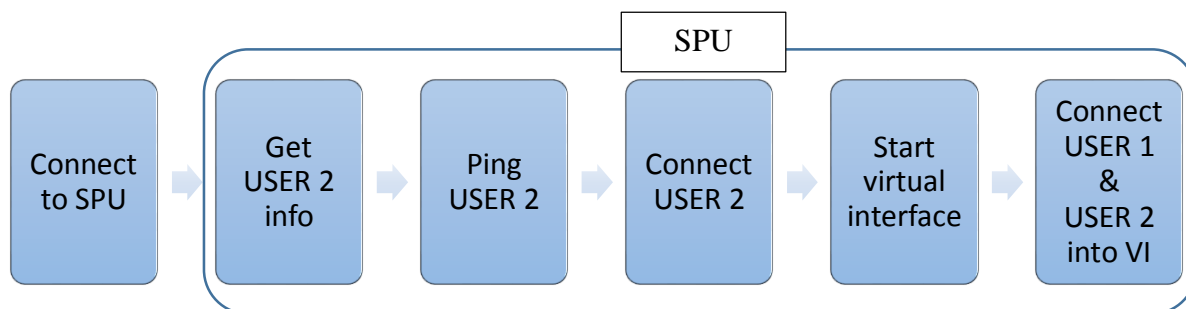
Algoritmus přenosu a šifrování zprávy si rozdělím do dvou částí. Vzhledem ke skutečnosti volby koncepce End-to-End, veškeré šifrování bude probíhat na straně koncových zařízení. Pro šifrování by bylo vhodné zvolit algoritmus AES kvůli odolnosti a kompatibilitě s rozhraními nižší výpočetní kapacity.



Obrázek 39: Postup odeslání zprávy

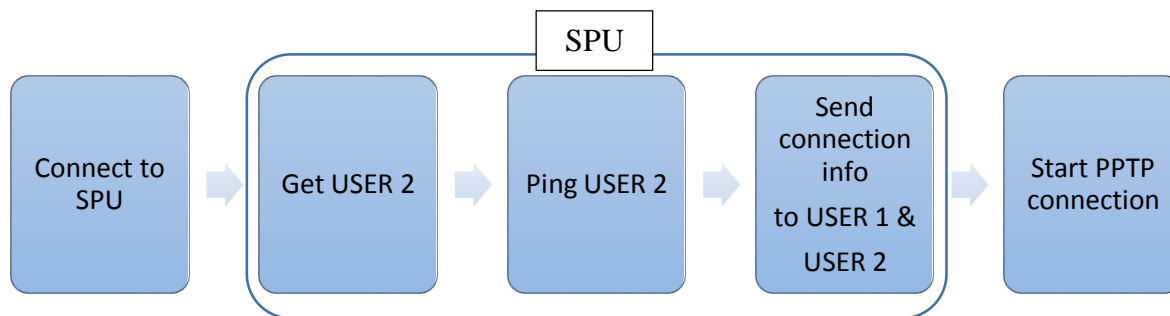
Prvním bodem koncepce musí být přesměrování vstupu do rozhraní aplikace. Následně bude zpráva zašifrována. V tuto chvíli se nabízí dvě možnosti distribuce. První variantou je použití distribučního centra, které řídí celou komunikaci prostřednictvím přepojování rozhraní na straně vnitřní infrastruktury zabezpečeného centra poskytovatele (placené aplikace).

V tomto případě je vytvořené komunikační rozhraní pouze s inicializačním centrem. V takovém případě je možné zálohování přenosu textových zpráv a výpisů hovorů.



Obrázek 40: Schéma připojení

Druhou variantou je vytvoření virtuálního spojení mezi koncovými uživateli. K tomu je zapotřebí vytvořit inicializační pakety, které budou obsahovat cílové adresy obou koncových zařízení a definice komunikačních protokolů point-to-point spojení.



Obrázek 41: Inicializační proces

V obou případech je nutné zaměřit se na princip registrace účastníků. Vhodnější variantou je dosažitelnost pouze souběžně registrovaných uživatelů do sítě. Tato varianta snižuje inicializační dobu na minimum, ale na druhou stranu zvyšuje datovou náročnost v nečinnosti vzhledem k průběžnému vybuzování spojení na inicializační server. To je zapotřebí kvůli ověření polohy a stavu koncového zařízení, a to včetně údajů o formě služeb datového přenosu.

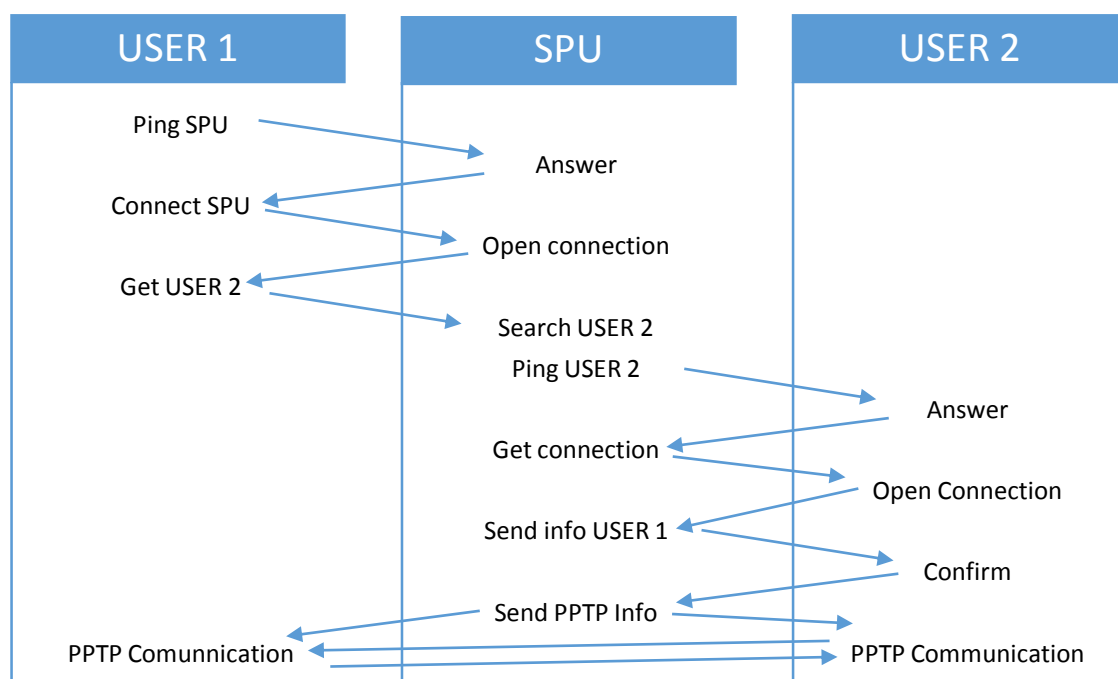
### 6.2.1 Zahájení přenosové trasy

Zahájení přenosové trasy vytváří aktivní vybuzení přenosového kanálu. Z tohoto důvodu je nutno zavést dotaz na stav přenosové linky a dostupnosti serveru. Server by měl vyhodnotit požadavek a vyhledat dotazovaného uživatele v databázi. Následně vyšle požadavek na stav linky koncového adresáta. Pokud je vyhodnocená dosažitelnost, server pošle potvrzení tazateli a může vytvořit stabilní spojení pro oba uživatele skrze zabezpečenou infrastrukturu.

Tato varianta je však s ohledem na latenci sítě méně vhodná. Proto by bylo vhodnější využít spíše přeposlání cílové adresy v zabezpečeném paketu a koncová zařízení pak nechat mezi sebou vytvořit stabilní připojení přímo, bez zprostředkovatele. Následně by mělo dojít k ověření platnosti šifrovacího klíče.

### 6.2.2 Příjem komunikace

Nejvhodnější metodou pro aplikaci je aktivní registrace všech uživatelů na inicializační servery zprostředkované služby. Uživatel pak aktivně v pravidelných intervalech vysílá údaje o koncové adrese a stavu přenosové linky. V takovém případě pak server vyšle dotaz na poslední známou adresu. Pokud je informace potvrzená server vyšle volajícímu podklady k vytvoření komunikačního kanálu v zašifrované podobě. Dále je vytvořeno stabilní připojení mezi koncovými uživateli mimo rozhraní zprostředkovatele. Následně by mělo dojít k ověření platnosti šifrovacího klíče.



Obrázek 42: Schéma přepojení

### 6.2.3 Způsob ověření a distribuce klíčů

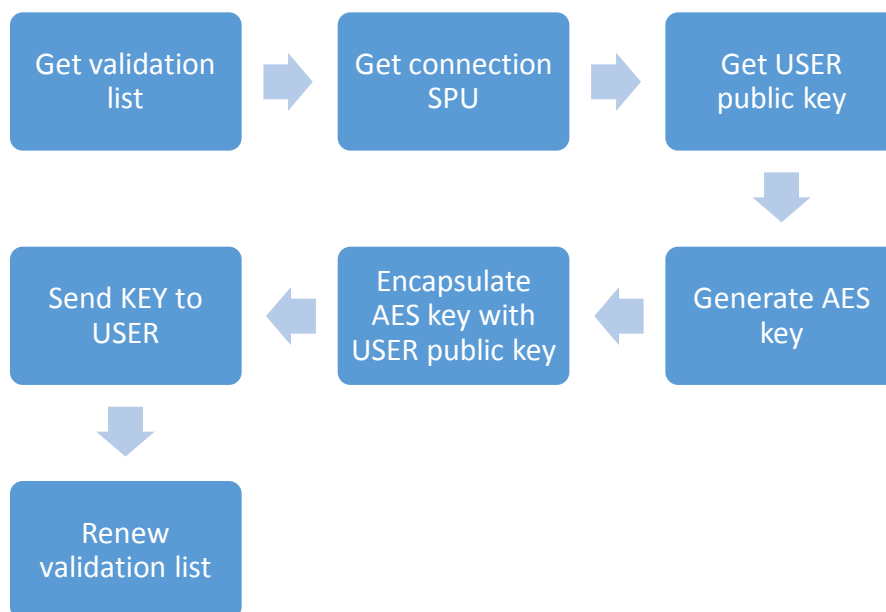
Ověření identity, autentizace, a princip distribuce klíčů tvoří nejdůležitější část každého návrhu kryptografického systému. Právě zde je definována odolnost celé skladby. Proto jsem kombinací možných schémat dospěl k následujícímu řešení.

Pro účely přenosu informací je vhodné zvolit protokol ZRTP, který vytváří efektivní formu zabezpečení i při nižší výpočetní schopnosti koncových zařízení. Na rozdíl od šifrování pomocí RSA nepřenáší identifikátory v nezašifrované podobě, tato skutečnost vzniká právě v důsledku vyšší výpočetní náročnosti. Bohužel hlavní nevýhodou je nemožnost skrýt účel přeposílaných paketů. Bude možné odhalit typ komunikace, ale ne její obsah a účastníky.

Klíče budou vytvářeny pseudonáhodně, pomocí generátoru, pro každý účastnický pár. V telefonu budou uchovány v zašifrované podobě. Ke zrychlení autentizace bude využito ověření hashe identifikačních údajů, podobně jako tomu je u přihlašování do operačního systému MS Windows. Jako hash algoritmus bych pro vyšší odolnost zvolil SHA-256.

Pro účely zrychlení procesu identifikace by bylo vhodné zvolit časově omezené ověření, namísto jednorázového ověření při každém hovoru. To bude mít za důsledek zvýšení rychlosti odezvy celého systému v kterémkoliv směru. Jak už bylo zmíněno, nejvhodnější je předem registrovaný systém. V takovém případě je možné začlenit proces ověření platnosti autentizace, v definované skupině účastníků, hned při registraci do systému. V případě nutnosti pak automatickou obnovu při dostupnosti uživatele. Tyto informace budou předávány pomocí inicializačního serveru, který bude na zabezpečeném databázovém serveru uchovávat pouze veřejné klíče účastníku, právě pro účely autentizačního procesu.

Samotné ověření při zahájení komunikace pak již není vázané na zprostředkovatele, a tudíž opět snížíme prodlevu systému na vytvářené komunikaci.



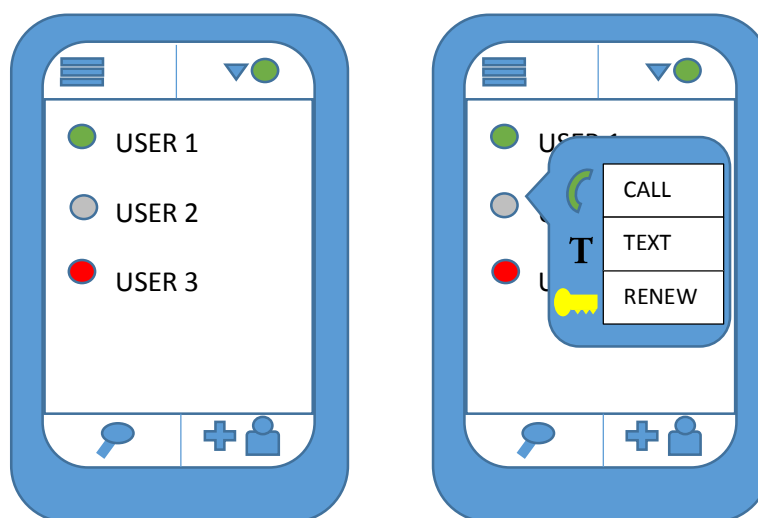
Obrázek 43: Schéma obnovy šifrovacího hesla

### 6.3 Tvorba rozhraní

Uživatelské rozhraní musí vytvářet především přehled o registrovaných účastnících komunikační skupiny a jejich stavu v systému. Proto je vhodné zvolit pouze jednoduchou aplikační nabídku, která obsahuje stav registrace držitele s možností volby dostupnosti a přihlášení.

Dále zde musí být právě seznam registrovaných účastníků s indikací stavu registrace, kdy zelená ikona signalizuje registrovaného a platně ověřeného účastníka, šedá ikona signalizuje registrovaného, ale neověřeného účastníka a červená ikona signalizuje nedostupného účastníka.

Pro inicializaci komunikace je vhodným využitím podnabídka s možností volby činnosti. V základním provedení by měla obsahovat možnost vytáčení hlasového hovoru, zaslání zprávy a možnost obnovení ověření. Dále zde musí být dostupnost funkce přidání uživatele a filtrování uživatelů.



Obrázek 44: Znáznornění rozhraní

### 6.4 Vyhodnocení

Tento návrh reprezentuje problematiku vývoje aplikace End-to-End komunikace. Především jsem se snažil vysvětlit možné konfigurace a problematiku výběru různých algoritmů, společně s jejich implementací do systému. Jako hlavní bod zájmu každého návrhu je zaměření se na výpočetní schopnosti zařízení, pro které je aplikace určena. Tímto vnímáním můžeme vhodně vybrat šifrovací algoritmy a snížit prodlevy mezi jednotlivými kroky přenosu.

Jako vhodné řešení považuji princip registrace systému do struktury poskytovatele inicializačního serveru a to zejména s pohledu automatizace některých z procesů před zahájením komunikace. To má za důsledek menší požadavky na autentizaci komunikace a v důsledku toho i zvýšení rychlosti celého systému.

Další výraznou otázkou při vytváření řešení je otázka dosažitelnosti v různých lokalitách i sítích. Zejména pak z pohledu globálního měřítka v porovnání s místním trhem.



## ZÁVĚR

Šifrování dnes hraje velkou roli v našich digitálních životech a dává nám trochu soukromí. Použití šifrování v počítačových technologiích je dnes běžné pro většinu z nás, ale téměř nikdo nepomýšlí na naše telefony a tablety, které jsou dnes nejen populární ale také poměrně inteligentní a mají své vlastní operační systémy. Všechny tyto kroky byly myšleny tak, aby nám přinesly trochu pohodlí, ale zároveň taky přinesly výhodu pro hackery a zpravodajské služby. Abychom zvýšily naše soukromí zpátky na normální úroveň, musíme použít technologii, která nám umožní skrýt, cokoli budeme potřebovat. Pro tyto účely můžeme použít různé aplikace a specifické systémy.

Pro účely své práce jsem vybral vzorové technologie na základě jejich metodiky použitelné pro běžného uživatele. V konečném důsledku nelze hledat rozdíly v závislosti na ceně prostředku a s ním spojených služeb. Hlavní problematikou se ukázalo být řešení konečného konceptu při kombinaci různých algoritmu a zároveň při dostupnosti služeb.

V placeném segmentu je prioritním zaměřením cílení na dostupnost služeb při různých podmínkách. Při bližším pohledu je však možné zjistit, že méně pozornosti je dáváno utajování údajů o uživateli a parametrech jeho účtu u společnosti. Velkou výhodou je pak automatizace procesů ověření a přenesení části závislosti výpočetního výkonu na stranu zprostředkovatelských serveru. Tím je především redukována náročnost na koncové zařízení a tím i definovaná aplikovatelnost.

V neplaceném segmentu jsou role poněkud obrácené. Kvalita služeb zaostává za kvalitou zabezpečení. Vzhledem k otevřenému přesměrování je kladen velký důraz na ochranu uživatelských údajů. To však není způsobeno důkladností, ale hledáním úspor v zabezpečené infrastruktuře. Jako vedlejší efekt, pro koncového uživatele, je rychlejší odezva systému, která je ovšem vyrovnána častou nedostupností služeb.

## ZÁVĚR V ANGLIČTINĚ

Encryption, nowadays, takes a big part of our digital life and gives us a little privacy. The use of encryption in computer science is normal for most of us, but almost no one thinks about our phones and tablets, which are very popular today and also smart with their own operating systems. This all was meant to bring us more comfort, but it is also a leverage for hackers and intelligence agencies. To improve our privacy back to normal level we need to take the piece of technology that provides us the chance to hide what we need. For this purpose we can use applications or specific system.

For the purpose of this thesis I chose sample technologies on basis of their methodology applicable for a common user. In the end is not possible to look for differences based on the price and connected services. The main problem appeared to be solution of final concept for combination different algorithms and availability of the services.

In the paid segment is priority aimed at availability of services in different circumstances. In closer inspection is possible to determine that less attention is aimed at concealing user data and parameters of his account in the company. Big advantage is automatization of authenticating processes and transferring part of the necessary computing power onto mediatory server. Thanks to that is reduced the demand on the terminal and thus defined applicability.

In the free segment are the roles inverted. The quality of services lags behind the quality of security. Because of open redirection is put bigger importance on protecting user data. This is not caused by carefulness, but by finding savings in secured infrastructure. As a side effect is for end user faster system response which is counterbalanced by frequent inaccessibility of service.

**SEZNAM POUŽITÉ LITERATURY**

- [1] BURDA, Karel. Aplikovaná kryptografie. 1. vyd. Brno: Vutium, 2013, 255 s. ISBN 978-80-214-4612-0.
- [2] BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5
- [3] Proudová šifra. *Wikipedia* [online]. 2013 [cit. 2014-12-09]. Dostupné z: [http://cs.wikipedia.org/wiki/Proudov%C3%A1\\_%C5%A1ifra](http://cs.wikipedia.org/wiki/Proudov%C3%A1_%C5%A1ifra)
- [4] Feistelova šifra. *Wikipedia* [online]. 2011 [cit. 2015-05-24]. Dostupné z: [http://cs.wikipedia.org/wiki/Feistelova\\_%C5%A1ifra](http://cs.wikipedia.org/wiki/Feistelova_%C5%A1ifra)
- [5] Twofish. *Schrenier on Security* [online]. [cit. 2015-05-24]. Dostupné z: <https://www.schneier.com/twofish.html>
- [6] Asymetrická kryptografie. *Wikipedie* [online]. 2014 [cit. 2014-12-09]. Dostupné z: [http://cs.wikipedia.org/wiki/Asymetrick%C3%A1\\_kryptografie](http://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie)
- [7] Úvod do VoIP. *Mbdata* [online]. [cit. 2015-05-24]. Dostupné z: <http://www.mbdata.cz/uvoddovoip.htm>
- [8] Základy VoIP. *Joyce* [online]. [cit. 2015-05-24]. Dostupné z: <http://www.joyce.cz/cz/voip-sekce/vse-o-voip-rady-tipy/1-dil-zaklady-voip/>
- [9] VODRÁŽKA, Jiří a Ivan PRAVDA. Principy telekomunikačních systémů. Vyd. 1. Praha: Česká technika - nakladatelství ČVUT, 2006, 130, [7] s. ISBN 800103366x
- [10] JANSSEN, Horst a Heinrich RÖTTER. Informační a telekomunikační technika. Vyd. 1. Praha: Europa - Sobotáles, 2004, 399 s. ISBN 8086706087
- [11] Přístupová síť UTRAN. *Technologie pro mobilní komunikaci* [online]. 2013 [cit. 2014-12-09]. Dostupné z: <http://tomas.richtr.cz/mobil/utran.htm>
- [12] Základy sítí 3. generace. *UMTS* [online]. 2013 [cit. 2014-12-09]. Dostupné z: [http://www.umts.wz.cz/Mob\\_radio\\_site\\_3G/uvod\\_do\\_site\\_3G.htm](http://www.umts.wz.cz/Mob_radio_site_3G/uvod_do_site_3G.htm)
- [13] Družicové telekomunikační spoje. *Access server* [online]. 2010 [cit. 2015-05-24]. Dostupné z: <http://access.feld.cvut.cz/view.php?cislocclanku=2010020002>
- [14] Abeceda satelitního příjmu: Satelitní telekomunikace. *Parabola* [online]. [cit. 2015-05-24]. Dostupné z: <http://www.parabola.cz/abc/satelitni-telekomunikace/>

- [15] Telekomunikace z oběžné dráhy. *Mobil.idnes.cz* [online]. 2004 [cit. 2015-05-24]. Dostupné z: [http://mobil.idnes.cz/telekomunikace-z-obezne-drahy-dk4-/mob\\_tech.aspx?c=A040504\\_5257356\\_mob\\_tech](http://mobil.idnes.cz/telekomunikace-z-obezne-drahy-dk4-/mob_tech.aspx?c=A040504_5257356_mob_tech)
- [16] Diskrétní signál. *Computer Vision* [online]. [cit. 2015-05-24]. Dostupné z: [http://midas.uamt.feec.vutbr.cz/ZVS/Exercise01/content\\_cz.php](http://midas.uamt.feec.vutbr.cz/ZVS/Exercise01/content_cz.php)
- [17] Cellcrypt. *Inmarsat* [online]. 2013 [cit. 2014-12-09]. Dostupné z: [http://www.inmarsat.com/wp-content/uploads/2013/10/Inmarsat\\_Cellcrypt.pdf](http://www.inmarsat.com/wp-content/uploads/2013/10/Inmarsat_Cellcrypt.pdf)
- [18] Cryptography or Encryption. *Kryptotel* [online]. 2010 [cit. 2014-12-09]. Dostupné z: <http://en.kryptotel.net/encryption.html>
- [19] *GSM Security and Encryption*. [online]. 2010 [cit. 2014-12-09]. Dostupné z: <http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html>
- [20] Korporátní bezpečnost: mobilně šifrovat end-to-end. *Root* [online]. 2013 [cit. 2014-12-09]. Dostupné z: <http://www.root.cz/clanky/korporatni-bezpecnost-mobilne-sifrovat-end-to-end/>
- [21] *Babel*. [online]. 2014 [cit. 2014-12-09]. Dostupné z: <http://getbabel.com/cs/jak-to-funguje>
- [22] *PhoneX*. [online]. 2014 [cit. 2014-12-09]. Dostupné z: <https://www.phonex.net/cz/jak-phonex-funguje>
- [23] *Open Whisper System* [online]. [cit. 2015-05-24]. Dostupné z: <https://whispersystems.org/>
- [24] MARTINEZ, Aitor Sanchoyerto. Evolution towards tetra+lte. In: *Teltronic - Critical Communication* [online]. 2014 [cit. 2015-05-24]. Dostupné z: <http://www.slideshare.net/ASanchoyerto/evolution-towards-tetralte-teltronic-june2014-pub>
- [25] RT-N18U. *Asus* [online]. [cit. 2015-05-24]. Dostupné z: <http://www.asus.com/cz/Networking/RTN18U/>
- [26] *TP-Link* [online]. [cit. 2015-05-24]. Dostupné z: <http://cz.tp-link.com/>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

3G	Označení sítě 3. generace
A/D	Převod analogového signálu na digitální
AES	Advanced Encryption Standard
AP	Access point
ARP	Address Resolution Protocol
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multi Access
DSCP	Distinct Satellite Connection Provider
DSPU	Distinct Services Provider Unite
ESPU	Encription Services Provider Unite
FDD	Frequecy Division Duplex
GSM	Global System for Mobile Communication
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
ISP	Internet Service Provider
LSCP	Local Satellite Connection Provider
NATO	North Atlantic Treaty Organization
NSS	Network and Switching Subsystem
PCM	Pulse-code modulation
PPTP	Point-to-Point Tunneling Protocol
RSA	Iniciály jmen tvůrců (Rivest, Shamir, Adleman)
SIM	Subscriber Identity Module
SHA	Secure Hash Algorithm

SPU	Services Provider Unite
TDD	Time Division Duplex
UMTS	Universal Mobile Telecommunications System
UTRA	UMTS Terrestrial Radio Access
VoIP	Voice over Internet Protocol
W-CDMA	Wideband CDMA
XOR	Exkluzivní disjunkce
ZRTP	Zimmerman Real-time Transport Protocol

**SEZNAM OBRÁZKŮ**

Obrázek 1: Proudová šifra[3].....	12
Obrázek 2: Blokovaná šifra[4] .....	12
Obrázek 3: Princip AES[1] .....	13
Obrázek 4: Asymetrické šifrování[6] .....	14
Obrázek 5: Metoda RSA[2] .....	15
Obrázek 6: Schéma VoIP telefonie[7].....	16
Obrázek 7:schéma GSM[9] .....	17
Obrázek 8: Podstata CDMA[11].....	19
Obrázek 9: Struktura rámce TDD[11].....	20
Obrázek 10: Struktura rámce FDD[11] .....	20
Obrázek 11: Satelitní komunikace SPEROS[13].....	21
Obrázek 12: Převod signálu[16] .....	22
Obrázek 13: PCM typy[10].....	22
Obrázek 14: Zabezpečená infrastruktura[17] .....	25
Obrázek 15: End-to-End spojení přes server .....	26
Obrázek 16: Point-to-Point připojení .....	26
Obrázek 17: Šifrovací síťové prvky[18].....	27
Obrázek 18: Šifrovaný telefon[18].....	27
Obrázek 19: Schéma zapojení.....	30
Obrázek 20: BABEL[21] .....	32
Obrázek 21: Schéma připojení do infrastruktury BABEL[21] .....	32
Obrázek 22: PhoneX[22] .....	33
Obrázek 23: Schéma připojení do infrastruktury PhoneX[22] .....	34
Obrázek 24: Obnova telefonního seznamu při přihlášení .....	35
Obrázek 25: Přenos požadavku.....	36
Obrázek 26: Přenos hlasu .....	36
Obrázek 27: Výpis TCP streamu komunikace .....	36
Obrázek 28: Měření odezvy.....	37
Obrázek 29: Aplikace TextSecure a RedPhone[23].....	38
Obrázek 30: Přenos stavu uživatele .....	39
Obrázek 31: Komunikace pomocí aplikace RedPhone .....	39
Obrázek 32: Zahájení komunikace.....	40

Obrázek 33: Přidělení komunikačních portů .....	40
Obrázek 34: Architektura modernizované sítě Tetra[24] .....	42
Obrázek 35: End-to-End připojení .....	43
Obrázek 36: Princip šifrování v síti GSM[11] .....	44
Obrázek 37: Schéma kombinace komunikačních rozhraní[7] .....	46
Obrázek 38: Schéma kombinace globálního spojení .....	47
Obrázek 39: Postup odeslání zprávy .....	47
Obrázek 40: Schéma přepojení .....	48
Obrázek 41: Inicializační proces .....	48
Obrázek 42: Schéma přepojení .....	49
Obrázek 43: Schéma obnovy šifrovacího hesla .....	50
Obrázek 44: Znázornění rozhraní.....	51
Obrázek 45: Asus RT-N18U[25] .....	63
Obrázek 46: TP-Link TL-SG1005D[26] .....	64
Obrázek 47: TP-LINK TL-WR543G[26] .....	65



**SEZNAM TABULEK**

Tabulka 1: Rozdělení kódování [11] .....	23
Tabulka 2: Měření odezvy PhoneX.....	37
Tabulka 3: Měření odezvy RedPhone .....	41
Tabulka 4: Vybrané technické parametry Asus RT-N18U [25] .....	63
Tabulka 5: Vybrané technické parametry TL-SG1005D [26] .....	64
Tabulka 6: Vybrané technické parametry TL-WR543G[26].....	65

## SEZNAM PŘÍLOH

PŘÍLOHA P I: ASUS RT-N18U .....	63
PŘÍLOHA P II: TP-LINK TL-SG1005D (V4).....	64
PŘÍLOHA P III: TP-LINK TL-WR543G (V2) .....	65
PŘÍLOHA P IV: VZORCE PRO VÝPOČET ODEZVY.....	66
PŘÍLOHA P V: OBSAH DISKU CD .....	67

## PŘÍLOHA P I: ASUS RT-N18U



Obrázek 45: Asus RT-N18U[25]

Tabulka 4: Vybrané technické parametry Asus RT-N18U [25]

Rozhraní	4 x RJ45 pro 10/100/1000/Gigabitový BaseT pro LAN 1 x RJ45 pro 10/100/1000/Gigabitový BaseT pro WAN USB 2.0 x 1 USB 3.0 x 1
Standardy bezdrátové sítě	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IPv4, IPv6
Bezdrátové režimy	Wireless router mode, Range extender mode, Access point mode, Media bridge mode
Signální rychlost	802.11b : 1, 2, 5.5, 11Mbps 802.11g : 6,9,12,18,24,36,48,54Mbps 802.11n : až do 450Mbps 802.11n TurboQAM : up to600Mbps
Typ sítě WAN	Automatická IP, Statická IP, PPPoE (podpora MPPE), PPTP, L2TP  Podpora technologie WAN Bridge  Podpora technologie Multicast Proxy  Podpora technologie Multicast Rate Setting

## PŘÍLOHA P II: TP-LINK TL-SG1005D (V4)



Obrázek 46: TP-Link TL-SG1005D[26]

Tabulka 5: Vybrané technické parametry TL-SG1005D [26]

Rozhraní	5 x 10/100/1000Mbps RJ45 Ports AUTO Negotiation/AUTO MDI/MDIX
Způsob přenosu	Store and Forward
Pokročilé funkce	802.3X Flow Control, Back Pressure Auto-Uplink Every Port

## PŘÍLOHA P III: TP-LINK TL-WR543G (V2)



Obrázek 47: TP-LINK TL-WR543G[26]

Tabulka 6: Vybrané technické parametry TL-WR543G[26]

Rozhraní	4 x porty 10/100 Mbit/s LAN 1 x port 10/100 Mbit/s WAN
Standardy bezdrátové sítě	IEEE 802.11g, IEEE 802.11b
Bezdrátové režimy	Režim směrovače AP (S WDS) Režim směrovače AP klienta (WISP klient)
Signální rychlost	11g: až 54 Mbit/s (dynamická) 11b: až 11 Mbit/s (dynamická)
Typ sítě WAN	Dynamická IP/statická IP/PPPoE/ PPTP/L2TP/BigPond
DHCP	Server, klient, seznam klientů DHCP, rezervace adres

## PŘÍLOHA P IV: VZORCE PRO VÝPOČET ODEZVY

$$\Delta t = t_2 - t_1$$

(3)

Kde:  $\Delta t$  odezva komunikační linky

$t_2$  příjem komunikace

$t_1$  odeslání požadavku

$$v\acute{y}sledna\ odezva = \frac{\sum_{i=1}^n \Delta t_i}{n}$$

(4)

Kde:  $n$  počet měření

$\Delta t$  odezva komunikační linky

$$sm\acute{e}rodatn\acute{a}\ odchylka = \sqrt{\frac{1}{n} * \sum_{i=1}^n (\Delta t_i - v\acute{y}sledn\acute{a}\ odezva)^2}$$

(5)

Kde:  $n$  počet měření

$\Delta t$  odezva komunikační linky

## PŘÍLOHA P V: OBSAH DISKU CD

