Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Moderní protokoly pro P2P sítě

Bakalářská práce

Autor: Libor Novotný
Studijní obor: Informační management

Vedoucí práce: Ing. Karel Mls, Ph.D.

Hradec Králové Duben 2023

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 21.4.2023 _____

Poděkování:
Děkuji vedoucímu bakalářské práce Ing. Karlu Mlsovi, Ph.D. za metodické vedení práce a poskytnutí odborných konzultací.

Anotace

Tato bakalářská práce je v úvodu zaměřená na stručný popis historie sítí a základních síťových modelů TCP/IP a ISO/OSI. Dále se věnuje základním rozdílům mezi sítěmi typu klient-server a klient-klient neboli P2P. Hlavním tématem je popis problematiky P2P sítí a jejich protokolů. Dále je tato práce věnována některým vybraným nejznámějším P2P protokolům a snaží se zodpovědět otázky jak tyto protokoly fungují, jak je řešeno jejich zabezpečení a k čemu jsou tyto protokoly nejvhodnější. Nakonec se tato práce věnuje možnému využití P2P sítí v blízké budoucnosti, jako je například uplatnění v chytrých domácnostech. Výsledkem této práce je seznámení čtenáře s problematikou P2P sítí, pochopení funkce P2P protokolů a dozvědět se o výhodách a nevýhodách jejich použití, případně kde všude se využívají.

Annotation

Title: Modern protocols for P2P networks

This bachelor's thesis is initially focused on a brief description of the history of networks and the basic network models TCP/IP and ISO/OSI. It also covers the basic differences between client-server and client-client or P2P networks. The main topic is the description of P2P networks and their protocols. Furthermore, this work is devoted to some selected best-known P2P protocols and tries to answer the questions of how these protocols work, how their security is solved and what these protocols are best suited for. Finally, this work addresses the possible use of P2P networks in the near future, such as application in smart homes. The result of this work is to introduce the reader to the issue of P2P networks, to understand the function of P2P protocols and to learn about the advantages and disadvantages of their use, or where they are used.

ObsahS

1 Úvod 1

2 Cíl práce 2

3 Metodika zpracování 3

4 Vlastní text práce 6

4.1 Účel sítí 6

4.2 Historický vývoj sítí 7

4.3 Základní síťové modely 8

4.3.1 ISO/OSI model 8

4.3.2 TCP/IP model 10

4.4 Sítě klient-klient a klient-server 11

4.5 Možná řešení P2P sítí 13

4.6 Bezpečnost P2P sítí 14

4.7 Protokoly P2P sítí 16

4.7.1 Nejznámější programy využívající P2P protokoly 17

4.8 Možnosti využití P2P protokolů v blízké budoucnosti 24

5 Shrnutí výsledků 26

5.1 Počátek sítí a základní rozdělení 26

5.2 Porovnání sítí klient-server a klient-klient 27

5.3 Možná řešení P2P sítí a jejich zabezpečení 28

5.4 Porovnání P2P protokolů a možný vývoj do budoucna 29

5.4.1 Protokoly pro sdílení dat 30

5.4.2 Další P2P protokoly 34

5.4.3 Výhled do budoucna 39

6 Závěry a doporučení 40

7 Seznam použité literatury 41

Seznam obrázků

Obrázek 1 Mapa ARPANETu (1980) 6
Obrázek 2 Referenční model ISO/OSI 8
Obrázek 3 ISO/OSI model 9
Obrázek 4 Porovnání ISO/OSI a TCP/IP modelu 10
Obrázek 5 Rozvržení sítě klient-server 10
Obrázek 6 Rozvržení sítě klient-klient 11

Seznam tabulek

Tabulka 1 Protokoly P2P sítí 14
Tabulka 2 Porovnání verzí Bluetooth 19

1 Úvod

Počítačové sítě jsou v dnešní době kritickou části infrastruktury. Jsou využívány téměř ve všech možných odvětvích lidské činnosti, jako je například výzkum, podnikání, zábava a mnoho dalších.

Jak ale počítačové sítě fungují, jaké jsou mezi nimi rozdíly, jaké existují protokoly, nebo jaké problémy je potřeba řešit při jejich používání? Tuto problematiku se pokusím přiblížit pomocí této práce.

2 Cíl práce

Představit a porovnat moderní P2P protokoly a zhodnotit jejich praktickou využitelnost.

3 Metodika zpracování

K dosažení cílů této práce budou použity rešerše odborných zdrojů, případně analýza odborných článků nebo jiných odborných materiálů. V případě čerpání informací z internetových stránek budou data ověřována na základě více zdrojů. Závěry budou vyhodnoceny na základě zpracovaných informací.

Literární rešerše

Austin Halliday se v práci nazvané „Peer-to-Peer Networking: Explanations, Applications, and Implications“ zabývá různými kategoriemi sítí a peer-to-peer sítěmi, které se v těchto kategoriích nacházejí. Dále se snaží čtenáři přiblížit, jak tyto sítě fungují a jaké překážky musejí zvládnout. Hlavním cílem tohoto autora je zvýšit povědomí o této problematice a zhodnotit využitelnost a zvážit rizika při používání těchto protokolů.

Autor postupně představuje jednotlivé oblasti využití, vysvětluje jejich fungování a zmíní i některé programy, které v dané kategorii pracují.

Autor nakonec dospěje k závěru, že peer-to-peer sítě mají velký potenciál, ovšem musí se dávat pozor na nebezpečí zneužívání peer-to-peer sítí pro ilegální šíření souborů a verbální urážení na diskusních fórech. Závěrem je, že pro vzdělaného administrátora můžou být peer-to-peer sítě dobrým nástrojem [44].

Autoři práce s názvem „Resolving Problems Based on Peer to Peer Network Security Issue's“ se zabývají problematikou bezpečnosti na peer-to-peer sítích. Autoři krátce představili, co jsou P2P sítě, dále uvádějí možná rizika. Poté se věnují metodám zabezpečení a předcházení rizikům. Také popisují problémy, které mohou v zabezpečení nastat.

Autoři nakonec dospěli k závěru, aby se předešlo možnému zneužití dat a dalším rizikům, bylo by zapotřebí centrální autority, která by kontrolovala pravost původních dat a zasílaných dat, tak aby nedocházelo k pozměnění v průběhu přenosu. Dále uvádějí, že se těmto problémům budou věnovat i v budoucnu [11].

Phillip Kisembe a Wilson Jeberson se v práci nazvané „Future of peer-to-peer technology with the rise of cloud computing“ zaměřují na budoucnost peer-to-peer technologie s nástupem cloud computingu.
Nejdříve seznámí čtenáře s historií P2P technologii. Následně informují o evoluci P2P protokolů sloužící ke sdílení dat, jako je Napster, Gnutella, Kazaa, Bit-Torrent. Dále se věnují P2P streamování videa a distribuovaným sociálním sítím. Poté následuje kapitola věnovaná porovnání P2P s ostatními technologiemi. Také upozorňují na hlavní výzvy P2P technologii.
Nakonec došli k závěru, že P2P je stále populární a lze využít i v cloud computingu. Dále upozorňují na důležitost P2P technologie [45].

Satoshi Nakamoto popisuje v práci „Bitcoin: A Peer-to-Peer Electronic Cash System“ využití P2P technologie k provádění transakcí. Nejdříve specifikuje problémy s důvěryhodností při provádění transakcí jak fyzických, tak elektronických. Dále popisuje systém provádění transakcí a ověřování důvěryhodnosti těchto transakcí. Poté se věnuje problematice systému „Proof-of-Work“, kde popisuje princip kontroly pomocí matematických operací. Také popisuje model sítě, kde probíhají transakce, model ukládání na disku, zjednodušené ověřování plateb a spojování a rozdělování hodnot. Ke konci práce se autor věnuje ještě problematice soukromí a popisuje matematické výpočty. Autor došel k závěru, že popsal rámec na provádění transakcí, který je nezávislý na důvěře, má dohledatelnou historii transakcí a je odolný vůči zneužití [22].

Karl Molin se ve své práci „Measurement and Analysis of the Direct Connect Peer-to-Peer File Sharing Network“ zaměřuje na studium protokolu Direct Connect, který slouží ke sdílení obsahu po internetu pomocí P2P sítě. Data vycházejí z uživatelských statistik. V úvodu autor vyjmenuje různé využití protokolů a programů na internetu. Následně se věnuje ostatním pracím, které ho inspirovaly k této studii. Po úvodu se věnuje základním principům P2P sítě, kde tuto problematiku přiblíží, také se věnuje oblasti architektury P2P sítí. Následuje vysvětlením principu protokolu Direct Connect. Věnuje se oblastem jako je architektura protokolu, možné role prvků v síti tohoto protokolu a jeho možné režimy. Také vysvětlí detailněji samotné fungování tohoto protokolu.

Po vysvětlení problematiky se autor věnuje proceduře tvorby síťových grafů. Další kapitolu autor věnuje popisu měření sítě Direct Connect. Také vysvětluje práci s nástroji použitými k získání analytických dat. V další části se věnuje analyzování dat a diskuzi nad získanými výsledky.

Závěrem autora je upozornění, že studie, kterou provedl je možná první svého druhu, zároveň se mu podařilo vytvořil detailnější obraz fungování protokolu a zmapování komunikace po síti Direct Connect [27].

Autoři práce „Private Communication Through a Network of Trusted Connections: The Dark Freenet“ se věnují problematice protokolu Freenet, který má umožňovat svobodnou komunikaci mezi uživateli. Nejdříve přiblíží podstatu protokolu Freenet a zmíní předchozí práce. Dále se věnují popisu funkcionality protokolu, kde popisují detaily navazování spojení, získávání a odesílání dat, ověřování klíči a získávání dokumentů. Také detailněji popisují proces šifrování a ukládání dat. Dále popisují proces tvorby simulací, ze kterých získali analytická data. Nakonec se věnují problematice implementace nové verze protokolu. Také rozebírají problematiku anonymity a soukromí.

Autoři došli k závěru, že se jim podařilo popsat novou verzi protokolu Freenet, který je založen pouze na důvěryhodných spojích. Autoři se také domnívají, že představili nový koncept P2P, který zaručuje soukromí uživatelů a pevné základy pro tvorbu komunikační sítě [30].

4 Vlastní text práce

4.1 Účel sítí

Počítačová síť je propojení dvou a více zařízení, která jsou schopna spolu komunikovat, navzájem si sdílet informace a data nebo například nabízet své funkce pomocí síťových protokolů [1]. Hlavním důvodem, proč vůbec počítačové sítě vznikly a proč jsou tak masově využívány, je lidská potřeba sdílet informace. V současnosti je kromě sdílení informací dalším důležitým faktorem využívání sítí vzájemná propojenost infrastruktur a různých systémů a zařízení. Kvůli ulehčení složitosti těchto různých propojení dělíme počítačové sítě podle mnoha hledisek, například podle jejich **velikosti** [2]

- LAN – Local Area Network – místní síť, jsou v ní zahrnuty počítače a zařízení, v rámci jedné budovy, domácnosti, či firemní pobočky
- PAN – Personal Area Network – osobní síť, patří do ní propojená zařízení v malé vzdálenosti, nejčastěji do 10 m, nejčastějším příkladem jsou zařízení propojená pomocí Bluetooth
- MAN – Metropolitan Area Network – počítačová síť, která většinou svojí velikostí pokrývá plochu města nebo regionu, většinou se jedná o několik propojených sítí LAN
- WAN – Wide Area Networ – velké sítě, svojí velikostí pokrývají celé státy nebo i kontinenty, může se jednat i o internet, jako celek.

logické topologie [3]

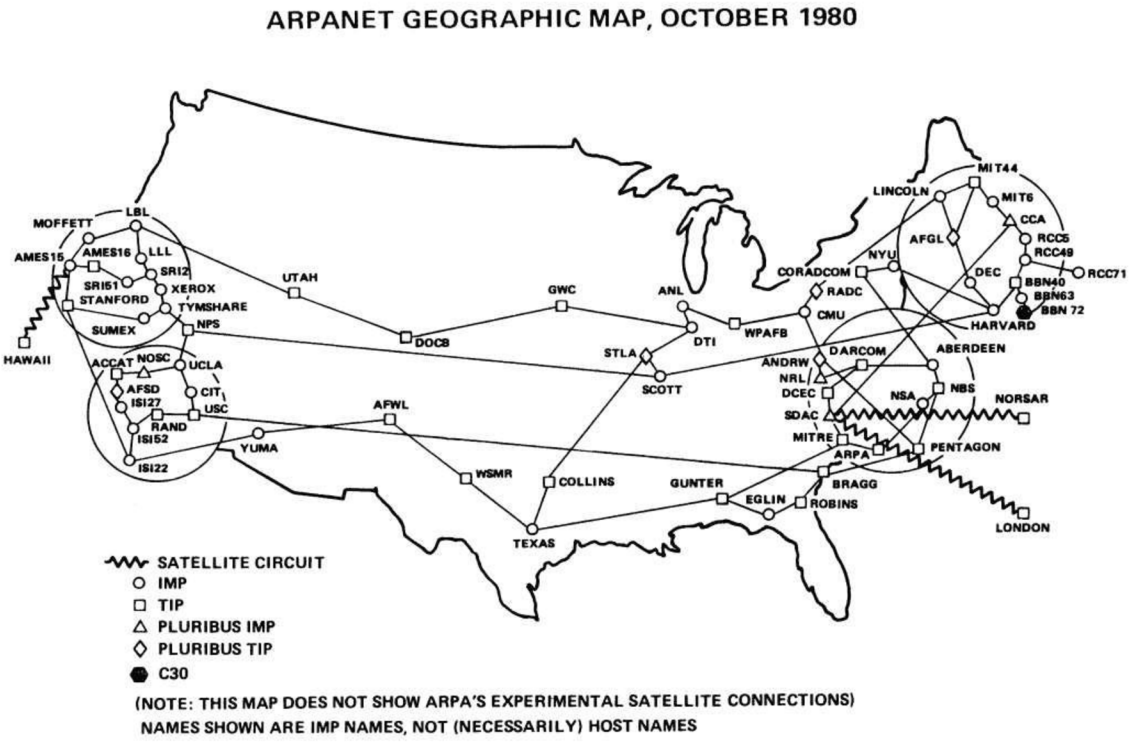
- Point-to-Point – propojení bod-bod, jedná se o přímé propojení dvou zařízení
- Bus – sběrnice, zařízení jsou zapojena k jedné centrální lince, jedná se o nejstarší topologii, která se dnes již moc nevyužívá.
- Star – hvězda, dnes jedna z nejčastějších topologii, prvky jsou navzájem propojeny pomocí jednoho centrálního prvku, kterým může být síťový prvek, jako např. switch nebo hub nebo také server
- Mesh – propojení každého zařízení s každým, tento druh sítě je nejspolehlivější díky množství redundantních spojů, zároveň je také nejsložitější
- Ring – kruh, každý prvek je propojen v sérii s následujícím prvkem do kruhu
- Tree – strom, několik topologií typu hvězda propojených dohromady (jsou propojeny centrální prvky)

nebo dle **úlohy prvků sítě** (Klient-server, Klient-klient – toto rozdělení je jedním z hlavních témat této práce)

4.2 Historický vývoj sítí

Nejdříve, než si přiblížíme dnešní sítě, je potřeba si ujasnit, jak tyto sítě vznikly. Nejstarší počítačové sítě začaly vznikat jako propojení jednoho centrálního počítače s terminály, jednalo se o terminálové sítě, následovalo propojení více samostatných počítačů, nejprve v rámci LAN, následně, když byly postupně připojovány i vzdálenější počítače tak došlo ke vzniku prvních WAN.

Nejstarší počítačové sítě vznikly pro vojenské účely, jedna z prvních se objevila již v druhé polovině 50. let 20. století. Jednalo se o propojení radarové sítě armády USA. První rozlehlejší sítě začaly vznikat v 60. letech. Jednou z nejvýznamnějších sítí, která dala vzniknout modernímu internetu byl ARPANET (viz obr. 1).



Obrázek 1 Mapa ARPANETu (1980) [48]

ARPANET byl spuštěn v roce 1969, vznikl na žádost ministerstva obrany USA, které potřebovalo umožnit fungování vládních složek USA i v případě jaderné války, proto jednotlivé uzly měly být na sobě nezávislé, pro případ, že by byla některá část zničena. Při spuštění obsahoval ARPANET čtyři uzly, které se nacházely na univerzitách v Los Angeles, Santa Barbaře, Stanfordu a v Utahu. V následujících letech se síť začala rozrůstat, místo čistě vojenských účelů se začala využívat ke

sdílení vědeckých poznatků. V roce 1973 se k ARPANETu připojily první zaoceánské sítě, Velká Británie a Norsko. V roce 1983 se ARPANET propojil se sítí CSNET, která sloužila čistě pro vědecké účely. Téhož roku se armádní část oddělila a vytvořila vlastní síť nazvanou MILNET. Od téhož roku, až do roku 1986 došlo k implementaci síťového protokolu TCP/IP, který sjednotil komunikaci v rámci celé sítě. V roce 1986 vznikla i síť NSFNET, která převzala roli ARPANETu, a v roce 1990 byl ARAPANET vypnut. Některé jeho části se ale staly součásti dnešního internetu, který existuje od 80. let minulého století [4, 5].

4.3 Základní síťové modely

4.3.1 ISO/OSI model

ISO/OSI model (obr. 2) byl vytvořen standardizační organizací ISO v roce 1979. Společně s modelem TCP/IP se jedná o jeden z nejpoužívanějších síťových standardů. ISO/OSI model se skládá ze 7 vrstev, které na sebe navazují. Každá vrstva má za úkol jinou část síťové komunikace (obr. 3).

Nejníže se nachází **Fyzická vrstva**, sem patří podoba fyzického signálu, typy přenosových médii a konektorů.

Další je **Linková vrstva**, která se zabývá spojováním jednotlivých bitů do tzv. rámců (frame). Následně tyto rámce kontroluje, aby nedocházelo k chybám. Pokud dojde k poškození rámce musí tato vrstva poslat upozornění odesílateli, aby rámec odeslal znovu. Linková vrstva zvládne komunikovat pouze na přímých spojích.

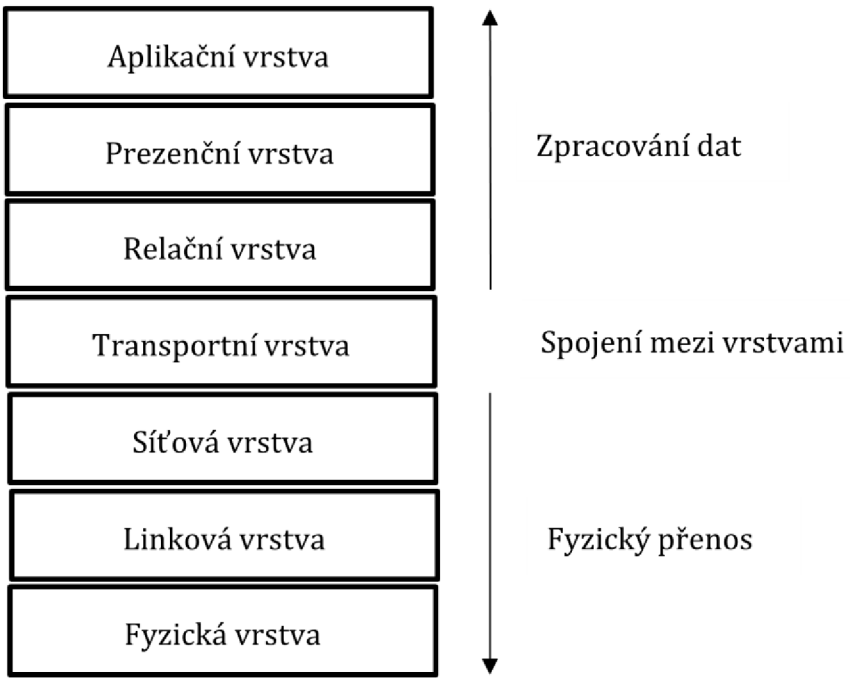
Komunikaci v rámci sítě zajišťuje **Síťová vrstva**. Ta z rámců skládá packety tím, že přidá ještě informace o IP adresách příjemce a odesílatele a doplňkové informace, jako může být informace, kdo řídí komunikaci. Do této vrstvy spadá Směrování (routing), to rozhoduje, jak se data dostanou skrze síť od odesílatele k příjemci. Mezi tyto rozhodovací procesy patří i výpočet nejvhodnější cesty.

Uprostřed modelu se nachází **Transportní vrstva**. Tato vrstva se zabývá skládáním packetů do balíčků dat a jejich rozkládáním dle směru komunikace. Tato vrstva umožňuje přenos dat mezi spodními fyzickými vrstvami a vrchními logickými. Umí rozpoznat, jaká data jsou určena, pro jaký program a následně mu je předat k dalšímu zpracování.

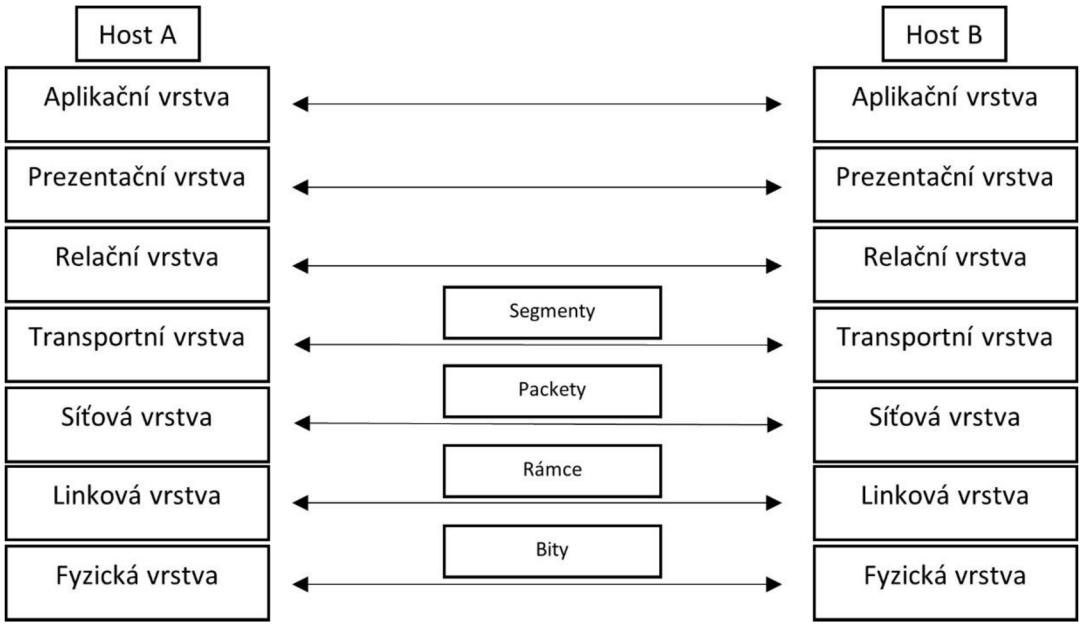
Relační vrstva se stará o navázání, udržování a ukončení komunikace mezi jednotlivými síťovými uzly. Také rozhoduje, jestli komunikace bude jednosměrná (half duplex) nebo obousměrná (full duplex). Může se také rozhodnout, kdy bude komunikace šifrovaná.

Prezentační vrstva funguje jako překladatel. Stará se o překládání dat z Aplikační vrstvy pro nižší vrstvy a naopak.

Nejvyšší **Aplikační vrstva** se stará o poskytování síťových služeb aplikacím. Nestará se ale o celé aplikace, ale pouze o jejich programové části. Proto součástí Aplikační vrstvy není uživatelské rozhraní [6].



Obrázek 2 Referenční model ISO/OSI [49]

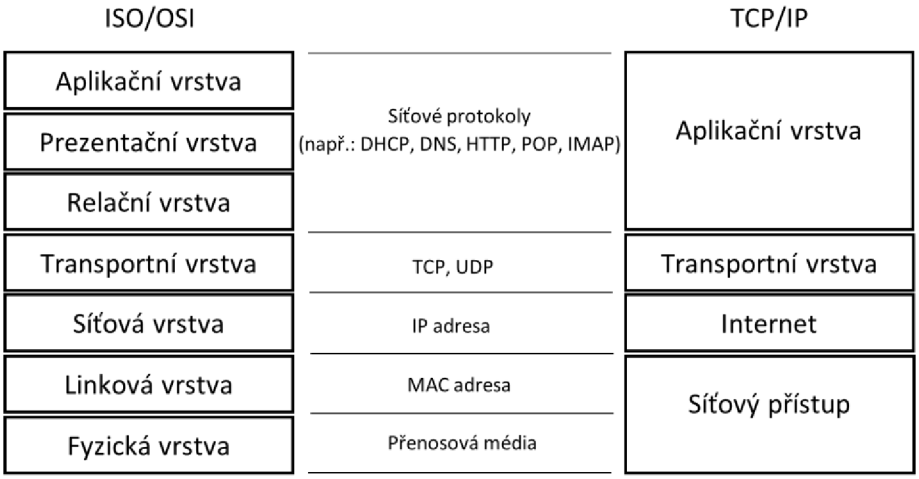


Obrázek 3 ISO/OSI model [50] - upraveno

4.3.2 TCP/IP model

TCP/IP sdružuje sadu protokolů nutnou pro komunikaci po síti. Zároveň se jedná o světově nejvíce využívaný protokol pro komunikaci v rámci internetu. TCP/IP byl vyvíjen pod organizací DARPA, která patří pod americké ministerstvo obrany. První myšlenka pochází z roku 1972, cílem bylo vytvořit nový standardizovaný protokol pro komunikaci v rámci ARPANETu. V průběhu 70. let a začátkem 80. let probíhal výzkum a experimenty s TCP/IP protokoly. Od 1. ledna 1983 se TCP/IP začal plně využívat a dostal současnou podobu.

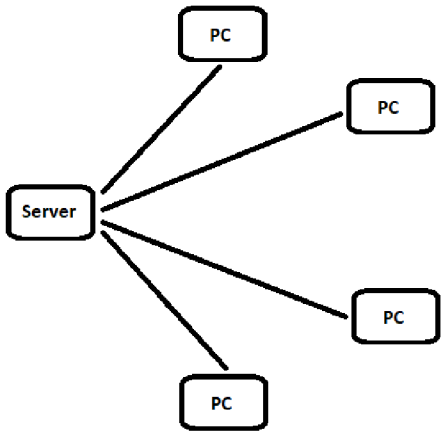
TCP/IP model má pouze 4 vrstvy (ISO/OSI model má 7): aplikační, transportní, síťová a síťové rozhraní. Funkce jednotlivých vrstev TCP/IP odpovídají několika vrstvám ISO/OSI modelu (viz obr. 4) [7, 8].



Obrázek 4 Porovnání ISO/OSI a TCP/IP modelu [51] - upraveno

4.4 Sítě klient-klient a klient-server

Sítě typu klient-server (obr. 5) se skládají z klientů (koncových zařízení), která posílají dotazy (nejčastěji přes webový prohlížeč) hostitelskému serveru, který buď sám zašle odpověď nebo dotaz přesměruje dál na další server, nebo jiný prvek, dokud se nenalezne klientem požadovaná odpověď. Klient je v této síti aktivním prvkem, který zasílá dotazy a čeká na odpovědi, server je pasivní prvek, který čeká na dotaz a zasílá odpověď. Klient je typicky připojen najednou k více serverům.

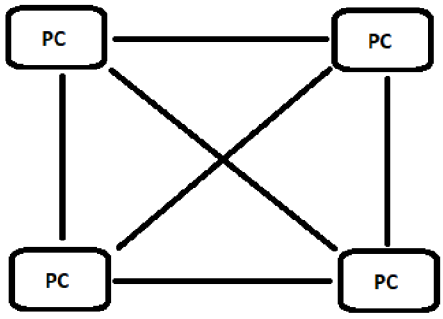


Obrázek 5 Rozvržení sítě klient-server Zdroj: autor

Komunikace v takové síti je často brzděna tím, že dotazy i odpovědi musí projít skrze server, kterému často hrozí zahlcení množstvím dotazů. Takto zahlcený server má delší odezvu a tím negativně ovlivňuje rychlost sítě. Hlavní výhodou sítě klient-server je její přehlednost a uspořádanost. Pokud se klient dotazuje, je dotaz rychle

přesměrován na konkrétní server, který dokáže dotaz obsloužit. Hlavními nevýhodami je velká finanční náročnost na pořízení a provoz serveru, další velkou nevýhodou je stabilita takové sítě, protože pokud vypadne server, který je hlavním prvkem této sítě, celá takováto síť přestane fungovat [9].

Protikladem je zapojení sítí klient-klient (obr. 6) (též peer-to-peer nebo P2P, tato zkratka bude využívána ve zbytku této práce). V této síti si jsou všechna zařízení rovna, to znamená, že každé zařízení může být v roli hosta i serveru. Toto zapojení je jednodušší než architektura klient-server, často je i komunikace mezi jednotlivými zařízeními rychlejší. Dalšími výhodami je větší robustnost těchto sítí, protože pokud vypadne jeden prvek, je možné v rámci takto vytvořené sítě nalézt alternativní. Další nespornou výhodou tohoto typu sítě jsou i menší náklady na provoz, jelikož je síť tvořena samotnými uživateli, proto tento typ sítě často využívá mnoho freeware programů. Často se využívá ke sdílení souborů mezi uživateli, ale hlavním problémem těchto sítí je, že jednotlivá zařízení nejsou často uspořádaně propojená (propojení mezi jednotlivými zařízeními v P2P síti je často náhodné), proto čím je propojených více zařízení, tím déle trvá prohledání sítě k nalezení požadované odpovědi (požadovanou odpověď obsahuje většinou pouze jeden konkrétní síťový uzel) a tím dochází k prodloužení odezvy a delšímu navazování spojení oproti síti typu klient-server, kde všechny dotazy jdou přes server (který je zároveň centrálním uzlem sítě) [10].



Obrázek 6 Rozvržení sítě klient-klient Zdroj: autor

4.5 Možná řešení P2P sítí

Jedním z řešení nestrukturovaných P2P sítí jsou strukturované P2P sítě, ve kterých jsou jednotlivé prvky členěny do topologie (můžeme uvažovat třeba stromové, hvězdicové a další). Aby v takové síti mohla komunikace probíhat efektivně, tak každý uzel musí znát seznam svých sousedů s jejich kritérii pro vyhledávání. V praktickém použití to znamená velmi velké a datově objemné seznamy, kterými musí disponovat každý klient. Kvůli těmto zásadním problémům je rozšířenějším řešením, kdy klient disponuje pouze základními daty o sobě a případně o svých nejbližších sousedních uzlech, v takovém případě je ale vyhledávání časově velmi náročné, jelikož pokud klient nenalezne požadovaná data u sousedních uzlů, musí dotaz pokračovat systematicky řetězově dál skrze síť, dokud není nalezen požadovaný uzel s hledanou odpovědí. Poté je teprve navázáno datové propojení a je umožněna následná výměna dat. Toto řešení je i přes svoji hlavní nevýhodu v podobě vyšší počáteční odezvy pro mnoho uživatelů daleko přijatelnější, než aby museli mít ve svém zařízení uložené záznamy o všech uzlech které existují v dané P2P síti. Tento přístup je i lepší z pohledu bezpečnosti, jelikož pokud je jeden uzel napaden, útočník stále nemá jednoduchý přístup k celé síti, protože stále nebude mít přehled o celé síti.

Dalším možným způsobem, jak zlepšit propojení mezi zařízeními nebo uzly je Hybridní model. Tento model využívá výhod propojení klient-server i klient-klient. Počáteční vyhledávání v síti probíhá přes server, který disponuje informacemi o všech ostatních uzlech. Když server nalezne v síti požadovaný spoj, komunikace přejde na propojení typu klient-klient. Tímto řešením se urychlí prohledávání sítě, dále toto řešení má pozitivní vliv na rychlost, odezvu a vytížení sítě, jelikož následně jednotlivé prvky komunikují přímo bez další účasti serveru a nevytěžují danou síť velkým množstvím dotazů (příkladem tohoto přístupu může být Skype) [10].

4.6 Bezpečnost P2P sítí

Jako všechny sítě, i P2P sítě musí v dnešní době řešit otázku zabezpečení komunikace a uživatelů, kteří využívají tuto technologii. Vývojáři P2P protokolů musí brát v potaz spousty možný hrozeb, jako jsou: odposlouchávání komunikace, DDoS útoky, Sociální inženýrství a různý Malware.

Nejčastějším řešením těchto problémů je šifrování komunikace. V tomto ohledu existují dva hlavní směry. Jedním je šifrování a skrývání veškeré uživatelské komunikace po síti, tak aby nebylo poznat, která data se týkají P2P komunikace, a případný útočník nepoznal, která data chce odposlouchávat. Další metodou je šifrování dat pouze v rámci daného komunikačního protokolu, klíčem k jejich rozšifrování potom disponují pouze uživatelé, kterým byla tato data zaslána, klíč jim je předán pomocí Diffieho-Hellmanovy výměny klíčů [46].

Dalšími možnostmi zabezpečení P2P sítí jsou klasická opatření, která jsou dnes běžná pro většinu programů.

Základním opatřením je identifikace uživatele na základě jména a hesla, také může být použit speciální token nebo jiné metody ověření.

Dále je důležitá ochrana soukromí, jelikož pro vyšší bezpečnost je lepší anonymita uživatelů a ochrana jejich skutečné identity. Nejjednodušší implementací tohoto pravidla je například přihlašování pomocí přezdívky, většina programů zároveň zvládá šifrovat uživatelovu IP adresu, aby nemohl být na jejím základě lokalizován.

Dalším podstatným bodem je zajištění integrity dat. Tato vlastnost musí zajistit, že data jsou původní. Data musí být chráněna před jakýmkoli neautorizovaným přístupem. Pokud by k takovému přístupu mohlo dojít, podstatně se zvyšuje riziko, že by některý útočník mohl mezi sdílená data vložit vlastní kód, který může jakýmkoliv způsobem poškodit koncové uživatele nebo úplně změnit význam sdílených dat.

Uživatelská přívětivost programu je také vhodnou částí zabezpečení. Uživatel by při používání programu měl vědět co přesně dělá, aby věděl, jaké zabezpečení zrovna využívá případně byl schopen vše správně nastavit. Toto opatření napomáhá eliminaci zbytečných rizik, jako může být chybějící nebo příliš slabé heslo.

Lehce pokročilejší metodou zabezpečení je řízení přístupu, to má na starost filtrovat vyžádanou a nevyžádanou komunikaci a zabraňovat nevyžádaným datům v přístupu. Tuto činnost má typicky na starosti firewall, ten může být zabudovaný na různých místech. Nejčastěji je přímo součástí operačního systému, dále může být na různých síťových zařízení, jako jsou routery a switche, dále se dá také využít firewall jako fyzicky samostatné zařízení (nejčastěji se s tímto řešením můžeme setkat u firemních sítí). Firewall se také může nacházet přímo v některých programech (jako může být Antivirus, nebo některé VPN klienty) [11].

4.7 Protokoly P2P sítí

Příklady známějších P2P protokolů:

Tabulka 1 Protokoly P2P sítí [52] – upraveno

Název protokolu	Příklad programu	Účel programu
Advanced Peer-to-Peer Networking (APPN)	Systems Network Architecture	Správa zařízení
Bitcoin	Bitcoin	Transakce
BitTorrent	BitTorrent, µTorrent	Sdílení souborů
Direct Connect	ApexDC++, BCDC++	Sdílení souborů
eDonkey	eMule, FileScope	Sdílení souborů
FastTrack	MLDonkey, XNap	Sdílení souborů
Freenet	Freenet	Anonymní komunikace
Gnutella	WireShare	Sdílení souborů
Gnutella2	Shareaza	Sdílení souborů
IRC (XDCC)	Weechat, Xchat	Chat /Sdílení souborů
OpenFT	MLDonkey	Sdílení souborů
OpenNap	WinMX	Sdílení souborů
Overnet	XNap	Sdílení souborů
WebTorrent	WebTorrent Desktop	Sdílení souborů
WinMX Peer Networking Protocol	WinMX	Sdílení souborů
Skype	Skype	Videohovory/komunikace

4.7.1 Nejznámější programy využívající P2P protokoly

- ***BitTorrent***

Jedním z nejpoužívanějších protokolů je BitTorrent. Ten se využívá ke sdílení souborů, díky využití decentralizovaného P2P mohou být soubory stahovány poměrně vysokou rychlostí, proto se tento protokol využívá především pro sdílení velkých objemů dat, jako mohou být celé programy nebo objemné soubory. K využití tohoto protokolu je zapotřebí, aby uživatel měl nainstalovaného BitTorrent klienta a připojení k internetu.

Nejznámějším klientem je klient přímo od společnosti BitTorrent, Inc., která protokol vyvinula. BitTorrent klient je také dostupný i od jiných vydavatelů, jako je třeba µTorrent, tento klient je nejvíce rozšířený mezi uživateli.

Společnost BitTorrent, Inc., která je zodpovědná za vývoj protokolu v současné době patří pod společnost Rainberry, Inc., která vlastní i klienta µTorren a několik dalších BitTorrent klientů.

Protokol navrhl Bram Cohen, první verze byla vydána v roce 2001. V současné době existuje 7. verze.

BitTorrent protokol funguje tak, že jeden uživatel nasdílí soubor, ten je k dispozici ke stažení ostatními uživateli. Když si tento soubor někdo stáhne, může být jeho zařízení využito jako další bod, ze kterého daný soubor lze stáhnout. Z toho vyplývá, že čím více uživatelů si daný soubor stáhne, tím rychleji lze daný soubor stahovat. Zároveň pokud si chce někdo další tento soubor stáhnout, je přepojen na nejbližší dostupný bod. To je výhodou, protože díky decentralizaci není síť tolik vytížená, oproti stahování z jednoho centralizovaného serveru.

Jedním z hlavních problémů protokolu BitTorent je, že je často zneužit uživateli ke sdílení souborů, které je v rozporu s autorským právem. Z tohoto důvodu si velká část uživatelů spojuje BitTorent s pirátským obsahem. Tento protokol je ale využíván mnohými společnostmi. Například na základě tohoto protokolu bývají distribuovány aktualizace softwaru, konkrétně třeba počítačových her. Dalším častým využitím protokolu BitTorrent jsou různé streamovací služby, kde si mohou uživatelé stáhnou sdílený obsah, např. pro přehrávání offline.

Jedním z velkých problému protokolu BitTorrent je, že uživatel může vidět IP adresy ostatních uživatelů BitTorrent klienta, kteří jsou na stejné úrovni jako on. Z tohoto důvodu jsou uživatelé náchylní k různým počítačovým útokům. Z tohoto důvodu v současnosti existují BitTorrent klienti, kteří dokážou skrýt identitu uživatele, třeba pomocí VPN, nebo díky různému přesměrovávání spojení. Tyto řešení ale zpomalují rychlost stahování [12, 13, 14, 15].

- ***Skype***

Dalším z běžně rozšířených programů, který využívá výhod P2P protokolů je Skype. Tento program slouží především pro video komunikaci v reálném čase.
Skype patří mezi freeware, tudíž je jeho používání zcela zdarma, a stal se jedním z velkých konkurentů tradičních operátorů, kteří poskytují placené služby.
První verze programu Skype se objevila již v roce 2003. Jeho název je odvozen ze „Sky peer to peer“. Zakladatelé původní firmy Skype byli Niklas Zennström a Dane Janus Friis. Ti již v této době provozovali službu Kazaa, která sloužila k P2P sdílení souborů přes internet. Z této myšlenky vychází i nápad uskutečňování videohovorů přes internet pomocí P2P protokolu, ze kterého se stal Skype.
V roce 2005 byla vydána verze 2.0, která zásadně přepracovala vzhled aplikace, a umožnila snadnější a přehlednější ovládání rozhraní. Tím se Skype stal dostupnějším pro širší veřejnost a vzrostla jeho popularita. Díky této popularitě byl zakoupen firmou eBay za 2,5 miliardy dolarů. V roce 2010 se objevila mobilní verze na systémech Android a iOS. V roce 2011 byl Skype zakoupen firmou Microsoft za 8,5 miliardy dolarů.
Hlavní technologie, na které se protokol Skype zakládá je VoIP. VoIP umožňuje přenášet hovory místo klasických telefonních linek, pomocí internetové sítě. Jelikož Skype patří mezi P2P protokoly, tak hovory nejdou od volajícího přes servery Skypu k volanému, ani přímo mezi koncovými uživateli, ale protokol Skypu se snaží najít mezi koncovými uživateli nejlepší možnou cesto přes uzly, které jsou tvořeny ostatními uživateli Skypu. Díky tomuto řešení nedochází k zahlcení sítě. Někteří uživatelé jsou využiti jako super uzly, to znamená, že slouží jako rozcestníky mezi cestami, přes které se mohou uživatelé spojit. Aby uživatel v této síti uzlů figuroval,

musím mít na svém zařízení zapnutý Skype, jinak samozřejmě do této sítě zapojen není [16, 17, 18, 19].

- ***Bitcoin***

Bitcoin využívá P2P protokoly k provádění plateb mezi jednotlivými uživateli. Konkrétně využívá decentralizovaný systém propojení, kde je využitá síť uzlů, které představují jednotlivá uživatelská zařízení k ověření legitimnosti platby. Zároveň tím vzniká systém odolný vůči cenzuře, který dovoluje provést jakoukoliv platbu, bez jakýchkoliv překážek.

Bitcoin je první blockchainová síť (Blockchain je decentralizovaný databázový systém, který obsahuje stále se rozšiřující seznam záznamů. V tomto případě se jedná o účetní knihy, které obsahují záznamy o transakcích všech uživatelů, zároveň zachovávají anonymitu těchto uživatelů, také jsou odolné vůči jakýmkoliv zásahům z vnějšku i zevnitř systému), která obsahuje tzv. „Proof of Work" blockchainový mechanizmus kde se počítače podílí na řešení matematických rovnic, za které získávají odměny, v tomto případně jednotky Bitcoinu. Dnes je tato činnost známá jako těžba kryptoměn.

Zdrojový kód Bitcoin protokolu je šířen pod open source licencí, díky tomu je Bitcoin udržován komunitně, a má velkou podporu [20, 21, 22, 23].

- ***APPN***

APPN (Advanced Peer-to-Peer Networking), je protokol vytvořený firmou IBM.

Tvoří součást architektury SNA (Systems Network Architecture). Pomocí protokolu APPN lze vytvářet P2P sítě, bez nutnosti přímého propojení. Hlavní vlastností tohoto protokolu je dynamické vytváření nejvhodnějších cest mezi propojenými body, zvolenou cestu dokáže průběžně měnit, tak aby bylo zachováno co nejlepší spojení. Každá vytvořená APPN cesta obsahuje kompletní mapu sítě včetně routrů a propojení. Díky těmto informacím lze vybrat nejvhodnější trasu [24].

- ***Bluetooth***

Bluetooth je bezdrátový P2P protokol, jeho hlavním účelem je poskytovat datové propojení mezi dvěma zařízeními. V současnosti se s technologii Bluetooth nejčastěji setkáme ve spojitosti s mobilními telefony a nositelnou elektronikou (chytré hodinky, bezdrátová sluchátka), kde zajišťuje vzájemné propojení. Také tuto technologii využívají některé televizory pro připojení dálkového ovladače, jelikož na rozdíl od infračerveného ovladače není potřeba mířit přímo na televizor. Technologie Bluetooth má samozřejmě daleko širší využití než jenom jmenované, obecně se hodí všude, kde je potřeba si vyměňovat navzájem data o malém objemu, to především kvůli nízké rychlosti tohoto protokolu, která u Bluetooth 5 činí v základu zhruba 2Mb/s. Proto není příliš vhodný pro sdílení objemných souborů.
Protokol vznikl již v roce 1994, kdy ho vyvinula společnost Ericsson. Jeho hlavním účelem bylo nahradit zastaralé sériové rozhraní RS-232. Bluetooth je specifikován pod standardem IEEE 802.15.1 a patří do kategorie osobních sítí (PAN). Bluetooth funguje na rádiové frekvenci 2,4 GHz, jako Wi-Fi. Zařízení se jsou schopna identifikovat pomocí adresy Bluetooth Device Address (*BD_ADDR*) která funguje podobně jako MAC adresa u síťových zařízení.
Bluetooth vzhledem k době své existence vystřídal řadu verzí, kdy každá následující v některém ohledu vylepšovala předcházející verzi, především se zlepšovaly vlastnosti týkající se přenosové rychlosti, dosahu a zabezpečení, viz tabulka 2 [25, 26].

Tabulka 2 Porovnání verzí Bluetooth [25, 53] – zpracováno autorem

Verze Bluetooth	Přenosová rychlost	dosah	novinky
1.0	732,2 Kb/s až 1 Mb/s	10 m	První verze
1.1			Oprava chyb 1. verze, přidána podpora nešifrovaných kanálů
1.2			Rychlejší propojení, zlepšena kvalita přenosu
2.1	2,1 Mb/s	30 m	Zlepšení zabezpečení, snížená energetická spotřeba
3.0	24 Mb/s (přes Wi-Fi)	30 m	Možnost využít Wi-Fi k rychlejším přenosům dat
4.0	1 Mb/s až 25 Mb/s	60 m	Výrazné snížení spotřeby energie
4.2			Zvýšená bezpečnost
5	2 Mb/s až 50 Mb/s	240 m	Vylepšená konektivita, zvýšená bezpečnost, snížení spotřeby energie
5.3			Aktuální verze (2022), přidána podpora propojení typu Mesh

- ***Direct Connect***

Direct Connect je P2P protokol, který umožňuje uživatelům napřímo sdílet soubory, případně podporuje funkci chatu, kdy si uživatelé mohou navzájem zasílat zprávy.
První verze protokolu byla vytvořena Jon Hessem v roce 1999, od té doby byl protokol dále rozvíjen, například bylo vylepšeno zabezpečení. Protokol zasílá mezi uzly jednotlivé příkazy zcela bez šifrování ve formě čistého textu. Pokud uživatel vyžaduje šifrování, musí si nainstalovat dodatek, který šifrování umožní.
Bohužel neexistují žádné oficiální informace k tomuto protokolu, proto musela být většina dokumentace vytvořena zpětně na základě analýzy protokolu. Díky tomuto problému je spousta dokumentace nekompletní, nebo nepřesná.
Každý klient, který chce tento protokol využívat, může vystupovat proti ostatním klientům jako server. Přiřazování serveru k jednotlivým klientům probíhá na základě první odpovědi. To znamená, že zařízení, které odpoví danému klientovi jako první, bude považováno za server.
V rámci protokolu neexistuje žádný globální identifikační systém, každý uživatel vystupuje pouze pod svou přezdívkou. Toto opatření zajišťuje, že žádný dotaz nemůže být spojován s žádným navázaným spojením, případně odpověď nemůže být spojena s žádným vyhledáváním.
Další vlastností protokolu je koncepce „slotů“. Ta umožňuje uživatelům nastavit, kolik dalších uživatelů má dovoleno v jeden okamžik využít dané zařízení pro stahování. Toto opatření zajistí, že uživatel nebude mít zcela vytížené připojení k internetu, nebo přetížený počítač, případně jiné zařízení, které danou službu poskytuje.
Dále protokol umožňuje uživatelům zvolit, zda chtějí být v „aktivním“ či „pasivním“ režimu. Aktivní režim umožňuje stahovat data od jakéhokoliv jiného uživatele nebo zařízení. Pasivní režim umožňuje stahování pouze ze zařízení v aktivním režimu.
Díky otevřenosti celého systému, který tento protokol vytváří, mohou být uživatelé bohužel často obětmi DDoS útoku. Hlavním důvodem je samotný koncept, na kterém protokol funguje. Kdokoliv může vystupovat jako hub, který může přesměrovávat veškerou komunikaci, která jde přes něj na jednu určitou oběť. Množství příchozí komunikace oběť zcela zahltí. Naštěstí tento problém byl částečně vyřešen pomocí

dodatku, který umožňuje uživatelům určit spoj, který jim přebytečnou komunikaci zasílá a následně ho zablokovat [27].

- ***eDonkey network***

eDonkey je decentralizovaný P2P protokol, sloužící k výměně objemnějších souborů mezi uživateli. Opět, jako u většiny ostatních P2P protokolů, vyhledávaná data nejsou uložena na serveru, ale u jednotlivých uživatelů, kteří je poskytují ostatním. V rámci sítě eDonkey existují servery, ty ale slouží pouze k nasměrování a lokalizování uživatele, který může poskytnout hledaný soubor, samotné servery žádná data neposkytují.

Protokol byl vytvořen v roce 2000 americkými vývojáři Jedem McCalebem a Samem Yaganem. Díky využití vyhledávacích serverů, které usnadňují hledání dat, patří tento protokol mezi hybridní P2P protokoly. Největší rozmach zažil eDonkey mezi lety 2004 až 2007, kdy byl nejvíce využívaným protokolem ke sdílení souborů na světě, od roku 2007 se stal nejvyužívanějším protokolem BitTorrent [28, 29].

- ***Freenet***

Freenet je P2P protokol umožňující komunikaci mezi uživateli, který je odolný proti cenzuře a je zcela anonymní. K ukládání dat využívá decentralizovanou distribuci informací, to znamená, že data nejsou uložena na jednom zařízení, ale jsou distribuována napříč zařízeními, to zajišťuje větší stabilitu a odolnost celého systému. Systém decentralizace je běžný u většiny P2P protokolů.

Základy protokolu vytvořil v roce 1999 Ian Clarke, jehož hlavním cílem bylo vytvořit protokol, který dokáže ochránit svobodu projevu a anonymitu na internetu.

Anonymita Freenetu je zachována díky systému decentralizovaného ukládání dat. Data jsou ukládána po malých šifrovaných kouscích napříč zařízeními. Pokud si data někdo vyžádá, jsou mu zaslána a složena dohromady. Díky jejich rozdělení, nelze při přenosu zjistit jejich celý obsah.

Hlavní myšlenkou tohoto protokolu je poskytnout každému uživateli internetu možnost se svobodně vyjádřit bez rizika cenzury a se zárukou anonymity, tyto vlastnosti vedou i k tomu, že je tento protokol využíván i ke komunikaci na darknetu. Dokonce samotní vývojáři přidali v roce 2008, kdy vyšla verze 0.7, režim podporující

připojení na darknet. Pokud je režim darknetu aktivovaný, je velmi těžké vystopovat komunikaci zvenčí.

Díky decentralizaci je Freenet velmi odolný, jelikož se jedná o P2P protokol, který nepotřebuje k fungování žádné servery. Dále se šíří v rámci freeware licence, může ho distribuovat kdokoli. Také patří mezi software s otevřeným kódem, proto může být dále rozvíjen komunitně.

Jelikož k ukládání sdílených dat jsou využívána koncová zařízení, může si každý uživatel zvolit, jak velkou část svého disku poskytne Freenetu k ukládání dat, většinou se přidělený prostor pohybuje okolo několika gigabytů. Každá sdílená informace se rozdělí na menší šifrované části, ty se rozešlou k uložení na různá zařízení, tak aby nebyla uložena pohromadě. Typicky se rozdělená data rozešlou vícekrát, aby byla k dispozici záloha, případně byla stále dostupná, jelikož se ukládají na koncová zařízení, která nemusí být stále online [30, 31, 32, 33].

4.8 Možnosti využití P2P protokolů v blízké budoucnosti

Současným trendem se stalo obklopování se chytrými zařízeními, ať už se jedná o různé doplňky k chytrým telefonům, jako jsou chytré hodinky či náramky, nebo se jedná o pokročilejší systémy vzájemné spolupráce mezi jednotlivými zařízeními, jako mohou být chytré domácnosti nebo obecně IoT. Dá se předpokládat, že se tento trend bude rozšiřovat stále mezi více uživatelů. S tímto prudkým nárůstem chytrých prvků se zároveň začalo velmi zvyšovat zatížení internetu, jelikož většina těchto zařízení aktivně komunikuje se svým serverem, který se často nachází někde v internetu. Některá zařízení využívají ke vzájemné komunikaci P2P protokoly, jedním z nejjednodušších systémů je Bluetooth. Současně některé prvky chytré domácnosti podporují protokoly pro vzájemnou komunikaci mimo Bluetooth. Některé tyto systémy vyžadují pro správné fungování nějakou formu centrální řídící jednotky (která je zde v roli lokálního serveru). Skrze tuto jednotku si navzájem předávají data a synchronizují se. Zároveň se ale i začínají objevovat systémy, které tuto centrální jednotku nepotřebují a dokážou si předávat informace přímo mezi sebou (formou P2P architektury). Hlavními výhodami tohoto přístupu by měla být menší cenová náročnost, díky nepotřebě řídícího prvku, a i větší robustnost, jednotlivé prvky by měly být schopné fungovat nezávisle na sobě.

Trend chytrých domácností se i zároveň začíná rozšiřovat na trend chytrých měst [47]. Tento trend znamená, že v současné době se začíná objevovat snaha zkvalitnit život ve městech pomocí moderních technologií [34]. Můžeme si pod tímto termínem představit třeba snahu zefektivnit dopravu pomocí řízených semaforů, které vyhodnocují vytíženost jednotlivých silnic a dle toho upravují provoz. Další částí může být snížení energetické náročnosti měst pomocí různých systémů, které se starají o vytápění a osvětlení budov nebo veřejné osvětlení. Dalšími prvky jsou samozřejmě různé městské informační systémy a samotné chytré domácnosti. Pro zprovoznění chytrých měst lze také uplatnit principy P2P komunikace, možné uplatnění lze nalézt u veřejného osvětlení. To nemusí být řízeno klasicky kabelem, ale lze využít P2P bezdrátové propojení, kdy dáme pokyn k rozsvícení pouze prvnímu světlu, tuto informaci předá bezdrátově následujícímu a tak dále, dokud se všechna světla nerozsvítí. Toto řešení je výhodné zejména díky částečnému snížení nákladů na výstavbu a dále to snižuje náročnost rozšiřování infrastruktury. Ovšem tento přístup se dá využít i ve spoustě jiných případů, jako třeba u výše zmíněného zefektivnění dopravy. Zde mohou být jednotlivé semafory propojené navzájem mezi sebou a předávat si informace o dopravním vytížení nezávisle na dispečinku a automaticky se synchronizovat tak, aby co nejlépe rozložily dopravní zátěž. Zároveň díky omezení dopravních kolon se sníží emise vyprodukované dopravou, to může částečně zlepšit ovzduší ve městech.

5 Shrnutí výsledků

5.1 Počátek sítí a základní rozdělení

S vývojem prvních počítačů v období od 50. do 80. let minulého století souvisí i rozvoj prvních sítí. Nejprve v rámci samotných institucí, kdy docházelo k propojení sálových počítačů s terminály sloužícími pro vstup a výstup dat, zde můžeme uvažovat o prvních jednoduchých sítích jak typu klient-klient tak i klient-server, pokud terminálů bylo více, jelikož terminály (klienti) komunikují pouze s hlavním počítačem (serverem), nikoliv s dalšími terminály. Další vývoj vedl k propojení několika sálových počítačů nacházejících se v různých institucí dohromady, to vedlo k vytvoření prvních základů sítě, ze které vychází dnešní internet [4, 5]. Takové první sítě byly typu klient-klient, jelikož počítačů nebylo mnoho, všechny byly propojené dohromady v jedné síti. Se zvyšujícím se počtem počítačů začalo být nutné zavést standardy, které by ulehčily komunikaci po síti, tím vznikly první síťové protokoly, které vytvořily standart pro komunikaci na síti.

Hlavními jsou modely TCP/IP a ISO/OSI, oba tyto modely dělí komunikaci po síti do vrstev a tím určují, co jaké zařízení v rámci sítě má za funkci [6, 7]. Vznik těchto modelů pomohl sjednotit komunikaci po síti a tím umožnily další rozšiřování sítí. Od 90. let minulého století existuje dnešní internet, který dnes propojuje celý svět a umožňuje nejsnadnější výměnu informací za celou historii lidstva. Jelikož dnešní internet je kvůli velkému množství zařízení velmi složitý, je pro usnadnění dělený na menší celky, a to: PAN (Drobné sítě, dnes nejčastěji tvořena telefonem a k němu připojenými zařízeními), LAN (sítě v rámci budovy), MAN (síť propojující větší oblasti jako je větší město nebo region) a WAN (síť propojující státy nebo celé kontinenty) [2].

Co se týká nejčastěji sítí LAN, můžeme i uvažovat o rozdělení dle topologie, která nám schematicky určuje, jak jsou jednotlivá zařízení v rámci sítě navzájem propojená (hvězda, bus, mesh, kruh, nebo stromové rozdělení) [3].

5.2 Porovnání sítí klient-server a klient-klient

Při porovnávání sítí klient-server a klient-klient, nemůžeme jednoznačně říct, které řešení je lepší, toto rozhodnutí lze učinit teprve, když známe kontext, v jakém daná síť má fungovat. Teprve když jsme seznámeni se všemi okolnostmi a požadavky, které se týkají daného využití sítě můžeme posoudit, který přístup je v dané situaci vhodnější.

Hlavními výhodami sítě klient-server je jejich organizovanost a z toho vyplývající rychlá odezva. Dotaz klienta jde přímo na server, ten klientovi hned odpoví. Problémem tohoto řešení je především jeho nákladnost. Server musí být velmi stabilní, to znamená, že musí disponovat velmi výkonným hardwarem a spolehlivým operačním systémem. Také musí mít dobré připojení k internetu, nejlépe o rychlosti v řádu několika Gb/s. Z těchto důvodů jsou náklady na jeho pořízení a provoz velmi vysoké. Přesto i nejvýkonnější servery jsou náchylné k občasným výpadkům způsobeným chybou, vnějšími okolnostmi, jako je výpadek elektřiny, případně útokem z vnějšku (např. DDOS) nebo příliš velkým počtem uživatelů. Pokud přestane fungovat server, nefunguje celá síť. Na druhou stranu díky rychlé odezvě je server vhodný pro provoz internetových stránek, nebo jiných služeb, které budou těžit z centralizace sítě [9].

Opakem je síť typu klient-klient. Tyto sítě pro svůj provoz vyžadují pouze uživatelská zařízení. Z tohoto důvodů je většina P2P sítí tvořená komunitou uživatelů. Hlavní výhodou je, že každý k provozu poskytuje vlastní zařízení, tím se radikálně snižují náklady na provoz takové sítě. Také díky velkému počtu zařízení jsou tyto sítě daleko méně náchylné k výpadkům. Nevýhodou je častá neorganizovanost této sítě, proto vyhledávání odpovědi na dotaz v této síti trvá déle než u řešení klient-server. Ovšem pokud se podaří nalézt požadovanou odpověď následně navázané spojení dokáže dosahovat vyšších rychlostí přenosu. Další výhodou je anonymita, jelikož data musí často cestovat přes několik různých zařízení, není většinou dohledatelný zdroj ani cíl těchto dat. Díky tomu odesílatel neví, komu přesně data poslal a příjemce neví odkud data přišla. Sítě klient-klient jsou vhodné především pro sdílení souborů nebo jiné služby, které jsou datově náročné [10].

5.3 Možná řešení P2P sítí a jejich zabezpečení

Sítě typu P2P lze řešit více způsoby. Můžeme mít úplně jednoduché nestrukturalizované sítě tvořené dvěma nebo více zařízeními třeba pouze v rámci jedné budovy. Tato drobná síť tvořená pouze napřímo propojenými zařízeními nepotřebuje žádné složité řízení. Problém nastává při vyšších počtech zařízení, které jsou propojena pomocí některého P2P protokolu. Takové sítě můžou obsahovat od několika stovek po několik milionů zařízení. Zde se začnou projevovat nedostatky nestrukturalizovaných P2P sítí.

Největším problémem P2P sítí s velkým počtem uživatelů je jejich nepřehlednost vyplývající z jejich neuspořádanosti. Hledání dat v neorganizované síti trvá velmi dlouho oproti síti typu klient-server. Některé P2P protokoly rozdělují síť do menších částí nebo vytváří centrální uzly, které tvoří most mezi menšími částmi sítě. Vyhledávání se tím může zrychlit, protože nejprve proběhne v rámci menší sítě, do které dané zařízení patří, poté může kontaktovat centrální uzel, který může daný dotaz nasměrovat do jiné části sítě, kde by mohla být hledaná odpověď.

Další využívanou možností je hybridní P2P síť. Tato síť disponuje prvky, které fungují jako server. Buď se jedná o přímo dedikovaný server nebo to může být významný síťový uzel (uživatelský počítač s dobrým připojením k internetu a dostatečně výkonným hardwarem). Vyhledávání v této síti je směřované nejprve na server, ten dotaz rovnou nasměruje nebo zjistí kam má dotaz nasměrovat. Následná komunikace mezi koncovými uzly probíhá bez další účasti serveru. Toto řešení je výhodné jak pro koncová zařízení, jelikož nemusí dlouho čekat na navázání spojení tak pro server, protože není zatěžován následnou komunikací, kterou by musel přeposílat [10].

Velkým problémem, kterým musí čelit všechny sítě, je zabezpečení. Hlavní výhodou P2P sítí je jejich anonymita. Žádný uživatel není schopný zjistit všechna zařízení obsahující nějaká konkrétní data. Prvky, které si předávají data při navázané komunikaci neví, odkud data přesně přišla nebo kam přesně jsou zasílána. Co se týče anonymity uživatelů, jsou P2P sítě bezpečnější než sítě klient-server. Anonymita ovšem také často znamená velké riziko, protože také často nelze přesně určit, kdo může být možný útočník, při probíhajícím DDoS útoku, nebo jestli náhodou někdo

neodposlouchává nebo nepozměnil data která se pohybují po síti. Zde přichází na řadu šifrování dat. Většina moderních P2P protokolů využívá nějakou metodu šifrování. Lze šifrovat veškerou komunikaci včetně té, která se nemusí přímo týkat daného P2P propojení, aby nešlo poznat, co která data představují nebo lze šifrovat pouze data, která jsou v rámci P2P propojení zasílána. K rozšifrování dat je nutné, aby druhá strana disponovala klíčem. Dalšími metodami zabezpečení jsou obecná pravidla, která by měla platit všude, kde hrozí nějaké riziko narušení. Příkladem těchto obecných pravidel je třeba dostatečně bezpečné heslo. Důležitá je také podpora vývojářů, kteří se starají o to, aby v používaných programech nebyly bezpečnostní díry, které by šly zneužít [11].

5.4 Porovnání P2P protokolů a možný vývoj do budoucna

Porovnat všechny P2P protokoly dohromady nelze. Při porovnávání se musí zohlednit účel jejich použití (sdílení souborů, komunikace, video komunikace, správa zařízení, kryptoměny), jestli jsou stále podporované a vyvíjené, kolik uživatelů daný protokol využívá. Další problém představuje množství různých programů, které využívají stejný protokol. Většina těchto programů je tvořena třetími stranami a často autoři jednotlivých protokolů nemají nic společného s autory programů, které protokol využívají. Jeden z posledních problémů představuje fakt, že mnoho protokolů je vyvíjeno na komunitní bázi. Výhodou je, že takto vyvíjené programy patří mezi freeware s otevřeným kódem, proto je může kdokoli vyvíjet a šířit. Problém je, že díky tomuto řešení může existovat mnoho neoficiálních variant, které jsou různě modifikované a často neexistuje oficiální dokumentace k těmto protokolům, proto získávání informací o přesné funkcionalitě je velmi složité a často nepřesné.

Jelikož existuje velmi velké množství různých P2P protokolů, budu pro účely této práce srovnávat pouze některé vybrané protokoly. Ve výběru by měly být zahrnuty pouze známější protokoly, případně známé programy využívající daný protokol. Srovnání protokolů bude rozděleno do několika kategorií.

5.4.1 Protokoly pro sdílení dat

Protokoly pro sdílení dat jsou asi nejrozšířenější kategorii P2P protokolů. Pomocí programů, které využívají P2P protokoly ke sdílení se šíří velká část souborů po internetu. V současné době tuto technologii využívá mnoho programů ke sdílení aktualizací, příkladem může být i Microsoft Windows a jeho služba Windows Update, která může ke stažení aktualizace využít buď přímo servery Microsoftu, nebo má i podporu P2P stažení aktualizací, která funguje tak, že počítač aktualizaci stáhne přímo ze serveru nebo jiného počítače, který má aktualizaci již staženou a po instalaci je schopný soubory aktualizace poskytnou dalším zařízením v síti. Hlavní výhodou takového kaskádovitého šíření je, že Microsoft zbytečně nezatěžuje vlastní servery, některým uživatelům to také může pomoci ušetřit čas, protože rychlost připojení v rámci domácí sítě bývá často vyšší než samotná přípojka na internet. Proto, pokud mají více zařízení se stejnou verzí Windows, stačí, když aktualizaci stáhne jedno zařízení, které dále distribuuje soubory ostatním zařízením v rámci domácí sítě.

Hlavním důvodem oblíbenosti programů, které umožňují P2P sdílení souborů je především snadná dostupnost téměř jakéhokoliv obsahu. Lidé mohou snadno sdílet textové soubory, hudbu, video, instalační soubory různých programů atd. Bohužel zde se naráží na autorské zákony, sdílet se mohou pouze programy, které patří mezi volně šiřitelný obsah. Uživatelé často ale sdílí soubory, které mezi tento obsah nepatří, a tím dochází k porušování licence. Tito uživatelé se tedy dopouští pirátství, někteří uživatelé o tomto problému ani nevědí, nebo ho neřeší. Pirátství se dopouštějí i při stahování souborů, které nepatří mezi volně šiřitelný obsah. Jelikož je pirátský obsah jednoduše dostupný, využívá ho mnoho uživatelů. Mezi nejvíce sdílený nelegální obsah patří především pirátské kopie různý seriálů, filmů a hudby. Programy se v tak velkém množství již nešíří, jelikož disponují různými protipirátskými ochranami, dalším důvodem je, že většina uživatelů je i seznámena s riziky, které tento obsah obnáší, jako jsou různé viry, trojské koně, nebo právní následky. Pirátství má i přesto velký vliv na oblíbenost těchto programů.

V současné době je asi nejoblíbenějším protokolem pro sdílení souborů BitTorrent, dalšími oblíbenými protokoly především v minulosti je eDonkey a Direct Connect,

existuje i mnoho dalších protokolů, jako je např. Gnutella, FastTrack, WebTorrent a mnoho dalších, těmi se ale v tomto srovnání nebudu zabývat.

BitTorrent

První verze tohoto protokolu byla vydána v roce 2001, aktuální verze má číslo 7.11.0, byla vydána na konci roku 2022 [37]. Hlavní podstata fungování protokolu BitTorrent spočívá v rozdělování souborů na bity, ty poté dokáže posílat i přijímat ve stejný okamžik, tím se zefektivňuje komunikace oběma směry. Patří mezi decentralizované P2P protokoly. Hlavním nedostatkem BitTorrentu je, že nezachovává anonymitu svých uživatelů, veškeré použité IP adresy jsou pomocí tohoto protokolu veřejně viditelné. Řešením mohou být klienty třetích stran, některé disponují funkcí VPN, ta skryje aktuální adresu uživatele, ale za cenu zpomalení připojení, případně účtování datového objemu, jelikož k této funkci je již zapotřebí dedikovaný server, který se bude tvářit jako zařízení uživatele a přes který uživatelů data stáhne [14, 15].

Protokol BitTorrent je vlastněný společností BitTorrent Inc. Největší podíl uživatelů pochází z USA. V roce 2016 měl BitTorrent celosvětově 45 milionů uživatelů aktivních každý den, v roce 2019 byl BitTorrent nainstalovaný na jedné miliardě zařízení a je využíván ve 138 státech světa [36].

Oblíbenost tohoto programu nejspíše rostla i s množstvím přibývajících streamovacích služeb, které například přinesly množství nových oblíbených filmů a seriálů. Jelikož existuje problém internetového pirátství, začaly se tyto filmy a seriály šířit i neoficiálními cestami. Díky dostupnosti služeb na sdílení souborů, jejichž používání na rozdíl od většiny streamovacích služeb bývá zcela zdarma, někteří uživatelé mají snahu ušetřit i přes riziko ve formách porušování autorského zákona nebo vyšší riziko vystavení se potenciálnímu malwaru. Ovšem P2P služby na sdílení souborů jako je BitTorrent žádný zákon neporušují a ani porušovat nemohou, jelikož pouze poskytují službu sdílení uživatelského obsahu, která je naprosto v pořádku. Samotným používáním tohoto programu uživatel nic neporušuje, k porušení zákonu dochází až při sdílení obsahu chráněným autorským zákonem [35].

Direct Connect

Konkurentem protokolu BitTorrent může být například Direct Connect. Na rozdíl od protokolu BitTorrent je Direct Connect centralizovaný P2P protokol, který ke sdílení dat mezi uživateli využívá systém uzlů nazvaných jako hub. Hub funguje jako křižovatka, přes kterou si mohou uživatelé předávat data. Navíc Direct Connect podporuje kromě přeposílání souborů i funkci chatu.

Direct Connect byl vytvořený firmou NeoModus v roce 1999. Původním účelem protokolu bylo šířit adware, tedy software propagující reklamu. Tento protokol využívalo a stále využívá množství programů, v současnosti asi nejvíce využívaným je DC++, který jako jeden z mála Direc Connect klientů nemá funkcionalitu adwaru, proto je velmi oblíbený a existuje i množství dalších programů, které z DC++ vycházejí.

Informace zasílané v rámci sítě Direct Connect jsou ve výchozí verzi zasílána jako obyčejný text, to je v současnosti velmi nebezpečné, jelikož kdokoliv si může snadno zjistit co kdo komu zasílá, proto existují dodatky, které umožňují šifrované zasílání zpráv, které zlepšuje bezpečnost komunikace. Jelikož neexistují žádné oficiální specifikace tohoto protokolu, musejí být zjišťovány zpětně. Prvky v síti, které slouží jako hub potřebují dobré připojení k internetu, kvůli množství komunikace, která přes ně proudí. Anonymitu sítě zachovává systém hubů a využívání přezdívek, díky tomuto opatření uživatelé pouze vidí, z jakého hubu, na který se daný uživatel připojil, ale již nezjistí, kde přímo se nachází [7].

eDonkey Network

Dalším oblíbeným protokolem pro sdílení dat v minulosti byl eDonkey. První verze vznikla v roce 2000, poslední oficiální verze se objevují okolo roku 2005. V prvním desetiletí 21. století patřil mezi nejoblíbenější služby ke sdílení souborů, ale v druhé polovině desetiletí byl vystřídán BitTorrentem, který je nejoblíbenějším protokolem tohoto typu dodnes. Ovšem existují odvozené verze tohoto protokolu, které i využívají stejnou síť jako eDonkey, nejznámější odvozená verze je asi eMule. Poslední verze eMule nese označení 0.60c a je z roku 2022 [38].

Pokud se vrátíme zpět k eDonkey, jedná se o decentralizovaný P2P protokol, který využívá hybridní architekturu. To znamená, že při vyhledávání využívá servery,

které hledaná data lokalizují, následné navázané spojení již probíhá bez účasti serverů [28, 29].

Zhodnocení

Jelikož eDonkey není v aktivním vývoji od roku 2005, nelze jej považovat za moderní P2P protokol, ovšem lze brát v potaz eMule, který přímo z eDonkey vychází a dokonce je schopen využívat stejnou síť kterou eDonkey používal. V dnešní době není tento protokol tak moc široce využíván, to se projevuje malým počtem aktivních uživatelů a také menším veřejným povědomím o tomto protokolu.

Direct Connect je zajímavý základ pro programy, které chtějí využívat P2P sdílení souborů, ovšem díky množství klientů třetích stran jsou možnosti jeho využití velmi široké. Kvůli vývoji na komunitní bázi, ale není v podstatě žádná oficiální verze. Díky této vlastnosti existuje velmi mnoho programů, které jsou odvozené z původní verze protokolu. Díky tomuto množství se jednotlivé verze mohou lišit a je složité posoudit, která verze protokolu je ta hlavní. Dalším problémem Direct Connect je chybějící oficiální dokumentace, veškeré dokumentace k programu vychází až ze zpětné analýzy již zveřejněného kódu.

Nejlepším programem v tomto porovnání je BitTorrent. Dlouhodobě se jedná o nejvíce používaný protokol na sdílení souborů. Do povědomí většiny uživatelů se ale nejčastěji dostal ve spojitosti s internetovým pirátstvím. Ovšem hlavní účel tohoto protokolu není šíření pirátských kopii, ale možnost sdílet libovolný obsah mezi uživateli, tato funkce je pro fungování mnoha programů klíčová. Díky vlastnostem, které BitTorrent má je tento protokol využíván i programy, kde by ho běžný uživatel úplně neočekával, jako mohou být například aktualizace některého softwaru. Hlavním důvodem, proč je tento protokol oblíbený mezi softwarovými společnostmi je, že nemusejí vyvíjet vlastní protokol a také, že nemusí mít zbytečně výkonné servery třeba k poskytnutí již zmíněných aktualizací. Proto BitTorrent patří mezi vůbec nejznámější a nejpoužívanější P2P protokoly.

5.4.2 Další P2P protokoly

P2P protokoly mají daleko širší využití než jenom sdílení souborů, ovšem zde je složité najít konkurenční programy, nebo protokoly, které jsou ve stejné kategorii využití a zároveň patři mezi P2P protokoly. Hlavními důvody je nedostatek konkurenčních řešeních z důvodu přílišné složitosti dané problematiky nebo malé oblíbenosti konkurenčních programů, které po pár měsících přestaly být dále vyvíjeny. Zajímavým rysem P2P programů, které se v těchto kategoriích uchytily je, že často byly prvními programy ve své třídě.

Bitcoin

Bitcoin je zajímavé využití P2P sítě k provádění transakcí. Jelikož transakce probíhají na úrovni P2P komunikace, jsou anonymní, velmi odolné a nelze je cenzurovat nebo jinak ovlivnit. Zároveň se jedná o první využití blockchainu na síti. Tato technologie zaručuje legitimnost transakcí, jelikož se jedná o sdílené databáze účetních záznamů. Každý uživatel může mít přehled o provedených transakcích a může vlastní záznamy porovnat s ostatními a tím prokázat správnost transakce. Zároveň tento protokol zavedl systém odměňování za řešení složitých matematických rovnic, který je známý jako „těžba kryptoměn“ [22].

V počátcích tohoto protokolu neměly jednotky Bitcoin téměř žádnou hodnotu, v průběhu času, kdy začaly fungovat korekce, které snižují počet Bitcoinu, které jsou přidělovány za odměnu uživatelům a s rostoucí popularitou, kdy se Bitcoin začal dostávat do obecného povědomí, vzrostla jeho hodnota na velmi vysoký kurz oproti reálné měně. Doposud nejvyšší dosažená hodnota byla dosažena 12.11.2021, a to 64 400 amerických dolarů na jeden Bitcoin. Současná hodnota se v první polovině dubna 2023 pohybuje okolo 30 000 amerických dolarů za jeden Bitcoin [39].

Vzor Bitcoinu se rozhodlo následovat mnoho dalších společností i nezávislých vývojářů, ale většina těchto pokusů selhala a většina ostatních kryptoměn nedosahuje tak vysokých hodnot jako Bitcoin. Mnoho kryptoměn se pohybuje na úrovni amerických centů, občas i několika dolarů.

Dále je s Bitcoinem a s kryptoměnami spojeno i mnoho kontroverzí, například podvodné kryptoměny, které slibovaly astronomické zisky, nakonec skončily jako zcela bezcenné nebo také různé investiční podvody vztahující se k investicím do

Bitcoinu. Další kontroverzí může být nedostatek grafických karet na trhu způsobený velkým nadšením, které panovalo kolem těžby kryptoměn, kdy mnoho lidí mělo představu, že zbohatnou s minimálním úsilím a investicemi. Situace se v současné době již zlepšila, ale její dopady jsou dodnes viditelné (grafické karty stále mají ceny v rozpětí od 2 000 Kč až klidně k 50 000 Kč, před touto krizí se ceny pohybovaly od 1000 Kč do 20 000 Kč. Pokud vezmeme v potaz inflaci, stále kryptoměnová krize měla velké dopady na cenu).

Díky své anonymitě se také Bitcoin stal velmi populární na černém trhu, kdy se mu podařilo vytvořit elektronickou alternativu ke zlatu.

V poslední době se také začaly řešit dopady této kryptoměny na životní prostředí. Jelikož k těžbě kryptoměn je zapotřebí ohromné množství výpočetního výkonu, provoz těžebních sestav je velmi náročný na spotřebu elektřiny. Některé krypto farmy využívají vlastní zdroje energie, ovšem většina uživatelů, kteří se podílí na těžbě, je závislá na veřejné rozvodné síti, která ve většině případů využívá k výrobě elektřiny fosilní paliva. Řešení tohoto problému jsou algoritmy, které rozdělují přidělované Bitcoiny na menší části, a tím zpomalují jeho těžbu, jelikož aby si Bitcoin zachoval hodnotu, je přesně určeno množství, jaké může být vytěženo. Až bude vytěžen poslední Bitcoin, nebude těžba nových jednotek již povolena, a tím se výrazně sníží energetické nároky na obsluhu tohoto protokolu.

Celkově Bitcoin působí jako velmi zajímavý koncept, především v jeho počátcích byl vnímán jako velmi dobrý zdroj přivýdělku, ovšem v dnešní době se již tak zajímavě nejeví. V blízké budoucnosti bude dle mého názoru představovat největší konkurenci Bitcoinu elektronická varianta oficiálních státních měn, o které se začínají dělat diskuse.

Skype

Skype vznikl v roce 2003 jako internetová alternativa ke klasickým mobilním operátorům, jeho hlavní výhodou je, že jeho pořízení a používání je zcela zdarma. V roce 2011 byl zakoupen firmou Microsoft, která ho chtěla využít jako základ pro svůj vlastní projekt. Když ovšem viděla, jak je Skype oblíbený mezi uživateli, rozhodla se Skype zachovat a původní projekt byl zrušen. Firma Microsoft podporuje a stále vyvíjí Skype dodnes, aktuální verze je 8.96.0.207, která vyšla 27. února 2023. Skype má verzi pro každý hlavní operační systém (Windows, Mac, iOS, Linux, Android), dokonce existuje i verze, která běží v rámci internetového prohlížeče, bez nutnosti instalace [40].

Skype funguje jako hybridní P2P síť, to znamená, že k navázání spojení mezi uživateli je využit server, který vyhledá druhou stranu, se kterou chce být uživatel spojen, po navázání spojení se již server na komunikaci nějak nepodílí. Cesta, kterou server při kontaktování vytvoří, je volena na základě co nejnižší možné odezvy, jelikož se jedná o komunikaci v reálném čase. K samotnému umožnění spojení je využita síť uzlů, která je tvořena jednotlivými uživateli Skypu, dále v rámci této sítě existují i tzv. „super uzly“, které představují body, kde se kříží více cest, většinou se jedná o uživatele s dobrým připojením k internetu. Toto řešení napomáhá snižovat celkové zatížení sítě, také výrazně snižuje náklady na provoz Skypu [16, 17, 18, 19]. Skype byl pro mnoho uživatelů prvním programem, který umožňoval videohovory v reálném čase. V současnosti existuje mnoho alternativ, například přímo Microsoft má svůj další program nazvaný Teams, který také umožňuje videohovory, z dalších oblíbených alternativ lze uvést Zoom, WhatsApp, FaceTime, Google Meet, Signal, Facebook Messenger, Viber a mnoho dalších [41]. Z tohoto množství konkurence je jasné, že Skype nemá jednoduché udržet si uživatele, i přes tuto konkurenci je ale stále velmi populární.

Bluetooth

Protokol Bluetooth je P2P protokol pro bezdrátovou komunikaci. První verze protokolu vznikla již v roce 1994 jako bezdrátová náhrada za sériové rozhraní RS-232. Zároveň měl být spolehlivější než infračervené rozhraní (IR), jehož hlavní nevýhodou bylo, že přijímač i vysílač musely být v přímé viditelnosti. Na rozdíl od IR funguje Bluetooth na rádiových vlnách, tím stačí aby obě propojená zařízení byla v okruhu dosahu signálu, toto řešení poskytuje uživatelům této technologie daleko větší volnost, co se týká umístění oněch zařízení.

V současné době existuje již verze Bluetooth 5.3. Verze Bluetooth jsou navrženy tak, aby umožňovaly zpětnou kompatibilitu. Největším rozdílem mezi verzemi bývá zlepšování dosahu, rychlosti přenosu, snižování spotřeby energie a zvyšování zabezpečení [25, 26].

Alternativami k Bluetooth může být NFC, které má ale velmi malý dosah (vzdálenost do 4 cm), Wi-Fi Direct, má sice vyšší rychlost než Bluetooth, je ale více energeticky náročný, dále máme také například ZigBee, hlavní výhodou ZigBee je velmi vysoký počet zařízení, která mohou být zapojena dohromady v jeden okamžik, hlavní využití má v dnes oblíbené automatizaci domácností [42].

Bluetooth je revoluční protokol, navíc patří mezi první bezdrátové protokoly, které byly specifikovány. Hlavním přínosem Bluetooth je, že dokázal propojit zařízení bezdrátově. V současné době má velmi široké využití, je využíván různými periferiemi u PC, jako jsou klávesnice, myši nebo sluchátka. Daleko větší význam má ale u nositelných zařízení, kdy například k telefonu nebo tabletu můžeme připojit různá další zařízení jako jsou chytré hodinky a náramky, externí reproduktory, sluchátka a další různé typy nositelných zařízení. Široké využití má Bluetooth i v chytrých domácnostech a ostatní automatizaci lidského okolí, zde umožňuje snadné propojení zařízení bez nutnosti kabeláže, která by mohla v některých situacích představovat problém. V tomto segmentu existují ale alternativy, jako například výše zmíněné ZigBee. Dle mého názoru bude ale Bluetooth stále zásadní využívaná technologie.

Freenet

Freenet je P2P protokol pro anonymní sdílení textů, názorů a zpráv, bez obav z jakékoliv cenzury, nebo jiných překážek. Dle autora protokolu se má jednat o nástroj, který má zachovat svobodu projevu na internetu. Byl specifikován v roce 1999, aktuální verze byla zveřejněna v lednu 2023, nese označení 0.7.5 build01496 [43]. V dnešní době se jedná stále o aktuální protokol, největší využití bude mít ve státech se silnou cenzurou. Systém ukládání záznamů je zajímavý, jelikož data nejsou jako u většiny P2P protokolů uložena pohromadě na jednom zařízení, ale jsou rozdělována na menší šifrované části, které jsou následně distribuovány na mnoho různých zařízení. Zásadní pro toto rozdělování je, aby data byla rozeslána vícekrát z důvodu zálohování. Každý uživatel protokolu má možnost specifikovat kolik prostoru k ukládání dat dá k dispozici. Nevýhodou tohoto řešení může být možná nedostupnost částí dat, kdy nemusí být k dispozici úplně celý soubor, jelikož se spoléhá na uživatelská zařízení, která nemusí být stále online k dispozici.

Zajímavostí tohoto protokolu je, že přímo podporuje režim darknetu, v tomto režimu je velmi těžké vystopovat komunikaci, jelikož zařízení komunikují pouze se zařízeními, která jsou považována za důvěryhodná, pro pozorovatele zvenčí je tedy téměř nemožné zjistit odkud kam data jdou [30, 31, 33].

Tento komunikační protokol je velmi zajímavý, lze jej použít jak pro sdílení kontroverznějších názorů, které by se nehodily k veřejné diskusi, tak k šíření informací v zemích se silnou cenzurou. Také se hodí pro komunikaci, kde si autor jednoduše přeje zachovat soukromí a anonymitu. Tento protokol může oslovit velké množství uživatelů i v budoucnosti, jelikož se začíná diskutovat co je a není vhodné zveřejňovat na internetu a běžné sociální sítě mají občas až příliš přísná pravidla pro obsah příspěvků. Na druhou stranu se nabízí diskuse, co je opravdu za hranou a co je ještě svoboda projevu. Tato problematika je velice složitá a není předmětem této práce, v budoucnu ale bude jistě představovat zásadní diskusi.

5.4.3 Výhled do budoucna

Do budoucna dle mého názoru bude vliv P2P protokolů stále velmi důležitý, jelikož bude existovat velmi velké množství zařízení, která budou pro svoji funkci vyžadovat připojení k dalším zařízením. Pokud by komunikace mezi nimi probíhala pouze na bázi klient-server, bylo by zapotřebí mít mnoho velmi výkonných serverů a daleko lepší infrastrukturu sítě, tak aby bylo všude k dispozici připojení o rychlosti alespoň několik Gb/s, takové podmínky jsou zatím neproveditelné v takové míře, v jaké se bude moderní elektronika vyskytovat.

Řešením je komunikace na bázi P2P, která se v minulosti prokázala a stále se prokazuje jako vhodné řešení pro práci s velkým množstvím dat nebo tam, kde je zapotřebí komunikace v reálném čase. Další výhodou v prostředí IoT bude jejich jednoduchost na instalaci. Zařízení, která disponují možností komunikace přes P2P protokoly jsou ideální například pro chytré domácnosti, jelikož nevyžadují nutnost vlastnit server nebo jiné řídící jednotky, které bývají často velmi drahé. Pokud bude v rámci takového řešení použita nějaká forma řídící jednotky, která by v dané síti zařízení fungovala jako server, P2P komunikace pro ni bude také výhodná, jelikož nebude zbytečně zatěžována velkým množstvím informací. Koncová zařízení mohou komunikovat napřímo bez účasti centrálních prvků, takže například inteligentní vytápění může komunikovat přímo s venkovním senzorem teploty bez účasti serveru. Server může například dostávat pouze informace o aktuálním stavu nebo o provedené změně.

Dalším prostorem, kde se P2P technologie jistě uplatní, budou inteligentní města, která budou efektivní v ohledu k dopravě, spotřebě energie a s tím spojeném omezení emisí a zkvalitnění dalších služeb, které se týkají obyvatel těchto měst.

Velké využití stále také bude v dnes již klasických případech jako je sdílení souborů, propojování zařízení a další podobné služby.

Všeobecně P2P protokoly zůstanou důležitou technologií, jejich vliv se může ještě rozrůst, budeme muset počkat co přinese budoucnost.

6 Závěry a doporučení

Hlavním cílem této práce bylo seznámit čtenáře s moderními P2P protokoly, následně tyto protokoly porovnat. Práce se věnovala stručné historii vzniku internetu a jeho základních protokolů. Dále byly představeny základní struktury organizování sítí. Byly představeny známější P2P protokoly, jejich historický vývoj a základní principy, na kterých fungují. Následně bylo provedeno shrnutí informací a zhodnocení uvedených protokolů.

Hlavní cíle této práce byly splněny. V práci se ukázalo, že většina P2P protokolů má za hlavní cíle svobodu a anonymitu. Svoboda může být myšlená v různých formách, jako je například svobodné sdílení dat, nebo svoboda projevu. Jak se ukázalo, P2P protokoly jsou velmi odolné proti jakékoliv cenzuře, tato odolnost nejspíše vyplývá z velkého množství zařízení, která se na provozu protokolů podílejí. Dalším společným rysem pro zde uvedené protokoly je, že často jsou dostupné zcela zdarma, dokonce některé jsou komunitně vyvíjené. Společným rysem také může být vznik těchto protokolů, první verze většiny zde uvedených protokolů byla zveřejněna okolo roku 2000.

Posledním faktem, který vyplývá z této práce je, že mnoho P2P protokolů je díky svým vlastnostem anonymity a dostupnosti zneužívaná k nelegálním činnostem, ovšem ze samotné podstaty těchto protokolů je velmi těžké možná i nemožné tomuto zneužívání předejít.

P2P protokoly jsou velice široké téma, které by jistě šlo rozdělit na menší části, které by šlo odborně zpracovat. Tato práce je spíše obecná a seznamuje čtenáře s většinou oblastí, které se týkají P2P protokolů.

7 Seznam použité literatury

[1] Co je to počítačová síť?. *Home* [online]. [cit. 07.07.2021]. Dostupné z: http://ijs.8u.cz/index.php/pocitacove-site/co-je-to-pocitacova-sit

[2] Types of Computer Networks - GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online]. Dostupné z: https://www.geeksforgeeks.org/types-of-computer-networks/

[3] Computer Network Topology: What It is and Types - javatpoint. Tutorials List - Javatpoint [online]. Copyright © Copyright 2011 [cit. 15.04.2023]. Dostupné z: https://www.javatpoint.com/computer-network-topologies

[4] SMYSITELOVÁ, Lucie. Historie rozlehlých počítačových sítí. *Www.fi.muni.cz* [online]. 1999 [cit. 2021-8-20]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/xsmysit.html

[5] Networking & The Web | Timeline of Computer History | Computer History Museum. [online]. Copyright © [cit. 08.07.2021]. Dostupné z: https://www.computerhistory.org/timeline/networking-the-web/

[6] Referenční model ISO/OSI. *Úvodní strana* [online]. [cit. 12.07.2021]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=13&Itemid=119

[7] History of TCP/IP - Scos Training. Home - Scos Training [online]. Copyright ©2023 scos.training [cit. 15.04.2023]. Dostupné z: https://scos.training/history-of-tcp-ip/

[8] TCP/IP: What is TCP/IP and How Does it Work?. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/TCP-IP

[9] OLUWATOSIN, Haroon Shakirat. Client-server model. IOSR Journal of Computer Engineering, 2014, 16.1: 67-71.

[10] What is Peer to Peer (P2P) Network? With Architecture, Types, Examples. *DigitalThinkerHelp - Provide Helpful Information in Technology* [online]. Copyright © 2021 [cit. 21.07.2021]. Dostupné

z: https://digitalthinkerhelp.com/what-is-peer-to-peer-p2p-network-with-architecture-types-examples/

[11] WARARKAR, Pravin, et al. Resolving Problems Based on Peer to Peer Network Security Issue's. *Procedia Computer Science*, 2016, 78: 652-659.

[12] About BitTorrent | Creator of the World's Leading P2P Protocol. *BitTorrent | The World's Most Popular Torrent Client* [online]. Copyright © [cit. 24.01.2023]. Dostupné z: https://www.bittorrent.com/company/about-us/

[13] µTorrent. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2023 [cit. 2023-04-18]. Dostupné z: https://en.wikipedia.org/wiki/%CE%9CTorrent

[14] BitTorrent. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2023 [cit. 2023-04-18]. Dostupné z: https://en.wikipedia.org/wiki/BitTorrent

[15] The BitTorrent Protocol Specification v2 [online]. In: . 10-Jan-2008 [cit. 2023-04-14]. Dostupné z: https://www.bittorrent.org/beps/bep_0052.html

[16] The History Of Skype | History of Branding. *Home | History of Branding* [online]. Copyright © 2023. [cit. 24.01.2023]. Dostupné z: https://www.historyofbranding.com/the-history-of-skype/

[17] Skype Guide: History, Origin, and More - History-Computer. *History-Computer* [online]. Copyright © [cit. 24.01.2023]. Dostupné z: https://history-computer.com/skype-guide/

[18] How Does Skype Work? [Technology Explained]. Make use of [online]. 2009, JUL 30, 2009 [cit. 2023-04-14]. Dostupné z: https://www.makeuseof.com/tag/technology-explained-how-does-skype-work/

[19] How Does Skype Technology Work? | Small Business - Chron.com. *Small Business - Chron.com* [online]. Copyright © 2023 Hearst [cit. 24.01.2023]. Dostupné z: https://smallbusiness.chron.com/skype-technology-work-57268.html

[20] Attention Required! | Cloudflare. *Attention Required! | Cloudflare* [online]. Dostupné z: https://atomicdex.io/en/blog/what-is-bitcoin-btc/#bitcoin-source-code

[21] Bitcoin network. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2023 [cit. 2023-04-18]. Dostupné z: https://en.wikipedia.org/wiki/Bitcoin_network

[22] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 2008, 21260.

[23] BARBER, Simon, et al. Bitter to better—how to make bitcoin a better currency. In: Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers 16. Springer Berlin Heidelberg, 2012. p. 399-414.

[24] What is APPN? - Cisco. Networking, Cloud, and Cybersecurity Solutions - Cisco [online]. [cit. 2023-04-18]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/ibm-technologies/advanced-peer-to-peer-networking-appn/12235-33.html

[25] Bluetooth. Microsoft Wiki [online]. [cit. 2023-04-09]. Dostupné z: https://microsoft.fandom.com/wiki/Bluetooth

[26] Bluetooth Technology Overview | Bluetooth® Technology Website. Bluetooth® Technology Website – The official website for the Bluetooth wireless technology. Get up to date specifications, news, and development info. [online]. Copyright © 2023 Bluetooth SIG, Inc. All rights reserved. [cit. 09.04.2023]. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

[27] MOLIN, Karl. Measurement and Analysis of the Direct Connect Peer-to-Peer File Sharing Network. *rapport*, 2010, 2009.

[28] HECKMANN, Oliver, et al. The eDonkey file-sharing network. *Informatik 2004, Informatik verbindet, Band 2, Beiträge der 34. Jahrestagung der Gesellschaft für Informatik eV (GI)*, 2004.

[29] EDonkey network. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2023 [cit. 2023-04-18]. Dostupné z: https://en.wikipedia.org/wiki/EDonkey_network

[30] CLARKE, Ian, et al. Private communication through a network of trusted connections: The dark freenet. Network, 2010.

[31] CLARKE, Ian, et al. Freenet: A distributed anonymous information storage and retrieval system. In: Designing privacy enhancing technologies: international workshop on design issues in anonymity and unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 46-66.

[32] Freenet. Freenet [online]. Copyright © Copyright The Freenet Project Inc. [cit. 08.04.2023]. Dostupné z: https://freenetproject.org/

[33] Freenet. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2023 [cit. 2023-04-18]. Dostupné z: https://en.wikipedia.org/wiki/Freenet

[34] The Future Of Devices Peer-To-Peer Communication – ACiiST. ACiiST – ACiiST Smart City Cyber Switch Using the Lamppost as a Platform [online]. Dostupné z: https://www.aciist.com/the-future-of-devices-peer-to-peer-communication/

[35] Torrenting - 39 Facts and Statistics - VPNCrew. The Top Ten VPN Services! - VPNCrew [online]. Copyright © [cit. 13.04.2023]. Dostupné z: https://www.vpncrew.com/torrenting-facts-and-statistics/

[36] BitTorrent Statistics, User Count and Facts (2023). DMR - Business Statistics | Innovative Gadgets [online]. Copyright © 2023 DMR. All rights reserved. [cit. 13.04.2023]. Dostupné z: https://expandedramblings.com/index.php/bittorrent-statistics-facts/

[37] All versions of BitTorrent for Windows - FileHippo.com. FileHippo.com - Download Free Software [online]. Dostupné z: https://filehippo.com/download_bittorrent/history/

[38] eMule Download (2023 Latest). FileHorse.com / Free Software Download for Windows [online]. Copyright © 2023 Full Stack Technology

FZCO. All rights reserved. [cit. 13.04.2023]. Dostupné z: https://www.filehorse.com/download-emule/

[39] Google Finance. Google.com [online]. [cit. 2023-04-13]. Dostupné z: https://www.google.com/finance/quote/BTC-USD?window=MAX

[40] What's New in Skype for Windows, Mac, Linux, and Web?. Microsoft.com [online]. 2023 [cit. 2023-04-19]. Dostupné z: https://support.skype.com/en/faq/fa34778/what-s-new-in-skype-for-windows-mac-linux-and-web

[41] The Best Free Skype Alternatives of 2023. Lifewire: Tech News, Reviews, Help & How-Tos [online]. [cit. 2023-04-19]. Dostupné z: https://www.lifewire.com/best-free-skype-alternatives-4842385

[42] Comparison of Wireless Technologies: Bluetooth, WiFi, BLE, Zigbee, Z-Wave, 6LoWPAN, NFC, WiFi Direct, GSM, LTE, LoRa, NB-IoT, and LTE-M. Predictable Designs is where electronics and entrepreneurship intersect [online]. [cit. 2023-04-19]. Dostupné z: https://predictabledesigns.com/wireless_technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/

[43] Release build01496 · hyphanet/fred · GitHub. GitHub: Let's build from here · GitHub [online]. Copyright © 2023 GitHub, Inc. [cit. 19.04.2023]. Dostupné z: https://github.com/hyphanet/fred/releases/tag/build01496

[44] Peer-to-Peer Networking: Explanations, Applications, and Implications [online]. Lubbock Christian University [cit. 2023-04-14]. Dostupné z: https://www.ccsc.org/southcentral/E-Journal/2008/Papers/P-0008-final.pdf

[45] KISEMBE, Phillip; JEBERSON, Wilson. Future of peer-to-peer technology with the rise of cloud computing. International Journal of Peer to Peer Networks (IJP2P), 2017, 8.2/3: 45-54.

[46] KARA, Mostefa, et al. Secure key exchange against man-in-the-middle attack: Modified diffie-hellman protocol. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, 2021, 7.3: 380-387.

[47] O smart city: Co to je a jak funguje inteligentní město – smart city. Smartcityvpraxi.cz [online]. 2023 [cit. 2023-04-21]. Dostupné z: https://www.smartcityvpraxi.cz/o_smart_city.php

Zdroje obrázků a tabulek

[48] Zrození internetu 14: Internet přichází, Arpanet ustupuje – Živě.cz. Živě.cz – O počítačích, internetu, vědě a technice [online]. Copyright © 2023 Copyright CZECH NEWS CENTER a.s. a dodavatelé obsahu. [cit. 16.04.2023]. Dostupné z: https://www.zive.cz/clanky/zrozeni-internetu-14-internet-prichazi-arpanet-ustupuje/sc-3-a-170471/default.aspx

[49] Referenční model ISO/OSI. Internet a jeho služby [online]. [cit. 2023-04-16]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=13&Itemid=119

[50] Referenční model ISO/OSI. Upce.cz [online]. [cit. 2023-04-16]. Dostupné z: https://ct.upce.cz/machalik/puitk-stare/site/druha.htm

[51] Main differences between the ISO/OSI model and TCP/IP | Informatica e Ingegneria Online. INFORMATICA E INGEGNERIA ONLINE | Informatica e Ingegneria Online [online]. [cit. 2023-04-16]. Dostupné z: https://vitolavecchia.altervista.org/main-differences-between-the-iso-osi-model-and-tcp-ip/

[52] List of P2P protocols. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- 2023 [cit. 2023-04-16]. Dostupné z: https://en.wikipedia.org/wiki/List_of_P2P_protocols

[53] Does Bluetooth Versions Differences is Matter? History of Bluetooth v1.0 to v5.0 - xiaomiui. Xiaomi & MIUI News | Xiaomiui [online]. Dostupné z: https://xiaomiui.net/bluetooth-versions-differences-19725/

Oskenované zadání práce

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Libor Novotný**
Studium:	I1900625
Studijní program:	B0688A140001 Informační management
Studijní obor:	Informační management
Název bakalářské práce:	**Moderní protokoly pro P2P sítě**
Název bakalářské práce AJ:	Modern protocols for P2P networks

Cíl, metody, literatura, předpoklady:

Cíl: Představit a porovnat moderní P2P protokoly a zhodnotit jejich praktickou využitelnost

Osnova:

Analýza zdrojů

Počítačové sítě

Porovnání P2P protokolů

Závěr, vyhodnocení

DJAMAA, Badis, et al. Efficient and Stateless P2P Routing Mechanisms for the Internet of Things. *IEEE Internet of Things Journal*, 2021.

OLIVEIRA, Leonardo B.; SIQUEIRA, Isabela G.; LOUREIRO, Antonio AF. On the performance of ad hoc routing protocols under a peer-to-peer application. *Journal of Parallel and Distributed Computing*, 2005, 65.11: 1337-1347.

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Karel Mls, Ph.D.
Datum zadání závěrečné práce:	15.10.2021