5G
Möjligheter och hot

PER HURTIG och **TOBIAS PULLS**, Institutionen för Matematik och Datavetenskap, Karlstads universitet

Med framtidens 5G-nätverk kommer en rad hot och möjligheter. Framöver kommer användare ha flera snabba vägar till internet, så som WiFi hemma, eller på jobbet, och tillgång till en snabb 5G-uppkoppling. Projektet **PAF5G** vid Karlstads universitet, finansierat av Internetstiftelsen, kommer i tre år att forska på hur slutanvändare bäst kan använda flera uppkopplingar samtidigt för att få så bra prestanda och anonymitet som möjligt. Förhoppningen är att moderna transportprotokoll som MPTCP kan användas för att få bästa möjliga prestanda genom att på ett smart sätt använda alla tillgängliga uppkopplingar samtidigt. I anonymitetsnätverk som Tor gör flera vägar det möjligt för användare att sprida ut sin trafik på så sätt att det förhoppningsvis blir svårare för attackerare att analysera trafiken och samtidigt bidrar till bättre prestanda.

Om projektet PAF5G

Namn
Performance and Anonymity in Future 5G Networks (PAF5G)

Vilka
Per Hurtig och Tobias Pulls

Finansiär
Internetstiftelsen

När
2019-2022

Mål
Att bättre förstå hur framtida 5G nätverk kan användas
för att förbättra prestandan och anonymiteten för slutanvändare
på internet genom att använda flera uppkopplingar samtidigt.

1. Introduktion

Både användningen av, och antalet, mobila enheter som kommunicerar över internet har skjutit i höjden. Det amerikanska företaget Cisco undersöker årligen våra mobilvanor och slog redan för ett par år sedan fast att antalet mobila enheter nu är större än antalet människor på jorden[1]. Denna enorma utveckling var svår att förutse när det första mobila kommunikationssystemet standardiserades för ca 40 år sedan. Detta, den första generationens, mobilsystem var helt analogt och enbart till för vanligt tal. När sedan den andra generationen (2G) standardiserades och lanserades 1991 fanns nya funktioner som gjorde det möjligt att skicka både text- och bildmeddelanden (SMS/MMS) till andra användare. Det tog ett tag innan SMS och MMS började användas, men det tog så småningom en väldig fart och år 2010 skickades det nästan 6.1 biljoner SMS, vilket motsvarar 193.000 meddelanden per sekund[2]. De senare mobilnäten (3G och 4G) bjöd inte på några liknande succéer vad gäller tjänster, men gjorde det istället möjligt att använda tjänster på internet med, för den tiden, godtagbar prestanda. Det går att komma upp i hastigheter på ca fyra megabit per sekund (Mbps) med 3G och att ligga på ca 17 megabit per sekund med 4G[3,4]. Att surfa på internet var förvisso tekniskt möjligt redan med 2G-standarden, men sällan med en prestanda som gjorde det meningsfullt.

När nu den femte generationens mobildatanät (5G) standardiseras är det uppenbart att telekombolagen inte bara vill uppgradera kapaciteten för att matcha den teknikutveckling som sker på internet. Tanken är snarare att 5G ska driva utvecklingen genom att tillgodose tre olika kravprofiler (se Bild 1):

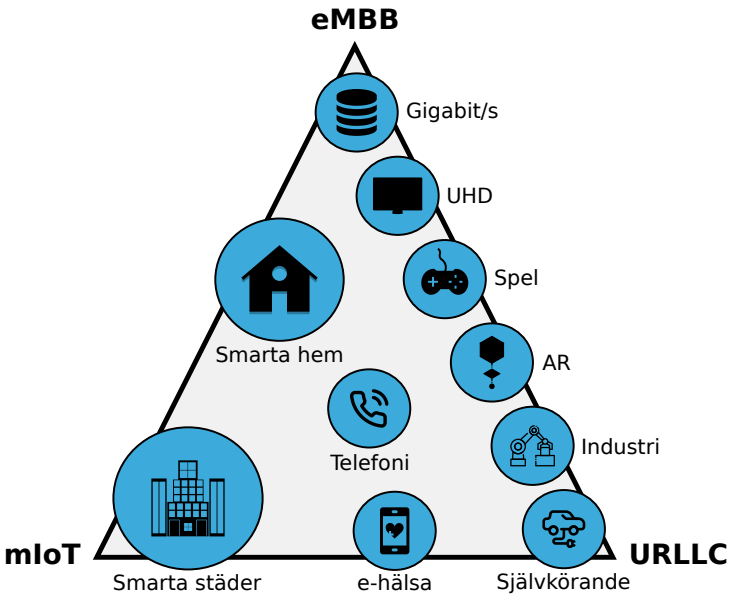


Bild 1. Användningsområden för 5G.

[1] Cisco Systems Inc. *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper.* Febr. 2017.

[2] International Telecommunication Union (ITU). *The World in 2010: ICT facts and figures.* https://www.itu.int/net/itu-news/issues/2010/10/04.aspx. Dec. 2010.

[3] Opensignal. *The State of LTE.* https://www.opensignal.com/reports/2018/02/state-of-lte. Febr. 2018.

[4] Dessa hastigheter är genomsnittsvärden baserade på mätningar över hela världen. Den version/variant av 3G och 4G som används, samt i vilken del av världen man befinner sig, och många fler faktorer spelar väldigt stor roll för den hastighet man kan uppnå. Det är, med 3G, teoretiskt möjligt att nå hastigheter upp till 21.6 Mbps och med 4G upp till 1 Gbps, även om detta sällan, eller aldrig, har gjorts.

(i) **eMBB** (enhanced mobile broadband) ska möjliggöra väldigt höga nedladdningshastigheter. I tätbefolkade områden ska eMBB kunna erbjuda hastigheter mellan 300 Mbps och 1 Gbps. I glesbebyggda områden ska åtminstone 50 Mbps kunna nås. Denna profil liknar de uppgraderingar som tidigare gjorts av mobilnäten, dvs högre hastighet. Exempel på applikationer som eMBB ska stödja kan ses i Bild 1 och inkluderar streaming av ultra HD och augmented reality (AR).

(ii) **URLLC** (ultra-reliable low-latency communication) som ska garantera låg fördröjning för kommunikation som har krav på snabb interaktivitet snarare än hög bandbredd. Tanken är att URLLC ska garantera att fördröjningen mellan ändpunkter inte överstiger en millisekund, och målet är att möjliggöra applikationer inom processindustri och kontroll av självkörande fordon.

(iii) **mIoT** (massive IoT) ska möjliggöra att en väldigt stor mängd med mindre enheter, ofta placerade på en liten yta, ska kunna kommunicera effektivt. Dessa enheter kräver ofta inte så mycket bandbredd (undantag finns) men kräver oftast rätt så låga fördröjningar. Sensorer i hem och stadsmiljö är det primära fokuset här, men även enheter som exempelvis pulssensorer och dylikt.

För att realisera dessa kravprofiler så kommer 5G-nätet bland annat att använda sig av flera olika accessteknologier. Det kommer, till exempel, vara möjligt att koppla upp sig med både 5G New Radio (NR) och vanligt WiFi direkt mot sin 5G-operatör. 5G NR är en ny radioteknologi som är framtagen för att kunna erbjuda höga hastigheter och låga fördröjningar, vilket bland annat möjliggörs av mycket högre frekvensband än dagens 4G-nät. För att utnyttja förekomsten av flera accessteknologier fullständigt kommer det även vara möjligt att koppla upp sig med, och använda sig av, flera teknologier samtidigt.

5G har alla förutsättningar för att bli väl mottaget av användarna. Förutom att surfa snabbare kommer 5G möjliggöra applikationer vi inte tidigare förknippat med mobilnät. Det finns dock, som alltid, några moln på himlen. Undersökningar visar att användandet av ett högre frekvensband gör att 5G NR är mycket känsligare för störningar än tidigare radioteknologier. Att gå förbi ett träd på nära håll kan t.ex. ge ett kort avbrott i kommunikationen. Sådana korta avbrott har visats fungera väldigt dåligt med de protokoll som mobila enheter (och datorer generellt) använder för att skicka och ta emot data[5]. Användandet av högre frekvensband oroar även meterologer(!) då de satelliter som används för att samla in väderdata har frekvensband som ligger på kollisionskurs med 5G NR[6].

Det finns även flera risker som kretsar kring säkerhet och integritet. Mängder med nya IoT-enheter som ständigt är uppkopplade bådar inte gott med tanke på hur pass dåliga vi är med säkerhetsuppdateringar idag. Vems ansvar är det att se till att den "smarta" äggkokaren eller barnvagnen inte används för industrispionage eller våld i nära relationer[7]? När vi förväntar oss att våra städer och samhället i stort blir "smarta" genom att vara uppkopplade via 5G så får leverantörerna av 5G utrustning och operatörerna av näten mycket makt. Det här ser vi inte minst kring diskussioner om Huawei i västvärlden[8] och t ex när även försvaret visar intresse för att använda den nya tekniken[9].

[5] M. Zhang m. fl. "Will TCP Work in mmWave 5G Cellular Networks?" I: *IEEE Communications Magazine* 57.1 (jan. 2019), s. 65–71. doi: 10.1109/MCOM.2018.1701370.

[6] Alexandra Witze. *Global 5G wireless networks threaten weather forecasts.* April 2019. doi: 10.1038/d41586-019-01305-4.

[7] https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not

[8] https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview.pdf

[9] https://www.foi.se/en/foi/news-and-pressroom/news/2019-08-26-can-5g-be-the-technological-solution-for-defence.html

Med 5G på plats så är det inte heller problemfritt att använda flera accessteknologier. Det är svårt att koordinera kommunikation över flera vägar när dessa vägar har olika egenskaper, egenskaper som dessutom ändrar sig snabbt över tid. Tidigare forskning visar att dålig koordination kan göra att prestandan blir sämre än att bara använda en accessteknologi[10]. Det är även problematiskt ur integritetssynpunkt. Genom att använda flera accessteknologier så sprids trafiken så flera kan få tillgång till den. Trots att trafiken kan vara krypterad så kan det här vara användbart för en attackerare, speciellt om målet är att avanonymisera personer. Det är just de här två perspektiven–prestanda och anonymitet–i framtida 5G nätverk där flera accessteknologier kan användas som projektet PAF5G utforskar. Här näst så tittar vi lite närmare på hur just presentanda och anonymitet kan tänkas påverkas och vart utmaningarna finns.

2. Hur påverkas prestandan?

Det finns inget som automatiskt gör att användandet av fler accessteknologier förbättrar prestandan. Både 5G-system och andra som använder sig av flervägskommunikation behöver en uppsättning smarta mekanismer för att utnyttja vägarna på bästa sätt. Det har under senare år blivit allt vanligare att använda flera vägar när enheter kommunicerar med varandra. Fenomenet som sådant är med andra ord inte ett 5G-specifikt påhitt utan återfinns lite varstans, t.ex., i datacenter.

2.1 Hur data skickas över internet

Innan vi kommer in på hur flervägskommunikation fungerar så börjar vi med hur den fungerar över en väg. Bild 2 visar, schematiskt, hur det ser ut när data skickas från en enhet som är uppkopplad mot internet. Låt oss säga att applikationen som används är en webbläsare. För att den skall kunna kommunicera med en webbserver så behöver de ett gemensamt "språk", eller protokoll som det kallas. För webbklienter och webbservrar heter detta protokoll HTTP. När webbklienten konstruerat vad den vill förmedla till webservern, m.h.a. HTTP, så måste detta på något sätt skickas vidare till själva servern. Eftersom webbläsaren inte vet hur detta skall gå till så överlämnar den detta till ett transportprotokoll, och väntar på svar. Transportprotokollets uppgift är att skicka och ta emot data enligt den servicemodell de erbjuder. Många har säkert hört talats om TCP[11]som är det mest använda transportprotokollet. TCP erbjuder en avancerad transporttjänst där data garanteras att komma fram i oskadat skick. Dessutom innehåller TCP mekanismer som förhindrar stockning på internet, genom att reglera hur fort data får skickas. Det finns även enklare protokoll, såsom UDP[12], som inte ger några garantier alls. Eftersom det är viktigt att all information kommer fram i oskadat skick när man surfar så används TCP-protokollet för att skicka HTTP-trafik. De lager som ligger under transportlagret används sedan för att sköta adressering, routing samt att fysiskt flytta data mellan noder på internet. Vi kommer i den här texten inte fokusera så mycket på dessa lager, inte mer än att de finns och att de kan vara av olika slag.

[10] P. Hurtig m. fl. *Low-Latency Scheduling in MPTCP*. IEEE/ACM Transactions on Networking, February 2019.

[11] Jon Postel. *Transmission Control Protocol*. RFC 793 (INTERNET STANDARD). Updated by RFCs 1122, 3168, 6093, 6528. Internet Engineering Task Force, sept. 1981. url: http://www.ietf.org/rfc/rfc793.txt.

[12] Jon Postel. *User Datagram Protocol*. RFC 768 (INTERNET STANDARD). Internet Engineering Task Force, aug. 1980. url: http://www.ietf.org/rfc/rfc768.txt.

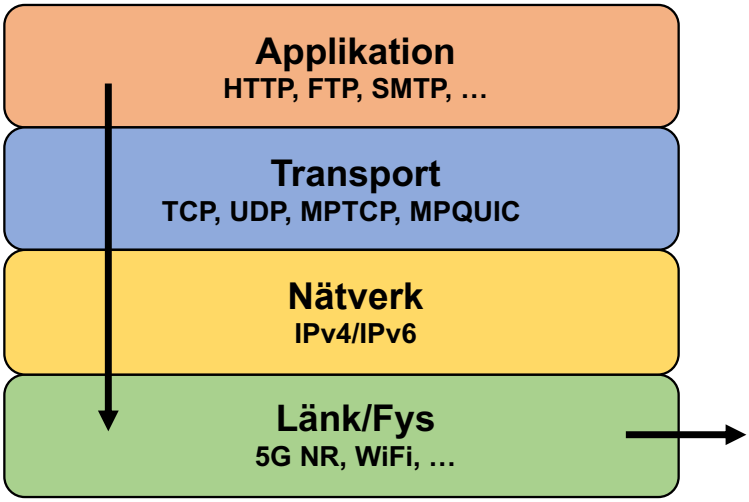


Bild 2. Hur data skickas från en uppkopplad enhet

Sammanfattningsvis kan vi säga att en applikation ofta använder sig av ett applikationsprotokoll för att kommunicera över internet. Detta protokoll är oftast bundet till ett transportprotokoll. Bindningen är inte tvungen men finns oftast eftersom applikationsprotokollet kräver en viss servicenivå från transporten för att fungera. Eftersom TCP erbjuder en så komplett transporttjänst används den av en majoritet av alla applikationer. Som kuriosa kan nämnas att användandet av TCP har blivit så självklart att optimeringar och anpassningar av andra delar av internet har gjorts för att TCP skall fungera så bra som möjligt. Dessutom har allt mer funktionalitet pressats in i transportlagret. Detta har, i praktiken, gjort det omöjligt att lansera nya transportprotokoll. Eftersom det är svårt att lansera nya protokoll så är en möjlig lösning att utöka TCP med ytterliggare funktionalitet. I nästa kapitel beskriver vi hur en sådan utökning, MPTCP, kan användas för att möjliggöra flervägskommunikation.

2.2 Hur flervägskommunikation fungerar

Hur fungerar det då om vi helt plötsligt får flera vägar att kommunicera över? Till skillnad mot envägskommunikation så kommer vi nu få två olika länk/fys-lager samt två nätverkslager, eftersom vi nu har två uppsättningar adresser/nät. Bild 3 visar hur det hela skulle kunna se ut för en enhet som är uppkopplad med 5G NR och WiFi samtidigt. Bilden avslöjar även att vi använder oss av ett annat transportprotokoll än TCP, nämligen MPTCP (Multi-Path TCP)[13]. MPTCP är en utökning av TCP som gör det möjligt att använda flera vägar samtidigt för kommunikation mellan applikationer. Låt oss återgå till vårt förra exempel. Om vi använder en webbklient så kommer applikationen, precis som då, överlämna sin HTTP-data till MPTCP som tar ansvar för att datat levereras till mottagaren. Webbklienten vet inte om, och behöver därför inte anpassas till, att datat kan ta flera vägar samtidigt. Det är sen upp till MPTCP att fördela all data över de olika vägarna så att kommunikationen fungerar så bra som möjligt.

[13] Alan Ford m. fl. *TCP Extensions for Multipath Operation with Multiple Addresses*. RFC 6824 (Experimental). Internet Engineering Task Force, jan. 2013. url: http://www.ietf.org/rfc/rfc6824.txt.

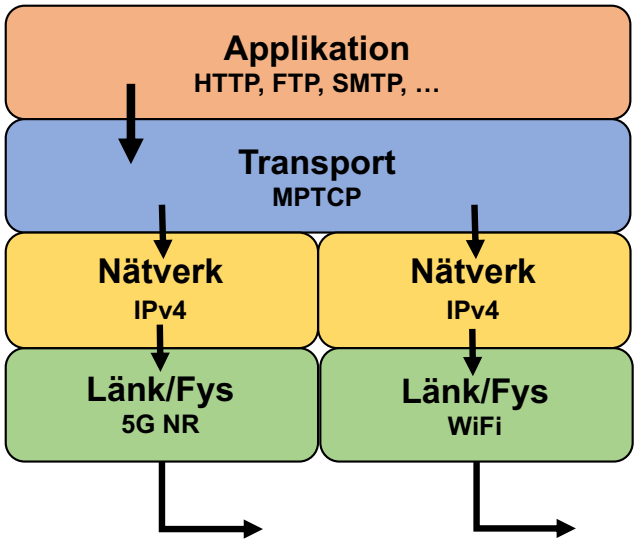


Bild 3. Hur data skickas över flera vägar

Nu skall inte detta exempel ses som den enda sanningen. Det finns även andra protokoll som klarar av flervägskommunikation, och det går att lösa flervägskommunikation på andra ställen än transportlagret. Ett primitivt sätt att hantera flervägskommunikation har säkert de flesta som läser detta testat. Dagens mobiltelefoner är ju oftast utrustade med både 4G och WiFi. Man kan oftast inte använda båda vägarna samtidigt, men det är inte helt ovanligt att man p.g.a. "seg" WiFi förbindelse manuellt slår över till 4G-kommunikation. Detta är kanske den mest primitva formen av flervägskommunikation; då man manuellt växlar aktiv väg. En fördel med att istället använda sig av ett protokoll på transportlagernivå är att det finns mycket information här. Det går att göra väl informerade beslut om hur och när data skall skickas över olika vägar. Det är dessutom bra att använda ett protokoll som är kompatibelt med TCP, eftersom redan existernade applikationer inte behöver göras om och de anpassningar och optimeringar som gjorts i nätet p.g.a. TCPs dominans kan fortsätta att användas.

2.3 Bättre prestanda med fler vägar? Kanske!

Blir det automatiskt bättre om fler vägar används då? Nej, det är inte säkert. Man kan också använda flera vägar för att uppnå olika syften. Ett syfte kan vara att ha en reservväg att hoppa över till om den huvudsakliga vägen slutar att fungera, lite som i exemplet ovan när man byter till 4G från WiFi. Det har dock visat sig svårt att veta exakt när man skall hoppa över till reservvägen i vanliga IP-baserad nät (t.ex. internet). Om det sker först när vägen helt har slutat att fungera så kan det vara för sent för att inte användaren skall märka av det. Om det sker för tidigt, det vill säga när systemet anar att vägen börjar gå sönder, så kan skiftningen ske för fort. Det kanske inte var något problem egentligen, och så har man bytt till en väg med sämre prestanda i onödan.

Det vanliga är dock att använda flera vägar för att öka prestandan, genom att skicka data över vägarna för att på så sätt lastbalansera. MPTCP har visat sig mycket kapabelt i att överföra stora datamängder snabbt. I ett test som gjordes för några år sedan överförde man data över sex olika vägar i en hastighet som gjorde det möjligt att fylla en DVD-skiva

i sekunden[14]. Det finns dock flera fällor när man försöker använda flera vägar för lastbalansering. Om en av vägarna är betydligt långsammare än den andra vägen kommer datat som skickas över denna väg fram senare. Eftersom TCP (och MPTCP) garanterar att data som skickas kommer fram i samma ordning som den skickades kan detta vara ett problem. Låt oss säga att det tar 10 ms att skicka en viss mängd data över 5G NR och 100 ms att skicka samma mängd data över WiFi. Om nu MPTCP väljer att lastbalansera datat över båda vägarna tar det minst 100 ms för den att komma fram. Om bara 5G NR hade valts hade det kunna ta bara 10 ms. Nu är detta ett kraftigt förenklat problem, men i princip skulle det kunna bli så. Det behövs alltså ett smart sätt för att ta reda på vilken väg som skall användas för att skicka data över. MPTCP, och många andra protokoll, har en schemaläggare som räknar ut vilken den bästa vägen är att skicka data över. De schemaläggare som typiskt används är ofta enkla men relativt bra på att fördela data. Det finns dock forskning som visar att man kan åstadkomma mycket bättre prestanda genom att mer noggrant beräkna hur datat bör schemaläggas[15].

Ett annat, intressant, problem är vilken väg som skall användas först. När man påbörjar kommunikation med MPTCP kan man bara göra det över en väg. Först efter att man skickat lite data över denna väg kan man använda nästa. Det har visat sig att valet av denna, första, väg är väldigt viktig för prestandan. Det har också visat sig att det inte är helt enkelt att veta vilken väg som är den bästa.

3. Hur påverkas anonymiteten?

Det finns inget i 5G som direkt leder till bättre anonymitet mot en måttligt stark attackerare: en användares publika IP-adress är lika tillgänglig som tidigare och operatören har tillgång till trafiken. Den "extra väg" man nu kan tänkas få till internet med 5G behöver alltså precis som tidigare något extra för att värna om anonymiteten, såsom världens största anonymitetsnätverk: Tor[16].

Hur påverkas då anonymiteten som Tor ger av att det potentiellt framöver finns flera snabba uppkopplingar att använda? För att förstå hur man kan besvara den frågan behöver vi först titta på hur Tor fungerar och hur man kan tänkas använda flera uppkopplingar i Tor.

Men mixnätverk då?

Du kanske har hört talas om mixnätverk och undrar varför de inte är lika intressanta i sammanhanget. Svaret är att mixnätverk är byggda för att vara säkra mot en attackerare som kan se *all* nätverkstrafik. Med andra ord så spelar det i princip ingen roll om en användare kommunicerar i ett mixnätverk med en eller flera uppkopplingar. Priset för det här starka skyddet är såpass hög fördröjning att det i praktiken inte är användbart för att surfa på nätet, till skillnad från Tor.

Vill du veta mera om mixnätverk?
Läs om Katzenpost på **katzenpost.mixnetworks.org.**

[14] C. Paasch m. fl. *The fastest TCP connection with Multipath TCP.* http://multipath-tcp.org/pmwiki.php?n=Main.50Gbps. 2012.
[15] Hurtig m. fl., *Low-Latency Scheduling in MPTCP.*
[16] https://www.torproject.org/

3.1 Hur Tor fungerar

Tor har miljontals dagliga användare som framförallt använder Tor Browser–en webbläsare baserad på Firefox–för att surfa anonymt och gå runt censur via Tor-nätverket. Tornätverket består av ungefär 6000 *reläer*: servrar som körs av frivilliga världen över som trafik skickas genom[17].

Anslutningar i Tor bygger en krets (eng. circuit) genom tre mer eller mindre slumpvist valda reläer i nätverket, som ett teleskop, med flera lager kryptering där ett lager försvinner per hopp. Genom kretsen kan en klient genomföra TCP/IP anslutningar till valfria publika IP-adresser på internet, där målet endast ser IP-adressen från det tredje och sista reläet i kretsen, inte klientens adress. Bild 4 visar en krets.

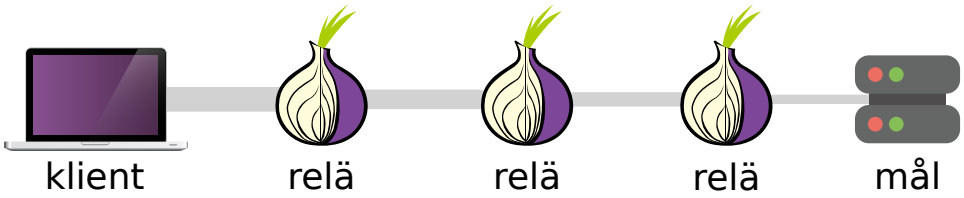


Bild 4. En krets ungefär som ett teleskop med flera lager kryptering från klient till mål genom tre reläer.

Klientens anonymtet skyddas genom att ingen enstaka relä i en krets vet både klientens publika IP adress och målet:

- Det första reläet, vakten (eng. guard), vet klientens och det andra reläets adresser. Reläet kallas en vakt eftersom det "vaktar" klientens riktiga adress från resten av nätverket och det slutgiltiga målet.
- Det andra reläet vet det första och tredje reläets adresser. Det här reläet kallas mitten (eng. middle) reläet eftersom det är i mitten av kretsen.
- Det tredje reläet vet det andra reläets och målets adresser. Eftersom det är här trafiken går ut ur (eng. exit) anonymitetsnätverket till resten av internet så kallas det tredje reläet för ett exit-relä.

En klient skapar många kretsar genom nätverket. I regel får en krets inte användas i mer än tio minuter och trafik isoleras till olika kretsar från webbläsaren, bland annat per öppen flik. Det finns många detaljer som är viktiga här. I vårt fall är det extra viktigt att veta att just det första reläet inte väljs helt slumpmässigt, utan en klient försöker använda samma relä i flera månader. Det är för att det första reläet är extra känsligt då det vet klientens riktiga adress. Om vi antar att en attackerare har kontroll över en del (men inte alla) reläer i nätverket: om du en gång har valt en relä som attackeraren inte har kontroll över, varför byta? Framförallt för användare där konsekvenserna av att bli identifierade är katastrofala är det här extra viktigt. Det är ungefär som att spela rysk roulett, det gör man gärna inte mer än nödvändigt. Att slumpa det andra och tredje reläet i en krets gör att från ett måls perspektiv ser alla Tor-användare likadana ut.

[17] I Sverige finns ungefär 200 Tor-reläer: https://metrics.torproject.org/rs.html#search/country:se.

3.2 Flera uppkopplingar till Tor-nätverket

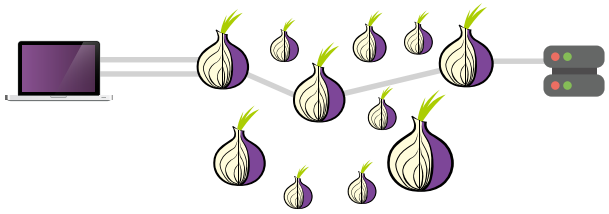
Vi kan tänka oss en rad olika sätt att dela upp uppkopplingarna till och inom Tor-nätverket med olika för- och nackdelar. Bild 5 visar tre intressanta alternativ:

(a) Klienten skapar helt enkelt två eller flera anslutningar över olika uppkopplingar till det första reläet i kretsen: vakten.

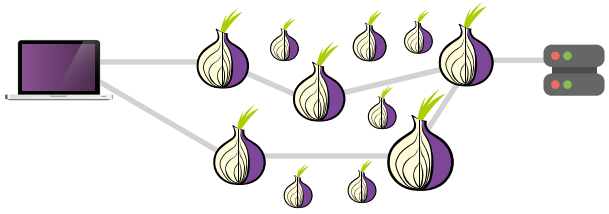
(a) Klienten skapar två separata kretsar genom nätverket som möts genom att använda samma tredje exit-relä.

(a) Klienten skapar två helt separata kretsar med inga gemensamma reläer i Tor-nätverket. All trafik sätts ihop först hos målet.

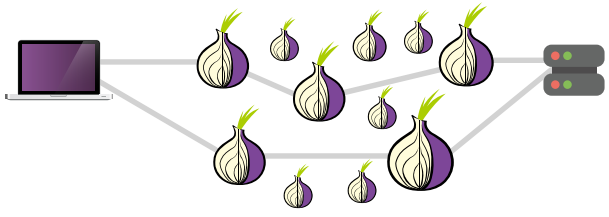
Rent praktiskt så behöver vi bara ändra hur klienten och reläet fungerar för de första två alternativen (Bild 5a och Bild 5b). Det tredje alternativet (Bild 5c) är det värre med: utöver att ändra hur Tor fungerar så behöver alla potentiella mål på internet stödja nya protokoll såsom MPTCP . Vem vet, kanske kommer 5G och framtida tekniker bidra till att protokoll som MPTCP blir vanliga, men det är långt i framtiden om så. Oavsett alternativ så kan vi vara rätt så säkra på att flera uppkopplingar borde bidra till bättre prestanda, speciellt om flera kretsar skapas genom nätverket[18].



(a) Delad vakt



(b) Delad exit



(c) Delat mål

Bild 5. Tre olika sätt att använda flera uppkopplingar i Tor

[18] Mashael AlSabah m. fl. *The Path Less Travelled: Overcoming Tor's Bottlenecks with Traffic Splitting*. PETS 2013.

3.3 Mer eller mindre anonymitet? Nja!

Å ena sidan, om en attackerare endast får tag i en del av trafiken mellan klient och mål blir det svårare för en attackerare att lyckas avanonymisera med de flesta typer av attacker vi känner till. Till exempel så behöver korrelationsattacker en viss mängd trafik för att ge tillförlitliga resultat. Å andra sidan, så sprids trafiken till andra delar av internet när flera uppkopplingar används vilket ger attackerare större chanser att se trafiken.

Med en delad vakt sprids trafiken endast mellan klient och vakt via uppkopplingarna. Detta hjälper mot lokala attackerare såsom internetleverantörer, men trafiken kommer troligen till del använda samma "väg" till vakten då infrastruktur och nätverk delas mellan olika operatörer i hög grad på internet. Det här är speciellt fallet om vakten ligger geografiskt långt bort från klienten, vilket är troligt för klienter utanför Europa och USA, där de flesta reläer i Tor-nätverket finns.

Alternativet med en delad exit sprider trafiken i betydligt större grad. Att använda två uppkopplingar med olika vakt-reläer gör att ett enstaka flöde med trafik kan sakna vital information för en attackerare. Nackdelen är att två vakter känner till klientens IP-adress. Frågan är om det, ur anonymitetssynpunkt, finns så stora vinster med fler än två dock. Det här alternativet är en favorit bland Tor-utvecklare och har visat lovande resultat i en utvärdering för några år sedan.

Sist men inte minst, ett delat mål sprider trafiken maximalt. Ingen enstaka server eller nätverk måste se all trafik, bara klienten och målet. De praktiska hindren är stora dock, då internet behöver fundamentalt ändras eftersom målen behöver stödja tekniker såsom MPTCP. Frågan är om 5G kommer långsiktigt bidra till detta?

4. Sammanfattning

Det har under senare år blivit allt vanligare att använda flervägskommunikation över nätverk, i syfte att öka prestanda och redundans. Med lanseringen av 5G, där flera accessteknologier kommer att användas, kommer denna utveckling troligtvis accelerera. I och med att denna typ av kommunikation kommer att bli vanligare tror vi även att andra forskningsfrågor–frågor som inte bara rör prestanda–kommer att bli mer uppmärksammade. Ett område som få forskare inom transportprotokoll undersöker, men som påverkar alla användare på ett fundamentalt sätt, är anonymitet. Hur anonymiteten påverkas av flera uppkopplingar beror på hur uppkopplingarna används. Det är en fördel att kunna begränsa tillgången till trafik för vissa attackerare, men flera uppkopplingar leder oundvikligt till att potentiellt flera attackerare kan få tillgång till trafiken. I fallet Tor har vi flera möjliga vägar att gå framöver. Avvägningarna är många i anonymitetsnätverk och det gäller att hitta bästa möjliga lösning för att få så många fördelar som möjligt–inte minst bättre prestanda–nu när det tekniska landskapet ritas om av 5G. Oavsett på vilket sätt flera uppkopplingar används så behöver klienter förstå hur dom ska dela upp trafiken mellan uppkopplingarna för att optimera inte bara prestanda utan göra det så jobbigt som möjligt för attackerare. Det här kommer vi titta vidare på inom ramen för PAF5G projektet.