DPI – Deep Packet Inspection

mag. Roman Kotnik

Univerza v Ljubljani
Fakulteta za elektrotehniko
Laboratorij za telekomunikacije

Ljubljana, 10. maj, 2011

Razlogi za DPI

- Novi viri prihodkov
  - ISP-ji, podjetja
- Reševanje problemov tipa "ozko grlo"
- Zaznavanje vdorov
  - napad DOS
  - „Buffer overflow"
- Ciljno oglaševanje
- Izboljšanje kakovosti storitev
  - preprečevanje P2P prometa
  - povratne informacije od uporabnikov

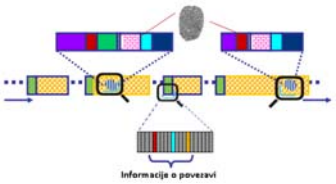
Kaj je DPI

- DPI – Deep Packet inspection
- Vpogled v vsebino komunikacij
  - pomembna tehnologija za identificiranje in preverjanje istovetnosti protokolov in aplikacij
  - analiza se izvaja glede na vsebino in ne glede na glavo IP-paketa – analogija s poštnim sporočilom

4-bit	8-bit	16-bit	32-bit
Različica	Dolžina glave	Tip storitve	Celotna dolžina
Identifikacija		Zastavice	Zamik
Čas življenja paketa	Protokol	Vsota za preverjanje paketa	
Naslov izvora			
Naslov ponora			
Možnosti in zamiki			
Vsebina oz. payload			

Osnovni mehanizmi za DPI

- Kaj je elektronski podpis?
  - elektronski podpis so vzorci, ki so izbrani za unikatno identifikacijo aplikacije ali protokola



- Napake pri podpisih
  - "False negative"
  - "False positive"

Kaj omogoča DPI

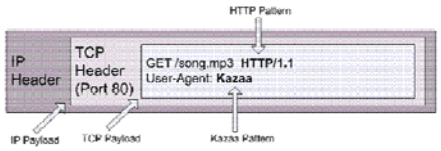
- Nadzor nad uporabniki in omrežjem
  - poznamo vsebino, posledično poznamo uporabnike in omrežje
- Zaračunavanje glede na vsebino
  - interes ISP – konflikt internetne nevtralnosti
- Nadzor prometa
  - prioritiziranje določenega tipa prometa
- Izboljšave elektronske varnosti
  - interes podjetij – preprečevanje napadov
  - preprečevanje uhajanja vsebin
- Legalni nadzor

Analiza glede na vrata

- Najenostavnejša in najbolj poznana
- Aplikacije večinoma uporabljajo privzeta vrata
  - POP3 – vrata 110
  - SMTP – vrata 125
- „Sindrom vrat 80"
  - Druge aplikacije delujejo na vratih 80 s tem namenom, da se pretvarjajo, kot da so HTTP promet.
- Nekatere aplikacije uporabljajo naključna vrata, da bi prikrila svoje delovanje
- Analiza ni zadostna in jo moramo uporabljati v kombinaciji z drugimi

Analiza glede na ujemanje z besedno zvezo

- Iskanje sekvenc tekstovnih znakov znotraj vsebine paketa
- Aplikacija, kot je npr. Kazaa, uporablja besedo „Kazaa“ znotraj HTTP GET zahteve
- Uporaba regularnih izrazov



Analiza glede na numerične lastnosti

- Preiskovanje aritmetičnih in numeričnih karakteristik znotraj paketa ali več paketov
  - dolžina vsebine paketa (payload)
  - število poslanih paketov
  - numerični zamik neke besede
- Primer povezava preko UDP v Skype

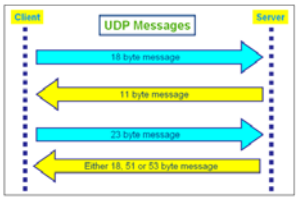


Figure 4: Skype (versions prior to 2.0) numerical properties analysis

Analiza glede na obnašanje in hevristiko

- Deluje glede na delovanje protokola
- Iskanje statističnih parametrov
- Iskanje vzorkov in posledic, ki se ujemajo
- Zahtevna analiza, ki zahteva poznavanje delovanja aplikacije
- Primerjava HTTP in P2P prometa

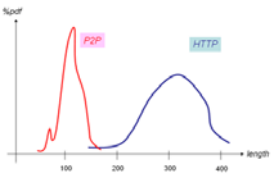


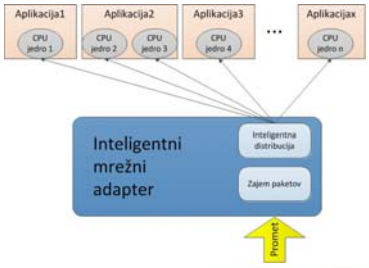
Figure 5: HTTP vs. P2P

Enkripcija in obfuskacija

- Namen: prikrivanje podatkov
- Enkripcija:
  - kodiranje
  - matematični algoritmi
  - uporaba ključa
  - RC4 enkripcija – Bittorrent
- Obfuskacija
  - „zameglitev“
  - dodajanje nepomembnih vsebin z namenom prikrivanja tiste, bistvene

Izvajanje DPI

- DPI sestavljen iz dveh glavnih funkcionalnosti
  - zajem paketov
  - procesiranje paketov
- Uporaba PC strežnikov



DPI za mobilne operaterje

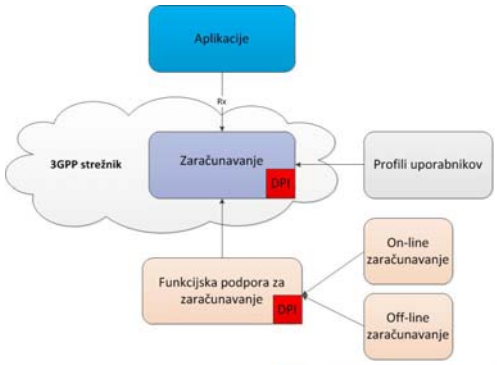
- Porast uporabe pametnih telefonov (HSDPA, HSUPA)
- Trenutno 5 milijard uporabnikov mobilnih telefonov
- Statistika prometa
  - 5 % uporabnikov uporablja 90% kapacitet
  - vsakih 6 mesecev se prenosi povečajo 2×
  - do 2014 – video predstavlja 66 % prometa
- Aplikacije so podatkovno požrešne (YouTube)
- Problematika zagotavljanja pasovne širine
- ISP-ji želijo poznati uporabnike, da lahko zagotovijo QOS
  - to jim omogoča DPI

DPI za mobilne operaterje

- Operaterji morajo zagotoviti pasovno širino in QOS
- Glavni izziv je zagotoviti delovanje omrežja z nizkimi investicijami
  - mesečno zaračunavanje je rizično – z večjo porabo porabnika ne dobimo več denarja – "efekt škarij"
- DPI omogoča mobilnim operaterjem, da se zavedajo vsebin, ki se pretakajo po njihovih omrežjih v realnem času
  - primer prenosa videa
- DPI "throttling"
  - povečevanje in zniževanje prioritet posameznega prometa

DPI in zaračunavanje

Implementacija DPI v mobilno omrežje



DPI pri podjetjih

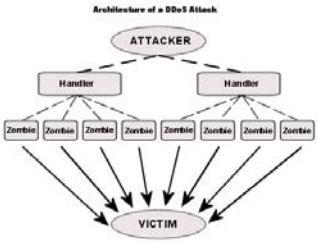
- Elektronska varnost
  - zaščita pred vdori, ki lahko povzročajo milijonske škode
- Nadzor nad zaposlenimi
- Preprečitev uhajanja informacij
- Zaščita avtorskih vsebin
- Proizvajalci DPI opreme
  - Cisco
  - Pcube
  - Nokia
  - Ericsson
  - Juniper
  - Ellacoya

Možnosti DPI pri zaračunavanju

- Trenutno deluje sistem le glede na prenesene podatke
  - 100 MB/mesec = x €, 1 GB/mesec = x + €
- Uporabniki, ki ne uporabljajo veliko aplikacij plačujejo za tiste, ki jih uporabljajo v velikih količinah
- S pomočjo DPI poznamo profil uporabnika
  - lahko mu zaračunamo glede na aplikacije, ki jih uporablja
    - lahko bi segmentirali posamezne pakete glede na aplikacije
      - npr: P2P paket, online gaming paket …
  - sistem cenejši za tiste, ki ne uporabljajo veliko aplikacij
- Možnost zaračunavanja glede na čas prenosa podatkov
  - npr. brezplačen prenos ponoči

Uporaba DPI – preprečevanje vdorov

- Požarni zidovi ne opazujejo vsebine paketov
  - napadi se selijo iz omrežnega nivoja na aplikacijski nivo
- S pomočjo DPI lahko zaznamo in izločimo promet, ki je potencialno nevaren
- Delovanje v realnem času
- IDS/IPS sistemi delujejo na osnovi DPI
- Napadi:
  - DOS
  - prenapolnjenje spomina

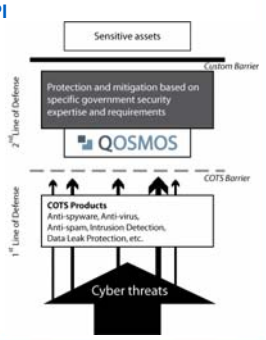


Uporaba DPI – Filtracija prometa

- Pri filtraciji pogledamo vsebino vsakega paketa in se na podlagi le-te odločimo, ali bomo paket pustili naprej ali ne
- Tipi filtriranja
  - statično – se ne zaveda ali je paket prvi ali zadnji ali vmes
  - dinamično – zavedanje ali gre za zahtevek ali odgovor, pomembno predvsem, ko je dovoljen UDP promet
- Klasifikacija prometa pri ponudnikih internetnih storitev
  - občutljiv promet – VoIP, Online gaming, video-konference
  - "Best-effort"– P2P, e-mail – pomembno samo, da pride čez
  - neželjen promet – spam, črvi, botnet, napadi
- Onemogočanje ilegalnih, piratskih vsebin

Uporaba DPI – Kibernetska varnost

- Poleg obstoječih aplikacij za zaščito lahko uporabimo tudi DPI
- Zaščita pred neželeno pošto, virusi in zlonamernimi programi (spyware, malware)



Uporaba DPI – Data retention

- Shranjevanje podatkov o povezavah
  - naslovniki in prejemniki poštnih sporočil
  - telefonski klici (VoIP)
  - obiskane spletne strani
- Glavni namen je analiza prometa in masovni nadzor
- Izvajajo ga vladne organizacije in večja podjetja
- Različno legalno ozadje v državah
  - EU – 6 mesecev do 2 leti shranjevanja
- Argumenti proti izvajanju
  - ni zasebnosti
  - veliko strojne opreme za shranjevanje vseh podatkov
  - zlouporaba

Dodatne uporabe DPI

- Starševski nadzor (parental control)
  - URL filtracija ni več dovolj
  - filtracija IM, P2P, IPTV
  - uporabnik sam nastavlja želene filtre
- Uveljavljanje uporabniške politike
  - nadzor nad avtentikacijami in avtorizacijami
- Filtriranje avtorsko zaščitenega materiala
  - veliko povpraševanja s strani YouTube za odstranjevanje avtorsko zaščitenih vsebin
- Ciljno oglaševanje
  - v kolikor poznamo strani, ki jih obiskuje uporabnik mu lahko ponudimo primerne oglase
- Legalni nadzor

Primeri uprabe DPI 1/3

- Proaktivna optimizacija storitev glede na navade in vrednost stranke/uporabnika
  - Pomembnost določenih storitev za uporabnika
  - Alarmiranje v primeru poslabšanja parametrov omrežja
  - Sprememba uporabnikovih nastavitev
    - Spremembe prioritet
  - Druge akcije glede na uporabnikovo vedenje
    - Prestavitev uporabnika v drugo omrežje (če je na voljo)
    - Alarmiranje (prenehanje uporabe storitve, nove naprave)
    - Možnost uporabe dodatnih storitev glede na obnašanje podobnih uporabnikov
  - Prilagajanje in ponujanje paketov za uporabnike ki uporabljajo malo storitev

Primeri uprabe DPI 2/3

- Starševski nadzor
  - Pametni telefoni in sirokopasovnia mobilna omrežja
  - Nadzor nad aktivnostjo otrok vedno bolj problematičen
  - Priložnost za razširitev in spremembo starševskega nadzora z uporabo DPI.
  - Operaterji lahko omogočijo:
    - Filtriranje neželjenih aplikacij in spletnih strani
    - Onemogočanje določenih aplikacij glede na lokacijo in čas
    - Obveščanje staršev o novih nevarnostih
    - Obveščanje o porabi
    - Obveščanje o neželjenih vsebinah
    - Analizo obnašanja uporabe interneta za otroke
  - Starševski nadzor kot aplikacija

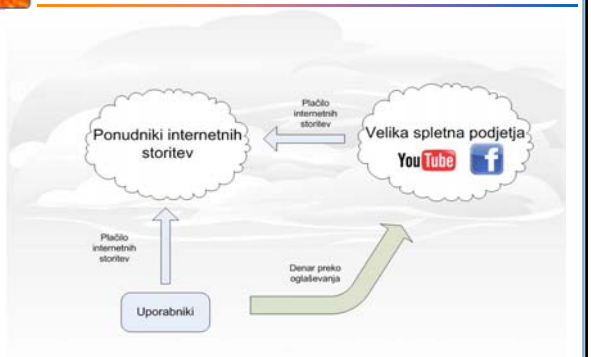
Primeri uprabe DPI 3/3

- Analize in podatki
  - Cilj mobilnih operaterjev je sodelovanje z zunanjimi ponudniki vsebin, razvijalci aplikacij in web portali
  - Operaterji imajo veliko podatkov ki so pomembni za razvijalce in ponudnike vsebin.
  - Vprašanja na katere lahko odgovorijo
    - Čas uporabe določene aplikacije.
    - QoE.
    - Kje je storitev uporabljena, na kateri napravi, kdaj?
    - Kaj uporabniki kupujejo, katere druge storitve uporabljajo?
    - Nasveti za vsebine in storitve
  - Informacije podlaga za
    - QoS
    - Ciljno oglaševanje
    - Avtomatsko prilagajanje na napravo ali lokacijo

Internetna nevtralnost

- Glavno načelo – ves promet na internetu je obravnavan enako
  - ISP-ji lahko prioritizirajo promet in sami določajo pravila po katerih bo internet deloval
  - imajo dober izgovor – preprečujejo napade
- Ekonomsko stališče
  - oskrba – pasovna širina – ISPji
  - povpraševanje – aplikacije – uporabiki
- ISP-ji prodajo več, kot lahko zagotovijo
  - iščejo rešitve za reševanje problema velikega porasta v povpraševanju po pasovni širini

Internetna nevtralnost



Primeri DPI aplikacij

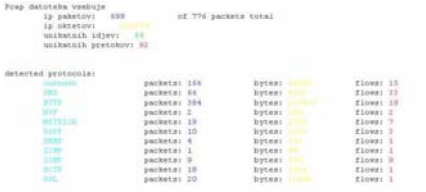
- Argus
  - nadziranje mrežnih storitev in strežnikov
  - odprtokodna rešitev
  - podpora IPv4 in IPv6, izrisovanje grafov
  - spletni vmesnik
- Arpwatch
  - spremlja ethernet – IP tabelo
  - uporaba libpcap
  - odprtokodna rešitev
- Barnyard
  - plugin za SNORT – pospešuje delovanje IDS/IPS sistema
- SILK (System for Internet-Level Knowledge)
  - za velika omrežja, srednje velike ISP

Primeri DPI aplikacij

- L7 – filter
- IPP2P
- HiPPIE
- nProbe
  - odprtokodna rešitev sonde za zaznavanje in zajemanje velike količine prometa
- Ntop
  - podobno kot linux ukaz top poraba mrežnih kapacitet
  - Libpcap, spletni vmesnik
- SANCP (Security Analyst Network Connection Profiler)
  - nadzira podatke o povezavah
  - zmožnost označevanja povezav
- OpenDPI

OpenDPI

- Odprtokodna DPI rešitev
- Prednosti
  - podpora za velik nabor protokolov
  - odprtokodna skupnost
- Slabosti
  - konzolno upravljanje
  - post-procesiranje



IWGDPT proti uporabi DPI

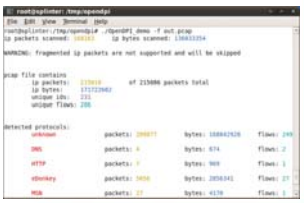
- Mednarodna delovna skupina za varstvo osebnih podatkov v telekomunikacijah (International Working Group on Data Protection in Telecommunications - IWGDPT),
- Mednarodna delovna skupina IWGDPT je v mnenju poudarila, da operaterji elektronskih komunikacij ne smejo na noben način posegati v zaupnost in celovitost komunikacije, če to ni izrecno dovoljeno ali zahtevano z zakonodajo. V luči navedenega mednarodna delovna skupina IWGDPT izrecno opozarja operaterje elektronskih komunikacij naj se ne poslužujejo uporabe DPI tehnologij za ciljno oziroma vedenjsko oglaševanj

Kontakt:

roman.kotnik@ltfe.org

OpenDPI

- **Odprtokodna DPI rešitev**
- **Prednosti**
  - **podpora za velik nabor protokolov**
    - **standardni (HTTP, FTP …), P2P, VoIP, IM, strujanje, tuneliranje, igralski …**
  - **odprtokodna skupnost**
- **Slabosti**
  - **konzolno upravljanje**
  - **post-procesiranje**
- **Delovanje obstoječe rešitve**
  - **zajem datoteke – Wireshark**
  - **izpis rezultatov OpenDPI**



Realne uporabe DPI danes

- **Traffic management control**
  - **Fair usage control/mandate/policy**
  - **IP session (DHCP model)**
  - **Assured QoS for third party applications and content (OTT)**
  - **Turbo button**
  - **Bill shock prevention (EU)**
- **Charging control**
  - **Variable charging and pricing (time of day, content downloads)**
  - **Quota limiting (EU mobile broadband roaming in FMC)**
- **Targeted advertising**
- **Security**
  - **Parental control**
  - **LI**
  - **Detection (DOS, DDOS, "buffer overflow")**