Analýza a identifikácia správania Tor klientov

Ing. Tibor Engler | Školiteľ: **Ing. Tomáš Čejka, PhD.**

Fakulta informačních technologií ČVUT v Praze

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Motivácia

- Sieť Tor by mala zabezpečiť anonymitu svojich užívateľov pomocou smerovania cez 3 náhodne vybrané servery.
- Ak budeme simulovať všadeprítomnú autoritu, dokážeme korelovať komunikáciu klienta s Tor-om a Tor-u s cieľovým webserverom a zistiť tak, aké stránky si klient pozerá?
- Predchádzajúce experimenty na túto tému využívali rôzne štatistické metriky (Pearson, Bayes), ktoré sa ukázali byť neefektívne.
- V roku 2018 bola prvýkrát použitá neurónová sieť – detekcia z prvých 300 paketov v každom smere – ich medzipaketové opozdenia (IPD) a veľkosti [2].
- V tejto práci použijeme konvolučnú neurónovú sieť (CNN) a agregované dáta len z prvých 100 paketov, čo je 6x menej dát.

Design experimentu

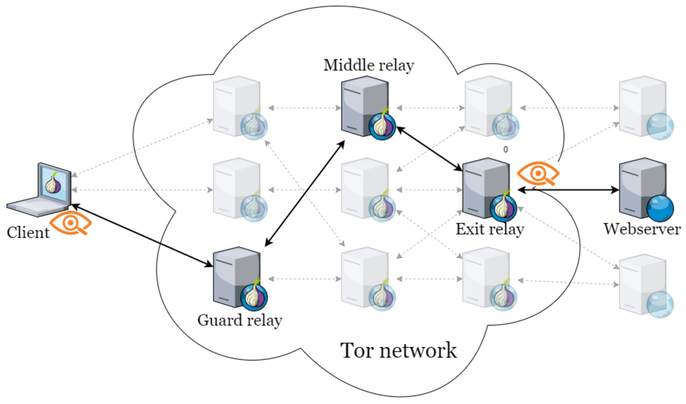

Fig. 1: Umiestnenie sond

- Aby sme sa priblížili čo najviac reálnemu scenáru, používame vlastný Tor server.
- Odpočúvame medzi klientom a vstupným Tor uzlom (Guard Relay) a medzi naším výstupným Tor uzlom (Exit Relay) a cieľovým webserverom. Na odpočúvanie používame monitorovací systém NEMEA [1], ktorý nám poskytuje agregované informácie o odpočúvaných sieťových tokoch a síce: IPD, dĺžky a smery prvých 100 paketov a histogramy rozdelenia týchto paketov v čase a veľkosti.
- Exit Relay je VPS hostované v ČR, na klientovi beží VMWare a štandardný Tor Browser. Pomocou Selenium a Stem ovládame klientský webový prehliadač, ktorý si automatizovane prezerá webstránky zo zoznamu Alexa's Top 15 000.

Spracovanie dát v CNN

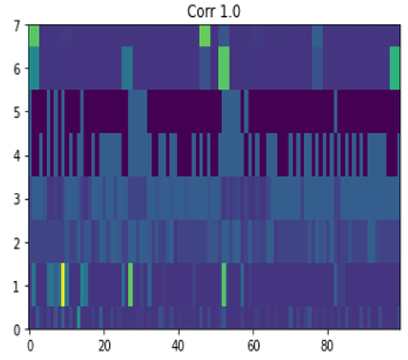

Fig. 2: Reprezentácia dát pre CNN

- Agregované dáta každej dvojice odpočutých dátových tokov následne transformujeme do dátovej štruktúry, špeciálne navrhnutej pre tento experiment a zobrazenej na obrázku č. 2, ktorá pozostáva z:
  0. riadok – Klient: IPD prvých 100 paketov
  1. riadok – Server: IPD prvých 100 paketov
  2. riadok – Klient: veľkosti prvých 100 paketov
  3. riadok – Server: veľkosti prvých 100 paketov
  4. riadok – Klient: smery prvých 100 paketov
  5. riadok – Server: smery prvých 100 paketov
  6. riadok – Klient: histogram IPD download, histogram veľkostí downoad, histogram IPD upload, histogram veľkostí upload
  7. riadok – Server: detto
- Takto odchytené a spracované dvojice tokov slúžia ako korelované vzorky pre trénovací proces CNN. Nekorelované vzorky si na požiadanie vieme vyrobiť kombináciou klientskej časti z jedného toku a serverovej časti z iného toku.
- Na trénovanie a detekciu používame model na obrázku č. 3. Trénovanie prebieha nad 884 000 vzorkami, z čoho 4 420 je korelovaných a ku každej korelovanej vzorke je dogenerovaných 199 nekorelovaných.

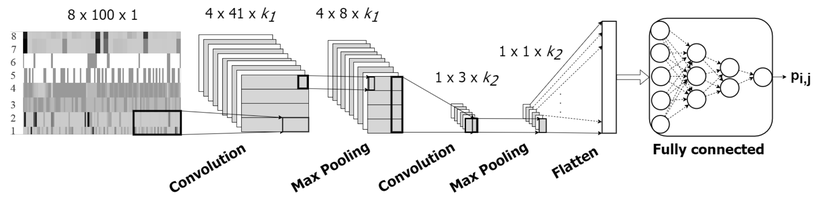

Fig. 3: Model CNN

- $k_1 = 2000$, $k_2 = 800$, $N_{pos} = 4420$ (Alexa's Top 1–5000), $N = 884\,000$

Výsledky

Výsledok na kontrolnom datasete

- $N = 3\,156\,000$ (Alexa's Top 5001–10 000 – disjunktné s tréning. datasetom)
- $N_{neg} = 999$ na každú korelovanú vzorku
- $Accuracy = 0.999$ – neobjektívne kvôli nevyváženému datasetu
- Použijeme F_4 skóre
  - nájdeme optimálny pomer medzi Precision a Recall
  - väčší dôraz na malý počet False Negatives (chceme vysoký Recall aj za cenu nižšej Precision)
- $F_4 = 0.917$ – výborný výsledok, $Recall = 0.934, Precision = 0.708$

Validačné datasety

- Spomalený dataset (rýchlosť na Tor uzle spomalená na polovicu): $N = 2\,005\,000$, $Recall = 0.925, F_4 = 0.903$
- Nekorelované vzorky z tej istej domény: $N = 6\,214$, $Recall = 0.992, F_4 = 0.992$
- Externý dataset (dataset z inej diplomovej práce obsahujúci iné správanie, než prezeranie webstránok): $N = 441$, $Recall = 0.952, F_4 = 0.867$
- Všetky datasety dohromady: $N = 2\,946\,900$, $Recall = 0.958, F_4 = 0.944$

Zhrnutie

- Sieť Tor neposkytuje zaručenú anonymitu, ak komunikáciu na oboch koncoch siete sleduje ten istý útočník.
- CNN s mojím modelom má úspešnosť cca 95 % za použitia agregovaných štatistík len z prvých 100 paketov.
- Vďaka tomu môže byť takáto detekcia nasadená v praxi, z čoho vyplýva nebezpečie zneužitia.
- Ponaučenie: ani Tor nechráni svojich užívateľov na 100 % a pri rastúcich možnostiach Deep Learningu je potrebné začať diskutovať o zmene jeho dizajnu.

Referencie

[1] Tomas Cejka et al. "NEMEA: A Framework for Network Traffic Analysis". In: *12th International Conference on Network and Service Management (CNSM 2016)*. 2016. DOI: 10.1109/CNSM.2016.7818417. URL: http://dx.doi.org/10.1109/CNSM.2016.7818417.

[2] Milad Nasr, Alireza Bahramali, and Amir Houmansadr. "DeepCorr". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Jan. 2018). DOI: 10.1145/3243734.3243824. URL: http://dx.doi.org/10.1145/3243734.3243824.