Forgalmi mérések a gyakorlatban

Mérési segédlet

Bevezetés

A különböző informatikai hálózatok tervezéséhez, fejlesztéséhez, menedzsmentjéhez elengedhetetlen, hogy megfelelő képünk legyen a rajtuk áthaladó forgalom főbb jellemzőiről. Különböző szoftvereknél szintén lényeges lehet a hálózati erőforrás igény (gondoljunk csak a mobiltelefonok üzemidejére). A hálózati forgalom mennyisége és jellege függ az adott hálózattól/alkalmazástól, és az idő múlásával jelentős változásokon mehet keresztül. Nyilvánvaló például, hogy egy internetszolgáltatónak egészen más típusú és mennyiségű forgalmat kell elvezetnie, mint akár csak néhány évvel ezelőtt. Emiatt ahhoz, hogy reálisan lássuk egy hálózat terheltségét forgalmi méréseket kell végeznünk, majd ezeket a méréseket megfelelő módszerekkel elemeznünk kell. A laborgyakorlat célja, hogy bemutassa, milyen eszközökkel lehet ezeket a mérési és elemzési lépéseket elvégezni, valamint betekintést adjon abba, hogy a különböző alkalmazásokra milyen forgalmi minták jellemzők, és ezek milyen hatással lehetnek a hálózat terheltségére. Egy részletes elemzés számos tulajdonság vizsgálatára kiterjedhet (pl. folyamok száma és időbeli hossza, használt protokollok stb).

Hálózati mérések és forgalmi jellemzők

A hálózati méréseket két nagy csoportra oszthatjuk: aktív és passzív mérésekre. Aktív mérés esetén valamilyen módon kommunikációt indítunk a hálózaton keresztül, mérjük a kommunikációs folyamot és elemezzük tuljadonságait. Passzív mérés esetén tipikusan a hálózat egy adott linkjén passzívan hallgatózunk, mérjük és rögzítjük az áthaladó üzenetek főbb jellemzőit.

Az aktív méréseknek számos formája létezik, kezdve az egyszerű pingtől alkalmazások forgalmának vizsgálatán át olyan mérésekig, melyek számos hálózati vég- és csomópontot ölelnek fel. A mérések korlátozódhatnak csak a végpontok vizsgálatára, de kiterjedhetnek a köztes hálózati csomópontokra is. Aktív mérések segítségével jól elemezhetjük egy adott alkalmazás forgalmi mintáit, valamint kiválóan alkalmasak végpontok közötti hálózati jellemzők mérésére (pl. késleltetés, késleltetés ingadozás, észlelt szolgáltatási minőség, stb.)

Passzív mérések segítségével általános képet kaphatunk a hálózaton (linken) lévő forgalomról. Gyakran vizsgált jellemzők például a link kihasználtsága és ennek változása, a forgalom protokollok és portok szerinti megoszlása, a csomaghosszak eloszlása, a flow-k (kommunikációs folyamok) hosszának eloszlása, stb.

Statisztikai alapok

A hálózaton mért forgalom jellemzésére különböző statisztikákat használhatunk. Amennyiben a forgalomra, mint csomagok sorozatára tekintünk, a csomagok minden egyes jellemzőjét egy $\{v_i\}$ vektorba foghatjuk össze.

Egy számokból álló $\{v_i\}$ mintasor legegyszerűbb jellemzői közé tartozik annak k-adik momentuma, melyet a

$$m_k = \frac{1}{N}\sum_{i=1}^{N} v_i^k$$

képlet segítségével számíthatunk, ahol N a mintasor elemeinek száma. Általában kitüntetett szerepet kap az első momentum (átlag) és a második momentum, melynek segítségével a minta szórása számítható. Adatsorok jellemzésére használnak magasabb momentumokat is, azonban tipikusan minél magasabb a momentum, annál jobban ingadozhat két azonos eloszlásból vett mintasor esetén.

Gyakran használatos jellemző a mintasor szórása is, mely az adatsor elemeinek átlagtól való eltérését, a minták „szétterültségét" jellemzi. Ezt a fenti jelölés segítségével a

$$\sigma = \sqrt{m_2 - m_1^2}$$

képlettel írhatjuk le. Ez a mennyiség azonban függ a mintasor elemeinek átlagos nagyságától, ezért sokszor célszerűbb a relatív szórás használata, mely a szórás normalizált változata és a

$$c_v = \frac{\sigma}{m_1}$$

képlet segítségével számítható.

Az eddigiekben néhány paraméterrel jellemeztük a mintasort. A mintasor eloszlásának részletesebb leírására többek között tapasztalati eloszlás- és tömegfüggvényket használhatunk. Egy X diszkrét valószínűségi változó eloszlásfüggvénye a

$$F(x) = Pr(X \leq x),$$

tömegfüggvénye a

$$f(x) = Pr(X = x)$$

képlet segítségével adható meg. A gyakorlatban ezeket a függvényeket a minták alapján a tapasztalati eloszlás- és tömegfüggvénnyel tudjuk közelíteni. A $\{v_i\}$ mintasorhoz tartozó tapasztalati eloszlásfüggvény

$$F_N(x) = \frac{1}{N}\sum_{i=1}^{N} I(v_i \leq x),$$

hol $I(\alpha)$ az indikátorfüggvény, aminek értéke 1, ha α igaz, és 0 egyébként, N pedig a mintasor elemeinek száma. Hasonlóképpen a tapasztalati tömegfüggvényt a

$$f_n(x) = \frac{1}{N}\sum_{i=1}^{N} I(v_i = x)$$

képlettel adhatjuk meg. A gyakorlatban sok esetben a mintasornak annyi különböző értékű eleme van, hogy a tapasztalati tömegfüggvény helyett célszerűbb vagy a tapasztalati eloszlásfüggvényt, vagy hisztogramot használni, amit a tömegfüggvény „kisebb felbontású" változatának is tekinthetünk.

Wireshark gyorstalpaló

A laborgyakorlat során elsődlegesen használt eszköz a Wireshark nevű csomaganalizátor, mely egyike a területen használt legnépszerűbb célprogramoknak. Segítségével megfigyelhetők, rögzíthetők és részletesen elemezhetők a hálózaton áthaladó csomagok. Rengeteg protokollt képes elemezni, ezekhez széleskörű szűrési és egyéb kényelmi funkciókat is biztosít, valamint megtalálható benne egy statisztikai elemző modul, mellyel egyszerűen megvizsgálható a forgalom néhány alapvető jellemzője.

A wireshark.org honlapon megtalálható a program részletes felhasználói útmutatója, ezenkívül az Interneten számtalan segédanyag fellelhető. Jelen fejezet csupán a labor során használt néhány főbb funkció bemutatására szolgál.

A felső menürsorból érhető el a funkciók többsége. A File menün belül található a rögzített csomagok mentésére szolgáló Save opció, mellyel különböző formátumokba menthetünk. A labor során a Save menüben mindig a .pcap vagy .pcapng kiterjesztést használjuk. Szükség lehet .csv formátumú fájlok előállítására is, ehhez a File menü Export Packet Dissections alpontját használjuk.

Egy másik, a labormérés során lényeges menü a Statistics. Itt tudjuk megtekinteni a Wireshark által feloldott címeket a Resolved Addresses menüpont alatt. A Protocol Hierarchy menüpontban megvizsgálhatjuk az elkapott csomagok protokollok szerinti lebontású statisztikáját. A Conversations menüpontban ugyanezt a végpontok közti párbeszédek szintjén láthatjuk, a különböző rétegek szerint csoportosítva. (Például az Ethernet fül alatt forrás és cél MAC cím szerint, míg az IP fül alatt forrás és cél IP cím szerint.) Az I/O Graph menüpont alatt megtekinthetjük a csomagforgalom időbeli változását. A menü többi pontja alatt főként a különböző protokollok szerinti részletesebb statisztikák érhetők el.

A menüsor alatti ikonsor a menüsor néhány központi parancsát tartalmazza, melyek közül mi csak a két balszélsőt fogjuk használni, melyekkel a csomagok elkapását indítjuk és leállítjuk.

Az ikonsor alatt található a display filter, mely segítségével megadhatjuk, hogy a Wireshark mely csomagokat jelenítse meg. Alapértelmezésben az Export Packet Dissections funkció a display által

szűrt csomagokat exportálja csak. (Hasonlóképp beállítható filter az elkapott csomagokra is, azonban ezt nem fogjuk használni.)

A felület többi része három ablakra osztható. A felső ablakban (Packet List ablak) láthatjuk a display filter által kiszűrt csomagok listáját azok főbb információival (csomag sorszáma, forrás és cél IP cím, protokoll, csomaghossz, további információ). Középen (Packet Details ablak) találhatók a kiválasztott a csomag különböző protokoll szintű információi. Az alsó ablak a kiválasztott csomag tartalmát mutatja hexadecimális és ASCII kódokban. (Utóbbiban a „.” karakter a nem-nyomtatható kódokat jelenti.)

A labor során megfelelő szűrőkkel állítjuk elő a számunkra érdekes csomagok listáját. A Wireshark egyik kényelmi funkciója, hogy a két felső ablakban bármelyik adatra jobb klikkelve automatikusan hozzáadhatjuk a megfelelő paraméter szerinti szűrést az Apply as Filter menüpont segítségével.

Néhány egyszerűbb szűrő:

ip.src == <ip addr>	szűrés az <ip addr> forrás IP című csomagokra
ip.dst == <ip addr>	szűrés az <ip addr> cél IP című csomagokra
ipv6.src == <ipv6 addr>, ipv6.dst == <ipv6 addr>	szűrés az <ipv6 addr> cél/forrás című IPv6 csomagokra
tcp.port == <port>	szűrés a <port> port számot használó tcp csomagokra
<protocol>	szűrés a <protocol> protokollt használó csomagokra (pl. tcp, udp, ip, stb)
!<cond 1>	szűrés azokra a csomagokra amikre <cond 1> nem igaz (pl. !tcp)
<cond 1> || <cond 2>	szűrés azokra a csomagokra amikre <cond 1> vagy <cond 2> igaz
<cond 1> && <cond 2>	szűrés azokra a csomagokra amikre <cond 1> és <cond 2> is igaz

A Wiresharkhoz tartozik több parancssoros alkalmazás is, melyek olyan funkciókat valósítanak meg, amiket a Wireshark grafikus felületén keresztül is elérhetünk. Ezek akkor hasznosak, ha sok és/vagy nagy capture fájlokkal dolgozunk, mivel segítségükkel könnyen tudunk szkripteket írni, és az erőforrás igényük is alacsonyabb. A labor során a tshark protokoll analizátort fogjuk használni, hogy a .pcap fájlokból a releváns információkat szöveges fájlokba exportáljuk. A tshark opcióit a `tshark -h` parancs segítségével tudjuk lekérni. Rengeteg opciót be lehet állítani, a labor során hasznos opciók:

-r <fájl>	bemeneti fájl megadása
-T fields -e <field 1> [-e <field 2>...]	a kimenetben lévő oszlopok megadása

A capture fájlok szétdarabolására jól használható eszköz a SplitCap nevű program (letölthető a https://www.netresec.com/?page=SplitCap oldalról). A SplitCap segítségével a capture fájl felbontható idő, csomagszám, host, flow és session alapján is.