Detekcija i izolacija problema u 4G mreži primjenom programske podrške WireShark

Kardum, Josipa

SVEUČILIŠTE U DUBROVNIKU
ODJEL ZA ELEKTROTEHNIKU I RAČUNARSTVO

Josipa Kardum

DETEKCIJA I IZOLACIJA PROBLEMA U 4G MREŽI PRIMJENOM PROGRAMSKE PODRŠKE WIRESHARK

ZAVRŠNI RAD

Dubrovnik, rujan 2020.

SVEUČILIŠTE U DUBROVNIKU
ODJEL ZA ELEKTROTEHNIKU I RAČUNARSTVO

DETEKCIJA I IZOLACIJA PROBLEMA U 4G MREŽI PRIMJENOM PROGRAMSKE PODRŠKE WIRESHARK

ZAVRŠNI RAD

Studij: Primijenjeno/poslovno računarstvo

Kolegij: Upravljanje komunikacijskim mrežama

Mentor: prof. dr. sc. Vlatko Lipovac

Student: Josipa Kardum

Dubrovnik, rujan 2020.

Sažetak

U radu su navedeni i opisani mogući problemi u 4G mreži. Cilj je detaljno predočiti sam proces detekcije mrežnih problema i opisati ih putem nekoliko karakterističnih primjera. Za navedene procese koristi se se programska podrška Wireshark.

Također, opisan je povijesni razvoj mobilnih mreža, odnosno kako je s vremenom došlo do pojave 4G mreže. Za obradu i rješavanje opisanog problema potrebno je razumijeti procese upravljanja mrežom, koji su također obuhvaćeni.

Slijedi prikaz razvoja korištenog programskog alata Wireshark, njegova primjena i brojne mogućnosti koje pruža. Opisano je i detektiranje sigurnosnih nepravilnosti i propusta, odnosno kako se Wireshark ponaša u ulozi sigurnosti unutar mreže.

Nakon upoznavanja sa Wiresharkom, prikazani su primjeri detekcije problema koji se mogu pojaviti unutar mreže i opisano analiziranje istih. Za lakše praćenje i razumijevanje problema, postupci su opisani slikama i tekstom, po koracima.

Na samom kraju nalazi se zaključak o obuhvaćenoj problematici koja se proteže kroz cijeli rad, ali i o zapažanjima za korišteni mrežni analizator protokola Wireshark.

Ključne riječi: Wireshark, 4G mreža, mrežni problemi

Summary

The paper lists and describes possible problems in the 4G network. The aim is to present in detail the process of detecting network problems and describe them through several characteristic examples. Wireshark software is used for these processes.

Also, the historical development of mobile networks is described, actually how the 4G network appeared over time. To process and solve the described problem, it is necessary to understand the network management procedure, which is also included.

The following is an overview of the development of the used software tool Wireshark, its application and the numerous possibilities it provides. It also describes the detection of security irregularities and vulnerabilities, that is, how Wireshark behaves in security roles within the network.

After getting acquainted with Wireshark, examples of detecting problems that may occur within the network are presented and their analysis is described. For easier tracking and understanding of the problem, the procedures are described in pictures and text, step by step.

At the very end, there is a conclusion about the covered problems that extend throughout the paper, but also about the observations for the used network protocol analyzer, Wireshark.

Keywords: Wireshark, 4G network, network problems

Sadržaj

1.Uvod

Broj korisnika mobilnih mreža svakim danom je sve veći. Unaprijeđenjem i dugogodišnjim razvojem mobilnih mreža, prijenos podataka i komuniciranje postaje sve jednostavnije i sastavni dio života mnogih ljudi. LTE (engl. *Long Term Evolution*) je 4G mreža koja predstavlja sljedeći korak u tehnologiji pokretne mreže. Svrstava se u inteligentne mreže i pruža velike brzine prijenosa podataka. Također, u današnje vrijeme korisnici se služe aplikacijama koje zahtijevaju sve veće brzine prometa podataka. Osim brzine, također preferiraju kvalitetu, sigurnost i što jeftiniji promet podacima. Najznačajnija inovacija u novoj generaciji mreža, s kojom se želi postići sve ono što tržište zahtijeva, je prelazak na arhitekturu koja je u potpunosti bazirana na protokolu IP (engl. *Internet Protocol*).

Međutim, samim razvijanjem mreža, raste i potreba za primjenjivanjem efektnih testnih alata i metododologija koje se bave greškama i pogoršanim performansama određenih aplikacija [1]. Dostupni su mnogi mrežni analizatori koji omogućuju detekciju mrežnih nepravilnosti i problema, koje ćemo kasnije prikazati i obrazložiti. Primjer mrežnog analizatora, koji se koristi u ovom radu je softverski alat Wireshark. Riječ je o alatu koji hvata podatke koji u paketima putuju mrežom i prikazuje ih na najdetaljniji mogući način.

2. Mobilne mreže

2.1. Povijest mobilnih mreža

2.1.1.Prva generacija sustava mobilnih mreža

Razvojem telekomunikacijske tehnologije početkom sedamdesetih godina dvadesetog stoljeća pojavljuju se prve mobilne mreže, poznate kao sustav mobilne mreže prve generacije (1G). Najpoznatije su NMT (engl. *Nordic Mobile Telephone*), AMPS (engl. *Advanced Mobile Phone System*) i TACS (engl. *Total Access Communication System*), zasnovane na analognom pristupu frekvencijskom podjelom (engl. *Frequency Division Multiple Access* - FDMA) i govornim uslugama.

Puštene su na tržište ranih osamdesetih godina dvadesetog stoljeća. Karakteristika mreža prve generacije, samim time i razlika od svih narednih je signal koji se koristi. Prva generacija koristi analogni signal. Upravo je ta značajka glavni nedostatak 1G mreža, te je iz tog razloga analogni signal zamijenjen digitalnim kod mreža druge generacije (2G). Analogni signal predstavlja manje učinkovito sredstvo za prijenos informacija [2].
Mobilni uređaji su bili veći, teži, s baterijama kraćeg životnog vijeka zbog slabijih tehničkih mogućnosti. U ovom periodu komunikaciju je moguće ostvariti samo glasovnim pozivima, dok se tekstualne poruke nisu mogle slati [3].

2.1.2Druga generacija sustava mobilnih mreža

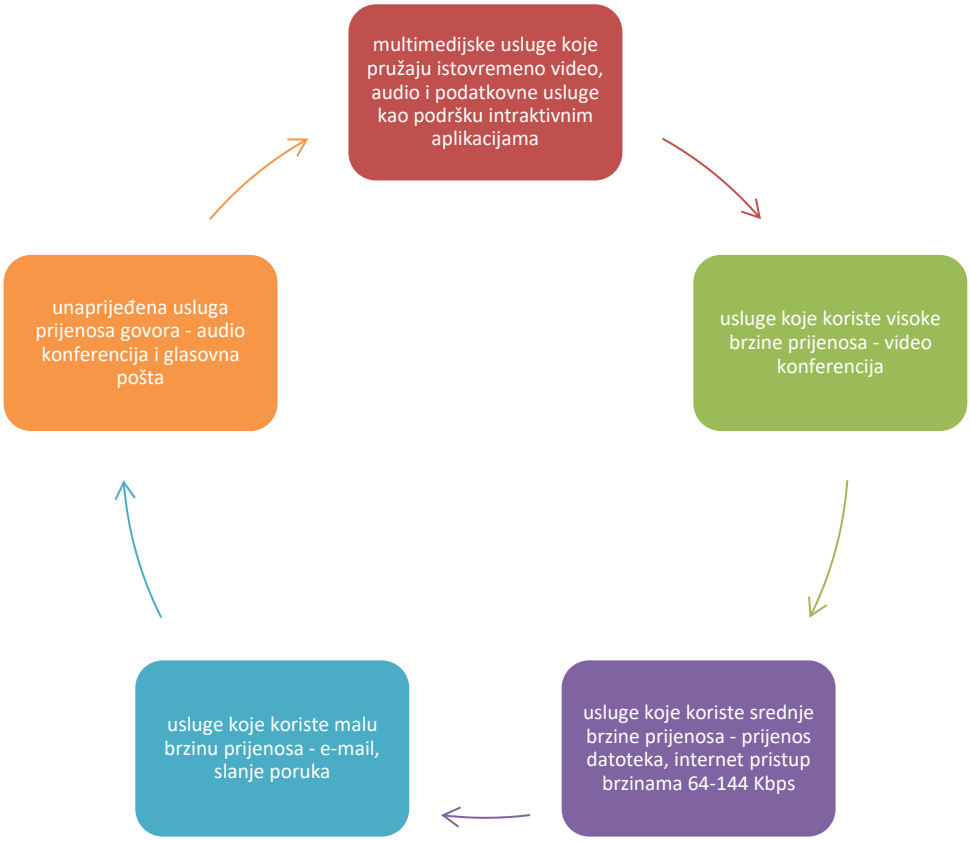
Mobilne mreže druge generacije (2G) kao globalni sustav za mobilnu komunikaciju (engl. *Globar System for Mobile Communication* - GSM), koriste digitalni signal, prijenos govora i podataka uporabom višestrukog pristupa s vremenskom podjelom kanala (engl. *Time Division Mulitple Access* - TDMA) ili višestrukog pristupa s kodnom podjelom kanala (engl. *Code Division Multiple Access* - CDMA). Ciklus razvoja se skraćuje te započinje uvođenje paketskog prijenosa podataka u drugu generaciju mobilnih mreža (isprva prijenos podataka paketskim modom u GSM mreži (engl. *General Packet Radio Services* - GPRS)), kasnije i prijenos podataka u GSM mreži većim brzinama (engl. *Enhanced Dana Rates for GSM Evolution* - EDGE) [2][4] .

Uvođenjem 2G sustava mobilnih mreža i unaprijeđenjem tehnologije, težina mobilnih uređaja postaje manja, baterije su kvalitetnije i učinkovitija je elektronika uvođenjem većeg broja ćelija i odašiljača. Inovacija, ujedno i prednosti koje je sa sobom donijela poja 2G sustava mobilnih mreža je slanje teskutalnih SMS-a (engl. *Short Meessage Service*), korištenje multimedijskih sadržaja preko mobilnih uređaja, korištenje preplaćenih mobilnih telefona i nagli porast uporabe mobilnih uređaja [3].

2.1.3. Treća generacija sustava mobilnih mreža

Treća generacija sustava mobilnih mreža proizlazi iz ideje integriranja žičnih i bežičnih sustava zajedno sa satelitskim mrežama u univerzalni multimedijski širokopojasni pokretni sustav. Tako se u Japanu 2001. Godine pokreće prva 3G mobilna mreža, zatim 2 godine kasnije i u Europi. Uspješan razvoj WCDMA (engl. *Wideband Code Division Multiple Access*) sustava omogućuje mreži treće generacije uvođenje brzog paketskog prijenosa podataka (engl. *High Speed Packet Access* - HSPA) kroz kontinuirana unaprijeđenja koja donose nova izdanja 3GPP (engl. *Third-Generation Partnership Project*) specifikacija. 3GPP je skup standardizacijskih organizacija koje zajedeno djeluju i izdaju specifikacije za razvitak novih standarda bežičnih komunikacijskih tehnologija.

Razvoj mobilnih mreža 2G prema 3G karakterizira promjena fokusa sa isključivo glasovnih na multimedijske mobilne usluge. Sustav treće generacije mreža će omogućiti veće brzine prijenosa i na taj način predstavlja temelj mnogo širem spektru usluga kao što su prikazane u dolje prikazanoj blok shemi[2][4].



Slika 1. Karakteristične usluge 3G mreže[4]

Upravo je 3GPP standardizacijsko tijelo odgovorno za razvoj i nastanak dugoročne evolucije – LTE (engl. *Long Term Evolution*) kao nove tehnologije, predstavljene javnosti 2009. godine. U Stockholmu, kao mobilna mreža četvrte (4G), a kasnije i pete (5G) generacije. 3GPP kao skup standardizacijskih organizacija djeluje zajedno i izdaje specifikacije za razvitak novih standarda bežičnih komunikacijskih tehnologija. Svaka specifikacija (engl.*Release X*, gdje X označava godinu) donosi nova poboljšanja u odnosu na prethodnu [2].

2.1.4.Četvrta generacija sustava mobilnih mreža

Četvrta generacija sustava mobilnih mreža (4G) je direktni nasljednik 3G sustava mobilnih mreža i pruža širokopojasni prijenos podataka kao evoluirani paketski sustav (engl. *Evolved Packet System*, skraćeno EPS) koji čine LTE (engl. *Long Term Evolution*) i SAE (engl. *System Architecture Evolution*). Brzine koje se postižu u LTE povećane su u odnosu na prijašnji sustav mobilnih mreža. Poboljšanja je arhitekture da bi se postigle veće brzine, koncept sigurnosti mehanizma bazira se na prethodnoj izvedbi u UMTS mreži.

UMTS (engl. *Universal Mobile Telecommunications System*) koristi širokopojasni višestruki pristup u kodnoj podjeli (WCDMA) u blokovima od 5 MHz što znači da svi korisnici koriste isti komunikacijski kanal, ali je njihova komunikacija kodirana drugim kodom za proširenje spektra koji je različit za svakog korisnika te pomoću njega korisnik iščitava informaciju namijenjenu njemu[4]. Jezgreni dio mreže UMTS-a ostao je baziran na načinu prijenosa komutiranim kanalom (kao u GSM-u) za govorne i video pozive. Pristupni dio mreže UMTS standarda je naslijeđen od GPRS standarda, s manjim promjenama jer je već zadovoljavao brzi prijenos paketa [5] [6].

3GPP pred LTE stavlja ključne ciljeve s aspekta performansi i mogućnosti:

- visoke brzine prijenosa – vršne brzine prijenosa podataka veće od 100 Mbit/s u silaznoj vezi, odnosno 50 Mbit/s u uzlaznoj vezi, te ostvarivost 2 do 3 puta većih brzina na rubu ćelije u odnosu na Release 6,
- smanjenje vremena čekanja – niska latencija (ispod 10 ms) u korisničkoj ravnini i smanjenje kašnjenja povezanog s procedurama u kontrolnoj ravnini (npr. Uspostava sesije, ispod 100 ms),
- visoka spektakularna efikasnost – 2 do 3 puta veća u odnosu na Release 6,
- umjerena potrošnja snage u terminalima,
- fleksibilnost upotrebe različitih frekvencijskih opsega – mogućnost upotrebe raznih frekvencijskih područja, uz široku mogućnost izbora širine pojasa i izbor između FDD ili TDD moda rada
- pojednostavljena arhitektura
- pojednostavljeno održavanje – podrška za samo-organizirajuće mreže,
- Isplativa migracija s trenutačnih mreža – mogućnost ponovnog korištenja dosadašnjih investicija [7].

2.2. Pojava i korištenje 4G WiFi-a

Razvojem 4G tehnologije mobilni podaci postali su važan izvor za internetsku vezu. 4G usmjerivači mogu koristiti mobilne podatke za dijeljenje internetskih veza i pružanje višestrukih pogodnosti. Internetska veza je koristan dio svačijeg svakodnevnog života. Prilično svatko koristi online vezu gdje god se nalazi. Iz tog razloga, WiFi ruteri/usmjerivači postaju sve rasprostranjeniji.

Trenutno je 3G, odnosno 4G usmjerivač najbolji izbor za uporabu. Ali u budućnosti definitivno će 5G zamijeniti 4G i dovesti mrežu na višu razinu.

U usporedbi s usmjerivačem samo za WiFi, koji podržava samo bežične standarde, 4G WiFi usmjerivač podržava mobilnu tehnologiju putem 4G bežičnog modula.

Prednosti korištenja su:

- Jako jednostavan za korištenje - uz integrirani 4G LTE modem i ugrađeni utor za SIM karticu, sve što treba napraviti je umetnuti mikro SIM karticu i uključiti usmjerivač.
- Moćna kompatibilnost - testirani na terenu godinama, 4G usmjerivači široko su kompatibilni s različitim ISP uslugama u više od 100 zemalja, osiguravajući univerzalnu kompatibilnost s 2 napredne antene za isporuku glatke veze.
- Niska cijena - Za razliku od tradicionalnog WiFi usmjerivača, nije potrebno kupiti širokopojasnu uslugu i neki drugi uređaj poput kabela i DSL-a. Također, nije potrebno postavljati kabele, samo kupiti SIM karticu i pretplatiti se na paket mobilnih podataka koji pruža odabrani mobilni operater.
- Više veza - Uz WiFi i LTE antene i Ethernet priključke, 4G usmjerivači mogu istovremeno dijeliti 3G/4G vezu s više bežičnih uređaja, poput telefona, tableta i prijenosnih računala, te pružiti internet za žičane uređaje poput stolnih računala.

3. Upravljanje mrežama

Upravljanje mrežom u raznolikom okruženju obuhvaća razne procese, metode i tehnike dizajnirane za uspostavljanje i održavanje integriteta mreže.

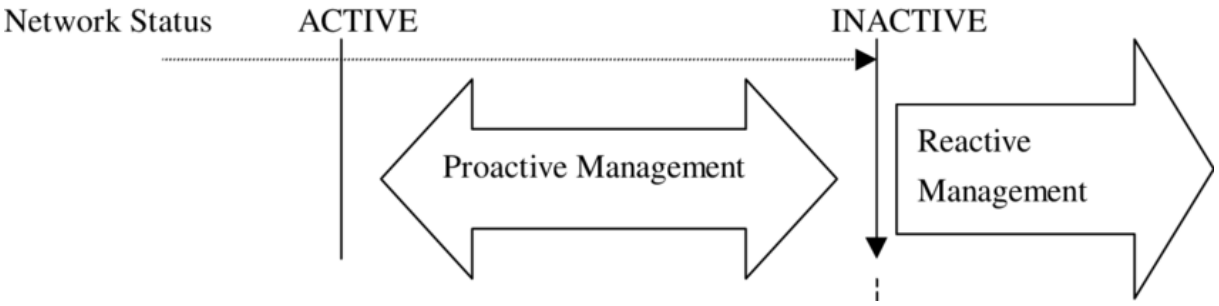
3.1. Upravljanje pogreškama unutar mreže

Najvažniji sastavni dio upravljanja mrežom je upravljanje pogreškama. Među ključnim tehnologijama koje se koriste za razne kritične komunikacijske aplikacije, suočavamo se s brzim rastom zabrinutosti upravitelja mreža. Ponekad je teško održavati mreže zbog rada velike brzine, novih i eskalirajućih problema u stvarnom vremenu, ali i zbog rada u već spomenutom složenom okruženju. Neki od primjera su: netočne konfiguracije uređaja, loše arhitekturirana mreže, neispravni kablovi ili veze, kvarovi hardvera itd. S druge strane, neki problemi ne uzrokuju ozbiljne kvarove, već mogu pogoršati performanse mreže i ostati neotkriveni.

Uz upravljanje pogreškama, upravljanje mrežom uključuje i druge aktivnosti poput: upravljanja konfiguracijom cjelokupnog hardverskog i softverskog dijela sustava, čiji se paramteri mogu redovito konfigurirati. Slijedom toga, integrirano upravljanje mrežom kontinuitet je u kojem je za učinkovit nadzor i kontrolu potrebno više alata i tehnologija.

3.2. Reaktivno i proaktivno upravljanje mrežom

Postoje dva temeljno različita pristupa upravljanju mrežom: raktivni i proaktivni pristup.



Slika 2. Proaktivno i aktivno upravljanje mrežom

Reaktivni pristup većina nas koristi većinu vremena. Jedno od najvažnijih reaktivnih rješenja je dijagnostički sustav. Simptomi se daju kao ulaz u sustav i kao izlaz imamo problem s dijagnozom. Dijagnostički sustavi obično se koriste u području upravljanja kvarovima. Neke je kvarove nemoguće spriječiti zbog djelovanja okoline iznad kabela ili već spoenute loše kvalitete opreme. Radnje rješavanja problema poduzimaju se tek nakon propadanja mreže (Slika 2). To je najveći nedostatak ove vrste rješenja.

U čisto reaktivnom načinu, alat za rješavanje problema jednostavno reagira na svaki problem jer se izvještava nastojeći izolirati kvar i što brže obnoviti uslugu. Uvijek će se naći neki element reaktivnog pristupa u životu svakog mrežnog alata za rješavanje problema. Stoga u reaktivnom upravljanju, IT odjel nastoji povećati dostupnost mreže, gdje se potrebne upravljačke značajke usredotočuju na detekciju, odnosno utvrđivanje mjesta nastanka kvarova i poticanje brzog oporavka.

Ako se akcije poduzmu prije propadanja mreže, radi se o proaktivnom pristupu upravljanja mrežom (Slika 2). Za razliku od reaktivnog upravljanja mrežom, proaktivno upravljanje nastoji poboljšati mrežne performanse. To podrazumijeva sposobnost praćenja uređaja, sustava i mrežnog prometa zbog problema s performansama, te preuzimanja kontrole i odgovarajučeg reagiranja na njih prije nego što utječu na dostupnost mreže. Dakle, glavni cilj proaktivnog upravljanja je otrivanje mogućeg problema u mreži, prije nego što se dogode [1].

4.Wireshark

4.1.Povijest razvoja alata Wireshark

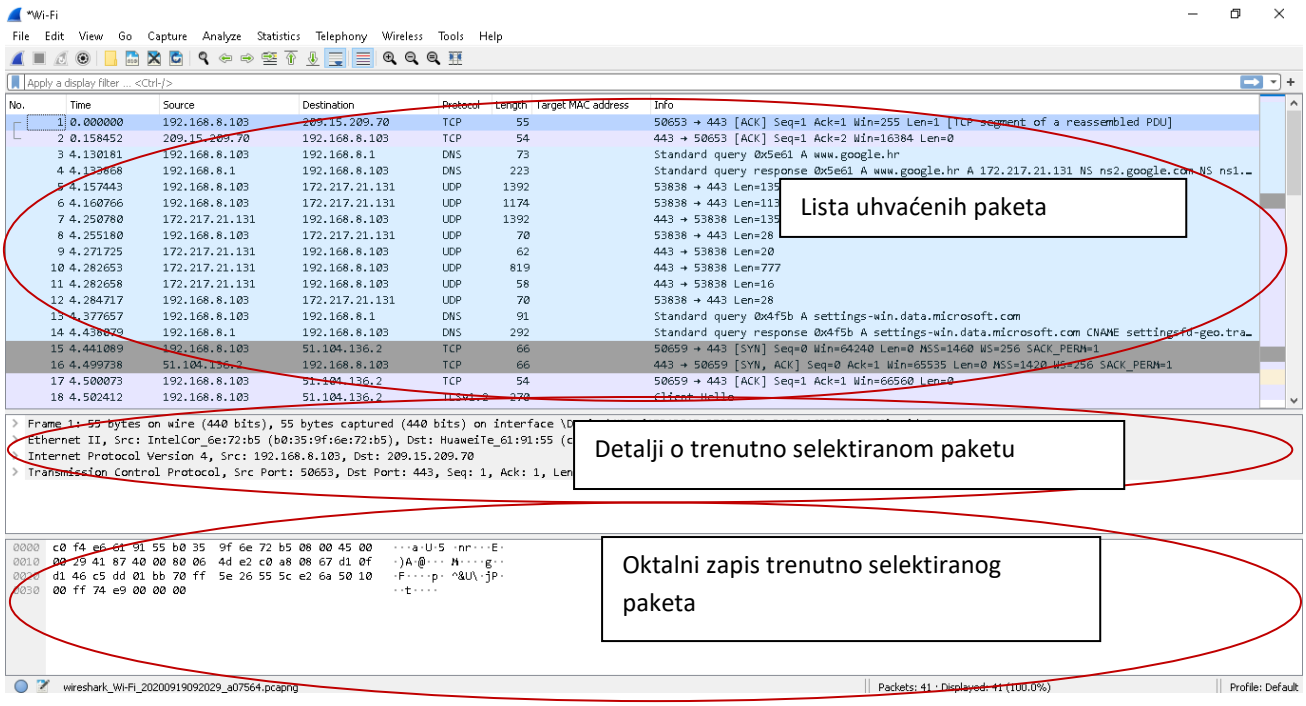
Gerald Combs je 1977. godine počeo pisati program Ethereal zbog potrebe da za alatom kojim bi pratio promet na mreži i time naučio više o upravljanju i administraciji mreže. Ethereal je preteća danas poznatog Wiresharka. Nakon stavljanja na tržište nije bilo daljnjeg razvoja, no u srpnju 1998. godine u inačici 0.2.0. Ethereal se nadogradio. Nedugo nakon toga, sistemski inženjer Gilbert Ramirez je uočio potencijal Ethereala i postao prvi suradnik projekta u kojeg je implementirano nekoliko radnji.

U listopadu 1998. godine, Guy Harris iz tvrtke Network Appliance pokušao je naći bolji alat za administriranje mreže od do tad korištenog alata *tepview*. Paralelno je počeo unaprieđivati Ethereal. Krajem 1998. godine stručnjak za područja TCP/IP, Richard Sharpe, počeo je pisati zakrpe i unaprijeđenja za protokole koji su mu bili potrebni. Lista pojedinaca koji su pridonijeli razvitku alata se znatno povećala. Većina je započela s novim protokolima koji su im bili potrebni, ali ih Ethereal, kasnije Wireshark, nisu još podržavali. To je dovelo do velikog broja protokola koje Wireshark podržava danas.

2006. godine. projekt se restrukturirao i promijenio ime u Wireshark. U proljeće 2008. godine Wireshark izlazi u inačici 1.0. Ta inačica je bila prva potpuna inačica na tržištu, ali je bila inačica s minimalnim značajkama, odnosno osnovna s mogučnošću nadogradnje. Inačica 1.0. izašla je istovremeno s održavanjem prve Wireshark konferencije za programere i korisnike nazvane SharkFest. Magazin eWEEK (engl.*The Enterprise Newsweekly*) tjedni poslovni informatički magazin proglasio je Wireshark *„najutjecajnijom open-source aplikacojm svih vremena “.* Budući da je *open source* alat, relativno je jednostavno implementirati programske dodatke za nove protokole. Koristi se za rješavanje problema s mrežom, analizu, razvoj softvera i komunikacijskih protokola te edukaciju[8].

4.2. Mogućnosti unutar programa Wireshark

Wireshark je programski alat koji praktički „razumije“ strukturu različitih mrežnih protokola. Iz tog razloga sposoban je prikazati podatke iz paketa specifičnih za različite protokole. Podaci se mogu uhvatiti izravno s aktivne mrežne veze ili se mogu učitati iz datoteke u kojoj su pohranjeni već uhvaćeni paketi. Uhvaćeni podaci mogu biti prikazani preko grafičkog korisničkog sučelja ili preko terminala (komandne linije) kod korištenja TSharka - alat naredbenog retka koji se koristiti za hvatanje, prikaz i dobivanje osnovne statistike o prometu uživo ili spremljenim datotekama tragova. Wireshark sadrži i filter za prikaz podataka pomoću kojega se može prikazati i samo dio podataka, ovisno o uvjetu filtriranja.



Slika 3. Sučelje Wireshark programa

Mogućnosti alata su brojne, a najbitnije su:

- Hvatanje podatkovnih paketa s mrežnog sučelja
- Prikazivanje paketa s vrlo detaljnim informacijama o mrežnom protokolu
- Otvaranje i spremanje paketa
- Uvoz i izvoz podataka u druge slične programe
- Pretraga i filtriranje paketa po raznolikim kriterijima
- Kreiranje različitih statistika

Wireshark može očitati podatke s više različitih vrsta mreža. Najpoznatije koje podržava su:

- Ethernet – najučestalija Lan(engl. *Local Area Networking*) tehnologija koja se, s 10 gigabitnom izvedbom, koristi i kao WAN(engl. *Wide Area Networking*) tehnologija. Ethernet šalje pakete od pošiljaoca prema jednom(engl. *Unicast*) ili više (engl. *Multicast/Broadcast*) prijamnika.
- IEE 802.11 – skup standarda za bežičnu računalnu komunikaciju (WLAN, engl. *Wireless Local Area Network*) na frekvencijskim pojasevima od 2.4, 3.6 i 5 GHz. Razvijen je od strane IEEE LAN/MAN Standards Committee(IEEE 802).
- PPP – (engl. *Point-to-Point Protocol*) protokol koji se koristi za izravno povezivanje dvaju čvorova računalne mreže. Omogućuje povezivanje računala serijskim, telefonskim ili optičkim kabelom, pomoću mobilnih telefona te posebno oblikovanom radio ili satelitskom vezom.
- Loop-back – virtualno mrežno sučelje implementirano softverski.

Format datoteke za spremanje paketa koji su uhvaćeni na mreži je standrardni libpcap format podržan od strane mrežnih biblioteka Libpcap i WinPcap. To znači da Wireshark može pročitati i podatke iz aplikacija kao što su tcpdump i CA NetMaster koje također koriste isti format. Osim toga, podatke uhvaćene Wiresharkom može se pročitati i drugim aplikacijama koje koriste Libpcap i W inPcap za čitanje uhvaćenih podataka, Tako Wireshark može čitati i podatke uhvaćene mrežnim analizatorima kao što su Snoop, Network General's Sniffer te Microsoft Network Monitor.

Neki od najrašireniji protokola koi se koriste u komunikacijskim mrežama, a koje Wireshark podržava su:

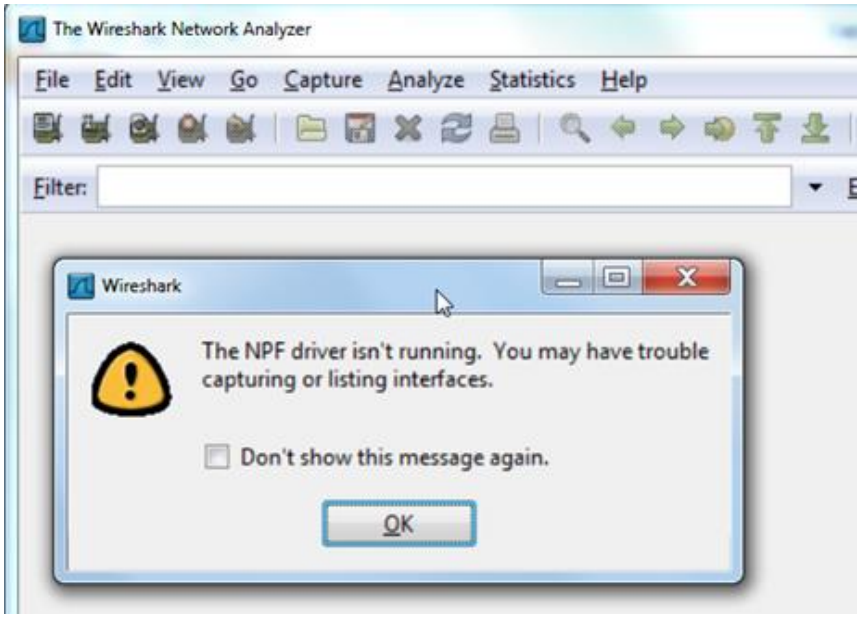
- Internet protokoli – TCP/IP skup protokola koji uključuju ARP, IP, TCP, itd.
- Protokoli mobilne mreže – skup protokola sadržanih u GSM-u(WCDMA, CDMA2000, …)
- VOIP protokoli – skup protokola za prijenos zvuka mrežom (SIP, H323,..)
- WAP protokoli – skup WAP protokola za omogućavanje servisa na bežičnim kominukacijskim mrežama(WTP, WSP,…)[9].

4.3. Wireshark u funkciji sigurnosti

Osim osnovnih funkcionalnosti, Wireshark omogućuje i detektiranje sigurnosnih propusta i nepravilnosti. Sigurnosni propust se očituje nedopuštenim, neovlaštenim, odnosno malicioznim radnjama koje mogu naštetiti mreži ali i njenim korisnicima. Wireshark sprječava sigurnosne propuste na način da analizira moguće probleme i radnje koje mogu stvoriti probleme.

Uočavanje problema na mreži prije nego što ih korisnik mreže osjeti spada u preventivne metode(zadatke) unutar Wiresharka. Na primjer, preventivne metode omogućuju uočavanje gubitka paketa prije nego taj gubitak počne utjecati na mrežnu komunikaciju i na taj način se izbjegava problem prije nego je uopće uočen od strane korisnika.

Što se tiče reaktivnih metoda analiza, Wireshark ih koristi nakon što su greške u radu mreže uočene. Na primjer, ako postoji problem s nekim poslužiteljem, program će problem prijaviti tek nakon što pokuša uhvatiti pakete s mreže. Općenito, u Wiresharku su više zastupljene reaktivne analize, što zapravo nije dobro jer kao što je već spomenuto, reaktivne analize uočavaju problem prije nego sam program može utjecati na mrežu.



Slika 4. Primjer reaktivnog zadatka u Wiresharku

Neke analize koje korisnicima Wiresharka mogu poslužiti u funkciji sigurnosti ali i uočavanja mogućih problema:

- Prepoznavanje najčešćih problema na mreži(spora veza, nemogućnost prepoznanja korisnika,..)
- Prepoznavanje da dolazi do kašnjenja između korisničkog naloga za rad s mrežnim paketima i samog procesa rada s paketima
- Prepoznavanje krivo konfiguriranih korisnika(npr. duplicirana IP adresa)
- Definiranje mreže ili korisnika koji usporavaju promet na mreži
- Uočavanje neuobičajenih protokola
- Identificiranje asinkronog prijenosa na mreži
- Identificiranje neuobičajenog pregleda prometa na mreži
- Brzo identificiranje HTTP (engl. *HyperText Transfer Protocol*) grešaka koje indiciraju probleme korisnicima i poslužitelju
- Brzo identificiranje VoIP(engl. *Voice over Internet Protocol*) grešaka koje indiciraju probleme korisniku ili poslužitelju te globalne pogreške
- Identificiranje aplikacija koje ne šifriraju podatke koji se prenose
- Identificiranje prosječnog i neprihvatljivog vremena odziva mrežnih servisa(SRT, engl. *Service Response Time*)

Mreže jako variraju u prometu. Broj i vrsta analitičkih zadataka koji se mogu izvršiti na nekoj mreži ovisi o svojstvima prometa na mreži, tj. o vrsti prometa koji mreža može podržati[10].

5. Primjeri detektiranja i izoliranja mrežnih problema u Wiresharku

5.1. Problemi u WLAN prometu (4G usmjerivač)

Da bismo uspješno pronašli probleme s WLAN prometom, ključno je pravilno bilježiti promet. Drugim riječima, potrebno je uhvatiti 802.11 okvire za upravljanje, kontrolu i podatke, zaglavlje 802.11 i primijeniti pseudo zaglavlje - zaglavlje Radiotap ili zaglavlje PPI (po paketu).

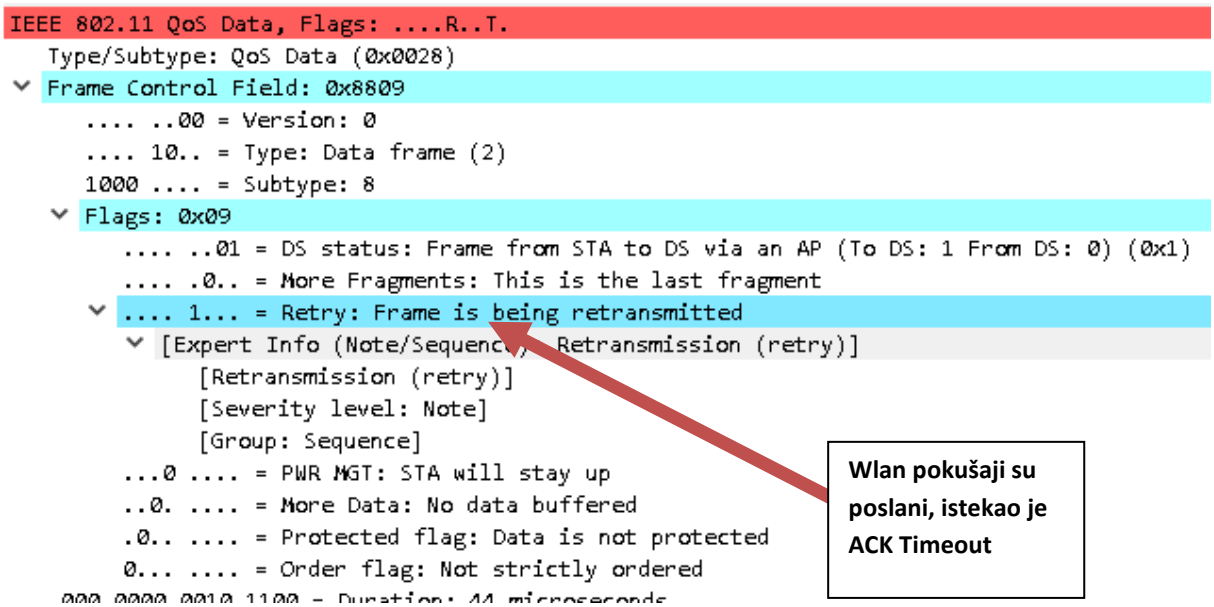
Okviri za upravljanje i kontrolu neophodni su za prepoznavanje problema s pridruživanjem i autentifikacijom WLAN-a. Okviri podataka pružaju nam stvarne brzine protoka na WLAN-u.

Zaglavlja Radiotap i PPI sadrže metapodatke o primljenom okviru. Ovi metapodaci uključuju snagu i frekvenciju signala u trenutku primanja. Niska jačina signala može biti znak slabog odašiljanja ili predaleka pošiljatelja. Vrijednost frekvencije govori nam na kojem je kanalu paket stigao.

5.1.1. Snimanje zaglavlja 802.11

U početku se može činiti vrlo jednostavnim zadatkom, ali ukoliko za hvatanje koristimo svoj izvorni WLAN adapter, taj adapter uglavnom skine zaglavlje 802.11. Wireshark će umjesto njega prikazati Ethernet zaglavlje.

Zaglavlje 802.11 sadrži postavku „*Retry bit“* (*wlan.fc.retry*) koja pokazuje je li paket 802.11 ponovni pokušaj(engl. *retry*). Ovo predstavlja ponovni prijenos MAC sloja. Na primjer, lokalni uređaj 802.11 šalje podatkovni paket pristupnoj točki. Ako se 802.11 ACK ne vrati unutar vremenskog ograničenja ACK, podatkovni će se paket ponovno poslati s bitom *Retry* postavljenim na 1(Slika 5).



Slika 5. ACK vremensko ograničenje

ACK vremenska ograničenja se mogu pojaviti zbog preslabog signala ACK-a ili su smetnje(sudari) oštetile ACK pakete.

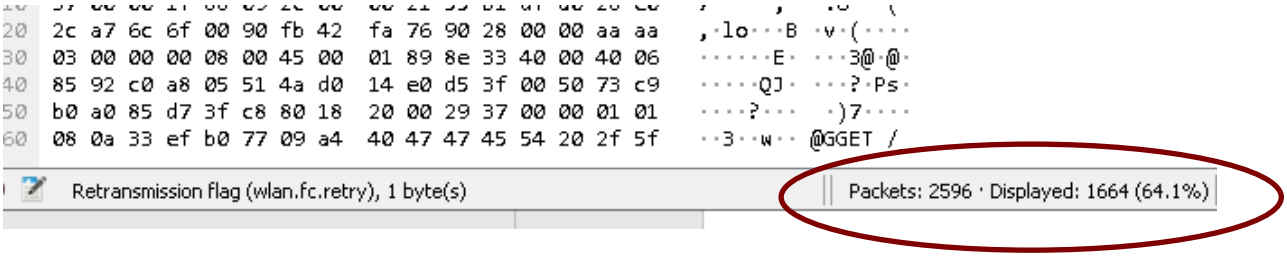
5.1.2. Filtriranje WLAN Pokušaja(engl. *Retries*) i ispitivanje snage signala

Korak 1: Za početak otvaramo odgovarajuću snimljenu .pcapng datoteku u kojoj je zabilježen promet. Zaglavlja Radiotap i 802.11 su vidljiva.

Korak 2: Desnom tipkom miša kliknemo na redak*: „IEEE 802.11 QoS Data, Flags: .... R..T“*, koji se nalazi u paketu 1, pa zatim odaberemo opciju: Proširi podstabla.

Korak 3: Bit za ponovni pokušaj nalazi se u odjeljku: Zastave (engl.*Flags*) u području Kontrole okvira(engl. *Frame Control area*).

Desnom tipkom miša zatim odaberemo polje: *„Retry bit“* i odaberemo opciju *„Apply as Filter“* , zatim na*: „ Selected“*. Možemo uočiti da je Wireshark stvorio i primjenio filtar prikaza za: *„wlan.fc.retry == 1“*.



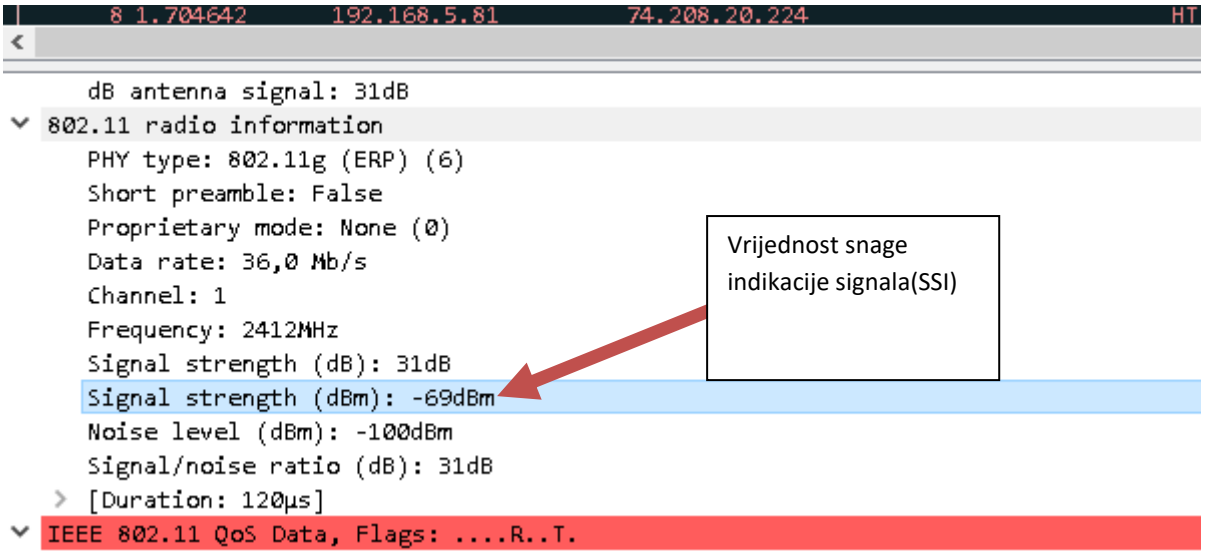
Slika 6. Prikaz broja i postotka paketa

Vidljivo je da u ovoj datoteci praćenja, 1.664 paketa (64,1% prometa) predstavljaju MAC slojevi ponovnog slanja(Slika 6.). Vrijednost vremenskog ograničenja ACK istekla je kod pošiljatelja, pa je potrebno ponovno poslati pakete.

Korak 4: Primjećujemo također da su paketi 8, 9 i 10 GET zahtjevi za istu datoteku, sor.css. Wireshark ih je označio kao TCP Retransmisije i *„Retry bit"* je postavljen u svakom paketu.

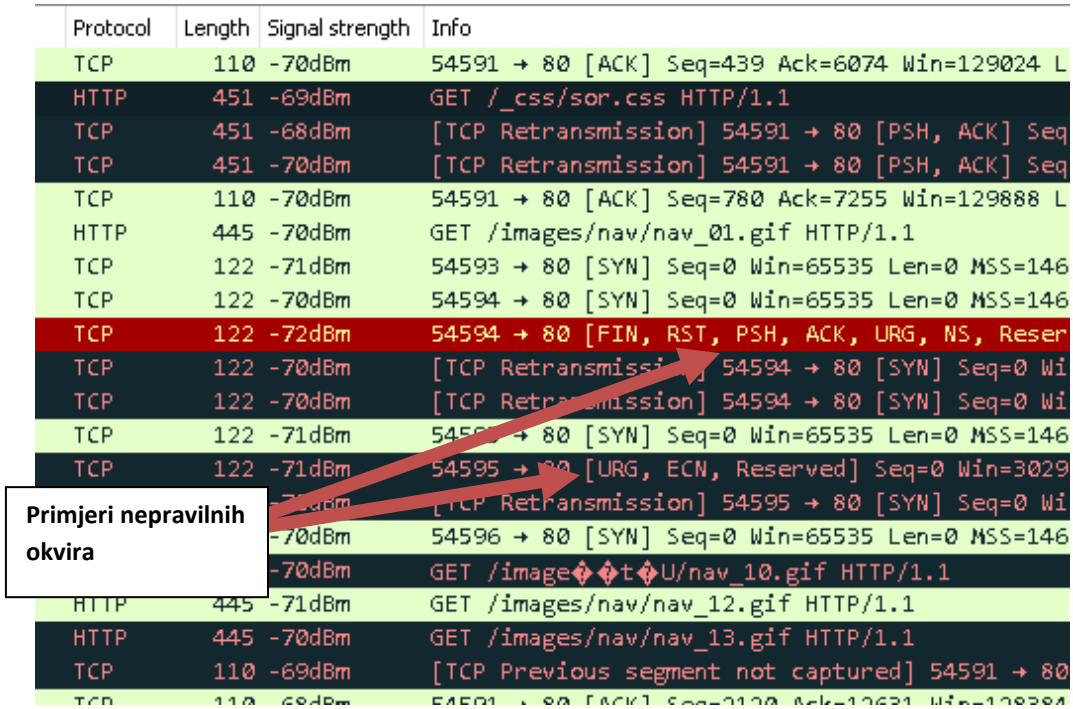
Sljedeće što trebamo napraviti je ispitati vrijednost SSI (engl.*Signal Strength Indication*), tj. snagu indikacije signala (dBm) u tim paketima. Te se informacije šalju iz upravljačkog programa za WLAN adapter. Opće pravilo vrijedi da je: što je jači SSI signal (dBm),to je bliži nuli. Na primjer, -20 dBm je jači signal od -70 dBm.

Desnom tipkom miša odaberemo liniju *„Radiotap Header"* u paketu 8 i odaberemo opciju: Proširi podstabla(engl. *Expand Subtrees*). Zatim desnom tipkom miša kliknemo na liniju: SSI Signal (dBm) i odaberemo: Primijeni kao stupac(engl. *Apply as Column*).



Slika 7. Vrijednost SSI(dBm)

Također je važno potražiti neispravne okvire(engl. *malformed frames*). Nepravilno oblikovani okviri pojavljuju se u području: Pogreške stručnih informacija(engl. *Expert Infos Errors*) i mogu biti pokazatelji pogreške disektora Wireshark-a, slabog signala ili sudara/kolizije.



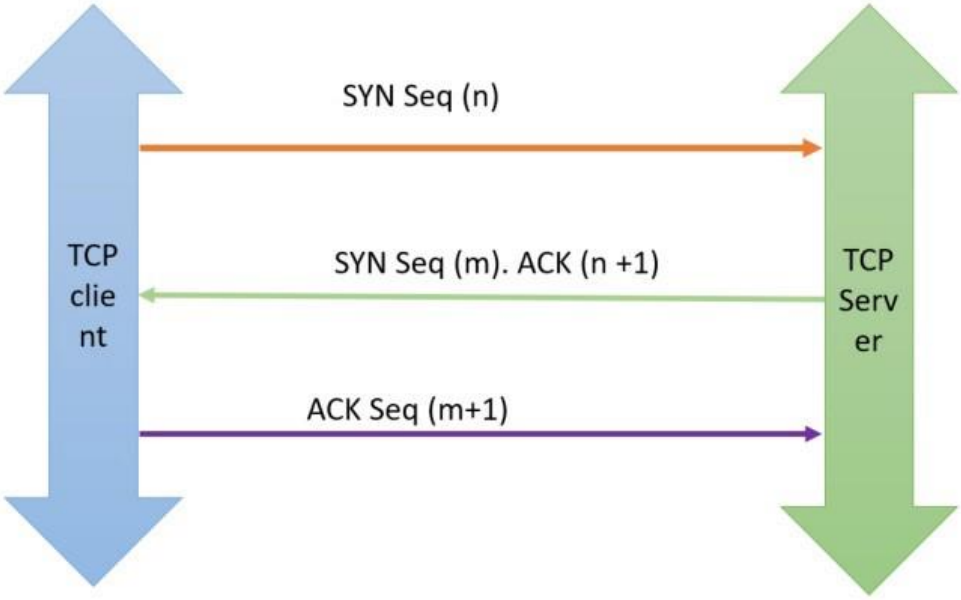
Slika 8. Nepravilno oblikovani okviri

Ova datoteka praćenja prikazuje klasični WLAN problem gubitka paketa. Na mjestu hvatanja vidimo da su neki od klijentovih paketa oštećeni, a mnogi od njih su retransmisije tj. ponovni prijenosi(engl.retransmissions).

Ako bismo snimali blizu pristupne točke, približili bismo se klijentu da vidimo je li udaljenost problem ili je problem ako se pojavila korupcija. Pazili bismo na mjesto na kojem se korupcija(engl.courruption) ne pojavljuje i gdje je jačina signala primjerena.

5.2. Nema odgovora na zahtjev za TCP vezu

Naime, poznato je da TCP koristi trostruko rukovanje (engl. *Three-way handshake*) tj. dvije strane se dogovaraju o uspostavi veze izmjenom tri segmenta sa upravljačkim porukama (Slika 9).



Slika 9. TCP trostruko rukovanje

Postoji nekoliko razloga zbog kojih poslužitelj neće odgovoriti. Moguće je da SYN paket nije stigao na poslužitelj. Razlozi za to mogu biti: izgubljen je SYN paket, vatrozid je duž staze ispustio SYN paket, ili je *host-based* vatrozid na poslužitelju blokirao pristup priključku(engl. *port*).

Odgovor (SYN/ACK) možda neće stići klijentu. Postoji mogućnost da je SYN / ACK paket izgubljen na putu ili je vatrozid na putu blokirao SYN / ACK kako bi spriječio završetak rukovanja(engl. *handshake*).

Ako se snima blizu klijenta, a SYN / ACK nisu vidljivi, trebali bi obaviti snimanje blizu poslužitelja, kako bi utvrdili je li SYN / ACK stvarno poslan. Ako je SYN / ACK poslan, sada možemo zaključiti da je uređaj za povezivanje duž puta odbacio paket. Nastavljamo približavati točku hvatanja klijentu sve dok ne ugledamo točku na kojoj se ispuštaju SYN / ACK.

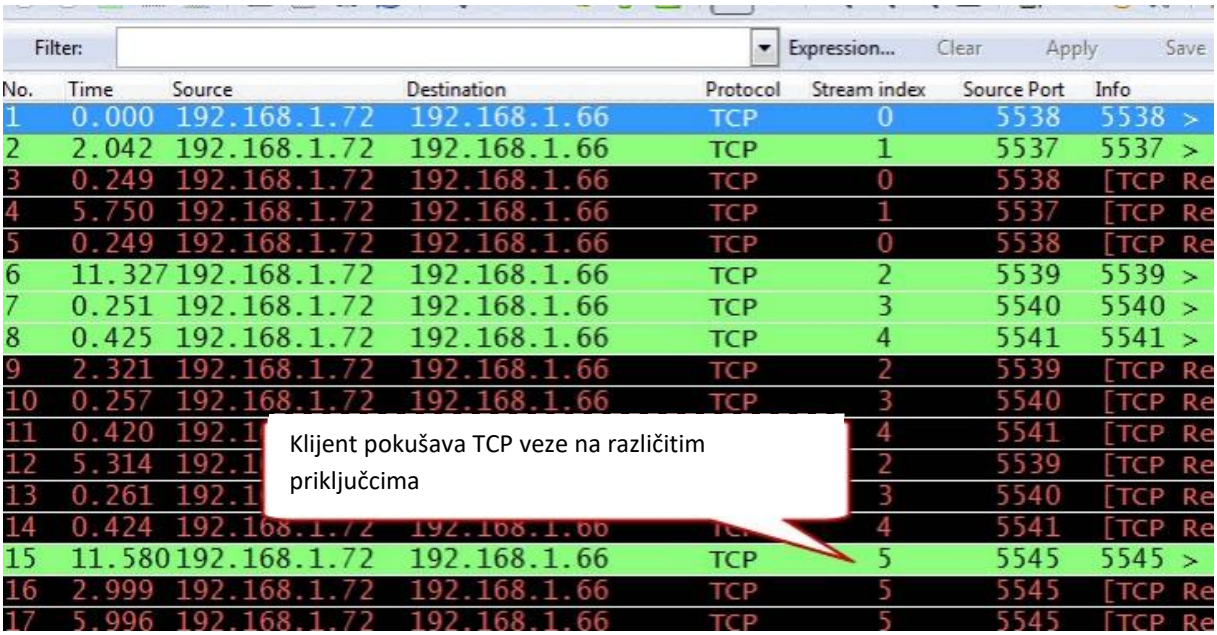
Korak 1: Otvoramo odgovarajuću .pcapng datoteku.

Korak 2: Pomičemo se kroz ovu datoteku praćenja. Ova datoteka praćenja sadrži samo SYN pakete od 192.168.1.72 do 192.168.1.66. Dakle, nijedan od SYN paketa nije primio SYN / ACK odgovore.

Proširujemo TCP zaglavlje u paketu 1. Desnom tipkom miša kliknemo na redak: *„Stream index: 0“* i odaberemo opciju: *„Apply as Column“*. Wireshark svakom jedinstvenom pokušaju povezivanja dodjeljuje zasebni TCP tok zasnovan na izvornoj/odredišnoj adresi i brojevima izvornog/odredišnog porta. Šest je zasebnih veza koje klijent pokušava uspostaviti u datoteci praćenja (engl. *TCP Stream Index 0 - TCP Stream Index 5*).

Korak 3: Desnom tipkom miša odaberemo polje: *„TCP Source Port“* u bilo kojem paketu i zatim na: *„Apply as Column“*.

Sada možemo jasnije vidjeti da je klijent postavio brojne priključke za ove veze. Međutim, klijentski priključci(engl. *ports*) nisu susjedni(Slika 10). Razlog bi mogao biti zato što klijent uspostavlja druge veze s drugim uređajima i ti paketi nisu uhvaćeni u ovoj datoteci praćenja.



Slika 10.TCP veze na različitim priključcima

Korak 4: Neki od ovih SYN paketa odgovaraju HTTP pravilu bojanja, dok se drugi podudaraju s pravilom „*Bad TCP bojanja“*, jer su SYN paketi retransmisije(engl. *retansmissions*).

Wireshark prati svaki pokušaj povezivanja i može automatski odrediti koji su SYN paketi retransmisije (engl. *retransmissions*). Proces TCP *backoff* može se vidjeti ako stupac: Vrijeme postavimo na: Sekunde od prethodnog prikazanog paketa. Desnom tipkom miša odaberemo naslov stupca: Izvornog priključka (engl.*Source Port*) i odaberemo opciju: Sakrij stupac. U slučaju da kasnije želimo ponovo pregledati ovaj stupac, samo desnom tipkom miša kliknemo na bilo koji naslov stupca, pa odaberemo: Prikazani stupci. Zatim, kliknemo na stupac s popisa.

Nakon uspješnog TCP rukovanja i dalje je moguće suočavanje s odgovorima poslužitelja.

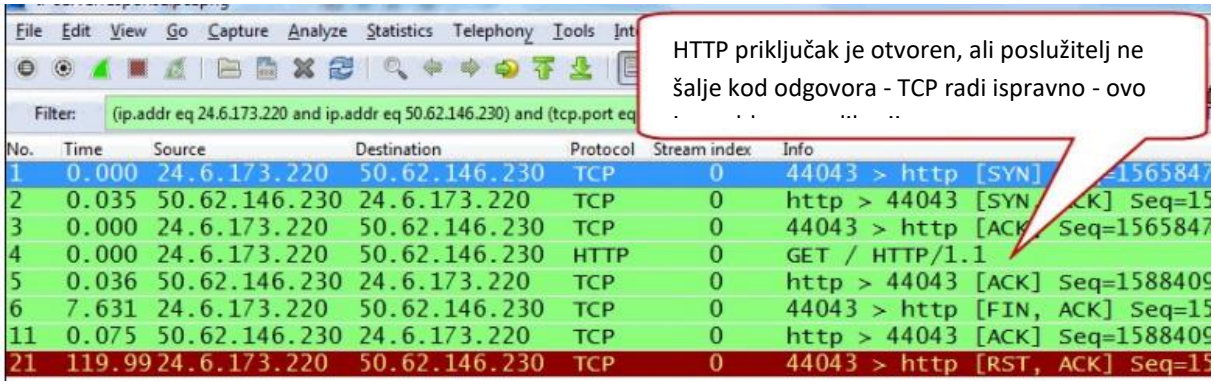
5.3. Nema odgovora na zahtjev za uslugom

U ovom primjeru će se izdvojiti i prikazati jedan razgovor za analizu prometa na poslužitelju, koji pri tom ne odgovara na zahtjeve za uslugom.

Korak 1: Za početak otvaramo odgovarajuću .pcapng datoteku.

Korak 2: Pomičemo se kroz ovu datoteku praćenja da bismo se upoznali s obrascem prometa. Stupac: Indeks toka može nam pomoći razlikovati zasebne veze između 24.6.173.220 i 50.62.146.230.

Izdvojimo samo jedan od razgovora metodom desnog klika. Desnom tipkom miša odaberemo Paket 1 u oknu: Popis paketa i zatim odaberemo Filtar razgovora, pa TCP(Slika 11).



Slika 11. Poslužitelj ne odgovara na zahtjev

Analiza ovog razgovora:

1. U paketima 1-3 vidljivo je kako se TCP rukovanje(engl. *handshaking*) uspješno dovršilo.
2. U paketu 4, klijent traži "/" (zadana datoteka iz korijenskog direktorija web mjesta).
3. Paket 5 je potvrda od poslužitelja. Ovaj paket sadrži broj potvrde 288, što znači da je poslužitelj primio svaki sekvencijski broj do 287, a sljedeći očekuje sekvencijski broj 288. Iz čega zaključujemo da je poslužitelj primio zahtjev.
4. Umjesto vraćanja tražene zadane stranice ili možda preusmjeravanja, poslužitelj se utišava.
5. TCP ne preusmjerava GET zahtjev jer je klijent dobio ACK za taj zahtjev.
6. Pretpostavlja se da klijentov preglednik istječe i šalje FIN / ACK nakon gotovo 8 sekundi. Klijent završava sa slanjem podataka poslužitelju i započinje implicirani prekid veze. Klijent je trenutno u stanju FIN-WAIT-1.
7. Poslužitelj šalje ACK. Klijent je sada u stanju FIN-WAIT-2. Očekivali bismo da će poslužitelj poslati FIN kako bi počeo zatvarati svoju stranu veze, ali to ne čini.
8. Klijent čeka gotovo 120 sekundi prije nego što potpuno odustane od veze slanjem RST / ACK.

Svaka od veza prolazi kroz isti obrazac. Ovo nije samo privremeni „kvar“ u mrežnoj komunikaciji ili jednokratni problem sa uslugom koja se izvodi na poslužitelju. Čini se da TCP pravilno funkcionira u ovoj datoteci praćenja.

5.4. Otkrivanje niske propusnosti zbog malih veličina paketa

Prijenos datoteka pomoću malih veličina paketa zahtjeva predugo trajanje izvršavanja samog procesa. Male veličine paketa može uzrokovati aplikacija koja namjerno želi prenijeti manje količine podataka. Male veličine paketa također mogu biti pokazatelj niskih postavki maksimalne veličine segmenta (MSS – engl. *Maximum Segment Size*).

Nizak MSS može biti posljedica pogrešne konfiguracije na klijentu ili čak dodatne funkcije (kao što je učitan VLAN upravljački program).

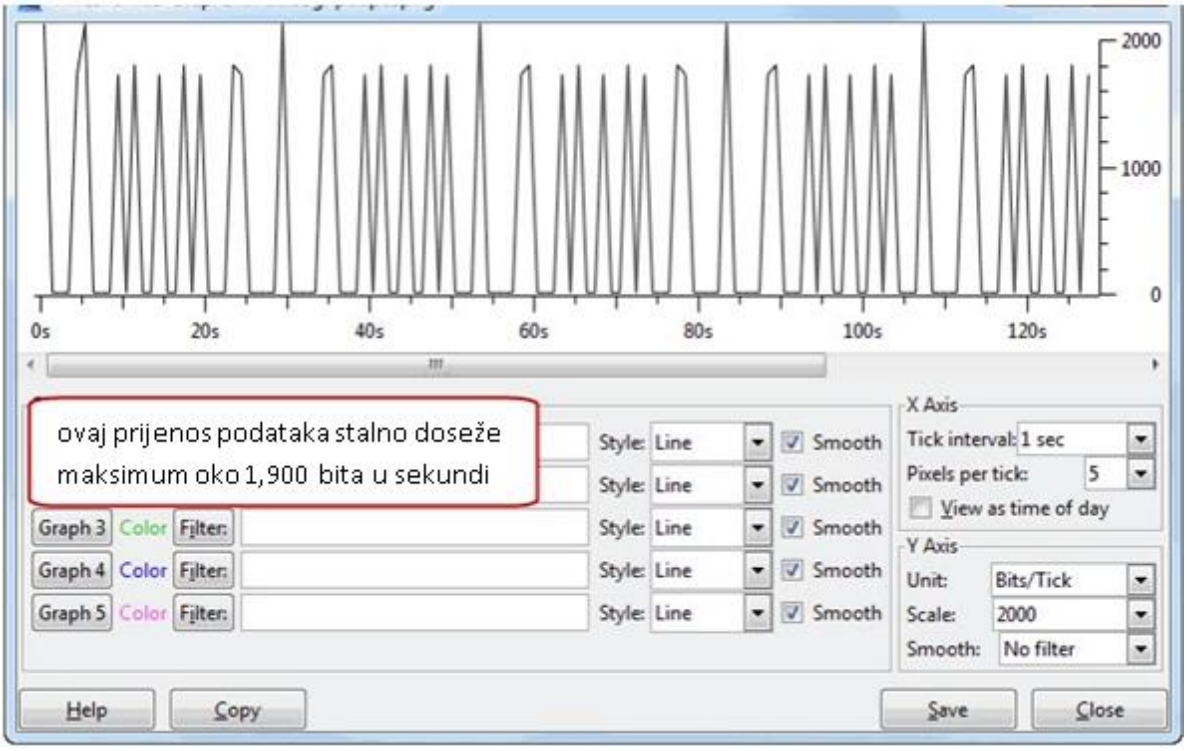
5.4.1.Grafikon niske propusnosti zbog paketa malih veličina

Korak 1: Za početak otvaramo datoteku praćenja .pcapng, koja se sastoji od HTTPS veze između *hostova*. Budući da nemamo ključ za dešifrirati promet, možemo analizirati samo do točke TCP sloja. Pomičemo se kroz datoteku praćenja s ciljem da vidimo vrijednost stupca: Dužina(engl. *Length*).

Također, u ovoj datoteci praćenja postoji puno malih podatkovnih paketa. Prvo isključimo niske MSS(engl. *Maximum Segment Size*) postavke kao mogući uzrok malih veličina paketa.

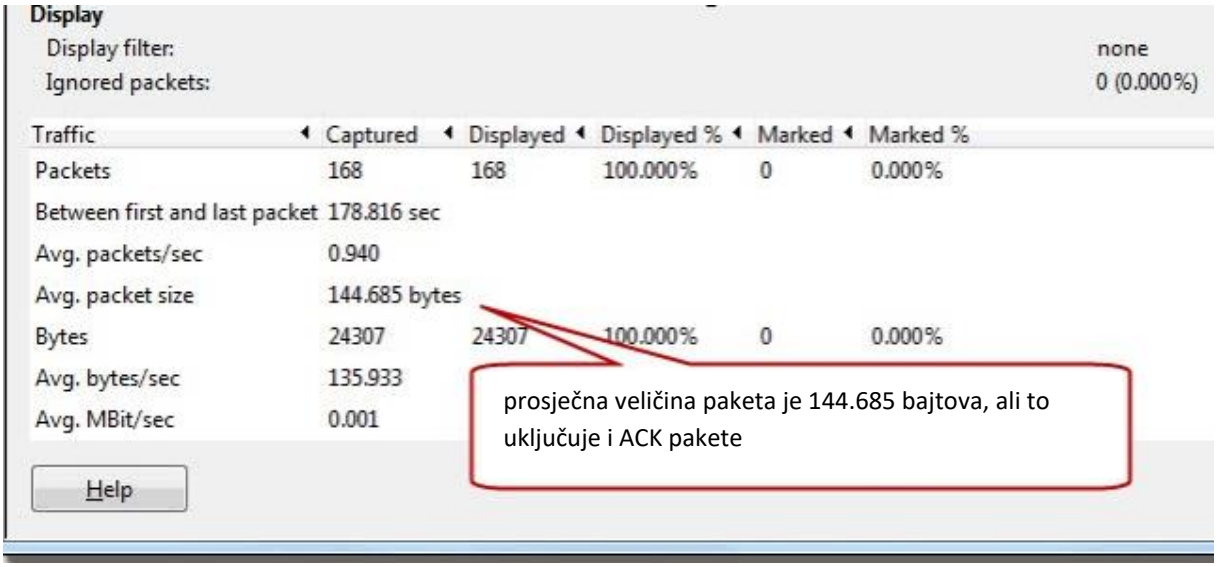
Korak 2: Zatim ispitujemo odjeljak TCP opcija u paketu 1 i paketu 2. Primjećujemo da MSS vrijednosti oglašava svaki *host* - paket 1 i paket 2 oglašavaju MSS od 1.460 bajtova. Znamo da MSS konfiguracija nije razlog za male veličine paketa.

Korak 3: Odaberemo opciju Statistika, pa IO Grafikon. Postavljamo vrijednost jedinice osi Y na „*Bits/Tick“*. Zatim, mijenjamo ljestvicu osi Y na 2000. Uočavamo da se radi o maloj propusnosti(Slika 12).



Slika 12. Prikaz vrijednosti maksimuma

Korak 4: Sada kliknemo na: Zatvori. Zatim odaberemo opciju: Statistika, pa: Sažetak. To će nam dati prosječnu veličinu paketa u datoteci praćenja(Slika 13).

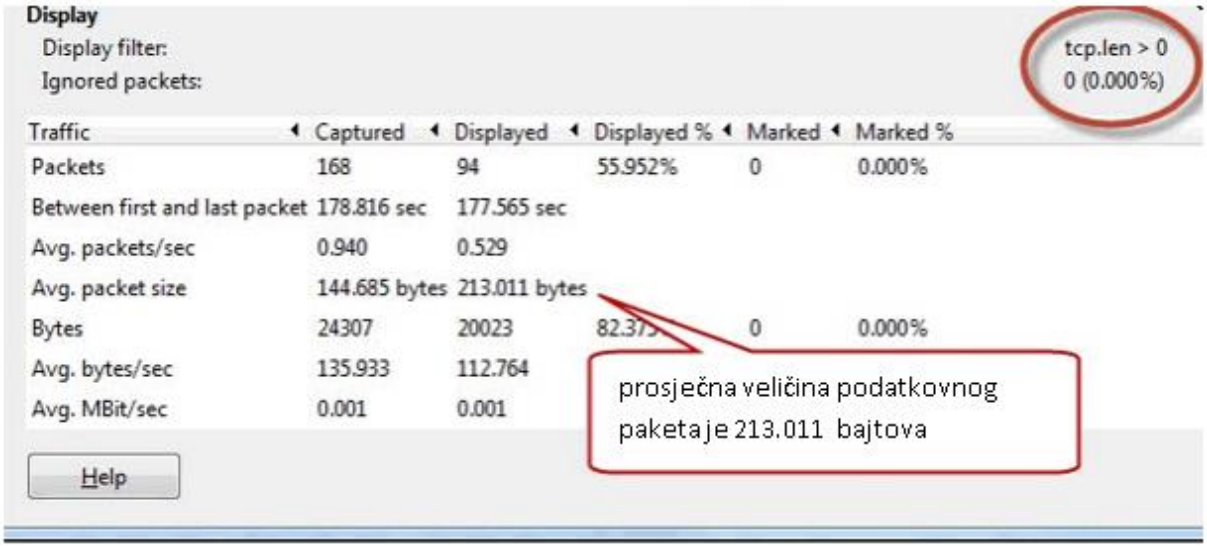


Slika 13. Prikaz prosječne veličine paketa

Ova prosječna veličina paketa uključuje ACK pakete. Primjenjujemo filtar na promet kako bismo odredili prosječnu veličinu podatkovnog paketa.

Korak 5: Stisnemo na gumb: U redu da bismo zatvorili prozor: Sažetak. Zatim, unosimo: „tcp.len> 0“ u područje filtra zaslona i kliknemo na: Primijeni. Sada vidimo samo pakete koji sadrže podatke.

Korak 6: Zatim odaberemo opciju: Statistika, pa: Sažetak. Sada nam se prikazuje stupac. Ovaj stupac označava prosječnu veličinu podatkovnog paketa od 213,011 bajta(Slika 14).



Slika 14. Prikaz prosječne veličine podatkovnog paketa

Utvrdili smo da mali paketi nisu ograničenje koje je definirano TCP vezom. Već se najvjerojatnije radi o samim postavkama aplikacije. Moramo pogledati aplikaciju kako bismo utvrdili je li to namjerno tako postavljeno ili je problem u konfiguraciji.

6. Zaključak

4G mreža s vremenom je postala jako popularna. Telekomunikacijski operateri svakodnevno diljem svijeta ulažu u nadogradnju svojih mobilnih mreža. Također, danas je dostupna široka paleta 4G usmjerivača koji omogućuju korisnicima spajanje i korištenje putem uređaja kao što su prijenosna računala i pametni telefoni . Trenutno se LTE najbolje koristi u suradnji s tehnologijom bežičnog lokalnog umrežavanja(Wi-Fi) kao podatkovnom uslugom.

Međutim, svaka mreža zahtijeva i stalno praćenje prometa, problema u mreži i svega ostalog što je važno u održavanju ali i opstanku same mreže. Wireshark je primjer mrežnog alata koji je korišten, odnosno primijenjen u radu . Kada je riječ o alatima otvorenog koda za upravjanje mrežom i detekciju mrežnih problemima, Wireshark se pokazao kao vrhunski izbor. U pitanju je mrežni analizator protokola koji je 1997. stvorio Gerald Combs, koji je trebao alat za praćenje problema s mrežom. Wireshark se, osim žičanih mreža, također često koristi kako bi pomogao pri dijagnosticiranju raznih WiFi problema, s kojima se svakodnevno susrećemo.

Evidentno je da se radi o moćnom mrežnom analizatoru protokola koji pruža brojne korisne mogućnosti. Prilikom traženja i analiziranja problema unutar mreže prikazao je mrežne nepravilnosti i propuste na jednostavan i detaljan način. Također, lako se zaključuje da softverski alat Wireshark uvijek može naznačiti gdje se problem pojavio, ali ne može nam točno reći zašto se problem pojavio. Na primjer, može se lako utvrditi da preklopnik duž puta ispušta pakete. No, ne može se utvrditi zašto taj prekidač ispušta pakete.

7. Literatura

[1] V. Lipovac, »Expert System Based Network Testing,« IntechOpen, 2011.

[2] S. Maček, *Razvoj i karakteristike mobilne mreže pete generacije,* Zagreb, 2016..

[3] B. Hrvatić, *4G mobilne mreže,* Rijeka, 2013..

[4] T. Blajić, Evolucija radijske pristupne mreže u mobilnim sustavima treće generacije, Zagreb: Tesla, 2006..

[5] M. Sauter, From GSM to LTE- Advanced, Revised 2nd Edition, Germany: Wiley, 2014.

[6] T. Blajić, LTE - Nova tehnologija za mobilni širokopojasni pristup, Tesla d.d., 2010..

[7] W. team, »Wireshark,« kolovoz 2010.. [Mrežno]. Available: http://www.wireshark.org/about.html.

[8] G. G. P. LICENSE, »gnu,« 29. lipanj 2007.. [Mrežno]. Available: https://www.gnu.org/licenses/gpl-3.0.html.

[9] L. Chappell, Troubleshooting With Wireshark, Chappell University, 2014..

[10] N. CERT, »CERT,« 2010. [Mrežno]. Available: www.cert..hr.

8. Prilozi

8.1.Popis slika

IZJAVA

Izjavljujem pod punom moralnom odgovornošću da sam rad izradila samostalno, isključivo znanjem stečenim na studijima Sveučilišta u Dubrovniku, služeći se navedenim izvorima podataka i uz stručno vodstvo mentora prof.dr.sc. Vlatka Lipovca, kome se još jednom srdačno zahvaljujem.

Josipa Kardum