Безбедност на VoIP системите

Настески Владимир – Европски Универзитет – Факултет за Информатика

Сашо Гелев – Европски Универзитет – Факултет за Информатика

***Апстракт*—Voice over Internet Protocol е термин, односно интернет протокол, кој означува пренос на гласовни комуникации преку Интернетот. VoIP системите обично работат со PSTN (Public Switched Telephone Network), кој пак овозможува транспарентна телефонска комуникација низ целиот свет. Оваа технологија за пренесување на гласовни разговори преку Интернет до крајните корисници се овозможи во крајот на осумдесеттите години од минатиот век. VoIP системите го пренесуваат говорот како дигиталното аудио, користејќи ја техниката на компресија на говорен податок, пакување на мали единици, обично на десетици милисекунди од говор. Системот е повеќе подложен на застој и на DoS (Denial of Service) напади отколку традиционалните circuit switched системи, бидејќи IP телефоните и IP инфраструктурата се поврзани на рутери или сервери, кои зависат од поставеноста на електронската мрежа или некој друг локален генериран извор на струја, што не е случај кај вообичаените телефони, кои пак при пад на струјата, истите продолжуваат да функционираат преку backup генераторите или батерии лоцирани во телефонските централи. VoIP исто така обезбедува низа на сервиси кои засега можат тешко да се имплементираат, од функционална гледна точка. Потоа, бидејќи UDP не нуди механизам за осигурување на доставувачките пакети во секвенцијален ред, или не нуди сигурносен Quality Of Service – QoS (што е еден од најголемите проблеми на VoIP), VoIP имплементациите се соочуваат со проблемот на латентност, џитер, губење на пакети и ехо. Овој труд дава приказ на проблемите со кои се соочува VoIP и мерки кои можеме да ги превземаме доколку се појави одреден проблем при VoIP комуникацијата.**

Клучни зборови – Voice Over Internet Protocol, Public Switched Telephone Network, Quality of Service, Latency, Jitter, Packet Loss

I. Вовед

VOICE over IP и IP телефонските технологии ги заменија традиционалните аналогни телефонски линии во дигитални гласовни комуникации. Потребни беа декади да се продуцира постојаност, стабилност и сигурност што ја нудеа старите TDM (Time Division Multiplexing) мрежи. VoIP и IPT (IP Telephony) се млади технологии, па потребно е време за IP технологиите да бидат еквивалентни на TDM технологиите. На пример, постојат нови недостатоци во безбедноста; основните податочни мрежи и IT уреди веќе се соочија со многу проблеми со безбедноста. VoIP и IPT технологиите се менуваат како што се менуваа начинот на кој серверите работат, како доделување на нови крајни точки (endpoint) IP телефони и gateways.

Овие нови точки носат нови проблеми со безбедноста. Не постои никаква измама во податочните мрежи, но неавторизирани IP телефони може да предизвикаат сметката за телефон со пристап на PSTN да биде огромна. Лажните VoIP уреди може да се искористат за пристап до податочните сервиси. Мешањето со call серверите може да се искористи за прислушување на повици и илегална авторизација за користење на забранети сервиси. Кога VoIP/IPT уредите пристапуваат до системи со информации кои мора да се соочат со усогласени побарувачки, решението на безбедноста станува посериозно. VoIP/IPT уредите бараат постабилни податочни мрежи. Како и да е, решенијата за безбедност често пати се во конфликт со изведената цел. IT одделот треба да располага со нови алатки дизајнирани за VoIP/IPT околина и проширување на постоечките безбедносни решенија.

Постојат разни продукти како ClarusIPC, кои се интегрираат во системите, и ги прошируваат функциите на постоечките мрежни апликации со цел безбеден повик преку IP.

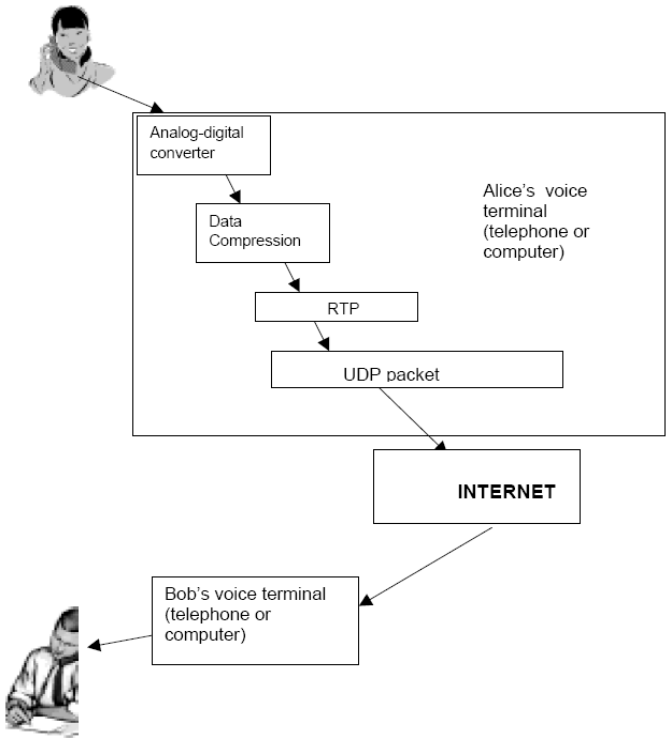
Накратко, VoIP технологијата е поевтина алтернатива во споредба со традиционалните PSTN телефонски линии. Иако имплементацијата е доста нова, оваа технологија сеуште е во развој и доживува експанзија во Северна Америка и Европа. Како и да е, VoIP полека си зазема доста важна позиција на телефонскиот пазар, заради големата флексибилност што ја нуди.

A. Пренос на сигналот преку VoIP мрежа

Во обичните телефонски системи, процесот на пренос на сигналот преку телефонска линија вклучува бирање на сакани бројки, кои подоцна се процесирани од страна на систем на телефонската компанија со цел воспоставување на сигнал. Со VoIP, корисникот мора да го внеси бараниот број, било да е на специјализирана VoIP опрема или телефонска тастатура, па подоцна се случува комплексни серии на размена на пакетот, базирани на VoIP протоколот. Проблемот е во тоа што компјутерските системи се адресирани користејќи ги нивните IP адреси, а корисникот внесува само обичен телефон. Телефонскиот број мора да се поврзи со IP адресата, со цел воспоставување на врска, слично на веб адреса која мора

да се поврзи со IP адреса на NIST (National Institute of Standards and Technology) веб серверот. Вклучени се доста протоколи во означувањето на IP адресата која кореспондира со телефонскиот број.

Односно, накратко, само што се воспоставува повикот, гласот се конвертира во дигитализирана форма, односно се сегментира во пакети. Првиот чекор е конвертирање на аналогните сигнали во дигитални, користејќи аналоген-дигитален конвертор. Бидејќи дигитализираниот глас бара голема бројка на битови, се користи компресиски алгоритам, што го намалува просторот на податоци кои треба да се пренесат. Протоколот за гласовните пакети е наречен Real-time Transport protocol (RTP). RTP пакетите имаат специјално header поле во кое се чува информација за гласовниот сигнал. Но, пакетите може да се пренесат и преку UDP (User Datagram Protocol) протоколите, кои често пати се користат за пренос на податоци. Со други зборови, RTP пакетите се пренесуваат како податоци од страна на UDP датаграмите, којшто се процесира преку обични јазли низ интернет. На другиот крај, процесот е обратен: пакетите се расклопуваат и се стават во соодветен редослед, дигитализираните гласовни податоци се екстрактираат од пакетите и се декомпресираат, потоа дигиталниот глас е процесиран од дигитален-аналоген конвертор со цел рендерирање на аналогни сигнали.



Слика 1: Процесирање на гласот преку VoIP

B. Брзина и квалитет

Теоретски, VoIP може да понуди редуцирана ширина на опсег, и квалитет подобар од претходните, конвенционални PSTN мрежи. Тоа значи дека, користењето на медија со висока ширина на опсег, својствена за податочните комуникации, го прави VoIP пофлексибилна алтернатива за говорна трансмисија. Но, ситуацијата не е толку едноставна. Рутирање на целиот сообраќај преку една мрежа, предизвикува пренатрупаност, и праќањето на истиот сообраќај преку Интернет може да предизвика големо задоцнување на говорот. Исто така, искористеноста на ширината на опсегот за дигитализација на глас користи кодеци, кола или разни софтверски процеси кои кодираат, а соодветно и декодираат податоци за нивна трансмисија. Тоа значи продуцирањето на поголема ширина на опсег може да го забави процесот на пренос и кодирање. Подобрувањата на брзината и квалитетот на гласот веќе се поставени во VoIP мрежите и телефоните, а многу организации што се пренасочија во VoIP имаат забележано слабост во брзината или пак квалитетот кај VoIP, кое пак се должи на несоодветната имплементација на VoIP сервисот и низа на пропусти и проблеми со безбедност со која се соочува истиот.

II. Проблеми со безбедност на VoIP

По овој вовед што го дадовме за VoIP, на ред е да се спомне и безбедноста на VoIP, што е главна тема на овој труд. Разгледувајќи како се пренесува гласот преку Интернет, доаѓаме до заклучок дека потребно е да ги заштитиме нашите податоци и нашиот глас. Тоа е од огромно значење за сечија приватност.

Во традиционалните телефонски системи, безбедноста е на прво ниво. Прислушувањето на разговорите бара физички пристап до телефонските линии или компромис на Private Branch Exchange (PBC). Само одредени безбедносни организации се занимаваат со енкриптирање на гласовен сообраќај преку традиционалните телефонски линии. На пример, кога се порачува одреден производ преку телефон, повеќе од луѓето ќе го прочитаат бројот на кредитната картичка на човекот на другиот крај. Броевите се пренесени без никаква енкрипција на продавачот. Во спротивно, ризикот на праќање на неенкриптирани податоци преку Интернет е многу побитно. Пакетите пратени од домашниот компјутер до online продавачот, потребно е да помини низ околу 15-20 системи кои не се под контрола на корисничкиот ISP или под контрола на продавачот. Бидејќи бројките се пренесуваат користејќи стандард за пренос на бројки, секој со пристап до овие системи може да инсталира софтвер кој ги скенира пакетите за информација на бројот на кредитните картички. Заради ова, online продавачите користат енкриптирачки софтвер со цел заштита на информацијата на корисникот и број на кредитна картичка. Па, според ова, доколку пренесуваме глас преку Интернет, потребно е да се воведат слични мерки на безбедност.

Вообичаената архитектура на Интернетот не нуди иста физичка жичана безбедност како телефонските линии. Целта на безбедноста на VoIP системите е да се користат безбедносни механизми кои треба да се воспостават на

податочните мрежи (firewall-и, енкрипција итн), со цел да се емулира безбедносното ниво што го уживаат корисниците на PSTN мрежите.

Вообичаените телефони се конектирани директно со други телефони преку телефонски линии, кои во случај на пад на енергијата, продолжуваат да функционираат од backup генераторите или батерии лоцирани на телефонските централи. Како и да е, IP телефоните и IP инфраструктурата се поврзани на рутери или сервери, во зависност од поставеноста на електронската мрежа или некој друг локален генериран извор на струја.

Понатаму во овој труд ќе се запознаеме со нападите и одбраните на VoIP и начините за обезбедување на ниво на безбедност на VoIP мрежите.

III. Проблеми со Quality of Service

Quality of Service (QoS) е фундаментален процес во една VoIP мрежа. И покрај сите пари што VoIP ги заштедува кај корисниците и мрежната отменост што ја нуди, доколку не можи да достави ни најблиску квалитетен повик, тогаш VoIP нуди малку од огромната вредност. Имплементацијата на различни безбедносни мерки може да го понижат QoS. Овие компликации се простираат од каснењето или блокирањето на повик од страна на firewall-ите, па се до енкрипциска латентност и варијација на каснење (џитер). QoS проблемите се централна точка на безбедноста на VoIP. Доколку се обезбеди QoS, поголемиот дел од истите безбедносни мерки имплементирани во денешните податочни мрежи, може да се искористи и во VoIP мрежите. Но, поради временско-критичната природа на VoIP, и неговата ниска толеранција за дистрибуција и губиток на пакети, повеќето безбедносни мерки имплементирани во традиционалните податочни мрежи и не се применливи во VoIP во истата форма. Најголемите QoS проблеми поврзани со VoIP кои даваат ефект врз безбедноста се: латентност, џитер, губиток на пакети, ехо, потребата за брзина, падот на струја и backup системите и др.

A. Латентност

Латентноста во VoIP се однесува на времето што е потребно за гласовната трансмисија да помине од изворот до дестинацијата. Се разбира води до каснење, а потоа до ехо. Тоа се предизвикува од страна на бавните мрежни линкови.

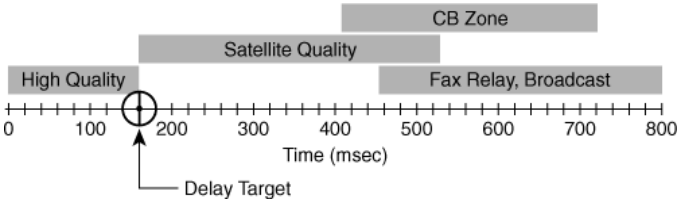
Постојат 2 вида на латентност кои можеме да ги измериме: латентност во еден правец и обиколна латентност (round-trip latency). Латентноста во еден правец е времето потребно пакетот да патува во еден правец од изворот до дестинацијата. Кружната или обиколната латентност е времето потребно пакетот да патува до и од дестинацијата, па назад до изворот. Всушност, не е истиот пакет кој се враќа назад, но така е општо прифатено, па се користи секаде во литературата дека пакет патува од изворот и дестинацијата и обратно.

Латентноста се мери во милисекунди (ms) – илјадници делови од секундата. Латентност од 150ms тешко се забележува, па затоа и се прифаќа. Повисока латентност од оваа, веќе се забележува на квалитет на врската. Кога достигнува повеќе од 300ms, латентноста е веќе неприфатлива.

Постојат неколку ефекти на латентноста преку гласовен квалитет:

- Ги забавува телефонските разговори;
- Ненавременоста може да резултира преклопување на шумови, преку фактот дека еден говорник му смета на друг;
- Предизвикува ехо;
- Вознемирува синхронизација помеѓу гласот и другите видови на податочни типови, особено за време на видео конференција;

Каснењето не е ограничено на крајните точки на системот. Секој хоп низ мрежата вклучува ново каснење. Исто така, поголемите пакети се стремат да предизвикаат пренатрупаност на bandwidth и зголемена латентност. Со овие проблеми, VoIP се стреми да работи на мали пакети во една мрежа, со цел да се држи латентноста на минимум.



Слика 2: End-to-end латентност

Како што е покажано на Слика 2, некои форми на каснење се подолги, и истите се прифатени бидејќи не постојат други алтернативи. Во сателитската трансмисија, на пример, потребни се околу 250ms да трансмисијата стигне до сателитот, и други 250ms за истата да се врати назад до Земјата. Ова резултира со каснење од 500ms. Иако ITU-T забележува дека ова е надвор од прифатениот опсег на гласовен квалитет, многу разговори денес се остваруваат преку сателитски врски. Често пати корисниците се навикнуваат и го прифаќаат ова каснење, па затоа и оваа врска е општо прифатена.

Воопшто неприфатливо е каснењето да достигне до 2 секунди (што доведува до отфрлање на пакетот). Оваа латентност е неприфатлива од скоро сите гласовни мрежи. Латентноста е една од компонентите на end-to-end каснењето. Друг начин на end-to-end каснење се случува преку џитерот.

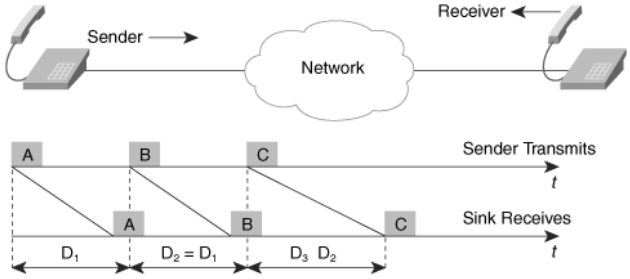
B. Џитер

Џитер (jitter) се однесува на неуниформирани каснења на пакетите. Често пати се појавува во ситуација на низок bandwidth во VoIP и може да биде исклучително штетно низ целосниот QoS. Големата бројка на варијации на каснења може да биде поштетна од обичните каснења. Џитерот може да направи да стигнат пакетите во измешан

редослед. RTP, протоколот кој се користи за пренос на гласовни податоци се базира на UDP протоколот, па пакетите кои се во безредие не се склопуваат на протоколно ниво. Како и да е, RTP дозволува апликациите да прават повторно склопување користејќи секвенца на бројки и полиња на временски маркици (timestamp).

Од страна гледано, подредувањето на овие пакети не е тривијално, особено кога се работи со тесното време на VoIP.

Кога џитерот е висок, пакетите до нивните дестинации пристигнуваат забрзано. Оваа ситуација е аналогна на патниот сообраќај. Кога семафорот е зелен (се отвора bandwidth-от), настанува натпревар во сообраќајот, односно секој вози сè побрзо да се стигне зеленото светло и да се премине семафорот. Основниот лек да се контролира џитерот на крајните точки на VoIP е користењето на баферот, но таков бафер што ќе ги испушта пакетите барем на секои 150ms, со цел ограничување на варијациите на каснења. Проблемот со бафер имплементацијата се влошува со несигурноста од тоа дали пакетот што недостасува касни анонимно низ времето, или всушност истиот е изгубен. Доколку џитерот е променлив, тогаш системот не може да ги користи минатите временски каснења како индикатор за статусот на изгубените пакети. Ова го остава системот отворен за имплементација на специфично однесување во зависност од пакетот.



Слика 3: Варијација на каснење (џитер);

На Слика 3 претставено ни е времето што треба пакетите А и В да се пратат или да се преземат, а и може да забележиме дека тоа е исто, односно D1=D2. Пакетот С касни во мрежата, односно се прима покасно од очекуваното. Затоа се користи џитер-бафер, бидејќи го крие интервалот помеѓу каснењето на пакетите. Гласовните пакети во IP мрежите имаат доста битни интервали на пакетите. Препорачана практика е да се избројат пакетите кои пристигнуваат покасно, па да се претстави однос помеѓу овие пакети и пакетите кои успешно пристигнати. Потоа овој однос може да се искористи да се намести џитер-баферот, со цел помала и полесна работа за пресметување на каснењето на пакетите.

Џитерот може да се контролира од страна на VoIP мрежата со користење на рутери, firewall-ови и други елементи кои ги поддржува QoS. Овие елементи процесираат и пуштаат низ времето итен сообраќај како VoIP пакети порано, наместо помалку итни податочни пакети. Како и да е, не сите мрежни компоненти се дизајнирани со добар QoS. Пример, мрежен елемент во кој нема имплементирано QoS, претставува криптирана направа која игнорира Type of Service (ToS) битови во IP header-от и доста други индикатори на итност на пакети. Друг метод за редуцирање на варијанти на каснење е да се изработи мрежен сообраќај за минимизирање на џитерот, со што е можно поефикасно искористување на bandwidth-от. Ефективниот bandwidth се остварува кога пакетите се проширени со нови header-и. Во нормален IP сообраќај, овој проблем е занемарлив сè додека се менува големината на пакетот во многу мали пакети, во споредба со големината на пакетот. Бидејќи VoIP користи многу мали пакети, само минимално зголемување е потребно, бидејќи зголемувањето се натрупува низ сите пакети и VoIP праќа многу голем обем од овие мали пакети.

Прозорецот на доставување на VoIP пакети е многу мал, па следи дека прифатливата варијација на каснење на пакетите е дури и помала. Така, иако се грижиме за безбедноста, крајната грижа е да каснењето на пакетите, односно доставувањето на пакетите, биде униформирано низ целиот проток на сообраќајот.

Битно е да се напомени дека *џитерот* и *вкупното каснење* не се исто, иако постоењето на доста голем џитер може да го зголеми вкупното каснење во мрежата. Ова е затоа што колку повеќе џитер имате, толку е потребен поголем џитер-бафер.

C. Губиток на пакети

VoIP е подлежен на губиток на пакети. Губитокот на пакети експоненционално се зголемува. Тоа се јавува како резултат на прекумерна латенција, каде одредена група на пакети пристигнува покасно и истата мора да се исфрли со цел прифаќање на новите. Исто така може да се јави како резултат на џитерот, односно кога пакетот пристигнува откако неговите околни пакети се пуштени од баферот, што значи бескорисно примање на пакетот. Некои проблеми на VoIP поврзани со губитокот на пакети се појавуваат и во податочните мрежи, односно во овој случај пакетот воопшто не се доставува. Пресметувајќи го проблемот на губиток на пакети се наоѓа во зависноста на VoIP од RTP, што користи несигурносен UDP за транспорт, и на тој начин не се гарантира пристигнувањето на пакетот. Како и да е, времето не дозволува да се користи сигурносен протокол како TCP за доставување на медија. Со тек на време, пакетот може да се пријави како исчезнат, повторно пратен и примен, додека времето на QoS истекува. Добрата вест е дека VoIP пакетите се многу мали, односно содржат payload од 10-50 бајти, што значи 12.5 до 62.5ms, односно повеќе имплементации во што помал опсег.

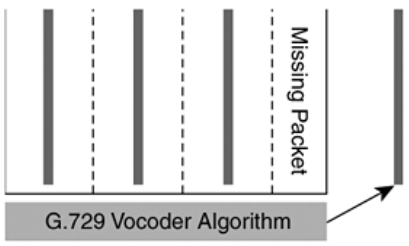
Губиток на толку мала вредност на говор не е запримeтлив од еден VoIP корисник. Лошата вест е дека овие пакети обично не се изгубени. Пренатрупаноста на bandwidth и други проблеми на губење на пакети, помагаат при навремено пристигнување на пакетите во иднина. Па, иако губењето на еден пакет е сосема безначајно, можноста за губење на еден пакет значи и

губење на повеќе пакети, што едноставно го намалува квалитетот на сервис во VoIP мрежата.

Како споредба на VoIP квалитетот со традиционалните circuit-switched мрежи, истражувањата од Telecommunications Industry Association [1] (TIA) покажаа дури помал процент на губиток на пакети, што нивото на QoS во VoIP мрежата е пониско отколку што корисниците го очекуваат во традиционалните телефонски линии. Секој кодек на TIA студиите искуси нагло опаѓање во задоволство на корисниците, кога латентноста ја премина точката на 150ms. Како и да е, дури со помала латентност од 150ms, губитокот на пакетот од 5% предизвикан од сообраќај на VoIP кодиран со G.711 (интернационален стандард за кодирање на телефонско аудио на 64 kbps) паѓа под нивото на квалитет на сервис. Слично, губиток од 1 и 2 проценти е доволно за одличен квалитет во VoIP мрежите, кодирани со G.723.1 (за компресија на говор со многу мала податочна стапка) и G.729A (за гласовна компресија на 8 kbps). Следствено, губиток од 3 и 4 проценти, пројавува незадоволни корисници. Овие резултати се потврдени од студиите на UCal – Berkley во 1998, што имаат утврдено дека "степенот на толерантност на губење на пакет е 1-3%, а квалитетот не нетолерантен кога повеќе од 3% од гласовните пакети се изгубени" [2]. И двете студии укажаа дека големата стапка на компресија резултира на поголема нестабилност и губење на пакетите. Процентуалностите презентирани од двете студии не укажуваат на големината на пакетите и на други особини што можат да предизвикаат губиток на пакети и QoS.

Не можеме да гарантираме дека сите пакети ќе стигнат, но доколку имаме bandwidth на располагање, праќањето на редундантна информација може да ја анулира шансата за губиток. Таков bandwidth не е секогаш достапен, па така мора да се изврши редундантната информација, вклучувајќи повеќе латентност во системот, а со тоа и поголем губиток на пакети. Развиени се нови кодеци, како internet Low Bit-rate Codec (iLBC), и истите нудат суров квалитет на гласот и комплексност на G.729A, со зголемена толеранција на губиток на пакетите.

VoIP имплементацијата на Cisco системите [3] овозможува гласовниот рутер да одговара на периодичен губиток на пакетите. Доколку гласовниот пакет не е примен кога што е очекувано, се претпоставува дека е изгубен, а пак последниот пакет што е примен е препратен, како што е покажано на Слика 4. Бидејќи губитокот на пакетот е само 20 ms на говор, обичниот слушател не забележува никаква разлика во квалитетот.



Слика 4: Губиток на пакети со G.729

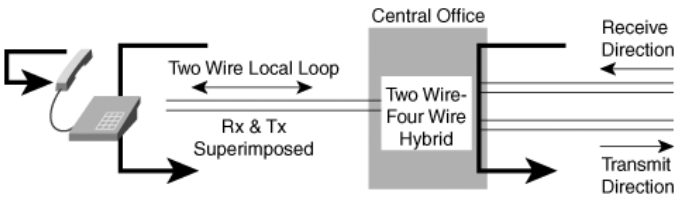
Користејќи ја G.729 имплементацијата на Cisco за VoIP, секоја од линиите на Слика 4 претставува пакет. Пакетот 1, 2 и 3 стасуваат до дестинацијата, но пакетот 4 е изгубен некаде во трансмисијата. Примателот чека за одреден временски период (во зависност од џитер-бадферот), а потоа се извршува стратегија на затскривање (concealment strategy).

D. Exo

Ехото е одличен феномен кој може да се доживее во Големиот Кањон. Но, ехото кај телефонските разговори варира од доста досадно до неподносливо, што го прави разговорот неразбирлив.

Слушањето на сопствениот глас во рисиверот додека зборувате е сосема нормално за говорникот и делува смирувачки. Слушањето на сопствениот глас во рисиверот со каснење од повеќе од 25 ms, може да предизвика прекини и модулација во разговорот.

Во традиционалните мрежи, ехото е предизвикано од грешка во импеданцата (Impedance Mismatch) од four-wire network switch конверзија до two-wire local loop (Слика 5). Ехото, во стандардните PSTN мрежи е регулиран со ехо прекинувачи (echo canceller) и добра контрола на грешните импеданци во вообичаените точки на рефлексија (Слика 5).



Слика 5: Ехо предизвикано од Impedance Mismatch

Ехото има два недостатоци: може да биде гласно и може да биде долго. Колку е погласно и подолго ехото, толку повеќе предизвикува нервоза. понервозно истото.

Телефонските мрежи во овие делови на светот каде аналогниот глас првенствено се користи, применуваат стабилизатори на ехото, кои го отфрлаат ехото со покривање на импеданцата во кругот. Ова не е најдобриот механизам што се користи за отфрлање на ехото, па истиот предизвикува и доста проблеми. Не можеме да користиме ISDN мрежи на линија која има стабилизатор на ехо, на пример, бидејќи стабилизаторите го пресекуваат фреквентниот опсег кој го користи ISDN.

Во денешните мрежи, може да искористиме прекинувачи на ехото во нискоопсежните кодеци и истите да ги искористиме на секоја DSP. Во некои мануфактурни имплементации, прекинувачите на ехото се софтверски поставени; оваа практика драстично ги редуцира предностите на ехо прекинувањата. VoIP имплементацијата на Cisco [4], целосното прекинување на ехото го извршува во неговиот DSP.

Да разбереме како работат прекинувачите на ехото, прво потребно е да разбереме од каде доаѓа ехото.

Во овој пример, да претпоставиме дека корисникот А зборува со корисникот В. Разговорот помеѓу корисникот А и В е наречен G. Кога G појавува грешка во импеданцата, или појавува ехо, тоа се враќа до А. Корисникот А може да ги слушне каснењето неколку милисекунди по неговото зборување.

Да се отфрли ехото од линијата, уредот на корисникот А прави инверзна слика на разговорот на корисникот А за одредено време. Ова е т.н. инверзен говор (-G). Прекинувачот на ехо го слуша звукот што доаѓа од корисникот В и го одзема –G, со цел тргање на ехото.

Прекинувачите на ехо се ограничени од вкупното време кои го чекаат да се рефлектира разговорот што е примен, т.н. феномен познат како ехо опашка. Cisco има конфигурирано ехо опашки за 16, 24, 32, 64 и 128 ms [4].

Битно е да се конфигурира соодветната големина на прекинување на ехото, со иницијална инсталација на VoIP опрема. Доколку се конфигурира премногу прекинување на ехото, би зело повеќе време за прекинувачот на ехо да го конвертира, па да го елиминира ехото.

IV. Заклучок

Денес VoIP сè повеќе се имплементира во замена на аналогната телефонија. Цените се сè поприфатливи за корисниците, со што денес VoIP е новиот тренд на телефонијата.

Неколкуте недостатоци кои се појавуваат од ден на ден се надминуваат, како што технологијата се усовршува. Како што податочниот сообраќај расте и сè повеќе го надминува гласовниот сообраќај, конвергенцијата и интеграцијата на овие технологии не само што ќе продолжи да се подобрува, туку исто така ќе создаде услови за вистинско обединето гледање кон комуникацијата. Имплементирањето на VoIP може да вметни вистински бенефиции и заштеди на било која компанија.

Иако во почетокот VoIP се соочи со проблемот на џитер, латентност и ехо, денес VoIP станува сè попопуларен и тие проблеми стануваат минато. Од ден на ден технологијата се подобрува и истата е одличен извор за подобрувањата на проблемите со безбедноста на VoIP.

Библиографија:

[1]. R. Sinden, “Comparison of Voice over IP with circuit switching techniques”.Department of electronics and Computer Science, Southampton University, UK, Jan. 2002

[2]. C-N. Chuah, “Providing End-to-End QoS for IP based Latency sensitive Applications”. Technical Report, Dept. of Electrical Engineering and Computer Science, University of California at Berkeley, 2000

[3]. http://www.ciscopress.com/articles/article.asp?p=606583&seqNum=6

[4]. http://www.ciscopress.com/articles/article.asp?p=606583&seqNum=5

[5]. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries “Security Considerations for Voice Over IP Systems” - Recommendations of the National Institute of Standards and Technology

[6]. Gary Audin, Delphi, Inc. And Richard Whitehead, Clarus Systems, Inc. “VoIP Security It’s More Than Data Security” – A Clarus Systems White Paper, June 12, 2006

[7]. http://www.ciscopress.com/articles/

[8]. http://www.bandwidth.com/

***Abstract*—Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet. Internet telephony refers to communications services—voice, that is transported via the Internet, rather than the Public Switched Telephone Network (PSTN). This technology became available in the early ‘80s. The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/translation of the signal into IP packets for transmission over the Internet. This system is more prone to congestion and DoS (Denial of Service) attacks than traditional circuit switched, because the IP phones and IP infrastructure are connected to routers or servers, which depends on the electricity of some local generator, which is not even the same with the infrastructure with the traditional phones, which have backup generator located inside the telephone center. Because the underlying IP network is inherently unreliable, in contrast to the circuit-switched public telephone network, and does not inherently provide a mechanism to ensure that data packets are delivered in sequential order, or provide Quality of Service (QoS) guarantees, VoIP implementations face problems mitigating latency, jitter, packet loss and echo. In this paper are described the problems which VoIP faces with, and the mechanism taken for solving those problems.**