МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ ХОЛБОО ТЕХНОЛОГИЙН СУРГУУЛЬ

Ууганбаяр Өнөбат

Voice encryption

Мэргэжил : Компьютерийн Системийн Хамгаалал

Компьютерийн ухааны бакалаврын төсөл

Улаанбаатар хот

2017 он

Гарчиг

Зургийн жагсаалт

Товчилсон үгсийн жагсаалт

ITU International Telecommunication Union

UAS User Agent Server

UAC User Agent Client

SIP Session Intitiation protocol ()

ISP Internet Service Provider

VOip Voice over internet protocol

RTP Real-time transport

RTCP Real-time Control protocol

EIM Enterprise Instant Messaging

CIM Consumer Insant Messaging

OSI Open system interconnection

Бүлэг 1

Ерөнхий агуулга

1.1 Удиртгал

Өнөөдөр хүн бүр өөрийн гэсэн компютер болон эцсийн төхөөрөмжүүдээр утастай болон утасгүй сүлжээгээр дамжуулан холбогдож харилцах боломжтой болсон.Өнөөдөр л гэхэд дэлхийн нийт хүн амын 30 хувь нь ухаалаг гар утас ашигладаг гэсэн судалгаа бий. Монгол орон л гэхэд хүн амын 70 хувь нь интернет ашигладаг гэсэн судалгаа гарсан байдаг. Үүнийгээ дагаад харилцаа холбооны орчиндох мэдээллийн сан өдөр бүр өргөжиж мөн бизнесийн үйл ажиллагаа маш эрчимтэйгээр явагдах болсон юм. Өдөр бүрийн харилцаа болон хүн бүрийн хувийн хэрэглээг хянах болон бусдад өөрийн нууц мэдээлэлээ алдахгүй байх боломжыг бүрдүүлж өгч буй гол арга нь Voice Encryption юм.

1.2 Зорилго

Энэхүү төсөлийн ажлын зорилго нь Voice Encryption -ийг судлах ба хэрхэн дуу хоолойг нууцалж дамжуулж байгааг судалж эдгээрийг ашиглан сүлжээнд хэрхэн яаж дамжуулах, замчлах,ямар пакет ашиглаж байгаа мөн өөр төстэй програмуудын ажиллагааг шалгах юм.Voice Encryption нь харилцааны үед мэдээллийг харилцагч 2 талд зөвхөн ойлгогдохуйц , үнэн зөв дамжуулах,гадны халдлагаас мэдээллийг хамгаалах юм.Энэхүү ажлаар хэрэглэгч хооронд нууцалсан дуун мэдээлэл дамжуулж туршиж үзэх болно туршиж үзэх болно.

Бүлэг 2

Онол, арга зүйн бүлэг

2.1 Дуу авиа гэж юу вэ?

Ямар нэгэн биет хэлбэлзэх үедээ орчин тойрныхоо агаарыг хэлбэлзүүлдэг.Бидний сонсож буй дуу авиа агаарын хэлбэлзлээр дамждаг.Чичирхийлэн хөдөлж байгаа бие дуу авиаг үүсгэдэг. Нэг ёсондоо дуу авиа нь шахагдсан долгион бөгөөд тасралтгүй үргэлжилдэг.Дуу авиа нь ойно,хугарна, тархана. Агаар байхгүй бол дуу тарахгүй. Хүний чих 20-20000Гц давтамжтай дууны долгионыг мэдэрдэг.Хүн амьтан бие биетэйгээ харилцах мөн ойлголцохын тулд дуу авиаг ашигладаг.Дуу авиа улам хөгжин өргөжиж харилцаа холбоо хэмээх том салбар гарч ирсэн.Өдөр бүр л хүн болгон утас болон интернетээр дамжуулж өөр хоорондоо харилцаж мэдээлэл солилцож байна.

2.2 Харилцаа холбооны хөгжлийн үе шат

Дуу хоолойг ширфлэж дамжуулах болсон үе нь Дэлхийн 2р дайны АНУ-н зэвсэгт хүчний ажиллагаа байсан юм.Тэр үед дайснууд урьдчилан сонсхоос сэргийлж зорилгоор дуут дохиог нэмсэн байна.Ингэснээр дамжуулагч 2 тал тухайн мэдээллийг унших боломжтой болсон.Өнөөдөр дуу хоолой шифрлэлтийн арга эрс хөгжсөөр байна.Аналагоос дижитал руу шилжин хуучин аргаа сольж дуу хоолойг шифрлэж,цогц алгоритм ашиглаж байгаа нь илүү аюулгүй ,илүү үр дүнтэй болгож байна.

Утасгүй харилцаа холбооы технологи 1940-өөд оны дунд үед үүсч бий болсон боловч 1980-аад оноос нийтийн хэрэгцээнд нэвтэрч эхэлсэн байна.Зарим мэргэжилтнүүд утасгүй холбооны технологийн хөгжлийн эхний шатыг 0G хэмээн нэрлэдэг. Гар утасны

технологийн хөгжлийн тухай Сүүлийн жилүүдэд дэлхийн улс орнууд гар утас буюу утасгүй харилцаа холбооны хөгжлийн 4-р (4G) үед шилжиж эхэлж байгаа билээ. Мөн манайд хэдэн жилийн өмнө хөдөлгөөнт интернетийн 4G Mobile Wimax утасгүй систем байгуулагдсан боловч гар утасны технологид хараахан нэвтэрч эхлээгүй байна. Энэ удаад гар утасны хөгжлийн үе шатуудын тухай товч танилцая.

0G Утасгүй харилцаа холбооны технологи 1940-өөд оны дунд үед үүсч бий болсон боловч 1980-аад оноос нийтийн хэрэгцээнд нэвтэрч эхэлсэн байна. Зарим мэргэжилтнүүд утасгүй холбооны технологийн хөгжлийн эхний шатыг 0G хэмээн нэрлэдэг. Энэ үеийн гар утаснууд радио долгионы зарчимаар ажилладаг бөгөөд овор, жин ихтэй байсан учир ихэвчлэн автомашинд суурилуулан ашигладаг байжээ. Мөн одоогийн Иридиум системтэй төстэй сансарын холбооны технологи бүхий гар утаснууд усан онгоцны холбооны зориулалтаар ашиглагдаж байсан байна.

1G 1982 оноос эхний шатны гар утаснууд бүтээгдэж хүний дуу хоолойг аналоги долгион хэлбэрээр дамжуулж дууны өнгөнөөс хамаарах тасралтгүй дохиоллыг ашигладаг болов. Дохиоллын зурвасын хүрээ өргөн боловч, харьцангуй том хэмжээний батерей шаардагддаг, хөндлөнгийн элдэв дохиоллын нөлөөлөлд өртөмтгий, хамгаалалтын систем муу буюу зарим онцлог төхөөрөмж бүхий хүн бусдын яриаг хөндлөнгөөс сонсох боломжтой байжээ. Хамгийн сул тал нь бусдын утасны дугаарыг хуулж аваад өөрийн дураар ашиглах боломжтой байв.

2G 1991 оноос 2G стандарт боловсруулагдаж PDC, GSM мэтийн дижитал системүүд ашиглагдах болов. Энэ технолиги нь дуу хоолойг 1 буюу 0-оор илэрхийлэгдэх тоон дохиолд хувирган дамжуулдаг учир дээр дурдсан дутагдалуудыг бүрэн арилгасан илүү найдвартай систем болсон байна. Мөн дохиоллыг кодлон хувиргаж хамгаалалтын шаардлагийг бүрэн хангасан учир дохиоллын илүү нарийн зурвасыг хамарч, харьцангуй бага энерги зарцуулдаг учир батерейн хэмжээг жижигрүүлэх боломжтой болов. Мөн үнийн хувьд харьцангуй хямд болсон байна. Өөр нэг онцлог нь энэ үеийн технологиос эхлэн гар утсаараа SMS буюу богино хэмжээний текст илгээх, хүлээн авах боломжтой болсон байна. Адил урттай радио долгионы хүрээнд их хэмжээний харилцан ярианы долгионыг шахах боломжтой болсон учир гар утасны оператор компаниуд олноор байгуулагдаж, дэлхий даяар түгэн дэлгэрч эхэлсэн юм.

3G Олон улсын Телефон Харилцаа Холбооны байгууллагаас IMT-2000 хэмээх хөдөлгөөнт утасны стандартыг тодорхойлсон бөгөөд анхны 3G системийг 2001 онд япон

улсын NTT Dokomo компани нэвтрүүлсэн байна. Энэ шатанд W-CDMA, CDMA2000 зэрэг өндөр хурдны дижитал системүүд голлож байна. 3G системийн гар утсаар дуу, дүрс болон өгөгдлийг өндөр үр ашигтайгаар дамжуулдагаас гадна интернетээр аялж мэдээлэл татаж авах, youtube видео үзэх, фото зураг агуулсан текст мэдээлэл илгээх боломжтой болсон байна. Мөн 3.5 G хэмээх завсрын ангиллыг гаргаж ирсэн бөгөөд интернетээс мэдээлэл унших хурдаар ялгаагдаж байна. 3G системээр интернетэд ойролцоогоор 200-700 кб/с хурдаар холбогддог бол 3.5 G системд 3.6 - 7.2 Мб/с хүртэлх хурдтай холбогдох боломжтой юм. Өөрөөр хэлбэл broadband буюу өргөн зурвасын интернетийг утсагүй технологиор хүлээн авах боломжтой болжээ. Харин 2009-2010 онд гарсан хамгийн сүүлийн үеийн зарим системүүд 15-24 мб/с хурдыг санал болгож байна.

4G Гар утасны TeliaSonera компани хамгийн анхны 4G сүлжээг Норвег болон Шведийн Осло, Стокольм хотуудад байгуулж 2009 оны 12 сард ашиглалтад оруулсан байна. Мөн 2010 оноос америк япон зэрэг улсуудад 4G системд шилжиж гар утас болон бусад хөдөлгөөнт төхөөрөмжүүд IP-д суурилсан хөдөлгөөнт өргөн зурвасын сүлжээнд 50 Бб/с-ээс 100 Мб/с хүртэлх хурдаар холбогдон интернет, өндөр чанар бүхий телевизийн нэвтрүүлэг, видео, онлайн тоглоом тоглох зэргээр орчин үеийн интернетэд суурилсан бүх төрлийн үйлчилгээг хүртэх боломжтой болж байна. Холболтын хурдаар өмнөх үеэс 10 дахин илүү бөгөөд цаашид 1Гб/с-д хүргэх боломжтой. 4G үеийн голлох 2 систем нь LTE-Advanced болон WiMax2 стандартууд бөгөөд аль аль нь хүчин чадал сайтай боловч өндөр өртөг шаардагдсан технологиуд юм. АНУ-д Sprint Nextel, Comcast компаниуд Mobile WiMAX сүлжээг байгуулж , 2010 оны 6 сараас анхны 4G гар утас HTC EVO-г худалдаалж эхэлсэн байна. Гар утасны дэлхийн хамгийн том оператор компани болох China Mobile ирэх жилээс 4G системд шилжихээ мэдэгдсэн билээ. Сүүлийн жилүүдэд дэлхийн улс орнууд гар утас буюу утасгүй харилцаа холбооны хөгжлийн 4-р түвшинд шилжиж байна.

2.2.1 4G түвшний давуу талууд

- Илүү хурдтай
  - 4G Интернэт протокол IP ашигладаг учир маш олон зүйл дамжуулж чадна
  - Илүү хол зайд дамжуулдаг.4G саад багатай орчинд 50км (WiMAX).
  - Сүлжээ хоорондын шилжилт тасалдалгүйгээр хийдэг.
  - Маш их хэмжээний хэрэглэгчтэй ажиллах чадвартай

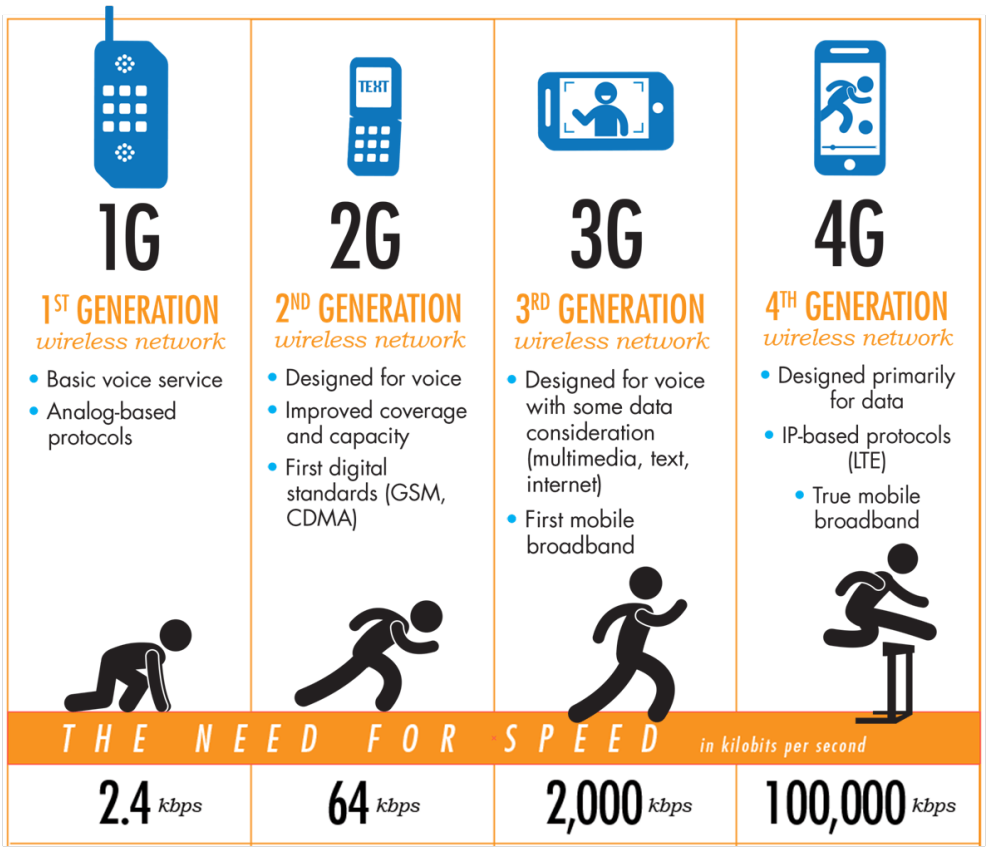
• Маш хурдтай ажилладаг алгоритмуудтай.

• Алдаа засалтын код хамт дамжуулдаг

•Бүх IP сүлжээ дэмжинэ. (Tunnel болон Firewall, authentication буюу нэвтрэлтийн нууцлал хамгаалал, ip -p байршил тогтоох)

•Нууцлал хамгаалалт (Encryption protocol ашигладаг)

•IPv6 дэмждэг

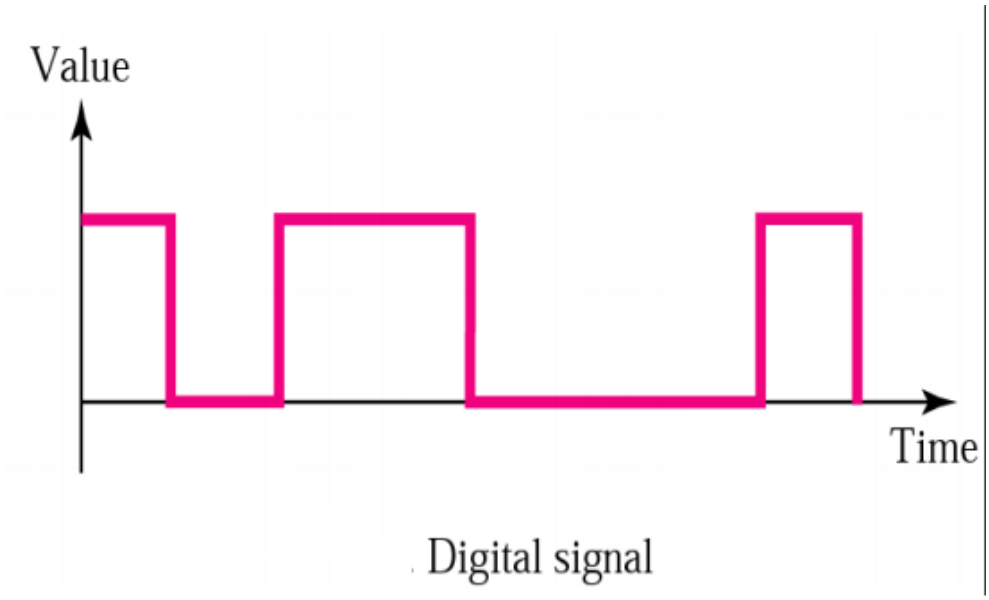


Зураг 2.1: Харилцаа холбооны хөгжлийн үе шат

2.3 Дижитал

Тоон өгөгдөл нь тасалдсан утга авна.Тоон дохио нь зөвхөн 2 хязгаарлагдмал утыг дүрсэлнэ. Ихэвчлэн 0, 1 байна.

Дижитал дуу хоолой ширфлэх арга нь ихэвчлэн 2 хэсгээс бүрдэнэ.Digitizer(ижил дохиог тоонд хувиргах)мөн тоон дохиог хөрвүүлэхэд шаардлагатай нууцлалыг хангах систем.



Зураг 2.2: Тоон дохио

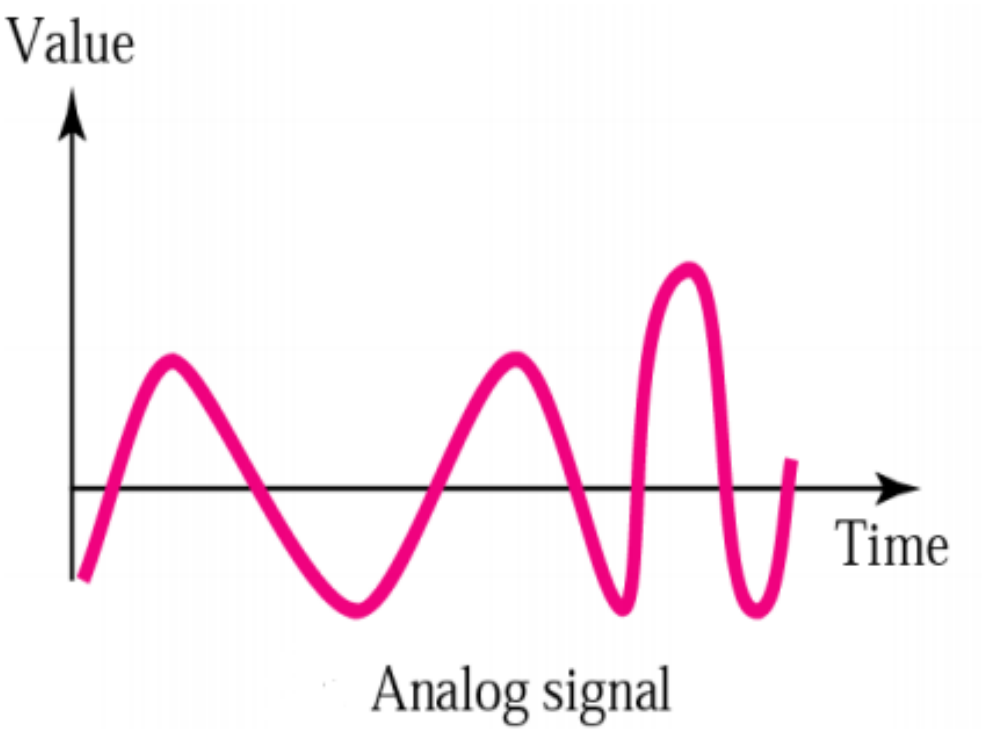
2.4 Аналог

1. Аналог өгөгдөл нь хугацааны турш тасралтгүй үргэлжилсэн утгатай байна

   Үйлилгээг хүссэн хэрэглэгчийг үйлчилгээ авах хүчинтэй эсэхийг баталгаажуулдаг.

   Бүртгэлтэй мэдээллээр дамжуулагдан хийдэг Жишээ нь нууц үг, тоон сертификат, утасны дугаар г.м

   Authentication амжилттай болсны дараа сессион эхэлдэг. Энэ нь сүлжээний холболт дуусах хүртэл үргэлжилдэг.



Зураг 2.3: Аналог дохио

2.4.1 Аналогоос дижитал

1. Аналог тоон дохиог хувиргах ажиллагаа нь үргэлжилсэн хугацаа мөн далайцын дохиог дискрэт хугацаа болон далайцын утгууд руу хөрвүүлэх зэргээс бүрддэг.Сорьц авч сонгох буюу sampling ,тоон хэлбэр лүү оруулах нь аналог тоон дохион хувиргалтыг гүйцээхэд хэрэгтэй алхамуудыг бий болгодог. Энэхүү хувиргалтыг хийх явцад үүсэж болох мэдээллийн алдагдлыг багасгахын тулд Sampling болон тоон утга руу шилжүүлэх зэрэг зүйлсийг ойлгох хэрэгтэй. Sampling-Quantization(тоон хэлбэрт шилжүүлэх)-Signal reconstruction(Дохиог сэргээн ашиглах)

2.4.2 Sampling

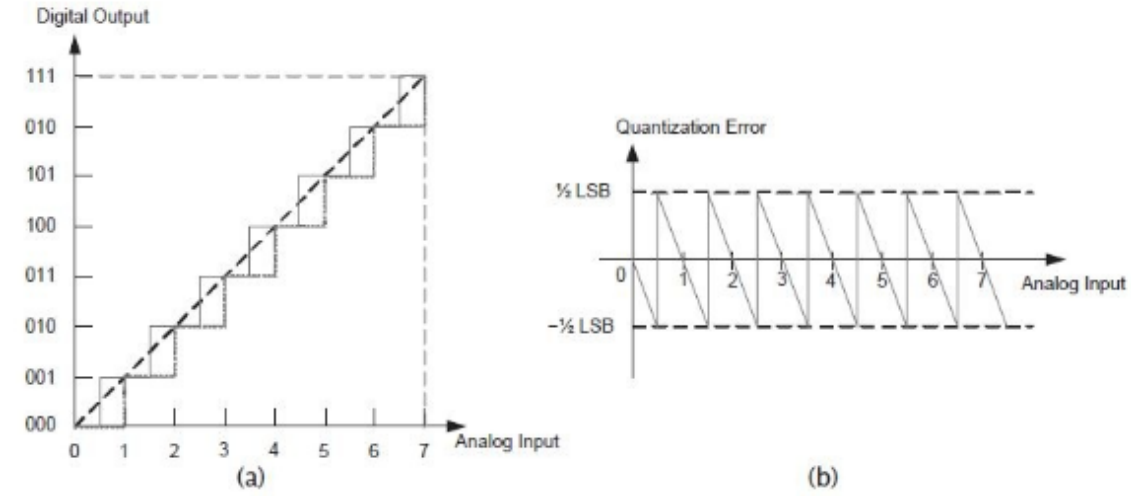
1. Sampling бол аналаг дохионоос дискрет хугацааны утгуудыг үүсгэх үйл явц юм.Нэн түрүүнд аналаг болон тоон дохионуудын давтамжын хамаарлын дурьдах хэрэгтэй.Аналог дохиог x(t)=Acos(wt+Totto) хэлбэртэй гэж үзье.t=nTs үетэй дохиог Ts хугацааны интервалд дээр сонгож аваах

2.4.3 Фурьегийн хувиргалт

1. Дискрет дохионы Фурье хувиргалт бол [0;fs/2] муж дахь давтамжинд тасралтгүй үргэлжилдэг.Тиймээс тооцооллоос харахад энэ хувиргалт ашиглахад тийм тохиромжтой биш.Проктикт дискрет Фурье хувиргалт (DFT) нь Фурье хувиргалтын оронд хэрэглэгддэг.DFT нь аналог муж дахь Фурьегийн цуваатай ижил юм.Фурье цуваа болон DFT-ийн систем тэгшитгэл нь дараах байдлаар илэрхийлэгдсэн

2.4.4 Тоон хэлбэрт шилжүүлэх

1. Аналаг тоон хувиргагчид хязгаарлагдмал тоотой битүүд (нарийвчлал) байдаг.Үүний улмаас дохионы далайцын утгыг ойролцоолсон дөхүүлж хөрвүүлдэг.Ингэж далайцын утгыг ойролцоолон дөхөх хувиргалтыг Quantization буюу тоон хэлбэрт шилжүүлэх хувиргалт гэнэ.



Зураг 2.4: Гурван битийн аналог тоон хувиргагч

а) Оролт/Гаралтын хувиргагчын функц б) Quantization noise

2.5 Өгөгдлийг шахах протоколууд

Ерөнхийдөө баталгаажуулалт хийх 3 төрлийн арга байдаг.

1. Өгөгдлийг шахах протоколууд Аналогийг тоон битийн цуваа руу хувиргах үндсэн

үүрэгтэй. Мөн шахах хэрэгцээгүй мэдээлэл дамжих боломжийг бууруулах(нэвтрүүлэх зурвас хэмнэх) зэрэг үүрэгтэй. Кодекийн хувьд давтамж хэмнэх,чанарыг нэмэгдүүлэхэд үнэ өртөгөснө. Үндсэндээ маш их хэмжээгээр шахна гэдэг нь их хэмжээний процесссорын хүчин чадлыг шаарддаг юм. Кодекийн үнэлгээ-Mean Opinion Score (MOS) Кодекийн олон төрөл байдаг ба тэдгээр нь ярианы тодорхой шинж чанарыг хангаж өгдөг. Дамжуулагдсан ярианы чанар нь сонсогчид хэр сонсогдож буйгаас болно. Ярианы кодекоос нь шалтгаалаад үндсэн үнэлгээ MOS-ийг өгдөг. Энэ үнэлгээ 1(муу)-ээс5(сайн) хүртэл оноо өгнө.

Шахалтын арга	Бит хурд([kbps)	MOS оноо	Шахах хугацаа
G.711 PCM	64	4.1	0.75
G.726 ADPCM	32	3.85	1
G.728LDACELP	16	3.61	3-5
G.729CS-ACELP	8	3.92	10
G.729*2 инкод	8	3.27	10
G.729*3	8	2.68	10
G.729a CS-ACELP	8	3.7	10
G.723.1MP-MLQ	6.3	3.9	30
G.723.1 ACELP	5.3	3.65	30

Зураг 2.5: Өгөгдөл шахах протоколууд

2. G.711 Энэ нь дууг кодлох олон улсын стандарт бөгөөд 64kbps –ийн PSTN сүлжээнд ашигладаг. Дууг Pulse coded Modulation (PCM)-ийн 8kHz –ийн 8bit-тэд ажиллахаар сонгож авсан. Онолын хувьд8 kHz дууг0 –ооc4kHz давтамжтай сигнал руу кодлох боломжтой. Гэвч PSTN сүлжээгээр нэвтрэхийн тулд 300Hz бага эсвэл 3400Hz-ээс их байх хэрэгтэй. Энэ стандарт дуу шахах үндсэн 2 алгоритмтай.

3. G.722 Уг протокол өргөн зурвас дижитал дууг шахах протокол бөгөөд дууны хэмжээг 4 дахин багасгаж чадна. 300Hz ээс 3400Hz-ийн уламжлалт телефон оронд 50Hz-ээс 7000Hz хүртэл аналог дууны сигналтай ажиллах чадвартай бөгөөд маш өндөр чанартай.

Бүлэг 3

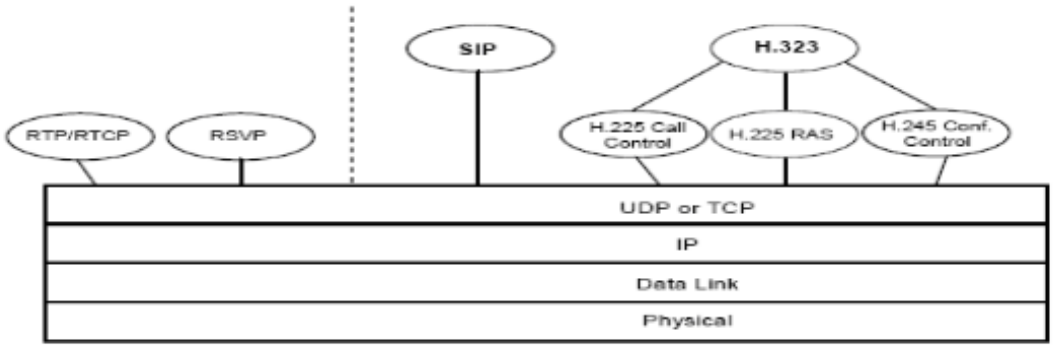
Судалгаа, шинжилгээний бүлэг

3.1 Voip

3.1.1 Ёрөнхий ойлголт

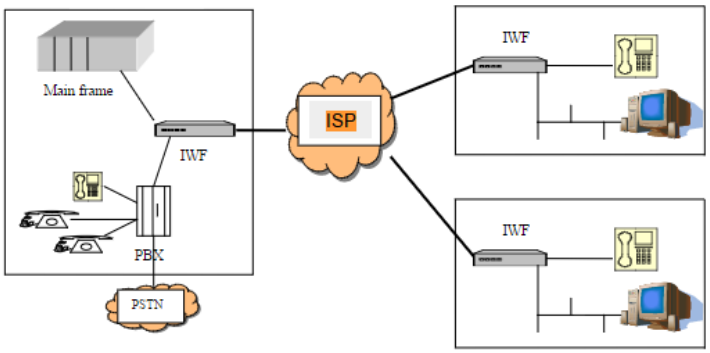
- VoIP нь уламжлалт холболтын технологийн оронд интернэтийг бүрдүүлэгч өгөгдлийн сүлжээнүүдээр телефон яриа, дүрс, өгөгдөл дамжуулах технологи юм. Энэ нь багц технологиуды агуулдаг бөгөөд Харилцаа холбооны компаниудаар дамжуулан сүлжээг ашиглаж ямар нь удирдлагагүйгээр тодорхой бус хэрэглэгчдийн хооронд холболт хийдэг.VoIP технологи нь ямар нэгэн холболт хийгдвэл дуу, дүрс болон өгөгдлийн цогц алгоритмаар шахаж тодорхой хэмжээний багцуудад хуваан холболт хийгдсэн хаягруу нь илгээдэг. Дамжуулалтын туршид зарим багцууд алдагдах болон алдаа гарах магадлал байдаг. Хэрвээ ийм тохиолдол гарвал тогтсон алдаа засах технологи ашиглан ашиглах боломжгүй болсон багц дахин дамжуулах хүсэлт тавьдаг. Энэ үеийн дамжуулалтын явцад бодит хугацаа гажуудал гарвал алдааг засах алгоритмаар алдагдсан хэсгийн дууг нөхдөг.Эдгээр үйлдлүүдийг стандарт протоколуудын тусламжтайгаар гүйцэтгэдэг. VoIP технологиH.323 болон Session Intitiation Protocol (SIP)гэсэн 2-н үндсэн протоколыг агуулдаг бөгөөд эдгээр нь бие тусдаа сүлжээ үүсгэж VoIP үйлчилгээг хангах чадвартай.

Өгөгдлийн тоон сүлжээ ба телефон сүлжээ хоѐр нь тус тусдаа хөгжиж ирсэн боловч IP телефон тэдгээрийг нэгтгэсэн. VoIP-ын өндөр багтаамжийн сүлжээний зохион байгуулалт нь сувган ба багц холболтын технологитой.



Зураг 3.1: VoIP технологийн протоколуудын бүтэц түүний элементүүд, ажиллагааны зарчим

3.1.2 Хэрэглээ



Зураг 3.2: Байгууллага болон салбаруудын хэрэглээ

- Эхний жишээ нь корпораци болон албан байгууллага удирдах газрын хооронд дуу, өгөгдлөөр хангах, салбаруудын хооронд мэдээлэл дамжуулах ингэснээр зардал төсөв хэмнэх сайн талтай ба сүлжээний бүтцийг авч үзье.Энэ нь өгөгдөлтэй шууд дууг ачаалах зөөх боломжийг олгох, стандарт өгөгдөл дамжуулалтыг хан-

гасан багц сүлжээг ашиглах боломжтой. Харилцан ажиллах функц(IWF) нь дуу багцлах, өгөгдлийг шахах, дамжуулах физик хэрэгсэл ба программ хангамжийн хэсгээс тогтоно. IWF интерфейс нь түлхүүр систем буюу телефонуудад шууд холбогдсон аналогиин терфейсын пультыг хангана. IWF нь албан газрын хувийн холбох станц(PBX) телефон терминалуудын функц, салбар байгуулгуудын PBX зэргийн компьютер программын функцыг гүйцэтгэнэ.

Voip уламжлалт утсанд байхгүй эсвэл байдаг боловч зөвхөн нэмэлт төлбөртэй олддог үйлчилгээ болон үзүүлэлтүүдийг агуулж байдаг. Мөн та өргөн зурвасын холболт болон уламжлалт утасны шугаманд хоёуланд нь сарын төлбөр хураамж төлөхөөс зайлсхийх бололцоотой. Холын зайн болон олон улсын дуудлага хийхэд мөн нэмэлт төлбөр төлөх хэрэггүй юм. Энэ нь packet switches технологийн нэг жишээ юм. Єрєєр хэлбэл IP phone буюу интернэт утас нь ийм технологи дээр суурилсан гэсэн vr юм. Cvvлийн veийн интернэт утас нь шахах алгоритм, хэт ачааллыг хянах функцуудтэйгаас гадна нууцлалын зэрэг нь маш єндєр тvвшинд хvрээд байна. Анх Унгарын Будапештийн политехникийн их сургуулийн компьютерийн сvлжээний судалгааны ажилтнууд 2003 оны 11 сард судалгаа хийж, IP phone нь шугам нь 1400bps хурдтай байхад боломжийн буюу яриа тасалдалгvйгээр дамжих боломжтой гэж тогтоожээ. Єнєєдрийн байдлаар энэ хурдыг 600bps гэж тодорхойлоод байна.

3.2 Шуурхай зурвас

3.2.1 Тойм

- Э-майл бол бидний мэдэх хамгийн хурдацтай харилцаа холбооны төрөл гэдгийг бид бүгд мэднэ. 10, 20-оод жилийн өмнө бол хүмүүс нээх их сонсож байгаагүй байх. Гэхдээ одоо бол бид утсаар мессеж бичиж дуудлага хийхээс илүүтэйгээр э-майл үйлчилгээг ашиглаж харилцаж байна. Өдөрт тербум гаруй э-майл хүмүүс хоорондоо дамжуулж байна. Гэхдээ зарим үед э-майл тийм ч хурдан байхгүй. Таны э-майл явуулсан хүн тэр үед тань онлайнд буюу интернэт сүлжээнд холбогдсон байх магадлал бага. Ийм л учраас шуурхай зурвас буюу Instant messaging - ийг хүмүүс ихээр хэрэглэх болсон юм. Шуурхай зурвас гэдэг нь нэгэн төрлийн онлайн чатын хэсэг бөгөөд интернэтээр өгөгдлийг ямар нэгэн хоцролтгүй хүргэж

буй дамжууллыг хэлнэ.Интернэтийг хүн бүр хэрэглэж эхэлхээс өмнө, хэдэн хүмүүс идэвхтэй интернэтийг хэрэглэж байсан. America Online(AOL), Prodigy болон CompuServe гэх мэт томоохон онлайн үйлчилгээний ажилчид онлайнаар хоорондоо харилцаж байсан билээ. Онлайн үйлчилгээ нь таньд өөрийн үйлчилгээний интерфэйсийг өгөхөөс гадна холбогдож буй хүнд мөн адил харагдахаар тодорхойлогдсон юм.

1990 оны өмнөхөн, хүмүүс ихээхэн цагийг интернэт өнгөрөөх болсон. Зарим нэгэн програм хангамж хөгжүүлэгчид вэб сервер дээр chat-room гэх програм хангамжийг байрлуулсан. Энэхүү чат өрөө нь, хэсэг бүлэг хүмүүс тэрхүү "өрөө"гэх тодотголтой зүйл дотор мессеж бичихэд тэрхүү мессеж нь бүх хүмүүст харагдаж байсан. Харин шуурхай зурвас нь хоёр хүний чат өрөөг хэлээд байгаа юм.

1996 оны 11-н сар интернэт сүлжээнд шуурхай зурвас нь маш их газар авсан билээ. Тэр үед Мирабилис буюу Mirabilis компани нь ICQ хэмээх үнэгүй хэрэглэх боломжтой шуурхай зурвасын мессенжерийн програмыг бүтээжээ. ICQ нь "I seek you"хэмээх үгний товчлол бөгөөд, компьютер дээр байрлах клиэнт програм юм. ICQ сервер мөн таны клиэнт ажилж буй үед та тэрхүү клиэнтийг ашиглаж бусадтай харилцаж чаддаг байсан юм. 1997 онд, AOL нь анхдагч онлайн холбоо болж хэрэглэгчдээ тэрхүү шуурхай зурвасын цонхыг ашиглаж хоорондоо чатлах боломжийг олгосон юм. 1998 оны 6 сард, AOL нь Mirabilis болон ICQ хувь дээрээ авсан. Одоо ашиглаж буй бүхий л шуурхай зурвасын програмуудын хэрэгслийг ICQ модел тавьсан юм.

- Хамгийн анхны онлайн чатны систем нь 1973 онд Иллинойсийн их сургуулийн ПЛАТО систем гэх газар Доуг Броун болон Дэйвид Ар. Вүүлэйя гэх хүмүүс Талкоматик хэмээх нэртэй үүсгэж байсан юм. Энэ нь хэд хэдэн сувгуудтай бөгөөд тус бүр нь 5 хүний багтаамжийг агуулж өөр хоорондоо чатлах боломжийг олгож байжээ. Талкоматик нь 1980 оны дунд ПЛАТО-гын хэрэглэгч дунд нэлээн алдартай болж байсан. 2014 онд Броун болон Вүүлэйя вэб дээр суурилсан Талкоматикийн хувилбарыг гаргасан.

  Харин хамгийн анхны онлайн системд чат хэмээх коммандыг ашигладаг системийг 1979 онд Dialcom - ийн Тоом Валкер болон Фрит Танэ нар үүсгэж байсан.

3.2.2 Хэрэглэгчийн бааз

- Шуурхай зурвасын бүтээгдэхүүн програм нь дотроо 2 хуваагддаг: Enterprise Instant Messaging (EIM) буюу Албан байгууллагын шуурхай зурвасын програм болон Consumer Insant Messaging (CIM) - Хэрэглэгчдийн эрх ашгын шуурхай зурвасын програм.Албан байгууллагын шийдэл нь дотоод IM серверээ ашигладаг хэдий ч, энэ нь зарим нэг жижигхэн оффис болон бас бус хязгаарлагдмал төсөвтэй албан байгууллагын хувьд тийм ч боломжтой хувилбар биш юм. Харин хоёр дахь сонголт нь хэрэгжүүлэхэд хямд хялбар бөгөөд жижигхэн хэмжээний хөрөнгө оруулалт серверийн програм хангамжид болон шинэ техник технолигид өгөөд бий болно.

  2010 оноос хойш хамгийн их хэрэглэж байгаа IM систем болон хамгийн их хэрэглэгчтэй үйлчилгээнууд:

  - Facebook (мөн Facebook Messenger, Instagram, WhatsApp)
  - Tencent Holdings Limited (WeChat, Tencent QQ, Qzone)
  - Google (Google+ болонYouTube хэрэглэгчид хамтдаа)
  - Microsoft (Skype болон Windows Live / MSN Messenger хамтдаа)
  - Twitter (API)
  - LinkedIn (API)

Шуурхай зурвасын клиэнт	Компани	Хэрэглээ
BlackBerry Messenger	BlackBerry	91 сая нийт хэрэглэгч (2014 он 10 сар)
AIM	AOL, Inc.	53 сая тогтмол хэрэглэгчид (2006 он 9 сар)
XMPP	XMPP Standards Foundation (XSF)	1200+ сая хэрэглэгчид (2011 он 9 сар)
eBuddy	eBuddy	35 сая хэрэглэгчид (2006 он 10 сар)
iMessage	Apple Inc.	140 сая хэрэглэгчид (2012 он 6 сар)
Windows Live Messenger	Microsoft Corporation	330 сая тогтмол хэрэглэгчид (2009 он 6 сар)
Yahoo! Messenger	Yahoo!, Inc.	22 сая хэрэглэгчид
QQ	Tencent Holdings Limited	840 сая тогтмол хэрэглэгчид
IBM Sametime	IBM Corp.	15 сая хэрэглэгчид
Skype	Microsoft Corporation	34 сая тогтмол хэрэглэгчид (2012 он 2 сар), 560 сая нийт хэрэглэгчид (2010 он 4 сар)
MXit	MXit Lifestyle (Pty) Ltd.	7,4 сая хэрэглэгчид
Xfire	Xfire, Inc.	24 сая бүртгүүлсэн хэрэглэгчид (2014 он 1 сар)
Gadu-Gadu	GG Network S.A.	6,5 сая тогтмол хэрэглэгчид
ICQ	ICQ LLC.	4 сая тогтмол хэрэглэгчид (2006 он 9 сар)
Paltalk	Paltalk.com	5,5 сая хэрэглэгчид (2013 он 8 сар)
IMVU	IMVU, inc.	1 сая хэрэглэгчид (2007 он 6 сар)

Зураг 3.3: Хэрэглэгчдийн тоон судалгаа

3.3 Messenger

End to end encryption -E2EE

- Энэ систем нь зөвхөн харилцагч талууд унших боломжтой байдаг.Зарчмын хувьд энэ нь сэм чагнахаас сэргийлэх мөн интернэт үйлчилгээ үзүүлэгч компани дундаас авсан ч тайлах тулд түлхүүр шаардагддаг.Систем нь хяналтын болон хөндлөнгийн 3 дагч этгээдийг ялах зорилготой учир нь ямар нэгэн 3 дагч этгээд харилцсан мэдээллийг хадгалж авсан байх боломжтой.

3.3.1 Түлхүүр солилцоо

- Түлхүүрийг зөвхөн харилцагч талууд мэдэж байх ёстой. Зорилгодоо хүрэхийн тулд E2EE систем урьдчилан зохиосон тэмдэгт мөрийг ашиглан ширфлэдэг,урьдчилан хуваалцсан нууц pre-shared secret (PGP) гэж нэрлэдэг эсвэл нэг удаагийн урьдчилан хуваалцсан нууц гаргаж авах гэдэгone-time secret derived from such a pre-shared secret(DUKPT).Тэд мөн Diffie-Hellman нууц түлхүүр солилцох хэлэлцээг ашигладаг Diffie-Hellman key exchange (OTR)

3.3.2 Хэрэглээ

- E2EE г PGP,GnuPG,Protonmail,Mailfence,S/MIME,inky оруулж өгсөн.2016 оны байдлаар ердийн серверийн дээр суурилсан харилцаа холбооны систем нь E2EE шифрлэлт аргыг оруулаагүй байна.Иймээс хэрэглэгч нар нь үйлчилгээг үзүүлж буй сервертээ л найдаж ашиглана гэсэн үг.Зарим төрийн бус E2EE систем жишээ нь Lavabit болон Hushmail , тэд байсан үед "E2EE"шифрлэлт санал болгох гэж өөрсдийгөө тодорхойлсон байдаг.

3.4 Протоколууд

- Протокол Протокол нь сүлжээний орчинд өгөгдлийг дамжуулах дүрэм, процедурыг тодорхойлдог бөгөөд маш олон янз ба өөр өөрийн функцтэй. Функцээсээ хамааран OSI загварын сүлжээний янз бүрийн төвшинд ажилладаг ба хэд хэдэн протокол хамтарч ажиллахаар зохион байгуулагдсан байдаг. Эдгээрийг протоко-

лын стек гэж нэрлэдэг. Илгээгчид протоколтой холбоотойгоор дараах үйлдлүүдийг хийдэг.

- Протоколыг боловсруулалт хийх боломжтой багцад хуваах.
- Хүлээн авагчид явуулахын тулд багцад хаягийн мэдээллийг нэмдэг
- Багцыг дамжуулахад бэлтгэнэ. Хүлээн авагчид түүний эсрэг үйлдлүүд хийгддэг.
- Сүлжээний кэбелиас өгөгдлийг хүлээн авах
- Сүлжээний адаптераас өгөгдлийг процессор луу дамжуулах
- Багцаас бүх нэмэлт мэдээллүүдийг салгаж, багцаас жинхэнэ өгөгдлийг буулган авч, өгөгдлийг анхны хэлбэрт оруулах
- Багцаас өгөгдлийг хуулан авч буферт хадгалах
- Тухайн хэрэглээний программд ашиглагдах форматаар өгөгдлийг програм руу дамжуулах Протоколыг боловсруулалт хийх боломжтой багцад хуваах.
- Хүлээн авагчид явуулахын тулд багцад хаягийн мэдээллийг нэмдэг
- Багцыг дамжуулахад бэлтгэнэ. Хүлээн авагчид түүний эсрэг үйлдлүүд хийгддэг.
- Сүлжээний кэбелиас өгөгдлийг хүлээн авах
- Сүлжээний адаптераас өгөгдлийг процессор уруу дамжуулах
- Багцаас бүх нэмэлт мэдээллүүдийг салгаж, багцаас жинхэнэ өгөгдлийг буулган авч, өгөгдлийг анхны хэлбэрт оруулах
- Багцаас өгөгдлийг хуулан авч буферт хадгалах
- Тухайн хэрэглээний программд ашиглагдах форматаар өгөгдлийг програмруу дамжуулах Дээрх үйлдлүүд дамжуулагч болон хүлээн авагчдад ижил аргаар гүйцэтгэгдэх èстой.

3.4.1 Протоколуудын стек

OSI загварын төвшин бүрд дараах дүрмийн дагуу протоколууд харгалздаг.

- Хэрэглээний төвшинд анхны төлөвийг тогтоох, хүсэлтийг хүлээн авах
- Үзүүлэмжийн төвшинд багцат форматлах, шифрлэх, мэдээллийг нэмэх
- Сеансын төвшинд маршрутын талаарх мэдээллийг нэмэх
- Тээврийн төвшинд алдаа боловсруулах мэдээлэл нэмэх
- Сүлжээний төвшинд хаягийн болон багцын дарааллын талаарх мэдээлэл нэмэх
- Сувгийн төвшинд алдаа шалгах мэдээлэл нэмэх, өгөглдлийг дамжуулахад бэлтгэх
- Физик төвшинд багцыг битийн дараалал мэтээр дамжуулах OSI загварын төвшиний адил стекийн доод төвшин тохиромжтой ажиллах дүрмийг заадаг бол дээд төвшинд сеансын гүйцэтгэх программыг хөрвүүлэх дүрмийг заадаг. Протоколын төвшинд дээшлэх тусам улам нарийн нийлмэл болно

3.4.2 TCP/IP протокол

- TCP/IP (Transmission Control Protocol/Internet Protocol) нь Интернетийн протокол юм. 1969 онд Defense Advanced Research Projects Agence (DARPA) ийн гаргасан ARPANET нэртэй сүлжээг одоогийн Интернетийн буюу дэлхийн хамгийн том компьютерийн сүлжээний эхлэл болсон гэж үздэг.TCP/IP протокол нь анх 1983 онд Military standarts (MILSTD)-аар батлагдсан бөгөөд эхэн үедээ батлан хамгаалах албадад ашиглагдаж байсан. Энэхүү протокол стандарт болсноор Интернэт өргөн тархах нөхцөл бүрэлджээ.
- TCP/IP протокол өргөн тархах болсон нөхцөл нь: Энэхүү протокол ньүнэгүй бөгөөд компьютерийн техник хангамж болон компьютерийн үйлдлийн системээс хамааралгүй ажилладаг.
- Ямар нэгэн физик сүлжээний техникээс хараат бус ажилладаг бөгөөд энэ нь олон төрлийн компьютерийн сүлжээг нэгтгэх боломж олгодог. TCP/IP нь Ethernet, Token ring,Dial up line, болонX25 net-д ажиллах чадвартай.

- Хэрэв сүлжээ Интернэт шиг том хэмжээтэй бол сүлжээнд буй төхөөрөмжүүдийг хаяглах боломжтой.

- Стандарчлагдсан хэрэглэгчдийн хэрэглээнд өргөн тархсан дээд түвшний протокол зэрэг юм.

  TCP/IP протокол нь ISO/OSI загварын Transport болон Network layer-уудын түвшинд функцнь гүйцэтгэгдэнэ.

3.4.3 UDP-User Datagram protocol

- Энэ төрлийн протокол нь ойрын зайнд, дотоод сүлжээнд холбогдсон компьютеруудын хооронд өгөгдөл дамжуулахад ашиглагддаг ба найдваргүй дамжуулалтад тооцогддог. Учир нь богино зайд дамжуулагдсан мэдээллийг дамжигдсан эсэхийг шалгах шаардлагагүй байдаг. UDP-нь өөрөө IP, ICMP, IGMP протоколууд дээр суурилсан байдаг. Өөрөөр хэлбэл UDP протоколоор дамжигдах өгөгдлүүд нь дээрх гурван протоколын ядаж нэгээр нь дамжигдан хүрэх газраа хүрнэ гэсэн үг. Харин энэ гурав нь компьютерийн физик хаяг MAC хаягийг ашиглан өгөгдөл дамжуулдаг ARP болон RARP протокол дээр үндэслэгдсэн байдаг. Эндээс харахад UDP протокол нь MAC хаягийн түвшинээс эхлээд IV түвшинд оршидог. UDP протоколыг ашиглан хийгддэг өөр нэг зүйл нь DNS буюу Domain Name Server юм. Энэ сервер нь сүлжээнд холбогдох логик хаягийг бодит хаяг болгон хувиргах хэрэгсэл юм. Энэ нь бидэнд ямар нэг байдлаар сүлжээнд холбогдох, интернетэд холбогдоход хэрэглэгддэг. Мөн энэ протокол нь TELNET, FTP, SNMP протоколын суурь болж өгдөг байна.

- UDP- н бүтэц Эхний 16 bit нь илгээгчийн портын дугаар, дараагийн 16bit нь хүлээн авагчын аль портоор пакетийг задлан дээш дамжуулахыг заадаг. Дараагийн 16bit нь уртын хэмжээ байдаг ба эндээс өгөгдлийн тухай бүрхүүл түвшинд мэдээлэл авч болдог. Үүний дараагийн 16bit нь өгөгдөл хүлээн авсан компьютер өгөгдлөө бүрэн гүйцэд олж авсан эсэхийг заадаг. Энэ хэсэгдэх өгөгдөл нь IP header, UDP header, Data өгөгдлүүдээс тооцоолон гаргасан өгөгдөл байдаг. Жишээ нь энэ талбарын мэдээллийн тусламжтай өгөгдлөө бүгдийг авсан, эсвэл дараагийн frame болон хуваагдсан datagram-г хүлээх эсэхийг шийдвэрлэхэд хэрэглэгдэнэ. Үлдсэн хэсэгт дамжуулагдах өгөгдлүүд байрладаг. UDP протокол нь 17-р портыг ашигла-

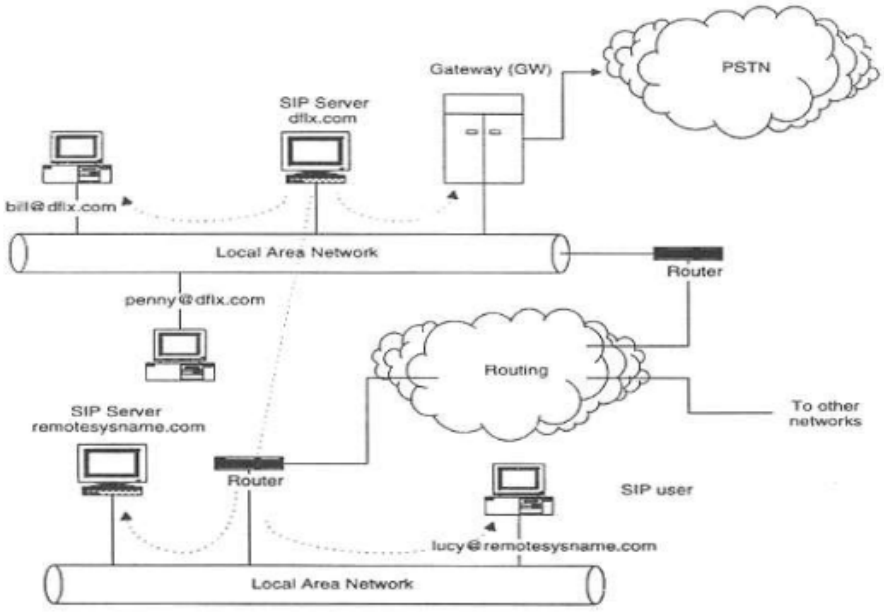
даг. Наймтын тооллын системээр 21 юм. Жишээнь: FTP 21, TELNET 23, TCP/IP 80-р портоор өгөгдлөө дамжуулдаг.

3.4.4 Session Intitiation Protocol (SIP)

- SIP нь хэрэглэгчийн түвшиний(application layer) протокол бөгөөд дурын нэг болон хэд хэдэн хэрэглэгчдийн хооронд Мултимедиа харилцаа холбоо үүсгэх, өөрчлөх, устгах үйлдлүүдийг хийдэг. Энэ протокол нь VoIP технологийн үндсэн гол 3-н протоколын нэг юм. SIP нь мэдээлэл дамжуулахдаа TCP болон UDP аль алинг нь ашиглах боломжтой боловч ихэнхдээ UDP-г ашигладаг. H.323 протоколыг бодвол илүү энгийн тусгай удирдлагын протоколууд байхгүй, өгөгдөл шахах дамжуулах нь H.323 –тай ижил протоколууд ашигладаг. Энэ нь ерөнхийдөө интернетэд ашиглахад зориулсан бөгөөд архитектур HTTP-той ижил.

Зураг 3.4: SIP протоколын стек

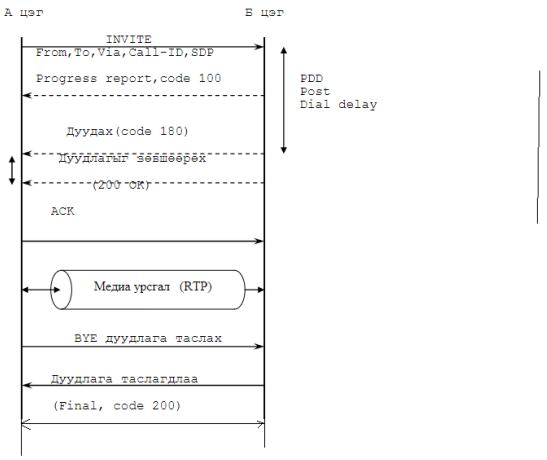
SIP протоколын стек SIP систем нэг болон хэд хэдэн сервэрүүдээс бүрдэж болох бөгөөд дурын сүлжээний хэсэг, интернэт, дотоод сүлжээ болон IP дэмждэг бүхийл сүлжээнд ашиглаж болно. Өөр төрлийн хэрэглэгчтэй холбогдох бол gateway ашиглана. SIP сүлжээнь үндсэн 2 бүрэлдэхүүн хэсгээс бүрддэг. 1.User agent 2.Network server 1. User agent нь SIP сүлжээ бүрт агуулагдах бөгөөд 2 төрлөөс бүрдэнэ. a)User Agent Client (UAC) хүсэлт гаргах үүрэгтэй. Өөрөөр хэлбэл Дуудлага хийгч терми-



Зураг 3.5: 2 SIP server-тэй сүлжээ

нал. b)User Agent Server (UAS) ямар нэгэн хүсэлтэд хариу өгөх үүрэгтэй. (Хүлээнавагч) Энэ нь H.323 сүлжээний терминалуудтай ижил үүрэгтэй буюу хэрэглэгчид юм. 2. Network server ямар нэгэн дуудлага хийх үйлажиллагаа хангах зорилгоор ашигладаг бөгөөд гол удирдах болон бүртгэх хэсэг юм. 3-н төрлийн SIP server байдаг. a)Redirect Servers: Энэ дуудлага хийхэд дуудах төхөөрөмжийн хаягийг тодорхойлдог. Энэ мэдээлэл нь дуудаж байгаа төхөөрөмж рүү буцаадаг. b)Proxy Servers: Энэ нь хэрэглэгчийн түвшний SIP хүсэлт болон хариултыг дамжуулах үйлажиллагагаар хангаж өгдөг. Энэ сервэр нь хүсэлт ирэхэд дуудлага хүлээн авах төхөөрөмжийн мэдээллийг агуулж байгаа сервер лүү илгээдэг. c)Registrar Servers: SIP болон төхөөрөмжийн хаягийг бүртгэхэд ашигладаг. Сервернь H.323 сүлжээний gatekeeper-тэй ижил үүргийг гүйцэтгэнэ. Харилцаа холбоог үүсгэхийн тулд тодорхой method-уудыг ашиглана.SIP нь 6 method-ийг ашигладаг. Эдгээрнь INVITE, ACK, OPTIONS, BYE, CANCEL болон REGISTER юм. INVITE Энэ нь дуудлагын процессийн циклрүү дуудлага хийх эхний мэссэжийг илгээдэг. Үүнд SIP толгой буюу дуудлага хийгч, Call-ID, дуудлага хүлээн авагч, дуудлагын дарааллын дугаар болон бусад мэдээллийг агуулагддаг. Үндсэндээ энэ нь дуудлага хийхийг тогтоодог. Мөн INVITE мэссэж ихэвчлэн дуудлагын параметр, медиа төрөл дамжуулалтын хаягийг агуулна.Хэрвээ холболт хүлээн зөвшөөрвөл(200) код

буцаан илгээдэг.ACK Энэ нь зөвхөн INVITE хүсэлтийн хариунд илгээх хүлээн авагчийн мэссэж юм. ACK нь холболт амжилттай болвол INVITE хүсэлтийн хариунд амжилттай болсонг баталгаажуулсан мэссэж(200) илгээдэг. ACK мессэж их биеэнд медиа төрлийн тайлбар SDP агуулдаг. OPTIONS Энэ мэссэж нь дуудлага гүйцэтгэгч зарим төрлийн мэдээллээс лавлах шаардлага гарвал илгээдэг. BYE Хэрэглэгч холболтыг таслах бол энэ мэссэжийг илгээдэг. Хэрвээ энэ мэссэж ирвэл медиа урсгалыг зогсоодог. CANCEL Энэ ямар нэгэн хүсэлтийг хүчингүй болгодог бөгөөд хүсэлт ирээгүй тохиолдол үйлдэл хийхгүй. REGISTER Клиент энэ method-ийг ашиглах бөгөөд дуудлага хүлээн авахын тулд сонсох хаягаа SIP серверд бүртгүүлдэг. Магадгүй хэрэглэгч бүртгүүлэх бол өөрийн хаягаа сервэр лүү илгээдэг.



Зураг 3.6: SIP протокол холболт үүсгэх,устгах

Session Initiation Protocol (SIP) нь 3GPP – ээс хөгжүүлсэн яриа, видео дуудлага, IM (Instant Messaging) гэх мэт мультимедиа session – үүдийг удирдах, эхлүүлэх үүрэг бүхий сигналин протокол юм. IETF – ээс H.323 – тай харьцуулахад илүү сайн стандарт гаргахын тулд хөгжүүлсэн гэж хэлж болно. H.323 нь интернет дээр суурилсан энэхүү маш хурдацтай өсч буй хэрэглээг хангахад тийм ч хангалттай байж чадахгүй. SIP нь Hypertext Transfer Protocol (HTTP) дээр суурилсан бөгөөд PSTN зэрэг уламжлалт сүлжээтэй холбогдох учраас IP дээр суурилсан холбооны системүүд дээр мөн ашиглагдах боломжтой зохион байгуулагдсан. SIP нь VOIP

– д PSTN – тэй адил хэмжээний чанар баталгаа бүхий үйлчилгээний боломжийг нээж өгсөн. SIP нь зөвхөн сигналингийн удирдаж боловсруулдаг бол яриа болон видео дамжуулах үүргийг Real-time Transport Protocol (RTP) гүйцэтгэдэг.Мөн SIP нь RTP – ийн packet stream – ийн нэг хэсэг нь гэж ойлгож болох юм. Тиймээс SIP – ийг Мультимедиа session – ны нэг хэсэг протокол нь гэж ойлгож болно. SIP – ийн үндсэн давуу тал нь уламжлалт цахилгаан холбооны сүлжээ болон IP сүлжээг зэрэг дэмждэгт оршино. Энэхүү протоколыг ашигласанаараа үйлчилгээ үзүүлэгч нь уламжлалт холбооны сүлжээ болон IP сүлжээтэй холбогдон үйлчилгээгээ үзүүлэх боломжтой болно гэсэн үг. SIP протокол нь уян хатан, хэрэглэх болон хэрэгжүүлэхэд хялбар өмнөх хувилбаруудтайгаа харьцуулахад дуудлага тохируулах хугацаа бага шаарддаг байх юм. SIP нь нэгэнт эхлэсэн ярианы session – ыг яриан дундуур өөрчлөх боломжтой байдаг учраас яриан дундуур өөр хэрэглэгч нэмж оруулах видёо дуудлага эхлүүлэх зэрэг нь ямар ч үед боломжтой байдаг. SIP нь цаашдын холбооны ертөнцөд маш ихээр хэрэглэгдэх нь тодорхой болж байгаа бөгөөд өнөөдрийн байдлаар гэхэд 3G гар утаснуудын хувьд дуудлага гүйцэтгэх стандарт протокол болж байна. Энэ нь цаашдаа IP voice дуудлагууд бүгд энэхүү протоколоор гүйцэтгэгдэнэ гэсэн үг юм.

3.4.5 H.323

- H.323 протокол нь Олон Улсын Холбооны Зөвлөлөөс ITU 1996 онд баталсан IP буюу интернэт бүхий багц холболттой сүлжээгээр телефон яриа, видео хурал, өгөгдөл дамжих стандарт юм. H.323 нь ITU-ээс баталсан нилээд олон хэсгүүдээс бүрдэх мультимедиа холболтын H.32x протоколуудын нэг хэсэг бөгөөд хоѐр болон түүнээс дээш тооны терминалуудын хооронд мөн сүлжээний төхөөрөмжүүдийн хооронд харилцан тогтсон мультимедиа холболтын стандарт болно. H.323 топологийн үндсэн сүлжээний элементүүд нь терминалууд, Gatekeeper (GK), MCU гарцуудаас тогтдог. MCU нь gatekeeper-ын нэг хэсэг юм. H.323 стандарт нь хэрэглэгчийн бүртгэлийн процедурыг тодорхойлж өгөх ба терминаль нь нэг юмуу олон хэрэглэгчдэд зориулсан дохиоллын төгсгөлийн цэгийг холбож өгнө. H.323 дуудлагын модель нь хоѐр терминалын хооронд, терминаль ба gatekeeper, терминаль ба гарцуудын хооронд

  гүйцэтгэдэг.Gatekeeper нь H.323 орчны гол цөм хэсэг юм. H.323 орчим нь бүх

Протокол	Протоколыг ашиглах сүлжээний төрөл
H.320	ISDN
H.321 and H.310	ATM
H.322	LAN's that provide a guaranteed QoS
H.323	LAN's and Internet
H.324	PSTN/Wireless

Зураг 3.7: Audio/Video/Data Харилцааны стандарт протоколууд

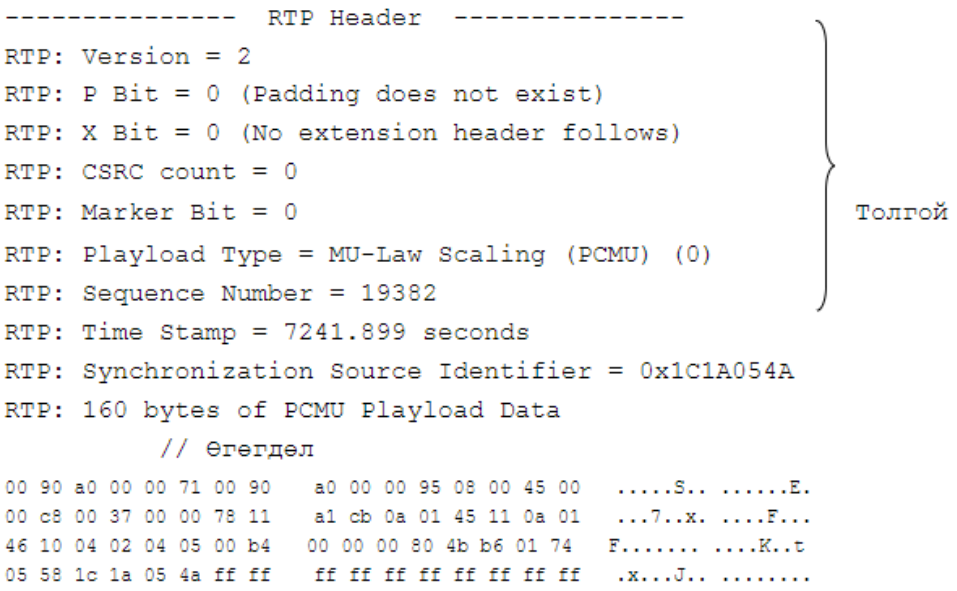
терминаль гарцууд болон нэг gatekeeper-ээр удирдагдаж байгаа мультикаст хяналтын удирдлагыг багтаадаг. Нэг орчны хувьд(zone) ганц gatekeeper байдаг. Орчин(zone) гэдэг нь төхөөрөмжүүдийн логик холболт замчлал ба холбогчуудтай холбогдсон топологуудын алслагдсан топологи байж болох элементүүдийг агуулна. Gatekeeper нь хөрвүүлэгчийн хаягийг зааж өгөх төхөөрөмжөөс ирэх хүсэлтийн холболтонд зориулсан зурвасын өргөнийг хангадаг. H.323-ндамжуулалт нь RTP буюу бодит дамжууллын протоколоор тодорхойлогддог. RAS-ийн хувьд UDP ээр ажиллахын тулд H.245, дуудлага дохиоллын хувьд TCP-г шаарддаг. H.225.0 нь дуудлага дохиоллын протокол бөгөөд бүртгэл, төлөв хяналтын хэсэгт, H.245 холболтын тодорхойломж, хяналт төхөөрөмжийн багтаамж логик сувгийн ерөнхий хяналт зэргийг тодорхойлдог.

- H.323 стандартын дуудлагын үндсэн загвар H.323 стандартын дуудлагын холболт тогтолт нь шууд чиглэсэн H.245 протоколоор хийгдэнэ.Gatekeeper нь замчлалыг тодорхойлоно. Шууд арга нь цэгээс цэг зарчимаар холболт тогтооход GK замчлал нь олон цэгийн телекомпрессид зориулагдана.H.323 –ын дуудлага нь таван үе шатаас тогтоно. Үүнд: 1.A шат - Дуудлага тогтоох 2.B шат – Төгсгөлийн цэгүүд ба сүлжээний станцуудын хооронд анхдагч холбоог тогтоох 3.C шат–Төгсгөлийн цэгүүдийн хооронд дуу дүрсийн холбоог тогтоох 4.D шат – Дуудлагат үйлчилгээнүүдэд хүсэлт өгөх дохио 5.E шат – Төгсгөл өгөх

3.4.6 RTP and RTCP (Real-time Transport Protocol ба Real-time Control Protocol

- RTP protocol нь сүлжээгээр media (дууболондүрс) -ийн багцыг дамжуулна.Эдгээр SIP болон H.323-ийн тусламжтайгаар хийгдэнэ. Энэ протокол нь хүлээн авагчид ирэх багцуудын ямар нэгэн алдагдлыг илрүүлэн, хэрвээ алдаа гарвал түүнийг засаж мөн хугацааны мэдээллээр хангаж өгнө. Энэ протоколын багц нь толгой

болон өгөгдөл гэсэн 2 хэсгээс бүрдэнэ. Толгойн хэсэг нь хүлээн авагч өгөгдлийг тайлах болон бусад нэмэлт мэдээллийг агуулна. Жишээ нь



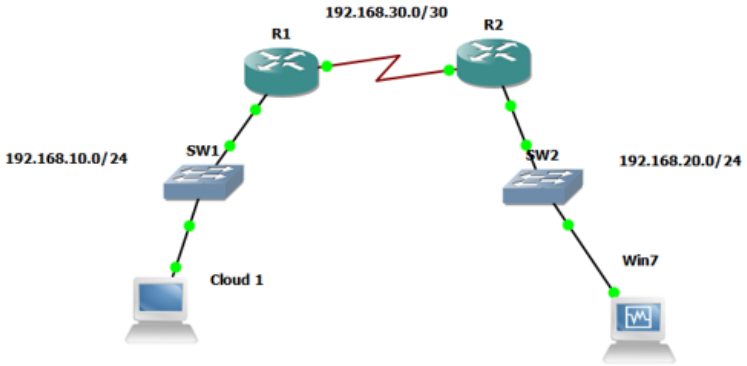
Зураг 3.8: VOip RTP багц

3.5 Төслийн ажил

Төслийн ажлаар VoIP server үүсгэж холболт үүсгэн packet барьж аван задлав

3.5.1 Ажиллагаа 1

- Өөрийн үндсэн Windows болон VirtualBoX win7 –г холбов
- Cloud 1 бол server гэж явах ба Win 7 person буюу хэрэглэгч маягаар сонгосон юм.
- Cisco iP Communicator үндсэн Winsows болон хэрэглэгч VirtualBox win7 дээр суулгаж асаах.
- Харилцах үед Cisco IP Communicator SoftPhone программыг татаж суулгасан . Өөр олон Softphone програм ашиглан улс хооронд холболт үүсгэн Voip үүсгэж болох ч амьдардаг бүсээсээ хамааран Voip Provider компанид бүртгүүлж эрх авах хэрэгтэй. Учир нь X-Lite ,Zoiper гэх free програмууд ашиглаж болох байсан ч

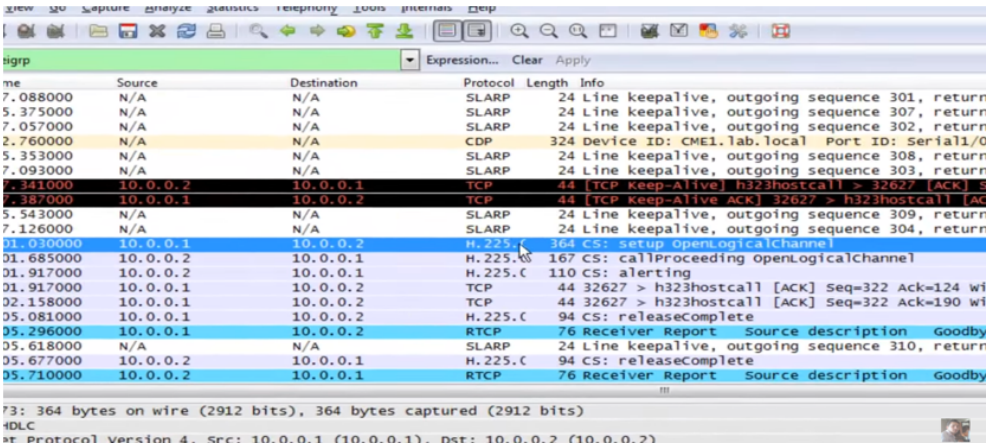


Зураг 3.9: GNS3 дээр server үүсгэн VirtualBox win7 холбов

төлбөртэй юм

- Whireshark аар packet барьж авав

Зураг 3.10: GNS3 дээр server үүсгэн VirtualBox win7 холбов



Зураг 3.11: GNS3 дээр server үүсгэн VirtualBox win7 холбов