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 **iv**

Товчилсон үгсийн жагсаалт **v**

1 Ерөнхий агуулга **1**

1.1 Удиртгал . . . 1

1.2 Зорилго . . . 1

1.3 Зорилт . . . 2

2 Онол, арга зүйн бүлэг **3**

2.1 Дуу авиа гэж юу вэ? . . . 3

2.2 VoIP . . . 3

2.2.1 VoIP гэж юу вэ? . . . 3

2.2.2 VoIP технологийн давуу тал болон сул талууд . . . 4

2.2.3 Quality of Service . . . 4

2.3 VoIP Протоколууд . . . 5

2.3.1 RTP and RTCP (Real-time Transport Protocol ба Real-time Control Protocol . . . 5

2.3.2 H.323 . . . 6

2.3.3 G.729 codec . . . 7

2.3.4 TCP/IP протокол . . . 7

2.3.5 UDP-User Datagram protocol . . . 8

2.3.6 Өгөгдлийг шахах протоколууд . . . 9

2.3.7 Session Intitiation Protocol (SIP) . . . 10

2.4 VoIP шифрлэлт . . . 13

2.4.1 SIPS . . . 13

2.4.2 SRTP 14
2.4.3 SSL/TLS 14

3 Судалгаа, шинжилгээний бүлэг **15**
3.1 CISCO ip communicator 15
3.1.1 Ажиллагаа 1 15
3.1.2 Ажиллагаа 2 17
3.2 Zioper 18
3.2.1 Asterisk 18
3.2.2 Asterisk протоколууд 18
3.2.3 Asterisk ба Zoiper 18

Зургийн жагсаалт

2.1 VOip RTP багц 5
2.2 Audio/Video/Data Харилцааны стандарт протоколууд 6
2.3 Өгөгдөл шахах протоколууд 9
2.4 SIP протоколын стек 10
2.5 2 SIP server-тэй сүлжээ 11
2.6 SIP протокол холболт үүсгэх,устгах 12

3.1 GNS3 дээр server үүсгэн VirtualBox win7 холбов 15
3.2 GNS3 дээр server үүсгэн VirtualBox win7 холбов 16
3.3 GNS3 дээр server үүсгэн VirtualBox win7 холбов 17
3.4 GNS3 дээр server үүсгэн VirtualBox win7 холбов 17

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.

1.3 Зорилт

- VoIP гэж юу болох тухай мэдэх
  - VoIP технологийн ажиллагаа
  - VoIP технологитой ижил төстэй программуудын судалгаа
  - VoIP технологийг ашиглаж өгөгдлийг нууцлалтай болгох код бичих

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 VoIP

2.2.1 VoIP гэж юу вэ?

- 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 технологи юм.

  VoIP сүлжээг дотор нь:

- Суурин VoIP
- Нүүдлийн VoIP
- Хөдөлгөөнт VoIP гэж ангилна.

2.2.2 VoIP технологийн давуу тал болон сул талууд

- VoIP технологи нь суваг ашиглалт сайн.Үүрэн телефоны операторуудыг бодвол үнэ өртөг хямд, хэрэглэгч ашиглахад хялбар гээд олон давуу тал бий. Мөн энэхүү технологийг ашиглаж олон хүмүүстэй нэгэн зэрэг харилцаа тогтоох боломжтой юм.

  Харин сул тал нь VoIP технологи нь PSTN шугам шиг найдвартай нууцлалыг хангаж чаддаггүй ч жил ирэх тусам илүү чанаржиж илүү ихээр үйлчлүүлэгчдээ тэлсээр байна.

2.2.3 Quality of Service

- IP технологийг ашиглаж сүлжээгээр мэдээлэл дамжуулах үед 3 төрлийн муугаар нөлөөлөх хүчин зүйлс бий.

Packet Loss

- IP сүлжээгээр VoIP багц дамжуулах нь найдвартай биш. Багц алдагдал нь сүлжээний ачаалал болон бусад хүчин зүйлээс болж өгөгдөл дундаасаа алга болохыг хэлнэ.Хэрэв багц алдагдал үүсэн багцыг дахин дамжуулвал хугацааны гажуудал үүсч болно. Өөрөөр хэлбэл дуу авиа хоцорч ирнэ гэсэн үг. Харилцааны үед өгөгдөл холболт хийгдсэн шугамаар дамждаг. VoIP технологид ачааллыг зохицуулах механизм зайлшгүй байх шаардлагатай.

Packet latency

- Багцын хоцрогдол бол 2 дахь хүчин зүйл.Мэдээллийг агуулсан сигналын багц алдагдах буюу сэргээгдэхгүй байхыг хэлнэ. Интернэт нь холболтгүй сүлжээ учраас дууны дохио бүрийг өөрсдийн сүлжээний аль замаар дамжих илэрхийлсэн хувийн багц тус тусд нь хувиарлаж өгдөг. VoIP технологи нь бага хоцрогдолтой байдаг ба шугамын хоцролт нь 150 м/сек байна.

Jitter

- Jitter бол хэлбэлзлийн хоцролт. VoIP сүлжээ хэлбэлзлийн хоцролт бас багатай байдаг.Дууны өгөгдөл нь ердийн өгөгдөлтэй харьцуулбал бодит хугацааны тасралтгүй их хэмжээний урсгал үүсгэж байдгаараа онцлогтой. Энэ үед багцуудын зарим нь хоцорж ирэх мөн заасан хугацаанаас хүлээгдэх үед тэр багцыг орхих болдог. Үүнээс болж гажуудал үүсдэг. ITU гаас гаргасан хэлбэлзлийн хамгийн их утга нь 100 м/сек.

2.3 VoIP Протоколууд

2.3.1 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

```
---------------  RTP Header  ---------------
RTP: Version = 2
RTP: P Bit = 0 (Padding does not exist)
RTP: X Bit = 0 (No extension header follows)
RTP: CSRC count = 0
RTP: Marker Bit = 0                                    Толгой
RTP: Playload Type = MU-Law Scaling (PCMU) (0)
RTP: Sequence Number = 19382
RTP: Time Stamp = 7241.899 seconds
RTP: Synchronization Source Identifier = 0x1C1A054A
RTP: 160 bytes of PCMU Playload Data
          // Өгөгдөл
00 90 a0 00 00 71 00 90   a0 00 00 95 08 00 45 00   .....S.. ......E.
00 c8 00 37 00 00 78 11   a1 cb 0a 01 45 11 0a 01   ...7..x. ....F...
46 10 04 02 04 05 00 b4   00 00 00 80 4b b6 01 74   F....... ....K..t
05 58 1c 1a 05 4a ff ff   ff ff ff ff ff ff ff ff   .x...J.. ........
```

Зураг 2.1: VOip RTP багц

2.3.2 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

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 2.2: Audio/Video/Data Харилцааны стандарт протоколууд

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

2.3.3 G.729 codec

- G.729 нь 1995 оны 11 сард ITU гаас баталсан. VoIP хуралдаан 1997 оны 3 сард хуралдаж G.729 - G.723.1 гэсэн дууны кодекийн техникийн тодорхойлолтыг гаргасан. Intel болон Microsoft -н үйлдвэрлэл нь дууны өндөр чанарыг гаргах хамгийн ашигтай зурвас бол G.729.1 6.3 kbps , G.729 7.9 kbps болохыг тодорхойлсон.Дууны кодекийг ашиглах явдал нь цэгээс цэгт IP холболттой интернэт урсгалын дууны чанар ба найдвартай ажиллагааг сайжруулахад чухал алхам болсон. Ийм чанартай PSTN сүлжээнд хүрхийн тулд стандартууд баталгаат интернэт холболтыг шаардана.

2.3.4 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.

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

2.3.6 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 2.3: Өгөгдөл шахах протоколууд

2. G.711 Энэ нь дууг кодлох олон улсын стандарт бөгөөд 64kbps –ийн PSTN сүл-

жээнд 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.

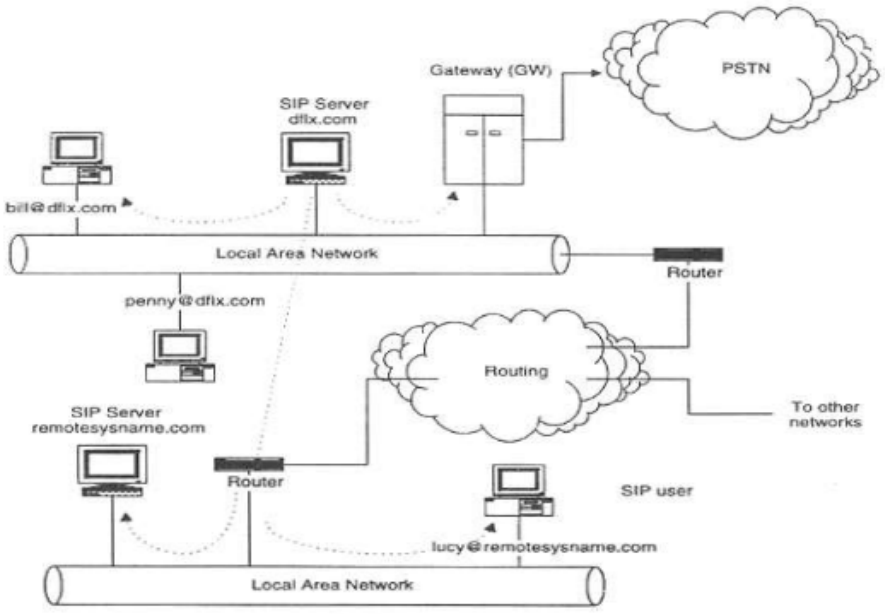
3. G.722 Уг протокол өргөн зурвас дижитал дууг шахах протокол бөгөөд дууны хэмжээг 4 дахин багасгаж чадна. 300Hz ээс 3400Hz-ийн уламжлалт телефон оронд 50Hz-ээс 7000Hz хүртэл аналог дууны сигналтай ажиллах чадвартай бөгөөд маш өндөр чанартай.

2.3.7 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 2.4: SIP протоколын стек

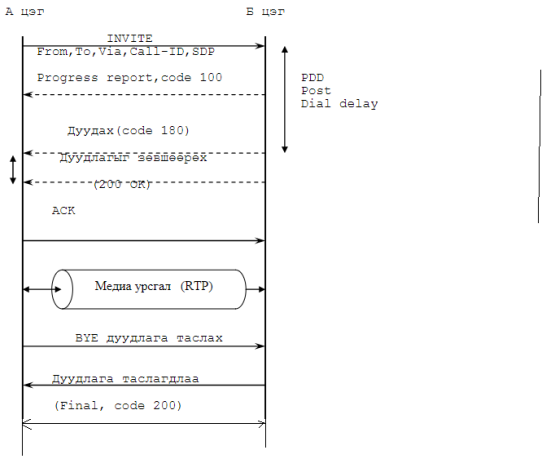
SIP протоколын стек SIP систем нэг болон хэд хэдэн сервэрүүдээс бүрдэж болох бөгөөд дурын сүлжээний хэсэг, интернэт, дотоод сүлжээ болон IP дэмждэг бүхийл сүлжээнд ашиглаж болно. Өөр төрлийн хэрэглэгчтэй холбогдох бол gateway ашиглана. SIP сүлжээнь үндсэн 2 бүрэлдэхүүн хэсгээс бүрддэг. 1.User agent 2.Network



Зураг 2.5: 2 SIP server-тэй сүлжээ

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 терминал. 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 2.6: 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.

2.4 VoIP шифрлэлт

2.4.1 SIPS

- Session initation control security нь SIP дээр TLS(Transport layer Security) хэрэгжүүлнэ.Ингэснээр өгөгдлийг нууцлаж аюулгүй байдлыг хангах боломжтой. SIP,RTP протоколууд өгөгдлийг нууцалдаггүй. SIP security нь өгөгдлийн бүрэн бүтэн байдал,баталгаажуулалт, нууцлалыг хангадаг. Ёрөнхийдөө SRTP, SIPS про-

токолууд ижил чиг үүрэгтэй боловч өгөгдлийг нууцлах механизм нь өөр юм. SIP протокол нь 5060 гэсэн портыг ашигладаг бол SIPS нь 5061 портыг ашишладаг.

2.4.2 SRTP

- Secure Real-time Transport Protocol нь сүлжээний интерфейсын хувьд заагдсан чиглэлд багц ярианы өгөгдлийг тодорхой багц үүсгэх дамжуулах үүрэгтэй.Энэ нь UDP порт протоколын дээд түвшинд ажиллах RTP юм. RTP протокол нь сүлжээгээр media багцыг дамжуулна. H.323 -н тусламжтайгаар хийгднэ. Харин SRTP протокол нь өгөгдлийг ширфлэж , баталгаажуулж ба өгөгдлийн бүрэн бүтэн байдлыг хангадаг. Өгөгдлийг нууцлахдаа AES алгоритмийг ашигладаг.Энэ нь RTP protocol-г нууцлалтай болгож сүлжээгээр дуу дүрсийн багцын дамжуулдаг.

2.4.3 SSL/TLS

- Secure socket layer сокетын хамгаалалт гэсэн утгатай. Мөн Transport layer security нь ижил үүрэгтэй бөгөөд 2 өөр компаниас гарч ирсэн юм. SSL гэдэг нь бидний өдөр тутам ашиглаж, илгээж буй өгөгдлийг дундаас нь гэмт этгээдэд алдхаас сэргийлэх зорилгоор ашиглагддаг.SSl нь хэрэглэгчээс серверт ирж буй өгөгдлийг encrypt буюу ширфлэж нууцлан илгээдэг бөгөөд серверээс ямар нэгэн өөрчлөлтгүй бүрэн бүтнээр нь дамжуулдаг. Иймээс дундаас нь таны мэдээллийг хэн нэгэн этгээд барьж авахгүй бас ямар нэгэн засвар ороогүй гэсэн үг юм.

Бүлэг 3

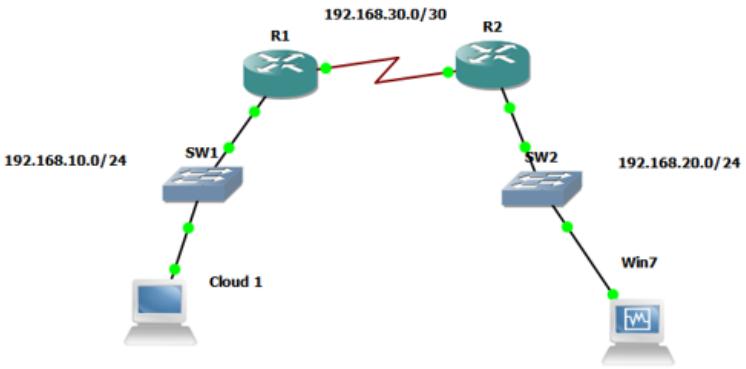
Судалгаа, шинжилгээний бүлэг

3.1 CISCO ip communicator

3.1.1 Ажиллагаа 1

- Өөрийн үндсэн Windows болон VirtualBoX win7 –г Cisco ip communication суулгаж харилцаа тогтоов.
- GNS 3 төхөөрөмж дээр жижиг холболт үүсгэв.

  Cloud 1 бол бидний одоогийн холбоонд server юм.Харин Virtualbox -оор асаасан Win 7 person буюу хэрэглэгч маягаар сонгосон юм.



Зураг 3.1: GNS3 дээр server үүсгэн VirtualBox win7 холбов

- Cisco iP Communicator үндсэн Winsows болон хэрэглэгч VirtualBox win7 дээр суул-

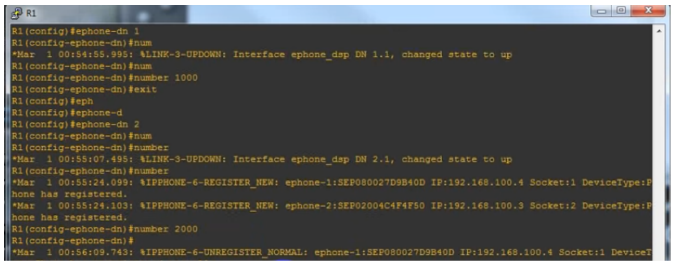
гаж асаах.

Зураг 3.2: GNS3 дээр server үүсгэн VirtualBox win7 холбов

- 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 төлбөртэй юм

3.1.2 Ажиллагаа 2

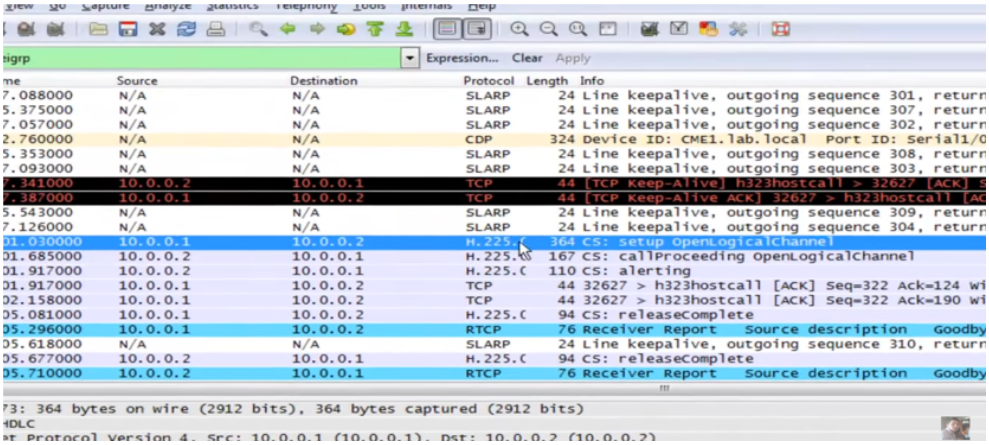
– GNS3 дээр тохируулсан жижиг сүлжээг асааж Cisco ip communicator дээр хэрэглэгч үүсгэв.



Зураг 3.3: 1000 болон 2000 дугаартай хэрэглэгчдыг тохируулж өгөв

Зураг 3.4: 1000 болон 2000 хэрэглэгч хооронд дуудлага амжилттай хийв

- Whireshark аар packet барьж авав



Зураг 3.5: GNS3 дээр server үүсгэн VirtualBox win7 холбов

3.2 Zioper

3.2.1 Asterisk

- Asterisk бол хамгийн өргөн хэрэглэгддэг нээлттэй сервер юм. Asterisk нь маш олон чадвартай бөгөөд PBX private branch exchange үүсгэдэг. Анх гарч ирэхдээ жижигхэн үйлчилгээний утасны систем маягаар гарч ирсэн ч явцын дунд томорсоор харилцаа холбооны түүхэнд чухал байр суурь эзлээд байна.Asterisk одоогоор IP PBX,VoIP gateway,Call center , дуут шуудангийн сервер болон RT харилцааг дэмждэг.

3.2.2 Asterisk протоколууд

- •SIP

  •H.323

  •Media gateway control protocol

  •IAX,IAX2 - inter Asterisk Exchange protocol

3.2.3 Asterisk ба Zoiper

-