**МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ**

**МЭДЭЭЛЭЛ ХОЛБОО ТЕХНОЛОГИЙН СУРГУУЛЬ**


**Шарав Мөнхтулга**

**J.SA13D023**

# Утасгүй сүлжээний тархалтыг тодорхойлох

**Мэргэжил: Компьютерийн Системийн Хамгаалал**

**Систем хамгааллын төсөл**

**Улаанбаатар хот**

**2017он**

# Гарчиг

# Хүснэгтийн жагсаалт

# Зургийн жагсаалт

# Бүлэг 1

# Ерөнхий зүйл

## 1.1 Удиртгал

Миний төслийн хүрээнд iptables-ыг хэрэглэхэд хялбар болгохын үүднээс вебээр хандаж болдог интерфэйс бүтээсэн.Уг төслийг хийхэд галт ханын ажигааг судалж цаашлаад үүнийгээ вебтэй нэгтгэж мэргэжлийн биш сүлжээний анхан шатны мэдлэгтэй хүмүүст зориулж хийх юм.

## 1.2 Зорилго

Энэ төслийн хүрээнд орчин цагт хүний амьдралд интернэт орж ирснээр бидний амьдралд тэр чигээрээ хамааралтай болж байдаг.Үүний хажуугаар халдлага,тагнах зэрэг олон асуудал гарч ирж байгаа.Энэхүү төсөлийн галт ханын нэгдсэн урирдлагын систем хөгжүүлэх явдал юм.

## 1.3 Зорилт

Энэхүү төслийг хийхэд галт ханын ажиллагаа,бүтэц зэрэгийг судалж Linux-ын IPTables программыг веб хандалттай интерфайс болгох явдал юм.

# Бүлэг 2

# Онолын хэсэг

## 2.1 Утасгүй сүлжээ

Утасгүй сүлжээ гэдэг нь 2 ба түүнээс дээш төхөөрөмж тархалтад долгион SSDM(spread spectrum division multiplexing)эсвэл OFDM(Orthogonal frequince division multiplexing) хувиргалтын технологи ашиглан утасгүй холбогдон мэдээлэл солилцохыг хэлнэ.Утасгүй сүлжээг гэр орон, сургууль, эмнэлэг гэх мэт албан байгууллагуудад өргөн ашиглах болсон. Учир нь ашиглахад хялбар үнэ өртгийн хувьд хямд утасгүй гэдэг утгаараа хэрэглэгч сүлжээтэй газраас хаанаас ч холбогдох боломжтой.Хэрэгжилтийн үе шат нь OSI загварын ,физик төвшин дээр явагддаг. Утасгүй сүлжээний жишээ нь гар утасны сүлжээ, утасгүй дотоод сүлжээ (WLAN), утасгүй мэдрэгч сүлжээ, хиймэл дагуулын холбооны сүлжээ, газрын богино долгионы сүлжээ зэрэг орно.Утасгүй сүлжээ нь агаараар өгөгдлийг дамжуулах болон өгөгдлийг хүлээн авдаг ба үүндээ радио давтамжийн технологийг ашигладаг.Анхны утасгүй сүлжээг Хавайн их сургуульд 1969 онд сүлжээг туршин боловсруулжээ. Энэ үеэс утасгүй сүлжээний үндсэн суурь тавигдсан. CDMA долгион болон тархалтад радио долгион ашиглан утасгүй холболт хийж болох талаар судалгаа болон зарим туршилтууд 1979, 1980-аад онуудад хийгдэж байв. 1997 он гэхэд IEEE-802.11 нэршилтэй стандарт болж батлагдсан.

### 2.1.1 Утасгүй сүлжээний ач холбогдол

Утасгүй сүлжээний ач холбогдол нь албан байгууллага , гэр орон , сургууль , цэцэрлэг, эмнэлэг гэх зэрэг хаанаас ч сүлжээнд холбогдох боломжтой юм. Энэ нь утасгүй технологи илүү хурдан өсөж байна гэдгийг харуулж байгаа юм. Энэ технологи нь маш хурдан


Зураг 2.1: Утасгүй сүлжээний технологиуд

сайжирч байгаа нь сайн хэрэг юм. Үүнийг дагаад утасгүй сүлжээний эрэлт хэрэгцээ ч хурдан өсөж байна. Хүмүүсийн ашиглаж байгаа гар утас, зөөврийн компьютер, таблет зэрэг ухаалаг технологиуд бүгд шууд утасгүй сүлжээнд холбогдож байна.Утасгүй сүлжээний ач холбогдол нь албан байгууллага , гэр орон , сургууль , цэцэрлэг, эмнэлэг гэх зэрэг хаанаас ч сүлжээнд холбогдох боломжтой юм. Энэ нь утасгүй технологи илүү хурдан өсөж байна гэдгийг харуулж байгаа юм. Энэ технологи нь маш хурдан сайжирч байгаа нь сайн хэрэг юм. Үүнийг дагаад утасгүй сүлжээний эрэлт хэрэгцээ ч хурдан өсөж байна. Хүмүүсийн ашиглаж байгаа гар утас, зөөврийн компьютер, таблет зэрэг ухаалаг технологиуд бүгд шууд утасгүй сүлжээнд холбогдож байна.

1. Утасгүй сүлжээг өргөтгөх боломж: Жижиг бизнесийн гол зорилгуудын нэг нь өсөлт үүнийг дагаад байгууллагын сүлжээ өргөжих шаардлагатай болдог. Гэтэл өргөтгөхөд асуудал үүсэж нэмж кабел, холболтын үзүүр тавих хэрэгтэй болдог. Энэ нь төвөгтэй мөн цаг хугацаа шаардсан байдаг . Гэхдээ утастай сүлжээний оронд утасгүй сүлжээг хэрэглэснээр илүү олон хэрэглэгчдийг шууд холбох боломжтой мөн өргөтгөхөд хялбар нэмж кабел тавих шаардлага байхгүй төхөөрөмж дээр нэмэлт өөрчлөлт хийхэд болдог.

2. Утасгүй сүлжээний зардал: Утастай сүлжээг суурилуулах, түүнийг өргөтгөх зардал нь утасгүй сүлжээний тоног төхөөрөмжийн үнэнээс өндөр юм. Утастай сүлжээний том асуудал нь кабел нэмж эсвэл солих шаардлагатай үед кабелыг худалдан авах шаардлагатай. Энэ эдийн засгийн хувьд үр ашиггүй юм. Утасгүй

сүлжээг ашиглан бага зардлаар бүтээмжийг нэмэгдүүлэх хэрэгтэй

3. Ашиглахад хялбар: Утасгүй гэдэг утгаараа хэрэглэгч зөөврийн компьютер, гар утас, эсвэл таблет зэрэг төхөөрөмжөөр хүссэн газраасаа сүлжээнд холбогдох боломжтой.

4. Хөдөлгөөнт байдал: Утасгүй сүлжээний гол онцлог нь хөдөлгөөнт байдал юм. Зөвхөн ажлын байрнаасаа эсвэл гэрээсээ интернетэд холбогдох нь хязгаарлагдахгүй болж. Утасгүй сүлжээ орсон хаанаас ч интернет орох боломжтой болсон.е

5. Ажлын бүтээмж: Ажлын бүтээмж нэмэгдүүлэхэд утасгүй сүлжээ нэн давуу талтай. Утасгүй гэдэг утгаараа хэрэглэгч нэг байрнаас нөгөө байранд шилжин ажиллахдаа сүлжээндээ холбогдсон хэвээрээ байх юм. Ингэснээр хүмүүсийн ажлын бүтээмж нэмэгдэх юм.

6. Суурилуулалт: Утастай сүлжээ тавихад кабел татахаас эхлээд механик ажиллагаа ихтэй байдаг. Харин утасгүй сүлжээний давуу тал суурилуулахад цөөхөн төхөөрөмж утастай сүлжээ бодвол багахан суурилуулалтын үеийн ажиллагаа ордог.

### 2.1.2 Утасгүй сүлжээний төрлүүд

Утасгүй сүлжээ нь Ad-Hoc буюу Infrastructure буюу дэд бүтэц гэсэн үндсэн 2 хэлбэрээр ажилладаг.Төхөөрөмж хоорондын гэдэг нь сүлжээний хэрэглэгч төхөөрөмжүүд нь өөр нэмэлт төхөөрөмжгүйгээр шууд хоорондоо холболт үүсгэн мэдээлэл дамжуулдаг. Дэд бүтэц гэдэг нь утасгүй сүлжээний замчлагч (router), хандалтын цэг (access point) ашиглан утасгүй болон утастай сүлжээнд олон төхөөрөмжүүдийг нэгдсэн сүлжээнд холбодог байна.

- Peer-to-Peer/Ad-Hoc буюу Төхөөрөмж хоорондын холболт: Хамгийн энгийн утасгүй сүлжээний төхөөрөмж хоорондын холболт нь Ad-Hoc холболт юм. Independent Basic Set (IBSS) буюу үндсэн үйлчилгээний багцыг ашиглан хийгддэг. Энэ нь утасгүй холбооны төхөөрөмжүүд шууд хоорондоо холбогдох боломжийг олгодог. IEEE 802.11 стандартуудад багтдаг үзүүлэлтийн дагуу урьдчилан IP хаяг болон утасгүй сүлжээний нэрийг тохируулсан 2 төхөөрөмж нь шууд холболт хийн мэдээллийг шууд солилцох боломжтой байдаг.

- Bridging буюу Утастай сүлжээнд гүүрэн холболт хийх: Ердийн дотоод сүлжээ нь тогтвортой ажиллаж байгаа байгууллага, хүмүүсийн хувьд өөрсдийн утастай сүлжээг шууд утасгүй болгон солих нь зардал мөнгө хийгээд нууцлал хамгаалалтын хувьд ч асуудалтай учраас сүлжээгээ өргөтгөн утасгүй сүлжээний хандалтын цэг (Wireless access point)-ийг суурилуулснаар сүлжээний тохиргоондоо бараг өөрчлөн хийлгүйгээр утасгүй сүлжээний хэрэглэгчидтэй холбогдох боломжтой байдаг.

## 2.2 WiFi технологи


Зураг 2.2: WiFi

Утасгүй сүлжээний тоног төхөөрөмж үйлдвэрлэдэг компаниуд нийлж бие даасан Wireless Ethernet Compatibility Alliance (WECA) гэсэн байгууллага байгуулсан ба уг байгууллагад Cisco, Lucent, IBM, Apple, Dell, Siemens, AMD зэрэг нэрд гарсан компаниуд гишүүнээр элссэн байдаг. Энэ байгууллагын тавьсан техникийн шаардлагыг хангасан бүтээгдэхүүнийг Wi-Fi тэмдэгтийн бүтээгдэхүүн гэж нэрлэдэг. IEEE 802.11 стандартад нийцэн гэрчилгээ авсан бүтээгдэхүүн дээр тавигддаг. Зарим улсуудад 802.11 утасгүй сүлжээг товчлон Wi-Fi гэж нэрлэдэг. Wi-Fi бол өндөр хурдны интернетийн холболтуудыг багтаасан компьютерийн сүлжээгээр дамжуулан утасгүй интернетийн өгөгдлийг солих цахим хэрэгслийг зөвшөөрдөг түгээмэл технологи юм. Wi-Fi Холбоо нь Харилцаа холбоо, цахим төхөөрөмжийн хувийн нийгэмлэг' (IEEE)-ийн 802.11 стандартад суурилсан ямар ч утасгүй дотоод сүлжээгээр (WLAN) Wi-Fi-ийг тодорхойлдог. Хэдийгээр хамгийн орчин үеийн WLAN-ууд эдгээр стандартуудад суурилагддаг боловч

Wi-Fi гэдэг нэр томьёо нь ерөнхий Англи хэл дээр "*WLAN*"-тай ойролцоо утгаар хэрэглэгддэг. Wi-Fi-ийг ашиглах хэрэгслүүд(хувийн компьютер(pc), дүрс бичлэгийн тоглоомын хэрэгсэл, ухаалаг гар утас, дижитал камер, таблет, дижитал дуу бичлэг тоглуулагч зэрэг ) утасгүй хандалтын цэгээр(AP эсвэл hotspot) дамжуулж байгааь интернет буюу сүлжээний нөөцтэй холбогдож болно. хандалтын цэг нь байшин дотор 20 метр орчим(65фит) бүст болон гадна талын хэсэг бүст байдаг. Хандалтын цэгийн хамаарал радио долгионыг хязгаарладаг жижиг өрөөг шиг орон зайд болон том талбайг бүрхэж чадна.

### 2.2.1 WiFI давуу тал

Тэр WiFi технологийг ашиглан хамгийн гол давуу тал нь утасгүй юм. WiFi сүлжээг ашиглан төрөл бүрийн төхөөрөмжүүд интернетэд холбогдох боломжтой. Өнөөдөр WiFi сүлжээнд жишээ нь: Нисэх онгоцны буудал, эмнэлэг, цэцэрлэгт хүрээлэнд гэх зэрэг хаанаас ч хандах боломжтой. Компьютер нь холболтын тохиргоог хадгалдаг бөгөөд ямар ч үед сүлжээг идэвхжүүлэхэд WiFi-ийн дохиог таньж автоматаар холбогддог.

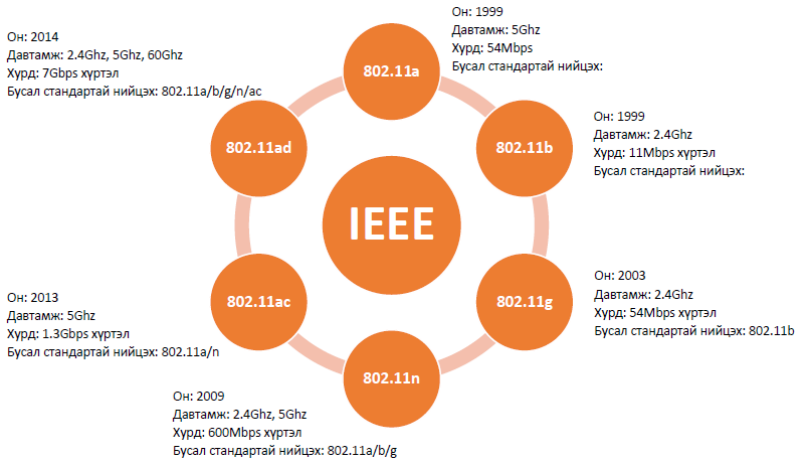
### 2.2.2 WiFi сул тал

Утасгүй сүлжээний долгионууд нь байшингийн хананаас гадагшаа нэвтэрч тардаг. Хэрэв хэрэглэгчийн сүлжээ хамгаалалтгүй бол энэ нь хэд хэдэн эрсдэлийг авчирдаг. Хэрэглэгчийн сүлжээнд зөвшөөрөлгүй хүний халдлага ирнэ. Сүлжээнд зөвшөөрөлгүй хэрэглэгчид холбогдох.Бодит байдал дээр утасгүй сүлжээгээр файл дамжуулах нь утастай сүлжээнээс хамаагүй удаан байдаг. WiFi-ын хамрах хүрээ нь хязгаарлагдмал байдаг. Утасгүй холболт болон хөдөлгөөнт төхөөрөмжүүд нь үнэндээ стандарт утастай холболтыг бодвол WiFi ашиглах илүү их эрчим хүч хэрэглэдэг.

## 2.3 Утасгүй сүлжээний IEEE 802.11 стандартын протоколууд

Утасгүй сүлжээний амин сүнс болсон эдгээр стандартуудын ачаар янз бүрийн үйлдвэрлэгчид нь хоорондоо зохицон, харилцаж ажиллах боломжтой. Сүлжээний төхөөрөмжүүдийг үйлдвэрлэн гаргаж ингэснээр хэрэглэгчдэд учрах эрсдэлийг арилгаж байгаа юм. Таны зөөврийн компьютер ямар пүүсийнх байхаас үл шалтгаалан та утасгүй сүл-

жээнд холбогдох, гэртээ сүлжээ суурилуулах боломжтой бөгөөд зөвхөн таны төхөөрөмжүүд нь сүүлийн үеийн, ижил стандартын байгаа эсэхийг шалгахад л хангалттай юм.




Зураг 2.3: Утасгүй дотоод сүлжээний стандартууд

- 802.11: Анх 1997 онд гарсан. Харин 1999 онд засварлагдан өөрчлөлт орсон бөгөөд өнөө үед хоцрогдсон стандарт юм. Энэ стандарт нь утасгүй сүлжээний анхны хувилбар тархалтад долгионы сүлжээгээр 1-2Мбит/с хурдаар, хэт улаан долгионоор 1Мбит/с хурдаар, дараалсан тархалтад долгионоор 1-2Мбит/с хурдаар 2.4ГГц долгионоор холбогдох боломжийг тодорхойлжээ. Энэ стандартын дараалсан тархалтад долгионтой хувилбарыг цаашид нь хөгжүүлэн 802.11b стандартыг гаргасан билээ.

- 802.11a: 802.11 стандартын дараа 1999 оны 10 сард 802.11a стандарт гарсан. OFDM дээр суурилсан Энэ стандартын дээд хурд нь 54Мбит/с бөгөөд алдааг засах кодлолыг багтаасан байсан. 2.4ГГц-ийн үелзэл их ачаалалтай үед 5ГГц-ыг ашиглах нь давуу талтай байсан ч бусад стандарттай харьцуулахад долгионы урт нь богино учраас хана болон бусад биетээс амархан сарниж ингэснээр сүлжээний хамрах хүрээ нь бага байсан.

- 802.11b: Өгөгдөлд хандах арга нь анхны стандарттай ижилхэн 11Мбит/с хурдтай байсан. Ийм ч учраас 802.11b стандартын төхөөрөмжүүд зах зээлд 2000 оны үед хурдан гарч ирсэн. 802.11b стандарт нь 2.4 ГГц давтамжийг ашигладаг. Нэг

дутагдалтай тал нь 802.11b стандарт нь ижил 2.4ГГц үелзэл дээр ажилладаг гэр ахуйн цахилгаан хэрэгсэл богино долгионы зуух, Bluetooth болон бусад хэрэгсэл нь хөндлөнгийн шуугианы нөлөөлөлд амархан ордог юм. 802.11b давуу тал зардал бага дохионы хүрээ нь сайн.

- 802.11g: 2003 оны 6 сард гуравдахь стандартыг батлан гаргасан. Ажиллах давтамж 2.4ГГц бөгөөд өгөгдөл дамжуулах хурд 54Мбит/с байдаг. 802.11b-гийн адил 2.4 ГГц үелзэл дээр ажилладаг хэдий ч 802.11a шиг OFDM дээр суурилсан дамжуулалтын зарчим ашигласан. Иймээс илүү дамжуулах хурдтай, үйлдвэрлэлийн зардал буурсан учраас бүүр 2003 оны эхнээс стандарт батлагдахаас өмнө хэрэглэгчид 802.11g стандартын саналын дагуух бүтээгдэхүүнүүдийг илүүтэй худалдан авч хэрэглэж эхэлжээ. 2003 оны зун гэхэд дийлэнх утасгүй сүлжээний бүтээгдэхүүнүүд 2-3 үелзлийг буюу 802.11a/b/g стандартуудыг нэг төхөөрөмжид багтаасан байдлаар гарчээ. b болон g-г хамтад ажиллуулах нь гол сорилт байсан бөгөөд 802.11g сүлжээнд 802.11b төхөөрөмж холбогдон мэдээлэл дамжуулахад нийт сүлжээний хурд бууруулдаг байна.802.11b гийн нэгэн адил 802.11g төхөөрөмжүүд нь 2.4ГГц үелзэл дээр ажиллаж байгаа бусад төхөөрөмжүүдийн нөлөөнд цохигдож болдог байна.

- 802.11ac: 2013 он батлагдсан.Өгөгдөл дамжуулах хурд 866Мбит/с Уг стандарт нь 5ГГц- ийн давтамжид ажиллах бөгөөд хамгийн багадаа секунд-д 1 гигабит өгөгдөл дамжуулах чадамж бүхий өндөр түвшиний multi-station WLAN, мөн багадаа 500Мбит/с дамжуулах чадамж бүхий дан холболтыг дэмжинэ. Ингэхдээ 80 эсвэл 160 MHz-ийн өргөн зурвасын радио долгион болон өндөр нягтруулагын модуляцын арга болох 256 QAM-ийг ашиглана.

- 802.11n: IEEE-гээс 2009 оны 11-р сард гарсан. 802.11n бас заримдаа "Wireless N"гэж нэрлэдэг. Ажиллах давтамж 5 ГГц ба 2.4 ГГц бөгөөд өгөгдөл дамжуулах хурд 150Мбит/с 802.11n нь өмнөх стандартуудын сайжруулсан хувилбар бөгөөд олон-оролт олон-гаралт ( MIMO - multi-input multi-output) болон бусад шинэ боломжуудыг нэмж байгаа. 802.11n нь давуу тал хурдан мөн гадны дохио шуугианд илүү тэсвэртэй. 802.11n сул илүү зардал ихтэй.

- 802.11ad: 2014 онд гарсан ба 2.4ГГц , 5ГГц, 60ГГц зэрэг давтамжийг ашигладаг. Хурд 2014 онд гарсан ба 2.4ГГц , 5ГГц, 60ГГц зэрэг давтамжийг ашигладаг.

Хурд 7 Гбит/с хүртэл байдаг . 802.11a/b/g/n/ac гэсэн бусад стандарттай нийцдэг. 802.11ad стандарт нь өгөгдлийг 4,6 Гбит/с дамжуулж байгаа. Өндөр хурдны өгөгдөл солилцоо нь миллиметрийн диапозоны шинэ хүлээн авах ба нэвтрүүлэх схем, шинэ дэлгэмэл өнцгийн антен, идэвхтэй модуляц болон демодуляцийн төхөөрөмж ашигласантай холбоотой юм. Бусад стандарттай харьцуулбал. Шинэ 802.11ad стандарттай төхөөрөмж 1/3000 секундэд сүлжээг хайж олдог тул нэгэн зэрэг олон төхөөрөмж сүлжээнд холбогдох боломжтой. Өмнөх технологитой харьцуулахад шинэ Wi-Fi технологийн ашиглаж байгаа 60 ГГц-ийн давтамжтай радио долгионы тархалт муу, төхөөрөмжийн сүлжээний хамрах хүрээ багатай.

- 802.11e: IEEE бүх утасгүй сүлжээний интерфейсүүдэд зориулсан хаяг- лалтын чанарын үйлчилгээний шаардлагыг тодорхойлдог. Энэ нь 802.11 сүлжээнд видео дамжуулах, IP дээгүүрх дуу (VoIP) зэрэг мультимедиа хэрэглээнүүдэд шаардлагатай протоколуудыг тодорхойлдог. 802.11i-тай адил 802.11e нь үйлдвэрлэлийн бүлгээс 802.11e-ийн дэд олонлог гэж тодорхойлсон, 802.11e-г батлахыг хүлээж байх хугацаанд мультимедиа хэрэглээнүүдийг идэвхжүүлэхэд ашиглаж болох WME (сүүлд WMM) гэгдсэн урьдчилсан тодорхойлолт байдаг. 802.11e болон WME/WMMийн талаар мэдэх ёстой хамгийн чухал зүйл нь утасгүй сүлжээний зэрэглэл тогтоогдсон урсгалын хэрэглээг Quality of Service (QoS) буюу үйлчилгээний чанарын протоколууд болон өргөтгөсөн зөөвөрлөгчийн хандалтын протоколуудын тусламжтайгаар идэвхжүүлдэг явдал юм. Эдгээр протоколуудын зөв шийдэл нь өгөгдлийн өндөр хурдтай тэсрэлт болон зэрэглэл тогтоогдсон урсгалыг идэвхжүүлдэг.
- 802.11f: P2P холболтын стандарт.
- 802.11h: Европ, Азийн бүсэд ашиглагддаг. 5ГГц өндөр хурдны утасгүй сүлжээ.
- 802.11i: Нууцлалын стандартыг тодорхойлдог. 802.1X, TKIP, AES.

## 2.4 Утасгүй сүлжээний технологиуд

Утасгүй сүлжээ нь хэрэглээний салбараараа хэд хэд хуваагддаг.

Үүнд:

1. Утасгүй хувийн орчны сүлжээ (WPAN)- IEEE 802.15

2. Утасгүй хотын сүлжээ (WMAN)- IEEE 802.16
3. Утасгүй улс орныг хамарсан сүлжээ (WWAN) - IEEE 802.20
4. Утасгүй дотоод сүлжээ (WLAN) - IEEE 802.11

Тус салбаруудад олон янзын шаардлагууд байдаг.

1. Зурвасын өргөн
2. Хамрах хүрээ
3. Чадал
4. Хэрэглэгчийн байршил
5. Санал болгох үйлчилгээнүүд
6. Сүлжээ эзэмшигч

Энэ бүх шаардлагуудыг нэгтгэн нэг цогц болгож стандартчилдаг хоёр том холбоо байдаг.

1. IEEE (Institute of Electrical and Electronics Engineers)
2. ETSI (European Telecommunications Standards Institute)

### 2.4.1 WPAN буюу Утасгүй хувийн сүлжээний үндсэн ойлголт

Бага хүрээтэй утасгүй өгөгдлийн сүлжээ ба өөрөөр хэлбэл утасгүй хувийн сүлжээ юм. Үүнийг телевизийн алсын удирдлагын механизмыг гар утас, PDA-д суурилуулж богино зайд өгөгдөл дамжуулж байгаа гэж ойлгож болно. Bluetooth технологи нь IEEE-с гаргасан 802.15 стандарт юм. Хамгийн анхны стандарт болох 802.15.1 нь маш бага зайд маш бага өгөгдөл дамжуулж байсан. Мөн бага зайд өргөн зурвасыг ашиглан өндөр хурдаар дамжуулах UWB нь 802.15.3 стандартаар гарснаар лицензгүй 1,5 ГГц болон түүнээс дээш давтамжийг ашиглах болсон. UWB нь маш бага чадлаар долгион дамжуулдаг учир дохио шуугианы түвшнээс доогуур дамжигддаг. Bluetooth радио долгион нь дохио дамжуулагч болон хүлээн авагчийн хооронд LMP (Link Management Protocol)-р дамжигддаг. WPAN технологийн төхөөрөмжүүд нь PHY ба DLC түвшинд ажилладаг. Bluetooth технологи нь 1 Mbps өгөгдөл дамжуулах чадварыг үзүүлдэг бол UBW нь түүнээс 400 дахин илүү буюу 400 Mbps өгөгдлийн үзүүлэлтийг үзүүлдэг юм.

### 2.4.2 WWAN Утасгүй улс хоорондын сүлжээний үндсэн ойлголт

Утасгүй WAN сүлжээ нь хөдөлгөөнт хэрэглээнд санал болгож байгаа улс орон, тив дэлхийг хамардаг. Утасгүй WAN сүлжээний дэд бүтэц нь холбооны үйл ажиллагааг хийж болмоор бөгөөд холын зайн холболттой том үйлчилгээний сууриар хангадаг. Бусадтай харьцуулбал илүү үнэ өртөг өндөртэй, түгээх байдлаараа хаа сайгүй олон хэрэглэгчдэд тархаж чаддаг. Нэг алсын холбооны үйлчилгээгээр хангаж байгаа газраас хэрэглэгч дэлхийн хаа нэгтэйгээс утасгүй WAN сүлжээгээр интернетийн үйлчилгээг авч ашиглаж чадна. Утасгүй WAN сүлжээний биелүүлэлт нь бусадтай харьцуулбал өгөгдлийн хурдны дээд тал нь 170 kbps ба жирийн хурд нь 56kbps байна. Утасгүй WAN сүлжээ нь хөгжлийн явцад төрөл бүрийн стандартын бүрэлдэхүүнийг өөртөө багтаасан байдаг. Үүнд үүрэн холбооны систем GSM болон GPRS, 3G зэрэг тив дэлхийг хамрах технологиуд утасгүй улс хоорондын сүлжээнд багтдаг.

### 2.4.3 WLAN буюу Утасгүй дотоод сүлжээний үндсэн ойлголт

1990 онд IEEE байгууллагын IEEE 802.11 стандартын зөвлөл байгуулагдаж, энэ зөвлөл нь 1 ба 2 мб/с -ийн хурдны хандалттай, 2,4 ГГц давтамж дээр ажиллах утасгүй сүлжээ болон радио төхөөрөмжүүдийн нийтэд хэрэглэгдэх стандартуудыг боловсруулах зорил-

готойгоор байгуулагдсан юм. 1997 онд анхны IEEE 802.11стандартыг нийтэд зарласан ба 1999 оны 7 сард IEEE нь өмнөх стандартын өргөтгөл болох IEEE 802.11b стандартыг гаргасан байна.

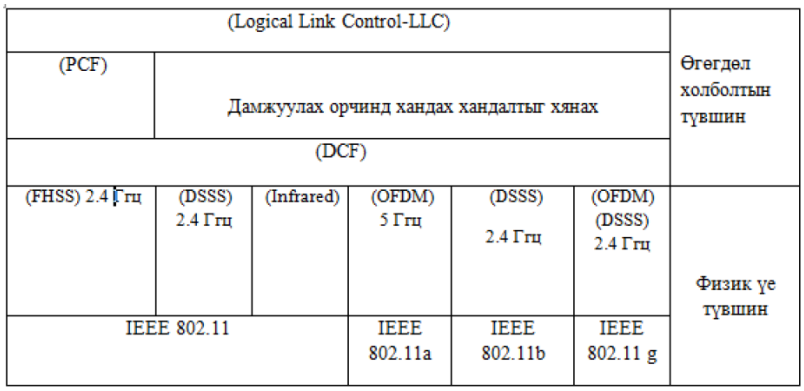
IEEE 802.11b нь 10мб/с -ийн хурдтайгаар өгөгдлийг дамжуулна. Утасгүй сүлжээний тоног төхөөрөмж үйлдвэрлэдэг компаниуд нийлж бие даасан WECA гэсэн байгууллага байгуулсан. Энэ байгууллагын тавьсан техникийн шаардлагыг хангасан бүтээгдэхүүнийг Wi-Fi тэмдэгтийн бүтээгдэхүүн гэж нэрлэдэг. Утасгүй суурин сүлжээнд зөөврийн компьютер болон PDA зэрэг хөдөлгөөнт зөөврийн төхөөрөмж хамаардаг бол утасгүй холбооны сүлжээний хамрах хүрээнд хөдөлгөөнт үүрэн телефоны сүлжээ (mobile telephone) орж байгаа юм. Зөөврийн компьютер болон PDA зэрэг хөдөлгөөнт зөөврийн станцууд хөгжихийн хэрээр хамрах хүрээ нь тэлсээр байна. Утасгүй сүлжээ нь хэдэн бүрэлдэхүүн хэсгээс тогтдог бөгөөд энэ нь радио болон гэрлэн долгион дээр тулгуурлан дохиог агаарын орчноор нэвтрүүлдэг.

- Хэрэглэгчид
- Компьютерийн төхөөрөмжүүд
- Сүлжээний интерфэйс карт
- Агаарын орчин

Үүнд байгаа Сүлжээний интерфейс карт нь компьютерийн төхөөрөмж болон утасгүй сүлжээ хоёрын хоорондох интерфейсийг бэлтгэж өгдөг бөгөөд өөрөөр хэлбэл сүлжээний адаптер юм.

**Утасгүй дотоод сүлжээний физик болон өгөгдөл холболтын түвшин**

Утасгүй дотоод сүлжээ нь IEEE 802.11 стандартууд нь OSI-ийн 7н түвшний физик болон өгөгдөл холболтын түвшинд ажиллана.




Зураг 2.4: IEEE 802.11-ийн физик болон өгөгдөл холболтын түвшин

**IEEE 802.11-ийн өгөгдөл холболтын түвшин**

IEEE 802.11-ийн өгөгдөл холболтын түвшин үүнд:

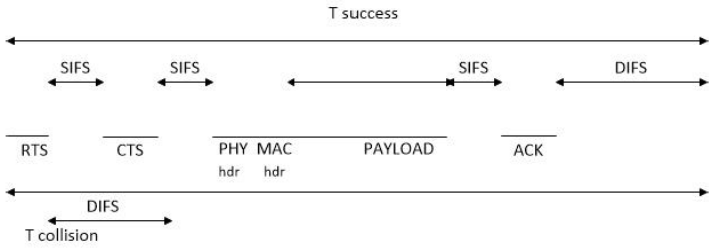
- Логик холболтын удирдлага (Logical Link Control-LLC)
- Дамжууллын орчинд хандах хандалтын удирдлага (Media Access Control- MAC)

Логик холболтын удирдлага (Logical Link Control-LLC) нь өгөгдөл холболтын түвшин дээр ажиллах протоколуудын (IP, IPx, Decnet, Appletalk,) өгөгдлийн урсгалыг удирдан зохицуулах, амжилттай илгээснийг мэдэгдэх үүрэгтэй.

MAC дэд үе давхарга нь 802.3-ийн MAC дэд үе давхаргатай нилээн төстэй боловч ялгаатай. Ethernet сүлжээнд мөргөлдөөнийг илрүүлэх чадвартай зөөгчийг таних (мэдрэх) олон цэгийн хандалт(carrier sense multiply access with collision detection-CSMA/CD) гэдэг аргыг хэрэглэдэг ба энэ арга нь дамжууллын нэг орчинг сүлжээнд холбогдсон төхөөрөмжүүд яаж зохистой хэрэглэхийг заасан арга байдаг. Мөн станц нь илгээх/-дамжуулын горим өөрөөр хэлбэл дуплекс горимд ажилладаг гэж үзсэн. Харин 802.11 хагас дуплекс горимд ажилладаг тул өгөгдөл илгээх тэр агшинд нэг зэрэг мөргөлдөөнийг илрүүлэх үйлдэл хийж чаддаггүй байна. Иймээс 802.11 нь мөргөлдөөнөөс зайлах чадвартай зөөгчийг таних (мэдрэх) олон цэгийн хандалт (carrier sense multiply access

with collision avoidance-CSMA/CA) гэдэг аргыг хэрэглэдэг. Эсвэл тархмал баримжаатай функц (Distributed Coordination Function DCF) гэсэн нэртэй технологи гэж ч ярьдаг. CSMA/CA хэрэглэх үед хүлээн авагч станц нь ACK гэсэн багцыг илгээгч станцруу явуулдаг ба энэ багцын тусламжтайгаар мөргөлдөөнөөс зайлсхийдэг гэж хэлж болно. Суваг чөлөөтэй эсэхийг тодорхойлохын тулд сувгийн цэвэр эсэхэд үнэлгээ өгөх (Channel Clearance Algorithm-CCA) алгоритмыг хэрэглэнэ. Хүлээн авч буй дохионы чадлыг тодорхойлж, антен дахь дохионы энергийг хэмжих аргууд үүнд хамаарна. Хэрэв хүлээн авч байгаа дохионы чадал тодорхой босгоноос доогуур байвал суваг чөлөөтэй гэж үзэн MAC түвшин нь сувгийг мэдээлэл дамжуулахад бэлэн гэсэн төлөвийг зааж өгнө.

1. Фрейм илгээхээс өмнө төхөөрөмж зөөгч давтамж дээрх хүчдэлийн түвшингээр орчныг шалгана. (Persistence strategy)
2. Request to Send (RTS) фреймийг илгээнэ. RTS фреймд суваг эзлэх ху- гацаа Network Allocation Vector (NAV) агуулагдсан байна.
3. RTS хүлээн авагдсаны дараа Short Interframe Space (SIFT) хугацааны турш хүлээгээд Clear to Send (CTS) фреймийг илгээнэ.
4. CTS хүлээн аваад SIFT хугацааны дараа өгөгдлөө илгээнэ.
5. Хүлээн авах төхөөрөмж мөн SIFT хугацаанд хүлээгээд ACK фреймийг илгээнэ




Зураг 2.5: RTS/CTS протоколын схем

**IEEE 802.11-ийн физик түвшин**

- FHSS (Frequency Hopping Spread Spectrum)

Давтамжаар харайлгах спектрэн тэлэлт. Давтамжаар харайлгах спектрийн тэлэлтийн аргын үед 2.4 Ггц дэх давтамжийн зурвас 1 МГц-ийн өргөнтэй 79 сувагт хуваагдана. Илгээгч ба хүлээн авагч нь сувгийг солих схемийг харилцан тохируулах ба өгөгдөл нь энэ схемийг ашигласан янз бүрийн сувгаар дамжигдана. 802.11 сүлжээний өгөгдлийн дамжуулал бүр өөр өөр сэлгээний схемээр хийгдэх ба энэ схем нь хоёр хэрэглэгч зэрэг нэг сувгийг хэрэглэх боломжийг аль болох багасгасан байдлаар хийгдсэн байна. FHSS арга нь илгээх/хүлээн авах ийм энгийн схемийг ашигладаг боловч 2 Мб/с-ийн хурднаас хэтэрдэггүй ба энэ нь нэг сувагт 1 МГц-ёийн давтамжийн зурвас өгөгдсөнтэй холбоотой. Сэлгээний байж болох хамгийн бага хурдны жишээ нь АНУ-д секундэд 2.5 байдаг.

- DSSS (Direct Sequence Spread Spectrum)

Шууд дарааллын спектрэн тэлэлт. DSSS арга нь 2.4 ГГц дэх давтамжийн зурвасыг 14 суваг болгон хуваах ба сувгууд нь үүүүхлээрээ биш, хэсэгчилсэн байдлаар бие биетэйгээ давхацсан байдаг. Хэд хэдэн сувгууд нэг зэрэг нэг байрлалд хэрэглэгдэж байхын тулд тэдгээр сувгууд нь бие биеэсээ 25МГц- ийн алхамтай байх ёстой байна. Тэгэхээр нэг байрлалд нэг зэрэг 3-аас илүү суваг хэрэглэж болохгүй гэсэн үг юм. Өгөгдлийг энэ сувгуудын аль нэгээр сувгийн сэлгээ хийхгүйгээр дамжуулдаг.Хажуугийн саад шуугианыг дарахын тулд 11 битийн дараалал өүхий Баркерийн кодыг ашиглана. Өгөгдлийн нэг бит 6wp энэ Баркерийн кодоор хувирна. Баркерийн кодыг хэрэглэснээр дамжуулалын найдваржилтыг дээшлүүлж, илгээх дохионы чадлыг багасгах сайн талтай.

- Infrared (IR) Инфра улаан зурвас дахь дамжууллын арга

802.11 стандартад хэрэглэгддэг энэ арга нь чиглүүлээгүй инфра улаан дохиог (diffuse IR) өсгөгч дамжуулагчаар цацах арга юм. 850-950 нм-ийн урттай долгионы зурвас ашиглах ба системийн үйлчлэх хүрээ 10 метрт байна. IR цацраг нь цаг агаарын нөлөөнд автамтгай учир байшин дотор хэрэглэхэд тохиромжтой. 1 ба 2 Мб/с-ын дамжууллын хурдыг дэмждэг ба илгээх дохионы чадлын дээд хэмжээ 2 Вт байна. Спектрэн тэлэлт гэдэг нь дамжуулж байгаа өгөгдлийн шуугианд тэсвэрлэх чадварыг ихэсгэх зорилгоор дохионы нарийн зурвасын спектрийг өргөн зурвасын спектрлүү шилжүүлэх арга юм.

- OFDM (orthogonal frequency division multiplexing)

OFDM нь 802.11a 802.11g 802.11n стандартууд дээр болон 802.16 WiMax технологиуд дээр хэрэглэгддэг. 5ГГц-д ажиллах утасгүй сүлжээний систем нь өөр өөр модуляцийн аргуудыг ашигласнаар өөр хоорондоо өгөгдөл дамжуулах боломжтой ба өгөгдлийн хурд болгоны хувьд өөр өөр кодлолын аргыг хэрэглэнэ. Энгийнээр тайлбарлавал хугацааны агшин бүрд давтамж бүр дээр өөр утгууд буюу тэмдэгтүүдийг илгээдэг гэсэн үг. OFDM нь нэг сувгаар хугацааны нэгж агшинд олон дохиог дамжуулна. Дохиог давтамж бүр дээр кодолж нэгэн агшинд зэрэг дамжуулна. OFDM нь өндөр спектер үр дүнтэй ашигладаг. Олон замын интерференцэд тэсвэртэй гадны шуугианыг хялбархан шүүж чадна. Uplink болон Downlink-ийн үүрэг зориулалт тус бүрд нь зориулж зөөгчийг өндөр нам янз бүрээр хувиарлаж болдог. Хамгийн чухал нь олон дэд зөөгчийг ашигладаг, тэдгээр нь бага битийн хурд болон урт хэмжээний буюу тэмдэгтүүдийн хурдыг тус тусад зөөдөг. Дохиог физик дамжуулах орчноор дамжуулахдаа энгийн замаар тодорхой хугацаанд бит битээр нэг зөөгч давтамжаар мэдээллийг илгээнэ. BPSK, QPSK, 16-QAM, 64-QAM модуляцийн аргуудыг 6-54 Мбит/с хурдтайгаар өгөгдөл дамжуулахад хэрэглэдэг. Мушгиа кодлолын арга нь ихэвчлэн зурвасын өргөнийг ашигтайгаар хэрэглэхэд ашиглана. Мөн алдаа засах болон илрүүлэхдээ мушгиа кодлол болон интерливинг ашигладаг.

# Бүлэг 3

# Судалгааны хэсэг

## 3.1 Утасгүй сүлжээг хамгаалах боломж, Нууцлалын протоколууд

Утасгүй сүлжээний сул эмзэг байдал мэдээлэл алдагдаж байгаа болон дээрх довтолгоонуудаас шалтгаалан IEEE 802.11-с доорх хамгаалалтын 2 аргыг тодорхойлон:

- Нээлттэй системийн баталгаажуулалт (open-system authentication)
- Түлхүүр хуваалцах баталгаажуулалт (shared-key authentication)

### 3.1.1 Нээлттэй системийн баталгаажуулалт

Нээлттэй системийн баталгаажуулалтын техник нь яг жинхэнэ баталгаажуулалт (authentication) байж чаддаггүй. Хандалтын цэг нь станцыг танин шалгахгүйгээр хөдөлгөөнт станцыг хүлээн авдаг. Хандалтын цэг дээр түгээмэл ашиглагддаг энэ арга нь утасгүй сүлжээнд хандах төхөөрөмж тус бүрт давхцахгүйгээр байдаг MAC Address-г нэг бүрчлэн бүртгэн тохируулах шүүх замаар зөвшөөрөлгүй хэрэглэгч сүлжээнд нэвтрэхээс сэргийлдэг. Эсвэл утасгүй сүлжээний таних нэр буюу Service set identifier (SSID)-г нууцлах маягаар хамгаалснаар утасгүй сүлжээг зөвшөөрөлгүй хүмүүс харах боломжгүй бөгөөд DHCP server ашиглахгүйгээр static ip хаяг хэрэглэвэл тохиргоог нэг бүрчлэн гараар тохируулах шаардлагатай болно. Ингэснээр сүлжээнд нэвтрэх асуудлыг шийдэж чадах боловч дамжигдаж байгаа мэдээлэлд бүрэн хамгаалалт нууцлалыг хангаж чаддаггүй. Учир нь SSID-г нууцлахад ямар нэгэн шифрлэлт хийгддэггүй бөгөөд дамжигдах мэдээллээр string хэлбэрээр дамждаг нь үүний сул тал байдаг.

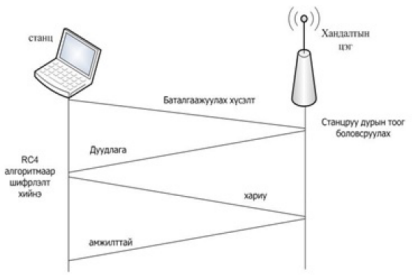
MAC хаягаар бүртгэж, нэвтрүүлж байхад баг өмсөх (Masquerade) (Spoofing) зэрэг халдлагад өртөх боломжтой байдаг.

### 3.1.2 Түлхүүр хуваалцах баталгаажуулалт

Утасгүй сүлжээний хамгаалалтын түгээмэл хэлбэр бол сүлжээнд холбогдон ажиллахын тулд урьдчилан тохируулсан нууцлалын нөхцөлийг зөв ханган нууц үгээр нэвтрэх бөгөөд нууцлалт нь (cryptography) дээр суурилсан байдаг.Утасгүй сүлжээний үндсэн 2 төрлийн нууцлал байдаг.

- WEP (wireless equivalent privacy)
- WPA, WPA2 (Wi-Fi protected access-2)

**WEP (Wireless Equivalent Privacy)** Wired Equivalent Privacy (WEP) нь утасгүй сүлжээний аюулгүй байдлын алгоритм юм. Энэ алгоритм 1997 онд 802.11 стандартын нэг хэсэг болгон танилцуулсан. Утасгүй сүлжээний мэдээлэл нь агаараар радио долгионоор цацагдан дамждаг учир ердийн утастай сүлжээг бодвол дохио замаас барьж аван "хулгайлах"боломжтой байдаг. Түүний зорилго нь утасгүй сүлжээний мэдээллийн нууцлалыг хангах зорилготой юм. WEP нь 40 бит-н нууцлах түлхүүрийн хэмжээтэй. Хэдийгээр 40 бит хэмжээний нууцлах түлхүүртэй боловч стандарт бус хэмжээгээр 104 битийн хэмжээтэй нууцлах түлхүүрийг нийлүүлэгчид гаргадаг. 24 бит-эхлэх вектор (initialization vector). Үндсэндээ нууц код (cryptographic)-н техникийн нууцлал нь түлхүүр үг нэмэгдэхэд сайжирдаг.




Зураг 3.1: WEP баталгаажуулалтын мэссежийн урсгал

Хандалтын цэг нь сонгосон дуудлагаа боловсруулаад утасгүй хэрэглэгчрүү хариу багцыг илгээдэг. Хэрэглэгч нууц түлхүүр (cryptographic) ашиглан хандалтын цэг дээр байгаа дуудлагыг шифрлэн аваад, буцааж хандалтын цэг рүү үр дүнг нь явуулдаг. Хандалтын цэг нь кодыг нээж (decrypt) хэрэглэгчээс ирсэн үр дүнг тооцоолж үзээд хандалтын цэгийн дамжуулсан дурын дуудлага зөв бол хэрэглэгчийг сүлжээнд хандахыг зөвшөөрдөг.

**WEP-н сул тал болон халдлагад өртсөн байдал** WEP-г идэвхжүүлсний дараа дамжигдаж байгаа packet дундаас нь Initialization Vector болон Root Key (хэрэглэгчийн нууц үг) 2-г мэдчихэд халдлага хийхэд амархан болдог. Тэрээр зөвхөн өгөгдлийн багцуудыг хамгаалах ба физик үе давхаргын толгой мэдээллийн хэсгийг хамгаалдаггүй учир WEP protocol-оор дамжиж байгаа пакет (долгион) дотроос header-г олоод унших хад бүх зүйл бичигдсэн байдаг. Иймээс сүлжээний бусад станцууд сүлжээгээр дамжих мэдээллийн зориулалтыг харах боломжийг олгодог. WEP нь 40-бит, 128-бит болон 256-битийн урттай түлхүүр ашиглан утасгүй сүлжээнд төхөөрөмж холбогдох үед урьдчилан тохируулсан нууц үгийг 16-тын тооллоор асуух байдлаар нууцлал хийдэг RC4 алгоритмыг ашигладаг хэдий ч нууц түлхүүрийн энгийн хэлбэр, радио долгионоор дамжуулж байгаа мэдээлэл дундаас чухал түлхүүр хэсгийг барих (man in the middle) болон бусад олон халдлагуудад өртөх боломжтой, зэргээс шалтгаалан харьцангуй хялбараар нууц үгийг тайлан сүлжээнд зөвшөөрөлгүй нэвтэрч болдог байна. Статик WEP key-н хэрэглээ утасгүй сүлжээний олон хэрэглэгчид урт хугацааны туршид ижил түлхүүрүүдийг хуваалцах нь сүлжээний нууцлалд халдах боломжийг олгодог нь бидний сайн мэдэх зүйл юм. Өнөө үед WEP-ийн түлхүүрийг програмын аргаар нээж илрүүлэх нь маш амархан болсон.

- RC4 алгоритм

RC4 нь одоогоор SSL/TLS (Secure Socket Layer/ Transport Layer Security) стандартад хэрэглэгдэж байгаа. Мөн IEEE 802.11 wireless LAN standard-д хэрэглэгдэж байгаа. RC4 Stream Cipher Algorithm нь дамжигдаж буй пакет бүр харгалзах түлхүүрээр RC4 алгоритмаар кодчилогдсон байдаг юм. RC4 түлхүүр нь Initialization Vector болон Root Key (хэрэглэгчийн нууц үг)-ийн нийлбэр байна.

Энэ нь хандалтын цэг нэг дурын сонгосон дуудлагаа боловсруулаад утасгүй хэрэглэгчрүү хариу багцыг илгээдэг. Хэрэглэгч нууц түлхүүр (cryptographic) ашиглан хандалтын цэг дээр байгаа дуудлагыг шифрлэн аваад, буцааж хандалтын цэгрүү үр дүнг нь явуулдаг. Хандалтын цэг нь кодыг нээж (decrypt) хэрэглэгчээс ирсэн үр дүнг тооцоолж үзээд хандалтын цэгийн дамжуулсан дурын дуудлага зөв бол хэрэглэгчийг сүлжээнд хандахыг зөвшөөрдөг. WEP нь зөвхөн 40 бит-н нууцлах түлхүүрийн хэмжээтэй. Хэдийгээр 40 бит хэмжээний нууцлах түлхүүртэй боловч стандарт бус хэмжээгээр 104 битийн хэмжээтэй нууцлах түлхүүрийг нийлүүлэгчид гаргадаг. 104 бит WEP түлхүүр нь 128 бит RC4 түлхүүрийн 24 бит-эхлэх вектор (initialization vector)-г авсан байдаг. Үндсэндээ нууц код (cryptographic)-н техникийн нууцлал нь түлхүүр үг нэмэгдэхэд сайжирдаг.Судалгаагаар үзүүлснээр 80 бит-н түлхүүрийн хэмжээтэй бол гүйцэтгэл болон сүлжээний дизайны бүтцийг хулгайчид код эвдлэн сүлжээнд халдах боломж нь багасаж бараг боломжгүй гэж үздэг. WEP-н сул тал халдлагад өртсөн байдал WEP-г идэвхжүүлсний дараа дамжигдаж байгаа packet дундаас нь Initialization Vector болон Root Key (хэрэглэгчийн нууц үг) 2-г мэдчихэд халдага хийхэд амархан болдог. Тэрээр зөвхөн өгөгдлийн багцуудыг хамгаалах ба физик үе давхаргын толгой мэдээллийн хэсгийг хамгаалдаггүй учир WEP protocol-оор дамжиж байгаа пакет (долгион) дотроос header-г олоод уншихад бүх зүйл бичигдсэн байдаг.Иймээс сүлжээний бусад станцууд сүлжээгээр дамжих мэдээллийн зориу- лалтыг харах боломжийг олгодог. WEP нь 40-бит, 128-бит болон 256-битийн урттай түлхүүр ашиглан утасгүй сүлжээнд төхөөрөмж холбогдох үед урьдчилан тохируулсан нууц үгийг 16-тын толлоор асуух байдлаар нууцлал хийдэг RC4 алгоритмыг ашигладаг хэдий ч нууц түлхүүрийн энгийн хэлбэр, радио долгионоор дамжуулж байгаа мэдээлэл дундаас чухал түлхүүр хэсгийг барих (man in the middle) болон бусад олон халдлагуудад өртөх боломжтой, зэргээс шалтгаалан харьцангуй хялбараар нууц үгийг тайлан сүлжээнд зөвшөөрөл- гүй нэвтэрч болдог байна. Статик WEP key-н хэрэглээ утасгүй сүлжээний олон хэрэглэгчид урт хугацааны туршид ижил түлхүүрүүдийг хуваалцах нь сүлжээний нууцлалд халдах боломжийг олгодог нь бидний сайн мэдэх зүйл юм. Өнөө үед WEP-ийн түлхүүрийг програмын аргаар нээж илэрүүлэх нь маш амархан болсон.

**WPA Wi-Fi Protected Access**

IEEE нь тусгай ажлын хэсэг байгуулан утасгүй сүлжээний стандартад оруулах шинэчилсэн нууцлалыг боловсруулсан бөгөөд 2003 онд IEEE 802.11i стандарт дээр нэмэлт өөрчлөлтөд оруулж WPA буюу Wi-Fi Protected Access нэрээр шинэ нууцлалын стандартыг гаргасан. WPA утасгүй сүлжээг найдвартай байлгах зорилготой аюулгүй байдлын протокол юм. WEP протокол төстэй гэхдээ wep-гийн сул талуудыг арилгахыг зорьсон байна. WPA нь TKIP (Temporal Key Integrity Protocol) агуулсан бөгөөд энэ нь өгөгдлийн бүрэн бүтэн байдал шалгалт, хуурамч үйлдлийг илрүүлэлт болон илрүүлсэн халдлагуудад хариулахад зориулсан мөн WEP-ийн ашигладаг үндсэн RC4 шифрт нэмэн өргөтгөсөн шифр юм. TKIP- IEEE 802.11 стандарт зориулсан нууцлалын протокол юм. WPA нь тодорхой хугацааны турш түлхүүр ашиглаж байгаад дараагийн хугацаанд шинэ түлхүүр ашиглаад явдаг.

- TKIP дээр 3-н төрлийн нууцлалын онцлог байдаг.

    1. Нууц үгээ хольж (mixing) дамжуулалт хийдэг.
    2. Янз бүрийн халдлага орж ирэхээс сэргийлдэг.
    3. Хэрэглэгчийн Mac хаяг болгонд өөр өөр түлхүүр тарааж өгдөг.

**WPA2 WiFi Protected Access** WPA2 нь WEP-ийн хаяглалтын асуудлыг шийдсэн. 802.11i стандартаас гаргаж ирсэн. Мөн WPA2 RC4 алгоритм ашигладаггүй.WPA-ийн TKIP нь хуучин тоног төхөөрөмж дээр зөвхөн програм хангамжийн өөрчлөлттэйгөөр ажиллахаар хийгдсэн, энэ нь аюулгүй байдлыг сайжруулдаг боловч халдлагаас бүрэн гүйцэд хамгаалж чаддаггүй. TKIP бас л тодорхой хэмжээний сул талтай, эрсдэлтэй байсан учир EAP (Extensible Authentication Protocol)г нэмж нэвтрүүлсэн байна. Хэдийгээр TKIP-г тайлж үзэж болж байгаа ч одоогоор нууц үгийг бүрэн тайлах арга нь арай олдоогүй байгаа. Их богинохон, хялбар үгээр WPA нууц үгээ хийсэн нөхцөлд программын аргаар хүчээр буюу brute-force дайралт хийн халдах боломж байдаг. WPA2 нь WPAгийн сайжруулсан хувилбар бөгөөд Wi-Fi Alliance-гийн гэрчилгээг шаардахаас гадна AES-CCMP (Advanced Encryption Standard Counter CBC-MAC Protocol) нэмснээрээ илүү сайн хамгаалалт болж чадсан бөгөөд боломжтой тохиолдолд үүнийг хэрэглэхийг урьтал болгодог. WPA2 нь өндөр нууцлалаар сайн хамгаалдаг хэдий ч хуучны зарим нэг зөөврийн компьютерийн сүлжээний карт нь нууцлалыг танихгүй байх тохиолдолтой. WPA, WPA2 нь Personal (эсвэл PSK буюу Pre-shared key) ба Enterprise гэсэн 2 янзын хувилбар байдаг.

- WPA-Personal

WPA-PSK нь бас WPA Personal гэгддэг бөгөөд өгөгдсөн нууц үгнээс үүсгэгдсэн pre-shared key буюу (PSK) урьдчилан хуваалцсан түлхүүр дээр суурилдаг бөгөөд утасгүй сүлжээнд мастер түлхүүр болон ашиглагддаг. Энэ нь утасгүй хэрэглэгч бүр адил түлхүүрийг хуваалцана гэсэн үг юм. WPA Personal хувилбарт 64 оронтой 16-тын тооллоор эсвэл 8-63 оронтой ASCII тэмдэгтээр оруулсан нууц үгийг өндөр түвшний нууцлалаар алгоритмаар тооцоолон 256битийн нууц түлхүүр болгох бөгөөд энэ нь утасгүй сүлжээгээр дамжиж байгаа мэдээллийн багц тус бүрийг нууцлахад хэрэглэгддэг байна.

- WPA-Enterprise

WPA-Enterprise хувилбар нь нууц үгийг хангах EAP (Extensible Authentication Protocol) өргөтгөсөн нэвтрэлт танилтын протокол, RADIUS сервертэй холбогдон ажилладаг бөгөөд томоохон байгууллагуудад хэрэглэгддэг. Энэ нь IEEE802.1X-д тодорхойлогдсон байдаг ба dynamic-WEP, WPA- Enterprise, WPA2- Enterprise протоколуудаар дамжигдах мэдээллээ шифрлэлт хийх боломжтой. EAP нь шифрлэлтийн аргагүй харин шифрлэгдсэн туннелийн дотор EAP-ийг суулгахаар шийдсэн байдаг.

# Бүлэг 4

# Хэрэгжүүлэлтийн хэсэг

# Бүлэг 5

# Хавсралт

# Номзүй