Mongolian Journal of Engineering and Applied Sciences, 2021, 3(1)

Мэдээлэл, харилцаа холбооны технологи

5G СҮЛЖЭЭН ДЭХ ТАРХСАН ХӨДӨЛГӨӨНТ БАЙДЛЫН УДИРДЛАГАД ЗОРИУЛСАН ХЭРЭГЛЭГЧИЙН БАТАЛГААЖУУЛАХ МЕХАНИЗМТАЙ ХЭНДОВР

Д.Шүхэрт, Д.Баттулга, Б.Өсөхбаяр*

МУИС,ХШУИС, Электроник, Холбооны Инженерчлэлийн Тэнхим

Received on 2021.04.13; Revised on 2021.07.05; Accepted on 2021.07.05

*Холбоо баригч зохиогч: usukhbayar@seas.num.edu.mn.

Хураангуй

Мобайл сүлжээний үндсэн үүрэг нь яриа дамжуулахаас өгөгдөл дамжуулах болон өөрчлөгдөж байна. 5G сүлжээ нь хөдөлгөөнт хэрэглэгчийг өндөр хурдны интернетээр хангах үндсэн зорилготой юм. Тэгвэл мобайл сүлжээнд хэрэглэгчийн хөдөлгөөнийг хянах үүрэгтэй нэгж нь интернет үйлчилгээний тасралтгүй, найдвартай байдлыг хангах чухал үүрэгтэй юм. 5G сүлжээний стандартад тархсан хөдөлгөөнт байдлын удирдлага багтсан боловч хэрэглэгчийн баталгаажуулах механизмгүйгээрээ сул талтай байна. Энэхүү судалгааны ажлаар бид хөдөлгөөнт байдлын удирдлагад хэрэглэгчийг баталгаажуулахад хэш функц ашиглах сайжруулалт хийснээ танилцуулсан. Энэхүү хэрэглэгчийг баталгаажуулах үйлдэл нь сүлжээн дэх системийн түвшний халдлагуудаас хамгаалах үндсэн зорилготой юм. Мөн энэхүү ажлаараа туршилтын орчин зохион байгуулж санал болгож байгаа сайжруулалт болон боломжит баталгаажуулалтын шийдлүүдтэй харьцуулалт хийж үр дүнг тайлагнав. Үр дүнгээс, бидний сайжруулалт хэндоврын хоцролтыг ихэсгэх боловч пакетын алдагдал багасгаж, хөнөөлт анкөртай үед алдаа бага гаргаж байгаа сайн талтай байна.

Түлхүүр үг: 5G, mobility management, handover, authentication.

1 Удиртгал

2020 оноос эхлэн Хөдөлгөөнт Холбооны 5 дахь үе (5G)-ийн технологийг дэлхий дахин нэвтрүүлж эхлээд байгаа билээ. 5G сүлжээ нь өмнөх үеэсээ 10 дахин бага хоцролт, 3 дахин их спектр, 10 дахин их хурд, 100 дахин их трафикийн багтаамж зэрэг олон үзүүлэлтээрээ давуу юм. Мөн сүлжээний архитектурын хувьд өөрчлөлт ихээхэн гарсан билээ. Жишээ нь 5G сүлжээний үндсэн загвар нь олон төрлийн үүрнээс бүтэх ба тэр дундаа нягт байршсан жижиг үүрүүдээр сүлжээний хоцролтыг багасгах, хурдыг нэмэгдүүлэх, найдвартай байдлыг хангахаар бүтэцлэгдсэн [1, 2].

Нөгөө талд хөдөлгөөнт, үүрэн сүлжээний оператор компаниудад хэрэглэгчийн тооны өсөлт, тэдгээрийн үүсгэх их хэмжээний дата урсгал (мобайл төхөөрөмжөөр үүсгэгдсэн болон дамжуулагдаж байгаа), дохиоллын болон тохиргооны мессежүүдийн хэт ачаалал зэрэг томоохон сорилтууд тулгарч байгаа билээ [3]. Ирээдүйн сүлжээ нь дэлхий даяар өсөн нэмэгдэж байгаа интернэтийн хэрэглээг хангах, үүсэх ачааллыг даах зохицуулалтуудыг хийх хэрэгтэй юм. Хөдөлгөөнт холбооны систем нь 2023 он гэхэд доорх үзүүлэлтүүдийг хангах хэрэгтэй болж байна [3].

- 2018 оны байдлаар дэлхийн хүн амтай харьцуулахад интернэт хэрэглэгчийн тоо 55% байсан бол 2023 он гэхэд 66% болж өснө.
- нэг үүр дунджаар 2018 онд 13 Mbps байсан бол 2023 онд 43 Mbps болж өснө. Үүнд бүх технологиуд буюу 3G,4G,5G -ууд хамрагдана.
- 2023 он гэхэд интернэт холбогдсон төхөөрөмжүүдийн 45% нь мобайл төхөөрөмж болно.
- 2018 онд 5G сүлжээний хэрэглэгчийн эзлэх хувь 0% байсан бол 2023 онд мобайл хэрэглэгчдийн тоо 10.6% болно.

Интернэтийн хэрэглээ хурдацтай нэмэгдэж байгаатай хамт нийтийн сүлжээ ба тэдгээрийн флатпормуудад багтсан аппликейшнууд, шууд дамжуулагдаж байгаа мултимедиа өгөгдөл зэрэг их хэмжээний зурвасын өргөн шаардах үйлчилгээнүүд нэвтэрч байна. Нөгөө талаас нь харвал огцом нэмэгдэж байгаа хэрэглээ нь сүлжээний технологийн хөгжлийг хурдасгах түлхүүр юм. Энэ жишгээр программаар тодорхойлогддог сүлжээ (SDN), сүлжээний функцийн виртуалчлал (NVF), сүлжээний зах дахь тооцоолол (Edge computing), үүлэн тооцоолол (cloud computing), автомашинд зориулсан холбоо (V2X communication), сүлжээг хэрчих (Network Slicing) зэрэг технологиуд нэвтэрч интернэт сүлжээг илүү комцлекс болгож байна.

Хөдөлгөөнт холбооны систем буюу мобайл сүлжээ нь хэрэглэгчдээ чөлөөт хөдөлгөөн, залгаасгүй үйлчилгээний боломжтой болгодог учраас бусад утастай, утасгүй сүлжээнүүдээс давуу талтай. Энэ нь үндсэн 3 функцүүдийн ажиллагааны үр дүн юм. Эдгээр нь:

а) хэрэглэгчийн идэвхтэй байгаа үйлчилгээг тасалдуулахгүйгээр бааз станцууд хооронд шилжүүлэх хэндоврын менежмент,

б) хэрэглэгчийн байршлыг мөрдөж хадгалах байршлын менежмент

в) Логик байршил дээр үндэслэж хэрэглэгч рүү чиглэсэн дуудлага зэргийг чиглүүлэх трафик менежмент

Одоогоор бидний ашиглаж байгаа 4G сүлжээнд дээрх дурьдсан функцүүдийг хөдөлгөөнт байдлын удирдлагын нэгж (MME) төвлөрсөн архитектуртайгаар гүйцэтгэдэг [4]. Тэгвэл 5G сүлжээний стандартуудад [5] хандалт ба хөдөлгөөний удирдлагын функц (AMF) гэсэн функцийг MME-ийн үүргийг гүйцэтгүүлэхээр загварчлахдаа тархсан бүтцийг дэмждэг болгосон. Тархсан бүтцийн хувьд анх IETF-ийн стандартууд 4G сүлжээний гүйцэтгэлийг сайжруулах зорилгоор тодорхойлогдсон [6]. Тархсан бүтэц нь төвлөрсөн удирдлагын хамгийн том асуудал болох нэг цэгийн алдааг шийдэхээс гадна дохиоллын мессежийн хэт ачааллыг баланслах зэрэг давуу талтай. Мөн хөдөлгөөний удирдахад гол үүрэгтэй функцүүдийг сүлжээний захад ажиллуулж, хэрэглэгч ба систем хоорондох хоцролтыг багасгана.

5G сүлжээнд тархсан AMF удирдлага нь давуу тал бий болгох хэдий ч хэндовр менежментэд оролцогч сүлжээний нэгжүүдийг баталгаажуулах механизмгүйгээр тодорхойлж сүлжээний хоёрдугаар түвшний аюулгүй байдлын протоколуудад найдсан байна [7–9]. Тэгэхлээр AMF-ийн үйлдлүүд гүйцэтгэгддэг 3-р түвшин буюу системийн түвшинд олон төрлийн халдлагууд (DoS, impersonation, MNTM, malicious node)-аас хамгаалах аюулгүй байдлын протокол зайлшгүй шаардлагатай юм [10]. Жишээ нь session hijacking, denial of service, malicious MAG, malicious CMD зэрэг 2-р түвшинд бүрэн хамгаалж чадахгүй халдлагууд байна.

Одоогийн хэндовр менежментэд хэрэглэгчийг баталгаажуулах үйлдлийг нэмж сайжруулах нь сүлжээний гүйцэтгэлд нөлөөлж хоцролт ихсэх, радио хандалтын сүлжээний орчинд гарах алдаануудыг нэмэгдүүлнэ. Иймд ТХБУ-д аюулгүй байдлыг нэмэгдүүлэх хэдий ч үр ашигтай байдлыг бууруулахгүй байх хэрэгтэй юм.

Энэхүү өгүүллээрээ бид 5G сүлжээний орчинд хэндовр менежментийн аюулгүй байдлыг сайжруулах зорилгоор хэрэглэгчийн баталгаажуулах механизмыг тодорхойлсноо танилцуулах болно. Бидний санал болгосон механизм нь хэндовр менежментийн үйлдэлд оролцож байгаа сүлжээний нэгжүүдийг хэш утга ашиглан баталгаажуулалт хийнэ. Ингэхдээ хэндоврт оролцож байгаа үйлчилгээ үзүүлж буй анкор (S-AMF), шилжиж орохоор сонгогдсон анкор (T-AMF), хэрэглэгч (UE) гэсэн сүлжээний 3 нэгжүүдийг баталгаажуулах үйлдлийг сүлжээний гарцын төхөөрөмж дээр хэш утгуудыг тулгах аргаар хийнэ. Энэ нь сүлжээнд нэвтэрсэн хөнөөлт ба хуурмаг нэгжийн үйл ажиллагааг хязгаарлах, түүний хөнөөлийг урьдчилан хориглох зорилготой байна. Жишээ нь сүлжээнд халдагч нэвтэрч хар-нүх (бүх хүсэлтэд зөвшөөрсөн хариу өгдөг) хөнөөлт AMF үүсгэсэн гэвэл таних, баталгаажуулах үйлдлүүдийн тусламжтайгаар түүн рүү чиглэсэн хэндовр үйлдлийг таслан зогсоох боломжтой болно.

Энэхүү ажлын шинэлэг тал ба ач холбогдлыг дараах байдлаар тодорхойлов. Үүнд:

(1) Бид 5G сүлжээнд хэндовр хийж байх үед сүлжээний нэгжүүдийг баталгаажуулах аюулгүй байдлын нэмэлтийг загварчилсан.

(2) Санал болгож буй сайжруулалтаа шалгахын тулд туршилтын сүлжээ байгуулсан. Энэ сүлжээндээ тархсан AMF болон бусад шаардлагатай өөрчлөлтүүдийг сүлжээний нэгжүүдэд нэмж зохион байгуулсан.

(3) Дараа нь бид түгээмэл ашиглагдаж байгаа болон 5G -ийн стандартад багтсан хэрэглэгч/нэгжүүдийг баталгаажуулах аргуудтай өөрсдийн санал болгож буй үр ашигтай аюулгүй хэндоврoо харьцуулсан.

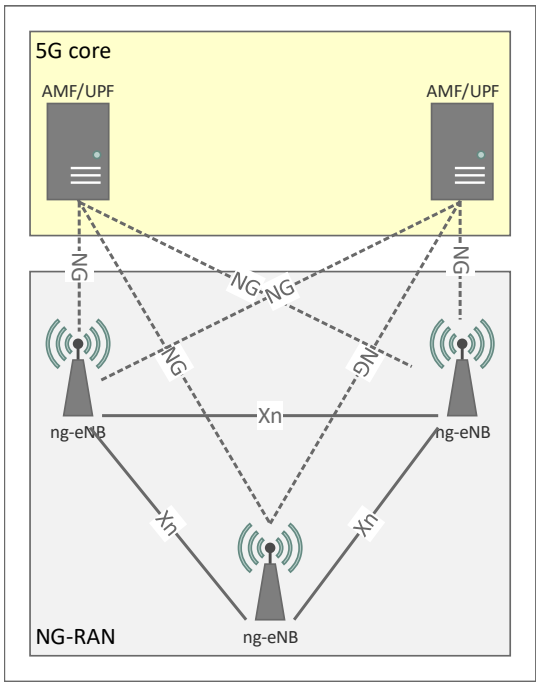
Энэхүү өгүүллийн бүтцийн хувьд хоёрдугаар бүлэгт хөдөлгөөнт байдлын удирдлагын тухай, гуравдугаар бүлэгт одоогийн системүүдэд хэрэглэгдэж байгаа хэрэглэгчийг баталгаажуулах механизмуудыг тайлбарлав. Дөрөвдүгээр бүлэгт бид санал болгож байгаа механизмаа дэлгэрэнгүй тайлбарлана. Тавдугаар бүлэгт туршилтын орчин ба үр дүнг танилцуулах бол дүгнэлтийг зургаадугаар бүлэгт бичив.

2 Суурь ойлголт ба судлагдсан байдал

2.1 Сүлжээний архитектур

Бид 5G сүлжээний орчинд тархсан AMF-уудтай үед хэндовр менежментийн аюулгүй байдлыг сайжруулах зорилгоор механизм хөгжүүлэх билээ. Зураг 1-д үзүүлсэн дангаараа ажиллах 5G сүлжээний ерөнхий зураглалыг үзүүлэв. Дангаараа ажиллах 5G гэдэг нь одоогийн 4G сүлжээнээс тусдаа ажиллах хөгжүүлэлтийн нэг хувилбар юм. Нөгөө талаас оператор компаниуд 5G сүлжээг бүрэн нэвтрүүлж 4G сүлжээгээ унтраасны дараах дангаараа ажиллах эцсийн хувилбар шийдэл юм.

5G сүлжээ AMF, SMF, UPF гэсэн 3 сүлжээний функц агуулах ёстой. Эдгээр дээр бид CMD гэсэн функцийг тархсан нэгжүүдийн хоорондын уялдааг хангах нэгдсэн сан байдлаар нэмж оруулсан. Ихэвчлэн эдгээр функцүүдийг суурь сүлжээ буюу сүлжээний төв хэсэгт байршуулдаг. Харин тархсан бүтцийг



Зураг 1: ТХБУ -тай 5G сүлжээний архитектур

бүрэн ажиллуулахын тулд бид боломжит функцүүдийг сүлжээний зах руу шилжүүлсэн. Бидний судалгааны ажил AMF-ийн үүрэг болох хэндовр менежментэд чиглэсэн.

- AMF нь хэрэглэгчийн сүлжээрүү хандах болон хөдөлгөөний удирдах үед хийх менежментийн үүргийг хүлээнэ. 5G сүлжээнд олон тооны AMF -ууд байрлуулах ба хэндовр хийх шаардлагатай гэж үзвэл хэрэглэгчийн холбогдсон байгаа $S-AMF$ нь шилжиж орох $T-AMF$ -ийг сонгох алгоритм ажиллуулна. Ингэж хэндов эхлэх бол хэрэглэгч $T-AMF$-тай холболт тогтооож, хэрэглэгчийн байршлын мэдээллийг шинэчлэснээр хэндовр дуусна.

- SMF нь сүлжээнд амжилттай нэвтэрсэн хэрэглэгчийн сейшнийг хадгалах, удирдах үүргийг хүлээнэ. Өөрөөр хэлбэл хэрэглэгч сүлжээнд анх холбогдох үед баталгаажуулалт болон бусад сүлжээний тохиргоо хийснийг сейшн байдлаар хадгалах сервер юм. Энэхүү сейшнийг ашиглаж хэрэглэгч сүлжээний гарцтай холбогдож оператороос үйлчилгээ авах, интернетэд гарах эрхтэй болно.

- UPF нь хэрэглэгчийн өгөгдлийн урсгалыг чиглүүлэх, дамжуулах үүргийг хүлээнэ. Хэрэглэгчээс оператор компаний үйлчилгээнүүд рүү эсвэл интернэт рүү холбогдох үед end-to-end логик зам үүсгэх, чиглүүлэх үйлдлүүдийг хийнэ. Хэрэглэгч рүү чиглэсэн ярианы дуудлага зэрэг мобайл сүлжээний үйлчилгээнүүдэд байршлын мэдээлэл дээр тулгуурлаж зам үүсгэх, чиглүүлэх үйлдлүүд хийнэ. Мөн хэндоврын үед хэрэглэгчийн байршил солигдоход өгөгдлийн замыг шинэчлэх, хэрэглэгчийн идэвхтэй байгаа трафикуудыг шинэ замаар дамжуулах үйлдлүүдийг хийнэ.

- CMD нь хэрэглэгчийн нэгдсэн мэдээллийн сан ба хэш утгуудыг тулгаж шалгах үндсэн үүрэгтэй.

2.2 Хэндовр Менежмент

Мобайл сүлжээний хэрэглэгч нь бааз станцууд хооронд идэвхтэй байгаа үйлчилгээгээ таслахгүйгээр шилжиж болдогоороо давуу билээ. Тэгвэл энэ процедурын цаана 4G сүлжээнд MME, 5G сүлжээнд AMF хянаж зохицуулах үйлдлийг хийдэг. Өөрөөр хэлбэл эдгээр функцүүд бааз станцууд хооронд шилжих хэндовр үйлдлийг удирдана.

Хэндоврт хэрэглэгч, түүний холбогдсон байгаа бааз станц, шилжиж орох бааз станц, гарц, MME гэсэн нэгжүүд оролцдог. Тэгвэл хэндоврын эхлүүлэх, шилжиж орох бааз станцыг сонгох гэх мэт үйлдлүүдийг аль нэгж ажиллуулж байгаагаас хамаарч хэрэглэгчид суурилсан (UE-based), сүлжээнд суурилсан (network-based) гэж хувилбарууд байдаг. Өнөөдрийн мобайл сүлжээнд ашиглаж байгаа хэрэглэгчид суурилсан төрлийн гол схем бол IETF (Internet Engineering Task Force) байгууллагаас хөгжүүлдэг Mobile IPv6 (MIPv6) юм [11]. Мөн MIPv6 болон түүний сайжруулсан хувилбарууд болох F-MIPv6, HMIPv6, F-HMIPv6 -ууд хэрэглэгчийн төхөөрөмжийг хөдөлгөөнтэй хамааралтай дохиоллын процесс буюу хэндоврын турш идэвхтэй байхыг шаарддаг байна [12–15]. Энэ төрлийн хэндоврын бааз станц сонгох гэх мэт үйлдлүүдийн дохиоллын мессежүүдийг сүлжээний нэгжүүдийн хооронд солилцоход хэрэглэгчийн төхөөрөмжийг голлох үүрэгтэй оролцуулдаг. Үүнээс үүдэж энэ төрлийн стандартуудыг өөрчлөх болон шинэчлэхэд төвөгтэй байдаг. Мөн хэрэглэгчийн төхөөрөмж тооцоолох олон үйлдэл гүйцэтгэснээр энерги зарцуулалт нэмэгдэнэ. Хэрэв хэрэглэгчийн төхөөрөмжийг шинэчлэвэл, хуучин сүлжээний төхөөрөмжүүд дэмжихгүй байх асуудал үүснэ. Нөгөө талаас сүлжээний операторт хэрэглэгчийн төхөөрөмжийг удирдах хэцүү болж радио хандалтын сүлжээний бааз станцтай холбогдох, бааз станцууд хоорондын уялдааг хангах, ачаалал тэнцвэржүүлэх гэх мэт чухал функцүүд ажиллах боломжгүй юм.

Сүлжээнд суурилсан хэндовр нь хэрэглэгчид суурилсан хэндоврын сул талыг нөхөж чадна. Энэ төрлийн гол схемүүд бол Proxy Mobile IPv6 (PMIPv6) ба Fast handovers for Mobile IPv6 (FPMIPv6) юм [16–18]. Эдгээр схемүүд хэрэглэгчийн төхөөрөмж дээр хийгддэг тооцоолол болон дохиоллын мессежүүд солилцох үйлдлээс боломжтой хэсгийг бааз станц руу шилжүүлсэн. Мөн эдгээр схемүүдийн гол давуу тал нь хэндоврийн хоцролт буюу хэрэглэгч нэг бааз станцаас холболтоо таслаад нөгөө бааз станцтай холболт тогтоох хугацааг богиносгодог [19]. Жишээ нь хэндоврын эхлүүлэх нөхцлийг шалгах, бааз станц сонгох үйлдлүүдийг хэрэглэгчийн холбогдсон бааз станц руу шилжүүлсэн. Хэндоврыг хийж дуу-

сах хүртэл хэрэглэгчийн дата урсгал гарцын төхөөрөмж дээр буфферлэгдэх ба хэндовр дуусахад дахин чиглүүлэгдэнэ.

Хэндоврыг гүйцэтгэх үедээ дохиоллын мессежүүдийн солилцож байгаа хэлбэрээр хоёр төрөл болгож хуваж болно. Эдгээр нь холбогдсон байгаа бааз станцаасаа холболтоо бүрэн салгаад шинэ рүү шилжих хатуу, шинэ бааз станц руу шилжсэний дараа хуучнаасаа холболтоо салгах зөөлөн хэндоврууд юм. Жишээ нь 3G сүлжээний хувьд зөөлөн хэндоврын голчлон ашиглаж байсан бол 4G сүлжээний стандартад зөвхөн сүлжээнд суурилсан хатуу хэндовр багтсан. Хатуу хэндоврын давуу тал нь хэрэглэгчийн идэвхтэй байгаа үйлчилгээг шилжин орж байгаа бааз станц руу тасалдалт багатайгаар шилжүүлэх юм. Тасалдалт ихэсвэл хэрэглэгчийн холболт салж үйлчилгээ тасалдана.

Хөдөлгөөнт байдлын удирдлагад хэндовр менежментээс гадна чухал функцүүд болох байршлын менежмент, чиглүүлэх менежмент гэсэн функцүүдийг харъялагдана. Байршлын менежмент хэрэглэгчийн төхөөрөмжийг баталгаажуулалт хийх үед холбогдсон үүрийн мэдээллийг цуглуулах ба хадгална. Ингэснээр тухайн хэрэглэгчийн сүлжээндэх байршил тодорхой болох ба энэхүү байршлыг ашиглаж хэрэглэгч рүү хийх дуудлагуудыг чиглүүлдэг. Сүлжээний менежмент нь хэрэглэгчийн трафикийг байршил дээр үндэслэн дамжуулах ба хэрэв байршил өөрлөгдвөл чиглүүлэлтийг дахин тохируулдаг. Тэгэхлээр хөдөлгөөнт байдлын удирдлагын үр дүнтэй байдал нь системд хийгдэж байгаа бүх хэндоврыг удирдах ачааллыг даах, хэндоврын турш хэрэглэгчийн датаг хадгалж дахин чиглүүлэх, хэрэглэгчийн идэвхтэй үйлчилгээнүүдийг алдаагүй шилжүүлэхээр тодорхойлогдоно.

2.3 Тархсан Хөдөлгөөнт Байдлын Удирдлага

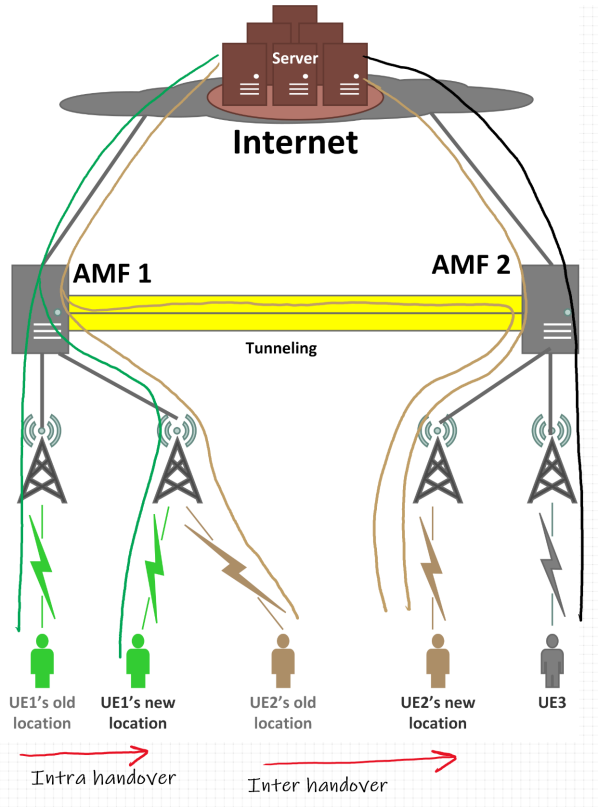
Төвлөрсөн хөдөлгөөнт байдлын удирдлагын функцүүд нь сүлжээнд өсөн нэмэгдэж байгаа хэт ачааллыг дийлэхгүй байх магадлалтай юм. Хэрэглэгчийн тоо болон тэдгээрийн хөдөлгөөнөөс үүсэх дохиоллын мессежүүдийн ачаалал нь төвлөрсөн удирдлага дээр бөглөрөл үүсгэнэ. Энэхүү бөглөрөл нь сүлжээний гүйцэтгэлд пакетын алдагдал, хоцролт ихсэх, байршлын менежментийн үйлдэл хийх хугацааг уртасгах зэргээр нөлөөлдөг [20]. Тархсан удирдлага нь хавтгай ба уян хатан архитектуртайгаараа нягт байршсан бааз станцууд бүхий 5G сүлжээний үндсэн хөдөлгөөнт байдлын удирдлагаар сонгогдсон [21].

Төвлөрсөн удирдлагын дутагдлаас зайлсхийх зорилгоор IETF байгууллагаас тархсан ХБУ (ТХБУ)-ийн стандартыг хөгжүүлсэн [22]. Тархсан шийдлийн үндсэн зорилго бол хөдөлгөөнт байдлын удирдлагын функцүүдийг сүлжээний зах буюу хандалтын сүлжээний чиглүүлэгч төхөөрөмж рүү шилжүүлж хэрэглэгчидтэй ойртуулах юм. Энэхүү хэрэглэгчийн хөдөлгөөнийг удирдаж чадах чиглүүлэгчийг сүлжээнд анкөр (зангуу) гэж нэрлэдэг. Өөрөөр хэлбэл чиглүүлэгч төхөөрөмж нь өөртэйгээ холбогдсон бааз станцуудын хоорондох дохиоллын мессежүүдийг зохицуулах, хэрэглэгчийн хөдөлгөөнийг удирдах, трафикийг чиглүүлэх зэргийг гүйцэтгэнэ. Анкөрт олон тооны хөрш бааз станцуудыг холбох ба үүнийг үйлчилгээний хамрах хүрээ гэнэ. Хэрэглэгч энэхүү үйлчилгээний хүрээ дотор бааз станцаа солих болвол тухайн анкөр удирдаж дотоод (Intra) хэндовр гүйцэтгэнэ. Харин үйлчилгээний хүрээнээс хэрэглэгч гарч өөр анкөрийн үйлчилгээний хүрээрүү орохоор болвол хоёр анкөрүүд хамтарч хоорондын (Inter) хэндовр гүйцэтгэдэг.

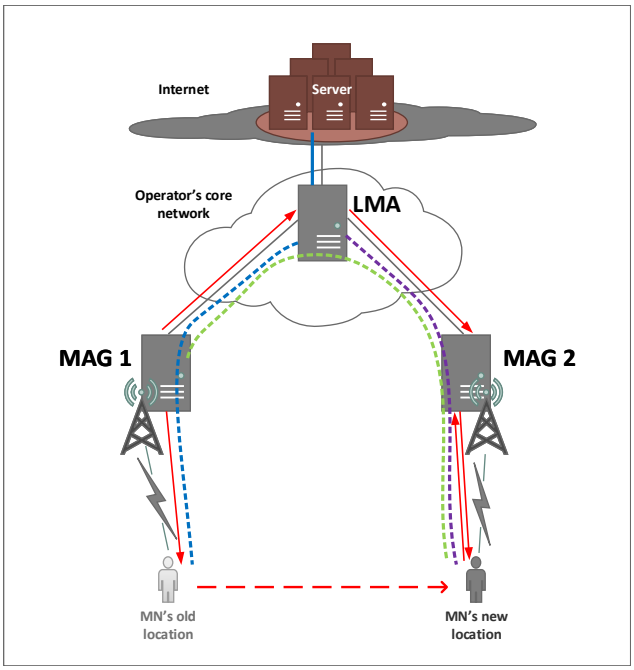
Зураг 2-д бид 5G сүлжээг тархсан AMF-тайгаар дүрслэв. Зургаас харвал флат архитектурт суурилж хандалтын сүлжээний хэсэгт анкөр ажиллаж байна. Анкөрүүд нь хэндовр, байршил, трафикийн менежментүүдийн үүргийг бие даан гүйцэтгэж чадна. Хэндовр менежментийн хувьд UE1-ийн дотоод хэндоврыг AMF1, UE2-ийн хоорондын хэндоврын AMF1 ба AMF2 хамтарч удирдаж байна. Мөн трафик менежментийн хувьд UE1-ийг AMF1, UE3-ийг AMF2 тус тус удирдаж байгаа бол UE2-ийнх AMF1-ээс AMF2-руу шилжиж байна.

Тархсан хөдөлгөөнт байдлын удирдлагын хөгжүүлэлтэд хагас тархсан ба бүрэн тархсан гэсэн хоёр хувилбар загвар байна [23]. Хагас тархсан хувилбар нь суурь сүлжээнд байрлах нэгдсэн өгөгдлийн сан руу бүх анкөрүүд хэрэглэгчийн талаарх мэдээллийг авах, шинэчлэх зэргээр хандаж байршлын менежментийг хэрэгжүүлдэг. Харин бүрэн тархсан хувилбар нь анкөрүүд тус тусдаа өөрийн өгөгдлийн санд хэрэглэгчийн байршлын талаарх мэдээллийг хадгалж, чиглүүлэлт хийдэг. PMIPv6 бол хагас тархсан хөдөлгөөнт байдлын удирдлагын нэг жишээ юм (Зураг 3). Local Mobility Anchor (LMA) гэсэн суурь сүлжээнд байрлах нэгж нь олон тооны Mobile Access Gateway (MAG)-уудад байршлыг менежментийг хэрэгжүүлэхэд мэдээллээр хангах үүрэгтэй юм. Мөн энэхүү нэгж MAG-уудаас интернэт рүү гарах гарцын үүрэг гүйцэтгэнэ.

5G сүлжээнд программаар тодорхойлогддог сүлжээг нэвтрүүлсэн, бүтэн ба хагас, хосолсон гэсэн тархсан хөдөлгөөнт байдлын удирдлагын шийдлүүдийг хөгжүүлж байна. Тархсан удирдлага болон PMIPv6 хоёрыг хослуулсан шийдлийг [24] -д санал болгосон. Энэхүү хосолсон шийдэл нь төвлөрсөн удидлагаар анкөруудын хооронд холбоо үүсгэж мэдээлэл солилцох боломжийг хангана. Харин [25, 26] -д, тархсан хөдөлгөөнт байдлын удирдлагын шийдэл нь хоёр шаталсан бүтэцтэйгээр танилцуулагдсан. Радио хандалтын сүлжээнд бааз станцууд хоорондох хөдөлгөөнийг дотоод буюу доод түвшний удирдлага хийнэ. Харин сүлжээний гарцуудыг дээд түвшний удирдлага гүйцэтгэнэ. [27]-д 5G-д програмаар тодорхойлогдох сүлжээг нэвтрүүлэх замаар тархсан удирдлагыг бий болгох шийдлийг танилцуулсан. Мөн [28,29]-д тархсан удирдлагыг SDN-ийн контролёр дээр аппликейшн сервер болгон байрлуулах шийдлийг санал болгосон. Энэ шийдлийн үр дүнд нь удирдлагын хэсгийг нарийн төвөгтэй байдлыг багасгаж хөдөлгөөнийг удирдах функцүүдийг сүлжээнийн үйлчилгээ хэлбэрээр ажиллуулс-



Зураг 2: Тархсан Хөдөлгөөнт Байдлын Удирдлага



Зураг 3: PMIPv6 ба төвлөрсөн ХБУ

наар дамжууллын болон хэндоврийн хоцролт зохицуулах боломжтой болгосон. [30]-д хөдөлгөөнтэй байдлыг дэмждэг шинэ протоколыг танилцуулсан. Энэ протокол нь хэрэглэгчид суурилсан тархсан удирдлага гэсэн шийдэл юм.

2.4 Тархсан Хөдөлгөөнт Байдлын Удирдлагын Эмзэг Байдал

Сүлжээнд халдагч нэвтэрч чадсан гэж үзье. Тэгвэл дараах халдлагууд үүсэх боломжтой болно. Үүнд:

- **man in the middle** дохиоллын мессежүүд нууцлал хийгдээгүй бол халдагч мессежийг хуулбарлаж авах ба түүнийгээ ашиглаж байболсон хэрэглэгчийн оронд сүлжээний үйлчилгээнүүд рүү хандах боломжтой болно. Үндсэндээ халдагч анкөр, хэрэглэгч хоорондын тогтоосон сейшнийг барьцаалж хэрэглэгчийн дүрд тоглох боломжтой болно.

- **malicious network information** хэрэв халдагч анкөрөөс хэрэглэгч рүү чиглэсэн чиглүүлэлтийн талаарх дохиоллын мессежид өөрчлөлт хийвэл бай хэрэглэгч сүлжээний буруу тохиргоо хийнэ. Өөрөөр хэлбэл халдагч сүлжээний тохиргоог өөрчлөх, буруу тохируулах зэргээр төөрөгдөл бий болгоно. Ингэснээр хэрэглэгч үйлчилгээ авч чадахгүй болно.

- **malicious anchor** халдагч анкөрийг хуурмаггаар үүсгэж хөдөлгөөнт байдлын удирдлагын бүх функцүүдийг ажиллуулах боломжтой болно. Ингэснээр хэрэглэгчийн талаарх бүх төрлийн мэдээллийг цуглуулж чадахаас гадна төвлөрсөн өгөгдлийн санд хандах боломжтой болно.

2.5 PMIPv6-д суурилсан ТХБУ -ийн аюулгүй байдал

Аюулгүй тархсан удирдлагыг хангахын тулд судлаачид дараах шийдлүүдийг санал болгосон. [7]-д трафикийг чиглүүлэх үйлдлийн аюулгүй байдлыг хангах болон оновчлолыг гүйцэтгэх протоколыг тархсан удирдлагатай үед зориулж санал болгосон. Энэхүү систем нь ухаалаг гэрийн системд зориулсан гэдгээрээ онцлог юм. Гэхдээ энэхүү шийдэл нь зөвхөн чиглүүлэлт ба түүний оновчлолыг гүйцэтгэхэд аюулгүй байдлыг хангахаар загварчилсан. Өөрөөр хэлбэл хэндовр эхлэх болон гүйцэтгэх алхмуудад аюулгүй байдлыг хангахгүй зөвхөн хэндовр дуусгах шатны дохиоллын мессежүүдийг хамгаалах юм.

[8] ба [10]-д PMIPv6-д суурилсан тархсан удирдлагад зориулсан хэрэглэгч баталгаажуулалтын протокол танилцуулсан. Энэ протокол нь хэрэглэгч болон анкөр хоороңд нууцлал хийх түлхүүрийг солилцох аргаар ID-д суурилж харилцан баталгаажуулалт хийнэ. Ингэснээр хэрэглэгч болон анкөр хоороңд аюулгүй холбоо үүснэ. Хэдий тийм боловч энэ протоколд дохиоллын мессежүүдийг солилцох дараалал нь энгийн байгаагаас хэрэглэгчийн хөдөлгөөний тухай мэдээллийг ашиглаж хөнөөлт анкөр бусад анкөрүүдийг хуурч чадах хэвээрээ байна. Мөн хэндовр гүйцэтгэж байхад хэрэглэгчийн сул талыг ашигласан халдлагад өртөх боломжтой ба анкөрөөр трафикийг дахин чиглүүлэх төрлийн халдлагад өртөх боломжтой байна. Хэрэглэгчийг халдлагад өртөмтгий болгож байгаа шалтгаан нь удаан хугацаанд өөрчлөлтгүй ашиглах ID ба түүнийг нууцлалгүйгээр дамжуулж байгаа явдал юм.

2.6 5G дэх EAP баталгаажуулалт

Extensible Authentication Protocol (EAP) бол сүлжээний аюулгүй байдлыг хангахад өргөн хэрэглэж байгаа фреймвөүкүүдийн нэг юм. Энэ фреймвөүк нь хэрэглэгчийн баталгаажуулах (authentication) үед тогтвортой байдал ба өргөтгөх боломж олгодгоороо давуу талтай юм. Сүлжээний нэгж бүрт EAP-ийг дэмжих функцийг ажиллуулснаар баталгаажуулах үйлдлүүдийг аюулгүй гүйцэтгэнэ. 5G-ийн стандартад EAP фреймвөүкийг багтаасан нь аюулгүй байдлыг хангах суурь болгон хэрэглэх нэг шалтгаан юм [31].

3 Хэрэглэгч Баталгаажуулах Механизмтай Хэндовр

Энэ бүлэгт бид санал болгож буй хэрэглэгч баталгаажуулах механизмтай хэндоврын тухай хоёр дэд бүлэгт хувааж тайлбарлах болно. Эхний дэд бүлэгт бид хэндоврыг гүйцэтгэхэд сүлжээний нэгжүүдийн оролцоо, хоорондоо солилцох дохиоллын мессежний блок-схемийг танилцуулна. Хоёрдахь дэд бүлэгт хэрэглэгчийг баталгаажуулахад ашиглагдаж байгаа хэш функийн талаар тайлбарлах болно.

3.1 Хэндовр Менежмент

5G сүлжээнд тархсан AMF-уудтай болсоноор хэндоврыг бааз станцууд хоорондоо, анкөрүүд хоорондоо гүйцэтгэнэ. Өмнөх бүлгүүдэд тайлбарласнаар эдгээр нь анкөр дотоод ба анкөрүүд хоорондын хэндовр гэж үзэж болно. Бидний судалгааны хүрээнд анкөрүүд хоороңд буюу хэрэглэгч нэг анкөрийн үйлчлэх хүрээнээс гарч нөгөөгийнх рүү шилжих шаардлагатай болох үед гүйцэтгэх хэндовр менежментийг авч үзнэ. Бидний гол зорилго бол хэрэглэгч MN ба AMF-уудийг хөнөөлт буюу халдлага үйлдэгч биш гэдгийг батлах юм. Өөрөөр хэлбэл MN -д шилжиж орох анкөр $T-AMF$-ийг, $T-AMF$-д MN ба $S-AMF$-уудыг жинхэнэ гэж батлах хэрэгтэй.

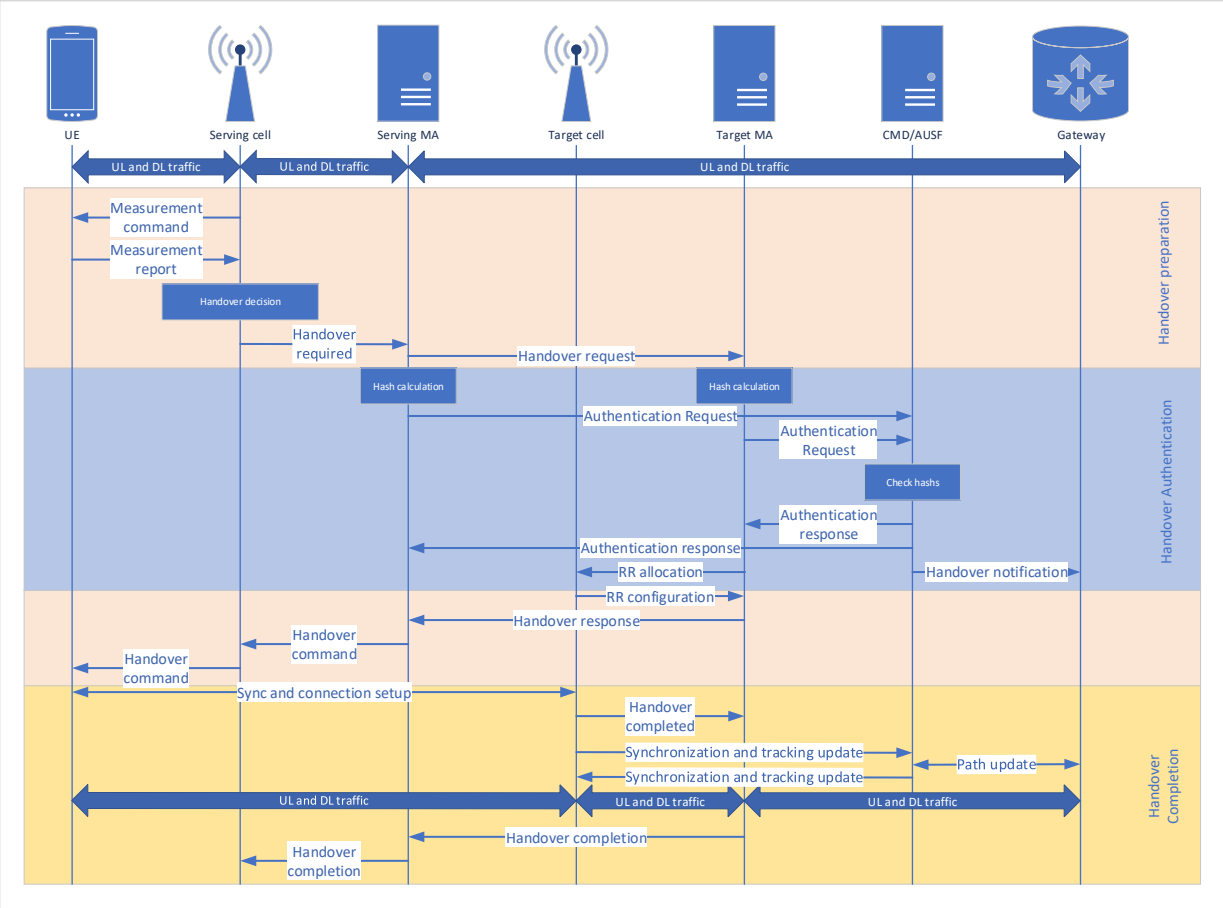
Эдгээр баталгаажуулалтыг удирдах боломжтой нэгж нь сүлжээний гарцын төхөөрөмж буюу тархсан удирдлагад зориулсан нэгдсэн өгөгдлийн санг ажиллуулж буй сервер CMD юм. Иймд бид хэндоврт оролцож буй сүлжээний нэгжүүд болох MN, $T-AMF$, $S-AMF$ -уудад хадгалагдаж байгаа түлхүүрүүдээр хэш утгуудыг үүсгэж, CMD -ийн тусламжтайгаар тэдгээрийг хянах үйлдлүүдийг хэндовр менежментэд нэмсэн. Бидний санал болгож байгаа сайжруулсан хэндовр менежментийг Зураг 4-д үзүүлэв.

Зурагт бид цэнхэр суурьтайгаар хэрэглэгчийн баталгаажуулалт хийж байгаа хэндовр менежментэд нэмсэн хэсгийг дүрсэлсэн болно. Энэ хэсгээрээ бидний санал болгож байгаа хэндовр нь уламжлалтаас ялгаатай юм. Аливаа хэрэглэгч нь оператор компаниас авсан сим карт дээрх мэдээллийн дагуу тохиргоо хийж сүлжээнд холбогдох, анхдагч баталгаажуулах үйлдлүүдийг хийсэн байдаг. Уламжлалт хэндоврын дундуур баталгаажуулалт хийдэггүй сул талтай. Тэгэхлээр бид хэндовр менежментээс өмнө хэрэглэгч сүлжээнд анх холбогдох үед дараах үйлдлүүдийг урьдчилан хийсэн гэж үзнэ. Үүнд:

- Хэрэглэгчийг анх сүлжээнд холбогдох үед баталгаажуулна.
- Хэрэглэгчийг баталгаажуулах үед түүний холбогдож байгаа AMF -ийг давхар баталгаажуулсан.
- MN, AMF-үүд, $AUSF$, CMD гэсэн сүлжээний нэгжүүд хугацааны синхрончлол хийсэн.
- CMD дээр хэш функцийн түлхүүрүүдийг үүсгэж MN, AMF-уудруу аюулгүй сувгаар дамжуулагдсан.

Бид Зураг 4-д дүрсэлсэн аюулгүй хэндоврт сүлжээний нэгжүүд дээр болон тэдгээрийн хоороңд дамжуулагдаж байгаа мессежүүдийг дараах байдлаар нарийвчлан тайлбарлав.

1. Хэрэглэгч MN нь $S-AMF$ -тэй $Cell_{serving}$ дээгүүр дамжиж холбогдсон байна.
2. $Cell_{serving}$ нь MN -ийн радио дохионы чанарыг байнга хянах ба зааж өгсөн түвшнээс доошлох үед (хэрэглэгч үүрийн зах руу ойртох үед)



Зураг 4: Санал болгож буй хэндовр менежментийн мессежүүдийн дараалал

Measurement command мессежийг хэрэглэгч рүү илгээнэ.

3. Хэмжилт хийх коммандыг хэрэглэгч хүлээн авааД радио дохио/орчны хэмжилт хийнэ. Хариулт болгож $Cell_{serving}$ -рүү *Measurement report* мессежийг илгээнэ. Энэхүү хариултад хэрэглэгчийн төхөөрөмжийн тухайн байршилд байх бааз станцуудын мэдээлэл, хэрэглэгчийн түлхүүр (анх сүлжээнд холбогдоход CMD-ээс авсан) байна.

4. $Cell_{serving}$ нь хэрэглэгчийг хэндовр хийх шаардлагатай эсэхийг "Event A3"нөхцлийг ашиглаж шалгана. Хэрэв хэрэглэгч хэндовр хийх шаардлагатай бол сонгогдсон үүр $Cell_{target}$ эсвэл $T-AMF$-руу хүсэлт илгээх ёстой. Хэрэв хэрэглэгчийн хэндовр хийж шилжиж орох үүр $Cell_{target}$ нь $S-AMF$-тэй холбогдсон бол ямар нэгэн баталгаажуулалт хийх шаардлагагүй юм. Харин $Cell_{target}$ нь $S-AMF$-ийн үйлчилгээний хүрээнээс гадна ба $T-AMF$-д холбогдсон бол $S-AMF$-ээс анкөр хоорондын хэндовр эхлүүлнэ. Бидний зорилго анкөр хооронд хийх хэндоврт чиглэсэн учир дараагийн алхамууд энэ төрлийн хэндоврынх байна.

5. Хэндовр шаардлагатай үед $S-AMF$ өөрийн болон хэрэглэгчийн хэш утгуудыг тооцоолно.

6. Дараа нь $S-AMF$-ээс $T-AMF$-руу *Handover request* гэсэн хүсэлтийг илгээнэ.

7. *Handover request* мессежийг хүлээж авсан $T-AMF$ нь өөрийн хэш утыг тооцоолно.

8. Дараа нь $S-AMF$-аас ирсэн HM_2 -ийг шалгана.

9. $S-AMF$ болон $T-AMF$-ууд өөрсдийн хэш утгуудаа $CMD/AUSF$ -руу *Authentication request* мессеж ашиглаж илгээнэ.

10. Хэш утгуудыг хүлээн авсан $CMD/AUSF$ нь өөрт байх түлхүүрүүдийг ашиглаж MN, $S-AMF$, $T-AMF$ тус бүрийн хэш утгуудыг тооцоолох ба ирсэн утгуудтай харьцуулна.

11. Хэрэв харьцуулалт амжилттай болж хэш утгууд ижил байвал $CMD/AUSF$-ээс $S-AMF$ болон $T-AMF$-руу *Authentication response* мессежийг илгээнэ. Энэхүү мессеж нь $S-AMF$-д $T-AMF$-ийг, $T-AMF$-д $S-AMF$-ийг тус тус баталгаажуулсан буюу хөнөөлт анкер биш гэсэн утгатай байна.

12. Дараа нь $T-AMF$ нь $Cell_{target}$-рүү хэндовр хийж орж ирэх хэрэглэгчид зориулж радио нөөцийн хүсэлт илгээж хариултад тохиргоо хүлээн авна.

13. $S-AMF$ дээр $CMD/AUSF$-ээс баталгаажуулсан мессеж, $T-AMF$-аас
Handover response мессеж ирсний дараа $Cell_{serving}$-ээр дамжуулж хэрэглэгчрүү *Handover command* мессежийг илгээнэ. Энэхүү *Handover command* мессеж нь $Cell_{target}$-тэй холболт тогтооход шаардлагатай тохиргооны мэдээлэл багтана.

14. Хэрэглэгч $Cell_{serving}$-ээс холболтоо салгаж $Cell_{target}$-руу холболт тогтооно.

15. $Cell_{target}$ нь хэрэглэгч өөртэй нь амжилттай холбогдсоны дараа $T-AMF$-руу хэндовр амжилттай дууссан тухай *Handover completed* мессежийг илгээнэ.

16. Дараа нь $Cell_{target}$-ээс CMD-тэй хэрэглэгчийн байршил болон өгөгдлийн замыг шинэчлэх харилцан мессежүүдийг солилцоно.

17. CMD нь *Gateway* -д хэрэглэгчийн өгөгдлийн замыг шинэчлэх мессежүүд солилцоно.

18. Өгөгдлийн зам шинэчлэгдсэний дараа $T-AMF$-аас $S-AMF$-руу хэндовр амжилттай дууссан тухай *Handover completion* мессежийг илгээнэ.

19. Дараа нь $S-AMF$-аас $Cell_{serving}$-руу хэрэглэгчийн хэрэглэж байсан радио нөөцийг чөлөөлөх комманд илгээж хэндовр төгсөнө.

3.2 Хэш функцийн тооцоолол

$S-AMF$ болон $T-AMF$-ууд $CMD/AUSF$-руу баталгаажуулалт хийлгэхээ хүсэлт илгээхдээ тус бүрдээ тооцоолсон хэш утгуудаас гадна хэрэглэгч болон хоёр анкөрүүдийн танигчууд, хугацааны цонх, тухайн хэрэглэгчийн хэндоврт зориулсан түлхүүр зэргийг илгээнэ. Харин тэдгээрийн түлхүүрүүд $CMD/AUSF$ дээр хадгалагдаж байдаг. Эдгээр ирсэн мэдээлэл, $CMD/AUSF$ дээрх түлхүүрийдийг ашиглаж $S-AMF$ болон $T-AMF$-ийн хэшүүдийг тооцоолж олно. Дараа нь $S-AMF$ болон $T-AMF$-аас ирсэн хэшүүдтэй тулгаж шалгана.

3.2.1 $S-AMF$ дээрх хэш тооцоолол

Хэндовр эхлэхээс өмнө $S-AMF$ нь $AID_{serving}$-ийг хадгалж байна. Хэрэглэгч анх сүлжээнд холбогдох үед түлхүүр K_{S-AMF}-ийг хэндоврт зориулж үүсгэнэ. $S-AMF$-аас илгээх хэндовр хүсэлтэд ID_{MN}, ts_1, K_{S-AMF}-уудыг агуулна.

Тооцоолол хийхэд дараах түлхүүр, танигчуудыг ашиглана. Үүнд:

- $AID_{serving}$ - $S-AMF$-ийн танигч
- AID_{target} - $T-AMF$-ийн танигч.
- ID_{MN} - хэрэглэгчийн танигч.
- K_{S-AMF} - хэрэглэгч $S-AMF$-тэй анх холбогдох үед хэндоврт зориулж үүсгэсэн түлхүүр.
- K_{CMD} - хэрэглэгчид $CMD/AUSF$-аас өгсөн түлхүүр.
- ts_1 - тухайн хэндовр хийж байгаа хугацааны цонх.

Доорх томъёоны дагуу хэш утгыг тооцоолж олно 1.

$$HM_S = HMAC(K_{CMD}, ID_{MN} \mid\mid AID_{S-AMF}) \mid\mid ts_1) \quad (1)$$

3.2.2 $T-AMF$ дээрх хэш тооцоолол

$T-AMF$ дээр ирсэн хэндовр хүсэлтэд агуулагдах мэдээлэл дээр тулгуурлан Томъёо 2 -ийг ашиглаж хэш утгыг тооцоолон олох ба $CMD/AUSF$-руу илгээнэ.

$$HM_T = HMAC(K_S, ID_{MN} \mid\mid AID_{T-AMF}) \mid\mid ts_1) \quad (2)$$

Хэрэв хэндовр амжилттай болвол $T-AMF$ нь хэрэглэгчид зориулж K_{T-AMF} хэндовр түлхүүрийг үүсгэнэ.

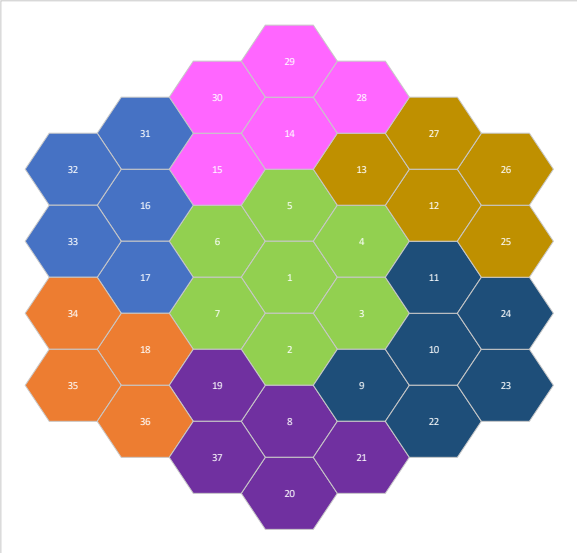
4 Туршилт ба Үр Дүн

Энэ хэсэгт бид санал болгож буй шийдлээ туршилтын орчинд EAP-д суурилсан баталгаажуулалтын арга болон баталгаажуулалт хийхгүй байх гэсэн хоёр шийдэлтэй харьцуулалт хийсэн үр дүнгээ танилцуулах болно. EAP-д суурилсан арга нь энэхүү протоколын хэрэглэгчийг анх нэвтрэх үед хийгддэг баталгаажуулалтыг хэндоврт шууд ашиглах хувилбар юм [32].

4.1 Туршилтын орчин

Бид туршилтын сүлжээ (Зураг 5)-ийг нээлттэй эхийн NS3 симулятар ашиглаж байгуулсан. Бааз станцууд болон анкөрүүдэд хоорондоо мэдээлэл солилцох зориулалттай функц нэмсэн.

Туршилтын сүлжээ нь 37 бааз станц, 7 анкер буюу AMF, нэг төвлөрсөн сан буюу $CMD/AUSF$, интернэтийн нэг гарц гэсэн нийт 46 сүлжээний нэгж болон тэдгээрийн холбосон холболтын төхөөрөмжүүдээс бүрдэнэ. Зураг 5-д өнгөөр ялгаж үзүүлсэнчлэн 7 анкер тус бүрийн үйлчилгээний хүрээнд бааз станцуудыг хамруулсан. Радио хандалтын сүлжээг байгуулахдаа 3GPP-ийн 15 болон 16 гэсэн стандартуутыг ашигласан. Туршилтанд ашигласан параметрүүдийг Хүснэгт 1-д үзүүлэв. Туршилт эхлэхэд хэрэглэгчдийг тоо, байршлыг санамсаргүйгээр сонгох ба хамгийн ойр байх бааз станцаар дамжиж анкеруу бүртгүүлнэ. Улмаар төвлөрсөн сан болон хэрэглэгчийг нэвтрэх зөвшөөрөл өгөх үйлдүүдийг стандартын дагуу хийж гүйцэтгэнэ. Туршилтын турш хэрэглэгч тогтмол хурдтай хөдөлж байнга идэвхтэй өгөгдөл дамжуулна. Бид хэрэглэгчийн хурдыг 3



Зураг 5: Туршилтын сүлжээний топологи

Параметрүүд	**Утга**
Зөөгч давтамж	1800 MHz
үүрийн тоо	37
үүрийн хэмжээ	1 км
Замын алдагдлын загвар	128.1+37.6log10d
Shadow fading гажилт	2dB
$AMFs$-уудын тоо	7
Хэндовр хийх давхцах талбай	үүрийн хэмжээний 30%
MNs-үүдийн тоо	1000 хүртэл
MNs-ийн хөдөлгөөний хурд	3km/h - 80km/h

Хүснэгт 1: Туршилтын параметрүүд.

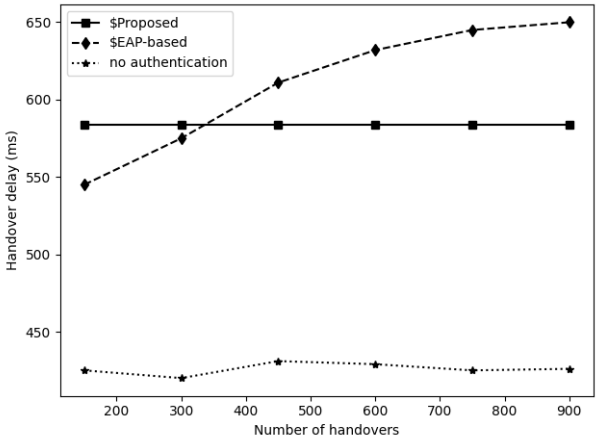
км/ц-аас 80км/ц-ийн хооронд санамсаргүйгээр сонгохоор тохируулсан болно. Туршилтын турш хэрэглэгчид ярианы дуудлага үйлчилгээг гарцын төхөөрөмжийн цаана байрлах сервертэй байнга идэвхтэй ашиглана. Сүлжээний аливаа нэгж дээр ирсэн дуудлагуудыг FIFO алгоритм ашиглаж дараалалд байршуулахаар тохируулсан.

4.2 Туршилтын үр дүн

Туршилтаа бид 20 удаа давтан хийсэн ба баталгаажуулалтын хоцролт, хэндоврын хоцролт, хэндовр хийх үед алдагдсан пакет, баталгаажуулалт хийж байх үед гарсан бусад алдаа гэсэн 4 үзүүлэлтийг тус бүрт дунджаар тооцоолсон.

4.2.1 Хэндоврын хоцролт

Хэндоврын хоцролт нь хэрэглэгчийн идэвхтэй үйлчилгээнүүдэд нөлөөлдөг чухал үзүүлэлт юм. Иймд бид туршилтын үр дүнгүүдээс хэндовр хийх үе дэх хэрэглэгчийн үйлчилгээний тасалдалтыг хэмжсэн. Хэмжихдээ хэрэглэгч хуучин анкераар дамжуулж авсан сүүлийн пакетийн ирсэн хугацаа, шинэ анкераар дамжуулж авсан эхний пакетийн ирсэн хугацаа гэсэн 2 хугацааны ялгавраар илэрхийлсэн. Зураг 6 -д хэндоврын хоцролтыг хэндовр хийсэн тоотой харьцуулж үзүүлэв. Бидний санал болгосон схэм нь EAP-д суурилсан баталгаажуулалтын аргаас ялимгүй их байна. Энэ нь баталгаажуулах үйлдэлд нэмэгдсэн хэш утгыг тооцоолох, тулгаж шалгах зэрэг үйлдлүүдтэй шууд хамааралтай юм.



Зураг 6: Хэндоврын хоцролтын харьцуулалт.

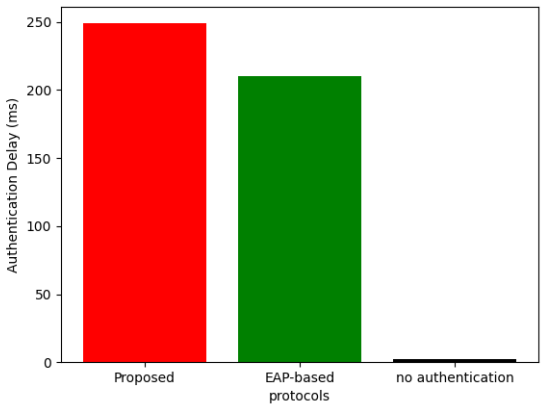
4.2.2 Баталгаажуулалтын хоцролт

Бид хэндоврын хоцролт дотроос баталгаажуулалт хийх мессежүүдийг солилцох, хэш утга бодох зэргээс үүдэн гарц байгаа хоцролт буюу баталгаажуулалтын хоцролтг Зураг 7 -д үзүүлэв. Зургаас харахад бидний санал болгож байгаа арга нь нөгөө 2-оос их байна. Мөн ямар нэгэн баталгаажуулалт хийхгүй байх үед хоцролт хамгийн бага байна. Ойролцоогоор 9 орчим милсекундыг зөвхөн хэрэглэгчийн өгөгдлийн замыг шинэчлэхэд зарцуулж байгаа хугацаа эзэлж байна. Харин EAP -д суурилсан аргын хувьд урьдчилан тараасан түлхүүрүүдийг шууд ашиглах, хэш утга бодохгүй ч дамжуулж байгаа мессежийн тоо, тэдгээрийн хэмжээнээс хамаарч хоцролт их гарч байна.

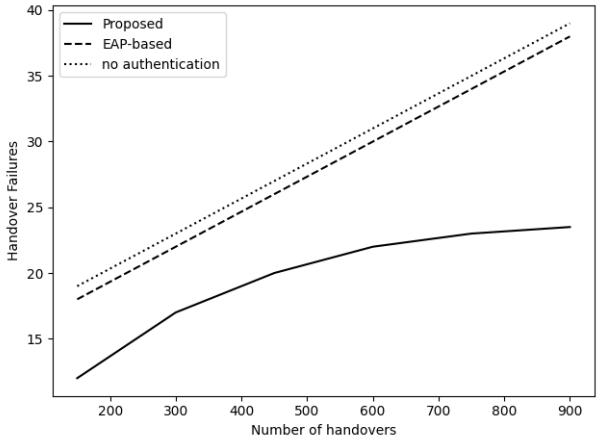
4.2.3 Баталгаажуулалтын үед гарсан алдаа

Бид зөвхөн баталгаажуулалт хийх үед гарч байгаа алдааны талаар Зураг 8-д үзүүлэв. Хэндовр хийх үед радио дохионоос хамаарсан алдаа болон системийн түвшинд дамжуулагдаж байгаа мессежүүд алдагдах зэрэг олон төрлийн алдаа гардаг. Тэдгээр дээр нэмээд хэрэглэгчийн өгөгдлийн замыг шинэчлэх үед алдаа гарч болно. Харин зурагт бид баталгаажуулах үйлдэл хийх үе дэх мессежүүдээс хамаарсан болон өгөгдлийн зам шинэчлэх үед гарсан алдаанууды ялгаж үзүүлсэн.

Туршилтын турш хийгдэж байгаа хэндоврууды шинжлэхэд баталгаажуулалт хийдэггүй болон EAP



Зураг 7: Баталгаажуулалт хийх үед үүсэх хоцролт.

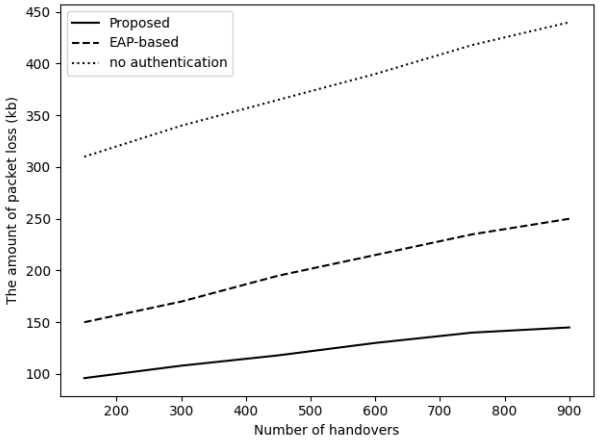


Зураг 8: Хэндовр хүсэлтийг бай зангуу татгалзсан байдал.

-д суурилсан аргуудыг хэндовр алдаа тогтмол өссөн үр дүн үзүүлсэн. Харин бидний санал болгож байгаа арга нь алдааг бага түвшинд хадгалж чадаж байна. Энэ нь баталгаажуулалтын эцсийн үр дүнг $CMD/AUSF$ дээр хийгдэж бүх нэгжид мэдэгдэж байгаагаар тайлбарлаж болно. Өөрөөр хэлбэл өгөгдөл дамжуулах, чиглүүлэх зэрэг үйлдлүүдийг давхар хариуцаж байгаа анкерууд дээр тооцоолол бага хийх, өгөгдлийн зам шинэчлэх гол нэгж дээр тооцоолол хийсэн зэрэг юм.

4.2.4 Пакет алдагдлын хэмжээ

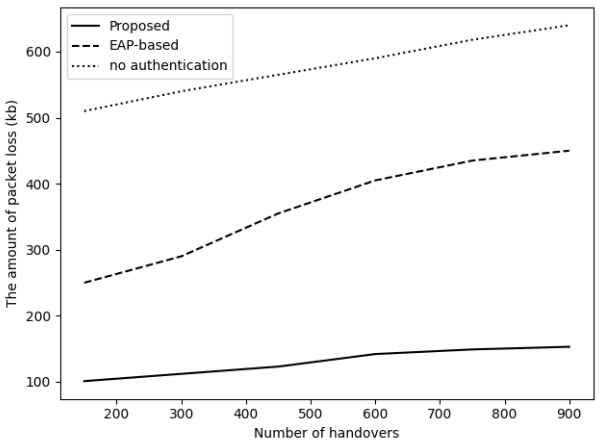
Зураг 9-д бид туршилтын үр дүнгүүдээс хэндовр хийх үед алдагдсан пакетуудын хэмжээг дундажлан үзүүлэв. Ингэхдээ гүйцэтгэсэн хэндоврын тоотой харьцуулав. Зургаас харвал хэндовр хийх үед баталгаажуулалт хийхгүй байх үеийн пакет алдагдал 300 -аас 440 хүртэл өссөн бол EAP -д суурилсан баталгаажуулалтын арга 150 -аас 250 хүртэл өссөн байна. Харин бидний санал болгож байгаа арга нь 100 -аас 145 хүртэл өссөн. Эндээс дүгнэвэл бидний санал болгосон арга нь хэндовр хийх үед пакетын алдагдал бага байна. Үүний шалтгаан нь хэндовр хийж байх үед гарах алдаа багасаж байгаатай холбоотой юм.



Зураг 9: Пакетын алдагдал ба гүйцэтгэсэн хэндоврын тоо.

4.2.5 Хөнөөлт анкертэй үеийн нөлөө

Бид хөнөөлт анкер буюу AMF -ийг нэмж туршилтаа давтан хийсэн үр дүнг Зураг 10-д үзүүлэв. Ингэхдээ бид хөнөөлт нэг анкерийг сүлжээний дурын байршилд байрлуулж ойр орших 7 үүрнээс ирэх хэндовр хүсэлтийг хүлээн авах боловч хариу өгөхгүй байхаар програмчлав. Энэ нь хэндоврын хүсэлтийг гээгдүүлж, хэндовр амжилтгүй болох магадлалыг ихэсгэх юм. Зураг 10-ийг Зураг 9-д харьцуулж харвал бидний санал болгосон хэндоврын пакетын алдагдалд өөрчлөлт бага гарсан. Харин нөгөө хоёр аргын пакетын алдагдал ихээхэн нэмэгдсэн байна. Пакет алдагдал нэмэгдэж байгаа үндсэн шалтгаан нь хэндовр хүсэлтийг хөнөөлт анкер руу илгээж хариу хүлээснээр $Cell_{serving}$ дээр түр хадгалагдаж байгаа хэрэглэгчийн пакетууд хүлээлтийн хугацаа дуусаж устаж байгаа юм.



Зураг 10: Пакетын алдагдал ба хөнөөлт анкер.

5 Дүгнэлт

Энэхүү судалгааны ажлаар бид 5G сүлжээнийн орчинд тархсан удирдлагатай үед хэндовр менежментэд баталгаажуулалтыг хангах зорилготой нэмэлт хийв. Өөрсдийн нэмэлтийг шалгах зорилгоор туршилтын орчин зохион байгуулж, санал болгож байгаа өөрчлөлттэй хэндовр, EAP -д суурилсан хэндовр, баталгаажуулалт хийдэггүй хэндовр гэсэн 3 төрлийн зохиомжилж туршив. Туршилтын үр дүнд бидний санал болгосон арга нь хоцрогдлыг тодорхой хэмжээгээр нэмэгдүүлэх боловч хэндовр хийх үед баталгаажуулалтаас хамаарч гарах алдааг багасгаж, хөнөөлт анкер нэмэхэд нөлөө багатай байсан давуу талуудыг үзүүлсэн. Бидний цаашдын ажил бол туршилтын орчинд халдлагуудыг зохиомжлох, тэдгээрийн эсрэг үзүүлж байгаа нөлөөг судалж өөрсдийн аргаа сайжруулах юм.

Зохиогчийн оролцоо

Д.Шүхэрт туршилтын орчин зохион байгуулж, санал болгож байгаа сайжруулалт болон боломжит баталгаажуулалтын шийдлүүдтэй харьцуулалт хийж үр дүнг боловсруулсан. Д.Баттулга, Б.Өсөхбаяр нар 5G сүлжээнийн орчинд тархсан удирдлагатай үед хэндовр менежментэд баталгаажуулалтыг хангах зорилготой нэмэлтийг боловсруулсан. Д.Шүхэрт, Д.Баттулга, Б.Өсөхбаяр нар өгүүллийг засаж сайжруулах, утга агуулгын алдааг хянаж, өгүүллийн сүүлчийн хувилбарыг бичсэн.

Ашиг сонирхлын зөрчилгүйн баталгаа

Зохиогчид ашиг сонирхолын зөрчилгүй гэдгээ баталж байна.

Ашигласан ном

[1] Hu RQ, Qian Y. An energy efficient and spectrum efficient wireless heterogeneous network framework for 5G systems. IEEE Communications Magazine. 2014;52(5):94–101.

[2] Ge X, Tu S, Mao G, Wang C, Han T. 5G Ultra-Dense Cellular Networks. IEEE Wireless Communications. 2016;23(1):72–79.

[3] Cisco U. Cisco annual internet report (2018–2023) white paper; 2020.

[4] Choi YJ, Lee KB, Bahk S. All-IP 4G network architecture for efficient mobility and resource management. IEEE wireless communications. 2007;14(2):42–46.

[5] Zhang X, Kunz A, Schröder S. Overview of 5G security in 3GPP. In: 2017 IEEE conference on standards for communications and networking (CSCN). IEEE; 2017. p. 181–186.

[6] Chan H, Liu D, Seite P, Yokota H, Korhonen J. Requirements for distributed mobility management. draft-ietf-dmm-requirements-16. 2014.

[7] Shin D, Yun K, Kim J, Astillo PV, Kim J, You I. A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. IEEE Access. 2019;7:142531–142550.

[8] Lee J. Secure authentication with dynamic tunneling in distributed IP mobility management. IEEE Wireless Communications. 2016;23(5):38–43.

[9] Dohyun Kim, Yongtae Shin. An enhanced security authentication mechanism in the environment partially distributed mobility management. In: 2017 International Conference on Information Networking (ICOIN); 2017. p. 457–462.

[10] Lee J, Bonnin J, Seite P, Chan HA. Distributed IP mobility management from the perspective of the IETF: motivations, requirements, approaches, comparison, and challenges. IEEE Wireless Communications. 2013;20(5):159–168.

[11] Johnson D, Perkins C, Arkko J, et al.. Mobility support in IPv6. RFC 3775, june; 2004.

[12] Perkins CE, Johnson DB. Mobility support in IPv6. In: Proceedings of the 2nd annual international conference on Mobile computing and networking; 1996. p. 27–37.

[13] Koodli R, et al. Fast handovers for mobile IPv6. RFC 4068, july; 2005.

[14] Soliman H, Castelluccia C, El Malki K, Bellier L. Hierarchical mobile IPv6 mobility management (HMIPv6). RFC 4140, august; 2005.

[15] Jung H, Kim E, Yi J, Lee H. A Scheme for Supporting Fast Handover in Hierarchical Mobile IPv6 Networks. ETRI Journal. 2005;27(6):798–801.

[16] Gundavelli S, Leung K, Devarapalli V, Chowdhury K, Patil B, et al. Proxy mobile ipv6. 2008.

[17] Schmidt T, Wählisch M, Krishnan S. Base deployment for multicast listener support in Proxy Mobile IPv6 (PMIPv6) Domains. IETF RFC6224, April. 2011.

[18] Yokota H, Chowdhury K, Koodli R, Patil B, Xia F. Fast handovers for proxy mobile IPv6. In: RFC 5949; 2010. .

[19] Sun K, Kim Y. Flow Mobility Management in PMIPv6-based DMM (Distributed Mobility Management) Networks. J Wirel Mob Networks Ubiquitous Comput Dependable Appl. 2014;5(4):120–127.

[20] Chan H, Liu D, Seite P, Yokota H, Korhonen J. Requirements for distributed mobility management. draft-ietf-dmm-requirements-16. 2014.

[21] Chan H. Problem statement for distributed and dynamic mobility management. Internet Draft, draft-chan-distributed-mobility-ps-00. 2010.

[22] Giust F, Cominardi L, Bernardos CJ. Distributed mobility management for future 5G networks: overview and analysis of existing approaches. IEEE Communications Magazine. 2015;53(1):142–149.

[23] Bertin P, Bonjour S, Bonnin J. A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures. In: 2008 New Technologies, Mobility and Security; 2008. p. 1–5.

[24] Lee J, Bonnin J, You I, Chung T. Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols. IEEE Transactions on Industrial Electronics. 2013;60(3):1077–1088.

[25] Nguyen TT, Bonnet C. A hybrid centralized-Distributed Mobility Management for supporting highly mobile users. In: 2015 IEEE International Conference on Communications (ICC). IEEE; 2015. p. 3945–3951.

[26] Nguyen TT, Bonnet C, Härri J. SDN-based distributed mobility management for 5G networks. 2016 IEEE Wireless Communications and Networking Conference. 2016:1–7.

[27] Ko H, Jang I, Lee J, Pack S, Lee G. SDN-based distributed mobility management for 5G. In: 2017 IEEE International Conference on Consumer Electronics (ICCE). IEEE; 2017. p. 116–117.

[28] Sanchez MI, De la Oliva A, Mancuso V. Experimental evaluation of an SDN-based distributed mobility management solution. In: Proceedings of the Workshop on Mobility in the Evolving Internet Architecture; 2016. p. 31–36.

[29] Valtulina L, Karimzadeh M, Karagiannis G, Heijenk G, Pras A. Performance evaluation of a SDN/OpenFlow-based Distributed Mobility Management (DMM) approach in virtualized LTE systems. In: 2014 IEEE Globecom Workshops (GC Wkshps). IEEE; 2014. p. 18–23.

[30] Lee JH, Bonnin J, Lagrange X. Host-based distributed mobility management support protocol for IPv6 mobile networks. 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). 2012:61–68.

[31] Chandramouli D, Liebhart R, Pirskanen J. 5G for the Connected World. John Wiley and Sons; 2019.

[32] Haddar W, Ameur SB, Zarai F. Securing Fast PMIPv6 protocol in case of Vertical HandOver in 5G network. In: 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC); 2019. p. 1037–1042.