Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai kar

Távközlési és Médiainformatikai Tanszék

LTE feletti beszédátvitel monitorozási módszerei a maghálózatban

Balog Zsolt

2016

Konzulensek: Dr. Varga Pál, Tóthfalusi Tamás

Tartalomjegyzék

Kivonat

A negyedik generációs mobilhálózat elterjedésével újabb fejlesztési igények merültek fel a mobiltelefónia képességeinek bővítésére és javítására. Manapság a sávszélesség növelése, az ultra-szélessávú szolgáltatások bővítése és a hangminőség javítása bizonyul fejlődési trendnek. Az LTE feletti beszédátvitel (Voice over LTE, VoLTE) megvalósítása számos előnyt nyújt a szolgáltatást igénybe vevő előfizetőknek. Magyarországon a jelenlegi 4G LTE hálózat tulajdonságait kizárólag az adatszolgáltatás terén használhatjuk ki. A letölteni kívánt adatcsomagokhoz a korábbiaknál nagyságrendekkel nagyobb sebességgel férhetünk hozzá, viszont az eközben beérkező hívás során leváltunk 3G, esetleg 2G hálózatra, mivel a beszédszolgáltatás 4G felett a dolgozat írásakor még nem nyilvános szolgáltatás. Az úgynevezett CS (Circuit Switched, áramkörkapcsolt) fallback során az új hálózat keresése időt és intenzívebb akkumulátor használatot vesz igénybe.

A VoLTE megvalósítása természetesen a jelzéshálózatban is új elemeket generál. A mobil entitások között új kapcsolatok létesülnek, ezáltal az üzenetek eddig nem ismert kommunikációt követve új paramétereket tartalmazhatnak. Egy VoLTE hívás alatt a jelzésüzenetek az LTE maghálózatából az IP feletti szolgáltatásokat vezérlő architektúrába (IP Multimedia Subsystem) jutnak, így különböző protokollokon keresztül követhetjük a hívás folyamatát. Egy komplexebb rendszerben a hibakeresés megoldása is nehezebb feladatnak ígérkezik. Az esetlegesen fellépő hibákat a szolgáltatók szeretnék a lehető leggyorsabban és legegyszerűbben megtalálni, erre a jelzésüzeneteket jól ismerő, monitorozó-rendszereket készítő beszállítók kínálhatják a legjobb megoldást.

E dolgozat az elvégzett VoLTE teszthívások során szerzett tapasztalatok alapján bemutatja a monitorozott jelzéshálózaton végzett hibakeresési és vizsgálati módszereket - a jelenlegi hálózati struktúrán már bizonyított monitorozó-rendszeren keresztül. Emellett a munkafolyamat automatizálására is ajánlást nyújt, még a technológia széles körű elterjedése előtt - így elkerülve az ismeretlen hibák okozta kezdeti problémákat.

Abstract

With the spread of the fourth generation mobile network, there is a general demand for further developments to expand and enhance the capabilities of mobile telephony. Nowadays, the increase of bandwidth, the extension of ultra-broadband services and the improvement of sound quality are the desired drivers for progression trends. Voice transmission over LTE (VoLTE) provides many benefits for its users. We can benefit from the advantages of LTE only in the field of data services in Hungary. We can access to the intended data to download with significantly higher speed than before. On the other hand, since the voice services over 4G have not been made available at the time of the present paper, the incoming calls make the device to switch down to 3G or 2G networks.

When the user's device is operating in LTE (data connection) mode and a call comes in, the LTE network pages the device. It falls back to 2G/3G to accept the incoming call, because voice over 4G service is not publicly available during the writing of this paper. The use of the so called CS fallback (Circuit Switched fallback) requires more time and intensive battery use by the searching of new network.

The actual implementation of the VoLTE service generates new elements and perspectives in the signalling network, as well. Between mobile entities, new connections are generated, and thus the messages contain new parameters through the monitoring of previously unknown communication interfaces. During a call over VoLTE, the signals and messages are travelling from the LTE core network to the IP Multimedia Subsystem. We can follow the call flow through different protocols with the help of a proper signalling monitoring system. In a more complex system the troubleshooting is an even more difficult task. Service providers intend to find a fast and simple way for the identification of potential failures. Those monitoring system suppliers who best understand the requirements and obstacles are able to provide the best solutions.

The current paper shows and explores the different troubleshooting and analysis methods across a monitoring system through test calls over VoLTE. This is shown through utilizing monitoring systems that proved their feasibility for the current network

structure. Furthermore, this paper also provides a recommendation for automating the workflow, in order to avoid the unknown errors caused by initial problems before the technology gets widely used and public.

1. Bevezetés

A mobilhálózati architektúrában az LTE (Long Term Evolution) jelentős változásokat hozott. Új hálózati elemek megjelenésével új kihívások jelentkeztek a hálózat-monitorozásban is. Az új entitások bevezetésének következtében eddig ismeretlen interfészek, és hálózati protokollok keletkeztek. A hálózat- és szolgáltatás-minőség javításában továbbra is elengedhetetlen szerepe van a passzív monitorozási vizsgálatoknak – sőt, az architektúra változásával egyre fontosabb szerepük van ezeknek a módszereknek a hálózati működés feltárásában.

Az EPC (Evolved Packet Core) elemei közötti kapcsolatok természetesen már IP alapúak, így a megszokott pont-pont kapcsolódással járó üzenetátadás a bonyolultabb útvonalválasztás felé mozdult el. A távközlési maghálózatban ez viszonylag újnak számít, emiatt alaposabban fel kell térképezni a kapcsolatok típusait, a szállítási, alagutazó, adaptációs és applikációs protokollokat, ezek üzeneteit és paramétereit. Az új környezet megismerése és megbízhatóvá tétele szempontjából fel kell térképezni a hibalehetőségeket, ezzel együtt a hibaüzenetek kiértékelésére is hangsúlyt kell fektetni. Az új közegben is biztosítani kell a csomagvesztés teljes mértékű elkerülését, ráadásul az esetleges vesztés észlelésének megvalósítására az egyes protokollokon különböző lehetőségek adódnak.

Egy VoLTE előfizető aktivitása több jelzésátviteli protokollon keresztül követhető az LTE maghálózatból egészen az IP Multimedia alrendszerig (IMS). A különböző vonalakon monitorozott protokoll üzenetek tárolása is nehéz feladatnak bizonyul az eltérő forgalomméretek miatt, a feldolgozás pedig széles körű ismeretet igényel a protokoll analízisre vonatkozólag. Az IMS bevezetésével egy addig ismeretlen felépítésű, és a távközlésben szokatlanul szószátyár módon kommunikáló rendszer került a mobil hálózat közvetlen közelébe, amely nagyságrendileg annyi funkciót és entitást tartalmaz, mint a teljes maghálózat. A VoIP szolgáltatásoknál megismert Session Initiation Protocol (SIP) jellegzetességei miatt adódó nehézségek új kihívásokat jelentenek, elsősorban az IP csomag-fregmentáció valósidejű megszüntetési igénye miatt. Az IMS eddig ismeretlen interfészeket használ a Diameter protokoll-forgalom számára, ahol a fejlesztőknek a távközlésben újnak tekinthető filozófiájú paraméter-hierarchiák és üzenettípusok dekódolását is szükséges elkészíteni. A GPRS alagút

protokollja, eddig LTE feletti beszédszolgáltatás hiányában, új bearer-ek kiépítését végzi, így az ezzel kapcsolatos interfészek is újdonságokat rejtenek.

Az LTE és az alacsonyabb generációs hálózatok közötti, területi lefedettségből adódó váltások fontossága az LTE feletti beszédátvitellel tovább nő. A váltások helyes követése az operátorok és szakértők számára is hasznos információt tartalmazhat a még kezdetlegesen kialakuló hálózati hibajelenségek további kiküszöbölése szempontjából. Egy kezdeti rendszer folyamatos monitorozása a gyakorlati hibák eredetének megtalálásával együtt elősegítheti a szolgáltatás minél gyorsabb elindítását és monitorozó rendszer felkészítését az éles üzemre.

E dolgozat bemutatja a VoLTE technológia első fázisait és annak jellemzőit, majd áttekintő képet nyújt az LTE maghálózattal szorosan összekapcsolódó IMS rendszerről. Az alapvető VoLTE protokollok rövid bemutatásával és a hálózatmonitorozási alapokkal bevezeti a monitorozott információk feldolgozásának módszereit. A monitorozás során gyűjthető vezérlőüzenetek jellemző paramétereinek követésével ajánlást ad automatizált folyamatokra, ezzel segítve a hálózati operátorok és a monitorozó rendszert alkalmazó felhasználók munkáját. A dolgozat az egyes protokollokra kitérve támpontokkal szolgál az esetlegesen bekövetkezett hibák felderítéséhez.

2. Műszaki háttér

Az IP feletti LTE beszédszolgáltatás valódi működési mechanizmusairól jelenleg – bevezetése hiányában – kevés információval rendelkezünk, ám az LTE hálózat ezen új funkciója miatt egészen biztosan a témakör vizsgálóinak látóterébe kerülnek az alábbi szolgáltatások, entitások.

2.1. Voice over LTE

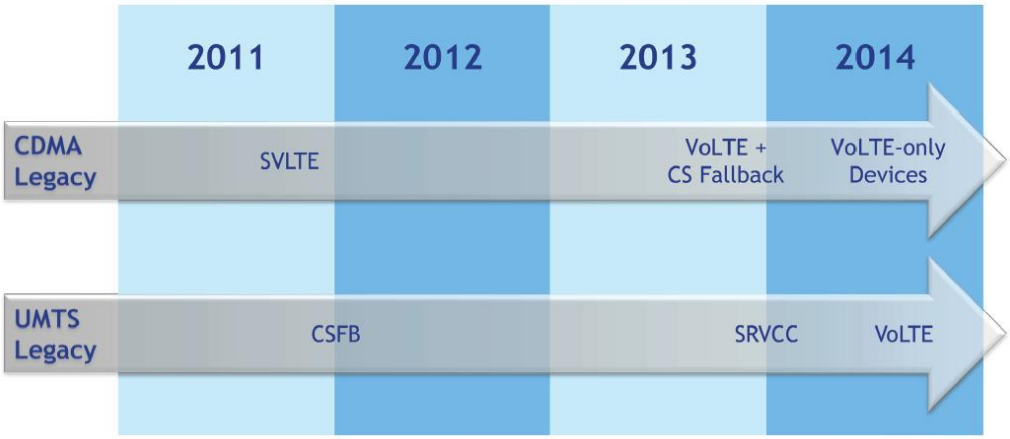
A 4G hálózatnak köszönhetően a mobil előfizetők jobb minőségű szolgáltatást, nagyobb videó hívás-kezdeményezési aktivitást tapasztalhatnak, valamint az instant üzenetek használata is ösztönösebbé válik a 4G által nyújtott átviteli lehetőségekkel. A Voice over LTE technológia megjelenése az egyre inkább elterjedő 4G, vagyis LTE hálózatoknak köszönhető. A beszédszolgáltatás teljesen IP-alapú, csomagkapcsolt rendszereken keresztül zajlik, ellentétben a megszokott áramkörkapcsolt megvalósítással [1]. A VoLTE a VoIP speciális megvalósításának tekinthető, amely az LTE hálózatokon keresztül is lehetővé teszi a csomagkapcsolt hanghívást. Ezzel a szolgáltatással egy új típusú probléma is felmerül az LTE lefedettség határához érve, ugyanis a hívásnak valamilyen módon ezután is folytatódnia kell – valamilyen, az előfizető által észre nem vehető megoldással.

A fejlődés során több megoldás is született a teljesen LTE alapú VoLTE rendszerig [2]. Kezdetben a Simultaneous Voice and LTE (SVLTE) jött létre, amely két rádiós egységet használt, hogy egyidejűleg kommunikálni tudjon egy áramkörkapcsolt hálózattal, amin keresztül folyt a beszéd, az SMS és a vészhelyzet esetén igénybe vehető szolgáltatások – valamint egy LTE csomagkapcsolt hálózattal, amely az adattovábbításért felelt. Ez a megközelítés gyors fejlődést tett lehetővé, ennek ellenére ez ideiglenes intézkedésnek tekinthető a további két fázissal ellentétben. A két rádiós modul nagy költséget jelent minden egyes SVLTE-képes eszköz esetén, emellett interferencia léphet fel a két rádió között, valamint az áramfelvétel növelése természetesen az akkumulátor élettartamát jelentősen csökkenti.

Az első fázisnak tekinthető Circuit Switched Fallback (CSFB) megoldás már egy rádiós egységet használ [3]. A CSFB az adatot az SVLTE-hez hasonlóan a 4G hálózaton keresztül továbbítja, mivel a készülék 4G-re van felcsatlakozva. Híváskezdeményezés

és fogadás során 2G, illetve 3G hálózatra csatlakozik, így visszakapcsol a csomagkapcsolt hálózatba. Ez a mechanizmus azért előnyös, mert annak ellenére, hogy LTE hívás közben nem képes a készülék egyszerre adatot is fogadni, UMTS vagy GSM hálózaton létesített hívás közben az LTE IP-alapú adatkapcsolat elérhető. Megjegyzendő, hogy a „fallback” időbe telik, így a hívásfelépítés akár több másodpercet is igénybe vehet.

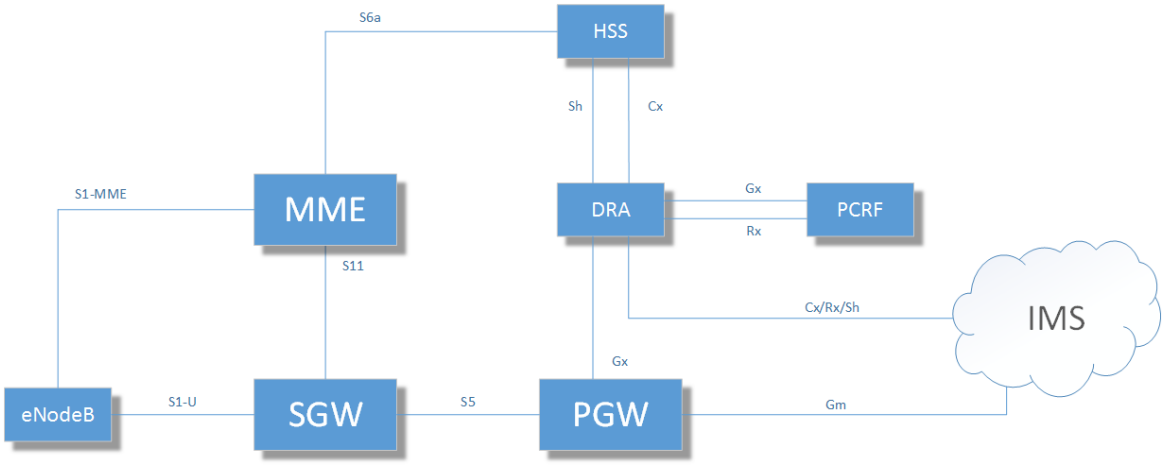
A második fázisú Single Radio Voice Call Continutity (SRVCC) megvalósítás egy csomagkapcsolt, IMS (IP Multimedia Subsystem) alapú hanghívást tesz lehetővé [4]. Az IMS rendszer kifejtésére a következő fejezetben kerül sor. Az előbb említett megoldásokkal ellentétben az SRVCC elérhetővé teszi a hívásfolytonosságot, amely egy rádiós egységet használ, engedélyezi mindenütt a hanghívást, még ott is, ahol az LTE lefedettség még nem teljesen megoldott. Az áramkörkapcsolt hálózatba való hívás közbeni átlépés során azonban mindig kisebb szünet lép fel a hangszolgáltatásban, amely 300 milliszekundumnál is kisebb, tehát a felhasználó beszéd közben nem észleli. Az 1. ábra foglalja össze a VoLTE hálózatok fejlődését [2].



1. ábra A VoLTE megoldások fejlődése

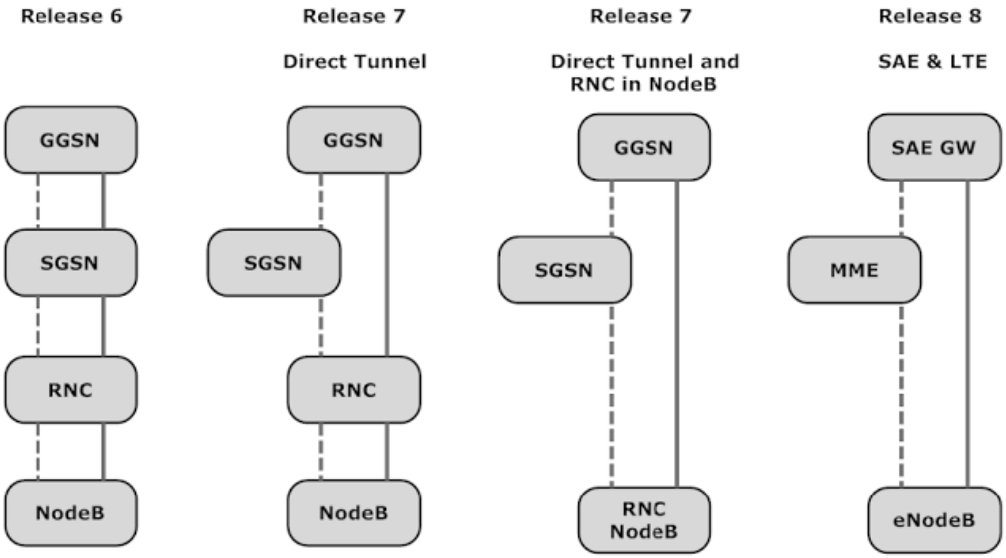
2.2. Az LTE maghálózat és az IP Multimedia Subsystem

A 2. ábra szemlélteti az LTE hálózat elemeit, amelyek funkciói megegyeznek az áramkörkapcsolt elemekkel, de IP-alapú megvalósítást tesznek lehetővé.



2. ábra Az LTE hálózat felépítése

Az UMTS rádiós hálózatának továbbfejlesztése során az E-UTRAN hálózati elemeinek száma gyakorlatilag egyre redukálódott, ezt a feladatot az eNodeB végzi [5]. Az UMTS rendszerekben használatos RNC vezérlő funkciói a maghálózatba kerültek, így az eNodeB közvetlenül kapcsolódik a maghálózathoz. Fejlődése az egyes Release-ekben az 3. ábra segítségével követhető [6]. Jól látható, hogy tartalmazza az RNC funkcióit, így csökkenti a késleltetést az IP hálózatban [7].



3. ábra A System Architechture Evolution (SAE) struktúra kialakulása

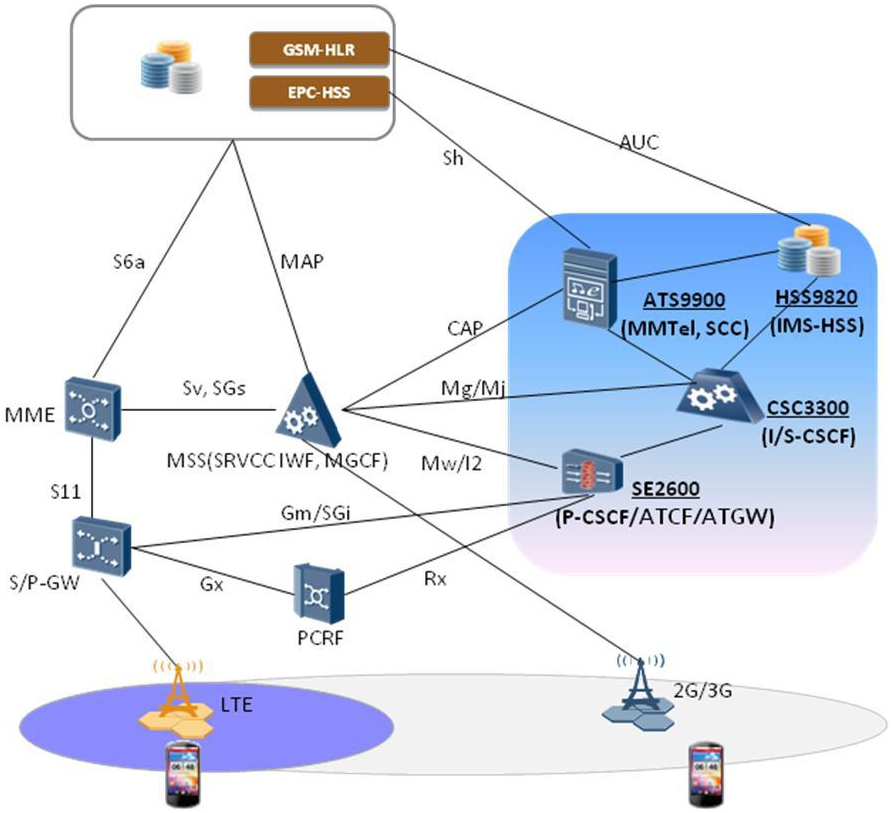
Az Mobility Management Entity (MME) az E-UTRAN és EPC közötti kommunikációért felelős. Ahogy az ábrán látható, ez kapcsolódik az eNodeB-khez és a

Home Subscriber Serverhez (HSS). Az UE eNodeB-hez való csatlakozása során az eNodeB választja ki a megfelelő MME-t. Funkciói között szerepel a handoverek kezelése, tehát az új elemek kiválasztásáért felelős, így a hívásátadást képes megvalósítani 2G vagy 3G hálózat során, akár 4G handover esetén másik MME-vel való kommunikációt is végez, valamint a dedikált vivők kiépítésére és bontására szolgál. Emellett azonosítási feladatokkal is rendelkezik a HSS irányában, ahol a bejelentkezéseket is kezeli.

A Serving Gateway (S-GW) segítségével kapcsolat létesíthető az eNodeB és EPC között, amely során felhasználói csomagok továbbíthatók közöttük. Mivel handover esetén nem változik, segít az eNodeB-k közötti váltásban. A Packet Data Network Gateway (P-GW) hozzáférést biztosít a más külső hálózatokhoz, többek között az IMS-hez is. Feladatai között szerepel a QoS vezérlés, a csomagszűrés, emellett a mobilitást is biztosítja.

Az előfizetői adatok tárolására szolgál a már említett HSS, amely tulajdonképpen az előző generációs hálózatokból ismert Home Location Register (HLR) és Authentication Center (AuC) feladatait látja el. A Policy and Charging Rules Function (PCRF) többek között a számlázásért felelős. Az említett berendezésekkel való kommunikációt a Diameter protokoll valósítja meg. A Diameter jelzéseket a szolgáltatók egy Diameter Routing Agent (DRA) berendezésbe irányítják, amely képes a megfelelő útvonalat biztosítani a különböző interfészek számára.

Az LTE maghálózathoz kapcsolódó IMS egy IP feletti szolgáltatás, amely globális rendszerként multimédiás kapcsolatokat tesz lehetővé. Az IMS létrehozásának célja a különböző platformok egységes kapcsolódási lehetősége. Az IMS elemeit és elhelyezkedését a hálózatban a 4. ábra szemlélteti [8].



4. ábra A széles körben elterjedt Huawei specifikus IMS elemei és kapcsolatai

Az IMS meghatározó elemei a CSCF-ek (Call/Session Control Function), amelyek logikailag különállnak, de jellemzően a valóságban fizikailag egy közös hardver valósítja meg, így a köztük lévő jelzésforgalom nehezen, vagy egyáltalán nem monitorozható. A P-CSCF (Proxy CSCF) feladata az előfizetők és az IMS közötti kapcsolat teremtése. Az S-CSCF (Serving CSCF) végzi a hitelesítést a HSS-en keresztül és a SIP üzenetek által létrehozott kommunikációt vezérli. Az I-CSCF (Interrogating CSCF) feladata egy másik IMS rendszerből küldött jelzések fogadása, melyeket jellemzően a küldő IMS-ben található S-CSCF továbbít.

Az IMS-ben található MGCF (Media Gateway Control Function) funkciója a SIP és ISUP jelzések közötti protokoll-fordítás, ezáltal a 2G- és 3G-képes telefonok az MGCF-en keresztül kapcsolódhatnak az IMS-hez.

2.3. Hálózat-monitorozás

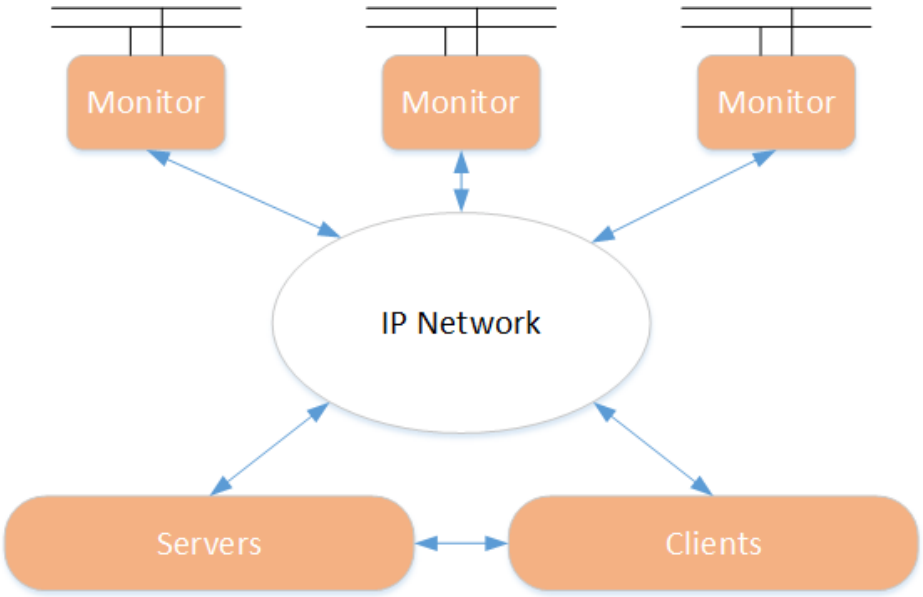
A folyamatosan bővülő távközlési hálózatok monitorozását kizárólag egy elosztott, és legfőképp jól skálázható rendszer képes megvalósítani. A széleskörű vizsgálhatóság miatt a nagy mennyiségű adat feldolgozása egyetlen központi rendszeren keresztül lehetséges. Egy minden igényt kielégítő monitorozó rendszer nemcsak az információ tárolásáért felelős, hanem a folyamatos statisztikák generálásától kezdve, a hívásrekord összeállításon át, a kiválasztott hívások nyomon követéséig vannak fontos, az operátori munkát támogató feladatai.

A távközlési hálózatok monitorozását megvalósító rendszerek, biztosítva a hálózati berendezésektől való függetlenségét, jellemzően passzív eszközök. Az hálózati entitások általában kész termékekként kerülnek beüzemelésre, ezzel együtt az egyes szolgáltatói igényeket tekintve elveszítik rugalmasságukat. Ezenkívül a dinamikusan növekvő forgalom mellett nem rendelkeznek a részletes vizsgálatokhoz elegendő számítási többlet kapacitásokkal sem, ráadásul egy berendezés monitorozás miatti átkonfigurálása nem okozhat a hálózatban működésbeli problémát.

A gyűjtést és feldolgozást nehezítheti, ha a jelzések egy vonalon titkosított módon érkeznek, amelyre a legismertebb példa a GPRS rendszer, vagy az LTE hálózat S1AP jelzésüzenetei (amelyek az eNodeB és az MME között titkosítva haladnak). Ezekben az esetekben elengedhetetlen a titkosított tartalom megjelenítéséhez a titkosító kulcsokat szállító interfészek monitorozása, amelynek és a titkosító algoritmusok ismeretének köszönhetően a rejtett tartalom megjeleníthető. A titkosítás már az üzenetek típusára is kiterjed, így a statisztikák készítése is nagyobb számításai kapacitást igényelnek. Természetesen a berendezések titkosított kommunikációja a hálózat működését nem befolyásolja, a kapcsolat zavartalanul fennáll az egyes vonalakon. Az eljárás során megjelenített információk nem minden felhasználó számára engedélyezettek, így a rendszer használatát jogosultságok szabályozzák. Az előfizetőkre vonatkozó érzékeny információk is feltételekhez kötötten jeleníthetők meg, tehát nem minden felhasználó láthatja az adott probléma felderítése során, hogy ki telefonált vagy forgalmazott adatot. A monitorozó rendszer különböző jogosultságok meghatározásával minden felhasználó számára kizárólag a neki szükséges információt biztosítja.

A rendszer elosztottságából adódóan könnyen megkülönböztethetők a funkcionális elemek. Az egyes vonalakról leszedett információk tárolását a monitor gépek végzik,

amelyek feladata az üzenetek szűrése és a pontos időpecsételés megoldása is. Az mikroszekundum pontosságú időpecsételés folyamatosan szinkronizált órajel segítségével történik. A monitorok a feldolgozás és üzenetszintű dekódolás során készíthetnek különböző statisztikákat, amelyek segítségével könnyen és gyorsan felügyelhető a rendszer. A skálázható tulajdonságból adódóan akár földrajzilag is különböző helyen lévő monitorgépek egyetlen szerverhez kapcsolódnak, amely az üzenetek sorba-rendezését végi. A központi szerver gépek készítenek összeállított rekordokat az üzenetekből, emellett biztosítják azok lekérdezhetőségét, így a monitorok számának növelésével probléma nélkül végrehajtható nagyobb forgalom feldolgozása. A szerverek és monitorok kapcsolatát mutatja az 5. ábra, amely a teljes monitorozó struktúráról képet ad.



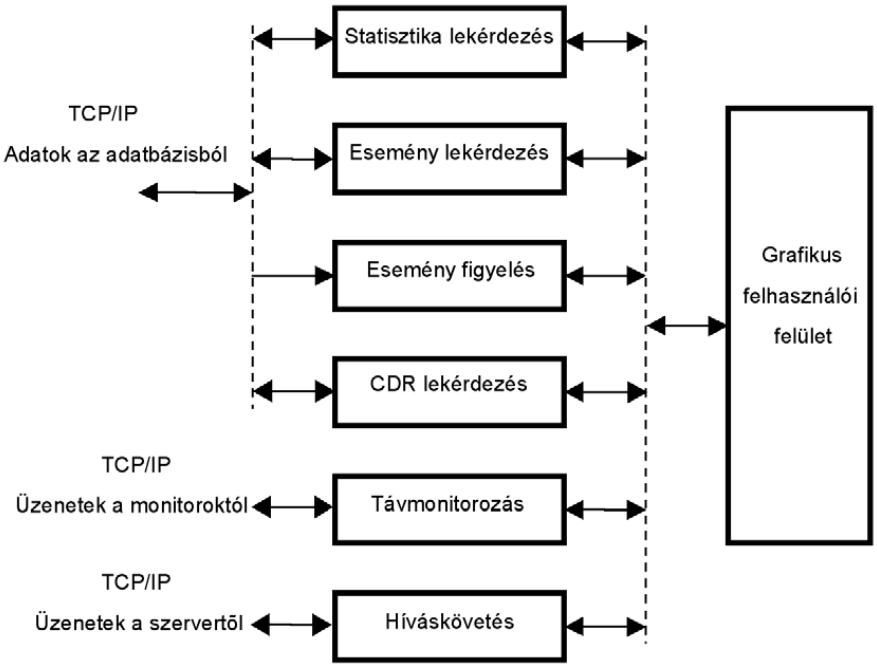
5. ábra Egy lehetséges monitorozó struktúra

Néhány protokoll esetén a rekordok összeállítása elvégezhető több, egymástól független szerveren, így a szerver gépek számának növelésével még hatékonyabb skálázhatóság érhető el. A szolgáltatók az LTE hálózatukban feladatmegosztásként több MME üzembe helyezésével képesek kiszolgálni az előfizetőket [9]. Az adatok lekérdezését végző kliens gépek számára biztosítani kell a helytől független, távoli hozzáférést. A monitorozó rendszer minden pontját elérő felhasználó a jelzésüzenetek és rekordok lekérdezése mellett a monitorozó rendszer elemeit is elérve, IP hálózaton

keresztül tudja felügyelni a rendszer állapotát, emellett távolról a szoftverfrissítések elvégzésére is képes [10].

A tárolt információk kerülhetnek ismert adatbázisokba is, de gyakrabban saját igényekre optimalizált egyedi tároló struktúrát részesítik előnyben. Az egyedileg tervezett adatbázisban nagyobb sebesség érhető el az új rekordok írása és a vele egy időben biztosított visszakeresés során.

Az átláthatóság érdekében a monitorok által adott időközönként továbbított statisztikák egyetlen központi helyre, egy saját minőségbiztosító rendszerbe jutnak el. Az ajánlások szerint több száz, fontos statisztika képes egyszerre jellemezni a rendszer állapotát, így a hívásokra vonatkozó adatok mellett akár fizikai szintű információk is követhetők. Különböző fontossági sorrendet szem előtt tartva számtalan riasztás és esemény definiálásával a szakértők számára egyszerűen kézben tartható rendszer valósítható meg. A riasztások a statisztikákkal ellentétben a bekövetkezés pillanatában eljutnak a központba, hogy a szükséges hiba-ok analízis minél előbb elvégezhető legyen.



6. ábra A kliens modulok funkciói

Funkcionálisan különböző kliens szoftverekkel (például a híváskövetést, a hívásrekordok vizsgálatát, vagy a protokoll-üzenetek elemzését támogató eszközökkel) szinte minden igényt kielégítő rendszer készíthető (6. ábra). A kész hívásrekordok

hozzáférése lehetővé teszi a vizsgálatot mélyebb elemzés nélkül. A rekord paramétereinek és tulajdonságainak megjelenítésével megkönnyítve a felhasználó feladatát egyszerűbb analízis elvégzése is elegendő. A vonalakról lekérdezett minden információ és egy hívás követése is hasznos funkció lehet a felhasználók számára.

2.4. VoLTE esetén használatos hálózati protokollok

Egy beszédszolgáltatás során az eddigiekhez hasonlóan VoLTE esetén is több különböző protokollon keresztül követhető végig a hívás, viszont az alábbi protokollok javarészt eddig csak adatforgalmazáskor látták el jelzésfunkciójukat. Egy IMS-ben végződő hívást a SIP segítségével követhetjük a legegyszerűbb módon, így a legfontosabb e protokoll mélyebb szintű ismerete.

2.4.1. S1 Application Protocol

Az E-UTRAN és EPC közötti kommunikációt az S1-MME interfész biztosítja, amely így az eNodeB-MME kapcsolatot valósítja meg. A GPRS-hez hasonlóan a kommunikáció jelentős része titkosított csatornán történik. Az S1AP számos különböző folyamat jelzésére szolgál, így részt vesz az LTE feljelentkezésben, a hordozócsatorna (bearer) kiépítésében és Paging folyamatokban, ezáltal hasznos információt szolgáltat a VoLTE előfizetők csatlakozása és hívása során is. A MME által végzett mobilitás-kezelés közben történő Handover procedúra is nyomon követhető az S1AP jelzések segítségével. A jelzések kizárólag kontroll funkciót látnak el, melyek nagy része előfizetői forgalomra vonatkozik, a kisebb hányadát pedig a berendezések közötti információátadás teszi ki [11].

A jelzésüzenetekből rekordok összeállítása lehetséges az egyedi eNodeB, illetve MME oldalon definiált azonosítók segítségével, ehhez mindkét végpont választ egy azonosítót kommunikációhoz.

Az S1AP szállítási rétegként az SCTP-t használja, ezáltal megoldandó feladat a szegmensek darabolódásának és újraadásának kezelése.

2.4.2. GPRS Tunnelling Protocol

A korábbi GSM rendszerek adatátviteli sebességeinek jelentős mértékű korlátozása miatt a hálózat továbbfejlesztésre szorult. Ennek eredménye többek között a General

Packet Radio Service (GPRS), amely csomagkapcsoláson alapul. Az előfizető adatforgalmazás közben folyamatosan kapcsolatban maradhat a hálózattal, aminek köszönhetően gyorsabb sebesség garantált, miközben mindvégig elérhető marad [12].

A GPRS Tunnelling Protocol (GTP) használatával lehetőség nyílik a GPRS gerinchálózat két GSN-je (Serving GPRS Support Node, Gateway Support Node) közötti csomagok szállítására [13]. A GTP elsődleges feladata az átvitelt biztosító csatorna kiépítése és vezérlése, majd a következő fázisban az alagút technika segítségével az adatok célba juttatása, ezáltal megkülönböztethetők a vezérlés támogatására szolgáló GTP-C (Control), és a felhasználói adatcsomagokra használatos GTP-U jelzések. Az alagutak azonosítása pedig egy Tunnel Endpoint Identifier (TEID) segítségével történik.

Kezdetekben a GTP protokoll első verziója az SGSN-ek és GGSN-ek közt volt használatos, ám később az LTE hálózatban található, hasonló szerepet betöltő SGW és PGW közötti kommunikációt, valamint a mobilitást menedzselő MME és SGW kapcsolatát biztosítja. A negyedik generációs hálózati entitások a GTP második verzióját használják.

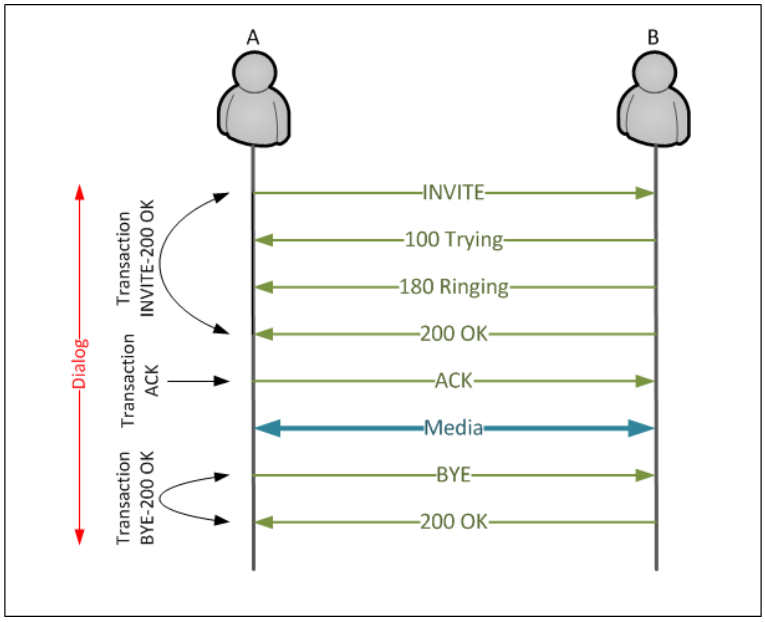
A GTP jelzésüzenetek szállítására az UDP használatos, amelynek köszönhetően nem biztosított a csomagvesztés elkerülése. A kérés-válasz típusú tranzakciók összeállítása adott IP cím és UDP port páros mellett egy sorszám (sequnce number) segítségével történik.

2.4.3. Session Initiation Protocol

Az IMS jelzéseinek átvitelére a Session Initiation Protocol (SIP) használatos. A SIP egy szöveges alapú protokoll, amely a HTTP felépítésére hasonlít, melyet a szállítási rétegben szereplő 5060-as port azonosít. Segítségével felhasználók kommunikálhatnak egymással, valamint IMS-en belüli regisztráció jelzéseit teszi lehetővé [14].

Mivel szöveges karakter-kódolású, feldolgozása egyszerű szöveges kereséssel történhet. A protokoll-technológiában megkülönböztetünk request és response üzeneteket, ahol előbbiek kéréseket, utóbbiak válaszokat hordoznak. A request-response alapú kommunikációból következően definiálható UAC (User Agent Client) és UAS (User Agent Server), amelyek a kapcsolat résztvevői. A felhasználó azonosítására használatos URI (Uniform Resource Identifier) általában a távközlésből ismert azonosítókat (MSISDN, IMSI) vagy IP címet tartalmaz.

A SIP által használt response üzeneteket a szabvány típusuk szerint több osztályba csoportosítja. Egy response üzenetet a neve előtt feltűntetett 3 jegyű szám egyértelműen azonosít. Az első számjegy egy adott csoportba sorolja a választ, ezáltal megkülönböztethető ideiglenes (1XX), sikeres (2XX) és átirányított (3XX) response üzenet. Természetesen lehetőség nyílik a hibát is response üzenetekkel jelezni, így léteznek kliens (4XX), szerver (5XX) és globális (6XX) hibát jelző válaszok [15].



7. ábra Egy tipikus hívás SIP-en, az üzenetek csoportosításával

A SIP üzenetek csoportosítására használatos fogalmak a tranzakció, a dialógus és a session. Minden kérés-válasz üzenetváltás tranzakciónak nevezhető, ahol a válasz egy 2XX osztályba sorolható vagy hibát jelző response üzenet. Egyetlen kivétel az ACK üzenet, amely nem igényel választ. A dialógus tranzakciókból áll, ahogy 7. ábrán látható [16]. Dialógust nyit egy INVITE és egy SUBSCRIBE üzenet, melyek közül az előbbi SIP session-t hoz létre. A SIP session hívásra vonatkozik, így kodek és egyéb jellemzők, beállítások egyeztetése céljából tartalmaz SDP (Session Description Protocol) paramétereket. Az egy tranzakcióba tartozó üzeneteket a Call-ID és a CSeq paraméterek egyértelműen azonosítják. A CSeq mezőben található azonosító egy 32 bites integer típus, amely kezdőértékét minden eszköz maga választja ki, az értéke pedig tranzakciónként inkrementálódik. Egy dialógus a Call-ID, From-tag és To-tag alapján fűzhető össze, ezt a szabvány Dialog-ID-nak nevezi [17].

2.4.4. Diameter Protocol

Bármely LTE forgalmazás esetén Diameter protokoll által hordozott vezérlőüzenetek is megjelennek a hálózatban. A Diameter protokoll mindenekelőtt az AAA (Authentication, Authorization, Accounting) funkciókat valósítja meg, így egy előfizető státusza a beazonosításától kezdve, a jogosultságainak meghatározásán át, a számlázásig e protokoll segítségével követhető a jelzéshálózaton [17]. Funkciójából adódóan kérés-válasz (request-answer) típusú tranzakciókból áll, melyeket a protokoll-specifikus Session-ID egyedileg párosít össze. A Diameter a mobilhálózatban számos entitás között, több különböző interfészen jelenik meg, ahogy a maghálózat jelentős részén, az üzenetek az előfizető IMSI-jét tartalmazzák. A Diameter jelzésüzenetek a veszteségmentes átvitelt biztosító TCP vagy SCTP transzport-protokollok üzeneteibe ágyazva utaznak.

Az LTE maghálózatban használatos titkosítás miatt - a 4. fejezet témájához kapcsolódóan - az egyik legfontosabb jelzésüzenet a 4G hálózatra való feljelentkezéskor az MME-HSS útvonalon (S6a interfészen) utazó *Authentication-Information-Request* (AIA) autentikációs kulcs lekérdezésért felelős üzenet. Fontos megjegyezni, hogy az említett folyamat kizárólag az első, hálózatba való feljelentkezésre vonatkozik, hiszen az elsőként 2G vagy 3G hálózathoz kapcsolódás során is történhet kulcskérő mechanizmus, viszont az LTE hálózatba áttérés során az egyes entitások képesek a kulcsokról szerzett információjukat egymással megosztani. Az S6a interfészen történő lekérdezés során a HSS autentikációs kulcs vektorokat küld az MME-nek válaszul. A titkosítás feloldásának folyamatát és módszereit a 4. fejezet részletezi.

Az említett interfész az autentikáción kívül hordoz többek között helyzetfrissítésre vonatkozó jelzéseket is, amelyre az *Update-Location* vagy a *Cancel-Location* kérés-válasz procedúra szolgál.

Mivel egy VoLTE előfizető kezelése az IMS belsejében is megvalósított, így az IMS berendezésen belül hordozott Diameter üzenetekkel is találkozhatunk. Ha a számlázást az IMS végzi, akkor a Charging Collection Function (CCF) irányában minden számlázáshoz köthető híváseseményre vonatkozó *Accounting-Request* (ACR) üzenet jelenik meg. A további Diameter jelzésüzenetek a következő fejezetekben kerülnek kifejtésre.

3. Titkosítás használata az LTE jelzéshálózaton

A 4G hálózat megjelenésével a 2G-n látottakhoz hasonló problémákba ütköztek a monitorozó rendszereket szállító szakemberek, ugyanis az LTE jelzéshálózat is alkalmaz titkosítási algoritmusokat [19]. Így a jelzéshálózat üzeneteinek felderítéséhez a titkosítás on-the-fly feloldása is elengedhetetlen. Jelen fejezet nem a "kititkosítási" algoritmusokat mutatja be, kizárólag a folyamat-mechanizmusokra ajánl megoldást.

A VoLTE funkció bevezetésével a már megismert előnyök ténylegesen kihasználhatóak, ennek ellenére Magyarországon a hiányos 4G területi lefedettség miatt nem biztosított a mindenkori használata. Ebből kifolyólag bárminemű tartós LTE forgalmazás során nagy valószínűséggel bekövetkezik a 4G-ről vándorlás eshetősége 3G vagy akár 2G hálózatra.

Az előfizető LTE hálózatra történő első feljelentkezési szándék alkalmával (Attach Request) a saját IMSI azonosítójukat adja meg az MME felé. A sikeres folyamat során az MME egy ideiglenes azonosítóval tárolja az említett előfizetőt. Az előfizető bármilyen következő aktivitása során az aktuális azonosítót fogja használni. Ebből következik, hogy a több mobilitás-kezelő egységet tartalmazó hálózat kezelése gátolja az egyszerűbb átláthatóságot. A VoLTE funkció használata során az LTE hálózaton használatos identifikációt elősegítő MME - Temporary Mobile Subscriber Identity (M-TMSI) mindenkori nyomon követése elengedhetetlen, mivel a GPRS kapcsolat alatt minden jelzésüzenet tartalmazza ezt az információt, ezáltal az előfizetők és a rekordok ismerete is könnyebb feladatnak bizonyult. Ha az előfizető a lefedettségből adódóan 3G hálózatra kényszerül leváltani, akkor az MME-ből átkerül az UMTS megfelelőjébe, vagyis az SGSN-be - bár ennek ellenére az MME egyelőre nem törli az adatbázisából. A folyamat hatására megjelenik Radio Access Network Application Part (RANAP) jelzésként egy Routing Area Update Request üzenet . A sikerességet igazoló titkosított Routing Area Update Accept jelzés tartalmazni fogja az előfizető új, 3G-n használatos azonosítóját. A váltásról GTPv1-C üzenet értesíti az SGSN-t, amely a titkosítási kulcsokat, azonosítókat is tartalmazza [20]. Két különböző MME közötti kommunikációért az S10 interfész felel, így a MME váltás során az LTE hálózaton használt alagutazásra alkalmas GTPv2-C üzenet értesíti az új MME-t a váltásról. Az LTE hálózatra váltás S1AP-n egy Tracking Area Update Request üzenetként látható,

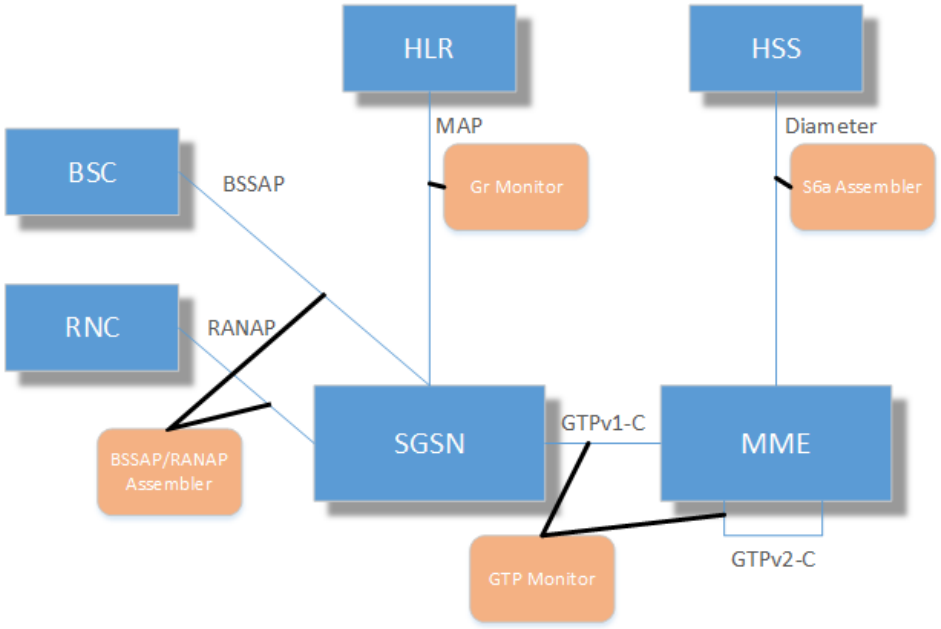
amely sikerességét a hozzá tartozó titkosított Accept igazolja egy újabb M-TMSI azonosítóval. Az új azonosítók megjelenéséből is látszik, hogy a titkosítás során használt azonosítók elvesztése a "kititkosítási" sikerességet rontja. Egy előfizetőre vonatkozó titkosított tartalom így a következő kulcskérésig rejtve marad.

Jelentős mértékben nehezítheti a berendezések közötti váltások nyomon követését egy már megszokott konfiguráció, amely során a szolgáltatók egyetlen hardverrel megvalósított SGSN és MME együttest alkalmaznak. Az említett elrendezés meggátolja az azonosítók és a titkosítási kulcs-vektorok monitorozását , ilyenkor szükség van a RANAP-on látott TMSI váltások követésére.

Az aktuális magyarországi lefedettség korlátai miatt jelenleg olyan területek is találhatóak, ahol nem érhető el LTE hálózat, így feljelentkezés során az előfizető nem az enodeB-hez kapcsolódik, tehát nem az MME kér a HSS-től az S6a interfészen autentikációs kulcsokat. Ebben az esetben az SGSN-HLR közötti Gr interfész szolgálja ki ezt a funkciót.

Az előző pontokban felsorolt valamennyi hálózati link tartalmaz a titkosított tartalom megtekintéséhez elengedhetetlen információt, viszont az adott forgalom csak az aktuális pillanatban hasznos, későbbi feldolgozás során hamis képet adhat az előfizető helyzetéről, állapotáról. A titkosítás visszafejtése elsősorban egy magas szintű, komplex monitorozó rendszer megvalósítását igényli, amely a felmerülő hibák azonnali detekciójára képes. Mivel az LTE szolgáltatásait igénybe venni szándékozók száma folyamatosan nő, a S1-MME interfész S1AP forgalma is évről évre többszörösére növekszik. A jelenség jól látható a 4G hálózat magyarországi elindítása óta, így a jövőbeli becslések alapján igény van egy jól skálázható, a jelenlegi forgalom többszörösét feldolgozni képes rendszerre. A feldolgozni kívánt adatmennyiség másik jelentős része a 2G/3G/4G váltásokból adódó azonosítók cseréje. A titkosított tartalom feloldásához szükséges mindig tárolni az aktuális azonosítót és a kapcsolódó aktuális kulcs-vektorokat, emiatt egy táblaszerkezetet kell létrehozni. Az azonosítók folyamatos frissülése miatt külön kell tárolni a 4G-re vonatkozó M-TMSI-t és a 2G-n, illetve 3G-n használt azonosítókat.

A 8. ábra bemutatja a "kititkosításhoz" szükséges interfészek monitorázását végző szoftvereket.



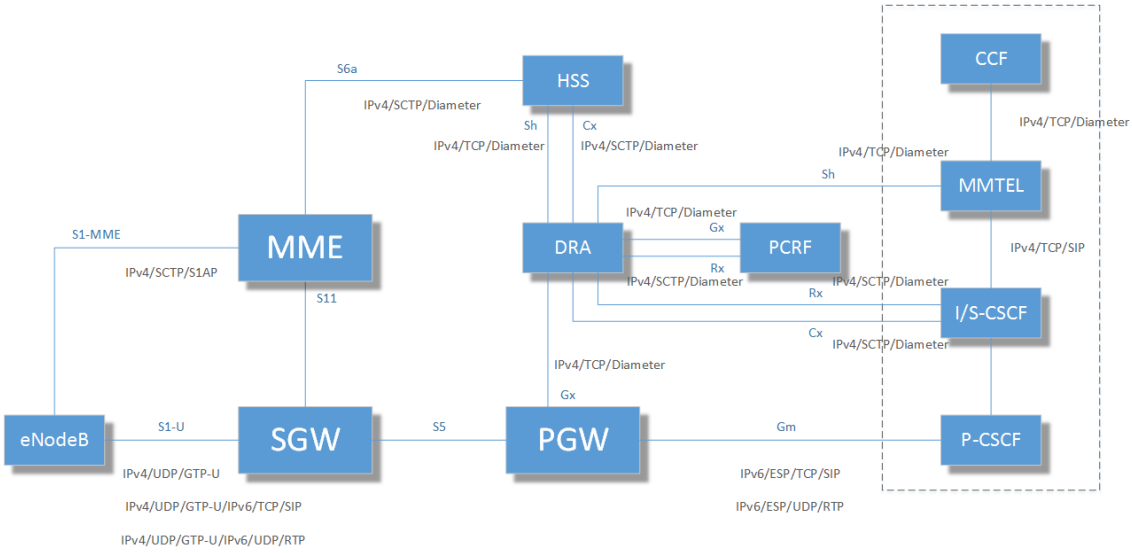
8. ábra A "kititkosítás" megvalósításához szükséges interfészek monitorozása

Az 8. ábrán szereplő Assembler szoftverek a kulcsok, illetve azonosítók küldésén kívül rekord-összeállító szerepük is van. Az ábrán jól látható a magas fokú komplexitás, amely több, különböző funkciójú és feldolgozási képességű szoftver megvalósítását követeli. Ebből kifolyólag a megbízhatóság és a hibadetekció a legfontosabb jellemzői a rendszernek. A forgalom méretéből következik, hogy valós környezetben egy-egy interfész monitorozását nem egyetlen, hanem akár több telephelyre is kihelyezett szoftverek végzik. Az előfizetői vándorlásokat követő információk küldéséért a 2G és 3G kulcsokat tároló szerver felé legalább tucatnyi szoftvermodul felel. A fizikai erőforrás-megtakarítások miatt ugyanazon szoftver látja el az egyes hálózati linkekről gyűjtött információ továbbítását a kulcsszerverek felé, amely a tárolási, vagy éppen rekord-összeállítási feladatokat végzi. Tehát a szoftvermodulok nagy példányszámának oka elsősorban a tárolókapacitás és gyors visszakereshetőség biztosítása.

4. A jelzéshalózat alakulása VoLTE használata során

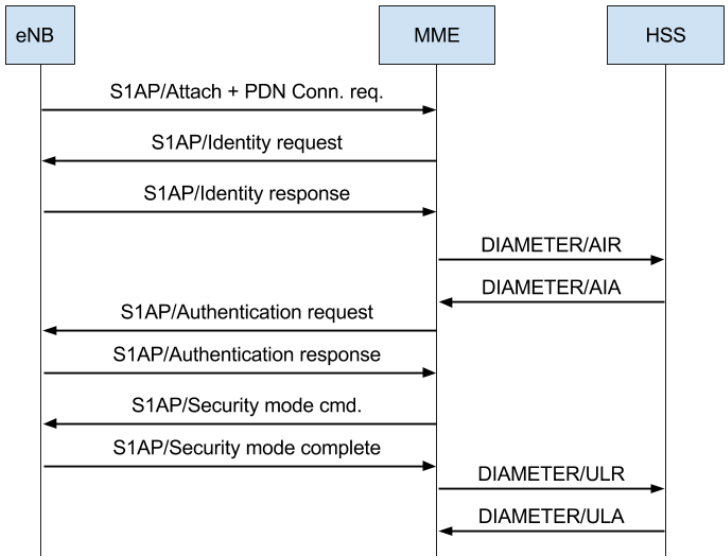
4.1. Csatlakozás a hálózathoz

A szolgáltatás-engedéllyel rendelkező VoLTE-képes előfizetői készülék bekapcsolása esetén regisztráció történik az LTE hálózatba, majd az IMS alrendszerbe is, így az autentikációs folyamat külön-külön lejátszódik mindkét regisztráció során. A 9. ábrán látható az összes használatos interfész a protokollok feltüntetésével együtt.



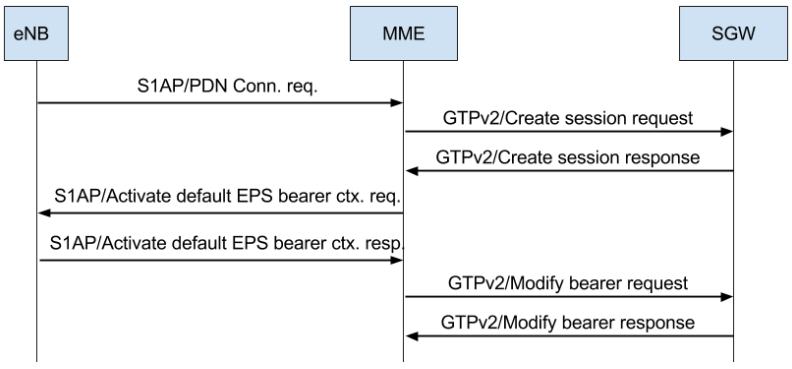
9. ábra A VoLTE regisztráció során használatos interfészek és protokolljaik

A maghálózatban történő autentikációs procedúra alapjai az LTE titkosításról szóló fejezetből már ismertek. A HSS-től kért kulcsok közül az MME kiválasztja a használni kívántat, majd az S1-MME interfészen *Authentication Request* üzenetben elküldi a kulcshoz tartozó RAND és AUTN értéket az eNodeB felé. A RAND értékkel ellenőrizhető a választott kulcs, majd sikeres autentikáció esetén az *Authentication Response* üzenet mezője tartalmazza a választott kulcs XRES értékét, amellyel szintén ellenőrizhető a kulcs. A 10. ábra tartalmazza az autentikáció jelzésrendszerét.



10. ábra LTE maghálózat autentikációs folyamata

Az alagutakat a sikeres autentikációs folyamat létrejöttekor építi ki az MME az eNB-SGW-PGW útvonalon a felhasználó számára. Mivel a tunnel kiépítéséhez GTPv2-C protokollt használ az MME-SGW-PGW úton, ezáltal újabb monitorozott ponton jelennek meg előfizetőt azonosítót paraméterek. A 11. ábrán látható módon a készülék az eNB-n keresztül S1AP *InitialUEMessage/PDN Connectivity Request* üzenetben jelzi az MME felé Default-Bearer kiépítési szándékát. A *PDN Connectivity Request* üzenet szerepelhet az első, *Attach Request* üzenetben is, ilyenkor egy másik, titkosítatlan DTAP-EMM rétegbe kerül. A készüléknek két lehetősége van az APN megadására: küldheti kérés nélkül az autentikációs folyamat előtt a még nem titkosított részben, vagy ha az APN ebben az üzenetben nem szerepel, akkor azt az autentikáció után, egy titkosított üzenetben kéri, illetve kapja az MME.

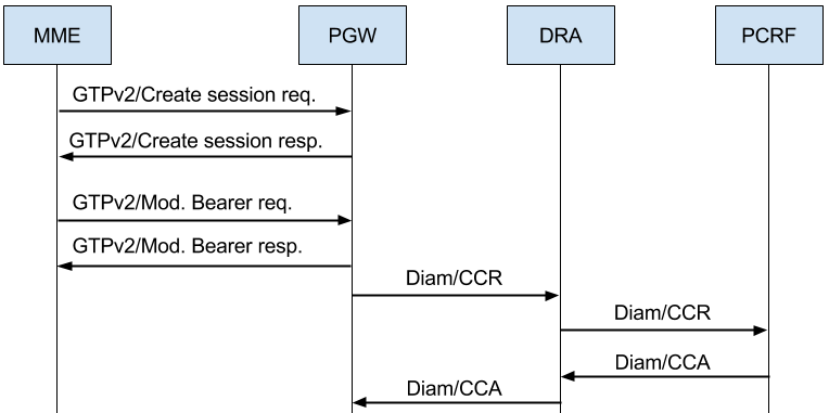


11. ábra A Bearer kiépítés folyamata

Az LTE maghálózat berendezései az adott APN-hez kapcsolódóan GTPv2-C *Create-session* üzenetben EPS Bearer ID (EBI) és Control-TEID azonosító párokat foglalnak a felhasználóhoz. A GTPv2 *Create Session Request* üzenet tartalmazza az említett azonosítókon kívül az MSISDN-t és IMSI-t is. A *Create Session Response* válaszüzenetben az MME megkapja az SGW/PGW oldali Control-TEID azonosítót, amelyet az SGW/PGW berendezés választott a felhasználónak. Az üzenet PDN Address Allocation mezőjében megtalálható a PGW által választott felhasználói IPv6 cím is. A sikeres Control-TEID lefoglalása után az MME az eNB-nek az S1-MME interfészen S1AP *Initial Context Setup Request/Activate Default EPS Bearer Context Request* üzenetben küldi el a sikeresen lefoglalt SGW oldali User-TEID-et. Az említett üzenet tartalmazza az EBI-t, amelyet az MME társít az adott bearer-hez. Az S1AP *EPS Bearer Context Response* üzenet segítségével jut el az eNodeB oldali User-TEID információ az SGW-hez.

Az előzőekben említett, felhasználóhoz tartozó IPv6 címen keresztül továbbítja a PGW a felhasználói forgalmat az IMS felé.

Az előző folyamatot követően a felhasználói készülék az első mellett létrehoz egy másik, IMS APN-hez és EBI-hez tartozó bearer-t is, amely alagúton keresztül GTP-U üzenetbe csomagolt SIP kontroll üzenetek segítségével történik majd a regisztráció az IMS alrendszerbe. A kiépítés után a PGW a Gx interfészen Diameter *Credit Control Request (CCR)* üzenetben értesíti PCRF-et az új felhasználó regisztrációjáról. A *Credit Control* tranzakció minden, IMS-hez tartozó Default Bearer aktiválását jelzi. A Diameter *CCR* üzenet tartalmazza az előfizető IMSI és MSISDN azonosítóját is, mindkettőt a Subscription-Id-Data mezőkben, az üzenetek a 11. ábrán követhetők. A Gx interfészen a Diameter Session-Id paraméter nemcsak egy request-answer párt fog össze, hanem több Diameter tranzakciót is azonosít, egy session-t létrehozva. Ezzel együtt CCR üzenet Session-Id paramétere fontos a későbbiek során is, mivel a regisztrációhoz tartozó, ugyancsak Gx interfészen utazó *Re Auth (RA)* kérés-válasz kizárólag ezzel a paraméterrel kereshető [21].



12. ábra A PCRF értesítése a kiépített Bearer-ről

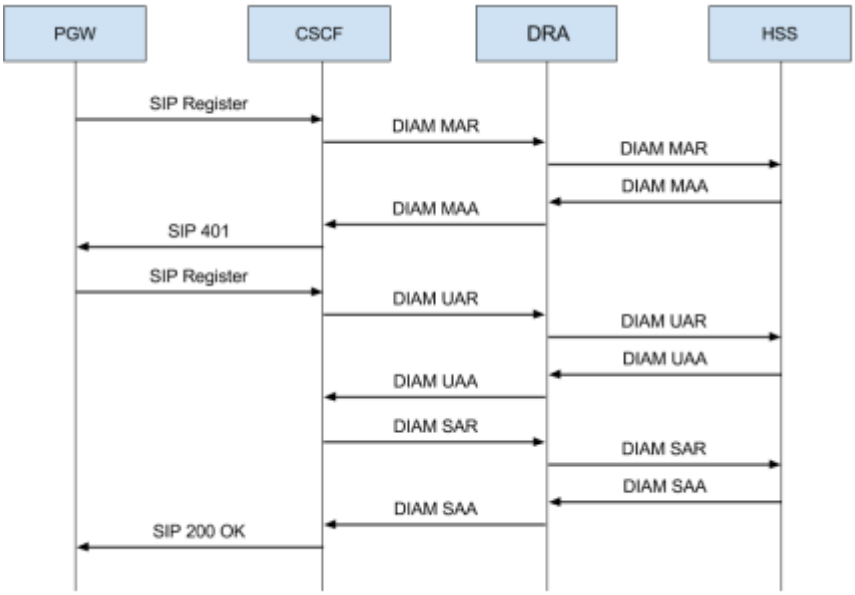
4.2. IMS regisztráció

Az LTE maghálózathoz csatlakozás mellett az előfizetői készülék regisztrációja az IMS alrendszerben is megtörténik. A kiépített GTP alagutat használva, az eNB-SGW-PGW-PCSCF útvonalon utaznak a regisztráció folyamatát jelző, GTP-U/IPv6/TCP-be ágyazott SIP kontroll üzenetek. A GTP-U üzeneten belül az IPv6 fejléc a készüléknek kiosztott IPv6 címet tartalmazza, amely az S1AP kapcsolatban, valamint a Gx interfészen utazó Diameter üzenetekben is megtalálható. A P-CSCF és PGW berendezések IPsec titkosításon keresztül rejtik el a forgalmat Gm interfészen [22]. Az előfizető regisztrációját az IMS az S-CSCF-ben tartja nyílván.

A felhasználói készülék az „IMS” Default Bearer-en keresztül a P-CSCF berendezésnek IPv6/TCP/SIP *Register* üzenetben küldi el regisztrációs szándékát, amelyben IMSI azonosítót használ. A P-CSCF a SIP *Register* üzenetet az I-CSCF modulnak küldi tovább, amely a HSS-től kérdezi le az előfizetőhöz tartozó S-CSCF helyét. Az I-CSCF a Cx interfészen Diameter *User Authorization Request* (UAR) üzenetben kérdezi az S-CSCF azonosítóját. Az UAR üzenetben az előfizető IMSI azonosítója szerepel a Public-Identity és a User-Name mezőben is [23].

Az S-CSCF az autentikációs folyamat lebonyolításához kulcsokat kér a HSS-től a Cx interfészen Diameter *Multimedia Auth Request (MAR)* üzenetben a DRA berendezéseken keresztül (S-CSCF – DRA – HSS útvonalon). A *Multimedia Auth Answer (MAA)* válasz üzenetben szereplő RAND és AUTN paraméter a SIP-Authenticate mezőben, az XRES a SIP-Authorization mezőben, valamint a CK és IK

kulcsok a Confidentiality-Key és Integrity-Key mezőkben található. A teljes autentikáció jelzéseit a 13. ábra mutatja.



13. ábra Az IMS regisztráció folyamata

A SIP *Register* üzenetre válaszul az S-CSCF egy 401-es response kóddal rendelkező választ küld a PGW-nek a P-CSCF-en keresztül, amelyben base64 kódolásban szerepel a RAND és AUTN érték. A felhasználói készülék ezután egy újabb SIP *Register* üzenetben elküldi a számolt autentikációs (XRES) értéket, ezzel azonosítva magát. Az újraküldött *Register* üzenet már IPsec titkosítással utazik a Gm interfészen, az első üzenetpárral ellentétben. A titkosított *Register* üzenet az elsővel megegyező útvonalon jut el az I-CSCF modulhoz, amely ismét lekérdezi Diameter *User Authorization Request (UAR)* üzenetben a felhasználóhoz tartozó S-CSCF modult a HSS-től. A sikeres regisztrációt jelző SIP *200OK* üzenetet megelőzően a S-CSCF a HSS-től lekérdezi az előfizetőhöz, illetve IMSI-hez tartozó MSISDN azonosítót. Ezt a folyamatot a Diameter *Server Assignment (SA)* kérdés-válasz valósítja meg, vagyis utóbbi Public-Identity mezője tartalmazza az MSISDN-t. Ezután az S-CSCF egy újabb *Register* üzenetben regisztrálja be az előfizető MSISDN azonosítóját az IMS alkalmazás szerverébe.

A teljes regisztrációs procedúrát követően az S-CSCF Rx interfészen keresztül Diameter *AAR* üzenetben elküldi a PCRF-nek az adott Default Bearer csatornájához tartozó QoS információkat, amely tartalmazza a felhasználói IPv6 címet is. Ezt követően a Gx interfészen jelzi a PGW felé egy *RAR* üzenetben, hogy ezentúl a PGW

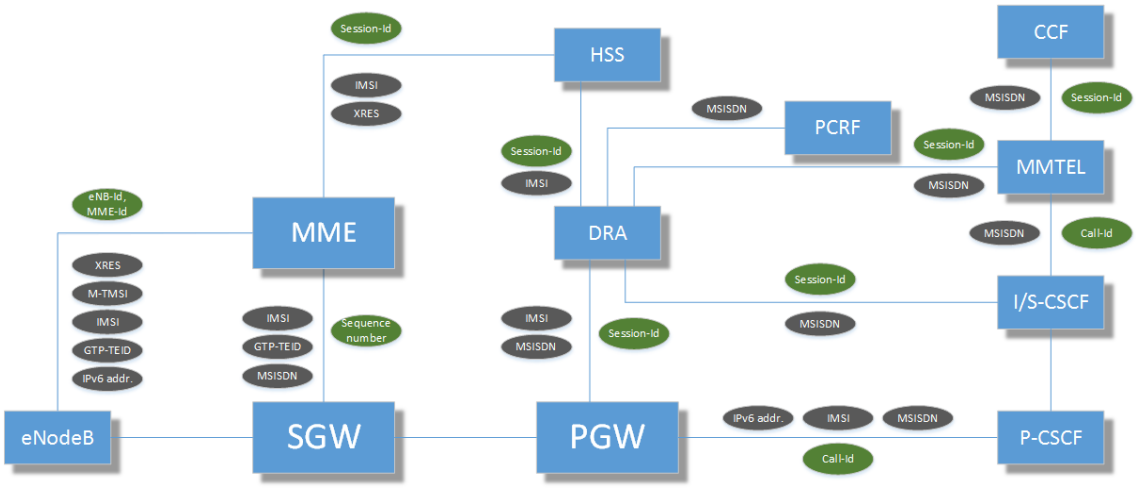
kérhet számlázási adatokat, tehát készen áll számlázási információk készítésére az adott IPv6 címhez, bearer-hez. Ettől függetlenül a számlázás VoLTE hívás esetén az IMS-ben zajlik. A Gx interfészen a *RAR* üzenetet a korábban látott *CCR* üzenet Session-Id mezője alapján kereshetjük meg, a CallTrace kliens modul segítségével.

A hívószámmal történő regisztrációt követően az MMTEL a HSS-től Diameter *User Data Request (UDR)* üzenetekben előfizetői információkat kér. Az *UDR* üzenet Public-Identity mezője tartalmazza az MSISDN-t, a User-Name mezője pedig az IMSI-t. CallTrace modult használva az előző Diameter keresésekhez hasonlóan, az *UDR/UDA* üzeneteket megtaláljuk az MSISDN vagy IMSI azonosítók és a Session-Id alapján. A regisztráció végén az információk, valamint az MSISDN és az IMSI azonosítók ismertté válnak az IMS alrendszerben található S-CSCF és MMTEL belső adatbázisaiban, és elérhetők más előfizetők számára.

A teljes regisztrációt követően lesz az előfizetőnek joga hívást indítani, illetve fogadni. A hívások során a paramétereket tekintve az azonosítók figyelésére hasonló módon van szükség. A regisztráció során ismert eljárások tökéletesen illeszkednek a hívás-felépítési folyamatokhoz. Újabb Bearer létrehozása mellett a SIP-en ismert jelzésüzenetek jól követhetővé teszik a hívás folyamatát. A VoLTE szolgáltatás aktiválása a jelzéshálózatban a kontroll üzeneteket tekintve nagyobb és összetettebb forgalmat jelent, így ennek kifejtése elegendő támpontot nyújt a hívás során generált jelzések lekérdezéséhez.

5. Automatizált folyamatok jelzésüzenetek lekérdezésére

Az üzenetek lekérdezése során egyértelműen a két legfontosabb azonosító a hívószám (MSISDN) és az IMSI, ám több más paraméter is segíti a jelzések megtalálását. Az előző fejezetben ismertetett jelzésüzenetek dialógusai a két azonosító valamelyikét szinte mindig tartalmazzák. Az 14. ábra tartalmazza az egyes berendezések közötti jelzéseket összekapcsoló paramétereket.



14. ábra A VoLTE specifikus interfészek azonosítói és összeállításukat segítő paraméterei

Az S1AP rekordok üzeneteiben legtöbbször nem szerepel IMSI, kivéve az első feljelentkezés során, vagy amikor az MME nem ismeri az előfizetőt. További csatlakozás (*Attach Request*), 2G-ről vagy 3G-ről 4G-re váltás (*Tracking Area Update Request*), vagy éppen adatforgalmazás (*Service Request*) idején kizárólag az M-TMSI szerepel az üzenetekben. Az S1AP rekordokhoz történő IMSI hozzárendelést nagy mértékben befolyásolja az aktuálisan helyesen kezelt TMSI-IMSI összerendelés, amely a titkosítás feloldásának a sikerességéből adódik. Az eNodeB-ID és MME-ID paraméterekkel összeállított rekordok lekérdezhetők a monitorozó rendszer segítségével. Amennyiben a "kititkosítás" nem volt sikeres, IMSI hiányában az S1AP jelzések felkutatásának folyamata nehézkessé válik. A HSS irányában történő autentikációs kulcskérés alatt az XRES paramétert tartalmazza az S6a és S1AP protokoll is, így a Diameter tranzakció összeállítása után is kideríthető az S1AP tranzakcióhoz tartozó IMSI azonosító. A

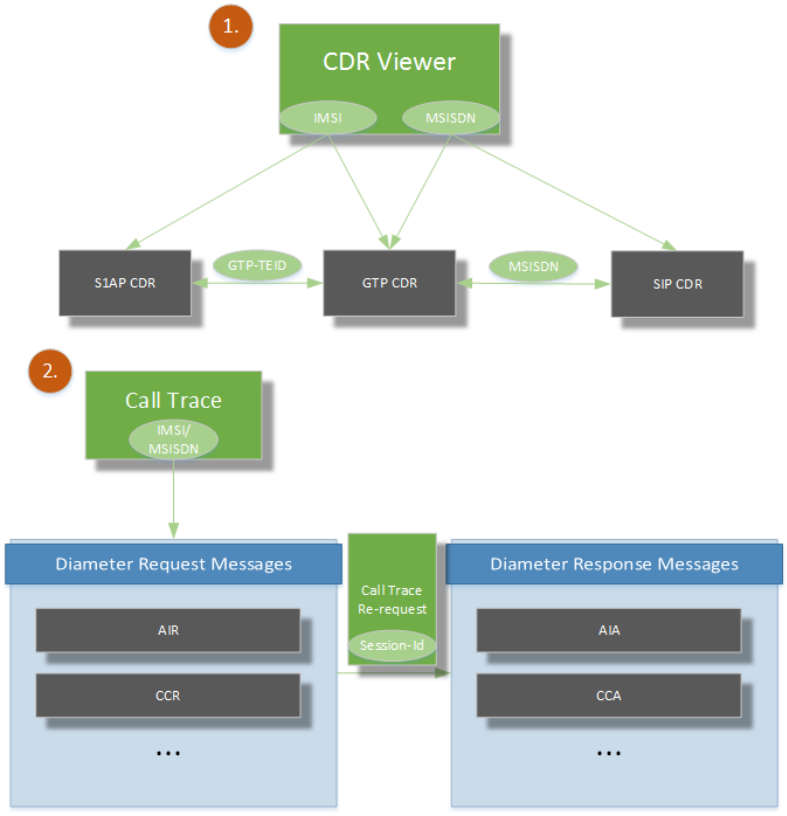
feljelentkezés során az előző fejezetben kifejtett alagutazásra vonatkozó TEID paraméterek megtalálhatók S1AP és GTP jelzésüzenetekben is, így összekötő kapocsként szolgálhatnak a rekordok, illetve jelzések visszakeresése során.

Tehát GTP tunnel-kiépítések jelzésének segítségével megtalálható az S11 interfészen utazó, hozzá kapcsolódó GTP tranzakció is, amellyel az S1AP "kititkosító" algoritmus által kapott IMSI-k leellenőrizhetők az S1AP rekordokban. A GTP request üzenetek minden esetben tartalmaznak IMSI-t, ezért alkalmazható fordított irányban is ez a módszer az S1AP hibás nyomon követése során. Az előfizetői IMSI ismeretének függvényében a TEID-et felhasználva visszakereshető minden S1AP rekord, aminek feltétele a GTP-n helyesen összeállított rekordok megléte és kereshetősége IP cím, port és a GTP rétegben található szekvencia számláló alapján. Némely GTP jelzésüzenetek MSISDN-t is tartalmaznak, ezáltal növelve a keresési lehetőségeket.

Az IMS APN-hez tartozó Default Bearer (alapértelmezett hálózati hordozócsatorna) kiépítésének jelzésére szolgáló Diameter *CCR* üzenet a Gx interfészen található. Az üzenetben szerepel a Subscription-Id mezőkben előforduló MSISDN és IMSI is. A Subscription-Id-Data mezőben található azonosítók típusairól a Subscription-Id-Type nyújt információt, így ez az üzenet akár a keresés egyik kiinduló pontja is lehet valamely azonosító ismeretében, ráadásul a VoLTE előfizetők IMSI-MSISDN adatbázisa is létrehozható a vonalról gyűjtött biztos információk alapján. A Gx interfészen a Diameter üzeneteket TCP szállítja, így szükséges a TCP szegmensek helyes kezelése és összeállítása, ezzel elkerülve az esetleges paraméterek helytelen dekódolását.

A Diameter üzenetek a hívások követését végző kliens modulban kereshetők, feltételként IMSI vagy MSISDN megadásával, ASCII vagy fordított bájtsorozat dekódolási lehetőséget választva. Az *Answer* üzenet egy újabb kereséssel található, amit opcionálisan a modul végez a Session-Id felhasználásával. A dekódolás megválasztására az egyes interfészekre vonatkozó, különböző kódolási eljárás miatt van szükség. Az intelligensebb kliensek tartalmazhatják ezeket az információkat az egyes interfészekre vetítve, emellett a különböző mezőkbe ágyazott paramétereket is kezelni képesek. Az *RA* üzenetek mivel nem tartalmaznak előfizetői azonosítót, kizárólag Session-Id segítségével kereshető vissza a teljes session.

Az S1AP, GTP és Diameter protokollok jelzései között is egyaránt megtalálható a készülék által adatátvitelre használt IPv6 cím, így valamely paraméter hiányában ez is plusz összekötő elemként szolgál. Az említett IPv6 címen kommunikál a PGW-n keresztül az LTE maghálózat az IMS alrendszerrel, így a közöttük elhelyezkedő Gm interfészen multimédia tartalom található. A SIP jelzésüzenetek mellett a hang adatcsomagokat tartalmazó RTP és az őket vezérlő RTCP csomagok is itt utaznak, amelyek közül az RTP csomagokat hatóságilag is tilos tárolni. A Gm interfészen haladó SIP jelzések Encapsulatin Security Payload (ESP) csomagolási technikával vannak ellátva, így kezelésük és dekódolásuk jelentősen nehezebb feladat. Az erre nem képes monitorozó-rendszer használata során, dekódolás hiányában hasznos lehet az IPv6 cím ismeretéről szerzett információ, mely elősegíti a jelzések különválogatását a többi előfizetőtől.

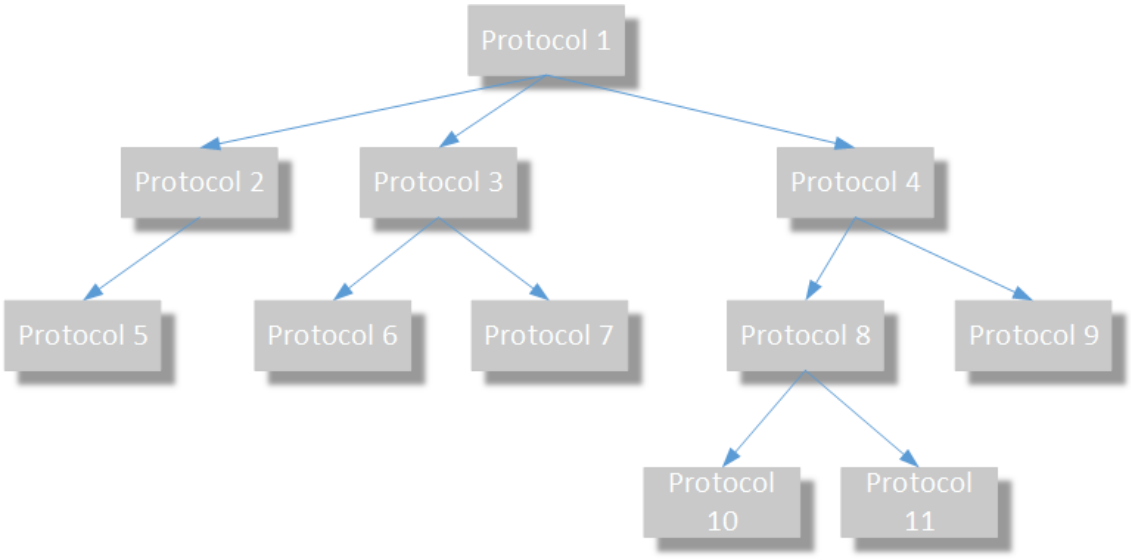


15. ábra A keresést megvalósító folyamatábra

Az IMS alrendszerben található jelzések jellemzően SIP és Diameter protokoll üzenetek, amelyek közül a SIP-en jelzett azonosítók kezelése jelentős vizsgálatot igényel. SIP esetén különböző mezőkben szerepelhet az előfizető hívószáma, valamint

hívás során a hívott MSISDN is. A hívószám sokszor nem tartalmaz helyinformációkat, ráadásul kezelésük nem egységes, így a némi intelligenciával rendelkező rendszerek gyorsabb és sikeresebb kereséseket képesek megvalósítani. A 15. ábrán megvalósított folyamatábra bemutatja a gyors keresési lehetőségeket. A művelet kezdetén a rekordokat lekérdező kliensben bármelyik azonosító megadásával, láthatóan mindhárom protokoll rekordjai megtalálhatók, ám az intelligencia bevezetéséhez kitüntetett paramétereket kell definiálni. A GTP-TEID vagy MSISDN paraméter megtalálása elősegíti a folyamat továbblépését. A Diameter üzenetek sokrétűségéből adódóan nehéz egységes Diameter rekordokat készíteni, ezt küszöböli ki a CallTrace híváskövető kliens, amely összerendeli az összetartozó jelzésüzeneteket.

Természetesen a felhasználók mindig egyszerűbb és gyorsabb funkciókat szeretnének, amelyhez az egész rendszerre kiterjedt okos kliens megvalósítása nyújthat megoldást. A kliens protokolltól függetlenül képes felismerni a kapcsolatokat létesítő kitüntetett paramétereket, így az algoritmus futása közben folyamatosan talál új paramétert, amely segítségével újabb interfészekre jut. A megvalósítás kizárólag alaposan átgondolt algoritmus elvén működhet helyesen, mivel az összerendelő paramétereket helyesen kell kezelni, ugyanis túl nagy időkorlát beállítása esetén található több előfizetőhöz is megegyező alagút végpont-azonosító (TEID), vagy éppen GTP szekvencia számláló. Más előfizetőhöz tartozó jelzések megtalálása kiküszöbölhető, ha a keresés egy fa struktúra szerint haladó folyamat (16. ábra).



16. ábra Az intelligens keresi folyamatot megvalósító fa struktúra

A 16. ábrán illusztrált módszer bemenete bármilyen paraméter vagy azonosító lehet, amely elindítja a folyamatot. A fa megvalósítás meggátolja a visszajutást a már megtalált interfészhez, így ellenőrizve a paraméterek helyességét kizárható a megtévesztő információ leszedése.

6. Hibakeresési algoritmusok

A minden szempontból egyszerűen használható monitorozó-rendszer biztosítja a könnyebb hibakeresési módszereket, segítségével gyorsan és egyértelműen meghatározható a fellépő hiba forrása. A szakértők egy monitorozó-rendszerben jóval inkább a problémák felderítésének lehetőségeit látják, a forgalom egyszerű visszakövetésével szemben. E fejezet a hiba-ok analízis során lehetséges folyamatokat mutatja be az egyes protokollokra vetítve.

Az előző fejezet alapján, a VoLTE funkciót igénybe venni szándékozó előfizető hálózathoz csatlakozása és hívása során több, különböző protokoll jelzésüzenetei monitorozhatók. Bármely protokoll esetén található hibaüzenet a forgalmazás során, így széleskörű hiba-ok analízis végezhető.

A maghálózatban monitorozott S1AP jelzésüzenetek közül néhány kérés (request) típusú üzenetre érkezhet hibát jelző válasz. A csatlakozás (attach) során számolható sikeresség, mely igen fontos mérőszám lehet az előfizetők feljelentkezését illetően. A sikeres csatlakozáskor *Attach Accept* üzenet érkezik, a sikertelen pedig *Attach Reject* válasszal zárul, így mindkét esetben számolható egy rendszert jellemző arány. Az S1AP során alkalmazott SCTP szállítási protokoll fellépő problémái, asszociációk megszakadásai és újraadásai a TCP-hez hasonló módon figyelemmel követhetők [23].

Az S1-MME interfészen vizsgálható Dedicated Bearer létrehozását jelző üzenetre sikeres esetben *Successful outcome* válasz érkezik, így a valódi sikeresség paraméterek figyelésével jól mérhető. Az itt tapasztalható sikertelenséget elsősorban a rádiós kapcsolat problémája okozhatja.

A GTP protokoll szállítása UDP-n keresztül megvalósított, így a veszteségmentes transzport a request-response darabszám számlálásával és szekvencia azonosítók követésével ellenőrizhető. Az alagút sikertelen felépülését a kezdeményező GTPv2-C *Create Session Request* üzenetre érkezett *Create Session Response* válaszüzenet különböző cause értéke egyértelműen mutatja.

Az IMS-ben zajló, berendezések közötti kommunikáció nagyrészt SIP üzenetek segítségével követhető. Az előzőekben bemutatott SIP szöveges kódolásának és az SDP tartalomnak köszönhető nagy mérete miatt gyakran IP szinten darabolódik. Az IP

összeszerelést valós időben ajánlott megoldani a helyes rekord-összeállítás eléréséhez. A szállítási funkciót mind az UDP, mind a TCP megvalósíthatja, mely helyességét előbbi esetén részletesebb tranzakció-szintű kérés-válasz figyelés ellenőrizheti, ugyanis az UDP nem biztosítja a veszteségmentes átvitelt. Ha a csomagokat TCP szállítja, a szegmentálódás során létrejött üzenet-darabok szorulnak összeszerelésre a helyes dekódolás és időpecsételés eléréséhez. A IMS-ben történő regisztráció helyessége előfeltétele a rendszerhasználati jogosultságnak, így kiemelt jelentőséggel bír. Hívás során a szabvány szerinti *INVITE* kezdetű és *BYE* üzenettel végződő SIP session figyelés elegendő lehet a hiba detekcióra. A SIP által használatos különböző hibakódokkal jelzett válasz-üzenetek is okot adnak a mélyebb analízisre, amelyre a hívásrekord-összeállítás során alkalmazott hibás zárási okok használata és a sikerestől való megkülönböztetés figyelmeztet [25].

Diameter protokollon történő hibajelzés előfordulhat sikertelen csatlakozás során, amelyet egy sikertelen Update Location jelez – ilyenkor gyakori probléma, hogy az előfizető a HSS-ben nincs regisztrálva. A Diameter válasz (answer) üzenetei Result code szerint is csoportosíthatók. Minden válasz üzenetben szerepel a Result code paraméter, amely sikeres tranzakció esetén *2001 diameter success*, ritkább esetben *2002 diameter limited success* kódot tartalmaz. Jellemzően roaming eseteknél túl nagy késleltetés léphet fel az üzenetváltás során, ekkor az MME leidőzítésének következményeként sikertelen feljelentkezés történik. Az átviteli út hibájának felismerésére használatos megoldás a Diameter Watchdog funkciója. A request-response folyamat során könnyen és gyorsan detektálhatóak a nem elérhető diameter agent-ek.

Az említett protokollok jelzésüzeneteiből a megfelelő paraméterek segítségével tranzakciós rekordok állíthatók össze. Az egyes rekord-összeállítás során a nyitó és záró üzenetekre tett feltételekkel az esetlegesen hiányzó üzenetek jelezhetők, így a hiányos rekordok jelzése is a hiba-ok analízis kiindulási alapjaként szolgálhat. A hibát jelző válaszüzenetek értékei viszont egyértelműen besorolhatóvá teszik a problémát.

Összefoglalás

A VoLTE specifikus jelzések lekérdezésére képes monitorozó-rendszer használata újabb ötleteket és praktikákat nyújt a felhasználók számára. A dolgozat a szabvány alapján leírt hálózati entitások viselkedését mutatja be a tényleges jelzés-hálózaton keresztül.

Egy monitorozó-rendszer a hálózat állandó változása és fejlődése miatt a végtelenségig fejleszthető, ezáltal garantált a felhasználói élmény folyamatos növekedése. A VoLTE szolgáltatásra jogosult előfizetőhöz tartozó jelzések rendszere rengeteg hálózati berendezést, ezzel együtt számos interfészt és protokollt ölel fel. A széleskörű protokoll-használat hatására a monitorozott forgalom feldolgozása és dekódolása egyre növekvő feladatnak bizonyul, ám az algoritmusok és hibakeresési praktikák felkutatása a folyamatosan növekvő és kiszolgálásra váró felhasználói igényeket igazolja. Az intelligens világhoz közeledve az új monitorozó-rendszer szállítók a megváltozott telekommunikációs hálózathoz és elvárásokhoz igazodva teljesen más elképzelésben készítik rendszereiket az évtizedekkel ezelőtti monitorozást végző szállítókhoz képest. Egy régi, jól megszokott rendszer a mindenkor aktuális igényeket kielégítő folyamatos okosítással megbízhatóvá és gyorssá tehető, ehhez kizárólag egyszerű lépések is elengedőek.

A keresési praktikák bemutatása irányadó lehet valamennyi üzenet megtalálására a jelzéshálózatban. Az alapos vizsgálat segítségével kifejlesztett kereső algoritmusok implementálásával olyan rendszer fejleszthető, amely bárki számára könnyedén visszakereshető jelzésekkel szolgál. Az analízis hálózati linkeket és protokoll dekódolást tekintve fontos információval látja el a kliens modulok fejlesztőit. A dolgozat a magasabb intelligenciával még nem rendelkező rendszerek intelligens felhasználói számára összefoglalást nyújt a keresési opciókról, így csökkenti a keresés és elemzés hosszadalmas munkafolyamatok idejét.

Az alapvető cél egy egyszerűen használható monitorozó rendszer szállítása, amely a szolgáltatás elterjedésének hiányában még alapos ismeretekkel nem rendelkező felhasználókat is képes kiszolgálni, így előnyben részesítését más rendszerekkel szemben biztosítva, széleskörű elterjedése garantált.

Irodalomjegyzék

[1] Wikipedia: *VoLTE*

http://en.wikipedia.org/wiki/VoLTE

[2] White Paper: *IMS Architecture*, SPIRENT, 2014. ápr.

http://www.spirent.com/~/media/White%20Papers/Mobile/IMS_Architecture_White_Paper.pdf

[3] White Paper: *Circuit-switched fallback*, Qualcomm, 2012

https://www.qualcomm.com/media/documents/files/circuit-switched-fallback-the-first-phase-of-voice-evolution-for-mobile-lte-devices.pdf

[4] White Paper: *VoLTE with SRVCC*, Qualcomm, 2012. okt.

https://www.qualcomm.com/media/documents/files/srvcc-white-paper.pdf

[5] Wikipedia: *3GPP*

http://en.wikipedia.org/wiki/3GPP

[6] Maros Dóra: *A Long Term Evolution (LTE) koncepciói*, 2013. 10. 15.

http://uni-obuda.hu/users/marosd/LTE.doc

[7] D. Áron: *LTE*, 2013. okt.

http://kozeljovo.blogspot.hu/2013/10/lte.html

[8] Huawei Technologies Co: *Network Design For MT VoLTE Trial*, Issue:0.6, 2013. 12. 30.

[9] Tatai Péter.: *Távközlő hálózati folyamatok monitorozása*, 2007.08.
https://www.researchgate.net/publication/242762086_Tavkozlo_halozati_folya matok_monitorozasa

[10] Varga Pál: *Az LTE maghálózat monitorozásának kihívásai és megoldásai*, 2012.12.

https://www.researchgate.net/publication/261061792_Az_LTE_maghalozat_mo nitorozasanak_kihivasai_es_megoldasai

[11] 3GPP TS 36.413: *S1 Application Protocol*

http://www.3gpp.org/ftp/Specs/archive/36_series/36.413

[12] 3GPP TS 29.060: *General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP)*

http://www.3gpp.org/ftp/Specs/archive/29_series/29.060

[13] Papp András, Poós Krisztián: *A GPRS adatátviteli technológia és a GTP protokoll bemutatása*, 2004.08.

http://www.hiradastechnika.hu/data/upload/file/2004/2004_08/HT0408-7.pdf

[14] Faigl Zoltán: *SIP alapú VoIP hívások vizsgálata, és az IP Multimedia Subsystem (IMS) szerepének bemutatása*, 2013. 09. 18.

http://www.mcl.hu/sites/default/files/SIP_meresi_utmutato.pdf

[15] Network Working Group: *RFC 3261 Session Initiation Protocol*

https://www.ietf.org/rfc/rfc3261.txt

[16] TelcoNotes: *SIP Transactions vs. Dialogs*, 2013. 03. 13.

https://telconotes.wordpress.com/2013/03/13/sip-transactions-vs-dialogs

[17] Cisco Systems, Inc.: *Configuring SIP Message, Timer, and Response Features*, 2010. 05. 17.
http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip _15_0_book/sip_cg-msg_tmr_rspns.html

[18] White Paper, AX Series: *AAA Protocol for IMS and LTE Networks*, 2011.05.

https://www.a10networks.com/sites/default/files/resource-files/WP-A10_Networks_Diameter.pdf

[19] Pál Varga, Péter Tatai: *Advanced Methods in GPRS Network Analysis*, 2004.06.

https://www.researchgate.net/publication/261060661_Advanced_Methods_in_GPRS_Network_Analysis

[20] Daniel Kozma, Pal Varga: *Traffic Analysis Methods for the Evolved Packet Core*

https://www.researchgate.net/publication/305641105_Traffic_Analysis_Methods_for_the_Evolved_Packet_Core

[21] 3GPP TS 29.212: *Universal Mobile Telecommunications System (UMTS); Policy and charging control over Gx reference point*

http://www.etsi.org/deliver/etsi_ts/129200_129299/129212/07.04.00_60/ts_129212v070400p.pdf

[22] GSM Association: *VoLTE Service Description and Implementation Guidelines*, 2014.03.26

http://www.gsma.com/network2020/wpcontent/uploads/2014/05/FCM.01-v1.1.pdf

[23] 3GPP TS 29.229: *Cx and Dx interfaces based on the Diameter protocol*

http://www.etsi.org/deliver/etsi_ts/129200_129299/129229/10.05.00_60/ts_129229v100500p.pdf

[24] E. Ko, S. Park, S. Kim: *SIP amplification attack analysis and detection in VoLTE service network*, 2016.03.10.

http://ieeexplore.ieee.org/document/7427126/

[25] A. Ali, A. Kuwadekar, K. Al-Begain: *IP Multimedia Subsystem SIP Registration Signaling Evaluation for Mission Critical Communication Systems*, 2016.02.04.

http://ieeexplore.ieee.org/document/7396578