HADMÉRNÖK

XI. Évfolyam 1. szám - 2016. március

SZABÓ András
szabo.andras@uni-nke.hu

AZ IP TELEFON RENDSZEREK KATONAI ALKALMAZHATÓSÁG-VIZSGÁLATÁNAK LEHETŐSÉGEI

Absztrakt

Az IP alapú hangtovábbítás napjainkra kiforrott technológiává vált. A csomagkapcsolt hálózat jellegéből fakadó minőségi, üzembiztonsági hiányosságok kivédésére így számos mechanizmust és protokollt fejlesztettek már ki. Iparági szabványok léteznek a polgári rendszerek megfelelőségének ellenőrzésére. Az IP telefónia katonai alkalmazhatóságának vizsgálata azonban túlmutat a szabványoknak való megfelelőség ellenőrzésén, hiszen nyilvánvaló, hogy a műveleti területen történő felhasználás során a polgáriaktól jelentős mértékben eltérő igényeknek kell megfelelni. Cikkemben ezeket az igényeket foglalom össze, valamint megfogalmazom azokat az elvárásokat, melyek nélkülözhetetlenek ezeknek a rendszereknek a tábori-, valamint a stacioner hálózatokhoz történő problémamentes illesztéséhez. Három fő vizsgálati területet azonosítottam: üzemeltetés és üzembiztonság, információvédelem, és a más rendszerekkel való együttműködés képessége (kompatibilitás). Ezek ellenőrzésére a katonai igényeknek megfelelő vizsgálati módszereket mutatok be.

Voice over IP (VoIP) systems are stable and well-designed communication infrastructures. Performance degradation issues caused by the packet switched network are solved by system design, robust routing, spare network capabilities and special protocols. The examination of the usability of VoIP system in military communication, however, does not only mean the verification of compliance with these standards, as it is obvious that the military utilization requires correspondence to demands highly different from civilian utilization. In my article I summarized these demands and defined those expectations that are essential for the trouble free setting of these systems in the tactical, and also in the strategic networks. I defined 3 main topic of my evaluation: system operation and management, information assurance, and interoperability. I concentrated to the possible system evaluation methods for protocol stack validation, interoperability tests, network load testing and quality of service measurements (both from the network and the user perspective)

Kulcsszavak: *IPT, IP telefon, hang, katonai ~ IPT, IP telephone, voice, military*

BEVEZETÉS

Mottó: „A híradás a hadsereg idegrendszere.”[1]

Ennek a régi mondásnak a jelentősége napjainkban egyre jobban érzékelhető, hiszen a vezetés dinamikájának fokozását informatikai rendszerek alkalmazásával oldjuk meg. Ezek az idegrendszerhez hasonlóan, hálózatokba szerveződnek, és ahogy testünk mozgatása az idegrendszer nélkül lehetetlen, úgy a csapatok összeköttetés hiányában cselekvésképtelenek.

Napjainkban már nemcsak a csapatok, hanem különböző eszközök (szenzorok és fegyverrendszerek) tevékenységének összekapcsolása és összehangolása is távközlési és informatikai hálózatokon keresztül zajlik. Újabb és újabb szolgáltatások, hálózati technológiák jelennek meg, melyek helyes felhasználásával növelhetjük hatékonyságunkat. Az elektronikusan kezelt adatok mellett ugyanakkor a hagyományos hangalapú szolgáltatások is megőrizték jelentőségüket, hiszen munkavégzés során az emberi agy könnyebben tudja a fülünk által érzékelt ingereket feldolgozni. Mellette szól az is, hogy az egyéb, audiovizuális (pl.: videokonferencia) vagy szöveges kommunikáció (pl.: harcászati chat, email stb.) megértéséhez, elolvasásához a felhasználónak a képernyőre kell néznie, mellyel elvonja figyelmét a környezeti ingerektől (mivel leköti az olvasás, így például nem észleli időben a támadót). A rendszerek vezérlése pedig még kezeit is igénybe veszi, megakadályozva ezzel, hogy a környezetében zajló eseményekre megfelelőképpen reagáljon (pl.: támadás esetén viszonozza a tüzet). A hang alapú szolgáltatásoknak további előnye a magas fokú interaktivitás, mely technikailag legegyszerűbben ezen a módon biztosítható.

A vezetékes távközlés hőskorában valós, fizikai áramkörök segítségével történt az előfizetők összekapcsolása, később a digitális technika fejlődésével már az un. virtuális áramkörkapcsolt rendszerekről beszélhettünk. Az ISDN[2] rendszerek már időosztásos hozzáféréssel oldották meg az egyidejűleg kommunikáló felhasználók hívásainak kapcsolását. Ezeknek a TDM[3] rendszereknek a hátránya egyben azok előnye is. Fix a csatornakapacitás, így attól függetlenül, hogy kihasználjuk-e vagy sem, az átviteltechnikai eszközöknek azonos vonali sebességet kellett garantálniuk. Az IP hálózatok ezzel szemben dinamikus (forgalomfüggő) csomagtovábbítással működnek. A forgalom irányítása nem feltétlenül előre definiált (statikus[4]), hanem a routerek egymással folytatott kommunikációja[5] révén alakul. Az esetleges hibákat így a hálózat adaptívan tudja kezelni és a csomagokat a routing protokoll döntési logikája szerint meghatározottan a mindenkori legkedvezőbb irányba továbbítja.

A korábbi áramkörkapcsolt rendszerekhez képest tehát előrelépés az eredetileg csak adattovábbítás céljából kialakított IP hálózatokon biztosított telefónia. Az un. „Best effort” elven[6] működő csomagkapcsolt hálózatokon a telefon szolgáltatások ugyanakkor további funkciók meglétét igénylik. Ezekkel a kiegészítő üzemeltetési intézkedésekkel és technológiákkal garantálni lehet a forgalom priorizálását és a forgalomirányítók torlódásvédelmét (ezzel csökkentve a feldolgozási késleltetést).

---

[1] Ennek a mondásnak az eredete nem ismert, de feltételezhetően Neumann János „A számológép és az agy” című művében leírt analógiákból fakad.

[2] Integrated Services Digital Network - integrált szolgáltatású digitális hálózat

[3] Time-division multiplexing – időosztásos többszörös közeghozzáférési eljárás

[4] Esetenként megmaradtak a statikus irányításnál, ilyen lehet például a szervezetek belső hálózatából az internetelérésre használható kilépőpont irányába (Internetszolgáltató routere felé) történő irányítás, vagy a forgalom tűzfalakon és egyéb hálózatbiztonsági eszközökön keresztül történő továbbítása (elkerülve azt az eshetőséget, hogy egyes csomagok kikerüljék ezeket a hálózatbiztonsági eszközöket).

[5] Melyet a routing protokollok használatával folytatnak.

[6] Ezek a hálózatok esetén a csomag garantált eljuttatása a cél, a továbbítási idő annak váltakozása nem számít. Azonban a hálózat alapkoncepciójától eltérően is használjuk ma már pl.: hang-, és video továbbítására

Az IP alapú beszédszolgáltatások két kategóriába sorolhatók [1]:

Voice over IP (VoIP), az interneten, vagy elkülönülten üzemelő csomagkapcsolt hálózatokon (azok végpontjain) kialakított hangátviteli szolgáltatás, mely magába foglalja a hang alapú információ digitalizálását, tömörítését és a hálózati továbbítás érdekében a csomagok képzését (darabolás, címzés és címkézés).

IP telefónia (IPT), mely a csomagkapcsolt hálózaton történő beszédátviteli, fax és egyéb távbeszélő szolgáltatásoknak a VoIP szabványokon alapuló biztosítását jelenti (ilyen értelemben az IPT a VoIP egyik részterülete).

A korábban említett IP alapú hangátviteli szolgáltatások esetén fontos tudnunk, hogy mivel (értsd: milyen rendszeren keresztül) kötjük össze azokat. Ezért az alábbiakban felsorolom az „együttműködési" lehetőségeket.

IPT alkalmazási szcenáriók:

- Előfizetők felé (hard- vagy softphone[7]-ok alkalmazásával)
- „Legacy" készülékek felé (analóg telefonok és központok felé[8])
- Kapcsolóközpontok közé telepítve (pl.: ISDN központok összekapcsolása IP segítségével)
- IPT szolgáltatók felé[9]
- IP társközponti irányokba (azonos protokollt használók, vagy akár eltérő technológiájú központok irányába)

Tény, hogy ezeknek az IPT szolgáltatásoknak a hibamentes működéséhez a hagyományos adatátviteli alkalmazásoknál lényegesen magasabb minőségi igényeket kell biztosítani (redundáns hozzáférési hálózat, robusztus transzport hálózat, kis kapcsolási idejű hálózati eszközök stb.).

Problémaként jelentkezik, hogy a csomagkapcsolt hálózatok működési mechanizmusa miatt biztos késleltetéssel kell számolni (a csomagok képzése, csomagolása és kibontása miatt). Az IP hálózaton kialakított beszédszolgáltatások több tekintetben is a kliens-szerver architektúrát követik. Egyrészt szervereknek nevezzük a hálózat különböző pontjára telepíthető IP kapcsolóközpontokat, melyek az IP telefonok regisztrációjáért és a hívásforgalom megfelelő irányításáért felelnek, továbbá maguk a végpontok is lehetnek kiszolgálók és kliensek is egyben (mivel a hívások szempontjából az aktuális hívók a hívottak szolgáltatásait veszik igénybe). Ezért a „mindenki kiszolgálóként működik" elvért nevezik elosztott erőforrású rendszernek.[10]

A korábbi ISDN rendszerek hívás felépülési logikájához nagymértékben hasonlít az IPT működési mechanizmusa. A hívások felépülése két logikai csatornán folyik, az egyik a hívási szándékot jelzi (ez a hívás felépüléséhez, fenntartásához és bontásához szükséges jelzéscsatorna), a másik a tényleges beszédjeleket szállítja, így hangcsatornának nevezzük.

Az alábbi ábrán egy IPT hívás jelzéscsatornának protokollanalízisén keresztül mutatom be az előzőekben említetteket. A szürke sorok a jelzéscsatorna egymást követő csomagjait jelzik (pl.: SETUP), alattuk pedig a mérés szempontjából lényeges 18. csomag részletes, rétegenkénti megjelenítését látjuk. A TCP réteg felett az ISDN D csatorna layer 3-as protokollját, a Q.931[11]-et látjuk.[12]

---

[7] A softphone, szoftver alapú telefon kliens, előnye, hogy PC-re telepíthető, nem igényel új hardvert.

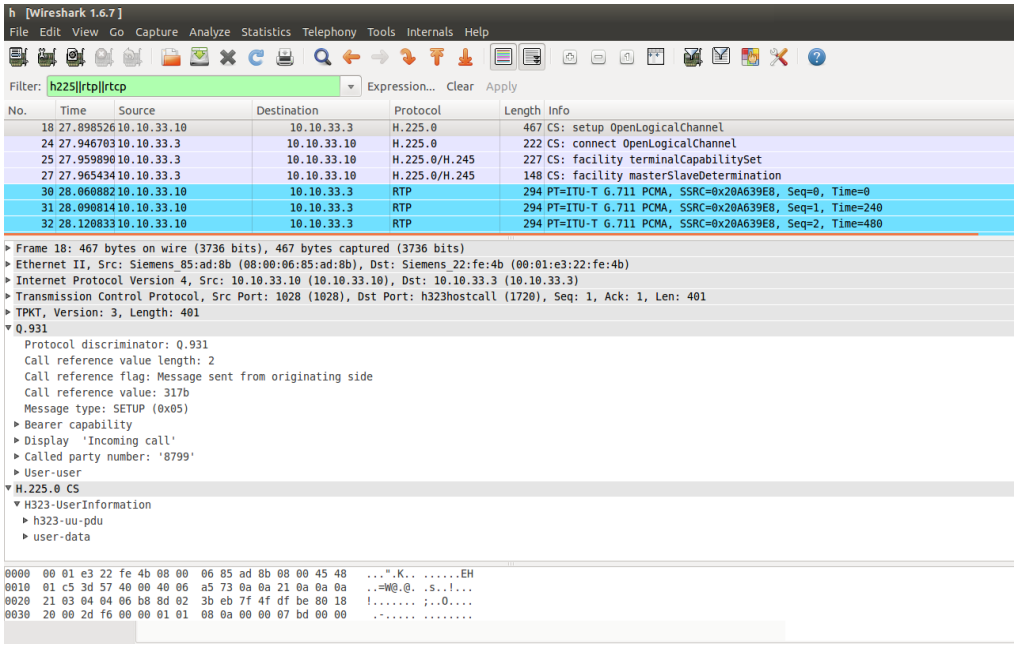
[8] Az analóg átjárást FXO (Foreign Exchange Office) , FXS (Foreign Exchange Station) eszközökön, kártyákon keresztül valósítja meg.

[9] Pl.: SIP (Session Initiation Protocol) trönk

[10] A korábbi kapcsolóközpontokban az intelligencia „központosított" volt, ezt a jelleget őrzi maga a kifejezés is.

[11] Forrás: http://www.itu.int/rec/T-REC-Q.931

[12] Megjegyzem, hogy több jelzésprotokoll is létezik, nem minden esetben ragaszkodtak a fejlesztők a távközlési hagyományokhoz, így néhány jobban hasonlít a szokványos IP hálózati protokollokhoz (pl.: a SIP protokoll szintaktikája a HTTP-hez hasonlít leginkább).



1. ábra. Az IPT és az ISDN jelzéscsatornája közti hasonlóság

A híváslogikát kiszolgáló réteg alatt a korábbiakban említett IP réteg található, mely a felhasználók számára láthatatlanul garantálja a folyamatos összeköttetést. Ez a kijelentés a kutatásomat alapvetően meghatározó kérdéseket veti fel: egyrészt hogy valóban „láthatatlan”-e a felhasználók számára, valamint, hogy ténylegesen garantálja-e a rendszer azt, amire szánták?

Elemzésemben összefoglalom azokat a szempontokat, melyeket az ilyen, katonai célú rendszerek tervezése, üzembehelyezése és továbbfejlesztése során szem előtt kell tartanunk.

ÜZEMELTETÉSI ÉS ÜZEMBIZTONSÁGI SZEMPONTOK

A katonai alkalmazásból több jellegzetesség is származik, melyek ezen rendszerek üzemeltetését, megbízható működését befolyásolják. Kezdeném a fizikai réteg sajátosságaival, hogy tábori körülmények között a polgári gyakorlattól eltérő átviteltechnikai berendezéseket és végpontokat használunk. Ezek a speciális átviteli utak jellemzően kis adatátviteli sebességet biztosítanak (pl.: RH és URH rádiók), nagy végponttól végpontig tartó késleltetést visznek a rendszerbe (pl.: műholdas kapcsolatok[13]), valamint csak időszakosan üzemelnek (pl.: az ellenséges felderítés valószínűségének csökkentése érdekében).

Ugyancsak fontos, hogy autonóm üzemre kell készíteni ezeket a rendszereket, így képesnek kell lenniük „túlélő üzemmódba” kapcsolni a külső kapcsolatok véletlenszerű leszakadása, vagy szándékos bontása (pl.: rádiócsend) esetén (és így továbbra is biztosítani a helyi érdekű összeköttetéseket).

13 VSAT: az átviteli kapacitás néhány kbps-tól 100 Mbps nagyságrendig; a késleltetés 600-900 msec (függ a földrajzi helytől és a földi állomáson végrehajtandó adatfeldolgozástól).
Inmarsat BGAN (és az ennek megfelelő fejlettségű tengeri és légi felhasználású rendszerek) átviteli kapacitása a n*100 kbps (szolgáltatástól függően lehet névleges vagy garantált); a késleltetés kb. mint a VSAT rendszereknél
Iridium: az átviteli kapacitás 2,4 kbps (garantált), vagy az Iridium Internet szolgáltatásban 10 kbps névleges, virtuális (tömörítik az adatot, így látszólag megnő az átviteli sebesség). Késleltetés kb. 100 ms (függ attól, hogy hány műholdon kell átjátszani, azonos footprintben gyakorlatilag nulla, ha a Föld túlsó felén van az ellenállomás, akkor több).

A műveleti területen telepített IPT eszközök, azok konfigurációja nehezen cserélhető, a szoftverek csak alkalmanként frissíthetőek (a leállási idők minimalizálása miatt), valamint a fizikai karbantartás (pl.: portalanítás, csatlakozók tisztítása) ritkán oldható meg.

Maga az alkalmazási környezet is számos módon nehezíti a felhasználást és az üzemeltetést. Példaképpen említhetjük a beszédérthetőségét (min. 60 dB jelszint) jelentősen rontó zajos környezetet[14]. További jellemző az impulzus-szerű zavarforrások időszakos beszédspektrumbeli „hangtüskéi" [2] (pl.: a merev, vagy forgószárnyas légi járművek le és felszállása, robbanások, kézifegyverekkel vagy tüzérségi eszközökkel kiváltott tűz, stb.), melyek a beszédjel érzékelő algoritmusok (VAD[15]) és beszédváltó (VOX[16]) áramkörök helyes működését akadályozhatják.

A felhasználás módja is eltérő, hiszen a hétköznapi életben megszokott kéttagú beszélgetésekhez képest a katonai műveletek irányítása során a csoportkommunikáció a jellemző. Ez gyakran földrajzilag nagy távolságban tevékenykedő személyek összekötését jelenti (akár eltérő hálózatok és eszközök összekapcsolása révén).

Elvárás, hogy a különböző vezetékes és vezeték nélküli eszközök egységes, egymással összekapcsolható rendszert alkossanak. Például egy, a műveleti területen tevékenykedő alegység rádión keresztül kapcsolatot tud létesíteni, a táborban vezetékes kapcsolattal rendelkező parancsnokkal, aki műholdas kapcsolaton keresztül egy szövetséges erőtől támogatást kérhet, vagy szükség esetén akár közvetlenül az elöljáró parancsnokságnak jelenhet. Ez magas fokú interoperabilitást igényel a rendszertől: a fizikai kapcsolatoktól egészen a rendszereken biztosított szolgáltatások közti átjárhatóságig. Ezek nem új típusú elvárások, a korábbi évtizedek katonai elektronikai eszközei mind ilyen igénybevételre lettek tervezve. Napjainkban azonban a polgári eszközök alkalmazása kezd terjedni, melyek elsősorban nem a katonai felhasználásra lettek fejlesztve.

Üzemeltetési szempontból az eszközök működési környezetének biztosítására is gondolni kell. Fontos szempont, hogy olyan csatlakozókkal, tartó/védő/amortizációs kerettel és belső kialakítással rendelkezzen, mely megvédi a külső mechanikus hatásokkal szemben. A hőtermelés, üzemi hőmérséklet és a tűrési tartomány is fontos paramétere az eszközöknek, hiszen egy harcjármű légkeverő-, cserélő- és szűrőrendszere (HVAC[17]) korlátozott kapacitással rendelkezik[18].

A terepen történő alkalmazás, a gyakori áttelepülések miatt az eszközöknek robusztusnak és alacsony hibavalószínűséggel üzemelőnek kell lenniük. Ez a kijelző mellőzésével, a fölösleges gombok és kapcsolók elhagyásával, az ütés-, hő-, és vízálló burkolattal, valamint a megerősített kábelekkel oldható meg.

A felhasználók kesztyűben, sisakban, lövedékálló mellényben kezelik majd ezeket, így a kézibeszélő kialakításánál ezt figyelembe kell venni. A korábban említett rádióhálókkal folytatott kommunikációnál (fél duplex üzemmód esetén) a beszédváltó gomb[19] hasznosnak bizonyul, mivel könnyebben szoknak hozzá a rádióforgalmazás szabályaihoz a felhasználók (a vezetékes távbeszélő készülékekről a rádióháló irányába indított hívások eleinte kényelmetlenek a felhasználóknak, mivel szokatlan, hogy a rádiófelvevő pont (RFP) rádióit adásba és vételbe kell a forgalmazás irányának függvényében kapcsolniuk).[20]

---

14 az irodai csendhez ~30-40 dB képest jelentősen magasabb háttérzaj ~90-110 dB egy reptéren, vagy harcjárműben stb.

15 Voice Activation Detection

16 Voice Operated Switch

17 Heating, Ventilation, Air Conditioning

18 Gyakran már létező harcjárműbe történik a beépítés, melynek HVAC rendszere nem képes kellőképp kezelni az új hőforrásokat.

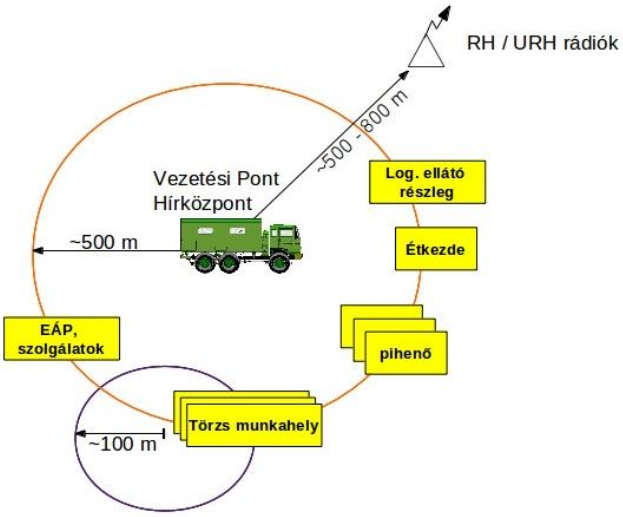
19 PTT – „Push to talk"

20 Az adás-vétel kapcsolást vagy a beszédhang érzékelésével (automatikusan), vagy DTMF jelzések kézi billentyűzésével oldják meg

Az egyszerűség a biztosított szolgáltatásokra is vonatkozik, így kerülni kell a fölösleges, a felhasználókat zavaró funkciókat[21]. A kezelőfelület ergonómiájának kialakításánál a katonai igénybevételeket kell figyelembe venni, a nagy kijelzők megnövelik az eszközök fogyasztását, karcolódhatnak, betörhetnek, valamint kültéri alkalmazásnál (napfényben) gyakran olvashatatlanokká válnak, a hosszú kábelek beakadnak a katona felszerelési tárgyaiba, a matricák, feliratok lekopnak.

Az energetikai igény szintén kulcsparaméter a tábori üzemeltetésű rendszereknél, hiszen egyrészt a kapcsolóközpontoknak képesnek kell lenniük alternatív betáplálás fogadására (ezt legegyszerűbben kettős tápegységek alkalmazásával valósítják meg), másrészt a végkészülékek helyi tápellátását sem feledhetjük. Míg az irodai környezetben „csak" csatlakoztatjuk az energetikai hálózatba a készülékeket, addig a terepen nagy árat kell fizetnünk ezért a kényelemért: egyrészt körülményes az erősáramú hálózat kiépítése (kábelezés), továbbá az aggregátoros üzemórák megnövelik az alegység üzemanyag fogyasztását (a „Wattokért literben fizetünk" és így a logisztikai biztosítást is jelentős mértékben nehezíti). Ezek alapján belátható, hogy nem mindegy, egy-egy tábori eszköznek mekkora az áramfelvétele.

Általában ezeknek a végpontoknak a tápellátását PoE[22] technológiával biztosítják az adatátvitelre használt kábeleken (az adatátviteli célra használt érpárok mellett), ezzel is csökkentve a kiépítésre szánt időt. Ez optikai kapcsolatok esetén nyilván nem alkalmazható, ami tovább nehezíti a híradó, logisztikai biztosító erők munkáját.



2. ábra. A Vezetési pont híradó és informatikai központjának (VP HIK) települési rádiuszai

A vezetési pontok hírközpontjától a törzsmunkahelyek tipikusan 100-300 m sugarú körön belül helyezkednek el (az alkalmazási környezet figyelembevételével készített híradó terv függvényében). A kültéri kábelek esetén készülve az EMC problémákra, a nem szándékos EM kisugárzás[23] elleni védelemre, valamint az elektronikus pusztítás lehetőségének kizárására optikai kapcsolatokat célszerű alkalmazni. Ellenkező esetben megfelelő túlfeszültség elleni védelemmel kell ellátni a réz vezetékeket (ennek alkalmazása a kábelek induktív és kapacitív jellegének változását, így a gyártó által vállalt vonalai paraméterek rontását vonja maga után).

[21] A zavaró alatt itt olyanokra gondolok, mint amelyek elvonják a figyelmét, vagy a szükségesnél bonyolultabban használhatóak
[22] PoE – Power over Ethernet
[23] ún. TEMPEST

3. ábra. A VP HIK technikai elemei

A fenti ábrán jól látható hogy különböző külső kapcsolati lehetőségek biztosítására kell készülni, melyek eltérő interfészek, protokollok használatát igénylik. Mindez (a belső, külső kapcsolatokban alkalmazott eltérő protokollok) megnöveli az üzemeltető állomány munkáját, hiszen ismerniük kell az eszközök, protokollok konfigurálásának módját, továbbá több hibalehetőségre is készülniük kell (a hibafa ágainak száma és azok komplexitása is növekszik [3]). A tábori körülmények közti alkalmazásnál figyelembe kell venni, hogy nincs minden alegységben rendszermérnök, ezért az eszközök távelérése, mélyreható távdiagnosztikai képessége nélkülözhetetlen.

LAN oldali követelmények

A hozzáférési hálózatok esetén azok kapacitása, redundanciája (eszközök és kapcsolatok szempontjából), hibatűrő képessége (pl.: hurokkezelés), a támogatott interfészek szabványossága, az adat, és a hangforgalom szeparációja (pl.: külön adat-, és hang VLAN) valamint a szolgáltatásminőséget biztosító technológiáik (priorizálás, torlódáskezelés) az elsődleges vizsgálati szempontok. Második, (pl.: 802.1Q [4]) és harmadik rétegbeli (pl.: IP DSCP [5]) jelölésekkel, hozzáférési listákkal, valamint megfelelő hardveres támogatással és tartalékkal, a kapcsolóeszközök felkészíthetőek a valósidejű forgalom minőségvesztés nélküli kezelésére. Ezek a képességek sajnos a katonai kivitelű switch-ek esetén gyakran nincsenek biztosítva, pedig már a hozzáférési hálózat is megalapozza a WAN oldali QoS[24] biztosítását.

WAN oldali követelmények

Az IP hálózatok nagyszerűsége abban a tulajdonságukban rejlik, hogy az egymással kommunikáló végpontoknak nem kell törődniük az egymáshoz vezető útvonal megtervezésével. Arról a hálózat saját „intelligenciája” gondoskodik. Bizonyos esetekben ugyan szükséges a statikus[25] irányítás, de az „öngyógyító” képességekkel bíró IP hálózat dinamikus forgalomirányítást igényel.

A kapcsolási logika különbözőképpen határozhatja meg a csomagtovábbítás irányát. A forgalomirányítási algoritmusok súlyozhatnak a legrövidebb (értsd: a legkevesebb forgalomirányító érintésével történő továbbítás), a legnagyobb sávszélességű, a legolcsóbb (pl.: bérelt vonalak, eltérő ár/bit értékű átviteli utak esetén), vagy a legkisebb késleltetésű (ahol a legkisebb lesz a torlódás) útvonal alapján. Az IPT rendszerek esetén még egy, az IP fölött

24 Quality of Service (QoS) - szolgáltatásminőség
25 Előre, kézzel definiált

működő kapcsolási logikára is ügyelni kell, a hívószám kiértékelésre. Az IP hálózatok forgalom irányítása összetettebb, több a hálózaton elosztott erőforrástól függ, mint a központ-orientált ISDN.

A korábbi ISDN rendszerekben a hívott fél telefonszáma (Called Party Number) alapján értékelték ki a kapcsolóközpontok a hívást, szükség esetén manipulálták azt, és végül irányították a megfelelő irányba. A hívó fél száma (Calling Party Number) a hívószám helyes megjelenítése miatt és egyéb kényelmi szolgáltatások (pl.: visszahívás) működéséhez kellett.

A hang (valamint minden egyéb valós idejű adat) továbbítása abban az esetben lehetséges a megfelelő minőség garantálása mellett, ha már a hálózat tervezésénél gondoltak erre. A különböző típusú forgalmakat így osztályokba lehet sorolni, majd ezekhez az osztályokhoz eltérő továbbítási prioritást lehet rendelni. Ezzel a forgalomirányítók döntési sebességét lehet növelni a késleltetésre érzékeny forgalom esetén. A forgalomirányítónkénti döntések elkerülése érdekében hozták létre a címke alapú kapcsolást (MPLS[26]), mely esetén a belépő (un. Ingress) és kilépő (un. Egress) routereken történik csak IP alapú irányítás (az MPLS hálózaton belül pedig a címke alapján kapcsolnak az eszközök). Ezzel a technológiával egyrészt csökkenthető a csomagtovábbítási-, feldolgozási késleltetés, valamint megoldható az eltérő jellegű forgalom logikai szeparálása is, így megteremtve a lehetőséget a priorizálásra.

Az MLPP[27] a katonai hálózatokra jellemző priorizálási séma, melynél a forgalom jellege mellett fontos a szervezeti hierarchiába betöltött szerep is. Ennek segítségével torlódás esetén objektív módon megállapítható a hívásra jogosultak köre, valamint biztosítható, hogy az erőforrások számukra legyenek csak kiosztva [6].

Információvédelmi szempontok

Fontos, hogy felhívjam a figyelmet arra, hogy a *„Minden IP felett”* és a *„Bármi bárhonnan elérhető”* valamint *„Mindent összekötni mindennel”* hangzatos koncepciók azonban a hálózataink nyújtotta szolgáltatásokat nem csak a jogosultak érhetik el, ezért számoljunk ezen mottók árnyoldalával is.

Nyilvánvaló, hogy katonai rendszerek esetén a hálózatbiztonsági és információvédelmi igények prioritást élveznek. Az IP alapú hangtovábbítás esetén ugyanolyan mértékben kell védeni a rendszert az illetéktelen hozzáféréstől, lehallgatástól és támadástól, mint ahogy az már a „hagyományos” elektronikus adatok esetén megszokott. A probléma abban rejlik, hogy a megszokott védelmi eljárások esetenként egyáltalán nem, vagy csak lényegi módosításokkal alkalmazhatóak. Így például az IP alapú csoportos rejtjelező berendezések megnövelik a csomagtovábbítási időt (késleltetést visznek a rendszerbe), a tűzfalak pedig nehezen kezelik a dinamikusan meghatározott port nyitásokat (pl.: az RTP forgalom számára). Mivel kevéssé ismertek az IPT rendszerek elleni támadások szignatúrái, így a védelmükben alkalmazható IDS/IPS rendszerek hatásfoka is alacsony. A végpontok jelzés és beszéd csatornáinak rejtjelezése nagy számítási kapacitást igényel (mely a beágyazott rendszerek processzorait jelentősen terheli), valamint további infrastruktúra elemek nélkül nem működik[28]. A végpontok szoftverének frissítése és a biztonsági javítások telepítése időigényes procedúra, amely sajnos gyakran csak kézzel oldható meg.

Az új technológia terjedését követően a támadások számának drasztikus emelkedésével is számolni kell. A jogosultságok kezelése ugyancsak fontos lehet, hiszen megakadályozható vele az illetéktelen felhasználás, vagy a megszemélyesítés jellegű támadások. A több szintre osztott hívásjogosultságok segítségével a kimenő forgalom mennyisége is csökkenthető, amennyiben csak azok kapnak a trönk kapcsolatokhoz hozzáférést, akiknek a munkájához nélkülözhetetlen.

26 Multiprotocol Label Switching
27 Multilevel Precedence and Preemption
28 Pl.: DNS (névfeloldás), DHCP (automatikus címosztás) szolgáltatás

Biztonsági szempontból is fontos a hang-, és az adat forgalom szeparálása. Ahogy korábban említettem, a hangforgalom bináris tartalom, így a használt jelzés protokollok a biztonsági eszközök számára nehezen feldolgozhatóak, ennek következtében egy támadó akár rejtett csatornát (covert channel-t) is kiépíthet, amennyiben hanghívásoknak álcázza kártékony forgalmát [7].

Az eszközök helyes konfigurációja a jogosulatlan hívások [8] kezdeményezése és az illetéktelen lehallgatás [9] megakadályozása miatt is lényeges.

Az IP alapú trönk kapcsolatok biztonsága növelhető VPN kapcsolatok kialakításával, valamint a társközponti hitelesítés bevezetésével [10].

Interoperabilitási-, kompatibilitási szempontok

Minden informatikai és távközléstechnikai innováció esetén, ha költséges, vagy nem megoldható a teljes rendszer lecserélése, akkor biztosítani kell a régi rendszerekkel történő együttműködés lehetőségét. Fontos kiemelni, hogy az eltérő technológiák sokszor nem, vagy csak korlátozott mértékben tudják egymás szolgáltatásait igénybe venni, esetleg összekapcsolásuk csak gyártó-specifikusan oldható meg (pl.: főnök-titkári híváskezelői szolgáltatás). A tábori és a stacioner hálózatokon biztosított szolgáltatások az azokat felhasználó alegységek eltérő igényei miatt különbözhetnek (pl.: műveleti területen a hangposta szolgáltatás nem feltétlenül szükséges).

Az interoperabilitás mint igény, stacioner hálózat esetén a társszervekkel való együttműködés (rendőrség, katasztrófavédelem, stb.), tábori hálózat esetén pedig a hadműveleti terület híradásának többnemzeti biztosítása során jelentkezik. A különböző szövetségi rendszerek standardizálási szándéka ellenére a gerinchálózaton (Core network) túl minden nemzet a saját igényei és lehetőségei szerint fejleszti hálózatát. Ezért fontos időszakosan tesztelni az új eszközök együttműködési képességét.

Ugyan hazai sajátosság, de fontos kiemelni, hogy a fejlesztések és eszközbeszerzések gyakran több ütemben folynak le, így eltérő gyártmányú, vagy eltérő verziójú eszközök kerülnek a hálózatba. Ezek között is biztosítani kell az összeköttetést és a szolgáltatások problémamentes elérését. A jelenlegi alkalmazási trendek és a várható szcenáriók alapján összefoglalva, egy katonai célú IPT kapcsolóeszköznek kompatibilisnek kell lennie:

- a települési hely szerinti polgári IPT szolgáltató rendszerével (akár műveleti területen is),
- más nemzetek, szövetséges haderők kapcsolóközpontjaival,
- régi, ún. „legacy" rendszerekkel (analóg, ISDN kapcsolóközpontokkal, RFP-kal),
- más gyártmányú IPT központokkal azonos, és eltérő protokollokon keresztül egyaránt.

Ezeket, a fent felsorolt lehetőségeket tesztelni kell a gyakorlatban is, hiszen az együttműködési képesség többet kíván, mint csupán az eszközök gyári leírásainak egyeztetését.

Fontos, hogy az IP kapcsolóközpontok más gyártók végkészülékeivel is kompatibilisek legyenek. Ezt a feltételt mind az alap, mind a kiegészítő szolgáltatások tekintetében vizsgálni kell. Ne felejtsük el továbbá, a végkészüléket a felhasználóknak a valós alkalmazási környezetben is tesztelniük kell. Az eszközszintű interoperabilitás-tesztek mellett rendszerszintű konfiguráció ellenőrzéseket is kell végezni, hogy az üzemeltetők ismerjék a lehetséges beállítások közül a megfelelőeket, és amennyiben a szituáció megköveteli, alkalmazni is tudják azokat. Erre jó példa a NATO kezdeményezésére 1995 óta minden évben megszervezésre kerülő „*Combined Endeavor*" [11] gyakorlatsorozat, mely a tagállamok informatikai és távközlési képességeinek összecsiszolására szolgál.

A korábban említett RFP-ok két csoportra oszthatóak: általános esetben az eszközök egy analóg (pl.: CB) távbeszélő mellékre csatlakoztathatóak, ritkábban valamilyen digitális (többnyire gyártó specifikus) mellékre köthetőek. Ezeknek a rendszereknek a vezérelhetősége,

valamint a biztosított hangkapcsolatok minősége kritikus, ezért vizsgálatuk feltétlenül szükséges.

Másik problémás terület a rejtjelezés. A biztonságos telefon, vagy fax összeköttetésre használt analóg rejtjelező berendezések, vagy modemek kommunikációjának digitális szakaszon történő átvitele kényes terület. Ezek egyedi, gyakran csak a fejlesztők, gyártók által ismert kommunikációs protokollokat használnak, és mivel általában meglehetősen kevés dokumentáció található ezekről, így vizsgálatuk csak empirikus teszteléssel, a paraméterek finomhangolásával oldható meg.

Ha az egyéni rejtjelző eszközök nyílt üzemmódban dolgoznak akkor un. *non secure-indication tone* [12] jelzést adnak ki. A felhasználóknak így felhívják a figyelmüket arra, hogy védtelen a csatorna és ezért csak nyílt információkat osszanak meg egymással. Az IPT-nél esetünkben ez azt jelenti, hogy a rendszernek kezelnie kell ezt a jelzést (bejövő hívás), esetenként pedig még generálnia is szükséges (kimenő hívás). Ugyancsak problémát jelenthet a RFP-kal történő kommunikáció esetén, hogy ez a folyamatosan generált beszédcsatornán belüli jelzés (pl.:*secure-indication tone*) adásban tartja majd a rádiókat.

Tesztkörnyezet

Korábbiakban felsoroltam számtalan elvárást, melyekre katonai rendszerek tervezése során ügyelni kell. A következőkben egy tesztkörnyezet kialakításának lépéseit vázolom, mely kifejezetten a távközlési igények vizsgálatára szolgál.

LAN / WAN tesztek

Mint ahogy korábban említettem, az IPT esetén előnyös, ha szeparált a hálózat különböző jellegű és rendeltetésű forgalma (belső levelezés, célrendszerek adatforgalma, hálózatmenedzsment stb.). Ez tesztelés esetén azt jelenti, hogy vlan-onként (sub interfészenként), vagy akár több fizikai interfészen is eltérő jellegű forgalmat kell generálnunk (web böngészés, fájltranszfer, mellette konstans sávszélességű radaradat, esetleg meteorológiai jelentések, valós idejű hang és video, stb.). Így a különböző forgalmak egymásra gyakorolt hatása is vizsgálható, valamint az eltérő forgalmi osztályokra érvényes továbbítási prioritás és a garantált sávszélesség is validálható.

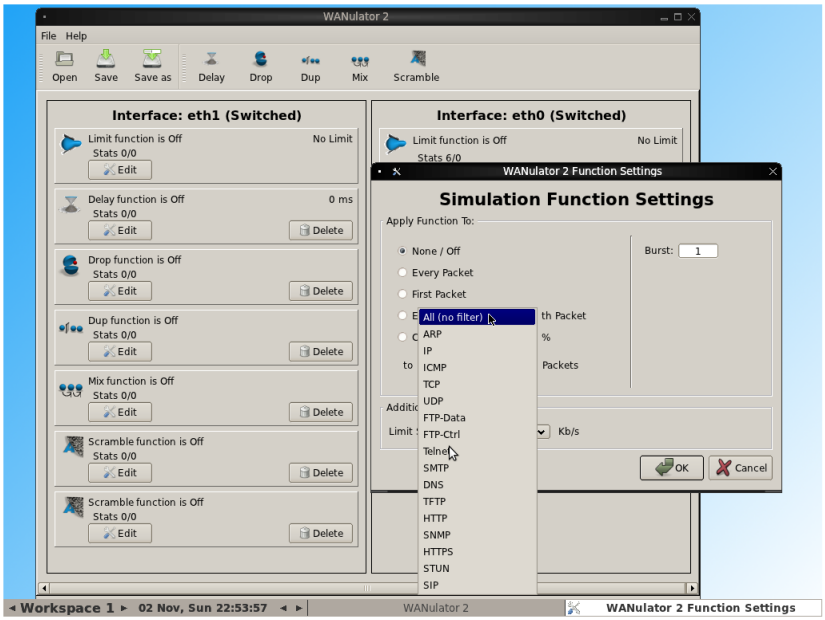
Az átviteli hibák minőségre gyakorolt hatását labor környezetben is lehet vizsgálni. Ethernet interfészek esetén az IP alapú átviteli út hibáinak szimulálására az alábbi ingyenesen elérhető eszközök alkalmazhatóak:

- WANULATOR[29]
- WanEM[30]
- WanBridge[31]
- Fragroute[32]

Saját tapasztalataim azt mutatják, hogy ezek az eszközök viszonylag könnyen kezelhetőek, a különböző mérési szcenáriók közti váltás könnyű, azonban célszerű a beállítások pontosságáról az „élés” mérés előtt külső alkalmazásokkal (ping, netcat, Ipref stb.) meggyőződni. Ennek a célja a kezelő általi mérési hibák kivédése. Az alábbi ábrán (4. ábra) látható, hogy például a WANulator kezelőfelülete könnyen átlátható (az oszlopokban a csatlakoztatott interfészek, a sorokban a hozzájuk beállított forgalmi paraméterek láthatóak), azonban hihetetlen komplex szcenáriók tervezhetőek segítségével (pl.: az adatátviteli

29 LÁSD: http://wanulator.de/
30 LÁSD: http://wanem.sourceforge.net/
31 LÁSD: http://code.google.com/p/wanbridge/
32 LÁSD: http://www.monkey.org/~dugsong/fragroute/

sebességet korlátozzuk 512 kbps-ra, az UDP csomagokat késleltessük 500ms-al, dobjuk el minden 5.dik IP csomagot, és minden 3. csomag beérkezési sorrendjét változtassuk meg).



4. ábra. WANulator kezelőfelülete

A felhasználói célú Ethernet interfészek (a laptopokba, PC-be szerelt általános felhasználású interfészek) nem képesek a vonali sebességet teljes mértékben kihasználni, amennyiben a mérés ezt megkövetelné, akkor speciális, kifejezetten ilyen célra kialakított interfészeket[33], vagy mérőműszereket[34] kell használni.

Speciális szabványok, interfészek (pl.: E1 keretstruktúrájú G.703 interfészek) esetén célhardver szükséges, mely segítségével az átmenő forgalomba lehet hibát iktatni („Error injection" funkció). Az optikai interfészek tesztelése szintén céleszközzel oldható meg, vagy esetleg média-konvertert (elektrooptikai átalakítást) igényelhet.

A valós interfészeken, átviteltechnikai berendezéseken lefolytatott hosszútávú mérések statisztikai elemzése révén kialakíthatóak olyan profilok, melyekkel később a fent említett tesztkörnyezetben szimulálhatóak egy kialakítás előtt álló rendszer minőségi mutatói.

A fizikai szintű hibák mellett a forgalomirányító eszközök hibás beállításaiból fakadó egyéb anomáliák (pl.: route irányok „billegése", aszimmetrikus routing, stb.) tesztelése is megvalósítható, azonban célszerű kerülni a hardver emulációt, mivel a forgalomirányítók speciális hardverére írt operációs rendszerek virtuális környezetben (pl.: GNS3) a valóstól lényegesen eltérő hálózati mutatókat (pl.: késleltetés, csomagvesztés) produkálnak.

Kompatibilitás tesztek

A hálózatok határain (a gateway-eken) a beszédkódolás algoritmusának váltása (az un. transzkódolás) veszteséges kodek-ek esetén problémát jelenthet, hiszen azok jelentősen ronthatják a beszéd érthetőségét. Ezek hatásainak megállapítása érdekében az eltérő szolgáltatás (pl.: konferenciahívás, egyéni hívás, hangposta, stb.) igénybevételével különböző irányokba és onnan visszafelé is hívásokat kell generálni, azokon pedig a beszédérthetőséget vizsgálni kell (lásd később). A hang mellett a fax közlemények továbbíthatóságát is ellenőrizni kell, mivel a veszteséges tömörítést használó kodekek a G3 szabványú, analóg fax berendezések

[33] Erre jó példa a Riverbed cég mérő interfésze Lásd: http://www.riverbed.com/products/performance-management-control/network performance-management/ethernet-packet-capture.html
[34] Erre példa Lásd: http://www.equicom.hu/?q=hirek/hir/303 , http://www.equicom.hu/?q=hirek/hir/79

jelzéseit torzítják (ezért célszerű digitalizálni az analóg fax közleményeket, és úgy továbbítani azokat a hálózaton).

A beszédjel feldolgozását célhardverrel un. DSP[35]-kkel oldják meg. Az eltérő kodekekhez más-más áramkör szükséges, esetenként előfordulhat, hogy egy nagyobb kapacitású eszköz (pl.: több analóg porttal rendelkező router, ATA[36]) egy időben csak néhány tömörítetlen (pl.: G.711) kapcsolatot képes kezelni, ha például a hadműveleti követelmény ezt nem engedélyezi, akkor több eszközzel, tartalék kapacitásokkal kell számolni.

Szolgáltatások tesztelése

Ezeknél a vizsgálatoknál megkülönböztetjük az alap (a kapcsolási mátrix, hangkodekek, feldolgozó áramkörök), és a kiegészítő szolgáltatások tesztelését. A gyártók eltérő szolgáltatásokat biztosítanak, még ha sokszor azonos néven is hirdetik azokat. Mivel azonban eltérő a megvalósításuk, ezért a felhasználón múlik, melyik rendszert részesíti előnyben a megbízhatóság, a szolgáltatás bőség, vagy épp az ár szempontjából. A különböző felhasználók ezért eltérő eszközöket vásárolnak, a probléma akkor kezdődik, ha ezeket megpróbálják közös rendszerbe illeszteni. Az alapszolgáltatások tekintetében semmiképpen sem, a kiegészítő szolgáltatások esetében mérlegelhetünk, hogy a korábbi elvárásainkból engedünk vagy sem.

Általában a gyártók a teljes szolgáltatási palettájukat csak a saját fejlesztésű protokolljukon keresztül biztosítják, ha másokkal együtt akarunk működni, akkor pedig az egyszerű, SIP protokollt javasolják. Meg kell jegyezni, hogy a SIP protokoll szolgáltatások terén visszalépés a 20 évvel idősebb ISDN-hez képest. Így ezzel nagy árat fizetünk az együttműködési képességért: bizonyos szolgáltatásokat csak saját hálózaton belül tudunk hibamentesen biztosítani.

Beszédérthetőség vizsgálatok

Az IPT hatékonyabbá tudja tenni egy szervezet távközlési infrastruktúráját, azonban ha az csak rosszminőségű hangot képes továbbítani, vagy a korábbi szolgáltatásokat nem támogatja, esetleg használata problémás, akkor e negatívumok miatt a felhasználók elutasítóak lesznek a technológiával szemben. A hangalapú szolgáltatások minőségének mérése nehéz, hiszen a mérés lényege az objektív ítéletalkotás, míg a beszéd érthetősége egyén függő.

Az IPT rendszerek minőségének megítélése tovább nehezedik, hiszen a csomagkapcsolt hálózatok műszerekkel mérhető mutatóival (késleltetés, jitter, csomagvesztés, stb.) összefüggésben kell a hang alapú szolgáltatások minőségét (beszédérthetőség, szolgáltatási minőség) értékelni.

A beszéd minőségének vizsgálatát mind a végkészülékek, mind a gateway (IP-IP, ISDN-IP, analóg-IP) eszközök bevonásával meg kell tenni, hiszen a protokoll vagy interfész konverziók jelentős torzítást iktathatnak be.

Megkülönböztethetünk:

Objektív[37] és szubjektív[38], valamint
Aktív[39] és passzív[40] méréseket.

A beszédérthetőség vizsgálata elvégezhető szubjektíven, emberi tesztalanyok bevonásával. A mérés pontossága ekkor függ a hallgatóság megítélésétől, ezért a statisztikai pontosság nagyszámú, hasonló körülmények között elvégzett értékeléssel növelhető. A hallgatóság

35 Digital Signal Processor, digitális jelfeldolgozó processzor
36 Analogue telephone adapter
37 Számítógépes mérések, melyek eredményei függetlenek a mérést folytató személytől
38 Az emberi értékelőtől, a vizsgálatot lefolytató személytől függő mérés
39 Mely esetén a beszédjelet a mérőműszer állítja elő/játssza le az adó oldalon, a vételi ponton pedig rögzíti
40 Ez esetben a forgalom generálásában nem vesz részt a mérőrendszer

általában szótag/szó/mondat érthetőséget, a hangerőt és a hangtisztaságot értékelik. A MOS[41] eljárást szokás ekkor használni.

Az automatizálható, ismételhető gépi megoldások napjainkban jellemzően a PESQ[42] eljáráson alapulnak.

MOS vizsgálat [13]

Segítségével 1 és 5 közötti skálán értékeljük a vevő oldalon értékelhető beszéd minőségét. Az ITU P.861 (PSQM), valamint a P.862 szabványa írja le teljes egészében számításának részleteit.

PESQ eljárás [14]

Ez a módszer előre felvett hanganyag adó oldali lejátszására és vevő oldali rögzítésére, vagy spontán tesztanyag készítése esetén adó és vevő oldali beszéd rögzítésére és későbbi összehasonlítására épül. Különböző algoritmusokkal kompenzálják a két hangfelvétel közti idő-, és amplitúdóbeli változásokat (annak érdekében, hogy összehasonlítható legyen a két hangfájl). Az amplitúdó csillapítás, frekvencia torzulás mellett az additív zajt, valamint az időszakos megszakadásokat is figyelembe veszi a módszer.

A korábban említett zajos környezet miatt a készülékek kézibeszélőjét is érdemes vizsgálni, valamint az olyan kiegészítő funkciókat, mint a VAD, vagy a komfortzaj előállítást[43]. Ezek például hangvezérelt (VOX) rádió-felvevőpontok esetében hibát generálhatnak (adás-vétel billegés) [15].

Veszteséges kodekek esetén a sávon belüli jelzések (pl.: DTMF kódok) torzulása is problémát jelenhet (megakadályozva az erre a jelzésre alapú szolgáltatások igénybevételét).

Terheléses vizsgálatok „Regression testing"

A csomagkapcsolt hálózatok kapacitás korlátai nem olyan markánsak, mint a vonalkapcsolt, vagy áramkör kapcsolt rendszereké. Így szükséges a maximális csatornakapacitás ellenőrzése annak érdekében, hogy validálható legyen az, hogy az erőforrások elégségesek a tervezett kapacitás kiszolgálására.

Az egyidejű hívások számát több tényező is befolyásolja. Így például a párhuzamos forgalom (web böngészés, letöltések, adatbázis elérés, online szoftverfrissítések stb.), a rejtjelezés, a traffic padding (forgalomanalízis elleni tevékenység), a használt alsóbb rétegbeli protokollok jellemzői (pl.: IPv4 vagy IPv6 használata), a használt hangkodekek kódolási „nyeresége", vagy a kapcsoló mátrix és a forgalomirányító logikai működési elve, esetleg az interfészek vonali sebessége.

Ugyancsak fontosak a QoS beállítások, és a különböző forgalmi osztályok közti helyes prioritás ellenőrzése, mely az alkalmazott technológia (DiffServ, MPLS, IPv6) függvényében eltérő módszerek alkalmazását kíván meg.

A szoftverminőség vizsgálata (Software Quality Testing)

A kapcsolóeszközök valamint az IPT infrastruktúra egyéb elemein futó szoftver komponensek minőségének ellenőrzése ugyanúgy fontos, mint bármilyen más eszközt vezérlő szoftver tesztelése (hiszen az esetleges hibák veszélyeztetik a rendszer üzem-, és információ biztonságát). A nehézséget az jelenti, hogy a gateway-ek, kapcsolóközpontok javítócsomagjai nem ellenőrizhetőek tesztkörnyezetben (mint például a PC operációs rendszereké), hiszen speciális hardvert igényelnek. A beágyazott rendszerek sokszor valamilyen kevésbé ismert

41 Mean opinion score

42 Perceptual Evaluation of Speech Quality

43 Szintetikus háttérzaj, annak érdekében, hogy az éppen beszélőt ne zavarja össze a hallgatóság felüli csend (ti. a rendszer az átviteli kapacitás hatékony kihasználása érdekében bizonyos jelszint alatt nem továbbítja a hangokat).

programozási nyelven írt, általában zárt forráskódú programkódokat futtatnak, így azok kód analízise szinte lehetetlen (a gyártótól függetlenül). Továbbá érdemes megjegyezni, hogy a firmware, vagy az operációs rendszerek újratelepítése az IPT végkészülékeknél, kapcsolóeszközöknél gyakran csak gyártói segítséggel oldható meg.

ÖSSZEGZÉS

A termékbemutatók ábráin jól mutatnak a felhőként ábrázolt IP hálózatok, azonban a való életben ezek mögött a felületes jelölések mögött nagyon is komplex és kézzelfogható berendezések állnak.

Anakronisztikus gondolatnak tűnhet, azonban sokszor igaz, hogy az „újabb" nem feltétlenül „jobb" is. Konkrét esetünkben például az IPT számos tekintetben visszalépés a hosszú időn keresztül fejlődő TDM rendszerekhez képest. Így például a rendelkezésre állás, a minimális késleltetés, vagy a beszédérthetőség terén elmarad a korábbi ISDN rendszerekhez képest (mely következtében számos szervezet szándékosan kerüli távközlési infrastruktúrájának IP alapokra történő helyezését), természetesen számtalan olyan előnnyel rendelkezik mely korábban elképzelhetetlen lett volna. Ilyen például a forgalmi terhelés függvényében történő dinamikus forgalomirányítás (a korábbi rendszerek statikus irányítása mellett az alternatív útvonalak tervezése inkább művészet, mint tudomány volt).

Az IPT általánosan nem értékelhető „jónak" vagy „rossznak", a rendszer megítélésénél fontos figyelembe venni, hogy a korábban említett IPT alkalmazási szcenáriók közül melyiket vizsgáljuk, a rendszer mely részeit tesszük IP képessé. Megítélésem szerint az ISDN kapcsolóközpontok közti IP kapcsolat egyszerűsíti az üzemeltetést, hatékonyabbá teszi az átviteltechnikai berendezések adatátviteli képességeinek kihasználását, növeli az üzembiztonságot. Ugyanakkor a végponti IP készülékek (hardphone-ok) alkalmazását a korábban említett igények miatt indokolatlannak tartom (különösen tábori körülmények között, ahol több szempontból is hasznosabbak az egyszerű analóg végkészülékek).

A társadalmi fejlődés és az ipari terjeszkedés is generál egy folytonos innovációs igényt az alkalmazott technológiák további korszerűsítésére. Sokszor a gyártók erre még rásegítenek erőszakos reklám kampányaikkal, vagy olyan drasztikus lépésekkel, mint a terméktámogatás megszüntetése.

Egy szervezet műszaki fejlesztési igényét csak a saját szakemberei képesek valósan megítélni. A jövőbeli fejlesztéseknek a szervezetre gyakorolt pozitív hatásait tehát nekik kell a döntéshozók elé tárniuk, figyelembe véve szervezetük működését és igényeit.

Az IP hálózatok minőségének, valamint az IPT rendszerek vizsgálatára már elfogadott méréseket dolgoztak ki. Publikációmban ezeket mutattam be a katonai sajátosságok figyelembevétele mellett. Elemzésemben kitértem a minőségi paramétereknek a hálózati biztonsággal és az üzembiztonsággal kapcsolatos vetületeire is.

Felhasznált irodalom

[1] CISCO: IP Telephony/Voice over IP (VoIP)
Forrás: http://www.cisco.com/c/en/us/tech/voice/ip-telephony-voice-over-ip-voip/index.html Letöltve:2014.12.15

[2] NATO: Military noise environments
Forrás: http://ftp.rta.nato.int/public/PubFullText/RTO/TR/RTO-TR-HFM-147/TR-HFM-147-03.pdf Letöltve:2014.12.15

[3] Lendvay Marianna–Zsigmond Gyula - Komplex villamos rendszerek megbízhatóság-elemzési módszerei Forrás:http://www.zmne.hu/kulso/mhtt/hadtudomany/2004/2/2004-2-11.html Letöltve:2014.12.15

[4] IEEE szabvány a vlan-ok létrehozására Ethernet hálózaton, Forrás: http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf Letöltve:2014.12.15

[5] F. Baker J. Polk: IETF RFC 5865, A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic, 2010, ISSN: 2070-1721
Forrás: http://www.rfc-archive.org/getrfc.php?rfc=5865 Letöltve:2014.12.15

[6] Verizon Enterprise: MLPP leírás
Forrás:http://www.verizonenterprise.com/solutions/public_sector/federal/contracts/wits3/products/voice/mlpp.xml Letöltve:2014.12.15

[7] Wojciech Mazurczyk, Krzysztof Szczypiorski:Covert Channels in SIP for VoIP signalling Forrás: http://arxiv.org/ftp/arxiv/papers/0805/0805.3538.pdf
Letöltve:2014.12.15

[8] MTI/Index: Hekkerek harmincmilliós számlát csináltak a hevesi önkormányzatnak (2012.06.01. 12:28)
Forrás:http://index.hu/tech/2012/06/01/30_millios_szamlat_csinaltak_a_hekkerek_a_hevesi_onkormanyzatnak/ Letöltve:2014.12.15

[9] Vassilis Prevelakis, Diomidis Spinellis:The Athens Affair IEEE Spectrum,2007 június 27, Online Forrás: http://spectrum.ieee.org/telecom/security/the-athens-affair
Letöltve:2014.12.15

[10] Cisco: Cisco IP Phone Certificates and Secure Communications Forrás: http://www.cisco.com/web/about/security/intelligence/IP_Phone_Security_WP.html
Letöltve:2014.12.15

[11] Szabó Levente Átalakulóban a Combined Endeavor gyakorlat
Forrás: http://www.kormany.hu/download/c/0f/50000/CE_fejlodes%20%281%29.pdf
Letöltve:2014.12.15

[12] Cisco: Configuring Secure and Nonsecure Indication Tone
Forrás:
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/8_5_1/secugd/sec-851-cm/sectone.html Letöltve:2014.12.15

[13] Call Quality Metrics
Forrás: http://www.voip-info.org/wiki/view/Call+Quality+Metrics Letöltve:2015.01.08

[14] Opticom:PESQ – Perceptual Evaluation of Speech Quality
Forrás: http://www.opticom.de/download/SpecSheet_PESQ_05-11-14.pdf
Letöltve:2015.01.08

[15] Haig Zsolt, Kovács László, Németh András, Salamon Dániel, Vass Sándor, Ványa László - Zavarás hatékonyság minősítő eljárás kidolgozása pp. 1-64. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett INTERJAM integrált elektronikai felderítő és zavaró rendszerhez. (2009)