REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

5G Varnost

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

5G Varnost - 1. faza Industrijska raziskava, podfaza IR.2

Ključne tehnologije v sklopu 5GSafety

Rezultat IR.4 taska T.2.2 Študija tehnologij za kritično uporabo

Tip dokumenta	Rezultat
Zapis v arhivu	5GVAR-IR2-R04-Javno.docx
Narejeno za	5G Varnost
Avtor	Gregor Bobnar, Bojan Dovč, Tomislav Goluža, Pavel Kralj, Rok Čotić (Telekom Slovenije d.d.), Miha Oman, Dušan Merklin, Ana Robnik (Iskratel, d.o.o., Kranj), Mojca Volk, Urban Sedlar (Univerza v Ljubljani, Fakulteta za elektrotehniko), Tomaž Grenko, Marko Šmid (OSI d.o.o.)

ISKRATEL

Stopnja zaupnosti Javno

1. Povzetek

Trg pametnih telefonov predstavlja ogromen in kompleksen trg, ki bo po nekaterih ocenah do leta 2020 obsegal do 3 milijarde aktivnih uporabnih pametnih telefonov, kar nedvomno prinaša izzive za vse deležnike. Kljub temu, da trg danes že ponuja terminale, ki so tehnološko dovršeni, imajo tudi kopico tehnoloških in ostalih pomanjkljivosti, ki pa najbolj izstopajo takrat, ko se terminalna oprema uporablja za kritične PPDR situacije. Med najpomembnejše tako štejemo:

- velika razpršenost proizvajalcev terminalne opreme in operacijskih sistemov,
- omejena avtonomija baterije terminala,
- pokritost z mobilnim signalom in dostopom do mobilnega podatkovnega prenosa,
- pogoste napake GPS lociranja terminalov in lociranje znotraj stavb,
- neprioritizacija urgentnih podatkovnih klicev,
- poplava 112 aplikacij na terminalu,
- vprašljiva zanesljivost in uporabniška prijaznost.

Podatkovno obogateni postopki interakcije človek - terminal se v praksi uporabljajo že nekaj časa, vendar bo šele prihod nove generacije omrežja v prihodnjih letih omogočal še hitrejši razvoj prihajajočih tehnologij kot so:

- obogatena resničnost (AR),
- navidezna resničnost (VR),
- prepletena resničnost (MR),
- napredni uporabniški virtualni asistenti.

Interakcijski postopki človek – terminal sodijo med zahtevnejša opravila terminala. Pogosto gre za procesiranje multimedijskega materiala (slika, video, zvok), kar običajno na terminalu zahteva procesorsko moč in večjo količino delavnega spomina. Terminali za tovrstne interakcije morajo biti procesorsko in strojno dovolj zmogljivi za podporo interakcijskim postopkom, aplikacije pa morajo biti zgrajena tako, da so preproste in intuitivne za uporabo v stresnih in kritičnih pogojih – primer AR za navigacijo v mestu do najbližjega defibratorja.

IoT tehnologije bodo v prihodnjih letih vstopile na trg na različnih področjih, tudi na PPDR. Že dandanes poznamo vrsto različnih senzorjev za dim, požar, avtomobilske trke, IoT naprave za sporočanje natančne lokacije pri športih na prostem ter mnogo najrazličnejših senzorjev za zajem varnostnih, okoljskih, zdravstvenih in drugih s PPDR povezanih parametrov. Vsi ti podatki že sedaj lahko pripomorejo ali pomagajo pri boljšem razumevanju stanja na terenu in pri hitrejšem odzivu na dogodek, v določenih scenarijih pa omogočajo celo napoved in potencialno preprečevanje urgentnih dogodkov (npr. zaznavanje potresnih sunkov, ki napovedujejo potres, pravočasno zaznavanje nevarnega dviga vodostaja na poplavno ogroženih območjih ipd.). Tehnologije za omrežja z nizko porabo in velikim dosegom (ang. Low Power Wide Area Network – LPWAN) predstavljajo osnovo za poslovno uporabnost IoT rešitev. Trenutno najbolj znane tehnologije predstavljajo ZigBee, LoRa, SigFox, Nwave, LTE-M in NB-IoT.

Prehod med obstoječimi in prihodnjimi sistemi PPDR bo potekal postopoma, v vmesnem obdobju pa je najverjetnejša uporaba hibridnih omrežij, ki pomenijo integracijo obstoječih ozkopasovnih s širokopasovnimi omrežji. Hibridna omrežja omogočajo skupinske govorne komunikacije med uporabniki ozkopasovnih omrežij, med uporabniki širokopasovnih omrežij, med uporabniki ozkopasovnih in širokopasovnih omrežij in z dispečerji v operativnih centrih. Uporabniki širokopasovnih omrežij poleg govornih storitev uporabljajo tudi aplikacije za prenos videa in večjih količin podatkov. Istočasno so hibridna omrežja razširljiva in omogočajo uporabo več organizacijam uporabnikov PPDR. Za integracijo in koeksistenco obstoječih in prihodnjih sistemov so ključnega pomena standardizirani vmesniki za povezavo in vzajemno delovanje teh omrežij. Proizvajalci opreme za kritična omrežja so pred izzivom kako uskladiti medsebojno povezavo ozkopasovnih kritičnih omrežij s širokopasovnimi.

Tehnologije, ki se uporabljajo za PPDR, se delijo v kategorije glede na njihovo sposobnost glede prenosa podatkov:

- ozkopasovne (NB – narrowband),
- širšepasovne (WB – wideband),
- širokopasovne (BB – broadband).

Potrebe uporabnikov PPDR glede govornih komunikacij so zaradi namenskega razvoja izpolnjene z obstoječimi ozkopasovnimi tehnologijami (TETRA, TETRAPOL, P25 in DMR). Te omogočajo širok nabor govorno orientiranih storitev, z omejenimi možnostmi prenosa podatkov. Poleg omenjenih digitalnih tehnologij so ponekod v uporabi še analogni sistemi, tako konvencialni kot snopovni (MPT1327), vendar jih v vse večji meri nadomeščajo digitalni. Ozkopasovne tehnologije so primerne tako za manjša omrežja, kot tudi za nacionalna omrežja, ki si jih deli več organizacij PPDR na določenem območju. V Evropi je za nacionalna omrežja za PPDR uporabo v večini primerov uporabljena tehnologija TETRA, v manjši meri tudi TETRAPOL.

Glavne omejitve ozkopasovnih PPDR tehnologij:

- premajhne zmogljivosti v primeru izrednih razmer,
- nezmožnost prenosa večjih količin podatkov,
- slaba interoperabilnost.

Mobilna radijska omrežja operaterjev so namenjena pokrivanju uporabnikov, kjer je vodilo komercialni interes. Operaterji zagotavljajo pokritost tam, kjer se večinoma nahajajo uporabniki mobilnih storitev. Posledično je pokritost prebivalstva (glede na naslove prebivalcev) zelo visoka, medtem ko so področja, ki niso naseljena, komercialno nezanimiva ali je gradnja baznih postaj onemogočena in so zato takšna območja slabo pokrita ali nimajo radijske pokritosti. Območja, ki danes komercialno niso zanimiva, bodo morala, v primeru uporabe za PPDR storitve, imeti zagotovljeno radijsko pokritost. Le to bo mogoče zagotoviti z gradnjo novih lokacij. Kjer to ne bo mogoče, bo v primeru izrednih dogodkov možno postaviti začasne bazne postaje za zagotavljanje radijske pokritosti.

Za zagotavljanje podpore delovanja naprav in storitev PPDR je potrebno dodeliti ustrezen radijski spekter za povezovanje naprav PPDR. Radijski spekter za delovanje naprav PPDR mora zagotavljati dovolj pasovne širine in pokrivanja s signalom. Spekter mora biti usklajen na državnem nivoju in med državami članicami EU. Tako bo omogočen večji razmah razvoja storitev PPDR na meddržavnem nivoju, prenosljivost terminalne opreme in s tem večja kvaliteta ter posledično tudi nižja cena. Obenem bo omogočena tudi interoperabilnost storitev med državami EU, kar bo omogočilo hitrejši razvoj storitev in njihovo široko uporabo ter mobilnost operativnih enot na teritoriju EU.

V prvi fazi bodo 5G omrežja uporabljala obstoječa LTE-A omrežja, nadgrajena z novimi funkcijami (arhitektura 5G) predvidenimi v 5G omrežjih. Sočasno z nadgradnjo baznih postaj poteka tudi razvoj in nadgradnja prenosnih sistemov in jedrnega omrežja. Država napoveduje novo dražbo frekvenc, ki bodo omogočala višje vršne hitrosti in boljšo uporabniško izkušnjo na podeželju (700 MHz pas) ter v mestih (3.5 GHz).

Evropska komisija je z Uredbo št. 2016/687, ki je bila sprejeta 28. 4. 2017, zagotovila pravno podlago za uporabo radijskega spektra na 700 MHz. Ta uredba zagotavlja:

- usklajene pogoje za delovanje storitve PPDR v 700 MHz zemeljskem brezžičnem frekvenčnem spektru v frekvenčnih pasovih 703-733 MHz in 758-788 MHz,
- sočasno uporabo storitev PPDR z drugimi storitvami zemeljskega brezžičnega širokopasovnega omrežja,
- uporabo storitev PPDR v posamezni državi članici,
- možno uporabo dodatnih frekvenčnih pasov za storitve PPDR glede na odločitve države članice v pasovih 698-703 MHz, 733-736 MHz, 753-758 MHz in 788-791 MHz.

Ministrstvo za javno upravo (MJU) je dne 1. 4. 2019 na Agencijo za komunikacijska omrežja in storitve (AKOS) naslovilo strateške usmeritve **Error! Reference source not found.** glede podeljevanja frekvenc v pasu 700 MHz, kjer usmerja AKOS, naj pri podelitvi frekvenc upošteva možnost pokrivanja potreb uporabnikov s področja javne varnosti ter zaščite in reševanja (PPDR) s storitvami mobilnih komunikacij komercialnih omrežij nove generacije tehnologije 5G.

Na trgu že obstajajo integrirana vezja za terminale v celotnem radiofrekvenčnem pasu 700 MHz, na voljo pa še ni komercialne opreme za bazne postaje za pas 68. Agencija je za PPDR uporabo predlagala spekter v dupleksnih režah in zaščitnem pasu v 700 MHz radiofrekvenčnem pasu, in sicer 2x5 MHz: 698-703 MHz / 753-758 MHz (3GPP pas 68).

V strategiji je navedeno tudi, da bi lahko z razvojem LTE tehnologij (Release 12-14) PPDR uporabljal LTE omrežja z lastno infrastrukturo, lahko pa tudi v kombinaciji z uporabo javne mobilne infrastrukture. Agencija je preučila možnost uporabe dupleksnih rež in zaščitnih pasov v 700 MHz pasu, kar bi pomenilo 2x5 MHz ter za namenska omrežja za zagotavljanje M2M za kritično infrastrukturo 2x3 MHz (M2M) na 700 MHz frekvenčnem pasu.

Arhitektura 5G jedrnega omrežja omogoča virtualizacijo po rezinah in posledično odpravlja potrebo po namenskih fizičnih virih. Ključna arhitekturna novost omrežja 5G je uvedba sebi podobnega hierarhičnega pristopa aktivnih sredinskih omrežnih elementov med zalednimi sistemi in končnimi uporabniki. Slednje omogoča doseganje nizkih zakasnitev med končnimi točkami.

Uporaba dodeljenega frekvenčnega spektra samo za PPDR storitve v začetni fazi omogoča kontrolo nad uporabo kapacitet in zagotavljanje kakovosti storitev (QoS ang. Quality of Service) za posamezne uporabnike ali storitve. V kasnejših fazah, z razvojem aplikacij, ki bodo zahtevale velike podatkovne hitrosti in/ali kratke odzivne čase, pa bo omejitev dodeljenega spektra privedla do preobremenitev radijskega vmesnika na območjih povečane uporabe (izredni dogodki). Zagotavljanje QoS za PPDR storitve v primeru uporabe celotnega frekvenčnega spektra javnih radijskih omrežij je mogoče zagotoviti s prioritizacijo prometa in z možnostjo gostovanja v vseh mobilnih omrežjih. Možna je tudi kombinacija uporabe dodeljenega frekvenčnega spektra za PPDR storitve ob hkratni souporabi (glede na zahteve) komercialnih radijskih omrežij. Komercialna omrežja bodo z uvedbo 5G tehnologije omogočala rezinjenje, zagotavljanje QoS-a za PPDR storitve pa bo mogoča z uvedbo dinamičnega dodeljevanja radijskih virov za posamezne rezine v mobilnem omrežju.

Za uporabo storitev TETRA uporabnik širokopasovnega omrežja uporablja običajen pametni telefon z lastno identiteto SIM 3GPP in z nameščeno namensko aplikacijo TETRA na pametnem telefonu, s svojo identiteto TETRA. Kvaliteta storitve in njena zanesljivost je odvisna od izvedbe širokopasovnega omrežja. S stališča uporabnika omrežja TETRA je uporabnik omrežja LTE eden od uporabnikov omrežja TETRA, ki lahko uporablja enake storitve TETRA in je lahko član istih skupin TETRA. Omrežje LTE je lahko komercialno ali zasebno.

V sklopu raziskav tehnologij in metodik za zagotavljanje primerne tehnološke osnove, smo zaznali področja ki so pomembna za zagotavljanje storitev, v okviru predlaganih uporabniških primerov. Identificirali smo kritična področja segmenta tehnologij, ki lahko bistveno vplivajo na parametre izvedbe aplikacij (DPaaS), ki bodo zagotavljale storitve za izvedbo uporabniških primerov.

Glavna področja kjer smo prepoznali tehnološke izzive so:

- Upravljanje RTP prometa za zagotavljanje govornih storitev, video komunikacij in snemanja.
- Snemanje dogajanja na operaterski konzoli.
- Implementacija aplikacij na osnovi principa distribuiranih aplikacij.
- Uporaba distribuiranih podatkovnih strežnikov.
- Tehnološki izzivi na izvedbi hibridnih komunikacij.
- Izzivi dinamičnega določanje kakovosti storitev 5G.
- Integracije aplikacij za občana v tehnologiji WebRTC.

Podatkovna analitika je inherentno dopolnjujoča z ostalimi trendi 5G tehnologije, kot so SDN (angl. Software Defined Networking)/NFV (angl. Network Functions Virtualization) in MEC (angl. Multi-access Edge Computing). Omejitve in tehnični izzivi pri uporabi analitike v 5G omrežju predstavljajo predvsem hitro spreminjajoči se podatki, podpora za aplikacijsko in omrežno inteligenco ter varnost na celotni poti.

Omrežja 5G bodo omogočila medsebojno izmenjavo podatkov med velikim številom med seboj zelo raznolikih naprav (senzorji, naprave, mobilne naprave kot so pametni telefoni, tablice, …). Da bi lahko bila ta varna in zanesljiva bodo uporabljeni varnostni mehanizmi morali biti učinkoviti in prilagodljivi. Zagotavljanje zasebnosti in celovitosti podatkov pri njihovi izmenjavi bo temeljilo na uporabi šifrirnih in avtentikacijskih mehanizmov, ki jih danes že uporabljamo. Na omrežnem nivoju bo to protokol IPSec, na transportnem pa protokol TLS. Da bi zagotovili višji nivo varnosti ključev, ki bodo uporabljeni za šifriranje in avtentikacijo, bo nujno potrebna uporaba namenskih strojnih, iz katerih ključev ni mogoče izvoziti, hkrati pa ti omogočajo natančen nadzor dostopa do samih ključev.

Najpomembnejša varnostna mehanizma za zaščito končnih točk bosta tako ostala programska oprema za zaščito pred zlonamerno programsko opremo (AV - antivirus) ter osebna požarna pregrada (FW – ang. Firewall), s katero bo mogoče omejiti dostop do virov na samih napravah. V primerih, ko bo zahtevana še višja stopnja varnosti končnih točk, bo mogoče te funkcionalno nadgraditi z uporabo osebnega sistema za preprečevanje vdorov (IPS - ang. intrusion prevention systems) s katerim bo mogoče preprečiti zlorabo znanih ranljivosti v uporabljeni programski opremi ali napak pri konfiguraciji.

Ključna izziva pri zagotavljanju varnosti končnih točk v 5G omrežjih bodo tako relativno velike razlike v funkcionalnostih programske opreme in zmogljivostih strojne opreme ter relativno dolga življenjska doba nekaterih naprav. Kibernetska varnost oziroma zaščita pred tveganji, ki večinoma izhajajo iz stalne in globalne povezljivosti, bosta imeli odločujoč vpliv na uspešnost uvedbe omrežij 5G. Zaradi predvidenega povečanja števila naprav v 5G omrežjih in posledičnega povečanja varnostnih dogodkov bo za učinkovito odzivanje nujna uporaba orodij za avtomatizacijo in orkestracijo varnostnih funkcij 0. Pomemben vir podatkov za analitike v varnostno operativnem centru, kateri se pretežno ukvarjajo z odzivanjem na varnostne incidente, predstavljajo podatki o dejanskih napadih in zlorabah.

Upravljanje in nadzor omrežja/omrežnih elementov – NOC (Network Operations Center) predstavlja integracijo in centralizacijo nadzora omrežja z namenom:

- optimizirati delovanje in vzdrževanje omrežja,
- nadzirati posege v omrežje,
- hitrejše odkrivati in odpravljati okvare v omrežju,
- zmanjševati čas izpada, posameznih delov omrežja,
- zmanjševati stroške in izpad prihodka,
- odkrivati kritične elemente oz. točke v omrežju in s tem dvigovati kakovost in razpoložljivost omrežja.