Implementacija zemaljskog digitalnog mobilnog radio sistema – TETRA u BiH

Mladen Mrkaja, Nejra Batalović, Zoran Koprivica
Sektor za informatiku i telekomunikacione sisteme
Ministarstvo bezbjednosti BiH
Sarajevo, BiH
mladen.mrkaja@msb.gov.ba, nejra.batalovic@msb.gov.ba, zoran.koprivica@msb.gov.ba

Sadržaj – **U ovom radu dat je pregled implementacije projekta izgradnje zemaljskog digitalnog mobilnog radio sistema -TETRA namijenjenog za teklekomunikacijsku podršku u operacijama policijskih agencija uz potpunu kontrolu poziva u svim organizovanim grupama i mrežama i svim uslovima koje mogu imati karakter krizne situacije. Projekat je implementiran na području Sarajeva i dijela Istočnog Sarajeva kao osnova za izgradnju TETRA sistema na području Bosne i Hercegovine. U radu je opisana topologija i arhitektura implementiranog sistema.**

I. UVOD

Schengenskim sporazumom od 14. juna 1995. godine uvodi se među zemljama potpisnicama veći stepen koordinacije, posebno između državnih tijela zaduženih za nadzor i kontrolu državne granice. Tako se sporazumom traži od država potpisnica da nastoje pojačati razmjenu informacija koje bi mogle biti od interesa drugim sporazumnim strankama, posebno u borbi protiv kriminala, (čl. 9. st. 1. Schengenskog sporazuma). Schengenski provedbeni sporazum od 19. juna 1990. godine predstavlja nastavak inicijative i snažniji poticaj u procesu normizacije (standardizacije) mobilnih komunikacija organizacija tzv. plavog svjetla (policija, carina, vatrogasci, hitna medicinska pomoć, organizacije za traganje i spašavanje, obalna straža). Članom 44. Schengenskog provedbenog sporazuma nastoji se urediti policijska i carinska međugranična saradnja. Stručnjaci iz područja telekomunikacija iz zemalja Schengenskog sporazuma, okupljeni u radnoj grupi nazvanoj Schengen telekom, sačinili su popis korisničkih zahtjeva koji se u budućnosti, u mobilnoj i radijskoj telekomunikaciji, trebati ispuniti. Time je započeo proces normizacije i izgradnje TETRA sistema.

U Bosni i Hercegovini projekat implementacije TETRA sistema započeo je 2007. godine, a sistem je zvanično pušten u rad 2009. godine. [1] [3]

A. Potreba za komunikacijom- trendovi u službama bezbjednosti

Proteklih dvadesetak godina komunikacijske potrebe ovih policijskih, vatrogasnih i graničnih službi, kao i službi spašavanja u Evropi uveliko prelaze mogućnosti konvencionalnih radio mreža. Prvi problem je što većina ovih službi ima svoje vlastite, često nekompatibilne radio sisteme. To su najčešće analogni sistemi s niskim nivoom zaštite informacija. Svaki sistem radi na svojim frekvencijama, što znači da je njihova međusobna komunikacija nemoguća, a događa se da u graničnim područjima određene službe jedne zemlje rade na frekvencijama na kojima u drugoj zemlji rade druge službe, te tako jedni druge ometaju. U nekim slučajevima, pojedine službe čak zavise od komercijalnih servisa, bez garancije da će u slučaju neke veće nezgode ili prirodne katastrofe uopšte biti u stanju da ostvare vezu. Drugi problem su tehnološka ograničenja sistema koji su u upotrebi. Konvencionalni analogni radio sistem sastoji se od određenog broja repetitora koji primaju i pojačavaju slab signal primljen od radio uređaja. U ovim sistemima nema komutacije (selektivnog rutiranja saobraćaja samo određenim učesnicima). Svi radio korisnici koji su podesili svoj radio na istu frekvenciju mogu slušati jedni druge i ne postoji nikakva zaštićenost tajnosti komunikacije. Korisnici se moraju unaprijed dogovoriti koje će frekvencije koristiti, što znači da se frekvencijski spektar, kao ograničeno prirodno dobro, neracionalno koristi. Mogućnosti zaštite prenesenih informacija kao i prenosa podataka na rudimentarnom su nivou. Savremene službe javne bezbjednosti, čiji su zadaci sve složeniji, imaju rastuću potrebu za širokim spektrom telekomunikacijskih servisa u mobilnim uslovima. U mnogim zemljama stara komunikacijska oprema je zamijenjena ili će biti zamijenjena tokom narednih nekoliko godina. Prelazak s konvencionalnih, analognih sistema na inteligentne, digitalne radio mreže, složen je zadatak, kako s tehničkog tako i s komercijalnog aspekta, i gotovo svugdje će biti neophodno, u određenom vremenskom razmaku, obezbjeđivanje istovremenog funkcionisanja i starih i novih sistema .[1]

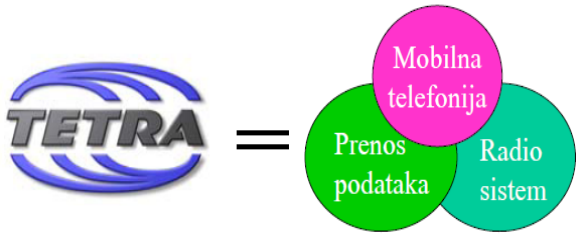
II. O TETRI

TETRA standard (engl.Terrestrial Trunked Radio) razvijen je za potrebe profesionalnih korisnika kojima su potrebne sljedeće mogućnosti:

a) trenutna uspostava poziva (ispod jedne sekunde),
b) komunikacija tačka – više tačaka: grupni pozivi, kao i upućivanje opštih poziva (engl. voice broadcast),
c) direktna komunikacija između terminala, bez „posredovanja“ infrastrukture (podrazumijeva se da je manjeg dometa),

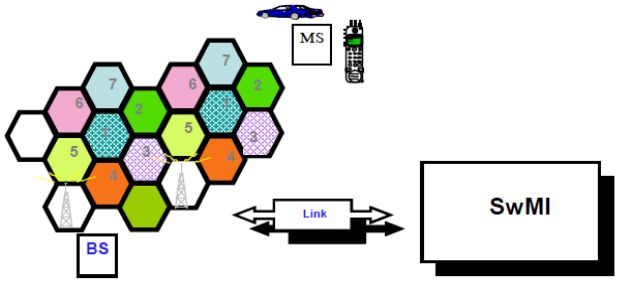
d) pozivi u hitnim situacijama, s automatskim uključenjem mikrofona,
e) individualni i telefonski pozivi.

TETRA objedinjava u sebi osobine mobilne telefonije i klasičnog radija, a osim govora obezbjeđuje i prenos podataka.



Slika 1. Struktura TETRE

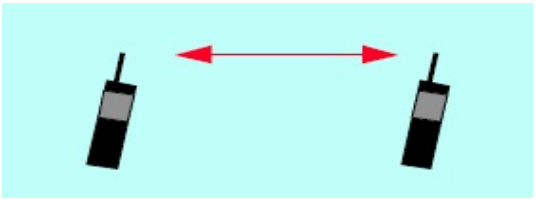
Za razliku od dosadašnjih analognih mreža za profesionalnu radio komunikaciju u širokoj upotrebi u našoj zemlji, TETRA je zasnovana na digitalnoj tehnologiji, ćelijskog tipa.



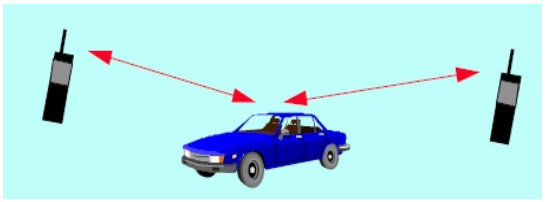
Slika 2. Ćelijska struktura TETRE

Ovo posljednje se postiže dijeljenjem jedne radio frekvencije na 3-4 korisnika tj. 4 vremenska slota, od kojih se jedan u najjednostavnijoj konfiguraciji upotrebljava za kontrolu i signalizaciju, a ostali za učesnike. TETRA je definisana standardima Evropskog telekomunikacijskog normizacijskog instituta (ETSI). TETRA norme (standard/i), u okviru ETSI organizacije, opisuju digitalni radijski sistem za prenos informacija koje mogu biti glas i/ili podaci i/ili slika u funkciji PMR usluga. Sistem karakteriše veliko područje pokrivanja radijskim signalom zbog niže radne frekvencije u odnosu na aktuelne alternativne tehnologije. Nadalje, TETRA sistem u funkciji PMR usluga karakteriše visoka pouzdanost i bezbjednost komunikacije te izuzetno kratko vrijeme uspostave poziva. Unutar sistema postoje mehanizmi koji funkcijama dinamičke dodjele prioriteta rješavaju problem preopterećenja te povećavaju dostupnost komunikacijske mreže za vrijeme kriznih situacija i velikih potreba za kapacitetom. TETRA sistem može raditi u trunking načinu rada, prilikom kojeg koristi mrežne resurse, ili u direktnom načinu rada (engl. Direct Mode Operation - DMO) za vrijeme kojeg se ostvaruje direktna komunikacija između mobilnih/ručnih stanica. Prednosti DMO načina rada su mogućnost direktne komunikacije izvan područja pokrivanja mrežne infrastrukture, dodatni kapacitet za vrijeme zagušenosti mrežnih resursa te mogućnost komunikacije za vrijeme nedostupnosti mrežne infrastrukture (npr. uslijed prirodnih nepogoda).

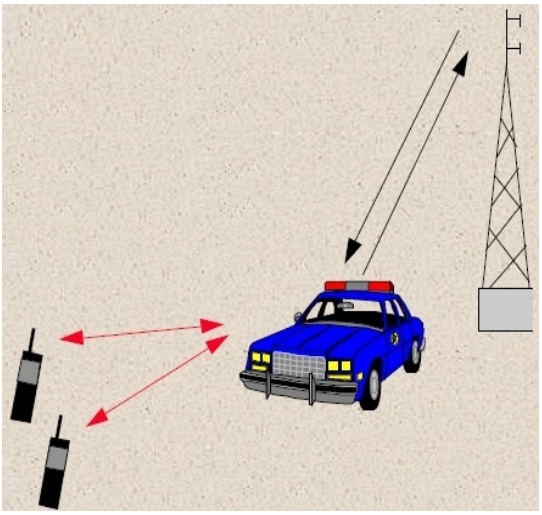
Postoje tri vrste DMO poziva:



Slika 3. Jednostavni razgovor između dva TETRA uređaja



Slika 4. Mobilni uređaj ugrađen u automobile služi kao repetitor između dva TETRA uređaja



Slika 5. Uređaj ugrađen u automobil predstavlja prenosnik između bazne stanice i TETRA uređaja

Uz brojne mogućnosti upravljanja govornom komunikacijom, kao npr. dodjela prioritetnog poziva (poziv u pomoć); zadržavanje poziva; stavljanje poziva na čekanje (uvažavajući prioritet poziva); dinamčko uspostavljanje pozivnih grupa; tzv. "ambijentalno slušanje" koje dispečeru omogućava slušanje zvuka ili razgovora u dosegu mikrofona (npr. koji je ugrađen u kolima za prevoz novca i drugih vrijednosnih papira); odobravanje poziva od dispečera; naknadno kasnije uključivanje u pozivnu grupu; kriptozaštita te usluge preuzete iz moderne telefonije; TETRA sistem pruža i velike mogućnosti podatkovne komunikacije, kao i prenosa slike ili audio-video snimke. Upravo na tu mogućnost primjene sistema treba staviti naglasak, te na TETRA 2 standard, tj. razvoj TETRA mreže u multifunkcionalnu širokopojasnu podatkovnu mrežu visokih kapaciteta koja bi, upotrebom

naprednih modulacijskih postupaka, omogućila korištenje vrlo zahtjevnih aplikacija kao npr. prenos video sadržaja u realnom vremenu (npr. slike osobe koju treba provjeriti ili identifikovati). TETRA sistem prihvaćen je i upotrebljava se u cijelome svijetu, ponajprije u državnim službama u sektorima javne bezbjednosti, gdje kroz multifunkcionalnost (pristup bazama podataka s terena, prenos slikovnih zapisa i videozapisa i sl.) i pouzdanost komunikacije povećava bezbjednost i učinkovitost rada u svakodnevnim i izvanrednim situacijama. Nadalje, u funkciji javnog prevoza najčešće se koristi za uslugu automatskog pozicioniranja vozila (engl. Automatic Vehicle Location — AVL) pomoću prijemnika globalnog sistema pozicioniranja satelita (engl. Global Positioning System — GPS), te za niz drugih usluga zavisno o potrebama/zahtjevima korisnika. S obzirom na stalni razvoj novih usluga i povećanje mogućnosti, sistem se sve više upotrebljava u industriji, saobraćaju, elektrodistribuciji te za potrebe mrežnih operatera. [2]

A. Osnovne bezbjednosne funkcije TETRA sistema

[1]Osnovne bezbjednosne funkcije TETRA sistema su:

a) autentikacija (uključujući uzajamnu autentikaciju koja podrazumijeva međusobnu provjeru validnosti pojedine stanice i infrastrukture na koju se vezuje),
b) enkripcija vazdušnog interfejsa – između radio stanice i bazne stanice (Nivo 2 – statički ključevi i Nivo 3 - dinamički ključevi),
c) mogućnost enkripcije s kraja na kraj veze (E2E),
d) ambijentalno slušanje, i
e) mogućnost daljinskog onesposobljavanja radio stanice (privremenog ili trajnog).

B. Servisi

[1]Pored bezbjednosnih funkcija TETRA standardima predviđena je i mogućnost različitih servisa za prenos podataka. Među njima su:

a) statusne poruke,
b) SDS - kratke tekstualne poruke (pandan SMS porukama u mobilnoj telefoniji),
c) prenos podataka paketskom i/ili kanalskom komutacijom (brzine prenosa podataka u standardu TETRA 1 ograničene su na oko 12 kb/s).

Takođe, podržan je izvjestan broj karakteristika koje su se pokazale kao veoma važne za organizacije koje su nadležne za javnu bezbjednost, kao što su:

a) telefonski interkonekcioni pozivi u punom dupleksu,
b) različiti nivoi prioriteta poziva i ulaska u vezu,
c) Opšti (broadcast) pozivi od strane operatora, itd.

C. Interfejsi

Sa tehnološke tačke gledišta, TETRA koristi vremenski multipleks od četiri kanala po jednom nosiocu s razdvajanjem nosilaca od 25 kHz. Kodiranje govora i modulacija su takođe standardizovani. TETRA sistemi u Evropi koriste pomenuti 380 MHz-400 MHz opseg za službe javne bezbjednosti i opseg 410 MHz-430 MHz za komercijalne primjene [4]. Standard ne ograničava upotrebu drugih frekvencija u skladu s lokalnom regulativom, tako da su van Evrope u upotrebi i sistemi koji rade u opsezima oko 800 MHz. Međutim, da bi se osiguralo da standard bude otvoren i da bi se omogućilo prisustvo većeg broja proizvođača na tržištu, TETRA standard definiše samo slijedeće najvažnije interfejse:

a) Vazdušni interfejs (AI) je najvažniji definisani interfejs i određuje način prenosa informacija između radio stanice i bazne stanice, u kom slučaju govorimo o tranking režimu (TMO), ili direktno između mobilnih stanica kada govorimo o direktnom režimu rada (DMO). Standardizacija ovog interfejsa omogućava interoperabilnost radio stanica različitih proizvođača s različitim infrastrukturama.
b) Interfejs terminalne opreme (TEI) određuje način povezivanja opreme za podatke na TETRA radio stanice. Standardni TEI olakšava nezavisnim firmama da razvijaju aplikacije za prenos podataka preko TETRA sistema.
c) Intersistemski interfejs (ISI) dozvoljava povezivanje različitih TETRA mreža i tako korisnicima omogućava međusobni roming. Ovaj interfejs je od ključnog značaja kada se govori o interoperabilnosti između graničnih službi susjednih zemalja. [1] [2]

D. Kriptozaštita u TETRI

ETSI je formirao specijalnu radnu grupu za definisanje kriptozaštite u sistemu TETRE. Grupa je definisala mehanizme kriptozaštite u TETRI za prenos govor + podatak (V+D). Od elemenata navedenih u definiciji kriptozaštite standardom su definisani mehanizmi za obezbjeđenje tajnosti govora, podataka i komandi i provjera autentičnosti učesnika. Takođe su definisani i mehanizmi za generisanje, distribuciju i čuvanje ključeva pri radio prenosu. Standardizovana je kriptozaštita pri radio prenosu dok su u načelu definisani mehanizmi koji obezbjeđuju zaštitu od kraja do kraja. Osnovne funkcije kriptozaštite (KZ) u TETRA sistemu su:

Mehanizmi kriptozaštite obezbjeđuju određivanje autentičnosti učesnika, šifrovanje i sve elemente od kojih je sačinjen sistem kriptozaštite;

Sistem za generisanje, kontrolu, upravljanje i distribuciju ključeva i rad induvidualnih mehanizama zaštite.

Definisanje algoritama za kriptozaštitu obuhvata standardizaciju specifičnih matematičkih funkcija kojima se obezbjeđuje visok kvalitet kriptoloških algoritama.

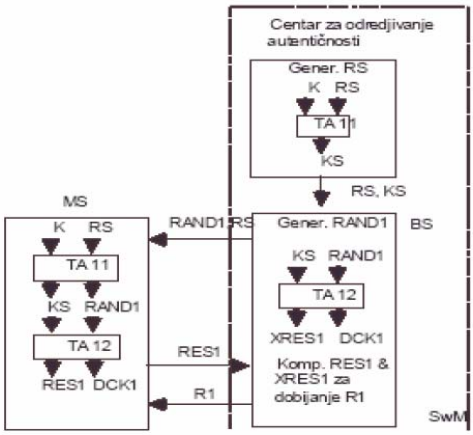
Funkcija prilagođavanja sistema kriptozaštite zakonskim regulativama pojedinih zemalja.

U opštem slučaju KZ obezbjeđuje:

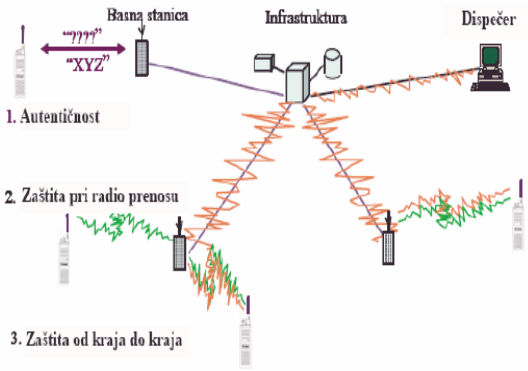
a) Autentičnost,
b) Šifrovanje u bežičnom, radio prenosu-Air Interface, Encryption,
c) Upravljanje ključevima,
d) Isključivanje terminala,
e) SIM (Subscriber Identity Module, Modul za identifikaciju korisnika), i
f) Šifrovanje od kraja do kraja

Metod određivanja autentičnosti koristi simetrični šifarski sistem. U ovom sistemu tajni ključ za određivanje autentičnosti je podjeljen između učesnika u procesu određivanja autentičnosti, mobilnog učesnika i centra, i samo oni znaju taj ključ. Provjera autentičnosti se svodi da bilo koja od dvije strane u procesu može provjeriti da li druga raspolaže ključem za provjeru autentičnosti. Provjera autentičnosti korisnika vrši se od strane SwMI. Bazna stanica generiše slučajni niz RAND1. Koristeći K, RS i algoritam TA11 centar za određivanje autentičnosti generiše KS i dostavlja RS i KS baznoj stanici. Bazna stanica šalje RAND1 i RS ka MS. Istovremeno na osnovu KS i RAND1 bazna stanica BS koristeći algoritam TA12 izračunava XRES1 i DCK1. Mobilna stanica MS na osnovu K sa kojim raspolaže i dobijenog RS od BS korištenjem TA11 izračunava KS. Zatim primjenom algoritma TA 12 na osnovu KS i RAND1 izračunava RES1i DCK1. Izračunati RES1 šalje ka BS koja upoređuje RES1 i XRES1. U slučaju slaganja autentičnost je potvrđena. U suprotnom BS ne dozvoljava MS pristup sistemu. Proces određivanja autentičnosti koji je iniciran od strane SwMI prikazan je na Sl. 6. Određivanje autentičnosti infrastrukture može biti inicirano i od strane MS. Budući da je ključ K smješten u MS, u cilju sprječavanja korištenja MS od strane neovlaštenog korisnika ključ K se može koristiti ako se ispravno unese identifikacioni broj koji je poznat samo legalnom učesniku. Kriptozaštita u radio dijelu odvija se u komunikaciji između MS i bazne stanice, primjenjuje softverska rješenja i koristi dva algoritma TA1 i TA2. Upotrebljavaju se ključevi SCK i DCK. Naravno svaki učesnik ima različite ključeve.

Šifrovanje šematski prikazano na Sl. 7. sastoji se od KZ pri radio prenosu i KZ od kraja do kraja. Oba dijela KZ čine cjelinu i oba su neophodna za kvalitetnu KZ. Bez KZ u radio dijelu ne bi se moglo vršiti efikasno određivanje autentičnosti MS od strane mreže i obrnuto. Ne bi se moglo obaviti uspješno upravljanje ključevima niti bi se moglo izvršiti isključivanje i uključivnje pojedinih MS u mrežu u slučaju potrebe (krađa i sl.). Osim ovoga ako bi se koristila samo zaštita od kraja do kraja podaci vezani za uspostavljanje veze kao i za signalizaciju i sinhronizaciju u mreži bili bi otvoreni. Radio aktivnost svakog učesnika mogla bi da se prati. Ovo su sasvim dovoljni razlozi za primjenu i KZ od kraja do kraja, budući da je tako dobijeno kompletno rješenje KZ. Na Sl. 8 je prikazana KZ i ključevi koji se koriste pri radio prenosu. Ključevi koji se primjenjuju pri KZ u radio dijelu su: **DCK,** koji se dobija u procesu određivanja autentičnosti i koristi se za šifrovanje komunikacije od MS ka BS; **CCK** je generisan od strane SwMI i distribuiran ka mobilnim stanicama, šifrovan sa DCK; **GCK** se koristi za određenu grupu učesnika. Generiše se od strane SwMI i distribuira se ka grupi mobilnih učesnika. Koristi se kao GCK ili modifikovan sa CCK za šifrovanje poziva za specifikovanu grupu učesnika; SCK je ključ koji se koristi bez prethodne provjere autentičnosti. Statički je u smislu da se ne mijenja u procesu određivanja autentičnosti.



Slika 6. Određivanje autentičnosti

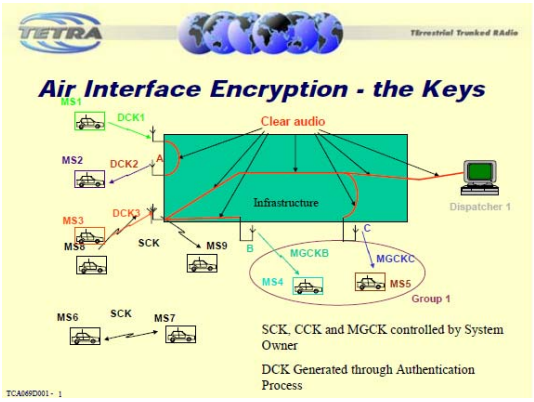


Slika 7. Kriptozaštita u TETRI

OTAR (engl. Over The Air Re-keying) se koristi za distribuciju CCK, GCK and SCK. Ovaj mehanizam obezbjeđuje veoma šifrovan prenos ključeva od mreže direktno ka mobilnim učesnicima (MS). OTAR poruka ka MS je šifrovana sa sesijskim ključevima koji su izvedeni iz ključeva za određivanje autentičnosti. Koristi se kako za individualne tako i za grupne pozive.

Zaštita od kraja do kraja uslovljava da:

a) Nema potrebe za specijalnim mjerama zaštite infrastrukture,
b) Dodatna sinhronizacija je potrebna,
c) Mogu da se koriste standardni algoritmi ili nacionalna rješenja, i
d) Upravljanje ključevima je prepušteno korisniku.



Slika 8. KZ I ključevi pri radio prenosu

Ključevi koji se koriste pri zaštiti od kraja do kraja su: **TEK**- Traffic encription key. Tri edicije se čuvaju radi preklapanja pri promjeni ključeva; **GEK**- Group Encription Key za kriptozaštitu TEK-a kada se koristi druga vrsta OTAR-a za šifrovanje od kraja do kraja; **KEK-** za kriptozaštitu KEK-a kada se koristi OTAR; **SEK**- Signalling Encription Keys koristi se opcionalno za zaštitu upravljačkih funkcija. [4]

E. Interoperabilnost TETRA sistema

Interfejsi unutar komutacione i upravljačke infrastrukture (SwMI) nisu standardizovani, te uprkos definisanom standardu, proizvođači još uvek oklijevaju da u potpunosti razviju i ponude intersistemski interfejs (ISI) [1]. Ovo je rezultat borbe za tržište, jer sadašnja situacija uslovljava organizacije koje su počele da razvijaju TETRU na infrastrukturi jednog proizvođača da nastave implementaciju sa istim proizvođačem. Loša posljedica ove situacije je činjenica da prekogranična komunikacija korištenjem TETRA sistema još uvijek ne funkcioniše na željenom nivou, odnosno na način koji bi osigurao puni roming kako za grupne, tako i za individualne pozive i prenos podataka. U toku su intenzivne i koordinisane aktivnosti TETRA Asocijacije i evropskih foruma za komunikacije bezbjednosnih struktura kao što su PSCE (engl. Public Safety Communications – Europe), PSRG (engl. Public Safety Radio Group), Telekomunikacijski komitet za prekograničnu saradnju zapadnobalkanskih zemalja i drugih, kako bi se proizvođači primorali da u potpunosti razviju i primjene ISI. [1]

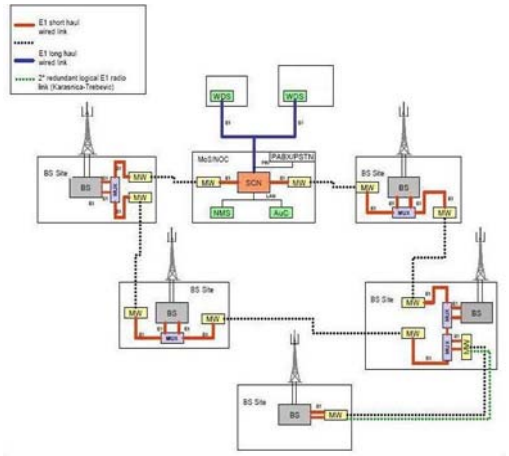
III. TETRA SISTEM MINISTARSTVA BEZBJEDNOSTI

A. Istorija realizacije projekata

Projekat uspostave TETRA telekomunikacijskog sistema finansiran je od strane Delegacije Evropske komisije iz fonda CARDS 2004, a dana 13.07.2006. godine između Delegacije Evropske komisije i Ministarstva bezbjednosti potpisan je Memorandum o razumijevanju o nabavci i uspostavi TETRA i VoIP telekomunikacijskog sistema za potrebe policije i organa bezbjednosti u Bosni i Hercegovini [3]. Memorandum o razumijevanju o nabavci i uspostavi TETRA i VoIP telekomunikacijskih sistema za potrebe policije i organa bezbjednosti u Bosni i Hercegovini između Ministarstva bezbjednosti i korisnika sistema potpisan je dana 02.10.2007. godine. TETRA sistem implementiran je početkom 2008. godine i nakon testiranja i provjere stanja sistema u skladu s odredbama ugovora između Delegacije Evropske komisije i izvođača radova potpisani su od strane Ministarstva bezbjednosti certifikati za privremeni i konačni prihvat sistema. [3]

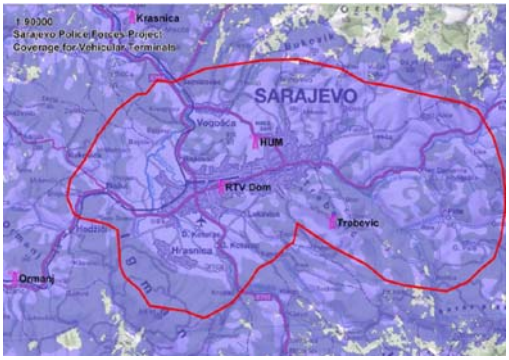
B. Topologija i arhitektura sistema

Topologija realizovanog TETRA sistema je prstenasta sa visokom vrijednošću raspoloživosti koja je uobičajena za profesionalne radio sisteme ćelijskog tipa.



Slika 9. TETRA sistem MS

Postavljenom topologijom se obezbjeđuje pokrivenost signalom Sarajeva i dijela Istočnog Sarajeva. Arhitektura sistema je realizovana u skladu sa relevantnim Evropskim standardima (ETSI standardi i ITU preporuke). [3] [4]



Slika 10. Pokrivenost TETRA sistemom

TETRA sistem se sastoji iz dvije sistemske grupe komponenata: zajednička bazična infrastruktura i terminalna oprema. Zajedničku bazičnu infrastrukturu čine:

a) Bazne stanice (5 kom)
b) NMS (Network Management System)
c) SCN (Switching Control Node)
d) Dispečerske stanice-WDS (2 kom)
e) Linkovi za povezivanje baznih stanica i SCN-a

f) Centri za autentifikaciju i enkripciju (AIKMT i KMC)

g) MoIP (Mobile over IP),

dok pomenutu terminalnu opremu čine:

a) Ručne stanice

b) Stanice za vozila

c) Stacionarne stanice

IV. ZAKLJUČAK

TETRA sistem omogućava ljudima zaduženim za upravljanje i kontrolu znatno bržu komunikaciju i pristup bitnim informacijama. Vremenska kritičnost komunikacije i informacija sve više postaje ključan faktor ne samo za policiju ili hitnu medicinsku pomoć, nego i kod drugih korisnika sistema. Baze znanja i informacija mogu znatno ubrzati proces odlučivanja i upravljanja. Ali i dalje je ključan faktor u cijelom sistemu čovjek kojem je TETRA sistem namijenjen kao pomoć u radu i to kao policijsko sredstvo u rukovođenju i policijsko sredstvo kod intervencija policijskih službenika. Zbog toga je TETRA sistem nužan i bitan, ali samo kao "osnovno" sredstvo za rad, dok je na čovjeku da maksimalno iskoristi mogućnosti TETRA sistema u provođenju zadataka i postizanju željenog policijskog cilja. U radu smo istaknuli moderni digitalni radiokomunikacijski sistem i standard TETRA i mogućnosti koje pruža. Implementirani TETRA sistem Ministarstva bezbjednosti se pokazao kao funkcionalan, pouzdan i kao takav predstavlja dobru osnovu za dalju dogradnju sistema. Budućnost će pred nas postaviti nove izazove, što znači stalno nadograđivanje postojećeg znanja i iskustva.

LITERATURA

[1] Željko Kujavić, Marijan Šuperina, Franjo Magušić, "Razvoj informacijskog sustava radijskih komunikacija u policiji – digitalni radiokomunikacijski sustav TETRA"

[2] Selex Communications, „Elettra TETRA radio mobile digital communications network –issue 4"april 2006.

[3] Projektna dokumentacija za TETRA sistem 2007-2009.

[4] Trans-European Trunking Radio (TETRA); Part 7: Security, ETSI 300 392-7, Decembar 1996.

ABSTRACT

In this paper, an overview of the implementation of the project of building a mobile terrestrial digital radio system - TETRA intended for telecommunication support to the operations of police agencies with complete control of calls in all organized groups and networks and all conditions that may have the character of a crisis situation. The project was implemented in the area of Sarajevo and East Sarajevo as a basis for building a TETRA system in Bosnia and Herzegovina. This paper describes the topology and architecture of the implemented system.

IMPLEMENTATION OF TERRESTRIAL DIGITAL MOBILE RADIO SYSTEM - TETRA IN B&H.

Mladen Mrkaja, Nejra Batalovic, Zoran Koprivica