ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Matyáš Rychetský

Analýza a vize bezpečnosti radiové komunikace pro složky IZS

Bakalářská práce

2022

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K614.....Ústav aplikované informatiky v dopravě

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Matyáš Rychetský

Studijní program (obor/specializace) studenta:

bakalářský – ITS – Inteligentní dopravní systémy

Název tématu (česky): **Analýza a vize bezpečnosti radiové komunikace pro složky IZS**

Název tématu (anglicky): Analysis and vision of radio communication security for Integrated Rescue System

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Vypracujte rešerši stávající radiové komunikace složek IZS jak u nás, tak ve světě.
- Analyzujte bezpečnostní systém radiové komunikace složek IZS v ČR.
- Vypracujte analýzu vhodnoti jednotlivých způsobů zabezpečení radiové komunikace pro složky IZS, včetně zhodnocení jednotlivých rizik.
- Navrhněte doporučení pro další možný vývoj systému radiové komunikace pro složky IZS v ČR.

Rozsah grafických prací: 10 - 20 obrázků

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Odborné časopisy
Internetové zdroje

Vedoucí bakalářské práce: **Ing. Martin Šrotýř, CSc.**
Ing. Michal Mlada, Msc.

Datum zadání bakalářské práce: **30. září 2021**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **8. srpna 2022**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Vít Fábera, Ph.D.
vedoucí
Ústavu aplikované informatiky v dopravě

prof. Ing. Ondřej Přibyl, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Rychetský

Matyáš Rychetský
jméno a podpis studenta

V Praze dne ..... 30. září 2021

Poděkování

Na úvod mé práce bych rád poděkoval všem, kteří mi poskytli podklady pro její vypracování. Zvláště pak děkuji panu Ing. Martinu Šrotýřovi Ph.D. za odborné vedení a konzultování diplomové práce a za rady, které mi poskytoval po celou dobu mého studia. Dále bych rád poděkoval svému kamarádovi Bc. Radku Veselému za poskytnutí odborných znalostí v rámci sítě LTE. Nakonec bych rád poděkoval své rodině a blízkým za morální a psychickou podporu, které se mi dostávalo po celou dobu studia.

Prohlášení

Předkládám tímto k posouzení a obhajobě bakalářkou práci, zpracovanou na závěr studia na ČVUT v Praze Fakultě dopravní.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 8. srpna 2022

Rychetský

Matyáš Rychetský
jméno a podpis studenta

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

ANALÝZA A VIZE BEZPEČNOSTI RADIOVE KOMUNIKACE PRO SLOŽKY IZS

Bakalářská práce

Srpen 2022

Matyáš Rychetský

ABSTRAKT

Cílem této práce je analýza bezpečnosti stávající radiové komunikace pro Integrovaný záchranný systém v České republice a následná analýza možnosti využití moderních radiových technologií a standardů využívané v ostatních zemích. Kromě technologické části je provedena i analýza rizik, které nové technologie mohou svojí implementací přinést.

KLÍČOVÁ SLOVA

Vysílačka, Radiová komunikace, Bezpečnost, Integrovaný záchranný systém, Šifrování, Pegas, LTE, Uživatelské zařízení, Odposlech

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of transportation science

ANALYSIS AND VISION OF RADIO COMMUNICATION SECURITY FOR INTEGRATED RESCUE SYSTEM

Bachelors thesis

August 2022

Matyáš Rychetský

ABSTRACT

The aim of the thesis is the analysis of the security of existing radio communication for Integrated rescue system in the Czech Republic and analysis of the possibility of using modern radio technologies and standards used in other countries. In addition to the technological part an analysis of the risks that new technologies can bring with their implementation is alco carried out.

KEY WORDS

Transmitter, Radio communication, Safety, Integrated rescue system, Encryption, Pegas, LTE, User equipment, Eavesdrop

Obsah

Seznam použitých zkratek

IZS	Integrovaný záchranný systém
RN	Regional network (Regionální síť)
MD	Mediation Device (Provozní servery řídícího subsystému)
MSW	Main Switch
SSW	Secondary Switch
RBS	Radio Base Station (Radiové základny)
CCH	Control Channel (Servisní kanál sítě PEGAS)
TCH	Traffic Channel (Hovorový kanál sítě PEGAS)
DIR	Přímý režim, komunikace mezi účastníky bez RBS
IDR	Independent Digital Repeater (Nezávislý digitální opakovač)
RSN	Identifikační číslo jednotlivých RBS
RFSI	Identifikační číslo jednotlivých terminálů
TPS	Terminal Programming Station (Speciální pracoviště pro nastavení vysílaček)
KMC	Key Management Center (Šifrovací stanoviště)
PK	Personalisation Key (Osobní klíč, unikátní pro každý terminál)
DMK	Direct Mod Key (Klíč pro DIR komunikaci)
TMK	Terminal Master Key
TWP	Tactical Working Position (Stanoviště technického dohledu)
OMN	Operational and Management Network (Páteřní síť)
TTI	Temporary Terminal Identification (Dočasný identifikátor)
TTK	Terminal Key of Key (Hlavní šifrovací klíč)
NNK	National Network Key (Společný klíč pro všechny organizace)
RNK	Regional Network Key (Komunikace v rámci jednoho regionu)
FRNK	Fleet Regional Network Key (Klíč flotily v rámci regionu)
FAK	Fleet Authorisation Key (Klíč pro vytvoření přímého hovoru)
ESOCH	Emergency Single-cell Open Channel (Otevřený kanál)
EMOCH	Emergenci Multi-cell Open Channel (Krizový kanál)
SU-MS	Short User Message Service (Krátká zpráva napsaná uživatelem)
ST-MS	Status Message Service (Zpráva obsahující předpřipravené statusy)
BB-PPDP	Broadband Public Protection & Disaster Relief
LTE	Long Term Evolution
EPS	Evolved Packet Systém (Architektura LTE)
UE	User Equipment (Užitelské zařízení)

E-UTRAN	Evolved UMTS Terrestrial Radio Access Network (Síť se základnovými stanicemi)
EPC	Evolved Packet Core
MT	Mobile Termination (Stará se o komunikační funkce)
TE	Terminal Equipment (Slouží pro zakončení toku dat v UE)
UICC	Universal Integrates Circuit Card (SIM karta v síti LTE)
HeNB	Home eNodeB (Femtobuňky)
eNB	evolved NodeB (Základnové stanice)
SCTP	Stream Control Transmission Protocol (Protokol pro přenos dat skrz S1 rozhraní)
GTP-U	GPRS Tunelling (dopomáhá k snadnému rozpoznávání trasy)
ANR	Automatic Neighbor Realation (Funkce hledající nejbližšího souseda)
P-GN	PDN Gateway
S-GW	Serving gateway
MME	Mobile Management Entity
HSS	Home Subscriber Server
PCRF	Policy Control and Charging Rules Function
IMS	IP Multimedia Subsystem
AITP	Air Interface Transport Protocol (Prostor mezi uživatelem a základnovou stanicí)
PDCP	Packet Data Convergence Protocol (Transportní funkce)
RLC	Radio Link Control (Řídí správné odesílání a přijímání jednotlivých packetů)
MAC	Medium Access Controll (Plánování přenosů dat mezi UE a eNB)
SDU	Service Data Unit (Přijaté packety)
PDU	Protocol Data Unit (Odesílané packety)
RRC	Radio Resource Control
NAS	Network Access Security
NDS	Netword Domain Security
IMSI	Jedinečná mezinárodní uživatelská identita
NAS	Non-Access Stratum (síťová vrstva v modelu OSI)
AS	Access Stratum (Linková vrstva v modelu OSI)
EIA	EPS Integrity Algorithm (Algoritmus pro integrity protection)
SEG	Security Gateway (Zabezpečující brána před vniknutím)
ProSe	Proximity-based Services
GCSE	Group Communication System Enabler
IOPS	Isolated E-UTRAN Operation for Public Security

MCPTT	Mission-critical push-to-talk
MCVD	Mission-critical video and data
PWS	Public Warning System
MBMS	Multicast Broadcast Multicast Service
PTT	Push-To-Talk
TETRA	Terrestrial Trunked System
ETSI	European Telecommunication Standards Institute (Institut pro kontrolu a vytváření nových standardů v rámci telekomunikací)
TDMA	Time Division Multiple Access (Metoda přenosu více dat v jednom frekvenčním kanálu)
FDMA	Frequency Division Multiple Access (Metoda přenosu více dat v jednom čase na různých frekvenčních kanálech)
SCN	Switching Controller Node (Kontrolér sloužící pro řízení a koordinaci mezi RBS)
NMS	Network Managment System (Zabezpečení řízení a dohled nad sítí)
RLS	Remote Line Station (Vzdálený přístup do sítě pro dispečera)
TMO	Trunked Mode Operation (Mód pro přímou komunikaci mezi teminály nebo mezi terminálem a RBS)
SCKs	Static Cipher Keys (Šifrovací klíč v standardu TETRA)
AI	Air Interface (Prostor mezi uživatelem a RBS)
TEAx	Tetra Encryprion Algorithms (Šifrovací algoritmy, x označuje úroveň bezpečnosti)
E2EE	End-to-end Encryption (Šifrovaná komunikace po celé komunikační cestě)
RSSI	Received Signal Strength Indication (Identifikátor vzdálenosti dvou zařízení od sebe)
SWOT analýza	Metoda, při které se zjišťují slabé a silné stránky, hrozby a příležitosti.

Úvod

Je smutné, že jakýkoliv technologický pokrok přijde až po tragické nehodě, při které mohou přijít o život stovky lidí a u radiokomunikací tomu není jinak. Přece jenom komunikace je jedním z nejdůležitějších faktorů pro záchranu lidských životů v rámci záchranných složek, a proto se snaží jednotlivé státy postupně svoji vnitřní radiovou infrastrukturu vylepšovat. Jednou z největších problematik v rámci radiové komunikace je výpadek spojení, a tudíž nemožnost vzájemné komunikace a kooperace. V rámci této problematiky lze řešit vývoj systémů na finančně náročnější či levnější variantu, kdy finančně náročnější varianta kouká do budoucnosti a jde ruku v ruce s přechodem na modernější a bezpečnější systémy, zatím co finančně levnější varianta se ohlíží na modernizaci stávajících systémů za cílem vyhnutí se dané problematiky.

Tato práce se zabývá problematikou stávající sítě a řeší, jakým směrem by se měla Česká republika vydat při vylepšování systému zvané PEGAS. Ten se do České republiky dostal již v roce 1995 a od té doby probíhá jeho neustála modernizace. V roce 2020 skončila jeho podpora a před ministerstvo vnitra přišla rozhodující otázka, zda zůstat na stávajícím systému a prodloužit jeho podporu a tím nadále modernizovat síť i přes velké nedostatky, či přejít na nový, modernější systém. Bohužel k přechodu nedošlo, a i nadále ministerstvo pokračuje v modernizaci sítě PEGAS.

Cílem této práce je zanalyzovat stav radiové sítě PEGAS pro záchranné a bezpečnostní složky IZS a navrhnout možné směry, kterým by mohl budoucí vývoj směřovat. V rámci návrhu jsou zohledněna všechna kritéria, která jsou potřeba pro správný chod radiové sítě neboli jedná se o zabezpečení komunikace proti výpadkům, dále bezpečnost komunikace proti odposlechu a v neposlední řadě podpůrné funkce, které jednotlivé standardy nabízí pro složky IZS. Nakonec je zohledněna i možnost v rámci finančních prostředků.

1 Současný stav radiokomunikační sítě v ČR

Na úvod je potřeba si popsat aktuální stav radiokomunikační sítě v České republice v rámci IZS (Integrovaného záchranného systému). Ty využívají jednotnou radiokomunikační síť PEGAS, která funguje na systému TETRAPOL.

1.1 Základní informace o systému TETRAPOL

TETRAPOL je plně digitální systém vytvořený pro účely šifrované komunikace mezi koncovými uživateli, proto lze říct, že již od začátku byl vytvořen pro bezpečnostní složky. Standard TETRAPOL nabízí dvě možnosti fungování rádiové komunikace: Konvenční a Trunkový.

1.1.1 Konvenční radiové sítě

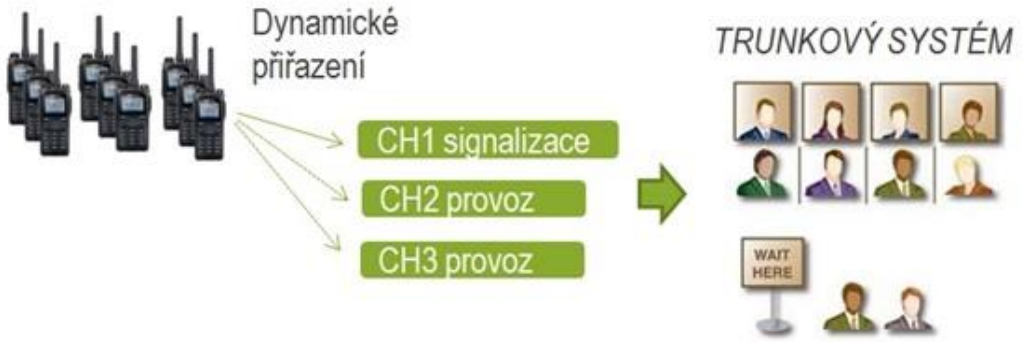
Konvenční, nebo také označovaný jako běžné radiové sítě, pracují na jedné provozní frekvenci, která je již dopředu nakonfigurována v jednotlivých koncových zařízení. S tím přichází hlavní nevýhoda tohoto systému a tím je zaplnitelnost jednotlivých provozních kanálů neboli není zde žádný řídící kontroler, který by dokázala rozdělit jednotlivé koncové zařízení do volných kanálů, a proto se může stát, že v jeden moment je kanál obsazen a ostatní účastnící čekají na jeho uvolnění, zatím co další kanál je volný a nevyužívá se. S tím přichází i další nevýhoda a tím je nemožnost rozdělení uživatelů dle priorit, což u nestandartních situací či větších havárií je problém. [1]

Obrázek 1: Infrastruktura konvenční sítě, zdroj: [1]

1.1.2 Trunkové radiové sítě

Základním rozdílem oproti konvenční radiové sítě je možnost využití obsluhy a řízení většího množství provozních kanálů, proto je tento typ sítě hojně využíván v případě velké kapacitní zátěže. Základem trunkové sítě je tzv. řídící kanál, který neustále komunikuje s jednotlivými terminály a předává řídící a informační data ohledně zaplnitelnosti jednotlivých provozních kanálů. Díky tomu mohou trunkové systémy dynamicky přidělovat jednotlivé frekvenční kanály jednotlivým koncovým zařízením a tím efektivně využít celou síť.

Dalším rozdílem oproti konvenčním sítím je přesunutí inteligence řízení z jednotlivých koncových zařízení na hlavní řídící kontroler. To znamená, že v jednotlivých radiostanicích je uložena pouze nezbytná konfigurace (jako například autorizace do sítě) a zbytek je nahrán do databáze hlavního řídícího kontroleru. Díky tomu lze změnit konfiguraci celé sítě pouze z jednoho bodu a nemusí se měnit všem radiostanicím jednotlivě. [1]



Obrázek 2: Infrastruktura trunkové sítě, zdroj: [1]

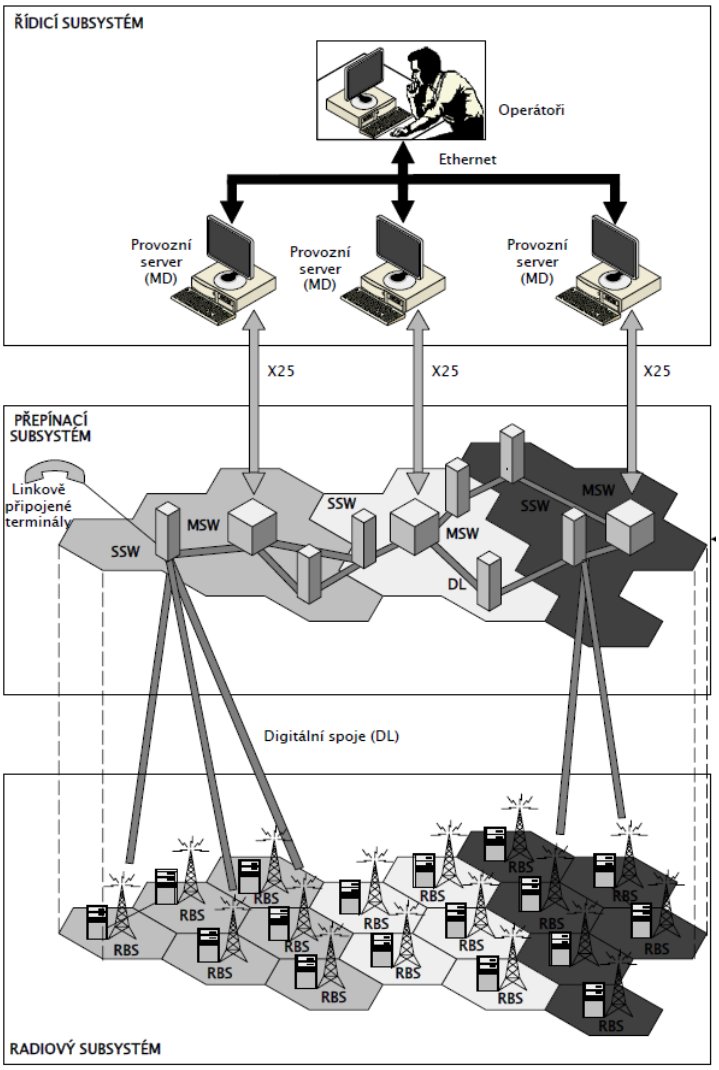
1.2 Základní parametry sítě PEGAS

Jak bylo zmíněno v úvodu kapitoly, tak síť PEGAS funguje na principu standardu TETRAPOL. Zde je pár základních parametrů, které síť PEGAS nabízí:

- Plně digitální síť trunkového typu
- Šifrování na celé své komunikace
- Využívá modulace FDMA
- Má vyhrazené frekvenční pásmo 380–430MHz a 440–490 MHz
- Celá síť je rozdělena do 14 oblastní dle regionálního rozložení ČR
- Vlastníkem je Ministerstvo Vnitra

1.3 Architektura sítě

Celá architektura začíná propojením několika elementárních sítí, které jsou označovány jako regionální sítě RN (Regional Network). V České republice se nachází 14 regionálních sítí, dle krajského rozdělení. Regionální síť následně lze hierarchicky rozdělit do tří navzájem propojených subsystémů: Řídící, přepínací a radiový. Řídící a přepínací subsystém je navzájem propojen páteřní sítí X25 (standard Mezinárodní telekomunikační unie), na kterou jsou připojeny provozní servery, dohledová a řídící centra a řídící jednotky MSW (Main Switch). [2], [3]



Obrázek 3: Architektura sítě PEGAS, zdroj: [4]

1.3.1 Řídící subsystém

Jak již název napovídá, jedná se o hlavní řídící centrum, kde základem všeho jsou provozní servery MD (Mediation Device). [3]

Řídící subsystém obsahuje tyto složky:

- Provozní server MD
- Stanoviště technického dohledu TMP, TDP
- Stanoviště taktického řízení TWP
- Samostatné dispečerské stanoviště SADP
- Stanice programování terminálů TPS
- Stanice programování mikročipových karet SCPS
- Stanoviště kontroly technických údajů a událostí EPC
- Stanoviště klíčového hospodářství KMC
- Jednotka pro zavádění klíčů KLU

1.3.2 Přepínací subsystém

Celý subsystém se skládá ze 2 typů ústředen: MSW (Main Switch) a SSW (Secondary Switch), kde pro každý RN se nachází právě jeden MSW neboli v České republice se nachází 14 MSW. Na ten jsou následně připojeny ostatní SSW, které jsou rozprostřené po celém regionu a tím vytváří hvězdicovou topologii. [3]

Hlavními funkcemi MSW jsou:

- Řízení databáze hlavní ústředny
- Řízení šifrování
- Propojování s ethernetovou sítí v případě datových komunikaci
- Propojování se sítí X25 v případě spojů s provozní a údržbovou sítí a s ostatními regionálními sítěmi
- Řízení a monitorování sítě
- Sběr informací o provozu, alarmech a účastnících
- Přepínání okruhů u hlasových komunikací
- Přepínání paketů u datové komunikace
- Zpracování hovoru
- Řízení datového přenosu
- Řízení připojených zařízení

Vedlejší ústředna SSW provádí:

- Přepínání okruhů u hlasových komunikací
- Přepínání paketů u datové komunikace
- Zpracování hovoru
- Řízení datového přenosu
- Řízení připojených zařízení

Jak je možné vidět z funkcí které jednotlivé ústředny dělají, tak SSW je pouhý spojovatel mezi rádiovou základnou RBS (Radio Base Station) a MSW. [3]

V rámci propojení jednotlivých RN je umožněno spojení dvou SSW z dvou různých RN a tím pádem je možnost komunikace do okolních RN ze dvou či více směrů v případě poruchy. Pokud nastane porucha mezi MSW a páteřní sítí, může komunikace nadále probíhat, jelikož si terminál uchovává v databázi autorizační údaje všech stanic daného RN a také všech stanic, které se za posledních 21 hodin zaregistrovali. Pokud ale nastane porucha mezi SSW – MSW, SSW – RBS nebo MSW – RBS, je provoz dočasně

omezen z důvodu nefunkčnosti autorizace nových terminálů a je pouze možnost komunikovat z již přihlášených terminálů, a to jen v rámci jedné RBS. [3], [4]

1.3.3 Radiový systém

Základní částí radiového subsystému jsou radiové základny RBS (Radio Base Station), které pomocí svých vysílačů zaručují radioelektrické pokrytí signálem v daném prostoru. K jednotlivým RBS se následně připojují jednotlivé terminály. Každá RBS je propojena pomocí digitální linky buď s MSW nebo s SSW, kde jedna SSW dokáže řídit až 8 RBS a tím řídí svoji část regionální sítě. V České republice je momentálně kolem 222 RBS, které se nachází na společných vysílacích stožárech. Pro zvýšení dostupnosti radiové sítě v prostorách, kam se běžná RBS nedostane, jako například pro pokrytí metra, tak se začaly využívat lokální opakovače signálu. [4], [8]

1.4 Typy rádiového spojení

Každý terminál má možnost využití tří typů přenosů rádiového spojení a těmi jsou: Síťový, Přímý nebo Převaděčový režim.

1.4.1 Síťový režim

Určuje komunikaci dvou terminálů přes RBS. Každá RBS neustále vysílá jeden datový servisní kanál CCH (Control Channel), často také označovaný jako řídící kanál. Ten slouží pro přenos provozních informací a dat ohledně stavu sítě a hovorových kanálů. Pokud se účastník tedy chce připojit, musí nejdříve dostat informaci od CCH, který hovorový kanál TCH (Traffic Channel) je dostupný a následně se přeladí na poslech. Posledním trvale vysílacím kanálem je DACH datový kanál sloužící pro přenos GPS pozic a dalších uživatelných informací. [4]

Síťový režim funguje v trunkovém režimu neboli má k dispozici 6 až 10 hovorových kanálů TCH, které jsou dynamický rozdělovány mezi účastníky. Pokud dojde k zaplnění všech TCH, dokáže RBS vytvořit další TCH, přes které mohou účastníci komunikovat. Udává se, že každý RBS má celkem 24 TCH a pokud nastane zaplnění všech TCH, jsou účastníci zařazeni do fronty a vyčkávají na uvolnění jednoho z nich. Rozdělení jednotlivých účastníků do fronty je následně řízeno i podle priority daného terminálu. Pokud se tedy přihlásí uživatel s nižší prioritou, musí vyčkat ve frontě na uvolnění TCH, zatím co uživatel s vyšší prioritou má možnost „násilně“ odpojit účastníka s nižší prioritou od hovorového kanálu. [4]

1.4.2 Přímý režim

Přímý režim DIR, nebo také označován jako direktní mód, zajišťuje přímé spojení dvou terminálů mezi sebou bez použití RBS. Každý terminál má různý počet DIR kanálů podle využití a standardů dané složky IZS neboli HZS má jiný počet DIR kanálů než PČR. Spojení je navázáno v simplexním modu, jinak řečeno využívá se jedna frekvence na příjem i vysílání a není možné vzájemné komunikace ve stejnou dobu. [4]

1.4.3 Převaděčový režim

V lokalitách, která nejsou dobře pokryta základním RBS, jsou využívána zařízení označené jako mobilní nezávislé digitální opakovače IDR (Independent Digital Repeater). Jedná se tedy nejčastěji o pokrytí míst, která se nachází buď v členitém prostoru nebo na velkých prostranstvích. IDR není připojen do páteřní sítě, ale jedná se pouze o „hloupý“ zesilovač signálu pro terminály. Terminál se následně připojuje na IDR kanál, který neustále vysílá informace o síle signálu a o stavu sítě. V ČR se z důvodu vysoké ceny nachází pouze pár desítek IDR opakovačů. Pro zajímavost má každý HZS kraje jeden vlastní IDR opakovač. [3],[4]

Obrázek 4: IDR opakovač, zdroj: [9]

1.5 Identifikace RBS a terminálů

Z důvodu bezpečnosti komunikace a identifikaci jednotlivých RBS a terminálů k nim připojených bylo zapotřebí vytvořit identifikační značky. V rámci RBS se jedná o takzvaný RSN číslo, zatím co u terminálu se jedná o RFSI.

1.5.1 RSN číslo

Jak již bylo řečeno, tak se jedná o identifikační číslo, které každá buňka neustále vysílá. Jedná se spíše o informativní typ identifikace, kdy uživateli je přidělena možnost se

podívat na tuto informaci a tím zjistit, na kterou RBS stanici je momentálně připojen, popřípadě je takto možné sledovat vzdáleně kam je jaký terminál připojen. [4]

Číslo RN	**Číslo MSW**	**Název lokace**
RN0	101	Praha
RN1	125	Středočeský kraj
RN2	222	Jihočeský kraj
RN3	322	Plzeňský kraj
RN4	362	Karlovarský kraj
RN5	422	Ústecký kraj
RN6	462	Liberecký kraj
RN7	522	Královehradecký kraj
RN8	562	Pardubický kraj
RN9	262	Kraj Vysočina
RN10	622	Jihomoravský kraj
RN11	662	Zlínský kraj
RN12	762	Olomoucký kraj
RN13	772	Moravskoslezský kraj

Tabulka 1: Identifikační tabulka pro RSN, zdroj: [4],[5]

Samotná identifikace poté vypadá následovně:

RRR SS NN

Přičemž jednotlivé části značí:

- RRR – Je číselné označení regionální sítě, v tab. 1 označené jako číslo MSW
- SS – Je označení SSW, na které je terminál připojen
- NN – Je vlastní jedinečné označení RBS

1.5.2 RFSI číslo

Zatím co RSN číslo slouží pro identifikaci jednotlivých RBS, tak RFSI číslo slouží pro identifikaci jednotlivých terminálů, které se připojují na RBS. Každý terminál má svůj unikátní identifikátor, který je obdobou SIM karet v GSM síti. [5]
Identifikátor vypadá následovně:

RRR F SS III

Přičemž jednotlivé části značí:

- RRR – Je číselné označení regionální sítě, v tab. 1 označené jako číslo MSW
- F – Číslo tzv. flotily, pod kterou daný terminál spadá. Flotilou se dá představit organizace, pod kterou daný terminál vysílá (HZS, Policie ČR, …).

Č. označení flotily	Skupina uživatelů
0	Servis systému
1	PČR – celorepubliková působnost
2	PČR – regionální útvar
3	Státní organizace, GIPS
4	Jiné organizace, rezerva pro další útvary
5	HZS ČR a HZS podniků
6	Jednotky SDH obcí a SDH podniků
7	ZZS
8	Ministerstvo obrany, Armáda ČR
9	BIS, rezerva pro další útvary

Tabulka 2: Označení jednotlivých flotil, zdroj: [5]

- SS – Číslo skupiny, která se liší pro jednotlivé flotily, pro HZS je to číslo kraje, pro Policii ČR číslo oddělení a další.
- III – Individuální adresa v rámci kraje nebo oddělení

1.6 Příprava terminálů

Každý terminál prochází před použitím dlouhou procedurou programování z důvodu bezpečnosti a správného fungování v síti. Celá procedura se skládá z 6 kroků, které se provádí na speciálním pracovišti označené TPS (Teminal Programming Station) vybaveným stejnojmenným programem. Jednotlivé kroky jsou:

- Nahrání základního projektu sítě PEGAS do stanice TPS
- Přidělení RFSI a nahrání personalizačních informací
- Zápis jednotlivých šifrovacích klíčů
- Vygenerování souboru daného terminálů pro přenesení do taktického dohledu
- Přiřazení priorit daného terminálu
- Aktualizace databáze uživatelů v příslušném MSW

Každý tento krok je nezbytný k funkčnosti jednotlivých terminálů, proto je zapotřebí si je popsat podrobněji. Celý průběh autentizace terminálu je možné vidět na obr. 5.

Krokem jedna je nahrání základního projektu sítě PEGAS do stanice TPS, jinak řečeno se jedná o nahrání globálního seznamu všech dostupných kanálů, které příslušná flotila či jednotka bude využívat. Krok druhý slouží k nahrání personalizačních informací, kde nejdůležitější z nich je RFSI číslo (viz. 1.5.2). Dále se nahrávají základní informace o nastavení sítě v daném RN. [6]

Nejdůležitějším krokem v rámci bezpečnosti komunikace a k samotné autentifikaci terminálů je zápis jednotlivých šifrovacích klíčů. O to se stará stanoviště KMC (Key Management Center), které má k dispozici všechny šifrovací algoritmy. Do každého terminálů se nahrávají 3 základní šifrovací klíče: PK (Personalisation Key), DMK (Direct Mode Key) a TMK (Terminal Master Key). [6]

1.6.1 Personalisation Key

Slouží jakožto dešifrovací klíč k identifikaci sítě a radiostanic. Každý terminál má v sobě nahraný dva PK, z toho jeden z nich funguje pro zašifrování dat sítě a druhý pro zašifrování identifikace stanic v simplexním módu. [6]

1.6.2 Direct Mode Key

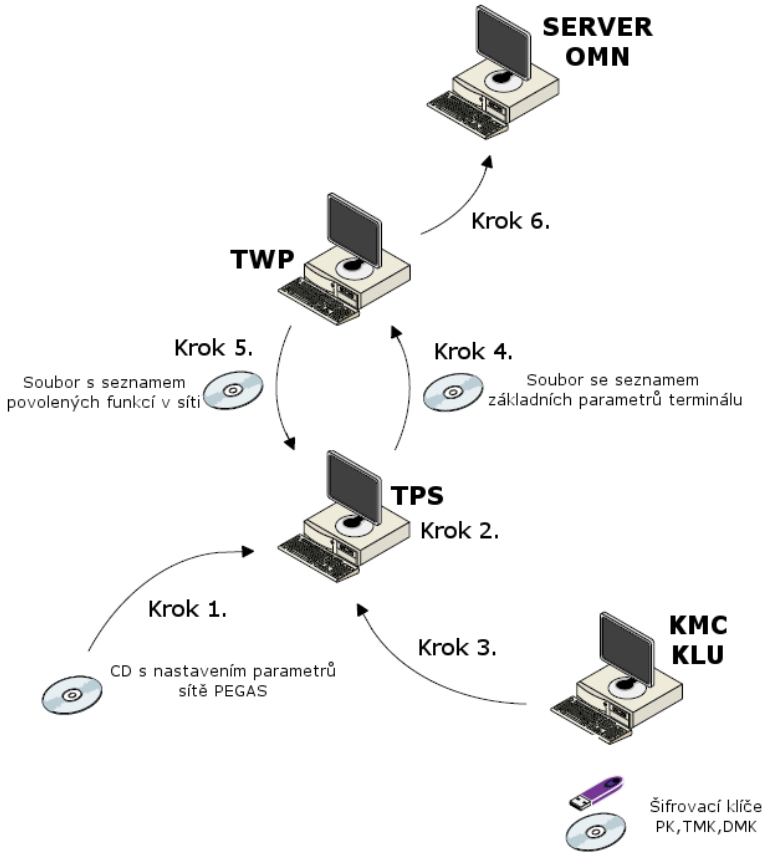
Druhým klíčem je DMK, který slouží jakožto hovorový šifrovací klíč pro komunikaci mimo síť v DIR nebo IDR provozu. Jedná se tedy o veřejný klíč, který mají všechny terminály stejný z důvodu umožnění komunikace mezi jednotlivými terminály v přímém módu. Lepší terminály následně umožňují změnit šifrovací klíč z DMK na libovolný, uživatelem definovatelný, avšak je oslabené celkové šifrování, jelikož lze použít pouze 9 dekadických cifer neboli je možné použít pouze 10^9 možností, zatím co u DMK klíče je možné použít 281 bilión kódů. [6]

1.6.3 Terminal Master Key

Poslední a zároveň nejdůležitější klíč slouží pro samotnou autorizaci terminálu do sítě neboli bez přidělení TMK nemůže terminál komunikovat skrz PEGAS s dalšími účastníky. Každý terminál má svůj jedinečný TMK, který má svoji kryptoperidou (dobu trvání). Pro každou složku IZS je kryptoperioda jiná, pro HZS to jsou 4 roky, zatím co pro PČR to jsou 2 roky. Po uběhnutí kryptoperiody je potřeba opět terminál přeprogramovat s novým TMK. Nemění se ovšem pouze po uběhnutí kryptoperiody, ale také v případě poruchy terminálu. Každý terminál má následně identifikátor, který upozorňuje na dobu skončení kryptoperiody. [6]

Čtvrtý krok slouží k přenesení všech dočasných informací o daném terminálu do stanoviště technického dohledu TWP (Tactical Working Position). Ten slouží především pro přidání informací ohledně seznamu skupin v síti a dostupných DIR a IDR kanálů. Následně lze přidat nadstandartní služby typu možnosti připojení k telefonní síti či možností posílání stavových a textových zpráv. Po přidání všech informací se soubor v kroku 5 nahraje do samotného terminálu. Následně se přidá ještě informace ohledně

priority, kterou daný terminál bude mít v síti neboli zda bude použit pro „obyčejné“ mužstvo zasahující v objektu či pro velitele zásahu. Posledním krokem je nahrání všech informací ohledně daného terminálu do serveru databáze příslušného MSW přes páteřní síť OMN (Operational and Management Network). [6]



Obrázek 5: Autentizace terminálu, zdroj: [6]

1.7 Provoz terminálů

Proces provozu terminálů lze rozdělit do 3 skupin:

- Vyhledávání dostupné RBS
- Autentifikace terminálu přes MSW
- Rozdělení klíčů a komunikace

Na začátku se snaží terminál vyhledat dostupný RBS. V síti PEGAS toto vyhledávání funguje principem hledání poslední RBS, ke které byl přihlášen a až následně se snaží vyhledat ostatní základny. Zde je důležité zmínit největší nevýhodu sítě PEGAS v rámci provozu a tím je nemožnost handoveru. To znamená, že pokud terminál „slyší“ svoji poslední RBS s velmi špatným signálem, tak se stále snaží na ní držet až do samotného vypadnutí, popřípadě se přepne na jinou RBS ale pouze v případě, pokud nový signál je minimálně o 15 dB silnější než poslední. Po vyhledání dostupné RBS se snaží terminál přihlásit do sítě. Ta mu přidělí dočasný identifikátor TTI (Temporary Terminal Identification), přes který terminál komunikuje s MSW. Ten si následně vyžádá

autorizační údaje (RFSI, číslo hardwaru) a vygeneruje kód, který je zašifrován pomocí TMK klíče. Jak bylo zmíněno v kapitole 1.6, tak TMK klíč je nahrán i se všemi údaji o teminálu do příslušného MSW daného RN, pokud se tedy chce uživatel přihlásit z jiného MSW, je zapotřebí nejdříve komunikace obou MSW mezi sebou a vyžádat si tak TMK klíč. Tím, že ho terminál dešifruje, uvede v platnost ověření a je zkontrolovaná priorita terminálu. Pokud se tedy přihlašuje někdo s vyšší prioritou, má větší možnost na přihlášení v zaplněné síti než terminál s nižší prioritou. [6]

Po přihlášení získá terminál od MSW několik časově omezených šifrovacích klíčů. Hlavním klíčem je TTK (Terminal Key of Key), který slouží k dešifrování dalších distribuovaných klíčů. Těmi jsou:

- NNK (National Network key) – Společný klíč pro všechny organizace umožňující komunikaci v celé síti
- RNK (Regional Network Key) – Komunikace v rámci jednoho regionu pro různé organizace
- FRNK (Fleet Regional Network Key) – Klíč flotily v rámci regionu
- FAK (Fleet Authorisation Key) – Pro vytvoření přímého hovoru

Jelikož se jedná o časově omezené klíče, tak vždy po pár hodinách dojde k jejich přeměně. Síť si „zavolá“ všechny terminály přes TTK a předá jim novou sadu klíčů. [6]

1.8 Dostupné služby sítě TETRAPOL

Standard TETRAPOL nabízí velikou škálu dostupných služeb, avšak ne všechny jsou v síti PEGAS využívány. Zde je výběr několika služeb.

1.8.1 Tísňové volání

Jednou z nejdůležitějších služeb je tísňové volání. Každý z terminálů je vybaven tísňovým tlačítkem, kterým upozorní ostatní účastníky na blížící se hrozbu. Při zmáčknutí tlačítka se vytvoří speciální kanál, na který se ostatní terminály připojí. [3] Speciální kanál má celkem 3 varianty:

- Otevřený kanál ESOCH (Emergency Single-cell Open Channel), jehož pokrytí je určeno RBS, pod kterou se daný účastník nachází a je určen všem terminálům bez ohledu na danou flotilu. [3]
- Krizový kanál EMOCH (Emergenci Multi-cell Open Channel), jehož pokrytí je dáno více RBS, které jsou předem nadefinované. Tento kanál slouží pro účastníky hovorových skupin, které mají oprávnění jej využít. [3]
- Nouzový kanál slouží pro terminály, které se nachází v přímém režimu nebo nejsou v dosahu žádného RBS. [3]

Který z kanálu se po zmáčknutí tlačítka danému uživateli otevře je dáno systémovým nastavením dle priority daného terminálu.

1.8.2 Slučování skupin

Slouží pro vytvoření nové hovorové skupiny, do které jsou následně přiřazeni jiní uživatelé z jiných složek IZS. Tento systém dává největší smysl v rámci rozsáhlých zásahů, u kterých bude zasahovat více složek najednou. [3]

1.8.3 Scan

Funkce scan umožňuje danému terminálu sledovat několik skupinových hovorů a následně se připojit do jim hledané. [3] Fungování scanu lze rozdělit do tří typů:

- Prioritní scan – Terminál scanuje uživatelem zvolenou prioritní hovorovou skupinu a následně se připojí. Pokud není nalezena, přihlásí se do neprioritní skupiny. [3]
- Neprioritní scan – Terminál poslouchá první aktivní komunikaci, kterou nascanuje.
- LPM (Listening in priority mode) scan – funguje na obdobném způsobu jak prioritní scan, avšak jsou zde zařazené i hovory v přímém režimu. [3]

1.8.4 Datové služby

Datové služby se dají rozdělit do dvou skupin:

- datové služby přes IP protokol
- Krátké textové zprávy SMS

Datové služby přes protokol IP fungují na obdobném principu jako datové služby založené v mobilním zařízením. Místo mobilního zařízení využívají složky IZS terminál UDT (User Data Terminal), někdy také označenou jako MDT (Mobile Data Terminal), ke komunikaci s rádiovým terminálem, popřípadě se serverem samotným. [3]

Krátké textové zprávy SMS fungují, jak již název napovídá, na principu posílání krátkých zpráv. Podle délky lze dělit tuto část služby na dva druhy:

- SU-MS (Short User Message Service) – Jedná se o zprávy, jejichž délka je maximálně 150 znaků. [3]
- ST-MS (Status Message Service) – Funguje na principu zasílání již předdefinovaných statusů jejichž délka je maximálně 24 znaků. Tyto statusy jsou hojně využívány složky IZS pro urychlení času. Příklady jednotlivých statusů je možné si přečíst v Řádu rádiových komunikací pro HZS. [3]

1.8.5 Systém lokalizace vozidel

V dnešní době velice používaná služba nejen u složek IZS ale i u městské či veřejné hromadné dopravy je systém automatické lokalizace vozidel AVL. Ta slouží pro lokalizaci jednotlivých vozidel za pomocí modulu, který je umístěn ve vozidle. Samotný modul má v sobě zabudovaný přijímač GPS signálu, který vysílají jednotlivé družice z oběžné dráhy planety Země. Informace, které modul získá z jednotlivých oběžných drah jsou následně distribuována na řídící stanoviště, kde je poté možné vzdáleně monitorovat jednotlivá vozidla. [3]

V rámci IZS je tato služba především využívána k efektivní navigaci jednotek k místě zásahu. U novějších vozidel se může nacházet i ve vozidle zařízení pro aktuální navádění vozidel. Další je možné využít data z vozidel a zjišťovat tak informace o stavu dopravy při cestě na místo zásahu. Tyto informace se hodí pro budoucí použití v rámci plánování tras podobným směrem.

2 Sítě využívané v cizině

Každý technologický pokrok přichází až po velké tragické nehodě, při které přijdou o život stovky lidí. Tuto skutečnost si postupně začali uvědomovat jednotlivé státy ostatních zemí a přišli s modernizací svých zastaralých standardů typu TETRAPOL, TETRA a dalších na modernější a výkonnější BB-PPDP (Broadband Public Protection & Disaster Relief) systém. Zde je ukázka dvou států, které se postupně začali technologicky rozvíjet v rámci radiových komunikací pro záchranné složky.

1. Spojené státy americké – První náznaky selhání rádiové komunikace se objevily již v roce 2001, přesněji dne 11. září při tragickém teroristickém útoku na světové obchodní centrum v New Yorku nazvaná jako „Dvojčata“. Postupně kolabující se radiovou sítí se nemohli záchranné složky dorozumět navzájem a tím pádem nemohla probíhat i vzájemná kooperace. V důsledku toho se k hasičům, kteří zasahovali v Severní věži, vůbec nedostala informace o hroutící se budově a bohužel jich stovky zahynulo. Dalším příkladem je rok 2005, kdy při řádění hurikánu Katrina a Rita také selhalo radiové spojení a záchranné složky neměli možnost vzájemné komunikace. Postupným hromaděním dalších tragických nehod se nakonec v roce 2012 rozhodl kongres Spojených států o výstavbu nové, modernější celosvětové komunikační sítě nazvanou FirstNet.
2. Korejská republika – Asijské státy se vždy snažily být technologicky dopředu oproti ostatním zemím, a proto bylo největší záhadou zklamání tehdejší komunikační sítě. Píše se 16. duben 2014 a u pobřeží Jihokorejské republiky se potopil trajekt Sewol, který převážel 470 cestujících. Tragická kooperace a nemožnost komunikace při záchranné akci z důvodu nekompatibilních systémů si vyžádala vysoké ztráty. Přesněji zde zahynulo 304 cestujících. Po nezdařilé záchranné akci se v červnu 2014 rozhodla jihokorejská vláda pro vybudování nové celonárodní komunikační sítě nazvanou SafeNet

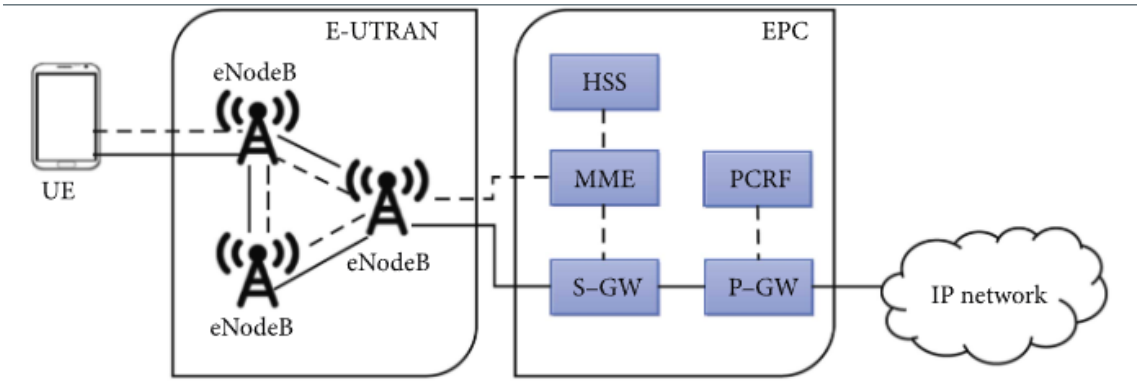
Evropské státy jsou v modernizaci svých komunikačních sítí nejpomalejší. První náznak modernizace ukázala Francie se svojí sítí PC STORM po útoku na Charlie Hedbo v roce 2015 a následném teroristickém útoku téhož roku. V závěsu se nachází Velká Británie se svým ESN systémem a postupně se přidávali další evropský státy. [11]

2.1 LTE

LTE (Long Term Evolution) je projekt vytvořený skupinou 3GPP (The Third Generation Partnership Project). Ta se rozhodla v rozvinutí svého stávajícího systému UMTS (Universal Mobile Telecommunication Systems), který fungoval na obdobné fázi jako sítě GSM.

2.1.1 Architektura LTE

Architektura LTE, také označována jako EPS (Evolved Packet System), se skládá ze 3 hlavních částí, které je možné vidět na obr. 6. Jednotlivé části jsou UE (User Equipment), E-UTRAN (Evolved UMTS Terrestrial Radio Access Network) a EPC (Evolved Packet Core).



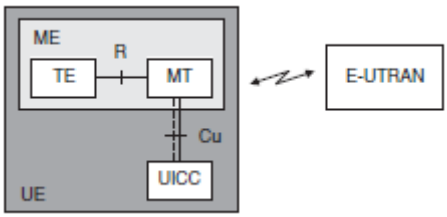
Obrázek 6: Architektura LTE, zdroj: [11]

2.1.1.1 UE

Pod pojmem uživatelské zařízení (UE) si lze představit mobilní zařízení či tablet, který má možnost se připojit do sítě LTE. UE lze rozdělit do 2 částí:

- MT (Mobile Termination) – Stará se o komunikační funkce
- TE (Terminal Equipment) – Slouží pro zakončení toku dat v UE

MT a TE poté dohromady dávají ME (Mobile Equipment). Na ten je připojena SIM karta, která je označená jako UICC (Universal Integrates Circuit Card), na které běží aplikace USIM (Univesal Subscriber Identity Module). Zde jsou uloženy informace o uživateli jako například telefonní číslo či identitu jeho domovské sítě, ale také se zde nachází šifrovací klíče potřebné k připojení do LTE sítě. [12]



Obrázek 7: Základní komponenty UE, zdroj: [12]

2.1.1.2 E-UTRAN

Hlavní funkcí E-UTRAN je propojení rádiové komunikace mezi UE a EPC a skládá se pouze z jedné komponenty, základnové stanice eNB (evolved NodeB). Ta dokáže obsloužit jedno UE v jedné či více buňkách, zatím co UE může být v jeden čas připojený pouze na jedno UE. eNB má 2 základní funkce. [12]

- Komunikace se všemi UE, na které jsou na ní připojené, prostřednictvím downlinku a následného přijímání vysílání přes uplink

- Handover mezi buňkami. To znamená, že postupně vzdalující se UE dostane od eNB signální zprávu o přepnutí na jiný eNB. Tím je zařízená plynulost přechodu mezi jednotlivými eNB.

Každá základnová stanice komunikuje s EPC přes rozhraní S1. Dále komunikuje s ostatními eNB prostřednictvím rozhraní X2. To slouží především pro přenos informací ohledně UE. [12]

Používají se i malé eNB, tzv. femtobuňky, které slouží k pokrytí malých vnitřních prostor, kam se nedostane klasická eNB. Těmto stanicím se říka HeNB (Home eNodeB).

Rozhraní S1

Slouží pro přenos informací a signalizačních zpráv mezi eNB a EPC. Základní struktura tohoto rozhraní funguje na principu SS7 signalizace neboli jsou signalizační a hlasový okruhy od sebe oddělené. [12] Rozhraní S1 lze rozdělit do dvou částí: Control a User plane.

- Control plane – slouží pro přenos signalizace přes protokol SCTP (Stream Control Transmission Protocol).
- User plane – slouží pro přenos hlasových informací a je vybaven GTP-U (GPRS Tunelling) protokolem, který dopomáhá k snadnému rozpoznávání trasy a usnadnění přenosu dat.

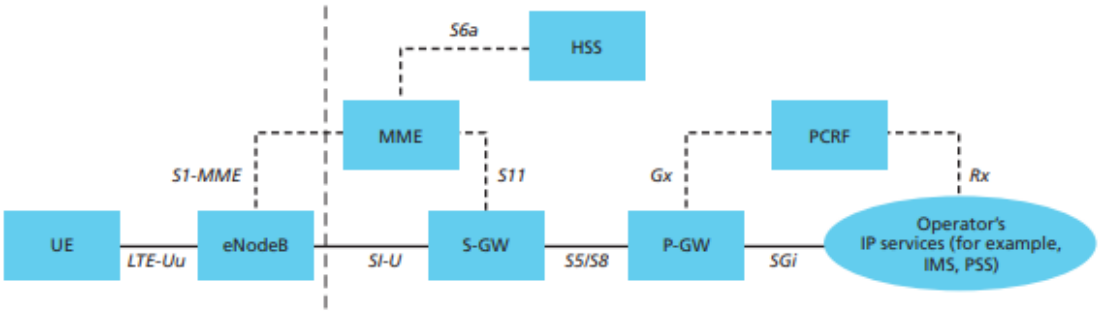
Rozhraní X2

Používá se pro propojení a k výměně informací mezi jednotlivými eNB. Hlavní informací, kterou si eNB předávají, je informace ohledně handoveru, proto pomocí funkce ANR (Automatic Neighbor Realation) hledá nejbližšího souseda, na kterého by se UE mohlo připojit. [12]

Rozhraní X2 se nejčastěji využívá u dvou sousedících eNB, které jsou od sebe na krátkou vzdálenost. Pro vzdálenější eNB se pro přenos informací ohledně handoveru používají dvě linky S1 přes EPC. [12]

2.1.1.3 EPC

EPC (Evolved Packet Core) je hlavním řídícím mozkem sítě LTE. Je zodpovědné za správnou funkčnost sítě, řízení jednotlivých UE a výrobu nositelů informací. Na obr. 8 je možné vidět základní prvky EPC. Hlavní části jsou: P-GN (PDN Gateway), S-GW (Serving gateway), MME (Mobile Management Entity), HSS (Home Subscriber Server) a PCRF (Policy Control and Charging Rules Function). [12]



Obrázek 8: Základní komponenty EPC, zdroj: [13]

Pojďme si popsat jednotlivé části.

- HSS – Hlavní uživatelská databáze uchovává všechny potřebné informace o uživateli a zároveň uchovává všechny potřebné šifrovací klíče, kterými se UE snaží autentifikovat do sítě.
- MME – Slouží ke zpracování signalizace mezi UE a EPC. Dále plní funkci řízení komunikace mezi UE a HSS a následnou volnou přes který S-GW bude uživatel svá data posílat. Stará se tedy o bezpečné řízení a připojení uživatele s EPC.
- S-GW – Skrz tuto bránu prochází všechny vysílané packety od uživatele do EPC a následně je směruje do příslušného P-GW.
- P-GW – Slouží k přidělování IP adres jednotlivým UE. Dále je zodpovědný za poskytnutí kvality služeb QoS (Quality of Service), které jsou popsány v PCRF.
- PCRF – Uchovává jednotlivá pravidla a služby, které jsou poskytovány uživateli v rámci QoS a kontroluje autorizaci jednotlivých packetů v P-GW a rozhoduje, jak s nimi bude zacházeno.
- IMS (IP Multimedia Subsystem) – Část nenacházící se přímo v EPC, avšak sloužící k přenosu multimediálních služeb jako jsou například VoLTE, SMS a MMS.

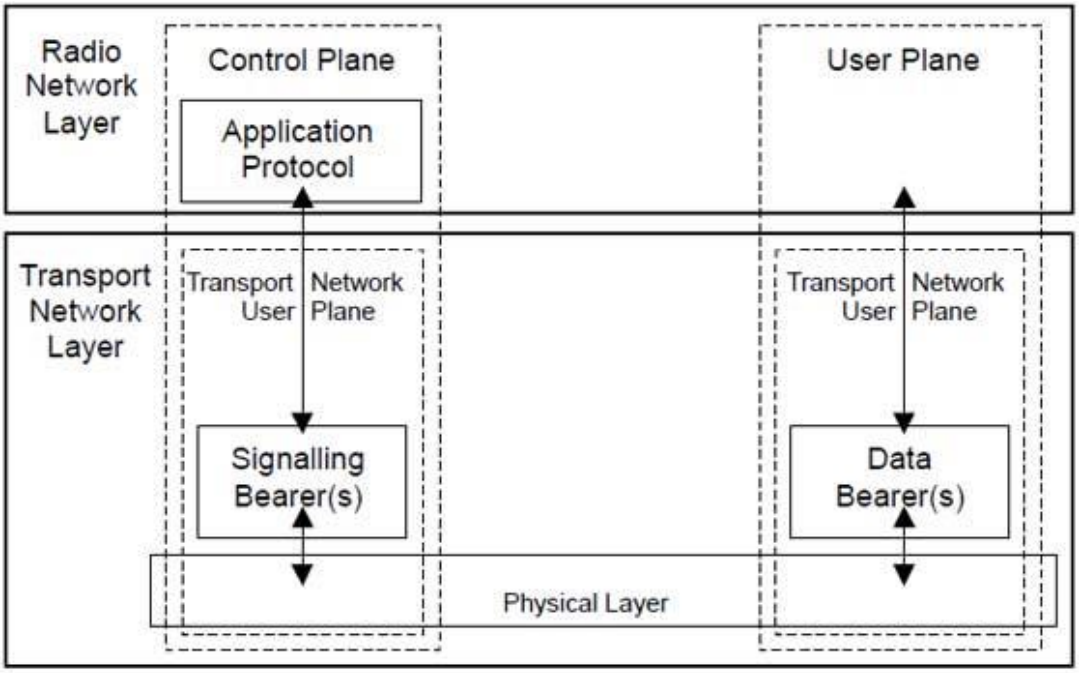
2.1.2 Komunikační protokoly

V rámci sítě LTE lze rozdělit protokoly do dvou skupin. Těmi jsou:

- Uživatelská část (User plane) – Stará se o přenos dat, která jsou zajímavá pro uživatele
- Řídící část (Control plane) – Stará se o přenos informací potřebných k chodu v síti.

Tyto dvě skupiny ještě následně lze rozdělit do 2 vrstev. Horní vrstva (Radio Network Layer) slouží k práci s informacemi přes radiové prostředí, zatím co spodní vrstva (Transport Network Layer) slouží pro přenos informací z jednoho bodu do druhého.

V rámci zjednodušení jsou zde představeny pouze tyto 2 skupiny, jelikož by se dali ještě rozdělit do dalších, menších protokolů, na kterých jsou stavěny. [14]



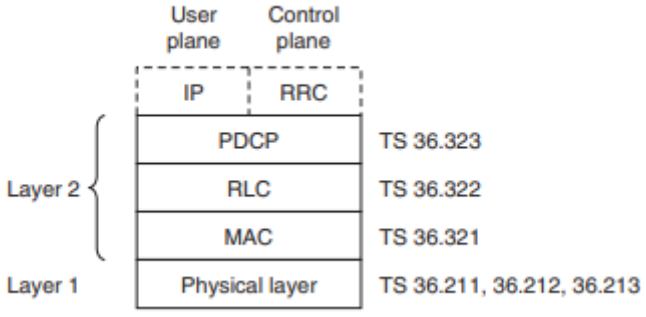
Obrázek 9: Základní rozdělení vrstev protokolu, zdroj: [14]

2.1.2.1 Uživatelská část

Uživatelská část, někdy také označovaní jako AITP (Air Interface Transport Protocol), se skládá ze dvou vrstev, jak je možné vidět na obr. 10. První vrstva, nazývána jako fyzická, obsahuje analogové a digitální funkce, které slouží pro odesílání informací z UE nebo eNB. Druhou vrstvou, nazývanou jako linkovou podle modelu OSI, lze rozdělit do 3 částí.

- PDCP (Packet Data Convergence Protocol) – Provádí transportní funkci na vyšší úrovni spojenou s kompresí a dekonpresí jednotlivých packetů a jejich zabezpečením.
- RLC (Radio Link Control) – Řídí správné odesílání a přijímání jednotlivých packetů.
- MAC (Medium Access Controll) – Provádí nízko-úrovňovou kontrolu fyzické vrstvy a stará se především o plánování přenosů dat mezi UE a eNB

Přijatým packetům se říká SDU (Service Data Unit), zatím co vysílaný se nazývají PDU (Protocol Data Unit). [13],[14]



Obrázek 10: Vrstvy AITP, zdroj: [12]

2.1.2.2 Řídící část

Jak již bylo popsáno na začátku kapitoly, tak řídící část slouží pro přenos informací potřebným k chodu sítě. Řídí tedy funkce, které se týkají rádiového přenosu a obsahuje protokol RRC (Radio Resource Control), která se nachází ve vyšší vrstvě a konfiguruje nižší vrstvu.

Řídící část pracuje ve 2 stavech. Prvním z nich je tzv. idle stav, při kterém uživatelské UE vyčkává na vhodnou eNB, ke které by se mohl připojit. Během vyčkávání monitoruje ostatní eNB a zjišťuje kvalitu radiového spojení, sílu signálu a další. Při připojení se přepne do tzv. connected stavu, kdy UE komunikuje s E-UTRAN a navzájem si předávají informace o síle signálu a následně E-UTRAN komunikuje s ostatními eNB o případném handlingu. [14]

2.1.3 Zabezpečení sítě

Jednou z nejdůležitějších částí v rámci LTE je zabezpečení komunikace proti odposlechu. Celou zabezpečovací síť lze rozdělit do 2 skupin: NAS (Network Access Security) a NDS (Network Domain Security). V této kapitole si popíšeme jednotlivé skupiny, jejich funkčnost a kroky k zabezpečení proti odpolechu. [12]

2.1.3.1 Network Access Security

Jednou z nejvíce ohrožených částí je komunikace mezi uživatelským UE a sítí LTE v radiovém prostředí. Network Access Security využívá v rámci ochrany údajů a komunikace 3 základní služby.

Autentizace

Průběh spočívá na vzájemné komunikaci mezi UE a EPC. Poté co se chce UE přihlásit do LTE sítě, EPC si zkontroluje v databázi HSS, zda se opravdu jedná o UE, které má oprávnění se přihlásit do sítě a nejedná se o klon. Zároveň UE kontroluje, zda se opravdu přihlašuje do správné sítě a nejedná se o síť, využitou pro krádež informací. [12]

Důvěrnost zařízení

Confidentiality, česky přeloženo jako důvěrnost, ochraňuje uživatelovu identitu. Každý z uživatelů má svou jedinečnou mezinárodní uživatelskou identitu (IMSI), kterou potřebuje narušitel získat, aby se mohl vydávat za uživatele. V rámci ochrany IMSI se

snaží síť LTE nevysílat tuto informaci co nejčastěji, a proto pro identifikaci uživatele využívají dočasnou identitu. [12]

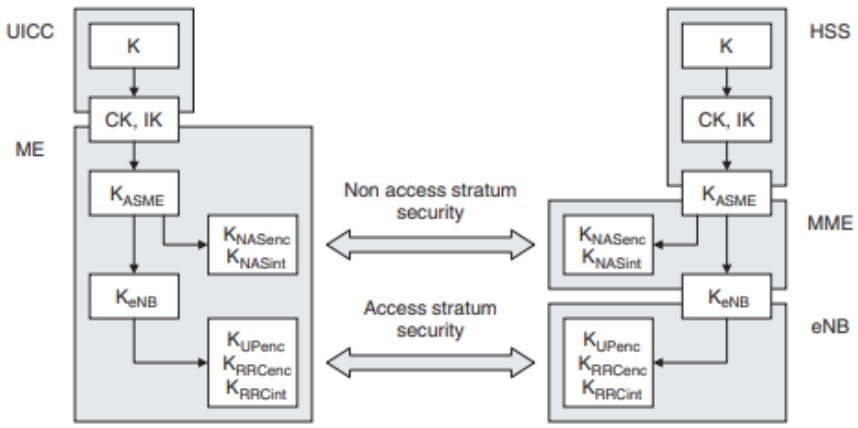
Šifrování

Jednou z důležitých částí bezpečnosti je šifrování. To zabraňuje narušiteli zachycovat signální zprávy a číst data. Podpůrnou službou je poté Integrity protection, která kontroluje, zda nebyla data zachycena, zmodifikována a poslána zpět za účelem ovládnutí UE či části sítě LTE. [12]

2.1.3.1.1 Zabezpečovací klíče

Princip zabezpečení začíná v architekturou zabezpečovacích klíčů, který je možné vidět na obr. 11. Nejzákladnější z nich je klíč K, který se nachází jak v uživatelově UE, přesněji v UICC, tak i v HSS. Klíč K je úzce spojen s jedinečnou mezinárodní uživatelskou identitou IMSI, proto se pro bezpečnost nekontroluje přímo kód IMSI ale klíč K. Ten následně vytvoří nové 2 klíče: CK a IK. Tyto klíče zde jsou pouze z historického důvodu a složí k přenosu a kontrole informací mezi klíčem K a novým klíčem v rámci ASME (Access Security Management Entity) K_{ASME}. Tento klíč se již nachází v části ME uživatelově UE, zatím co u EPC se nachází v MME. Jednotlivé komponenty poté vytvoří z klíče K_{ASME} 3 nové klíče. Těmi jsou: K_{NASenc}, K_{NASint}, K_{eNB} z toho první dva klíče slouží pro šifrování a integrity protection (viz. část Šifrování) v tzv. NAS (Non-access stratum) oblasti a poslední slouží k přenosu v rámci AS (Access Stratum). [12] Zde je popis jednotlivých oblastí:

- NAS oblast si lze představit jako síťovou vrstvu v modelu OSI. Slouží tedy pro přenos signalizačních zpráv a informací mezi UE a sítí, přesněji MME.
- AS oblast funguje na principu linkové vrstvy v modelu OSI neboli slouží pro přenos dat a informací mezí UE a eNB.



Obrázek 11: Hierarchie zabezpečovacích klíčů, zdroj: [12]

Poslední krok vytvoří z klíče K_{eNB} nové 3 klíče, které jednotlivě slouží pro šifrování a integrity protection v AS oblasti. Těmi jsou K_{UPenc},K_{RRCenc},K_{RRCint}. [12]

2.1.3.1.2 Autentifikace UE

Proces začíná spuštěním UE a vyžádáním se přístupu do sítě LTE. Toto vyžádání získá MME, které potřebuje zjistit pro autentifikaci správnost IMSI. Prvním krokem si MME vyžádá IMSI z uživatelské databáze HSS. Jak bylo zmíněno v části Zabezpečovací klíče, tak IMSI úzce souvisí s klíčem K. HSS tedy vytvoří pomocí klíče K tzv. autentification vector, který se skládá ze 4 částí. [12] Ty jsou popsané zde:

- RAND – Jedná se o náhodné číslo, které MME využije jako výzvu k ověření UE
- XRES – Na výzvu, kterou vytvoří RAND, očekává MME odpověď, kterou zná pouze UE, jelikož má správnou hodnotu K.
- AUTN – Funguje na stejném principu jako XRES, avšak pro síťovou část. Dále je zde přidána sekvence čísel, která ochraňují přes pachatelem, který by chtěl odposlouchávat autentifikaci zařízení a tím získat klíč K.
- K_{ASME} – Obsahuje v sobě zašifrovaný klíč K. Více informací lze najít v části Zabezpečovací klíče.

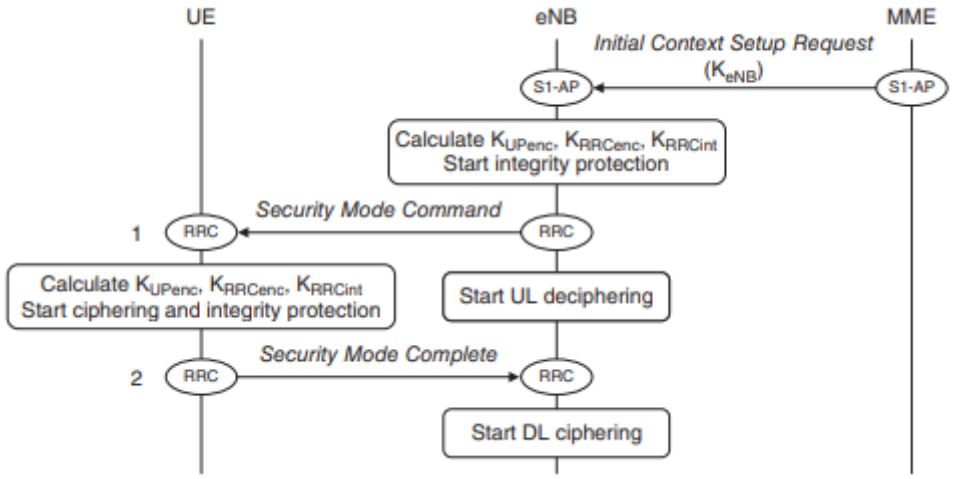
V druhém kroku jsou všechny tyto části předány zpět MME. Následně, v třetím kroku, MME posílá UE dvě části. Těmi jsou RAND a AUTN v rámci autentifikace. V UE si tyto části převezme část ME, která je přepošle do UICC. Zde USIM získá výzvu od RAND a následně zkontroluje AUTN, zda nedošlo ke změně sekvenci čísel od pachatele. Pokud tomu tak není, tak začne USIM vytvářet odpověď RES, která by u MME měla být stejná s XRES. Odpověď je následně poslána zpět do MME, kde proběhne kontrola mezi RES a XRES a pokud vše souhlasí, je možnost přejít k dalšímu bodu a tím je zapnutí šifrování a integrity protection mezi UE a MME a následně UE a eNB. [12]

2.1.3.1.3 Bezpečnostní část

Tato část se zabývá spuštěním šifrování a integrity protection mezi UE a eNB pře AS a UE a MME přes NAS. První z nich se spouští kontrola v rámci oblasti NAS. Hnedka po přijetí autentifikace uživatele začne MME komunikovat s UE ohledně zapnutí šifrování a integrity protection. Prvním krokem je vytvoření klíčů K_{NASenc} a K_{NASint}, které následně posílá do UE v rámci oznámení o aktivování NAS šifrování a integrity protection. Hnedka po odesílání začne MME se šifrováním uplink zpráv v rámci ochrany informací. Po přijmutí zpráv vytvoří UE vlastní kopie klíčů K_{NASenc} a K_{NASint} a odpoví zpět v již šifrované formě, že zapnulo NAS šifrování a integrity protection. Jakmile MME získá tuto zprávu, začne s šifrováním dat i po downlink straně. [12]

AS oblast funguje na podobném systému jako NAS, akorát s malou změnou na začátku. Nutno podotknout, je AS oblast se aktivuje až po ověření zapnutí NAS šifrování. Na začátku MME předá eNB informaci o zapnutí AS šifrování a integrity protection přes klíč K_{eNB}. Jakmile eNB získá tento klíč, probíhá výměna klíčů obdobná u NAS oblasti, jen s tím rozdílem, že se zde předávají mezi UE a eNB tři klíče. Těmi jsou: K_{NASenc}, K_{NASint}, K_{eNB}. Celý průběh aktivace zabezpečení v AS oblasti je možné vidět na obr. 12. [12]

Během handoveru je potřeba, aby si jednotlivé eNB předali informaci ohledně klíče K_{eNB}. Toho lze docílit dvojím způsobem. Buď přímou komunikací mezi jednotlivými eNB přes X2 rozhraní, nebo přes parametr NH (next hop), který je zaslán MME a ten přenese informaci dalšímu eNB. [12]



Obrázek 12: Aktivace zabezpečení v AS oblasti, zdroj: [12]

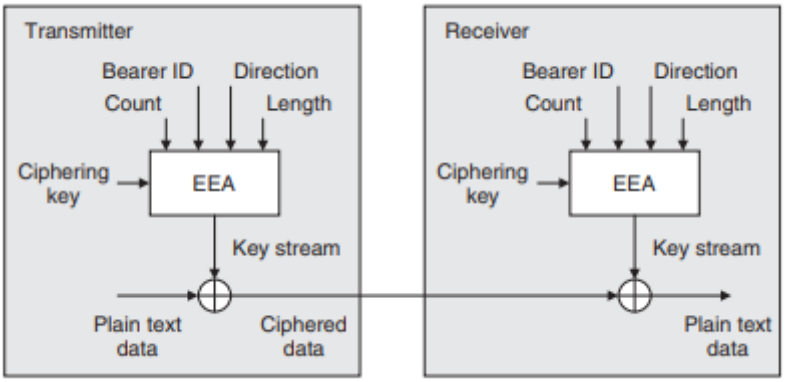
2.1.3.1.4 Šifrování

Šifrování je jednou z nejdůležitějších částí v rámci ochrany uživatelských dat. Útočník, který se k datům dostane, musí nejdříve prolomit šifrovací klíč, aby mohl samotná data přečíst.

Šifrovací proces lze rozdělit do dvou částí: Odesílací a přijímací. Obě tyto části fungují na podobném způsobu. Odesílací čas si nejdříve vezme šifrovací klíč a za pomocí ostatních informačních částí vytvoří pseudonáhodný klíč, kterým jsou zašifrována samotná data. K zašifrování se využívá logické funkce X-OR. Příjímací část vytvoří vlastní kopii pseudonáhodného klíče obdobním způsobem jako tomu je u odesílací části. Následně po příjímání jednotlivých dat využívá tento pseudonáhodný klíč k rozšifrování dat. Celý šifrovací proces je možný vidět na obr. 13. [12]

V rámci zvednutí ochrany se začaly využívat celkem 4 úrovně šifrovacích klíčů.

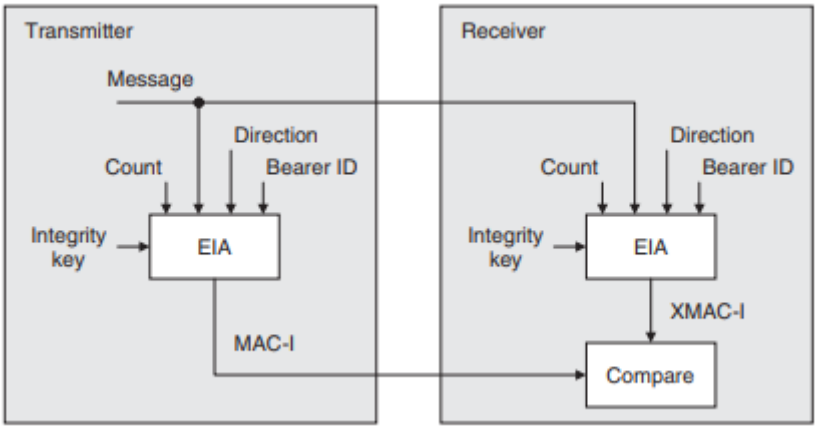
- Null – Nepoužívá se žádné šifrování. Tato úroveň se z velké části nevyužívá z důvodu bezpečnosti uživatelských dat.
- EEA1 – Je založen na obdobném šifrování jako bývalý UMTS. Jedná se o jednu ze základních šifrování, dnes také moc nevyužívanou. [7]
- EEA2 – Šifra založena na AES (Advanced Encryption Standard) algoritmu, který využívá 128,192 a 256 bitů pro šifrování a pro dešifrování jednotlivých bloků o délce 128 bitů. V LTE se využívá pouze 128 bitů jak pro šifrování, tak i pro dešifrování. [7]
- EEA3 – Poslední úrovní je šifrování založené na ZUC algoritmu, který využívá 128bitový počáteční klíč a 128bitový počáteční vektor na vstupu, zatím co na výstupu posílá zašifrovaný tzv. Key-stream o velikosti jednotlivého bloku 32 bitů. [7]



Obrázek 13: Průběh šifrování, zdroj: [12]

2.1.3.1.5 Integrity Protection

Integrity protection slouží k zjištění, zda pachatel neodposlouchává komunikaci mezi UE a eNB (Popřípadě UE a MME v NAS oblasti). Stejně jako u šifrování, tak i zde lze rozdělit fungování integrity protection na dvě části: Odesílací a přijímací. Odesílací část získává všechny signalizační zprávy, které si mezi sebou UE a MME posílají. Tyto zprávy následně vezme a přes EIA (EPS integrity algorithm) přidá tzv. MAC-I. Jedná se o 32bitovou zprávu slouženou z pseudonáhodného čísla. Takto složená zpráva je následně poslaná ven k přijímací straně. Ta nejdříve rozdělí MAC-I a signalizační zprávu. Přes vlastní EIA vytvoří identický MAC-I, tentokrát označený XMAC-I a porovná, zda jsou tyto zprávy podobné. Pokud tomu tak není, tak se nachází uprostřed útočník, který odposlouchává zprávy a posílá je dál. V takovém případě je signalizační zpráva smazána. Celý průběh tvorby integrity protection je možné vidět na obr. 14. [12]



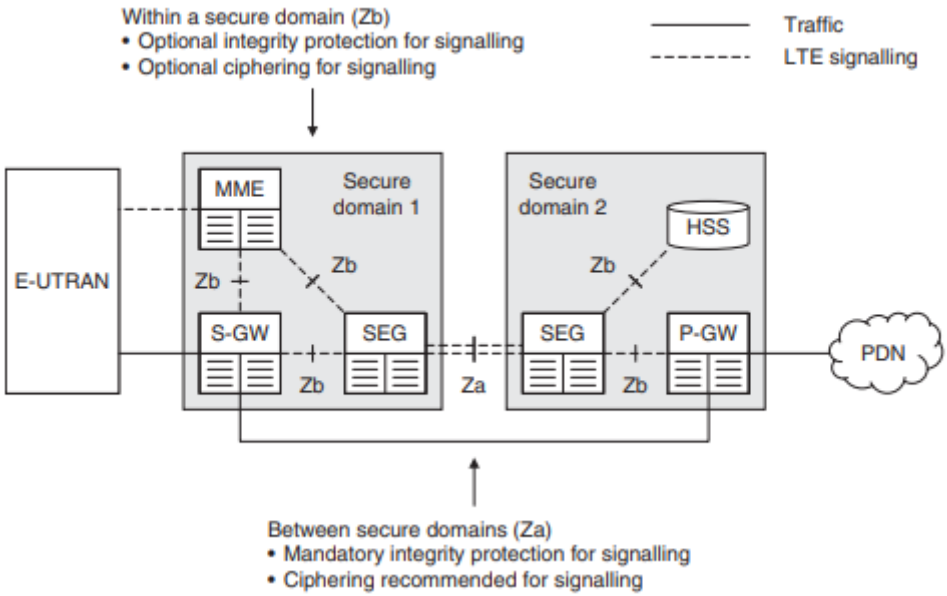
Obrázek 14: Průběh Integrity Protection, zdroj: [12]

2.1.3.2 Network Domain Security

Zatím co Network access security zajišťoval bezpečnost komunikace mezi UE a MEE (popřípadě UE a eNB), tak Network Domain Security zajišťuje bezpečnost sítě v rámci EPC a eNB u jednotlivých operátorů. Komunikace uvnitř sítě je založena na IP, založena na standardu IETF.

V EPC je vyžadována bezpečnost mezi různými sítěmi, které řídí odlišní operátoři, kvůli roamujícím uživatelům. Toho je docíleno pomocí bezpečnostní domén (security domains). Ta většinou odpovídá sktruktuře operátorově EPC, ale operátor má možnost rozdělit EPC do více domén, jak je to zobrazené na obr. 15. Jednotlivé domény jsou následně propojeny rozhraním Za a ostatní časti rozhraním Zb. Jednotlivé packety prochází skrz SEG (Security Gateway), aby se dostali k rozhraní Za. Zde se data připraví na možný průchod rozhraním. V LTE jsou totiž packety, procházející skrz Za, chráněni tzv. tunnel modem. To znamená, že se k jednotlivým packetům přidá IP adress hlavička a následně jsou zašifrovány a odeslány. Lze si to představit jako klasickou komunikaci mezi 2 počítači, kdy jedné počítač posílá svému modemu nešifrovaná data, ten je následně zašifruje společně s IP hlavičkou a pošle ven do internetu. Zatím co Za má povinnou ochranu dat, Zb je spíše dobrovolná, o které rozhodují jednotlivý operátoři, sloužící pro komunikaci mezi jednotlivými časti uvnitř domény. [12], [16]

V eNB si jednotlivý operátoři zajišťují bezpečnost v X2 a S1 rozhraní. To se především jedná i femtobuňkách, které komunikují s EPC přes veřejný IP backhaul nebo kde je potřeba vyřešit X2 a S1 rozhraní přes mikrovlnné spojení. Po zajištění bezpečnosti je doporučeno zapnutí ESP tunnel modu v rámci komunikace. [12]



Obrázek 15: Zabezpečení v EPC, zdroj: [12]

2.1.4 PS-LTE

PS-LTE neboli Public Safety LTE, je služba rozšiřující klasické LTE o podpůrné funkce pro složky IZS. Právě tuto službu využívají ostatní státy, které byli popsány v úvodu této kapitoly. Základní podpůrné funkce jsou vypsány zde a jsou znázorněny na obr. 16:

- ProSe (Proximity-based Services)
- GCSE (Group Communication System Enabler)
- IOPS (Isolated E-UTRAN Operation for Public Security)
- MCPTT (Mission-critical push-to-talk)
- MCVD (Mission-critical video and data)
- PWS (Public Warning System)
- Priority service

2.1.4.1 Proximity-based Services

Umožňuje přímou komunikaci mezi dvěma sousedícími UE bez nutnosti připojení do sítě. Jedná se tedy o obdobnou funkci, jako je v síti PEGAS přímý režim. ProSe využívá celkem 2 funkce. První funkce slouží jako vyhledávací maják, kdy se hledá v otevřeném prostoru sousední UE. Toho lze docílit dvěma způsoby. První funguje na bázi síťového dotazu, kdy UE pošle požadavek do sítě na vyhledání okolních UE. Druhý způsob funguje na bázi vysílacího majáku, kdy uživatelovo UE vysílá do volného prostoru ProSe code. Sousedící zařízení následně detekuje tento kód a následně dojde k připojení. Druhou funkcí je již zmíněné připojení obou UE. [17]

2.1.4.2 Group Communication System Enabler

GCSE funkce funguje na principu přenášení dat mezi více uživatelů. Tato funkce již je implementovaná i v síti PEGAS, ale slouží pouze pro přenos hlasu. Síť LTE podporuje přenos jak hlasu, tak dále videa a uživatelských dat zároveň a tím dopomoci většímu přehledu nad děním v místě zásahu. Jak bylo zmíněno výše, tak GCSE slouží pro přenos dat více uživatelům označované jako skupina (z anglického slova groups), kdy každá skupina může získávat jiné informace než jiná skupina. Funguje tedy na principu paralelního odesílání potřebných informací skupinám, které zrovna potřebují. Může se tedy stát, že hasiči v místě zásahu získávají pouze hlasové informace, zatím co přenos videa je přenášen do operačního a řídícího centra či k velitelům zásahu. V rámci architektury se vytvořila nová část v EPC nazvaná MBMS (Multicast Broadcast Multicast Service), která dopomáhá k chodu GCSE. [17]

2.1.4.3 Isolated E-UTRAN Operation for Public Security

K odolnosti a zvýšení konektivity v místech, kam nedosahuje klasická síť LTE či dochází k výpadkům v rámci zásahu, dopomáhá IOPS. Jedná se o přenosné eNB (NeNB), které lze namontovat v místě zásahu a tím rozšířit či posilnit signál LTE. [17]

2.1.4.4 Mission-critical push-to-talk

Jedna z nejdůležitějších podpůrných funkcí je MCPP. Jedná se o technologii, která umožňuje nouzovou komunikaci pomocí tlačítka PTT (Push-To-Talk). Pomocí zmáčknutí PTT tlačítka lze vybrat jednu z předpřipravených funkcí. Těmi jsou:

- One-to-one – Kontaktování pouze jednoho uživatele
- One-to-many – Kontaktování zvolené skupiny
- Tísňové volání – Kontaktování všech UE, které se nachází v dané eNB a okolí.
- Odposlech okolí – Umožnění odposlechu ostatních hovorů a v případě nouze potlačit jeden z nich k uvolnění kanálů.

Na stejném principu funguje i další podpůrná funkce a tím je MCVD (Mission-critical video and data), kde se ale jedná o přenos videa a dat, nikoliv hlasu. [17]

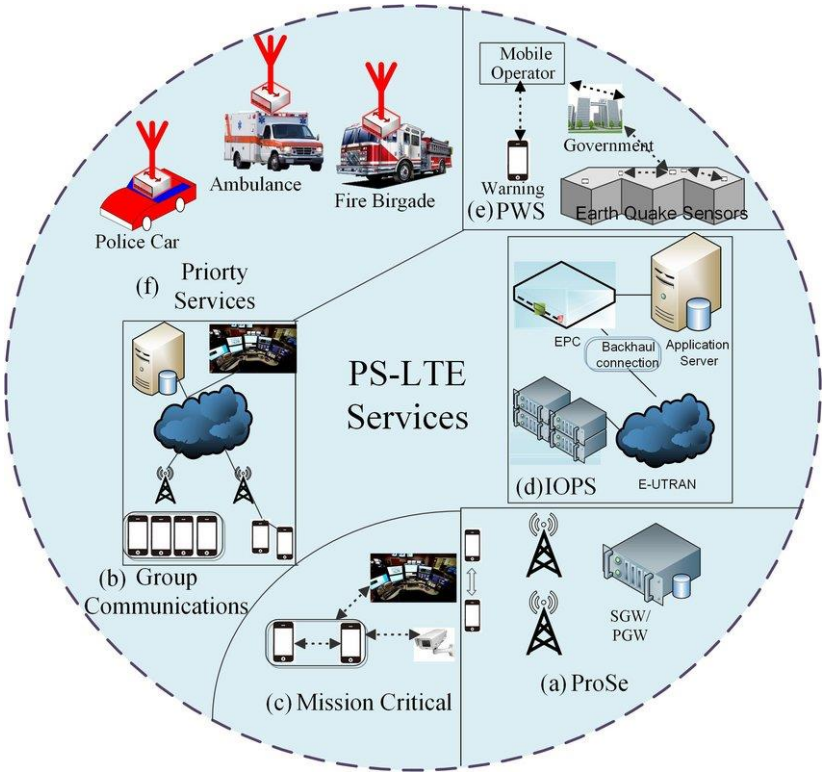
2.1.4.5 Public Warning System

Další z velice důležitých funkcí v rámci PS-LTE je PWS, které slouží pro varování před blíží se katastrofou. Příkladem může být senzor zaznamenávající zemětřesení, který když něco zaznamená, tak pošle varovný signál operačnímu středisku přes PWS, které přepošle zprávu jednak jednotkám k přípravě k výjezdu, a dále také mobilním operátorům, aby mohli včas varovat veřejnost v dané lokalitě. Nemusí se však jednak

pouze o zemětřesení, mohou to být další přírodní katastrofy typu tajfun, povodně či tsunami. Nejedná se tedy přímo o funkci nacházející se v UE. [17]

2.1.4.6 Priority service

Řízení priority je jednou z dalších důležitých funkcí implementovaných v PS-LTE. Jak název napovídá, tak se jedná o řízení jednotlivých účastníků podle priority v daný okamžik neboli při dané katastrofě jsou „obyčejní“ účastníci upozaďováni, zatím co příslušníci IZS mají větší prostor pro komunikaci a přenos informací, ať už hlasových či videa, v rámci kooperace. [17]



Obrázek 16: Podpůrné funkce PS-LTE, zdroj: [17]

2.2 Tetra

Většina státu neprošla vývojem a zůstala na stávajících systémech s cílem modernizace a vylepšení komunikační či datové sítě. Většina z nich funguje na standardu TETRA (Terrestrial Trunked System), který vznikl v roce 1989 pomocí institutu ETSI (European Telecommunication Standards Institute) za účelem vytvoření veřejně přístupné mobilní radiové sítě v celé Evropě a až později, v roce 1993, se za začal vývoj orientovat na bezpečnostní a záchranný systém. Vývoj se v pozdějších letech neorientoval pouze na Evropské státy, ale začal postupně přecházet i do okolních světadílů. Proto je možné se dnes setkat se sítí TETRA v Indii či v Kataru, popřípadě v Jižní Americe. [22]

Základní funkce standardu TETRA je obdobná standardu TETRAPOL, jelikož vychází z jeho základu a přidává k ní další podpůrné funkce ke zlepšení kvality přenosu dat a hovoru. Jedná se tedy o digitální radiovou síť založenou na trunkovém režimu (viz. 1.1.2). Oproti standardu TETRAPOL využívá pro přenos datového toku metodu TDMA, zatímco u TETRAPOLU se využívá metoda FDMA. [23]

- TDMA (Time Division Multiple Access) funguje na principu přenosu dat od více uživatelů na stejné frekvenci, kdy každý rámec je rozdělen do časových slotů, kde každý časový slot spadá pod jednoho uživatele.
- FDMA (Frequency Division Multiple Access) naopak funguje na principu přidělení jednoho či více frekvenčních pásem, na kterém daný uživatel komunikuje či posílá svá data.

Jak je možné si všimnout, tak FDMA má nevýhodu ve využívání více frekvenčních kanálů a tím více „zahltit“ ovzduší, proto se zdá, že TDMA je lepší volba. TDMA má ale vlastní nevýhodu a tím je maximální možná vzdálenost vysílací a přijímací stanice. U systému TETRA je tento dosah okolo 80 km. [23]

2.2.1 Architektura sítě

Architekturu sítě lze rozdělit do 5 částí. Těmi jsou:

- MS (Mobile Station) – Mobilní terminál využívaný uživatelem pro komunikaci.
- RBS (Radio Base Station) – Základnová radiostanice složena z vysílacích antén.
- SCN (Switching Controller Node) – Kontrolér sloužící pro řízení a koordinaci mezi RBS.
- NMS (Network Managment System) – Slouží pro zabezpečení řízení a dohled nad sítí.
- RLS (Remote Line Station) – Vzdálený přístup do sítě pro dispečera.

V některé literatuře lze najít označení částí jako TMS či TBS, kde písmeno T značí TETRA, tudíž se jedná pouze o jiný typ názvosloví. Dále je možné najít označení SwMI (Switching and Management Infrastructure), která označuje spojení více částí dohromady. Těmi jsou RBS, SCN a NMS.

2.2.1.1 Mobile Station

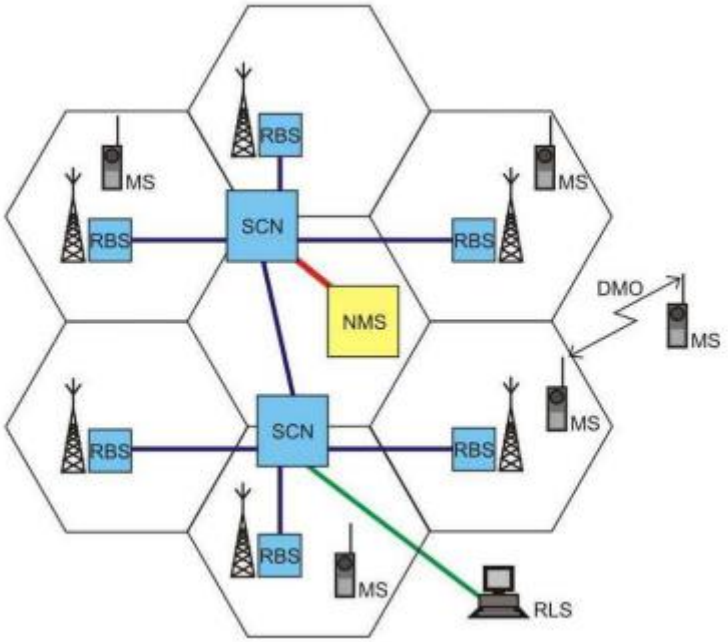
Terminály uživatelů mohou fungovat v několika modech. Jednotlivé mody jsou:

- TMO (Trunked Mode Operation) – Slouží pro klasickou komunikaci buď mezi jedním terminálem s druhým přes RBS či mezi jedním terminálem a více terminálů přes RBS.

- DMO (Direct Mode Operation) – Tento mod funguje na stejném principu jako přímý režim v systému PEGAS (viz. 1.4.2) neboli podporuje přímou komunikaci mezi dvěma terminály bez využití RBS.
- PDO (Packet Data Operaion) – Slouží pouze pro přenos datových informací.

V rámci terminálu lze využít přepínač nazývaný V+D (Voice + Data), který přepíná mezi přenosem pouze hlasového kanálu nebo datového kanálu, popřípadě umožňuje i přenos obou kanálů zároveň. [24]

Pod označením Mobile Station je možné si představit nejen uživatelské terminály, které jsou využívány v terénu, ale také vozidlové stanice, které mají vlastní využití. Slouží především pro rozšíření signálu, ať už signálu sítě či signálu DMO. To znamená, že pokud uživatel není v dosahu připojení do sítě, ale v dosahu sítě je vozidlová stanice, dopomůže danému terminálu se do něj připojit. [24]



Obrázek 17: Architektura standardu TETRA, zdroj: [22]

2.2.1.2 Radio Base Station

Hlavní částí základnové stanice jsou antény, které přijímají a odesílají packety mezi jednotlivé uživatele a tím je spojují. Jednotlivé RBS jsou mezi sebou propojeny přes SCN kvůli vzájemné komunikaci při předávání informací pro tzv. handover. Propojení mezi jednotlivými RBS může být v každém místě různě a řídí se podle nejefektivnější topologie v daném prostředí. Může se tedy stát, že na některých místech může být topologie kruhová, zatím co v některých částech musí být hvězdicová. Toto efektivní

využití topologií dopomáhá k snadnému předávání informací mezi RBS a také k zabezpečení chodu sítě v případě výpadku jedné či více RBS. SCN ne následně propojeno s dalším SCN v rámci předávání uživatelských informací opět pro handover v případě, že bude daný uživatel přecházet z jedné části SCN do další. Jak již bylo zmíněno v úvodu, tak nevýhodou v rámci TDMA je jeho krátký dosah, a to se projevuje na množství využití RBS v rámci komunikace. [24]

2.2.2 Zabezpečení sítě

Zabezpečení v standardu TETRA funguje ve 3 krocích:

- Autentizace uživatele
- Integrity Protection
- Šifrovaná komunikace

2.2.2.1 Autentizace uživatele

Obdobně jako v systému LTE či PEGAS, tak i zde má uživatel svůj unikátní identifikační klíč K, který zná pouze daný terminál a síťový NMS. Aby se uživatel mohl přihlásit do sítě a využívat všechny jeho funkce, přihlásí se nejdříve na nejbližší RBS s požadavkem o přihlášení. Ta je následně přeposlána do SCN a poté do NMS. Zde se vygeneruje kód, který lze rozšifrovat pouze uživatelským klíčem K a je poslán zpět do terminálu. Zde je rozšifrován kód a vytvořena odpověď s jiným kódem pomocí klíče K. Pokud ho dokáže NMS rozšifrovat, tak je navázána komunikace mezi uživatelem a sítí, popřípadě mezi dvěma uživateli. Tento způsob autentizace je možný pouze v případě zapnutí obou funkcí v V+D modu, jinak nelze tuto funkci využít. V rámci DMO modu se tedy využívá jiný šifrovaný klíč, označovaný jako SCKs (Static Cipher Keys), které mají jednotlivé terminály uložený ve svých databázích. [25]

Po autentizaci lze zapnout funkci integrity protection (viz. 2.1.3.1.5), která chrání uživatele před odposloucháváním venkovního vetřelce.

2.2.2.2 Šifrovaná komunikace

Při vzájemné komunikaci mezi uživateli je tzv. AI (Air Interface). Jedná se o vzdušný prostor, který je nejzranitelnější na odposlech. V rámci bezpečnosti se tedy využívá šifrovaná komunikace pře šifrovací algoritmy. V standardu TETRA se využívají 2 typy šifrování:

- Air Interface Encryption
- End-to-end Encryption

Air Interface Encryption

Slouží jako šifrovaná ochrana přenášených dat či hlasové komunikace mezi terminálem a RBS. Standard TETRA využívá v rámci šifrovaného ovzduší více druhů šifrovacích algoritmů, které jsou označovány jako TEA1, TEA2, TEA3 a TEA4 (Tetra Encryprion Algorithms). Jednotlivé druhy může daný uživatel přepínat a vybírat si tak vlastní šifrovací algoritmus. Číselné rozdělení, které se nachází za TEA, označuje sílu zabezpečení v rámci algoritmu neboli TEA1 je nejméně zabezpečená, zatímco TEA4 je nejvíce zabezpečená. Zajímavostí je, že TEA2 je šifrovací algoritmus, který se využívá pouze v rámci Evropské unie. Je tomu z důvodu následné rozšíření standardu TETRA mimo Evropsku unii, kde se začal vyvíjet algoritmus vhodný pro jejich systémy TEA3. [25]

End-to-end Encryption

Stejně jako v síti PEGAS, tak i zde je zabezpečena komunikace od uživateli k uživateli neboli je zabezpečený průchod dat v rámci odposlouchávání uvnitř sítě.

Autentizace, Integrity protection, AIE a E2EE jsou účinnými kroky v rámci zabezpečení komunikace od odposlouchávání a využití pachatelem. Poslední částí, která dopomáhá k zabezpečení komunikační sítě je TDMA. Jak bylo popsáno výše, tak TDMA funguje na principu přenášení více uživatelů na jedné frekvenci při rozdělený rámce do více časových slotů, tudíž i kdyby daný pachatel zachytil v ovzduší daný signál, musí se ještě nejdříve vypořádat se srovnáním jednotlivých časových slotů za sebou tak, aby následně mohl rozluštit šifrování buď přes AIE nebo E2EE.

3 Návrh optimalizace sítě v ČR

Tato kapitola se zabývá jednotlivými řešeními v rámci optimalizace sítě v České republice.

3.1 Přechod na LTE

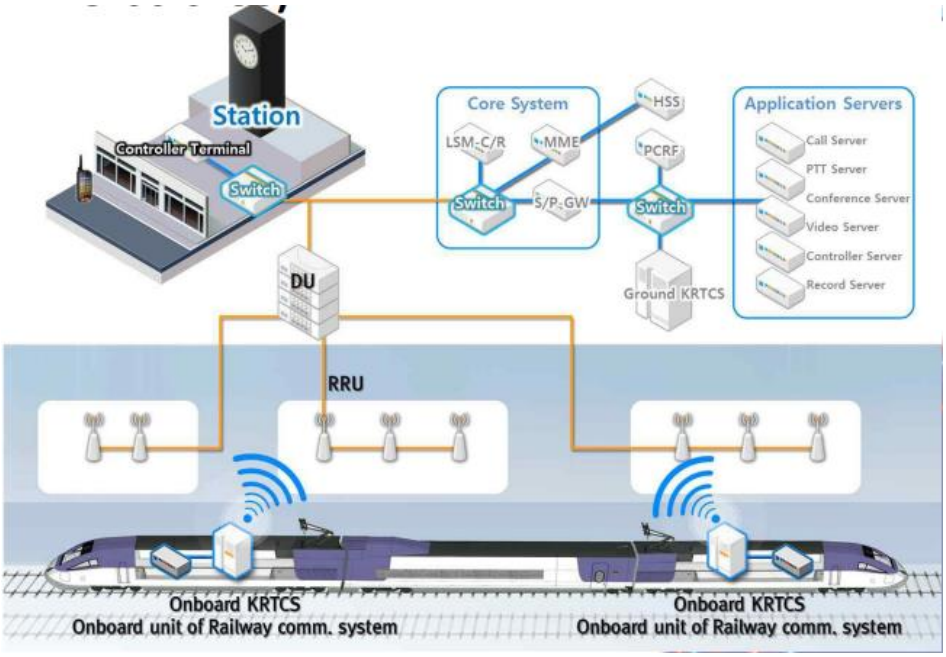
Prvním řešením je kompletní přechod stávající sítě PEGAS do nové, modernější sítě LTE. Toto řešení je sice ekonomicky náročnější, avšak se dá využít ve více směrech. Krásným příkladem je již zmiňovaná Jižní Korea, která začala v roce 2014 s výstavbou nové a výkonnější sítě SafeNet, založené na bázi LTE v pásmu 700MHz. Při realizaci základních prvků se konstruktéři rozhodli pro větší využití této sítě a začali expandovat do dalších oblastí. Nejednalo se tedy pouze o PS-LTE, ale začali rozvíjet i komunikaci a bezpečnost v rámci železniční dopravy, nazývané jako LTE-R, a dále také v rámci námořní dopravy, nazývané jako LTE-M. PS-LTE je popsáno v kapitole 2.1.4, tudíž ho není potřeba představovat nějak více. Ukážeme si tedy ostatní dva systémy: LTE-R a LTE-M.

LTE-R

Jak již bylo zmíněno, jedná se o pokrytí komunikace v rámci železniční dopravy. Celý proces je možné vidět na obr. 18. Ve vlaku se nachází jednotka, která neustále komunikuje s jednotlivými eNB a tím zasílá informace typu: Poloha vozidla, rychlost, zabezpečení a další a zároveň získává informace od řídícího centra ohledně problému na trati či volnosti trati. LTE-R využívá řazení priorit při odesílání dat, kdy TCD (Train Control Data) jsou jedny z nejdůležitějších, a tudíž mají větší priority před ostatními daty. To stejné platí i pro hlas, kdy má vlakové tísňové PTT tlačítko přednost před obyčejným hovorem účastníka. [18]

LTE-M

Tragická nehoda, která nastala 16. dubna 2004 při potopení trajektu Sewol nevedla pouze k zavedení lepší PS-LTE sítě, ale také k modernizaci sítě v rámci námořní dopravy. Na každé lodi se nachází LTE router, který komunikuje s LTE sítí o stavu lodi a zároveň o vzdálenosti mezi lodí a pobřežím. Právě vzdálenost je nejdůležitější v rámci komunikace v síti LTE, jelikož na ní úzce závisí i přenosová rychlost. Nejzajímavější oblastí pro korejské námořnictvo je 30 km od pobřeží, kde se nejvíce vyskytuje výletní loďstvo. Při této vzdálenosti je přenosová rychlost v průměru 6Mb/s. Limit stanovený korejskou vládou byl dosah do 100 km, kdy při této vzdálenosti je přenosová rychlost kolem 3Mb/s. [18]



Obrázek 18: Funkce LTE-R, zdroj: [18]

LTE-V

Avšak nejenom tyto dva podpůrné systémy lze využít v rámci dopravy. Dalším příkladem je V2X neboli komunikace mezi vozidlem a jinou částí systému. Tím pádem se může jednat o další vozidlo (V2V), okolní prostředí spojené s infrastrukturou neboli semafory, parkoviště a další (V2I), či komunikace s chodci (V2P). Celé toto je v LTE označované jako LTE-V. Tato funkce je velice užitečná v informovanosti daného řidiče o dění na silnici, popřípadě možnosti řízení dopravy přes jednotlivé světelně řízené křižovatky. [20]

3.1.1 Terminály LTE

Terminály v rámci LTE jsou označovány jako UE a fungují na obdobném způsobu autentizace a komunikace jako v síti PEGAS. Autentizace v rámci sítě LTE funguje na principu zjištění, zda uživatelovo IMSI je stejné, jako je nahrané v databázi, obdobně jako v síti PEGAS, kde se zjišťuje správné RFSI. To lze zjistit pomocí šifrované komunikace mezi MME a UE. Na rozdíl od sítě PEGAS je komunikace zabezpečena více šifrovacími a ověřovacími klíči, které musí uživatelovo UE rozšifrovat pro ověření identity. Po autentizaci probíhá zapnutí funkce identity protection, která chrání uživatele před odposlechem ostatních narušitelů. Ta funguje ve dvou fázích, kdy nejdříve se zapne kontrola mezi UE a MME a následně mezi UE a eNB (označení pro RBS v LTE). Komunikace probíhá přes páteřní síť LTE, která je na rozdíl od sítě PEGAS, více chráněna pomocí rozhraní S1 mezi eNB a MME a rozhraním X2 mezi jednotlivými eNB. Jak bylo popsáno výše, tak síť LTE je více zabezpečena oproti síti PEGAS, a to dopomáhá jednak k zajištění bezpečné komunikace bez odposlechu a zároveň ke kontrole správnosti dat a signalizačních zpráv pro chod celé sítě. Terminály disponují

řadou funkcí, které jsou obdobné v naší síti. Jednou z možností je přímý režim neboli komunikace dvou účastníků mezi sebou bez využití eNB. Tato komunikace je v síti LTE zašifrována a taktéž chráněna před odposlechem. Jednou z větších finanční zátěží v rámci přechodu na síť LTE by byla koupě nových terminálů pro jednotlivé uživatele, jelikož v naši síti se využívají terminály, které nepodporují funkci sítě LTE. Jak bude popsáno dále, tak nejlepším řešením je koupě hybridních terminálů, které dokážou využívat funkce sítě LTE, tak také komunikovat a fungovat na naši síti PEGAS.

3.1.2 RBS v LTE

RBS v LTE jsou označovány jako eNB a plní obdobnou funkci jako RBS v síti PEGAS. Jednak komunikují s hlavním řízením EPC a řídí chod komunikace mezi UE a MME, ale také se starají o komunikaci mezi sebou a UE. Na rozdíl od sítě PEGAS komunikují jednotlivý eNB mezi sebou přes chráněné rozhraní X2, kde si navzájem předávají informace o jednotlivých uživatelích v rámci backhaulu. Jelikož je Česká republika z velké části pokryta sítí LTE, tak by v rámci přechodu nebyla potřeba výstavba nových eNB. V lokalitách, kde se nenachází síť LTE, je možnost buď vytvoření nové eNB pro tuto část, anebo v případě zásahu využití přenosného eNB, podobně jako v naší síti, kde se využívá IDR. Co se týká menších lokalit jako například pokrytí metra, tak zde se dá využít menších eNB označených jako HeNB, což v síti PEGAS nelze.

Přechod mezi sítí PEGAS a LTE není radno uspěchat, jako tomu bylo například u britského ESN, kdy předpokládali nasazení LTE systému všem pracovníkům ve složkách IZS a následného okamžitého vypnutí jejich staré TETRA sítě. Spousta nevýhod se v tu doby objevila. Nejhlavnější z nich byla nepřipravenost jednotlivých složek a tím i tzv. krok do neznáma. Nevyškolení pracovníci následně měli problém s funkčností jednotlivých funkcí a tím docházelo k větším problémům v rámci koordinace. Další z nich byla nemožnost záložní komunikace v případě nefunkčnosti LTE sítě. Nakonec britská vláda zavedla opětovné zapnutí TETRA sítě a prodloužení její funkčnost až do roku 2022, což je dostatek času pro zaškolení jednotlivých členů IZS. [19]

Jak bylo ukázáno v úvodu druhé kapitoly, tak většina státu se začala rozvíjet v rámci bezpečnostních komunikací směrem k síti LTE. Česká republika je v dnešní době pokryta víc jak 98 % sítí LTE, a tudíž je možný pomalý přechod na tento typ sítě. V roce 2020 končila v ČR podpora pro síť PEGAS a řešil se možný vývoj tohoto systému. Firmy O2 a Nordic Telecom nabídnuli, že vytvoří na zakázku novou PS-LTE síť, na které by záchranné složky mohli komunikovat, avšak tento návrh bych ministerstvem vnitra zahozen a místo toho se přešlo na tzv. „modernizaci“ sítě PEGAS do roku 2027.

3.2 Přechod na DMR Tier III

Další možný přechod, který je ekonomičtější na rozdíl od sítě LTE, je přechod na standard DMR (Digital mobile radio). Ten lze rozdělit do tří kategorií:

- Tier I – Jedná se o bezlicenční kategorii, kterou mohou využívat radioamatéři či obyčejní lidé. Využívají radiostanice nazývané dPMR (Digital Personal Mobile Radio), které mají omezení jak v rozsahu, síle kanálu a výkonu, tak dále v zabezpečení, jelikož nedisponují žádným šifrovacím algoritmem [20]
- Tier II – Licencovaná konvenční síť určena pro služební a pracovní účely. Jednotlivé terminály jsou již šifrovány a komunikují přes konvenční rádiovou síť (viz. kapitola 1.1.1).
- Tier III – Vylepšená verze Tier II, která přidává možnost využití trunkové rádiové sítě.

Nejlepší možný přechod je na nejnovější kategorii Tier III, jelikož poskytuje obdobné funkce jako standard TETRAPOL, a tudíž by nebyl velký zásah do infrastruktury sítě. V rámci uskromnění textu nazveme DMR Tier III pouze DMR. Ten poskytuje trunkovou rádiovou síť (viz. kapitola 1.1.2), podobně jako síť PEGAS, která dopomáhá k dynamickému přidělování účastníků na volný hovorový kanál. Dále poskytuje možnost přenosu informačních dat, avšak na rozdíl od sítě PEGAS umožňuje přenos dat přes nezávislý datový kanály, nikoliv přes další, komunikační kanál, který by zabíral místo pro další účastníky. [21]

3.2.1 Terminály DMR

Terminály sítě DMR obsahují vylepšené funkce klasických terminálů sítě PEGAS. Při přihlášení probíhá opět autentizace terminálu pomocí RFSI čísla, který je unikátní pro všechny DMR terminály. Jelikož radiostanice podporují využití zkrácenější verze RFSI čísla, tak se může zredukovat počet vysílacích dat a tím zrychlit autentizaci. Příkladem může být úprava ze stávajícího 101-5-91-001 RFSI čísla na 1591001. Po autentizaci nastává bezpečnostní část. DMR síť podporuje více šifrovacích klíčů, které lze libovolně měnit či využít pro jednotlivý komunikační hovory či datový přenosy. Tím pádem má každý uživatel DMR terminálu možnost si zvolit libovolný šifrovací klíč, který je vytvořen přes 256bitové šifrování, a tím zabezpečit odposlechu hovorů či přenášených dat. 256bitové šifrování je jednou z nejbezpečnějších šifrovacích algoritmů, které se využívají u radiokomunikací, jelikož musí narušitel prohledat 2^{256} různých kombinací, aby uhodnul šifrovací klíč. Než se mu to nakonec podaří, tak si stejně buď samotný terminál či uživatel změní šifrovací klíč. Po autentizaci se terminál přihlásí do sítě a je požádán o sdílení své

GPS lokality. Pomocí toho, ale také pomocí RSSI (Received Signal Strength Indication), můžou jednotlivé RBS mezi sebou komunikovat a zjišťovat, zda není uživatel v příliš velké vzdálenosti od RBS a zda není potřeba k přepnutí na jinou RBS. Jinak řečeno se jedná o backhaul funkci, kterou síť PEGAS neumožňuje. Dále terminál kontroluje, zda stále komunikuje s RBS a nedošlo k výpadku sítě. V takovém případě mají terminály zabudovaný hlasový identifikátor, který upozorní uživatele o odpojení ze sítě. Terminály dále umožňují funkci přímého režimu neboli komunikace dvou terminálů mezi sebou bez využití RBS. Toho je zde umožněno pomocí DCDM (Dual Capacity Direct Mode) systému, který poskytuje možnost komunikace dvou terminálů mezi sebou na jedné frekvenci a navzájem se nerušili. [21]

3.2.2 RBS v DMR

Využití RBS by zůstalo stejné jako v síti PEGAS, poněvadž síť DMR je připravená pro stejné kmitočtové pásmo jako využívá naše síť. Nemuselo by se ani rozšiřovat o další RBS, jelikož DMR síť je stavěná na větší vzdálenosti než síť PEGAS. Jediné, co by se muselo změnit v rámci RBS, jsou zastaralé prvky jako propojovací kabely, vysílací antény a další. Co se týká identifikace jednotlivých RBS, tak i zde lze dojít k redukci RSN čísla, jako tomu je u RFSI, a tudíž lze zredukovat staré 101-01-01 RN číslo na 1-11. Tato redukce nijak nezasáhne do chovu sítě, jelikož uživatel tuto identifikaci nijak nevyužívá a pouze se přepíšou data v řídící části. Co se týká nezávislých RBS neboli IDR, tak i zde DMR nabízí možnost využití této funkce ve vylepšené formě. Využívá se zde nových nezávislých šifrovacích klíčů, které nezasahují do chodu sítě a zabezpečují šifrovanou komunikaci mezi uživateli v prostorách, kam RBS „nedosáhne“. Navíc umožňuje filtrování jednotlivých terminálů a v případě nouze i omezení provozu, což IDR neumožňuje. [21]

4 Analýza vhodnosti navrhovaných systémů

V rámci zlepšení kvality a bezpečnosti v rámci komunikace u složek IZS v ČR, je potřeba si nejdříve zhodnotit všechny výhody a nevýhody navrhovaných systémů. Toto zhodnocení je provedeno pomocí SWOT analýzy. SWOT analýza popisuje silné (Strengths) a slabé (Weaknesses) stránky a dále příležitost (Opportunities) a hrozby (Threats), které jsou spojené s daným systémem.

4.1 Analýza sítě PEGAS

Před zhodnocením jednotlivých systémů je zapotřebí zjistit stav aktuálního systému používaný v ČR k následnému porovnávání.

Silné stránky

- Největší silnou stránkou stávající sítě je fakt, že se u nás již nachází neboli není potřeba výstavba nových RBS či jiných zařízení, které by akorát stály peníze. Dále díky tomu není potřeba školení uživatelů, jelikož již tento systém znají a ví, jak s ním pracovat.
- Díky staršímu standardu lze najít na trhu spousty produktů, které jsou mezi sebou kompatibilní a lze s nimi pracovat.

Slabé stránky

- Mezi slabé stránky sítě PEGAS patří zastaralý standard TETRAPOL. Ten se sice postupem času vyvíjí a vytváří se různé modifikace a nové doporučení, ale pořád vše stojí na zastaralém základu.
- Modifikace přináší i další slabou stránku a tou je ekonomická náročnost, jelikož modifikováním jednotlivých částí stojí především čas a hlavně peníze, které lze využít místo vkládám do modifikací k transferování do jiného standardu.
- Menší kapacita sítě v daných lokalitách, která se zahltí při větších zásazích.

Příležitosti

- Jednou z příležitostí, kterou i nyní vláda provádí, je již zmíněná modifikace.
- Možnost kooperace s ostatními systémy jako LTE či TETRA.

Hrozby

- Největší hrozbou, kterou síť PEGAS má, je výpadek celkové komunikace při zásahu. V rámci ČR se toto stalo při řádění tornáda na jižní Moravě, kdy v jednu

chvíli kompletně vypadla rádiová komunikace a zásahové jednotky neměli příležitost mezi sebou kooperovat.

4.2 Analýza LTE

Silné stránky

- Česká republika je pokryta sítí LTE z 98 % a hojně je využívaná v rámci mobilní komunikace.
- Již vytvořena podpůrná modifikace PS-LTE pro záchranné a bezpečnostní složky
- Zabezpečení komunikace přes autentizaci pomocí unikátního IMSI klíče.
- Integrity protection proti odposlouchávání z venku.
- Šifrovaná komunikace mezi jednotlivými uživateli a zároveň mezi uživatelem a sítí.
- Vysoké přenosové rychlosti pro datovou komunikaci, tudíž lze využít streamovacích služeb pro přenos videa a zvuku.
- Lepší pokrytí v oblastech, kde se síť PEGAS nedostane, jako například hory či hustě rozvrstvená oblast
- Nabízí možnost využití backhaulu, kterou síť PEGAS nemá.

Slabé stránky

- Hlavní slabou stránkou při přechodu na síť LTE je cenová náročnost, především při koupi nových UE terminálů pro všechny uživatele.
- V rámci přechodu by muselo dojít k zaškolení všech uživatelů, aby dokázali v kritických situacích fungovat a neprobíhala panika v rámci neznalosti. To stejný platí v rámci zaškolení jednotlivých uživatelů v rámci operačních center.
- Nutnost koupě hybridních terminálů pro možnou kooperaci se stávající sítí což značí další finanční zátěž.
- Větší energetická náročnost, která v dnešní době není vyhovující

Příležitosti

- Největší příležitost je možná kooperace mezi sítěmi LTE a PEGAS pro situace, kdy síť LTE buď přestane fungovat, nebo pro vzájemnou komunikaci v případě, když některé jednotky ještě nebudou disponovat terminály pro síť LTE.
- Přechod na síť LTE pomůže k následným krokům na přechod na síť 5G, popřípadě budoucí 6G.

- Možnost využití pro jiné účely než pro radiovou komunikaci. Jak je zmíněno v kapitole 3.1, tak lze využít síť LTE i v rámci bezpečnosti komunikace a řízení v dopravě.
- Modernizace podpůrných funkcí o další funkce jako například monitoring vozidel a další.

Hrozby

- Nejedná se o nový systém, tudíž je možnost, že i síť LTE je v dnešní době z venku napadnutelná. Tato hrozba je ale pokryta pomocí autentizace a šifrování.
- Jelikož se bude jednat o společný vysílač, který využívají i běžní uživatelé, muselo by se začít s vysokou škálou priorit v případě většího zásahu a popřípadě úplně „odříznout“ běžného uživatele využívání této služby.

4.3 Analýza DMR Tier III

Silné stránky

- Využívá obdobné funkce a má stejnou architekturu jako síť PEGAS, tudíž při přechodu by nedošlo k tak finanční zátěži, jelikož i RBS by zůstaly stejné.
- Větší dosah radiového pokrytí než síť PEGAS.
- Využívá 256bitové šifrování, které je jedno z nejbezpečnějších šifrovacích algoritmů.
- Nabízí možnost využití backhaulu, kterou síť PEGAS nemá.
- Oproti sítě PEGAS zvýší standard DMR celkovou kapacitu sítě i při zachování stávajících radiových podmínek.
- Celková síť a ani terminály nejsou vázány pouze na jednoho výrobce, ale je možnost využití jakéhokoliv produktu, který podporuje standard DMR.
- GPS sledování polohy daného terminálu.

Slabé stránky

- Omezené možnosti v rámci zabezpečení vstupu u jednotlivých terminálů
- Autentizace stále přes RFSI číslo, které je sice unikátní pro každého uživatele, ale dá se snadněji zjistit než například IMSI klíč.

Příležitosti

- Kompatibilita mezi DMR sítí a dalšími sítěmi jako LTE či standardu TETRA

- Jelikož dokáže standard DMR pokrýt větší oblast než síť PEGAS, je možné v pozdější fázi přechodu některé RBS vypnout, nechat je v záloze a tím snížit energetickou náročnost

Hrozby

- Možnost využití stávajících šifrovacích algoritmů zvyšuje šanci napadnutí z venku
- Nutnost rozšíření funkcí pro záchranné složky, DMR používá stejné funkce jako síť PEGAS, které jsou v dnešní době sice dostačující, avšak v budoucnosti bude potřeba rozšíření těchto funkcí.
- V dnešní době se hojně využívají streamovací služby, které jsou přeposílány buď veliteli zásahu nebo na operační a řídící centrum. Aby video „došlo“ v rozumné kvalitě, musí být splněny požadavky na zrychlení přenosové rychlosti.

5 Návrh doporučení vývoje radiové sítě v ČR

Tato kapitola se zabývá mým osobním návrhem, jakým by se ministerstvo vnitra v rámci České republiky mělo vydat.

Síť PEGAS funguje na zastaralém standardu TETRAPOL, který se sice snaží stále vylepšovat, ale nedokáže přinést dostatečné výhody k jejímu dalšímu použití. Každá větší událost akorát ukazuje na fakt, že síť přestává fungovat a postupně se rozpadá. Krásným a již zmíněným příkladem je asi největší událost v rámci záchranných složek, a to tornádo na jižní Moravě, které zapříčinilo zahlcení kapacity sítě do maxima a tím omezení komunikace mezi jednotlivými složky. Proto se stávaly případy, kdy velitel zásahové jednotky chtěl zavolat na operační a řídící centrum do Brna, avšak se dovolal do Kladna, jelikož ho tam síť sama navedla přes volnou trasu. Přímý či převaděčový režim zde sice fungoval, avšak s tím odchází spousty podpůrných funkcí, které síť nabízí. A nejedná se pouze o tento příklad, ten ukazuje pouze na fakt, že i v roce 2021 mohou nastat takovéto situace. Dalším příkladem byly například povodně v roce 2006, které také způsobily rozsáhlý výpadek radiové komunikace.

V rámci mého osobního názoru existují 2 různé směry, kterým by se mohla Česká republika vést. Jedním z nich je přechod na síť LTE a společně s tím nechat síť PEGAS jako záložní systém v případě výpadku sítě LTE. Sice se jedná o energeticky a finančně náročnější krok, avšak využití sítě LTE by nebylo pouze pro záchranné a bezpečnostní složky, ale dá se využít i více odvětví, jak také zmiňuji v kapitole 3.1. Ideální řešení v rámci přechodu na nový systém LTE je postupným zaškolením všech členů sborů IZS a následného zapnutí podpůrných funkcí v rámci PS-LTE. Nejdůležitější části je již zmíněná možnost kooperace se stávající sítí PEGAS. Může se stát, že například sbory Hasičských záchranných složek již budou vlastnit UE terminály v rámci sítě LTE, avšak Policie ČR může stále mít starší digitální vysílačky využívané v síti PEGAS. Proto je vhodné tuto kooperaci nevynechat a pracovat s ní i nadále. Co se týká zabezpečení komunikace, aby nedocházelo k výpadkům spojení, tak Česká republika je hustě osídlena eNB a, jak již bylo zmíněno, tak 98% celé naší republiky je pokryto sítí LTE, tudíž procentuální šance k výpadku je zde nižší. Velkým plusem je funkce backhaul, kterou síť PEGAS neumí. Častokrát nejsou zásahy jednotek pouze na jednom místě, ale může se jednat o rozsáhlé místo jako například při pátrání ztracené osoby, a v takovém případě je backhaul užitečným nástrojem, jak efektivně přecházet mezi jednotlivými eNB bez výpadku spojení. Ostatní podpůrné funkce, které PS-LTE nabízí jsou více jak dostačující a postupně s každým vycházejícím Releasem přichází nové modifikace

některých funkcí, či kompletně nové podpůrné funkce. V rámci bezpečnosti hovoru, tak síť LTE disponuje komplexnějším způsobem autentizace, integrity protection a šifrování, než je v síti PEGAS, a tudíž útočník nemá tak velkou příležitost odposlechu. Posledním a jedním z hlavních důvodů v rámci přechodu na tuto síť je možnost otevření bran budoucím standardům typu 5G a později i 6G. V dnešní době již některé země testují funkčnost 5G v rámci záchranných a bezpečnostních složek a testují kooperaci mezi LTE a 5G. Z mého osobního pohledu je přechod na síť LTE krokem kupředu, a i přes to, že by se jednalo o časově a finančně náročný přechod, protože zaškolení jednotlivých uživatelů a koupě nových hybridních terminálů stojí čas i peníze, tak věřím, že to jsou lépe vynaložené peníze než v pokračování modernizace stávající sítě.

Druhým možným směrem je kompletní přechod na DMR Tier III. Tato varianta je ekonomičtější z důvodu podobnosti obou systémů, jak je popsáno výše v kapitole 3.2. Jelikož je zde veliká podobnost, tak přechod na tento standard by netrval tolik času a prakticky by se nezměnilo u běžného uživatele nic. Jediné, co by se muselo změnit, tak jsou terminály, které mají podporu pro DMR standard a jelikož vypadají a fungují stejně, jako terminály pro síť PEGAS, tak ani školení by nebylo potřeba. V rámci zabezpečení komunikace před výpadky je hlavním plusem rozšíření radiového pokrytí oproti síti PEGAS, čímž je možnost pokrýt oblasti, které dříve nebylo možné kvalitně pokrýt. Dále díky zvětšení pokrytí je možnost v hustě osídlených oblastí, jako například města, některé RBS vypnout a tím ušetřit na energetické zátěži. Dalším kladným bodem je zvýšení celkové kapacity i přes to, že se teoreticky jedná o stejnou síť. Ze všech zmíněných kladných bodů zní, že se jedná o ideální náhradu za náš stávající systém a je to pravda, avšak dle mého osobního uvážení by se nejednalo o krok kupředu, nýbrž o krok na stejné úrovni. DMR standard je vhodným kandidátem v rámci změny radiové sítě v České republice, avšak nejedná se o žádný velký krok, díky kterému by se mohla Česká republika v budoucnosti vyvíjet a vylepšovat. Dle mého osobního názoru by se po přechodu na standard DMR po pár letech stejně řešila problematika sítě a přechod na síť LTE či 5G, proto tento druhý směr beru jako ekonomicky levnější záležitost a poukázání na to, že taková varianta existuje, ale neberu ji jako jednu z hlavních a lepších kroků v rozvoji České republiky.

Závěr

V bakalářské práci byla řešena problematika stávající radiové sítě zvané PEGAS, která se využívá pro záchranné a bezpečnostní složky IZS. Nejdříve byl rozebrán aktuální stav sítě PEGAS a poté byly poukázány dva systémy, které se využívají v dnešní době v cizině. Jednou z nich je síť LTE, na kterou většina států momentálně přechází, a druhou je standard TETRA, který funguje na obdobném principu jako sít PEGAS. Následně se bakalářská práce zabývá návrhem systémů, které by mohly nahradit stávající síť. Jednou z navrhovaných systémů je již zmíněná síť LTE a druhým je standard DMR, přesněji DMR Tier III. Jednotlivé návrhy jsou zde řešeny v rámci funkčnosti a zabezpečení komunikace. Následně je řešena analýza vhodnosti jednotlivých navrhovaných systému včetně jednotlivých rizik. Analýza je řešena pomocí SWOT analýzy, která ukazuje silné a slabé stránky, příležitosti a hrozby navrhovaných systémů. Poslední část se zabývá osobním doporučením, jakým směrem by se měl stát vydat. Doporučení je zde rozdělení do dvou směrů, kde jeden směr je přes síť LTE, a tudíž se jedná o ekonomicky náročnější směr, zatím co druhý je přes standard DMR neboli přes finančně levnější směr.

Radiové komunikace u záchranných a bezpečnostních složek se postupem času neustále vyvíjí a vylepšuje. Zároveň ochrana obyvatelstva je jedním z nejdůležitějších bodů u záchranných složek a bez vzájemné koordinace a komunikace je tento bod těžce splnitelný, a proto je důležité se tímto tématem pečlivě zabývat.

Zdroje

[1] Digitální trunkový radiový systém Hytera DMR Tier III v Brně. Digitální radiostanice vysílačky Hytera DMR a TETRA - [online]. Copyright © 2020 DCom, spol. s r.o., Kšírova 32, 61900 Brno [cit. 16.06.2022]. Dostupné z: https://www.hyt.cz/digitalni-trunkovy-radiovy-system-hytera/

[2] Vysoká škola báňská – Technická univerzita Ostrava. Fakulta bezpečnostního inženýrství DIPLOMOVÁ PRÁCE – PDF Free Download. Documents Professional Platform – PDF Download Free - ADOC.PUB [online]. Copyright © 2022 ADOC.PUB. All rights reserved. [cit. 17.06.2022]. Dostupné z: https://adoc.pub/vysoka-kola-baska-technicka-univerzita-ostrava-fakulta-bezpe.html

[3] DOUŠA, Jan. *Radiokomunikační síť integrovaného záchranného systému Pegas a její technické a kryptografické zabezpečení*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2016, 54 s. Dostupné také z: http://hdl.handle.net/10563/38879. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství, [cit. 17.06.2022]

[4] Síť PEGAS II. – generace 2 a půl – KMITOCTY.cz. KMITOCTY.cz – Original OK1ZOO´s radiomonitoring website [online]. Copyright ©2007 [cit. 18.06.2022]. Dostupné z: https://kmitocty.cz/?p=253

[5] Řád rádiových komunikací – Hasičský záchranný sbor České republiky. Úvodní strana – Hasičský záchranný sbor České republiky [online]. Copyright © 2022 Generální ředitelství Hasičského záchranného sboru ČR, všechna práva vyhrazena [cit. 18.06.2022]. Dostupné z: https://www.hzscr.cz/clanek/rad-radiovych-komunikaci.aspx

[6] Síť PEGAS III. – provoz – KMITOCTY.cz. KMITOCTY.cz – Original OK1ZOO´s radiomonitoring website [online]. Copyright ©2007 [cit. 19.06.2022]. Dostupné z: https://kmitocty.cz/?p=280

[7] SALUS | Security and interoperability in next generation PPDR communication infrastructures [online]. Copyright © [cit. 19.06.2022]. Dostupné z: https://www.sec-salus.eu/wp-content/uploads/2014/05/SALUS_D5.1_v1.01.pdf

[8] Pro odborníky – Ministerstvo vnitra České republiky. Úvodní strana – Ministerstvo vnitra České republiky [online]. Copyright © 2022 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 19.06.2022]. Dostupné z: https://www.mvcr.cz/clanek/pro-odborniky.aspx

[9] Školní a výcvikové zařízení HZS ČR – Nezávislý digitální opakovač – IDR – Hasičský záchranný sbor České republiky. Úvodní strana – Hasičský záchranný sbor České republiky [online]. Copyright © 2022 Školní a výcvikové zařízení HZS ČR [cit. 19.06.2022]. Dostupné z: https://www.hzscr.cz/clanek/nezavisly-digitalni-opakovac-idr.aspx

[10] Záchranáři na LTE aneb Jak vypadá budoucnost PPDR systémů - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1997 [cit. 21.06.2022]. Dostupné z: https://www.lupa.cz/clanky/zachranari-na-lte-aneb-jak-vypada-budoucnost-ppdr-systemu/

[11] Beyond PS-LTE: Security Model Design Framework for PPDR Operational Environment. Publishing Open Access research journals & papers | Hindawi [online], [cit. 21.06.2022] Dostupné z: https://www.hindawi.com/journals/scn/2020/8869418/

[12] COX, Christopher. *An introduction to LTE* [online]. 2. John Wiley, 2014 [cit. 23.06.2022]. ISBN 978-1-118-81803-9

[13] Dr. Ram Dantu, *The LTE network architecture* [online]. 2009 [cit. 23.06.2022]. Dostupné z: http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf

[14] LTE Quick Guide. [online]. Copyright © Copyright 2022. All Rights Reserved. [cit. 24.06.2022]. Dostupné z: https://www.tutorialspoint.com/lte/lte_quick_guide.htm

[15] SAUTER, Martin. *From GSM to LTE* [online]. 1. John Wiley, 2011 [cit. 24.06.2022]. ISBN 978-0-470-66711-8.

[16] Tunnel Mode. In: hypr.com [online]. [cit. 24.06.2022]. Dostupné z: https://www.hypr.com/tunnel-mode/

[17] Kaleem, Zeeshan & Yousaf, Muhammad & Ahmad, Ayaz & Qamar, Aamir & Doung, Trung & Choi, Wan & Jamalipour, Abbas. (2019). UAV-Empowered Disaster-Resilient Edge Architecture for Delay-Sensitive Communication [online]. 2019 [cit. 26.06.2022], Dostupné z: https://www.researchgate.net/publication/327722095_UAV-Empowered_Disaster-Resilient_Edge_Architecture_for_Delay-Sensitive_Communication

[18] HONG, Young Sam & KIM, Dong Chan, Korea Public Safety Mobile Broadband Project Update [online], 2019 [cit. 26.06.2022], Dostupné z: https://critical-communications-world.com/media/16410/young-sam-hong-dong-chan-kim-korea-public-safety-mobile-brodband-project-update.pdf

[19] Tomáš Karabinoš (Nordic Telecom): BB-PPDR v 700 MHz prodraží náklady až pětinásobně - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1997 [cit. 28.06.2022]. Dostupné z: https://www.lupa.cz/clanky/tomas-karabinos-nordic-telecom-bb-ppdr-v-700-mhz-prodrazi-naklady-az-petinasobne/

[20] Vojáček, Antonín. V2X komunikace – jen inovace nebo revoluce? [online], 2021 [cit. 28.06.2022], Dostupné z: https://automatizace.hw.cz/v2x-komunikace-jen-inovace-nebo-revoluce.html

[21] DMR typu TIER III – skutečná alternativa k síti MATRA-PEGAS – KMITOCTY.cz. KMITOCTY.cz – Original OK1ZOO´s radiomonitoring website [online]. Copyright ©2007 [cit. 28.06.2022]. Dostupné z: https://kmitocty.cz/?p=4544

[22] HÁNA, Ivo. Digitální radiokomunikační systémy Tetrapol a Tetra [online]. Ostrava, 2009 [cit. 15.07.2022]. Dostupné z: http://hdl.handle.net/10084/73592. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava.

[23] Digitální trunkové sítě standardu DMR – KMITOCTY.cz. KMITOCTY.cz – Original OK1ZOO´s radiomonitoring website [online]. Copyright ©2007 [cit. 18.07.2022]. Dostupné z: https://kmitocty.cz/?p=1319

[24] PROKOP, Tomáš. Webový portál pro krizové řízení využívající standard TETRA [online]. Brno, 2011 [cit. 18.07.2022]. Dostupné z: https://is.muni.cz/th/wioje/. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Jiří HŘEBÍČEK.

[25] Handbook on TETRA Technology & its Applications on Indian Railways, Government of India, Ministry of Railways [online], 2021 [cit. 20.07.2022], Dostupné z: https://rdso.indianrailways.gov.in/uploads/Handbook%20on%20TETRA%20Technology%20%26%20its%20Applications%20in%20IR_August%202021.pdf

Seznam obrázků

Seznam tabulek