WIRELESS NETWORK ANALYZER - PRACTICAL APPLICATION

Tomáš Ocelík
Bachelor Degree Programme (1), FIT BUT
E-mail: xoceli00@stud.fit.vutbr.cz

Supervised by: Peter Jurnečka
E-mail: ijurnecka@fit.vutbr.cz

ABSTRACT

This document deal with an overview of software traffic analyzer of wireless networks based on existing technology. Theoretically describes its main parts and its purpose. Function of each part is ilustrated for prototype solution which was realized for MPT 1327 network.

1. ÚVOD

Bezdrátové sítě jsou v dnešní době nedílnou součástí informačních a komunikačních technologií. Našly obrovské využití zejména s rozvojem internetu (Wi-Fi), mobilních telefonních sítí (GSM), nebo komunikačních sítí sloužících specifické skupině lidí nebo organizaci, například policie.

Tento dokument popisuje software sloužící k analýze datových toků v bezdrátových sítích. Jedná se o komplexní softwarový systém, který se dá snadno nakonfigurovat na analyzování bezdrátových sítí pracujících na různých síťových technologiích. Jako prototypové řešení jsme vybrali analyzování bezdrátové trunkové sítě MPT 1327[3], kterou používá Dopravní podnik Města Brna.

2. ROZBOR

Systém vychází z diplomové práce Petra Jurnečky, Analyzátor protokolů řízený pravidly. Pomocí navrhnutého vstupního modulu umožňuje použít vyvinutý analyzátor v praxi ve spojení se školním spektrálním analyzátorem Rohde Schwarz FSQ8. Tím uvádí konkrétní příklad použití výsledku diplomové práce.

Celý systém je složen z několika komponent, které vzájemně spolupracují. Systém je navržen tak, aby jeho jednotlivé komponenty dokázaly pracovat autonomně. Zjednodušené schéma celého systému je zobrazeno níže na obrázku.

Jednotlivé softwarové komponenty jsou řešeny pomocí zásuvných modulů. Tím je umožněna jejich snadná výměna a rozšíření spektra analyzovatelných signálů, modulací a protokolů.

Následuje popis jednotlivých komponent:

1) **Signálový analyzátor Rohde&Schwarz FSQ8** – Pomocí tohoto analyzátoru je prováděno zachytávání a vzorkování rádiového signálu. Analyzátor obsahuje uživatelské rozhraní, přes které je možné nastavit všechny parametry analýzy. Zachycený signál lze uložit do textového souboru ve formě použitelné například v programu Matlab. Dále obsahuje ethernetové rozhraní, díky čemuž je možné analyzátor ovládat i vzdáleně přes počítačovou síť pomocí speciálního API[4]. Přenos zachycených dat je pak možné realizovat přímo po síti. Zachycený signál je reprezentován pomocí bodů, představujících fázové (in-phase) a kvadraturní (quadrature) složky signálu.

2) **Filtr** – Před samotnou demodulaci je možné předřadit filtr, který se bude aplikovat na vstupní I/Q data a bude například redukovat šum způsobený rušením. V našem prototypovém řešení používáme základní filtr, který pouze převádí vstup na výstup.

3) **Demodulátor** – Tato část zpracovává obdržená I/Q data a provádí jejich demodulaci[2]. V případě našeho prototypového řešení I/Q data představují signál vzniklý FSK modulací a bitové rychlosti 1200b/s[3]. Výstupem tohoto modulu je diskrétní signál tvořený dvěma hodnotami, představující demodulovaný digitální signál.

4) **Definice paketu** – Softwarový analyzátor potřebuje pro začátek analýzy znát jednotlivé datové rámce nejnižší vrstvy. Na tyto rámce pak aplikuje pravidla definovaná v XML zmíněném výše. Tato vrstva přijímá diskrétní dvouhodnotový signál z demodulátoru a hledá v něm počátek datového rámce a bitovou synchronizaci. V našem prototypovém řešení provádíme analýzu technologie MPT 1327. Ta definuje jako začátek datového rámce posloupnost střídajících se jedniček a nul, přičemž jich musí být alespoň šestnáct. Odsud je možné odvodit bitovou synchronizaci. Protože má datový rámec pevnou délku, je možné jej z datového toku snadno extrahovat.

5) **Analyzátor** – Je jádro celého systému, které obsahuje uživatelské rozhraní, přes které může uživatel nastavovat parametry analýzy a prohlížet výsledky. Tato část dále provádí vlastní analýzu získaných dat. Analýza je prováděna na základě XML souboru s popisem protokolů. XML definuje jednotlivé zprávy, pole v nich a jejich souvislosti. XML lze editovat přímo v prostředí programu.

6) **Rozhraní mezi analyzátorem a software** – na obrázku označeno číslicí 6. Úkolem této části je vytvářet softwarové rozhraní mezi softwarem a signálovým analyzátorem. Využívá se výše zmíněného API, které je dostupné pro běžné programovací jazyky platformy MS Windows. Zde je využita technologie C#.NET a plugin je uložen ve formě dynamické knihovny. Plugin umožňuje načítat zaznamenaná data i z textového souboru. Plugin definuje rozhraní pro začlenění tří podčástí, které jsou specifické pro danou bezdrátovou technologii. V našem prototypovém řešení jsme zvolili načítání analyzovaných dat z textového souboru.

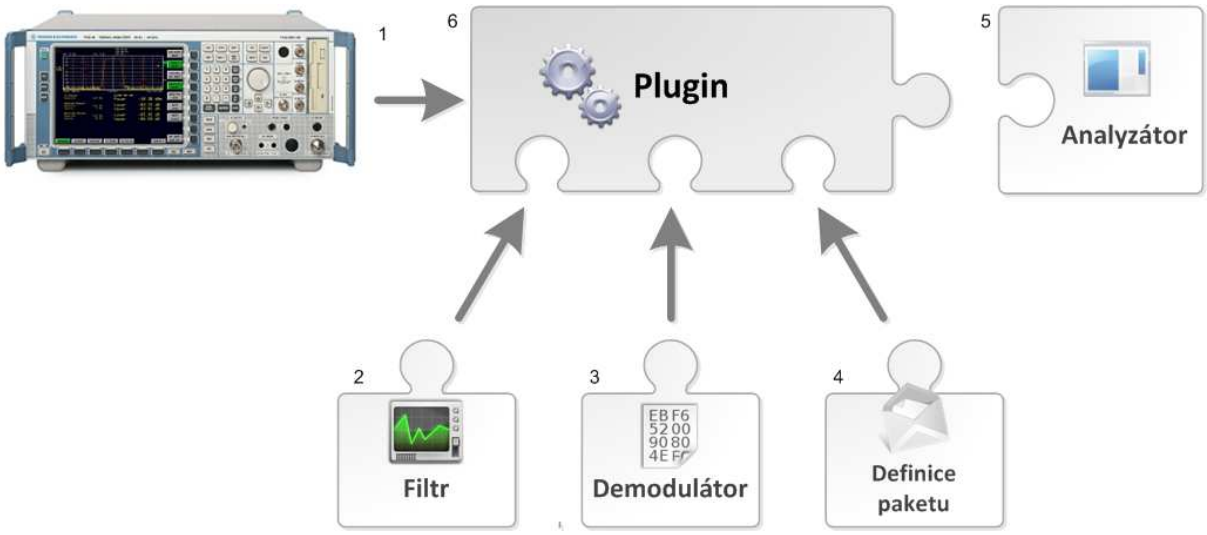

Schéma analyzátoru

3. ZÁVĚR

Navrhli jsme systém pro analyzování datových komunikací na bezdrátových sítích. Implementovali jsme prototypové řešení pro analýzu dat na kontrolním kanálu trunkové sítě MPT 1327 Dopravního Podniku Města Brna. Naše řešení je postaveno na rozšíření existujících technologií, které vhodným způsobem doplňuje. Systém byl navržen s důrazem na snadnou použitelnost, rozšiřitelnost a nízké náklady. Proto je vhodný například pro školy začínající výzkum v oblasti bezdrátových sítí. Celý systém je v současné době rozpracován v podobě prototypu, který dokáže detekovat a zpracovávat zprávy sítě MPT 1327.

PODĚKOVÁNÍ

Tato práce vznikla za částečné podpory grantu FIT VUT v Brně FIT-S-10-1 a specifického výzkumu MSM0021630528.

LITERATURA

[1] JURNEČKA, Peter. Sieťový analyzátor riadeny pravidlami. Brno, 2009. s. Diplomová práce. FIT VUT.

[2] TROJANOVIČ, Vladimír. Spracovanie AM a FM signálov s využitím princípov softvérového rádia. Košice, 2006. 71 s. Diplomová práce. TECHNICKÁ UNIVERZITA V KOŠICIACH, FAKULTA ELEKTROTECHNIKY A INFORMATIKY.

[3] MPT 1327. *A Signalling Standard for Trunked Private Land Mobile Radio Systems*. [s.l.] : [s.n.], January 1988. 290 s. Dostupné z WWW: http://www.ofcom.org.uk/static/archive/ra/publication/mpt/mpt_pdf/mpt1327.pdf

[4] *R&S®FSQ Signal Analyzer : Operating Manual*. Munich (Germany) : Rohde & Schwarz GmbH & Co. KG, 2009. 826 s. Dostupné z WWW: <http://www2.rohde-schwarz.com/file_5543/FSQ%20Operating%20Manual%20English%20FW%204.55.pdf>..