OPEN PACKET ANALYSER FOR ZIGBEE WIRELESS SENSOR NETWORKS

Martin Leixner

Master Degree Programme (1), FEEC BUT

E-mail: xleixn01@stud.feec.vutbr.cz

Supervised by: Lubomír Mraz

E-mail: mraz@phd.feec.vutbr.cz

Abstract: The aim of this work is to develop multiplatform, time-precise and low-cost packet analyser, which can be operated in various frequency bands and could be accessible remotely. Currently, analyser supports 2.4 GHz band and 780/868/915 MHz bands. Moreover, it provides high resolution timestamp for received packets. This feature is crucial for debugging wireless protocols. The device contains embedded web server which enabling its remote configurations. The data from analyser feeds the Wireshark packet inspection software.

Keywords: Packet analyser, Zigbee, Wireless sensor networks, IEEE 802.15.4, Wireshark

1. ÚVOD

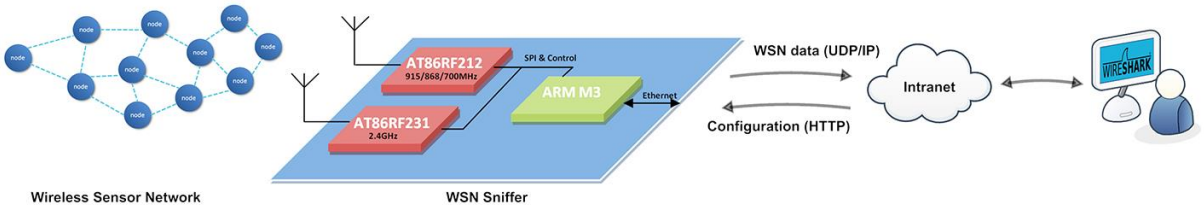
Pro profesionální vývoj v oblasti bezdrátových senzorových sítí je nutné mít k dispozici zařízení pro analýzu přenášených dat mezi senzorovými zařízeními. Hlavním problémem současných komerčních analyzátorů pro bezdrátové senzorové sítě jsou jejich vysoké pořizovací náklady. Jedná se o částky obvykle v řádu tisíců eur. Jejich další nevýhodou je nemožnost ovládání zařízení na větší vzdálenost, kvůli propojení s počítačem prostřednictvím USB rozhraní. Dále komerční analyzátory jsou obvykle pevně spjaty s operačním systémem Windows. Všechny tyto nedostatky odstraňuje navržený analyzátor, který je prezentován v tomto článku.

Cílem práce bylo implementovat otevřený paketový analyzátor pro kmitočtové pásmo 2.4 GHz a sub-gigahertzové pásmo, konkrétně 780/868/915 MHz. Analyzátor bude poskytovat přesné časové razítko k přijatým paketům, bude operovat vzdáleně prostřednictvím Ethernet rozhraní a bude ho také možné konfigurovat vzdáleně pomocí webového rozhraní. Navrhnutý analyzátor bude spolupracovat s multiplatformním vizualizačním softwarem Wireshark [4].

2. ARCHITEKTURA PAKETOVÉHO ANALYZÁTORU

Pro řízení analyzátoru byl vybrán mikrokontrolér z rodiny ARM typ Cortex-M3, konkrétně LM3S8962 [3] od Texas Instruments. Tento výkonný mikrokontrolér byl zvolen pro svou nízkou cenu a unikátní podporu Ethernet rozhraní včetně linkové vrstvy přímo na čipu. Dále je k obvodu volně dostupné propracované softwarové vybavení s názvem Stellarisware. Mikrokontrolér LM3S8962 obsahuje 256 kB FLASH paměť, proto do něj bylo možné integrovat webové rozhraní pomocí kterého je prováděna vzdálená konfigurace paketového analyzátoru. Pro zachycení dat ze senzorové sítě jsou využity dva rádiové moduly, konkrétně AT86RF212 [1] pro sub-gigahertzové a AT86RF231 [2] pro 2.4 GHz pásmo. Tyto nejmodernější rádiové moduly byly vybrány kvůli své bezkonkurenční citlivosti přijímače, přímou podporu standardu IEEE 802.15.4, nízké spotřebě a množství pokročilých funkcí. Mikrokontrolér komunikuje s rádiovými moduly přes rychlé sériové rozhraní SPI. Po této sběrnici jsou odesílány nastavovací parametry i samotné pakety ze senzorové sítě. Zachycené pakety, ze senzorové sítě jsou zpracovány a dále odeslány do cílového počítače pomocí rozhraní Ethernet, kde jsou dále vizualizovány v open-source softwaru Wireshark. Tento software je de-facto standard

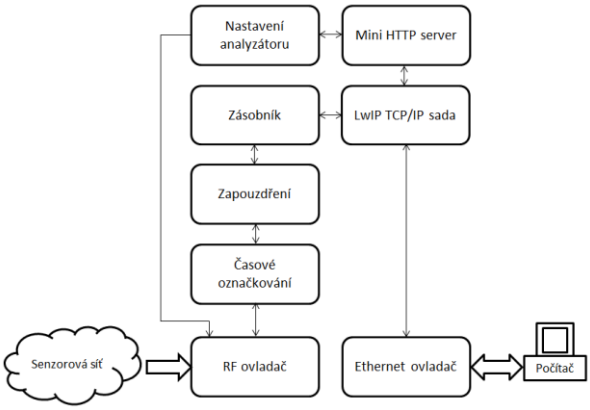
pro vizualizaci a analýzu paketů drátových i bezdrátových sítí, podporuje mnoho platforem a v současné verzi již obsahuje disektory pro nejznámější standardy využívané v senzorových sítích jako jsou IEEE 802.15.4, Zigbee a 6LoWPAN. Wireshark podporuje také doplnění nových disektorů v jazyku C, to však vyžaduje rekompilaci zdrojových kódů. Nový disektor je také možné napsat i ve skriptovacím jazyku Lua, který umožňuje runtime integraci do Wiresharku pomocí pluginu.



Obrázek 1: Komunikační architektura

3. FIRMWARE ANALYZÁTORU

Popis firmwaru pro mikrokontrolér LM3S8962 je blokově ilustrován na Obrázku 2. Rádiové moduly AT86RF212/231 jsou řízeny pomocí RF ovladače. Ihned po příjmu nového paketu je paket časově označkován a to s přesností 10 µs. To je možné díky využití dedikovaných pinů rádiových modulů a nejvyšší prioritě přerušení v mikrokontroléru. Dále je paket zapouzdřen do speciálního protokolu ZEP (ZigBee Encapsulation Protocol). Tento protokol byl zvolen pro podporu bezešvé integrace analyzátoru do vizualizačního programu Wireshark, který protokol ZEP přímo podporuje. Takto zapouzdřený paket je dále uložen na zásobníku a následně zpracován pomocí LwIP (Lightweight TCP/IP stack) sady, která opatří paket patřičnými hlavičkami pro komunikaci v síti. V současné verzi firmwaru je podporováno TCP/IP verze 4.



Obrázek 2: Blokové schéma firmwaru

Ve firmwaru je dále implementován mini webový server pro nastavení analyzátoru přes webové stránky. Je možné nastavit tyto parametry: kanál, vysílací výkon, citlivost přijímače, nastavení filtrace neplatných paketů, filtrace podle PANID, nastavení komunikačních atributů (síťová adresa, maska, brána) atd.

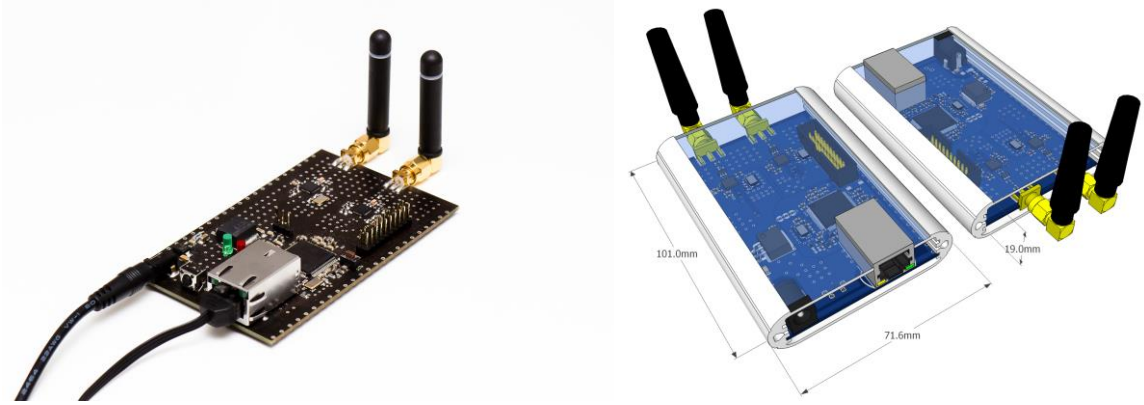
Analyzátor může pracovat ve třech módech:

- Paketový analyzátor. Jedná se o standardní režim pro odchytávání paketů.
- Analyzátor výkonové úrovně kanálů na fyzické vrstvě. Tento mód je určen pro zjištění výkonové úrovně na kanálech, obvykle pro detekci jejich obsazenosti nebo rušení.

- Kontinuální rádiový vysílač. Tento mód umožňuje generovat nepřetržité vysílání na zvoleném kanálu. To je možné využít například pro testování bezdrátových směrovacích protokolů, kde se určitá část sítě fyzicky úmyslně ruší.

4. REALIZOVANÝ ANALYZÁTOR

Funkční analyzátor je zobrazen na Obrázku 3. Z obrázků je patrné, že analyzátor má velmi kompaktní rozměry.



Obrázek 3: Z leva: funkční prototyp analyzátoru, 3D vizualizace finálního analyzátoru

5. ZÁVĚR

Navržený paketový analyzátor byl testován společně s profesionálními komerčními produkty Daintree a Perytons, u kterých se cena pohybuje v tisících eur. Konkrétně byl analyzován příjem paketů, jejich počet, správnost a dále přesnost jejich časového značení. Podle výsledků testů, navržený analyzátor obstál a své konkurenty i v mnohém předčil. Díky jeho parametrům a vybavenosti je možné říci, že v současnosti se jedná o konkurence schopný produkt pro analýzu bezdrátových senzorových sítí. Jedná se o první otevřený analyzátor, který podporuje jak 2.4 GHz tak i sub-gigahertzové pásmo. Dále umožňuje mikrosekundovou přesnost pro označení paketů a je ho možné ovládat vzdáleně pomocí webového rozhraní. Jednou z předních vlastností je také, že je plně integrován do multiplatformního vizualizačního nástroje Wireshark, který umožňuje přehledně pakety vizualizovat a dále analyzovat. Do budoucna by bylo vhodné analyzátor rozšířit o možnost napájení prostřednictvím ethernetu PoE (Power-over-Ethernet) případně doimplementovat podporu IPv6. V současné době se analyzátor využívá při výuce předmětu Senzorové Systémy MSSY na FEKT, VUT v Brně.

REFERENCE

[1] ATMEL. *AT86RF212: datasheet* [online]. 02/2010 [cit. 2013-03-02]. Dostupné z: <http://www.atmel.com/Images/doc8168.pdf>.

[2] ATMEL. *AT86RF231: datasheet* [online]. 09/2009 [cit. 2013-03-02]. Dostupné z: <http://www.atmel.com/Images/doc8111.pdf>.

[3] TEXAS INSTRUMENTS. *LM3S8962* [online]. © 1995-2013 [cit. 2013-03-02]. Dostupné z: <http://www.ti.com/product/lm3s8962>.

[4] WIRESHARK [online]. 2011 [cit. 2013-03-02]. Dostupné z: <http://www.wireshark.org>.

[5] WISLAB. *OPEN ETHERNET PACKET ANALYSER FOR IEEE 802.15.4 NETWORKS* [online]. 23. October 2012 [cit. 2013-03-23]. Dostupné z: <http://wislab.cz/our-work/open-ethernet-packet-analyser-for-ieee-802154-networks>.