VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bezdrátové senzorové sítě MPC-SSY 2020/2021

Projektová dokumentácia

LWM Sniffer

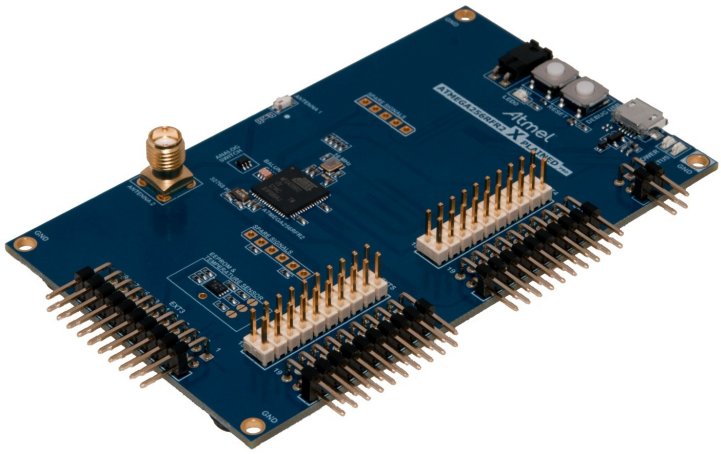
Patrícia Ramosová (204299)
Filip Kamenář (195352)
Alex Sporni (204633)

1. mája 2021

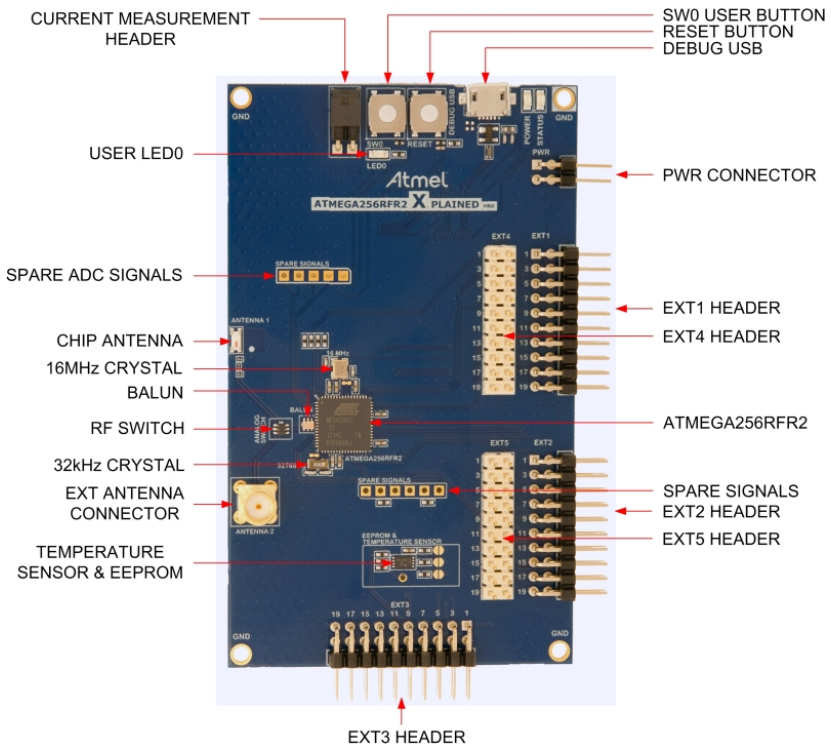
Obsah

1 Úvod

Cieľom projektu bolo vytvoriť program v jazyku C tzv. LWM Sniffer, ktorý má za úlohu zachytávať sieťovú komunikáciu medzi mikrokontrolérmi Microchip ATmega256RFR2 Xplained Pro viď 1. Zariadenie disponuje integrovaným debuggerom, 8-bitovým AVR procesorom, radou rozhraní (digitálnych aj analógových) ako sú: 4-wire SPI, TWI, ISP, JTAG, 2 analógové komparátory, UART, USART, časovač, PWM atď ... Mikrokontrolér pracuje v napäťovom rozsahu od 1.8-3.6 V. Podrobný popis rozhraní a súčastí mikrokontroléru je možné vidieť na obrázku 2. Program bol vyvíjaný vo vývojovom prostredí Atmel Studio od spoločnosti Microchip[1] [2], [1].



Obr. 1: ATmega256RFR2



Obr. 2: ATmega256RFR2 - rozhrania a súčasti

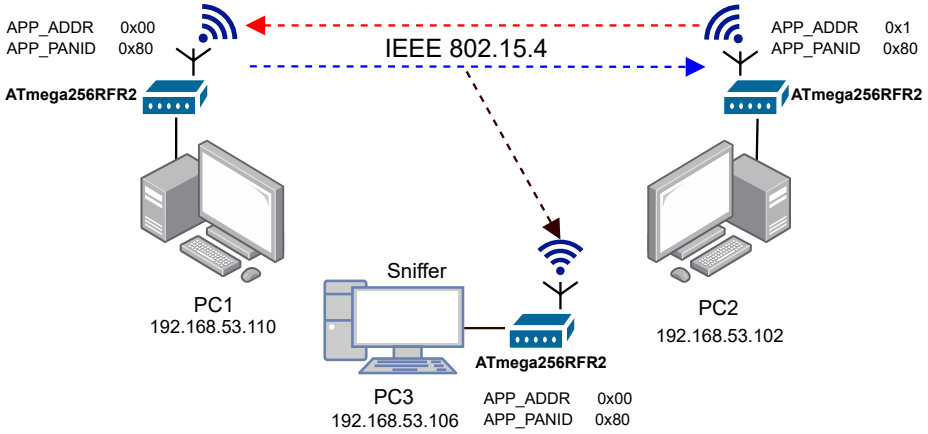
[1] https://www.microchip.com/

2 Implementácia

Zdrojové kódy k projektu jsou dostupné ve volně přístupném GitHub repozitáři, který je dostupný na `https://github.com/xramos00/SSY_Projekt`.

2.1 Zachytávání dat

Zařízení v síti light weight mesh (LWM) ve výchozím stavu zachytává veškerou rádiovou komunikaci. Kontrola, zda daný rámec zařízení patří, je prováděna až po přijetí rámce, kdy je srovnána PanID zachyceného rámce a PanID mikrokontroleru. To znamená, že všechny zařízení v síti light weight mesh se chovají jako sniffery, pouze rámce nezachytávají, ale ihned je zahazují, jakmile zjistí, že jim nepatří.



Obr. 3: Princíp fungovania zachytávania

Této skutečnosti je využito v tomto řešení, kdy přijaté rámce, které zařízení nepatří, nejsou zahozeny, ale jsou uloženy a poté skrz UART vytištěny do terminálu a uloženy do souboru. LWM stack pri prijatí rámca zavolá funkciu `nwkRxHandleReceivedFrame` to súboru `nwkRx.c`. V tejto funckii sa v pôvodnej implementácii rozhodovalo o type rámca, potrebe odoslať ACK, dešifrovaní pri zapnutom šifrovaní, atď.. Celá táto logika bola obídená a nahradená jednoduchým výpisom informácií o rámci cez UART. Informácie sú uložené v dátovej štruktúre typu `NwkFrameHeader_t`, ktorá sa nachádza v súbore `nwkFrame.h`. Ďalej je rámcu nastavený stav *NWK_RX_STATE_FINISH*, tým by malo prísť k predaniu rámca na vyššiu vrstvu.

2.2 Ukládání dat z UART do souboru

Pro ukládání dat byl využit open-source nástroj Tera Term v nejnovější verzi 4.105[2], který umožňuje připojení pomocí sériového portu a následně zvládne ukládat textové řetězce z výstupu konzole přímo do externího souboru. Výstupní soubor může být libovolného typu, např. *.txt* anebo *.csv*. Uložená data je možné zpracovávat jakýmkoliv textovým editorem.

V tomto případě jsou data exportována do souboru s příponou *.csv*. Program tiskne do konzole pevný počet sloupců, kdy data jsou od sebe oddělena čárkou. Ukázka takto vyexportovaných a zpracovaných dat je v tabulce 1.

[2]Tera Term - `https://ttssh2.osdn.jp/index.html.en`

macFcf	macSeq	macDstPanId	macDstAddr	macSrcAddr	nwkSeq	nwkSrcAddr	nwkDstAddr	PAYLOAD
34913	35	128	0	1	35	1	0	t
34913	36	128	0	1	36	1	0	e
34913	37	128	0	1	37	1	0	s
34913	38	128	0	1	38	1	0	t
34913	39	128	0	1	39	1	0	z
34913	40	128	0	1	40	1	0	a
34913	41	128	0	1	41	1	0	c
34913	42	128	0	1	42	1	0	h
34913	43	128	0	1	43	1	0	y
34913	44	128	0	1	44	1	0	t
34913	45	128	0	1	45	1	0	a
34913	46	128	0	1	46	1	0	v
34913	47	128	0	1	47	1	0	a
34913	48	128	0	1	48	1	0	n
34913	49	128	0	1	49	1	0	i

Tabuľka 1: Ukázka zachytených dat

Popis jednotlivých stĺpcov:

- **macFcf -** Frame Control Field, definuje typ rámca (beacon, data,..).
- **macSeq -** Sekvenčné číslo rámca na linkovej vrstve.
- **macDstPanId -** Identifikátor cieľovej PAN.
- **macDstAddr -** Cieľová MAC adresa.
- **macSrcAddr -** Zdrojová MAC adresa.
- **nwkSeq -** Sekvenčné číslo rámca na sieťovej vrstve.
- **nwkSrcAddr -** Zdrojová sieťová adresa.
- **nwkDstAddr -** Cieľová sieťová adresa.
- **Payload -** Obsah správy.

3 Záver

Na záver môže byť konštatované, že zadanie bolo v plnom rozsahu splnené. Výsledný program je schopný zachytávať prechádzajúcu komunikáciu a ukladať ju do externého súboru napr. typu csv. Riešenie by následne mohlo byť rozšírené o zobrazovanie zachytávanej komunikácie v reálnom čase. Dáta by mohli byť ukladané vo formáte vhodnom pre export do programu Wireshark.

Použitá literatúra

[1] Atmel: 8-bit Microcontroller with Low Power 2.4GHz Transceiver for ZigBee and IEEE 802.15.4. [online], 2021. Dostupné z: https://moodle.vutbr.cz/pluginfile.php/326761/mod_resource/content/1/atmel-8393-mcu_wireless-atmega256rfr2-atmega128rfr2-atmega64rfr2_datasheet.pdf?fbclid=IwAR2oukhi5Iz5xMv_IjPqHWFC-eOBERNTqnWal_2hhz7Qv9epiC4NVk6Qj0c

[2] Atmel: ATmega256RFR2 Xplained Pro, USER GUIDE. [online], 2021. Dostupné z: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-42079-ATMEGA256RFR2-Xplained-Pro_User-Guide.pdf