

UWB Sniffer

Debugging platform for RTLS Integrators and Developers

- Fully integrated with industry standard Wireshark
- 6 channels (802.15.4a UWB PHY)
- Ethernet Communication interface
- Easy to automate via HTTP interface
- Received Signal Strength Indication
- Injection Mode for sending packet
- Support for dissecting Decawave Two Way Ranging protocol
- Dimensions: 51 x 51 mm



Package Content									
1x	UWB Sniffer								
1x	USB to DC 1.3mm Power Cable								
1x	Ethernet Cable								

Requirements
Wireshark (Linux/ Windows)
USB port or DC Adapter 5V/500mA
Ethernet port



1	UW	B Sniffer Operation	3
2	Sni	ffer Installation	4
	2.1	Hook up cables to UWB Sniffer	4
	2.2	Setting TCP/IP at the host side	4
	2.3	Connect to the UWB Sniffer homepage	5
3	Wir	eshark Settings	ô
	3.1	Wireshark installation	ô
	3.2	Capture Frames	ô
	3.3	Start UWB Sniffer	6
	3.4	Let's sniff some communication	6
	3.5	Adjusting Wireshark for IEEE 802.15.4 Networks	7
	3.6	Wireshark columns	7
	3.7	Install ZEPv3 plugin	8
	3.8	Adjusting Wireshark columns to IEEE 802.15.4 compliant frame	9
4	UW	B Sniffer Configuration	1
	4.1	Home Page 12	1
	4.2	Setting Page12	2
	4.3	Sniffer IPv4 Settings	3
	4.4	Host Settings	3
	4.5	Injection Mode	3
5	Ana	alyzing Decawave Two Way Ranging (TWR)15	5
	5.1	Wireshark dissector for Decawave Two Way Ranging	7



1 UWB Sniffer Operation

UWB Sniffer provides following two operation modes: Sniffing and Injection. In the first one the sniffer device captures all the 802.15.4 UWB frames transmitted over the air and forward them to Wireshark. Injection mode enables to send arbitrary UWB frames directly from the sniffer's web interface.



Sniffing Mode

This is default mode of operation for the UWB Sniffer device. User needs to select desired channel and some other parameters. All captured frames on the particular channel are feed to Wireshark which is an open source industry-standard software for analyzing wired and wireless networks. Data encapsulation is depicted in picture above. Captured 802.15.4 frames are wrapped in ZEP (Zigbee Encapsulation Protocol) which is native protocol included within Wireshark. ZEP basically adding some interesting information to raw 802.15.4 frame such as RSSI or timestamp.

Injection Mode

802.15.4 frame

In this mode an user may set frame payload, channel, number of packets which are going to be sent over the air from UWB Sniffer. This mode is useful for a device development, testing or auditing. Thanks to the HTTP interface, this might be very powerful tool driven from a script language.



2 Sniffer Installation

2.1 Hook up cables to UWB Sniffer

Connect Ethernet cable and power cable to UWB Sniffer as it is depicted in picture below.



2.2 Setting TCP/IP at the host side

In this section we are going to adjust TCP/IP settings at PC host in order to be able to communicate with the UWB Sniffer device.

Default sniffer's settings are: IP address 10.10.10.2, mask 255.255.255.0

Host's IP address must be within the same network scope as the UWB Sniffer device. **Set host IP to 10.10.10.1** and network mask to **255.255.255.0**.

This can be done via "Network and Sharing Center" in Windows. Press CTRL+R and type "ncpa.cpl" Enter. Then you need to select network interface, where you have attached the sniffer and set IP and network address.





2.3 Connect to the UWB Sniffer homepage

UWE	3 Sniffer 🔲	HOME Settings Injection Mode
STOP		RUNNING
	SUM	MARY
	MAC address	IP address
	00:1e:c0:85:73:84	10.10.10.2
	Channel	(Non) Standard Frame Delimiter
	5	Non-Standard
	CRC filter	Data rate
	OFF	110 kbps

Now, point a browser to sniffer's home address http://10.10.10.2, homepage should appear.



3 Wireshark Settings

UWB Sniffer acts as a probe which capturing 802.15.4 frames and forwards them to a remote host computer. In order to be able to work with those frames Wireshark software is used.

3.1 Wireshark installation

Download, install and run <u>Wireshark</u>. Please select the latest stable appropriate for your operating system and architecture.

3.2 Capture Frames

Select the Ethernet interface (linked to UWB Sniffer) from the available capture interfaces and start capturing frames.



Wireshark implicitly shows all frames from wired and wireless networks delivered to the selected interface. Therefore, it is useful to apply 802.15.4 filter which is referred as "wpan".

6 Capturing from L	ocal Area Connection	[Wireshark 1.10.3 (SVN	Rev 53022 from /trun	k-1.10)]
<u>File Edit V</u> iew	<u>Go C</u> apture <u>A</u> naly	ze <u>S</u> tatistics Telephon <u>y</u>	<u>T</u> ools <u>I</u> nternals	<u>H</u> elp
0 0 🔏 🔳	1 🗟 🖉 🗶	2 🔍 🗢 🔿	7 ⊻ 🔳 🛢	0, 0, 0, 17 🕁 🛛 畅 💥 💢
Filter: wpan	— "wpai	n" ENTER	 Express 	sion Clear Apply Save

3.3 Start UWB Sniffer

Now the host side is ready and you need to start UWB Sniffer via web interface. Point the browser to sniffer's IP address and press RUN.

UΜ	/B 9	Snif	ffer	ſ				ŀ	IOME	Settings	Injection	Mode
RU	N)							S	OPPE	D

3.4 Let's sniff some communication

Sniff your own UWB hardware or download our captured file.



Adjusting Wireshark for IEEE 802.15.4 Networks 3.5

The previous chapter describes process of data capture and initial Wireshark configuration. User may download the sample file <u>uwb_twr_demo</u>.

3.6 Wireshark columns

Wireshark has default columns settings for wired Ethernet network, see picture below.

4													*Ether	rnet	fWire	shark	1.12.2	(v1.	12.2-	0-a8	398fa2	2 from	mas	ter-1	.12)]	
File	Edit	t Vie	w Go	Cantu	re A	nalvze	Stati	istics	Teler	hony	Tools	Intern	als H	lelp						- 9-						
0	0	41			1	K 2	_ C	\$ \$			F L			Ð,	0.0		8	1	8 %	. 0	D.					
Filte	n w	pan										✓ E	pressio	on	Clear	Apply	Save									
No.		Time		S	ource				Des	tinatio	n		Len	gth	Info							Pro	toce	bl		
	1	0.00	0000	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	ļ.
	2	1.01	1990	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	3	2.02	3904	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	4	3.03	6017	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	5	4.04	7919	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	6	5.06	0024	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000)1,	Src:	0x1	1001	I	EE	802.	15.4	
	7	6.07	2027	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	8	7.08	4062	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	9	8.09	6069	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	10	9.10	8072	000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	11	10.1	2007	9000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	12	11.1	3209	5000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	13	12.1	4411	3000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	ł
	14	13.1	5612	1000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000)1,	Src:	0x1	1001	I	EE	802.	15.4	
	15	14.1	6809	5000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	16	15.1	8010	6000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	17	16.1	9207	8000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	18	17.2	0414	9000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	19	18.2	1620	4000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	1,	Src:	0x1	1001	I	EE	802.	15.4	
	20	19.2	2821	9000		0x1	001			(0x000	1	8	88	Data,	Dst:	0x000	01,	Src:	0x1	1001	I	EE	802.	15.4	
 H F E H I H Z H Z I H D 	# Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0 # Ethernet II, Src: Microchi_85:73:84 (00:1e:c0:85:73:84), bst: compalIn_2e:21:5a (f8:a9:63:2e:21:5a) # Internet Protocol Version 4, Src: 10.10.10.2 (10:10.2), Dst: 10.10.10.1 (10.10.10.1) # User Datagram Protocol, Src Port: 17754 (17754), Dst Port: 17754 (17754) # Zigbee Encapsulation Protocol, channel: 1, Length: 14 # IEEE 802:15.4 Data, Dst: 0x0001, Src: 0x1001 # Data (3 bytes)																									
000 001 002 003 004 005		8 a9 00 4a 0a 01 04 00 04 00 00 01	63 05 45 00 00 10	2e 21 e3 00 5a 45 00 00 00 00 21 00	5a 00 5a 00 5a 00 50 00 00 00	0 1e f 11 0 36 9 0a 0 00 c 80	c0 8d 5b 18 00	85 7 a9 0 fb 4 d8 6 0e 4	3 84 a 0a 5 58 0 00 1 88	08 0a 03 00 5b	00 45 02 0a 01 01 00 b5 ca de	00 0a 73 06 01	c. .J EZ	!Z	s. 5 [.ex	E. s										

🔘 💅 Data (data), 3 bytes

Packets: 83 · Displayed: 80 (96.4%) · Dropped: 0 (0.0%)

Columns are defined for the default Wireshark profile as follows:

Column name	Description
No.	Frame number counted from the start of capture in Wireshark. This is NOT number of a frame received from UWB Sniffer. It includes all packets (wired&wireless) delivered to the host's ethernet interface
Time	Ethernet timestamp of the frame assigned by the operating system. This is NOT precise timestamp from UWB Sniffer.
Source	Source Address
Destination	Destination Address
Protocol	Protocol
Length	Length of entire Ethernet frame including transportation overhead. This is NOT length of 802.15.4 frame
Info	Protocol details



From the table above it is obvious the default column settings are not associated with 802.15.4. Therefore, user can adjust them to the 802.15.4 frame info. Let's refresh the encapsulation scheme for each 802.15.4 frame delivered to the host (see picture below). While the grey colored protocols are used only to transport the 802.15.4 frame through a network infrastructure, the ZEP – Zigbee Encapsulated Protocol carries all the important information such as sequence number, timestamp or channel number related to the every 802.15.4 captured by the UWB Sniffer device.



3.7 Install ZEPv3 plugin

Although, Wireshark natively contains ZEP protocol v2, we provide ZEPv3 which is backwards compatible and brings additional information related to band, channel page and precise timestamp information. In case that additional information are not interesting for user, just skip this chapter.

- 1. Download ZEPv3 plugin.
- 2. Extract and copy plugin to the Wireshark plugin folder. Windows c:\Program Files\Wireshark\plugins\1.x.x\, Linux /usr/local/lib/wireshark/plugins/1.x.x/.
- 3. Start Wireshark. menu Analyze -> Enabled Protocols (CTRL+SHIFT+E)
- 4. Uncheck ZEP, check ZEPv3
- 5. Apply, OK.
- If frames are not decoded with ZEPv3 go to menu Analyze -> Decode as -> ZEPv3 -> Apply, OK.

ZEPv3 contains fields depicted in picture below:

```
B Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
B Ethernet II, Src: Microchi_85:73:84 (00:1e:c0:85:73:84), Dst: CompalIn_2e:21:5a (f8:a9:63:2e:21:5a)
B Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
B User Datagram Protocol, Src Port: 17754 (17754), Dst Port: 17754 (17754)
Fortocol ID String: EX
Protocol ID String: EX
Protocol Version: 3
Type: 1 (Data)
Channel ID: 1
Device ID: 29572
LQI/CRC Mode: LQI
Link Quality Indication: 0
Timestamp: 0.000000000 seconds
Absolute Timestamp: 0.000000000 seconds
Absolute Timestamp: 0.000000000 seconds
Absolute Timestamp: 0.000000000 seconds
Frequence Number: 181
Frequency band: UWB Low band (6)
Channel page: 4
Length: 14 Bytes
B IEEE 802.15.4 Data, Dst: 0x0001, Src: 0x1001
B Data (3 bytes)
```



Zepv3 Field	description
zepv3.version	zep version
zepv3.type	type of packet
zepv3.channel_id	channel number
zepv3.device_id	unique ID of the sniffer, based on MAC address
zepv3_lqi_mode	LQI/CRC either LQI is send to Wireshark or CRC value
zepv3.lqi	LQI value, not used in UWB Sniffer
zepv3.time	Time elapsed since sniffing was started at UWB Sniffer
zepv3.reltime	Relative time since sniffing was started at UWB Sniffer
zepv3.abstime	Absolute time converted to host timezone
zepv3.difftime	Differential time among packets
zepv3.seqno	Sequence number of packet send from UWB Sniffer
zepv3.band	IEEE 802.15.4 frequency band
zepv3.chanpage	IEEE 802.15.4 channel page
zepv3.length	IEEE 802.15.4 frame length

3.8 Adjusting Wireshark columns to IEEE 802.15.4 compliant frame

Note: The procedure below describes how to adapt Wireshark columns to 802.15.4 frames. You may skip this section if you are satisfied with default settings.

Adjusting columns procedure:

- a. Right click on the columns header
- b. Select Column Preferences
- c. Adjust columns to 802.15.4

UWB Sniffer



												u١	wb_1	wr,	de	mo.	pcap	ong	[W	iresha	ark 1
Eile	Edi	t <u>V</u> iew	Go	<u>C</u> aptur	e <u>A</u> na	əlyze	Statis	tics	Telep	ohony	(I	ools	Inte	rnal	s <u>F</u>	lelp					
0	•	4 •	ø) ×	2	0	\$		٩	Ŧ	2			9	Ð	Q	Q	•		X
Filte	r.												~	Exp	ressi	on	Cle	ar A	Apply	Save	e
No.		Time		So	urce				Des	tinatio	on a	k			1	-					٦.
	1	0.000	0000	00		0x10	001				0x(0001		24	Sort	t Asc	endir	19			001
	2	1.011	9900	00		0x10	001				0x(0001		ž.,	Sort	t Des	cendi	ing			001
	3	2.023	9040	00		0x10	001				0x0	0001			No	Sorti	na	-			001
	4	3.036	0170	00		0x10	001				0x0	0001									001
	5	4.047	9190	00		0x10	001				0x0	0001			Sho	w Re	solve	d			001
	6	5.060	0240	00		0x10	001				0x0	0001	2000								- 101
	7	6.072	0270	00		0x10	001				0x(0001			Alig	yn Le	ft	(defa	ult)		001
	8	7.084	0620	00		0x10	001				0x0	0001			Aliq	an Ce	nter				001
÷ F	rame ther	6: 8 net I	8 by I, S	tes or rc: Mi	wir crock	e (7 hi_8	04 bi 5:73:	its) :84	, 88	le:	tes c0:	cap 85:7	tur 3:8	1	Alig	yn Rig	ght				ce 5a
• I	nter	net P	roto	col Ve	ersion	n 4,	Src:	: 10	.10.	10.2	2 (10.1	0.1	36	Col	umn	Prefe	renc	es	~	
• U	ser	Datag	ram	Protoc	:0], :	Snc	Port:	: 17	754	(17)	754), D	st		Edit	Col	umn	Detai	k		1
🗆 Z	igBe	e Enc	apsu	lation	Prot	toco	1, cł	nann	el:	1, 1	Len	gth:	14		Cun			Deter	1210		
	Pro	tocol	ID	string	: EX									2	Res	ize C	olum	n			
	Pro	tocol	ver	sion:	3										Die		d Cal				
	тур	e: 1	(Dat	a)											100	piaye	u co	Ginni			
	cha	innel	ID:	1										-	Hid	e Co	umn				
	De\	vice I	D: 2	9572										8	Ren	nove	Colu	mn			
	LQI	CRC /	Mode	: LQI																	and it

Default column settings

Displayed	Title	Field type
V	No.	Number
V	Time	Time (format as specified)
V	Source	Source address
V	Destination	Destination address
V	Protocol	Protocol
V	Length	Packet length (bytes)
V	Info	Information

Recommended column settings for 802.15.4

Displayed	Title	Field type
✓	No.	Custom (zepv3.seqno)
•	Time	Custom (zepv3.time)
•	Mac Src Address	Source address
•	Mac Dst Address	Destination address
-	Protocol	Protocol
~	Length	Custom (zepv3.length)
~	RSSI	Custom (wpan.rssi)
-	Info	Information

Adjusted Wireshark columns should seem like this:

4													u	wb_	twr_r	demo	.pca	png	[Wi	resha	ark 1	.12.2	? (v1	.12.2	-0-	g898	fa22	from	n mas	ster-1	.12)]										- 6	×
Eile	Edit	View	<u> </u>	Cap	ture	Ana	hyze	Statie	stics	Tele	phon	γI	ools	Inte	rnals	Help	•																									
۰	•	4 •	1			×	2	0	. 4	φ	٩	Ŧ	2			€		Q	۳		M	5	*	1																		
Filter	•													~	Expre	ssion.	. a	ear A	pply	Save																						
No.	Tin	e			- 1	Mac S	ec Ad	dress	M	ac Dst	Addr	ress	Prot	tocol			Le	ngth	1	RSSI		Info																				-
181		185.1	1694	0041	5	•	0x10	01		0x	:0001	1	IE	EE 8	302.	15.4		14		-8	4										Dat	a,	Dst:	0x00	001,	src	: 0	x10	01			
182		186.1	1814	5362	5		0x10	01		0x	.0001	1	IE	EE 8	302.	15.4		14		-8	6										Dat	a,	Dst:	0x00	001,	Src	: 0	x10	01			
183		187.1	1935	26764			0x10	31		0x	,0001	1	IE	EE 8	302.	15.4		14		-8	5										Dat	a,	DST:	0x00	, 100	src	: 0	x10	01			
184		188.4	2055	9468	5		JX10	31		0x	0000	1	IE	EE 8	\$02.	15.4		14		-8	6										Dat	a,	DST:	0000	, 100	src	: 0	x10	01			
185		189.4	1/0	0006	2		JX10	51		UX OX	,0001	1	TE	EE C	302.	15.4		14		-8	8										Dat	a,	DSt:	UXUG	, 100	SEC	: 0	XIU	01			
186		190.2	297	21200	2		JX10	01		0x	,0000	1	IE	EE 8	302.	15.4		14		-8	8										Dat	a,	DSt:	0x00	, 100	SPC	: 0	x10	01			
100		191.4	10000	53333		-	2210	01		0.	.0000		TE	EE C	202.	10.4		14		-0	2										Dat	d,	DSC:	0×00	, 101	SPC		×10	01			
180		102 3	0650	5741		-	V10	01		0.	0000	1	TE	CC S	802	15 4		14		-0	7										Dat	a,	Deti	0200	01,	SEC		10	01			
190		194 3	779	7802			v10	01		0	0000	1	TE		802	15 4		14		-8	8										Dat	a,	Det .	0000	001	Sec		10	01			
1.01		195 3	2000	1208		-	10	01		0.	0000	1	TE		802	15 4		14		- 8	8										Dat	3	Det :	0200	001	Sec		10	01			
192		196	2021	1001	5	-	v10	01		0	0000	î	TE		802	15 4		14		-8	8										Dat	a,	DST .	000	001	Sec	- 0	v10	01			
193		197.3	141	73400	5		0x10	01		0x	0000	1	TE	EE 8	802.	15.4		14		-8	8										Dat	a.	DST:	0x00	001.	Sec	: 0	×10	01			
<								-		-		-						-														.,				-	-					>
 Fr E1 Ir Us Z1 	ame ther nter igBe Pro Typ	1: 8 net 1 net F Datag e Enco tocol tocol	aps lin aps lin ve (Da	ytes Src: pcol Prot ulat Stri rsion ta)	on Mich Verstoco ion I ing: h: 3	wire roch sior 1, S Prot EX	(70 1_8 1 4, arc F ocol	4 b :73 Src Port	its) :84 : 10 : 17 hanr	, 80 (00).10. 754 mel:	8 by :1e: .10. (17 1,	tes c0: 2 (754 Len	cap 85:7 10.1), C gth:	3:8 0.1 st	ed (4), 0.2) Port	704 Dst: , Ds :: 17	bit: Cor t: 1 754	s) or npal: 10.10 (17)	n in (n_2).10 /54)	terf: e:21 .1 (1	ace :5a 10.:	0 (f8 10.1	:a9 0.1)	:63:	2e:	21:5	a)															^
0000 0010 0020 0030	Dev LQJ Lir Tin Rel Ahs 0 f	A Distance in the second secon	10: Mod alit p: 2 Ti 63 05 45 00	2957; e: L0 y Inc 185.1 mest; mest; 22 21 23 00 5a 45 00 00	2 2 1694 amp: 5 amo: 5 5 a 0 0 0 0 0 0 0 0 0 0	0041 0.0 00 ff 00 b9	1: 0 1: 0	c0 1 5b	ds 0 se 14 1 85 7 a9 0 fb 4 d8 6	5:24 3 84 3 0; 5 51 60 00	ds 9:43 4 08 a 0a 8 03 0 00	00 02 01 00	8917 45 0a 01 55	000 00 73 06	Cer . J	c. !Z EZEZ	Fur	00P 5	Sta .E.	ndarı	dτ	ime																				v
0050	6	0 01	10	1 00	000	ac	80	00 (ve 4	* 95	> >0	ca	ae	01		111		.A.																								



4 UWB Sniffer Configuration

Home Page 4.1

RUN/STOP button and status field are located below the top menu. RUN/STOP button is present on every subpage and always refers to packet sniffing or capturing frames on defined channel.

Home page contains following summary information about an analyzer: MAC address, IP address, current channel, (non)standard frame delimiter, crc filter and data rate.

Below summary section the counters are displayed. Counters (see picture below) have 12 bit resolution and they are related to selected events on PHY UWB layer. They might be quite useful during the network debugging and trouble shooting.

At the very bottom of the homepage a firmware version is displayed.

UWB Sniffer 🔲	HOME Settings Injection Mode
RUN	STOPPED
SUM	MARY
MAC address	IP address
00:1e:c0:85:73:84	10.10.2
Channel	(Non) Standard Frame Delimiter
2	Non-Standard
CRC filter	Data rate
OFF	110 kbps
COUI	NTERS
Number of good CRC received frames	Number of bad CRC (CRC error) received frames
0	0
Number of received header errors	Number of received frame sync loss events
0	0
Number of address filter errors	Number of receiver over-runs
0	0
SFD timeouts	Preamble timeouts
0	0
RX frame wait timeouts	Number of transmitted frames
0	0

UWB Sniffer

Datasheet



4.2 Setting Page

Radio parameters, network configuration and host settings are done via this page

Available Channels

Channel	Center Frequency (MHz)	Band (MHz)	Bandwdth (MHz)
1	3494.4	3244.8 – 3744	499.2
2	3993.6	3774 - 4243.2	499.2
3	4492.8	4243.2 - 4742.4	499.2
4	3993.6	3328 - 4659.2	1331.2 (real approx. 900)
5	6489.6	6240 - 6739.2	499.2
7	6489.6	5980.3 - 6998.9	1081.6 (real approx. 900)

Pulse Repetition Frequencies (PRF)

16 MHz / 64 MHz

Preamble Length

4096, 2048, 1536, 1024, 512, 256, 128, 64

Data Rate

110 / 850 / 6800 kbps

Preamble Code

1,2,3,4,5,6,7,8,9,10,11,12,17,18,19,20

PAC Size (symbols)

8 / 16 / 32 / 64

Frame Delimiter

Standard / Non Standard

LQI/CRC mode

LQI mode - frames are forwarded to Wireshark with signal strength values

CRC mode - frames are forwarded to Wireshark with CRC value received

CRC filter On/Off – 802.15.4 frames with wrong CRC are discarded



UW	B Sniffer 🔲	HOME Settings Injection Mode
RUN		STOPPED
	UWB RADIO	SETTINGS
	Channel number 2 (3993.6MHz)	PRF (Pulse repetition frequency)
	Preamble length [Symbols]	Data rate 110 kbps
	Preamble code (rx code)	PAC size [Symbols]
	(Non) Standard Frame Delimiter Standard Non-Standard	LQI/CRC mode ● LQI ● CRC
	CRC filter OFF ON	
	SUBMIT	& RUN

4.3 Sniffer IPv4 Settings

- IP mode DHCP client / Static IP address
- IP address
- Netmask
- Gateway

4.4 Host Settings

- Host IP address IP address of the host computer where Wireshark is running
- Host UDP port should be set 17754, this identifies 802.15.4 flow in Wireshark

4.5 Injection Mode

This mode is dedicated for a frame transmission. User needs to set UWB PHY settings as well as the payload, number of packet repetition and time gap among the packets. User might also set whether sniffing mode should be started right after the transmission ends.



UWB Sniffer 🔲		ном	IE Settings Injection Mode
RUN			STOPPED
		SETTINGS	
Channel number		PRF (Pulse repetition frequent	ncy)
2 (3993.6MHz)	•	16 MHz	T
Preamble length [Symbols]		Data rate	
1024	T	110 kbps	T
Preamble code (TX code)		(Non) Standard Frame Delim	iter
3	•	Standard	Non Standard
TX power coarse		TX power fine	
6	▼ dB	3.0	▼dB
PCdly (Pulse Constator Delay)		BY anabled after cond	
0xC2	•	⊙ Yes ● N	0
			-
Number of packet repeat	1	Time space between packets	1 mc
			1 1115
Packet payload ^{1,2}			
Bytes: 3 + 2 (CRC)		AutoC	CRC ³ CLEAR
01:02:03			
Estimated time of Injecting			
	~ 0.002	seconds	
		or	e packet ~ 1610 µs
	STA	RI	



5 Analyzing Decawave Two Way Ranging (TWR)

Decawave Two Way Ranging protocol is aimed for precise distance measurement based on UWB IEEE 802.15.4a standard. We provide feature-rich Ranging evaluation kit here.



There are three messages Poll, Response, Final exchanged between Tag and Anchor in order to get a precise distance. It is calculated based on Tag (TSP, TRR, TSF) and Anchor (TRP, TSR, TRF) timestamps. Distance is calculated on Anchor therefore Report message might be employed in order to transfer distance measurement from Anchor back to Tag.

Distance = ToF * speed of light

$$\mathbf{ToF} = ((T_{RR} - T_{SP}) - (T_{SR} - T_{RP}) + (T_{RF} - T_{SR}) - (T_{SF} - T_{RR})) / 4$$





Ranging messages are encapsulated within 802.15.4 frame, see details in picture below:



Raw captured frames between Tag and Anchor in Wireshark are displayed as follows

Invite this dome because _ INVisedady 112.2 (v1.12.2.0, e000fa22 from master 1.12)																											
uwp_twr_demo.pcapng [wiresnark I.12.2 (v1.12.2-u-g898fa22 from master-1.12)]																											
Eile	Edi	it <u>V</u> ie	W	<u>G</u> o	<u>C</u> apt	ure	Anal	yze	<u>S</u> tati	stics	Tel	epho	n <u>y</u>]	ools	Inte	rnals	Help										
D	•	4		Ø.			×	2		4	•	4	• 7	₽			⊕,		Q 🖭	1	Y	-	*	Ħ			
ilter															~	Expre	ssion	Clear	Apply	Save							
	Tir	ne				N	fac Sr	rc Ad	dress	N	lac D	t Ad	dress	Pr	otoco	bl		Length		RSSI			Info				
99		203	. 386	5557	458		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	L4		-83		Data	Dst:	0x0001,	Src:	0x1001
00		204	. 398	8625	383		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	L4		-83		Data	Dst:	0x0001,	Src:	0x1001
01		205	.410	0688	3791		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	14		-84		Data	Dst:	0x0001,	Src:	0x1001
)2		205	.41	5755	5225		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L 5		-90		Data,	Dst:	0x1001,	Src:	0x0001
)3		205	.421	1543	966		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	27		-84		Data,	Dst:	0x0001,	Src:	0x1001
)4		205	. 42	5475	858		0	x00	01		0	x10	01	I	EEE	802	15.4		17		-90		Data	Dst:	0x1001,	Src:	0x0001
)5		206	43	L753	8600		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	L4		-89		Data,	Dst:	0x0001,	Src:	0x1001
)6		206	.43	5820	058		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L 5		-90		Data,	Dst:	0x1001,	Src:	0x0001
07		206	.442	2608	3775		0	x10	01		0	x00	01	I	EEE	802.	15.4	2	27		-88		Data,	Dst:	0x0001,	Src:	0x1001
)8		206	.447	7545	833		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L7		-90		Data,	Dst:	0x1001,	Src:	0x0001
9		207	.452	2816	5750		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	L4		-88		Data,	Dst:	0x0001,	Src:	0x1001
.0		207	.45	883	191		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L 5		-90		Data,	Dst:	0x1001,	Src:	0x0001
1		207	.46	3671	.916		0	x10	01		0	x00	01	I	EEE	802.	15.4	2	27		-88		Data,	Dst:	0x0001,	Src:	0x1001
2		207	.46	3606	5375		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L7		-90		Data,	Dst:	0x1001,	Src:	0x0001
.3		208	.473	3884	808		0	x10	01		0	x00	01	I	EEE	802.	15.4	1	L4		-89		Data,	Dst:	0x0001,	Src:	0x1001
4		208	.478	3951	241		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L 5		-90		Data,	Dst:	0x1001,	Src:	0x0001
. 5		208	.484	1739	983		0	x10	01		0	x00	01	I	EEE	802.	15.4	2	27		-87		Data	Dst:	0x0001,	Src:	0x1001
6		208	.48	9673	8691		0	x00	01		0	x10	01	I	EEE	802.	15.4	1	L7		-89		Data	Dst:	0x1001,	Src:	0x0001
Frame 24: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0 Ethernet II, Src: Microchi_85:73:84 (00:1e:c0:85:73:84), Dst: compalIn_2e:21:5a (f8:a9:63:2e:21:5a)																											
Us	er	Dat	agra	am F	roto	ocol	. 5	rc F	Port	: 1	7754	(1	7754), [st	Port	: 177	54 (1	7754)								
zi	qB	ee E	nca	sul	atio	on P	rot	oco	1. c	han	nel:	1.	Ler	ath:	17												
IE	EE	802	.15	4 0	ata.	DS	t: (0x10	001.	Sr	c: 0	x00	01	-													
Da	ta	(6	byt	25)																							
000	1	F8 a	9 63	3 2e	21	5a	00 1	1e	c0	85	738	4 0	8 00	45	00		c.!z.	s	E.								
10	Ċ	00 40	1 0	5 fa	00	00	ff i	11	8d	8f	0a 0	a Ö	a 02	0a	0a	. M											
20	(Da 01	L 4	5 5a	45	5a	00	39	ea	0a 4	45 5	8 0	3 01	01	73		EZEZ.	9E	xs								
30	1	54 00		00	00	00	cd 1	19	6b	81	52 0	00	0 00	cc	06	•••		. K.R	• • • • •								
+0	5	04 00	00	00	00	00	00 0	30	00	11.	41 ð	0 0	T Ca	ae	UT.	•••		A									



TWR Wireshark plugin which is equipped with UWB Sniffer might further dissect those frames. Payload from frame is decoded as Poll, Response, Final or Report message with calculated distance.

										ι	wb.	_twr_d	emo	.pcapr	ng [Wire	shark 1	.12.2	(v1.1	2.2-0-g898t	fa22 f	rom master-1.12)]
<u>F</u> ile	Ed	it <u>V</u> i	ew <u>G</u> o	Capt	ure	Analyze	Stati	stics	Telep	ohony	Τo	ols <u>I</u> nt	ternal	s <u>H</u> elp)						
۲	۲					× 2	0	, \Leftrightarrow		4	T :	₽ [. €		•	X D	8 🐔	% 🕱		
Filter	•[~	Exp	ression	. Clear	Apply S	ave				
No.	Ti	me			M	lac Src A	ddress	Ma	ac Dst	Addre	ss	Protoco	bl		Length	RSSI	Calo	ulated	Distance		Info
203		205	.4215	43966		0x1	001		0x	0001		Decav	ave	TWR	27	-84	1 . (111)				Final Message
204		205	. 4264	75858		0x0	001		0x	1001		Decav	ave	TWR	17	-90	0		0.141		Report Message
205		206	.4317	53600		0x1	001		0x	0001		Decav	ave	TWR	14	-89	9				Poll Message
206		206	. 4368	20058		0x0	001		0x	1001		Decav	ave	TWR	15	-90)				Response Message
207		206	.4426	08775		0x1	001		0x	0001		Decav	ave	TWR	27	-88	B]				Final Message
208		206	.4475	45833		0x0	001		0x	1001		Decav	ave	TWR	17	-90	0		0.201		Report Message
209		207	. 4528:	16750		0x1	001		0x	0001		Decav	ave	TWR	14	-88	8				Poll Message
210		207	.4578	83191		0x0	001		0x	1001		Decav	ave	TWR	15	-90)				Response Message
211		207	.4636	71916		0x1	001		0x	0001		Decav	ave	TWR	27	-88	8 () () ()				Final Message
212		207	.4686	06375		0x0	001		0x	1001		Decav	ave	TWR	17	-90	0		0.145		Report Message
213		208	.4738	84808		0x1	001		0x	0001		Decav	ave	TWR	14	-89	9				Poll Message
214		208	.4789	51241		0x0	001		0x	1001		Decav	ave	TWR	15	-90)				Response Message
215		208	.4847	39983		0x1	001		0x	0001		Decav	ave	TWR	27	-87	7				Final Message
216		208	.4896	73691		0x0	001		0x	1001		Decav	ave	TWR	17	-89	9		0.223		Report Message
217		209	. 4949	49808		0x1	001		0x	0001		Decav	ave	TWR	14	-88	В				Poll Message
218		209	. 5000	16266		0x0	001		0x	1001		Decav	ave	TWR	15	-90)				Response Message
219		209	. 5058	04991		0x1	001		0x	0001		Decav	ave	TWR	27	-88	8				Final Message
220		209	. 51074	42991		0x0	001		0x	1001		Decav	ave	TWR	17	-89	9		0.16		Report Message
<		210	F4 CA-	14005		A4	104		A	0001		·····		-	**	~ ~ ~	•				n-11
	am	e 24	· 91	hvtes	on	wire (728	hits) 0	1 hv	tes	cant	ured	(728	hits)	on int	erfa	ce O			
E E1	he	rnet	TT.	Src:	Micr	ochi 8	5:73	:84	(00:	1e:c	0:8	5:73:	84).	DST:	Compal	Tn 2e:	21:5	a (f8	:a9:63:2e	:21:5	ja)
TI E	nte	rnet	Prot	ocol	Vers	ion 4.	Src	: 10	.10.	10.2	(1	0.10.	10.2). DS	t: 10.1	0.10.1	(10	.10.1	0.1)		
	er	Dat	agram	Prot	ocol	Src	Port	. 17	754	(177	54)	DST	Por	t · 17	754 (17	754)	(10				
	IOR	ee E	ncansi	lati	on P	rotoco		hann	-1.	1 1	eng	th. 1	7		1.24 (11						
		802	15 4	Data	De	t · Ovi	001	Src	. 0	0001	cing										
		wave	TWR	Repo	rt M	essane		JIC													
-	##	Tec	ting .	##	H	coodye	- NOUCHOU														
	E	ncti	on co	de · P	enor	t Mess	ane	(0x2	a)												
	Ca	lcul	ated	Dista	nce:	0.141	000	mete	rs												
0000)	f8 a	9 63 2	2e 21	5a	00 1e	c0	85 7	3 84	08	00	45 00		.c.!z	s.	E.					
0010		00 4	d 05 f	Fa 00	00	ff 11	8d	8f 0	a Oa	0a	02	0a 0a		м							
0020		0a 0	1 45 5	5a 45	5a	00 39	ea	0a 4	5 58	03	01	01 73	•	.EZEZ	.9EX	s					

5.1 Wireshark dissector for Decawave Two Way Ranging

- a. Download Decawave TWR plugin.
- Extract and copy plugin to the Wireshark plugin folder. Windows c:\Program Files\Wireshark\plugins\1.x.x\, Linux /usr/local/lib/wireshark/plugins/1.x.x/.
- c. Start Wireshark. menu Analyze -> Enabled Protocols (CTRL+SHIFT+E)
- d. Check Decawave-TWR
- e. Apply, OK.



UWB Sniffer

Sewio provides the enclosed product under the following conditions:

This UWB Sniffer is intended for use for ENGINEERING DEVELOPMENT, DEMONSTRATION, OR

EVALUATION PURPOSES ONLY and is not considered by Sewio to be a finished end-product fit for general consumer use. Persons handling the product(s) must have electronics training and observe good engineering practice standards. As such, the goods being provided are not intended to be complete in terms of required design-,marketing-, and/or manufacturing-related protective considerations, including product safety and environmental measures typically found in end products that incorporate such semiconductor components or circuit boards. This UWB Sniffer does not fall within the scope of the European Union directives regarding electromagnetic compatibility, restricted substances (RoHS), recycling (WEEE), FCC, CE or UL, and therefore may not meet the technical requirements of these directives or other related directives.

The user assumes all responsibility and liability for proper and safe handling of the goods. Further, the user indemnifies Sewio from all claims arising from the handling or use of the goods.

EXCEPT TO THE EXTENT OF THE INDEMNITY SET FORTH ABOVE, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES.

Sewio assumes no liability for applications assistance, customer product design, software performance, or infringement of patents or services described herein.

No license is granted under any patent right or other intellectual property right of Sewio covering or relating to any machine, process, or combination in which such Sewio products or services might be or are used.

FCC Warning. This UWB Sniffer is intended for use for ENGINEERING DEVELOPMENT, DEMONSTRATION, OR EVALUATION PURPOSES ONLY and is not considered by Sewio to be a finished end-product fit for general consumer use. It generates, uses, and can radiate radio frequency energy and has not been tested for compliance with the limits of computing devices pursuant to part 15 of FCC rules, which are designed to provide reasonable protection against radio frequency interference. Operation of this equipment in other environments may cause interference with radio communications, in which case the user at his own expense will be required to take whatever measures may be required to correct this interference.