

Lab 2: Decrypt Z-Wave RF Frames using the Zniffer

This hands-on exercise will demonstrate how to decrypt Z-Wave RF frames using the Z-Wave Zniffer tool.

This exercise is part of the series "Z-Wave 1-Day Course".

- 1: Include using SmartStart
- 2: Decrypt Z-Wave RF Frames using the Zniffer
- 3A: Compile Switch On/Off and Enable Debug
- 3B: Modify Switch On/Off
- 4: Understand FLiRS devices

KEY FEATURES

- Decrypt Z-Wave RF Frames
- Learn to use Z-Wave Zniffer tool
- Introduction to Z-Wave Command Classes.

1 Introduction

In this exercise, we will use the Z-Wave Zniffer tool to decrypt the RF traffic when knowing the security keys for the network.

We will decrypt Z-Wave frames and get a basic understand of the Z-Wave Command Classes.

1.1 Hardware Requirements

- 1 WSTK Main Development Board
- 1 Z-Wave Radio Development Board: ZGM130S SiP Module
- 1 UZB Controller
- 1 USB Zniffer

1.2 Software Requirements

- Simplicity Studio v4
- Z-Wave 7 SDK
- Z-Wave PC Controller
- Z-Wave Zniffer



Figure 1: Main Development Board with Z-Wave SiP module

1.3 Prerequisites

You need to have setup a Z-Wave network with a Controller and a Switch On/Off slave device.

For instructions in how to setup the network, refer to the previous exercise "1 Include using SmartStart".

2 Capture RF Packages using the Zniffer

In the previous exercise "1 Include using SmartStart", we learned how to include a device using SmartStart and we tested the basic functionality using the PC Controller.

2.1 Setup Zniffer

Now, let's use the Zniffer to see which frames are being sent to turn on and off the LED.

- 1. Make sure your Zniffer is plugged into your PC and open the Z-Wave Zniffer tool from Simplicity Studio Tools menu.
- 2. Select the COM port by clicking on the icon 3 next to Port. This will search for connected Zniffers.
- 3. Select the COM port in the drop down menu.
- 4. Select the Frequency by clicking on the icon 2 next to Frequency.
- 5. Select the Frequency that matches the frequency you programmed your device with. These exercises uses "EU".
- 6. Start a new Trace ▶.

The Zniffer tool is now ready and listening for Z-Wave RF Traffic.

76 C	\Users\	almun	dha\AppD	ata\Loc	al\Temp\;	nf_data.	zif - Z-	Wave Zr	hiffer														×
Eile	Edit	View	Captu	ure I	ools <u>H</u>	elp																	
		8	Ş I			5 <	> E	ا ب	٥		Ξ Τ χ Τ	Zoom: 100%	. ± :		nt: DM 31 (v2.5!	. 0	Freque EU	тсу:					
Line	Ŧ	Date	Time		Y Spee	d RSS	I Ch	Delta	Y Sro	T Ds	t T Home	T Data	T App	plicatio	n		Ŧ	Hex Data					
																						_	
rame	5:0(0)	frames/	sec; 0 B/s	ec) Li	ne: 0 Se	ected Co	ount: C), Timesp	an: 0 m	s				Is F	iltered: False Fi	Itered Cou	unt: 0 P	ort: COM 3	1 (v2.55 Z	W0500), 2	30400 kbp	s Freque	ency: E

Figure 2: Zniffer Setup and Listening for Z-Wave Traffic

You might see other traffic, despite you are not sending any to your device. Currently, the Zniffer is configured for listening for any traffic in the selected region. We need to filter the trace by "Home ID" to only show traffic from your network.

- From the PC Controller, find the "Home ID" in the "Network Management" tab.

 In Figure 3, the example HomeID is E2 16 BB FE.
- 2. Knowing the Home ID, click the small icon **I** next to "Home" in the Zniffer. Refer to Figure 4.
- 3. Write the Home ID in this field and click OK.
- 4. The green icon now turns red **T** symbolizing the Zniffer is filtering on Home Id.



Figure 3: Home ID from PC Controller

File	Edit View	Capture	Tools Help	<>>	ے ا	0	₫ Т . Т	Zoom:	± ⇒	Port:	. 0	Frequency:		
line	T Date	Time	▼ Speed	RSSI Ch	Delta	T Src 1	Dst T Home	T Data	Y Applicat	tion		T Hex Data		
21	Home Id:	E2 16	BB FE			 Show 	Hide A22DE5	Singlecast	Basic Get			F4A22DE50141040C0420020F		
3	Use the "	?' character to	allow any byt	e in this p	osition		A22DE5	Singlecast	Singlecast Basic Report F4A22DE50441860D012003008/				8D	
4	Use ';' ch	aracter to delir	nit values					CRC_ERRC				F4A22DE40103060A046B		
5							AZZDE5	Singlecast	Basic Get			F4A22DE50141050C08200202		
6						-		CRC_ERRC				F48225ED0841020D0120034B	4E	
7	07.02.19	13:16:13.571	40Kbit/s	51 1	10	1 8	F4A22DE5	Ack				F4A22DE50103020A0863		
8	07.02.19	13:16:13.586	6 40Kbit/s	50 1	7	0		CRC_ERRC				F4A22DE50841030D01200349	4E	
9	07.02.19	13:16:13.588	40Kbit/s	52 1	10	1 8	F4A22DE5	Ack				F4A22DE50103020A0863		
_														_

Hint If you press on "Enter" on the keyboard, instead of clicking OK in the pop-up box, the filter is not applied. This means, the

symbol will not turn red. Turn on the filter by clicking on Toggle Filter

in the menu bar.

2.2 Update Zniffer Nonce and SPAN Table

Nonce is only exchanged once during inclusion and is used to calculate subsequent SPANs in order to prevent replay attacks.

SPAN becomes out of sync if the message did not reach the destination. A new Nonce must then be requested to update the SPAN table.

As such; In order to decrypt a Z-Wave RF frame you need two things:

- The security keys for the network
- The Nonce key/SPAN table

This section will introduce how to add this information to the Zniffer so it can decrypt the individual frames.

Hint: More information on the key exchange can be found the Knowledge Base:

Secure S2 key exchange methods during inclusion

If a trace was started during inclusion, the trace will already contain the Nonce key and thus be able to calculate the SPANs. However, in this exercise we have not the inclusion process in our Zniffer trace and therefore we must provide the Nonce key to the Zniffer.

- 1. Make sure the Zniffer is still tracing as instructed in section 2.1.
- 2. In the PC Controller, click on Reset SPAN.
- 3. In the PC Controller, click on Basic Set ON. This will send a command to the device, which then triggers a reset of SPAN.
- 4. In the PC Controller, click on Basic Set OFF to turn off the LED again.



Figure 5: Reset SPAN in PC Controller

Return to the Zniffer tool and notice the following:

- A "Nonce Get" and a response "Nonce Report' is shown.
- Some encrypted S2 Messages that we cannot yet decrypt.

```
C:\Users\almunkha\AppData\Local\Temp\znf_data.zlf - Z-Wave Zniffer
                                                                                                                                                             X
<u>File Edit View Capture Tools H</u>elp
                                                                            Zoom: 100% - 1 = Port: COM 31 (v2.5! - 0) Frequency: 0
 ■■日戸 ▶ || ■ ひ 小目 ↩ ◘ ① 岳 🔭 🍸
        T Date Time
                             T Speed RSSI Ch Delta T Src T Dst T Home T Data T Application
                                                                                                                       T Hex Data
Line
        07.02.19 14:58:42.122 40Kbit/s 78 1 356 1 2
                                                                   E216BBFE Singlecast S2 Nonce Get
                                                                                                                       E21688FE01410000029F0174E6
        07.02.19 14:58:42.129 40Kbit/s
                                       65
                                                                   E216BBFE Ack
                                                                                                                       E21688FE02038D0A01C9
                                                                  E2168BFE Singlecast S2 Nonce Report
7
                                                                                                                      E21688FE02410D1E019F02AF01A92721D46429EE1C45496
        07.02.19 14:58:42.140 40Kbit/s 77 1 6
                                                           1
                 14:58:42.145 40Kbit/s 66
                                                                   E216BBFE Ack
                                                                                                                       E21688FE01038D0A02C9
        07.02.19
                                           1 11
                                                            2
                                                     1
                                                                                                                       E21688FE01410E28029F03750112412738AE36EDE03CA633
        07.02.19 14:58:42.166 40Kbit/s
                                       78
                                          1 12
                                                           2
                                                                   E216BBFE Singlecast S2 Message Encapsulation: Span
        07.02.19 14:58:42.171 40Kbit/s 65
                                           1 14
                                                                   E21688FE Ack
                                                                                                                       E21688FE02038E0A01CA
10
                                                     2
                                                           1
                 15:00:15.016 40Kbit/s
                                      77
                                                                   E216BBFE Singlecast S2 Message Encapsulation
                                                                                                                       E21688FE01410F19029F03760051168E018673355DC13619
52
        07.02.19
                                              1895
                                                                  E21688FE Ack
                                                                                                                       E21688FE02038F0A01C8
53
     07.02.19 15:00:15.022 40Kbit/s 82 1 10 2 1
Singlecast
                                      Command Class Security 2 ver.1
                           E2 16 BB FE S2 Nonce Report
  Home ID:
  Source Node ID:
                           2
                                         Sequence Number:
                                                             OxAF
                                                             0x01
 Properties1:

    Properties1:

                                        SOS:
   Header Type:
                            0x01
                                                              true
   Speed Modified:
                             false
                                          MOS:
                                                              false
   Low Power:
                            false
                                          Reserved:
                                                              0
                                         Receivers Entropy Input: A9 27 21 D4 64 29 EE 1C 45 49 62 4A DE 9E DD FA
   Ack:
                             true
   Routed:
                             false

    Properties2:

   Sequence Number:
                            13
E2 16 BB FE 02 41 0D 1E 01 9F 02 AF 01 A9 27 21 D4 64 29 EE 1C 45 49 62 4A DE 9E DD FA AB
Frames: 64 (0 frames/sec; 42 B/sec) Line: 0 Selected Count: 0, Timespan: 0 ms
                                                                                                  Is Filtered: True Filtered Count: 0 Port: COM 31 (v2.55 ZW0500), 230400 kbps Frequency: EU
```

Figure 6: SPAN Reset and Encrypted S2 messages

The frames we see in the Zniffer are still encrypted. We are still missing the network keys. Return to the PC Controller to find the needed network key.

- You can find the keys in the PC Controller by clicking on the icon 🖸 in the upper right corner.
- Network keys for all security groups are shown in the pop-up window, refer to Figure 7.
 - o **SO**
 - o S2 Unauthenticated
 - o S2 Authenticated
 - o S2 Access
- Since our device is included as S2 Authenticated using the DSK, we will be needed in S2 Authenticated key.
 In Figure 7, the example key is: D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3
- Click on the "Copy to Clipboard"

Hint: More information on the security groups can be found the Knowledge Bases:

Is S2-AccessControl more secure than S2-Authenticated?

Why use S2-Unauthentucated?

Lab 2: Decrypt Z-Wave RF Frames using the Zniffer Capture RF Packages using the Zniffer

Kecurity Setting	5		_		×
Pause					
Enable S0; 🗹 Ei	able S2 Unauthenticated; ☑ Enable S2 Auther	ticated; 🗹 Enable S2 Access; 📋 Join with CSA			
Network Key S0	AF E8 09 D0 38 81 59 88 A2 68 9E 84 B2 12 0E	0 02 Override 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
Unauthenticated	4B 33 6E 9B CC 48 54 98 12 3A 84 5F 90 34 2A	30 Override 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
Authenticated	D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7	B E3 Override 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
Access	1C 67 FA B7 22 F9 07 AF 59 3D CB 3E BB C4 8	B B7 Override 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
Last used Temp	2B 57 DE 1D EA 67 89 1C 25 D5 1C E6 40 42 6	D 61 0			
S0 Test Scheme S2	Test Scheme				
Enable security t	est schema		Save	Load	
– Security parameter	s overrides				
Enabled	Parameter Name	Value			
Test Span	.				
Clear	Delete Set / Add				
– Message overrides					
Enabled	Frame Delay Multicast Broadcast End	crypted Temp Network Key	Command		
Test Frame		KEXGet		•	
Command:		00 00 00 00			
Delay (sec):		0			
Is Multicast	-				
	d.				
is encrypte					
Save Security Ke	/s				
to Storage Folde	r:				
			OK Cancel	Ар	ply
	Figure 7: Netwo	ork Settings found in PC Controller			



Figure 8: Enter Network Key in Zniffer

When the key is known, it is time to decrypt the traffic using the Zniffer.

- 1. Click on a S2 Message, refer to Figure 8.
- 2. Click on "Decrypt"
- 3. Paste the network key.
- 4. Click "OK"

With the SPAN synchronization and the network key, the Zniffer can now decrypt the S2 messages.



Figure 9: Messages are now Decrypted using the Zniffer

Notice how the 2 frames contains a Command Class called "Basic", with command "Basic Set" and values "0xFF" (ON) and "0x00" (OFF).

Hint More information on the decrypting Z-Wave frames using the Zniffer be found the Knowledge Base:

Decrypt S2 frames in Zniffer trace

2.3 Using Command Class Binary Switch

When you send a Basic Set Command to the Switch On/Off, it is being mapped to the Binary Switch Command Class by the device. This is a requirement in the Z-Wave Specification for a Device Type of type "Binary Switch".

Refer to Z-Wave specification SDS14224 Z-Wave Plus v2 Device Type Specification.

4.5.9.3 Basic Command Class Requirements

The Basic Command Class MUST be mapped according to Table 17.

Table 17, Binary	Switch	Device	Туре	Basic	mapping
------------------	--------	--------	------	-------	---------

Basic Command	Mapped Command
Basic Set (Value)	Binary Switch Set (Value)
Basic Report (Current Value, Duration)	Binary Switch Report (Value, Duration).

Figure 10: Basic Mapping for Device Type Binary Switch

The reason for this requirement is to ensure all Z-Wave controllers can do basic communication with all Z-Wave devices.

In this section, we will try to turn the LED ON and OFF using the Binary Switch command class.

- 1. In the PC Controller, double click on "25 SWITCH_BINARY" under secure Command Classes in the lower left corner.
- 2. This opens the "Command Classes" view in the PC Controller and selects the Switch Binary Command class.
- 3. Set the Command to "0x01 SWITCH_BINARY_SET"
- 4. Set the "Target Value" to "FF-ON_ENABLE"
- 5. Click "Send".
- 6. Set the "Target Value" to "00-OFF_DISABLE"
- 7. Click "Send".



Figure 11: Command Class View in PC Controller

2.4 Capture RF packages using the Zniffer: Binary Switch Set

Now that we have learned how to send a Binary Switch Set, let's trace the RF communication again to understand which frames are being sent.

- Return to Z-Wave Zniffer tool, which should have been running in the background.
- The trace now contains a Nonce resync, 2 Basic Set frames and 2 Binary Switch Set frames.

76 C:\	Users\almunki	na\AppData\l	.ocal\Tem	p∖znf_d	lata.zlf	- Z-W	/ave Zn	iffer							_		×
<u>F</u> ile	Edit View	<u>C</u> apture	Tools	Help	1		21		6 6	• •	Zoom:	1 =	Port:	P Fr	requency:		
				0	N/		4	9		l× ∎	100% -	<u> </u>	COM 31 (v2.5!	E	u 🗸 🛡 🖕		
Line	▼ Date	Time	▼ Sp	beed	RSSI	Ch [Delta	T Sro	T Dst	▼ Home	🝸 Data	▼ Арр	lication		▼ Hex Data		
1	31.01.19	10:58:31.27	76 100K	Bit/s	84	0	0	1	3	E1CF0181	Singlecast	S2 Non	ce Get		E1CF01810141080E039F018	1533E	
2	31.01.19	10:58:31.28	32 100K	Bit/s	73	0	7	3	1	E1CF0181	Ack				E1CF01810303080B0193BD		
3	31.01.19	10:58:31.29	92 100K	Bit/s	73	0	7	3	1	E1CF0181	Singlecast	S2 Non	ce Report		E1CF01810341091F019F023	801C5D4	932D6C
4	31.01.19	10:58:31.29	97 100K	Bit/s	82	0	8	1	3	E1CF0181	Ack				E1CF01810103090B03C04C		
5	31.01.19	10:58:31.31	16 100K	Bit/s	82	0	14	1	3	E1CF0181	Singlecast	Basic S	et • S2ME: Span		E1CF01810141092C039F038	2011241	9C2868
6	31.01.19	10:58:31.32	21 100K	Bit/s	73	0	10	3	1	E1CF0181	Ack				E1CF01810303090B01A48D		
7	31.01.19	10:58:32.77	77 100K	Bit/s	84	0	1445	1	3	E1CF0181	Singlecast	Basic S	et • S2ME		E1CF018101410A1A039F038	300B882	524B23
8	31.01.19	10:58:32.77	77 100K	Bit/s	73	0	7	3	1	E1CF0181	Ack				E1CF018103030A0B01FDDD		
9	31.01.19	10:58:41.57	75 100K	Bit/s	84	0	8801	1	3	E1CF0181	Singlecast	Switch	Binary Set • S2ME		E1CF018101410B1B039F038	4008A25	F24674
10	31.01.19	10:58:41.58	31 100K	Bit/s	73	0	8	3	1	E1CF0181	Ack				E1CF018103030B0B01CAED		
11	31.01.19	10:58:44.18	37 100K	Bit/s	84	0	2605	1	3	E1CF0181	Singlecast	Switch	Binary Set • S2ME		E1CF018101410C1B039F038	500A702	21818C
12	31.01.19	10:58:44.19	93 100K	Bit/s	74	0	8	3	1	E1CF0181	Ack				E1CF018103030C0B014F7D		
cia ala														de la Piere			
Singled	ast		EA CE (Load	d Keys	S						Command Class SV	NITCH BINA	ary ver.2 Command Class Swi	tch Binai	r y ver
Hon	ne ID:		ETCEC	J1 81	Decry	pted	:						Switch Binary Set		Switch Binary Set		
Sou	rce Node ID:		1		Ne	etwork	k Key: 1	10 86 B	C 8D 71 I	34 F6 03 E1	7C 01 96 E2 F	0 D7 99	larget Value: off	/disable=	0x00 Switch Value: off/o	disable=0)x00
 Prop 	perties1:				Co	ntent	: 2	25 01 0	0 00				Duration: Ins	stantly=0x	00		_
He	eader Type:		0x01		Comn	nand	Class S	Securit	ty 2 ver.1								_
Sp	eed Modified	d:	false		52 M	essag	e Enca	psulat	ion								- 1
Lo	w Power:		false		Se	quen	ce Nun	nber:	0x85								
Ac	k:		true		▼ Pro	operti	ies1:		0x00								
Ro	uted:		false		F	vtens	ion [.]		false								
- Prot	oerties2:																
E1 CF 0	01 81 01 41 0	C 1B 03 9F 0	3 85 00 A	7 02 2	1 81 8	C F6	65 7E 9	8 01 2	B BB BA F	1							
Frames:	: 12 (0 frames,	/sec; 50 B/sec	Line: 0	Sele	cted C	ount:	0, Time	span: 0	ms		1	s Filtered	: False Filtered Count: (0 Port: CO	M 31 (v2.55 ZW0500), 230400 kb	ps Frequ	ency: El
		Fic	ure 1	2: ZI	niffe	er T	race	con	tainin	g Basic	Set and	l Bina	ary Switch Se	et Com	mand Class		

Notice how to Zniffer shows the command class used to transfer data between the PC Controller and the device.

Now try to send a "Switch Binary Get" from the PC Controller, and see the response in the Zniffer.

• What does the response show?

This concludes the tutorial in how to trace and decrypt Z-Wave RF traffic using the Zniffer tool.