DETECT HOME ACTIVITY VIA Z-WAVE SNIFFING

YAYING YE

YUEYANG SUN

UNDER SUPERVISION OF PROFESSOR MANI SRIVASTAVA

INTRODUCTION

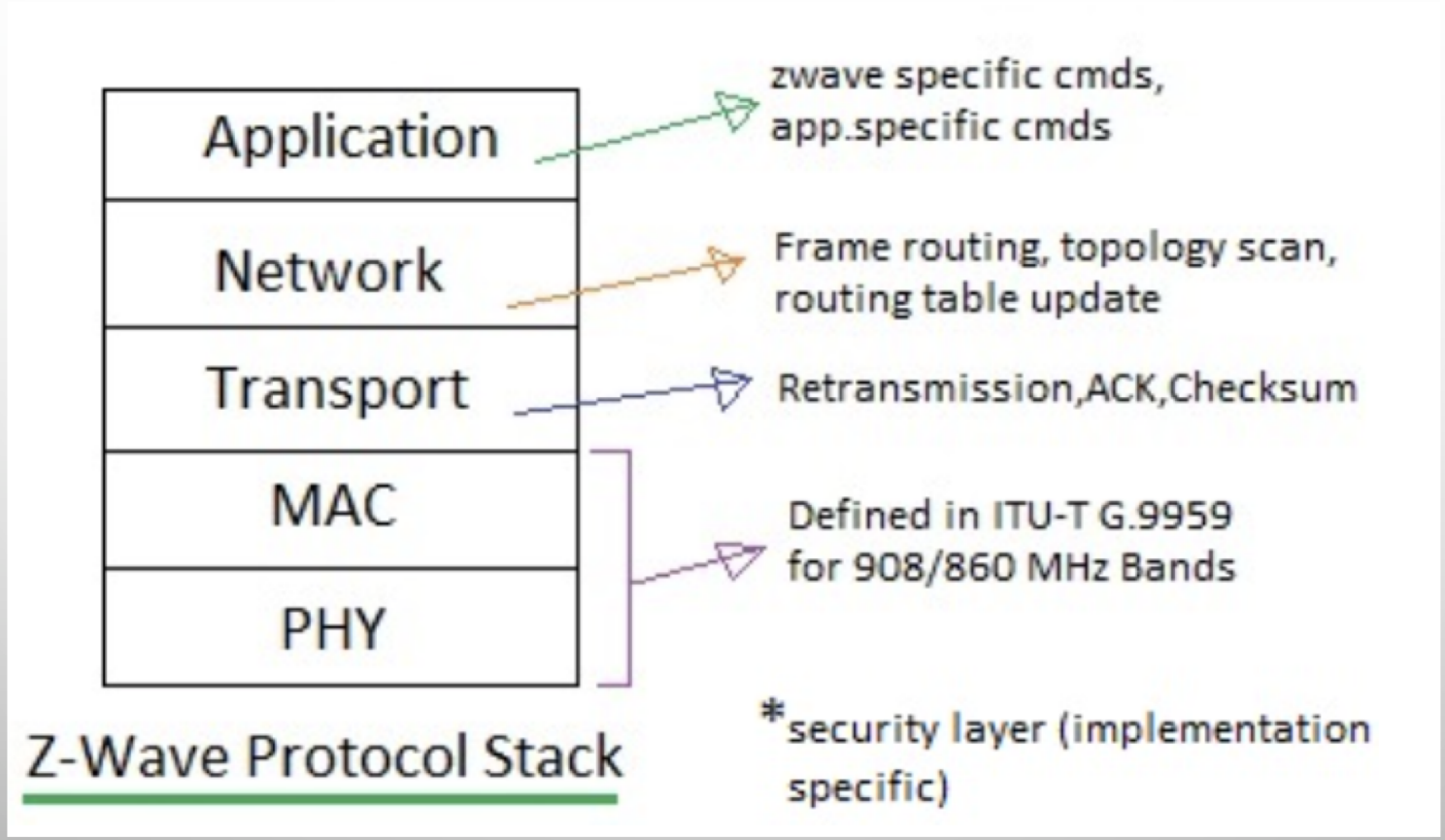
WHAT IS Z-WAVE?

- WIRELESS COMMUNICATION PROTOCOL
- USED FOR HOME AUTOMATION
- OPERATES AT 908.42 MHZ
- RANGE 80 FEET INDOOR AND 300 FEET OUTDOOR

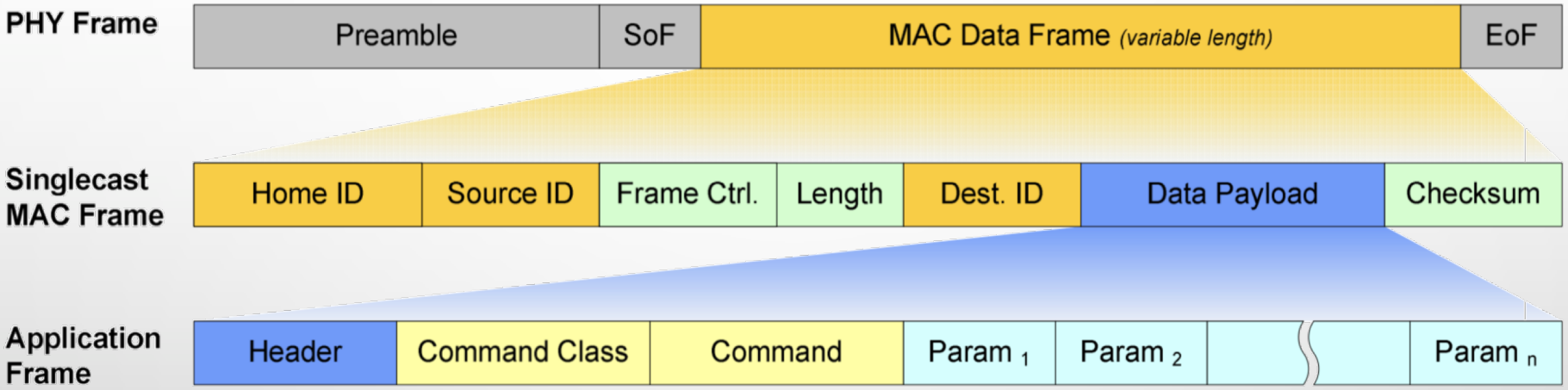
HOW DOES Z-WAVE WORK?

- MESH NETWORK
- ONE PRIMARY CONTROLLER
- UP TO 232 NODES UNDER THE SAME CONTROLLER NETWORK

INTRODUCTION



INTRODUCTION



Z-WAVE FRAME FORMAT IN DIFFERENT LAYERS

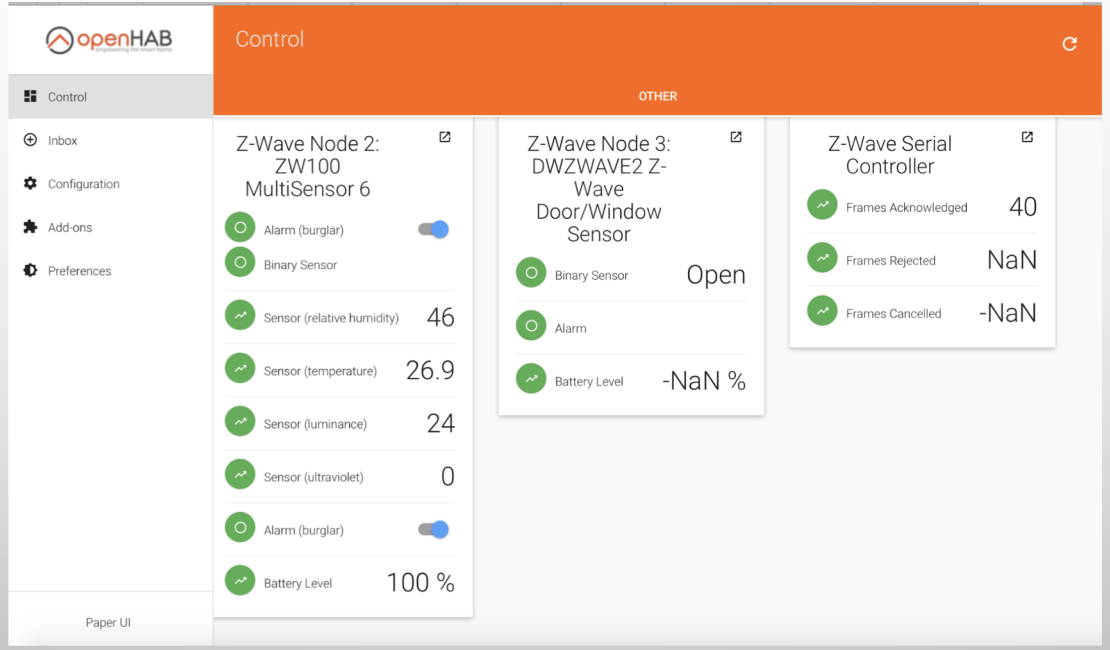
REF: HTTP://WWW.RFWIRELESS-WORLD.COM/TUTORIALS/Z-WAVE-PROTOCOL-STACK.HTML

HARDWARE IMPLEMENTATION

- RTL-SDR
- SENSORS
  - MULTILEVEL SENSOR 6 (ZW100-A)
    - TEMPERATURE SENSOR, LIGHT SENSOR, HUMIDITY SENSOR, VIBRATION SENSOR, UV SENSOR
  - DOOR AND WINDOW SENSOR
    - MOTION BINARY SENSOR
- Z-STICK GEN 5
- ANTENNA: 700 MHZ ~ 1200 MHZ

SOFTWARE

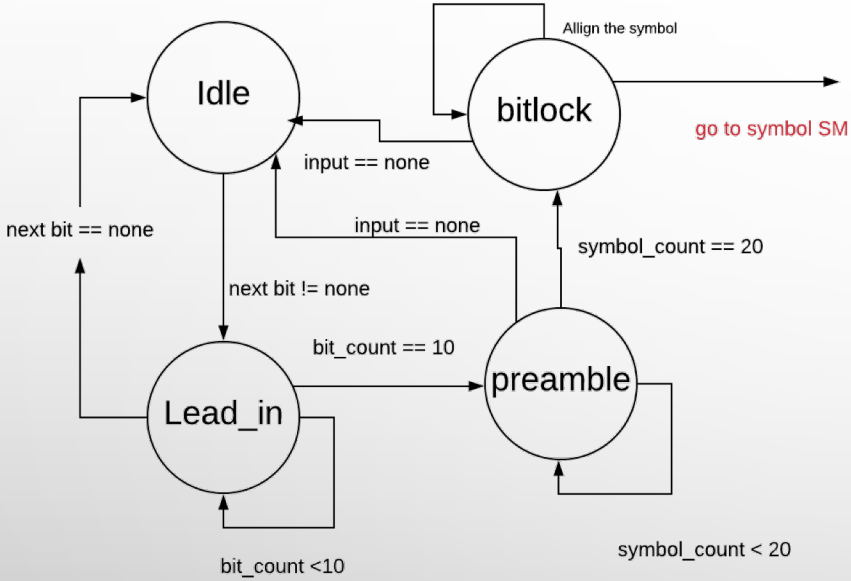
- OPENHAB
  - FOR SENSOR MONITORING AND DATA CHECKING PURPOSE.



CONFIGURATION

- SETUP PARAMETERS
  - OPERATING FREQUENCY: 908.42 MHZ
  - DATA RATE: 40 KBITS/S
  - SAMPLE RATE: 2M S/SEC
  - ENCODING STYLE: NRZ TYPE
- FSK DEMODULATOR

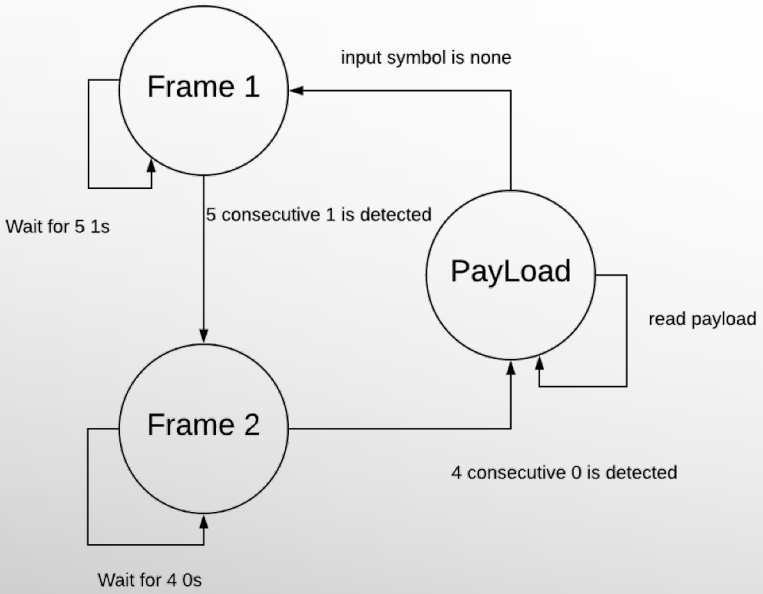
SYNCHRONIZING



SAMPLE STATE MACHINE

- Input bit is none
  Idle state -> Lead_in state
- Preamble is 01010101
  Skip 10 symbols of the preamble
- Calculate sps = sample_count/symbol_count after reading at least 20 preamble
- Skip incomplete symbol -> Symbol SM

DECODE PROCEDURES



Symbol SM

- FRAME 1: DETECT FIRST BYTE OF SOF
- FRAME 2: DETECT SECOND BYTE OF SOF
- READ AND STORE PAYLOAD

COLLECTING DATA ANALYSIS

```
yayings-MacBook-Pro:python yayingye$ python3 predict.py
Found home device:  c3f673a5
It has following node:
Node  03
This Node has the following command class:
Binary Sensor
Notification
Wake Up
Node  01
This Node has the following command class:
Basic
Battery
Powerlevel
Multilevel Sensor
No Operation
Binary Sensor
Node  02
This Node has the following command class:
Notification
Battery
Powerlevel
Multilevel Sensor
```

COMMAND CLASSES AND COMMANDS

SOME EXAMPLE COMMAND CLASSES AND COMMANDS...

Value	Command Class Name
0x71	Notification Command Class
0x80	Battery Command Class
0x31	Multisensor Command Class
0x30	Alarm Command Class
0x73	Powerlevel Command Class
0x00	No Operation Command Class

Multisensor Type Commands	
Value	Type
0x03	Luminance
0x01	Air temperature
0x05	Humidity
0x1b	Ultraviolet
0x00	Door Closed
0xff	Door Open

Command Class	Value	Action
Notification Command Class (0x71)	0x04	get
	0x05	report
Battery Command Class (0x80)	0x02	get
	0x03	report
Multisensor Command Class (0x31)	0x04	get
	0x05	report
Alarm Command Class (0x30)	0x04	get
	0x05	report
powerlevel Command Class (0x73)	0x02	get
	0x03	report

RESULTS AND INTERPRETAT

Temperature	00	Celsius Degree
	01	Farenheit Degree
humidity	00	%
	01	g/(m^3)
Luminance	01	Lux
Ultraviolet	00	UV index

precision(3) + scale(2) + size(3)

```
c3 f6 73 a5 02 41 0c 10 01 31 05 01 22 01 0d 59 00 10 00
[x] HomeId: c3f673a5, SourceNodeId: 2, FC0: 41, FC1: c, FC[speed=0 low_power=0 a
ck_request=1 header_type=1 beaming_info=0 seq=12], Length: 16, DestNodeId: 1, Co
mmandClass: 31, Payload: 05 01 22 01 0d
Temperature: 26.9C
```

22(HEX) - > 001 00 010

```
c3 f6 73 a5 02 41 08 0f 01 31 05 1b 01 00 77 00 00 00
[x] HomeId: c3f673a5, SourceNodeId: 2, FC0: 41, FC1: 8, FC[speed=0 low_power=0
ck_request=1 header_type=1 beaming_info=0 seq=8], Length: 15, DestNodeId: 1, Co
mandClass: 31, Payload: 05 1b 01 00
Ultraviolet: 0UV
```

01(HEX) - > 000 00 001

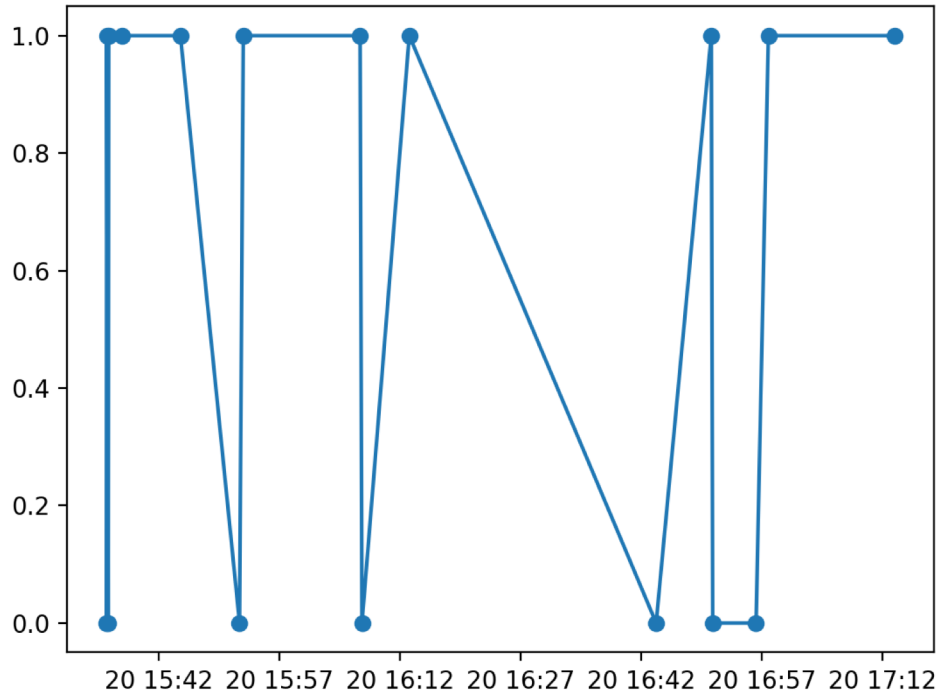
RESULTS AND INTERPRETATION

DOOR/WINDOW SENSOR DATA INTERPRETATION:

```
c3 f6 73 a5 03 41 02 0e 01 30 03 ff fe c0 00 00
[ ] HomeId: c3f673a5, SourceNodeId: 3, FC0: 41, FC1: 2, FC[speed=0 low_power=0 a
ck_request=1 header_type=1 beaming_info=0 seq=2], Length: 14, DestNodeId: 1, Com
mandClass: 30, Payload: 03 ff fe
Door OPEN
```

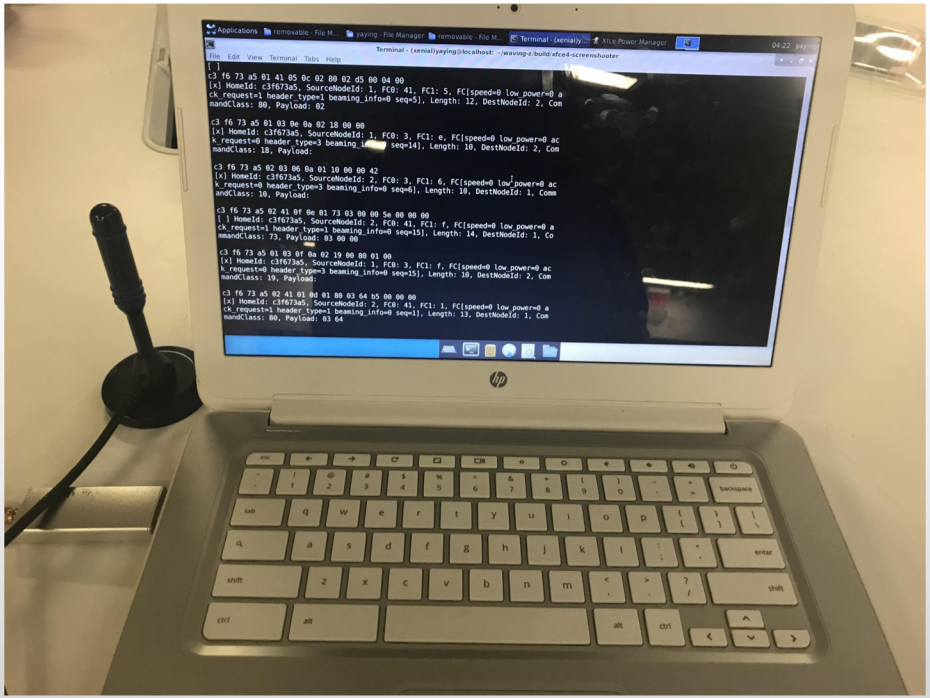
```
c3 f6 73 a5 03 41 02 0e 01 30 03 00 ff 9f 00 20 40 00
[x] HomeId: c3f673a5, SourceNodeId: 3, FC0: 41, FC1: 2, FC[speed=0 low_power=0 a
ck_request=1 header_type=1 beaming_info=0 seq=2], Length: 14, DestNodeId: 1, Com
mandClass: 30, Payload: 03 00 ff
Door CLOSED
```

RESULTS AND INTERPRETATION



DOOR/WINDOW SENSOR DATA RESULTS IN 2.5 HOURS.

DEMO


Terminal - (xenial)yaying@localhost: ~/waving-z/build/xfce4-screenshooter
c3 f6 73 a5 01 41 05 0c 02 80 02 d5 00 04 00
[x] HomeId: c3f673a5, SourceNodeId: 1, FC0: 41, FC1: 5, FC[speed=0 low_power=0 a
ck_request=1 header_type=1 beaming_info=0 seq=5], Length: 12, DestNodeId: 2, Com
mandClass: 80, Payload: 02
c3 f6 73 a5 01 03 0e 0a 02 18 00 00
[x] HomeId: c3f673a5, SourceNodeId: 1, FC0: 3, FC1: e, FC[speed=0 low_power=0 ac
k_request=0 header_type=3 beaming_info=0 seq=14], Length: 10, DestNodeId: 2, Com
mandClass: 18, Payload:
c3 f6 73 a5 02 03 06 0a 01 10 00 00 42
[x] HomeId: c3f673a5, SourceNodeId: 2, FC0: 3, FC1: 6, FC[speed=0 low_power=0 ac
k_request=0 header_type=3 beaming_info=0 seq=6], Length: 10, DestNodeId: 1, Comm
andClass: 10, Payload:
c3 f6 73 a5 02 41 0f 0e 01 73 03 00 00 5e 00 00 00
[ ] HomeId: c3f673a5, SourceNodeId: 2, FC0: 41, FC1: f, FC[speed=0 low_power=0 a
ck_request=1 header_type=1 beaming_info=0 seq=15], Length: 14, DestNodeId: 1, Co
mmandClass: 73, Payload: 03 00 00
c3 f6 73 a5 01 03 0f 0a 02 19 00 80 01 00
[x] HomeId: c3f673a5, SourceNodeId: 1, FC0: 3, FC1: f, FC[speed=0 low_power=0 ac
k_request=0 header_type=3 beaming_info=0 seq=15], Length: 10, DestNodeId: 2, Com
mandClass: 19, Payload:
c3 f6 73 a5 02 41 01 04 01 80 03 64 b5 00 00 00
[x] HomeId: c3f673a5, SourceNodeId: 2, FC0: 41, FC1: 1, FC[speed=0 low_power=0 a
ck_request=1 header_type=1 beaming_info=0 seq=1], Length: 13, DestNodeId: 1, Com
mandClass: 80, Payload: 03 64

FUTURE WORK AND LIMITATION

LIMITATION :

- LIMITATION OF SENSOR TYPE
- SDR MUST BE INSTALLED WITHIN CERTAIN RANGE
- SNIFFING DURATION CAN BE LONGER

FUTURE WORK:

- RESEARCH ON MORE Z-WAVE SENSORS TO BETTER PREDICT HOME ACTIVITIES
- DEVELOP SNIFFING FOR OTHER PROTOCOL E.G. ZIGBEE

CONCLUSION

- MOST OF Z-WAVE ARE NOT ENCRYPTED
- MOST COMMAND CLASSES AND COMMAND INFORMATION CAN BE FOUND FROM OFFICIAL ONLINE DOCUMENTATION
- ADVERSARY CAN EASILY INTERPRET Z-WAVE SIGNAL

QUESTIONS?