XKungfoo 2018
信息安全交流大会

LORA智能水表安全分析

曾颖涛

关于我

360 **Unicorn Team**

专注于使用无线电技术的所有领域的信息安全相关研究，任何使用无线电通信技术的产品，小到射频卡、遥控钥匙，大到无线医疗设备、交通信号灯、智能汽车、卫星通信...团队都会去研究其安全风险，并将形成研究及风险评估报告提供给相关企业、机构及政府部门来加固和阻止未知安全隐患。

神话行动一期学员。曾发现特斯拉、沃尔沃、别克、雪佛兰、等等多款汽车无线车锁程序的多个安全漏洞并被美国Jalopnik汽车评测博客、WIRED、央视等知名媒体报道。 HITB、BlackHat及 DEFCON安全会议演讲者。

国内首本汽车安全书籍《智能汽车安全攻防大揭秘》，
《Inside_Radio_An_Attack_and_Defense_Guide》作者。
HackKEY，Chimera，HackCube等攻防安全演示产品研发者

LORA智能水表架构

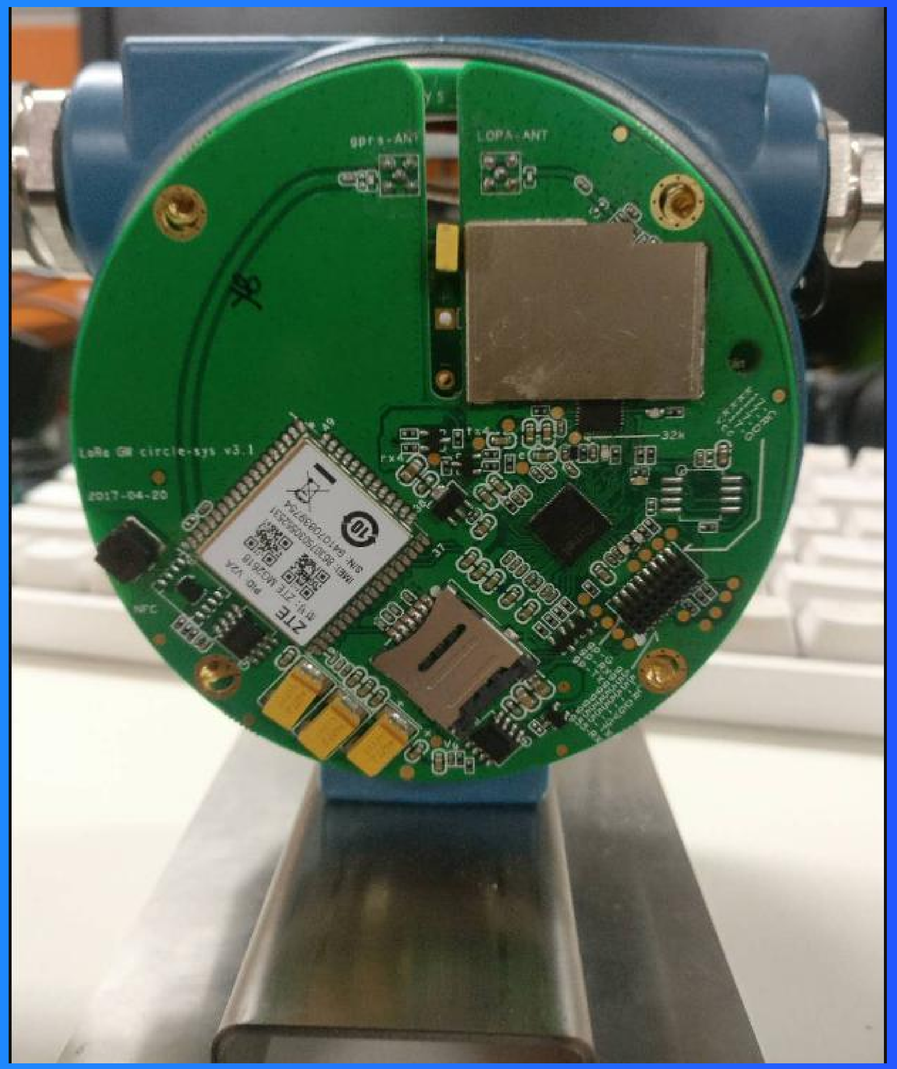

LORA水表
LORA网关
服务器
计费系统


LoRa
LORA
GPRS
WEB
LORA 水表
LORA 网关
服务器
计费系统

生活中见到的场景

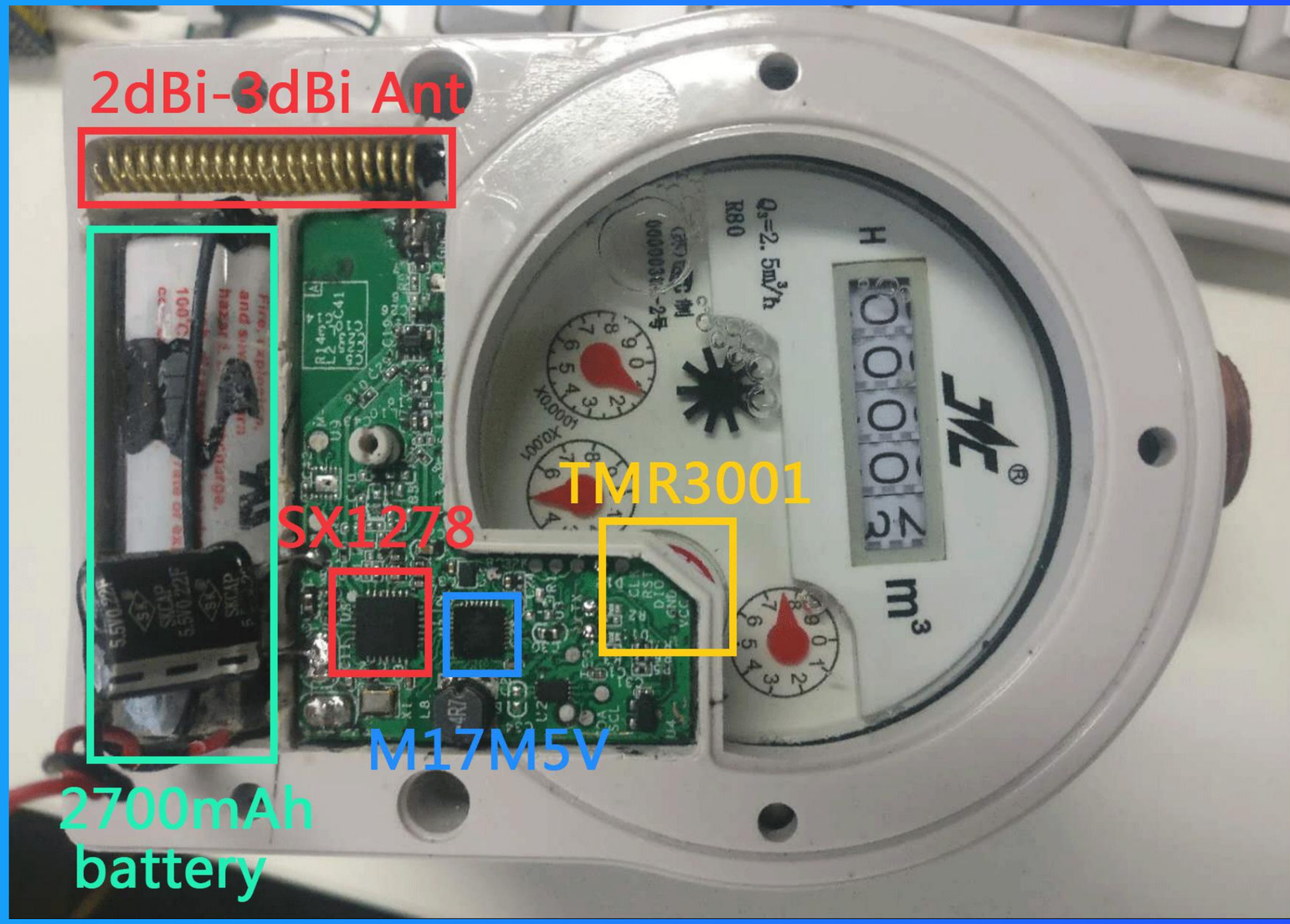
里面长什么样子


Q3=2.5m³/h
R80
m³


gprs-ANT
LORA-ANT
LoRa GR circle-sys v3.1
2017-04-20
ZTE

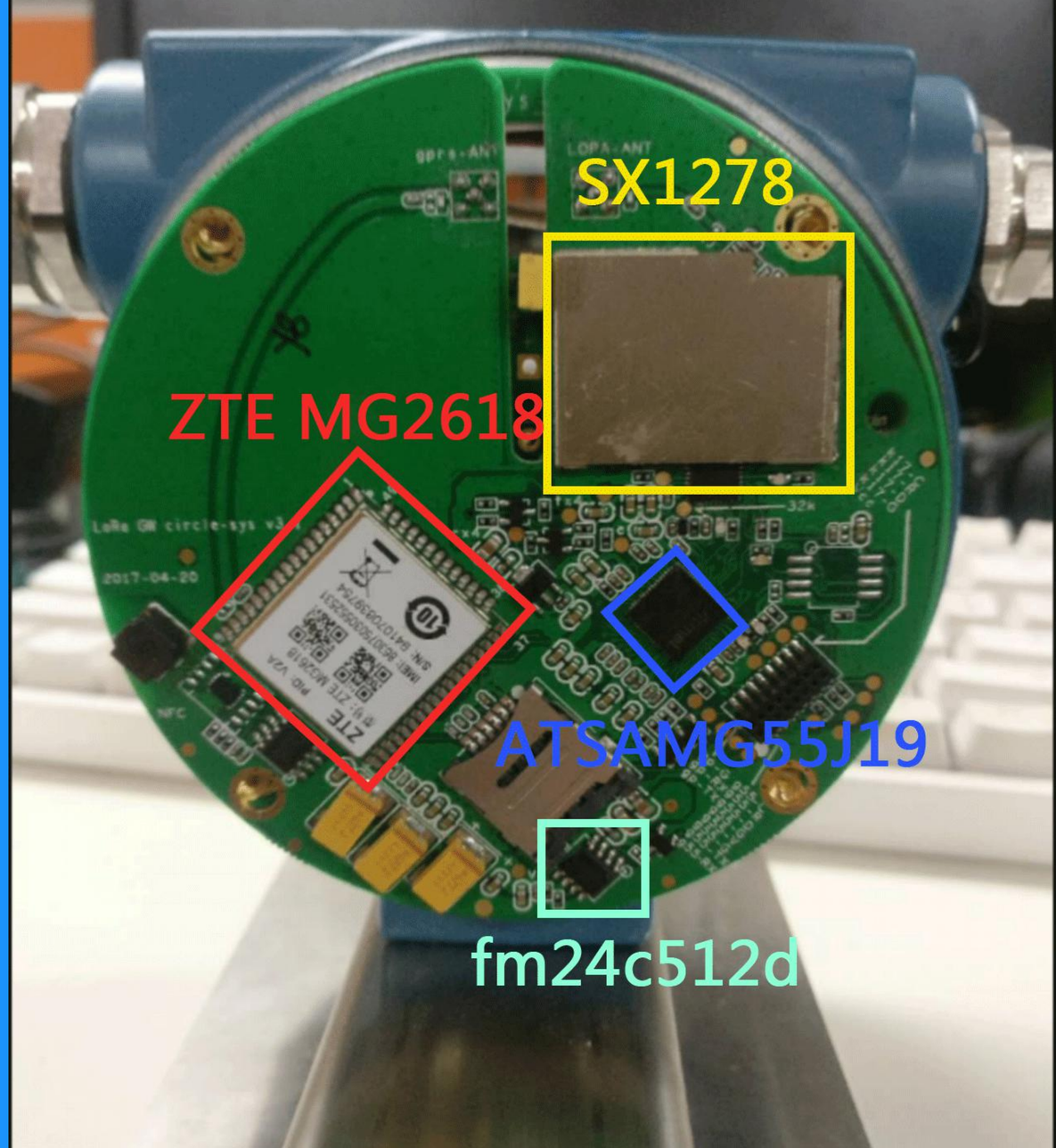
水表硬件拆解

- TMR3001 (磁能传感器)
- M17M5V (NXP MCU)
- SX1278 (LORA)
- 2dBi-3dBi (天线)
- 2700mAh (电池)



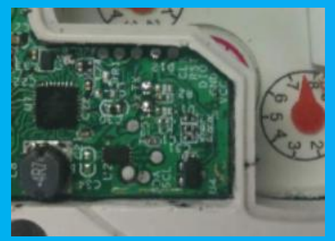
网关硬件拆解

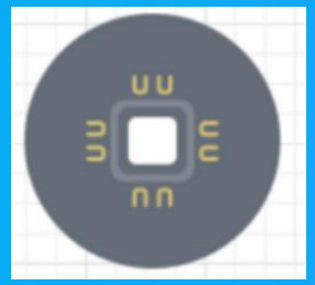
- ZTE MG2618 (GPRS)
- ATSAMG55J19 (MCU)
- SX1278 (LORA)
- fm24c512d (EEPROM)
- RT9048 (稳压芯片)



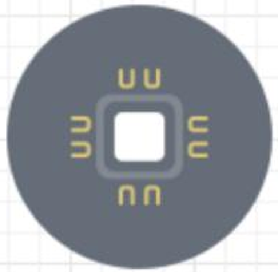
水表如何去读用量？

圆形两极磁铁



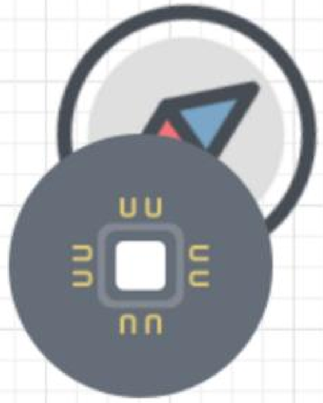


TMR3001
磁性传感器

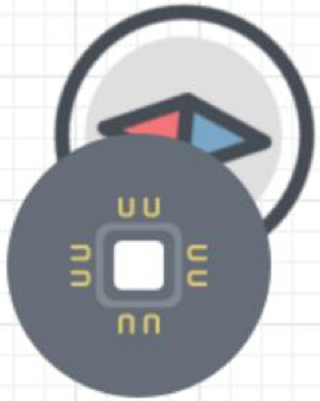


TMR3001
磁性传感器

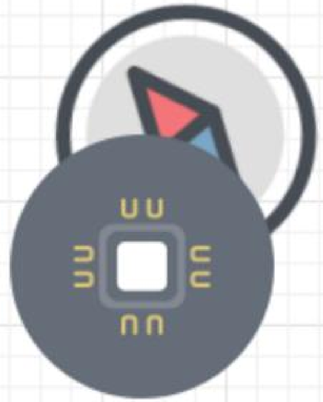
圆形两极磁铁



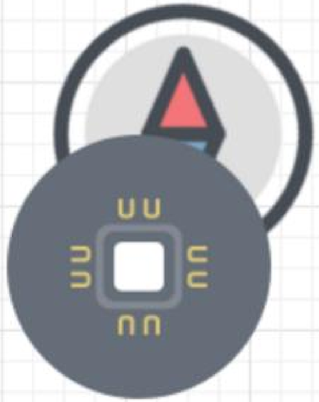
传感器输出电压:
400mv



传感器输出电压:
20mv



传感器输出电压:
-220mv



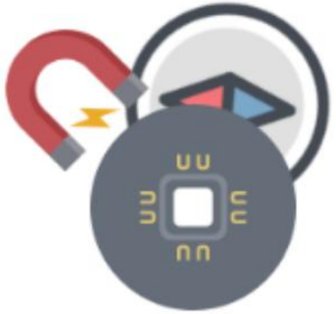
传感器输出电压:
-300mv

针对传感器攻击

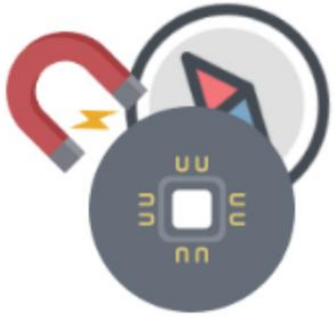
TMR3001
磁性传感器

圆形两极磁铁

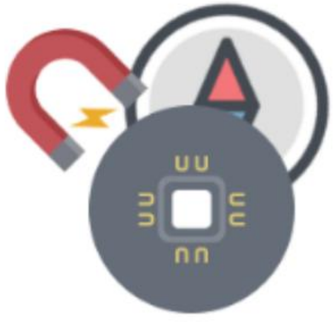
传感器输出电压:
200mv



传感器输出电压:
200mv

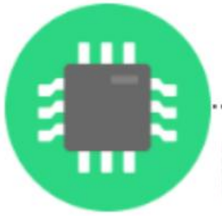


传感器输出电压:
200mv



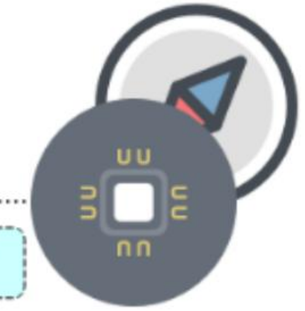
传感器输出电压:
200mv

攻击者

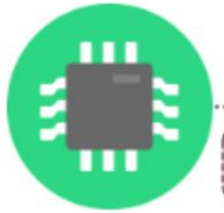


M17M5V
(NXP MCU)

传感器输出电压:
200mv

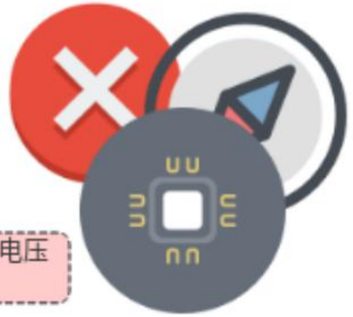


TMR3001
磁性传感器



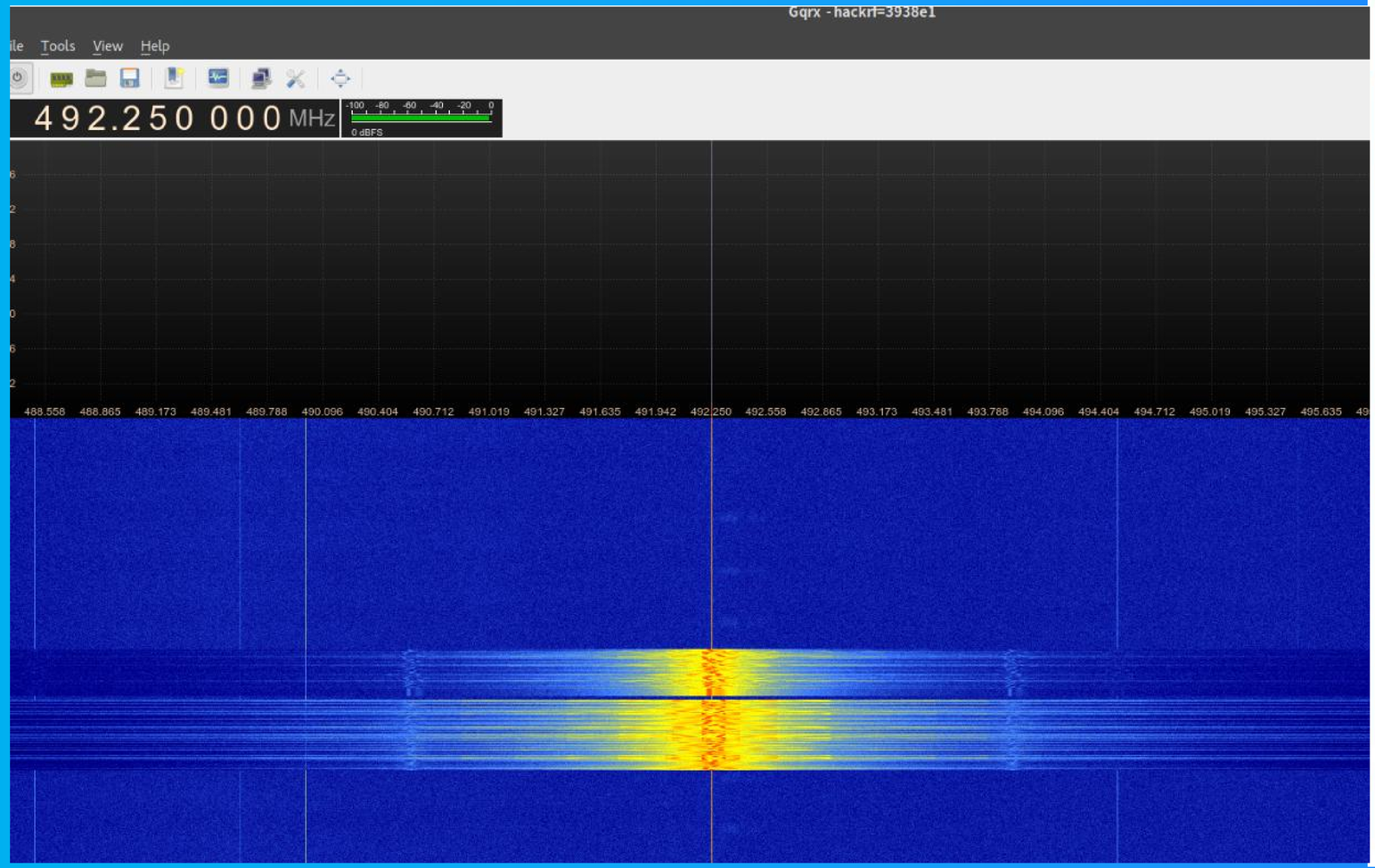
M17M5V
(NXP MCU)

攻击者输入的电压
200mv



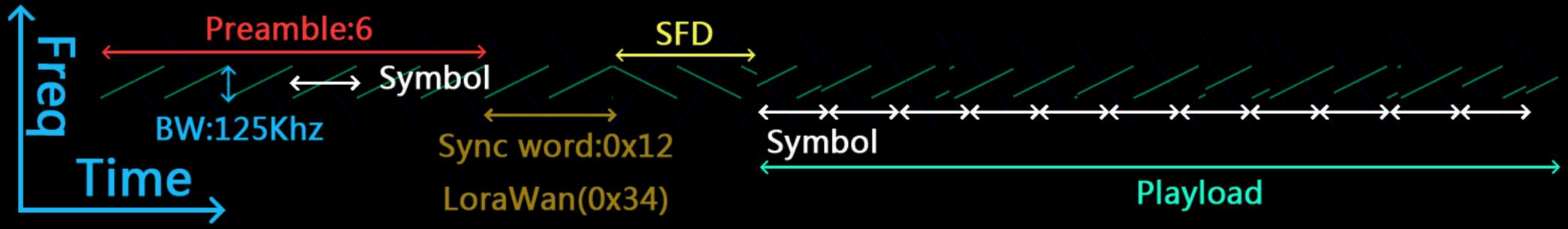
TMR3001
磁性传感器

LORA 射频频率



Countries	Frequency band review	Max. output power
EU	868 MHz	14 dBm
USA	915 MHz	20 dBm
Korea	900 MHz	14 dBm
Japan	920 MHz	
Malaysia	862 to 875 MHz	20 dBm
Philippines	868 MHz	
Vietnam	920 to 925 MHz	
India	865 to 867 MHz	
Singapore	922 MHz	
Thailand	920 to 925 MHz	
Indonesia	922 MHz	
ANZ	915 to 928 MHz	
Taiwan	920 to 925 MHz	
China	470 to 510 MHz	17 dBm

LORA 数据格式



Bandwidth:125Khz(BW)

Preamble:6

Sync word:0x12

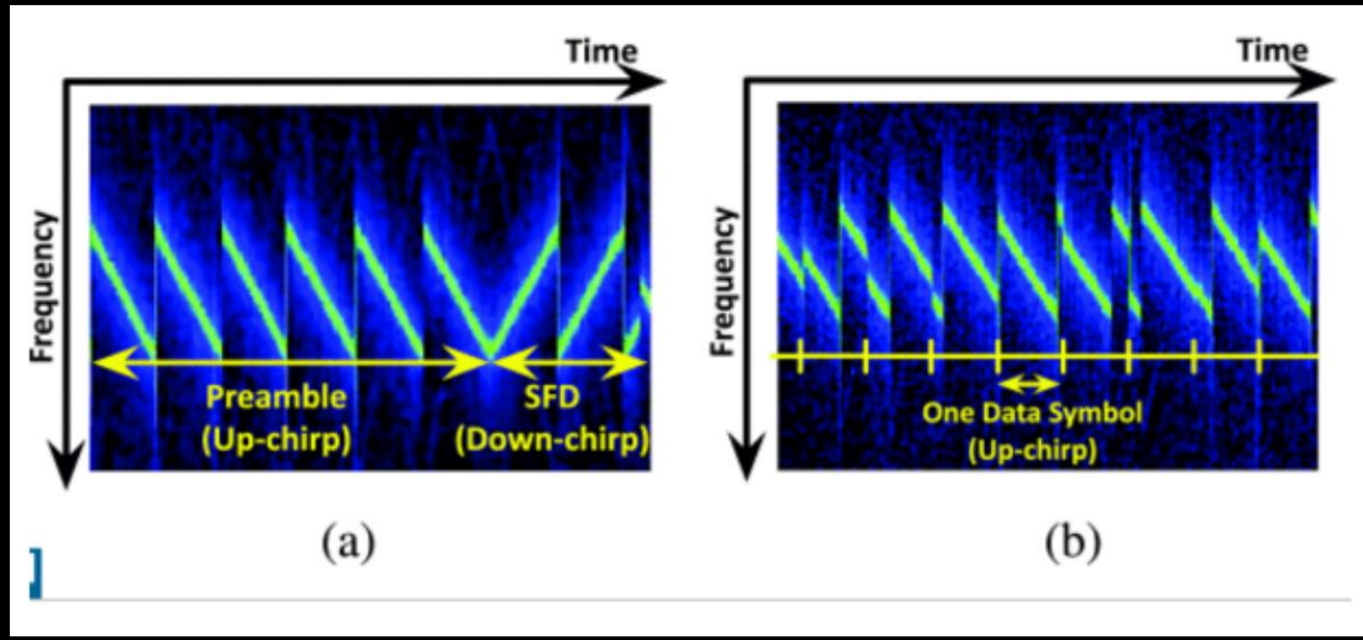
CodingRate:4/5(CR)

Spreading factor:8 (SF)

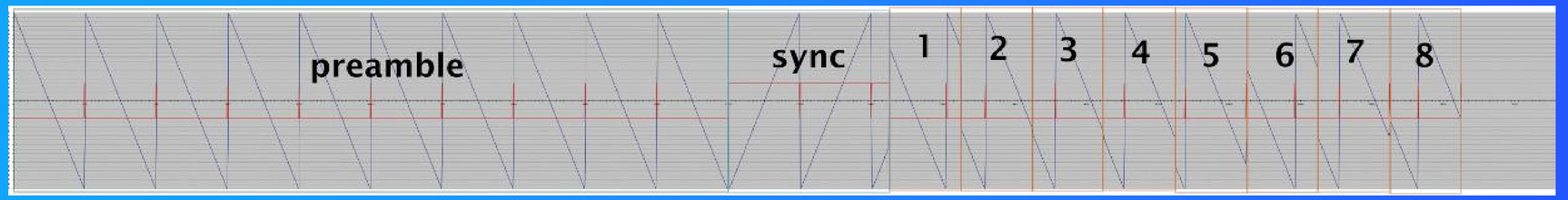
Symbol=BW/(2^SF)

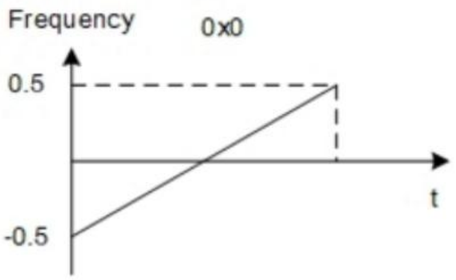
DownChirp

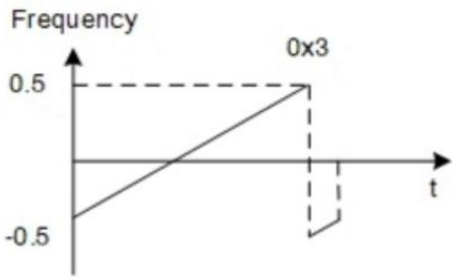
UpChirp

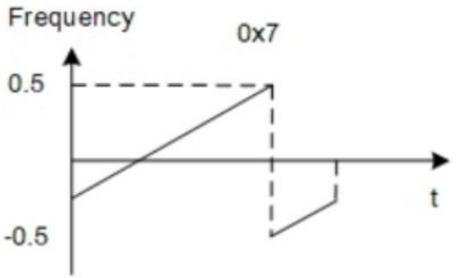


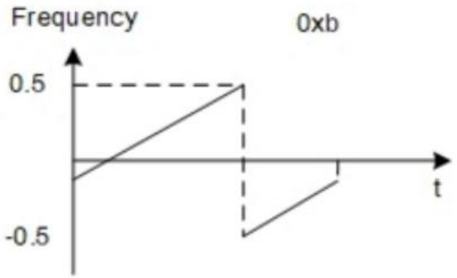
Playload编码

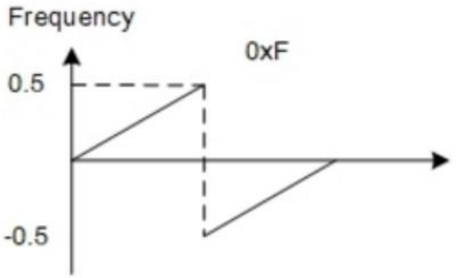






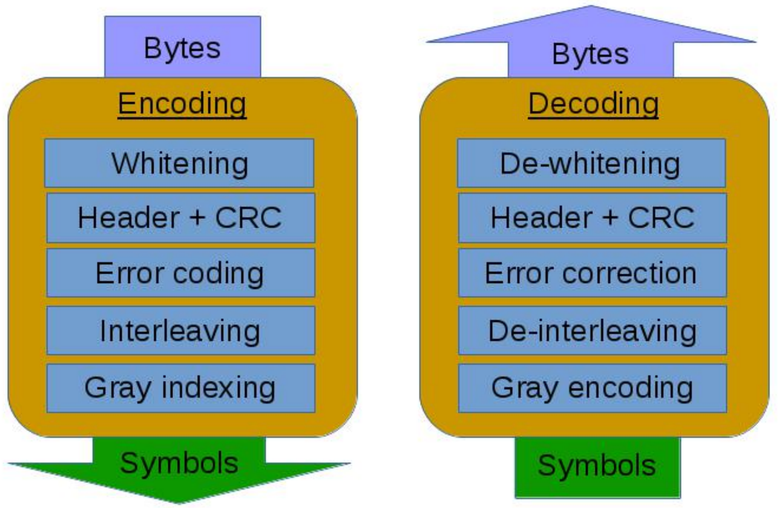






Code rate	Error Correction [bits]	Error detection [bits]
4/5	0	0
4/6	0	1
4/7	1	2
4/8	1	3

Table 2.1: Error correction and detection capabilities of LoRa



帧结构

Chirp 调制

Whitening – 白化

Error encoder – 汉明编码

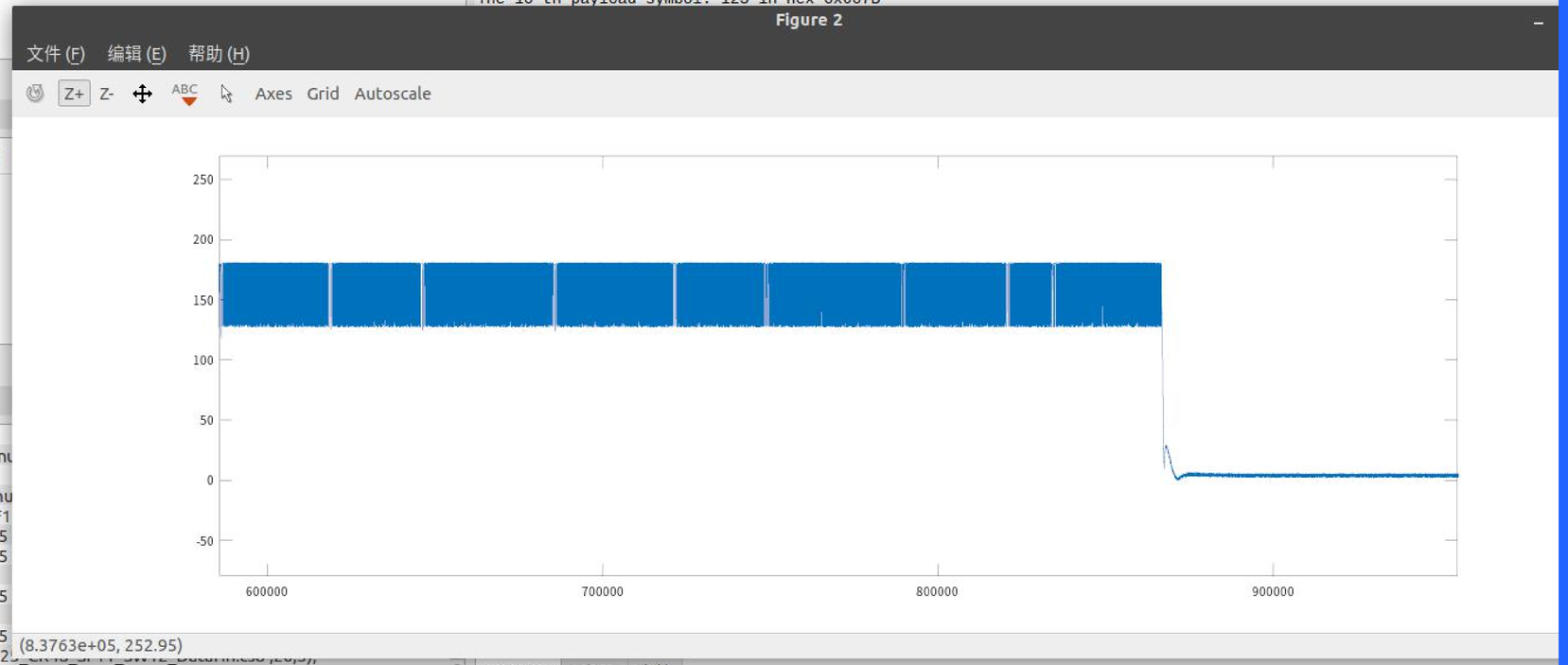
Interleaver – 交织器

Gray码映射

解调LORA信号

WaterMeter_NID1_PL6_BW125_SF11.cs8
SelfGen_PL6_BW125_CR48_SF11_SW12_DataHello.cs8
SelfGen_EnableCRC_PL6_BW125_CR48_SF11_SW12_DataHh.cs8
README.md
lora_sig_demod.m

```
The 1 th symbol peak index: 1
The 2 th symbol peak index: 1
The 3 th symbol peak index: 1
The 4 th symbol peak index: 1
The 5 th symbol peak index: 1
The 6 th symbol peak index: 1
==== Sync Word Part ====
The Sync Word is 0x 1 2
==== Start of Frame Delimiter Part ====
The 9 th symbol peak index: 248
The 10 th symbol peak index: 247
The 11 th symbol peak index: 62
==== Start of Payload Part ====
The 1 th payload symbol: 1363 in Hex 0x0553
The 2 th payload symbol: 1207 in Hex 0x04B7
The 3 th payload symbol: 1119 in Hex 0x045F
The 4 th payload symbol: 319 in Hex 0x013F
The 5 th payload symbol: 1227 in Hex 0x04CB
The 6 th payload symbol: 1903 in Hex 0x076F
The 7 th payload symbol: 1971 in Hex 0x07B3
The 8 th payload symbol: 1715 in Hex 0x06B3
The 9 th payload symbol: 1879 in Hex 0x0757
The 10 th payload symbol: 123 in Hex 0x007B
```



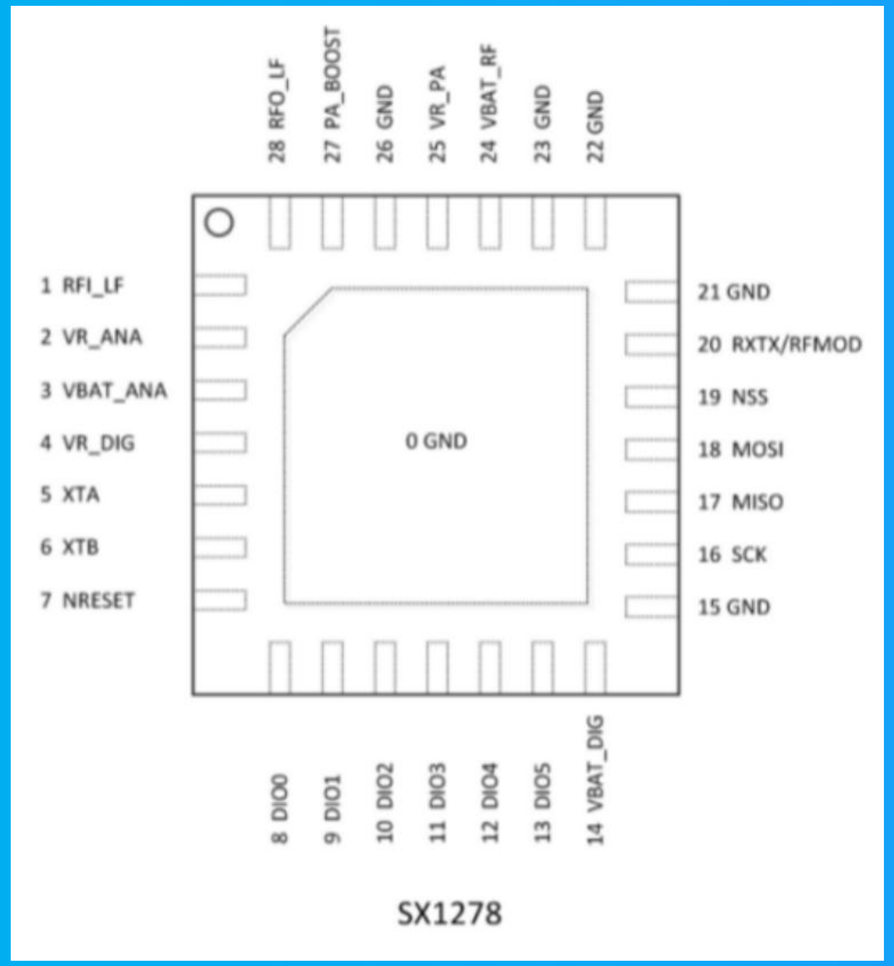
工作区
Filter
名称 类 维度 值
命令历史
Filter

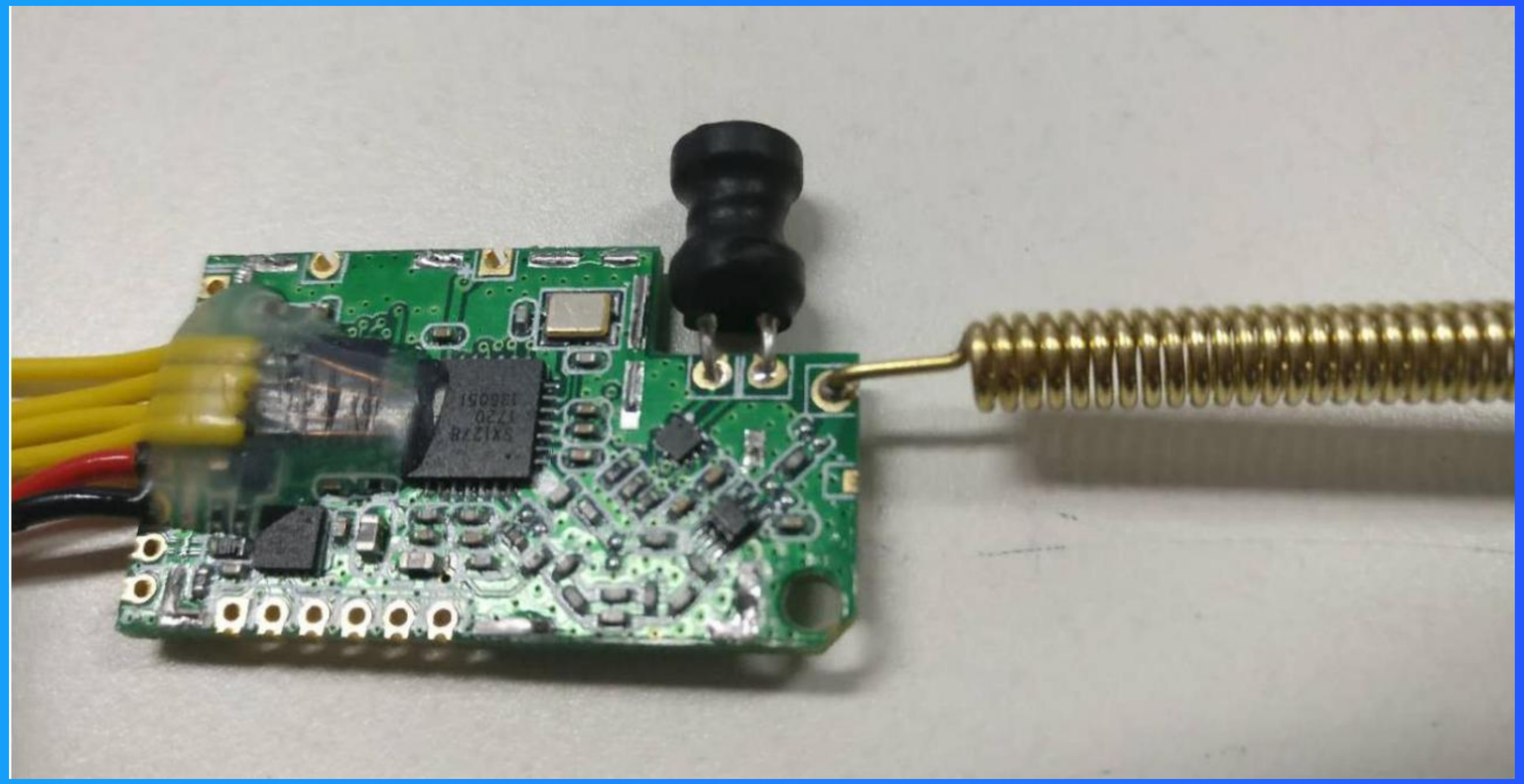
```
exit
# Octave 4.2.1, Thu Mar 29 19:14:47 2018 CST <nu
exit
# Octave 4.2.1, Sun Apr 01 13:27:09 2018 CST <nu
lora_sig_demod('SelfGen_PL6_BW125_CR48_SF1
lora_sig_demod('WaterMeter_NID1_PL6_BW125
lora_sig_demod('WaterMeter_NID1_PL6_BW125
pkg load signal
lora_sig_demod('WaterMeter_NID1_PL6_BW125
pkg load signal
lora_sig_demod('WaterMeter_NID1_PL6_BW125
lora_sig_demod('SelfGen_EnableCRC_PL6_BW12
```

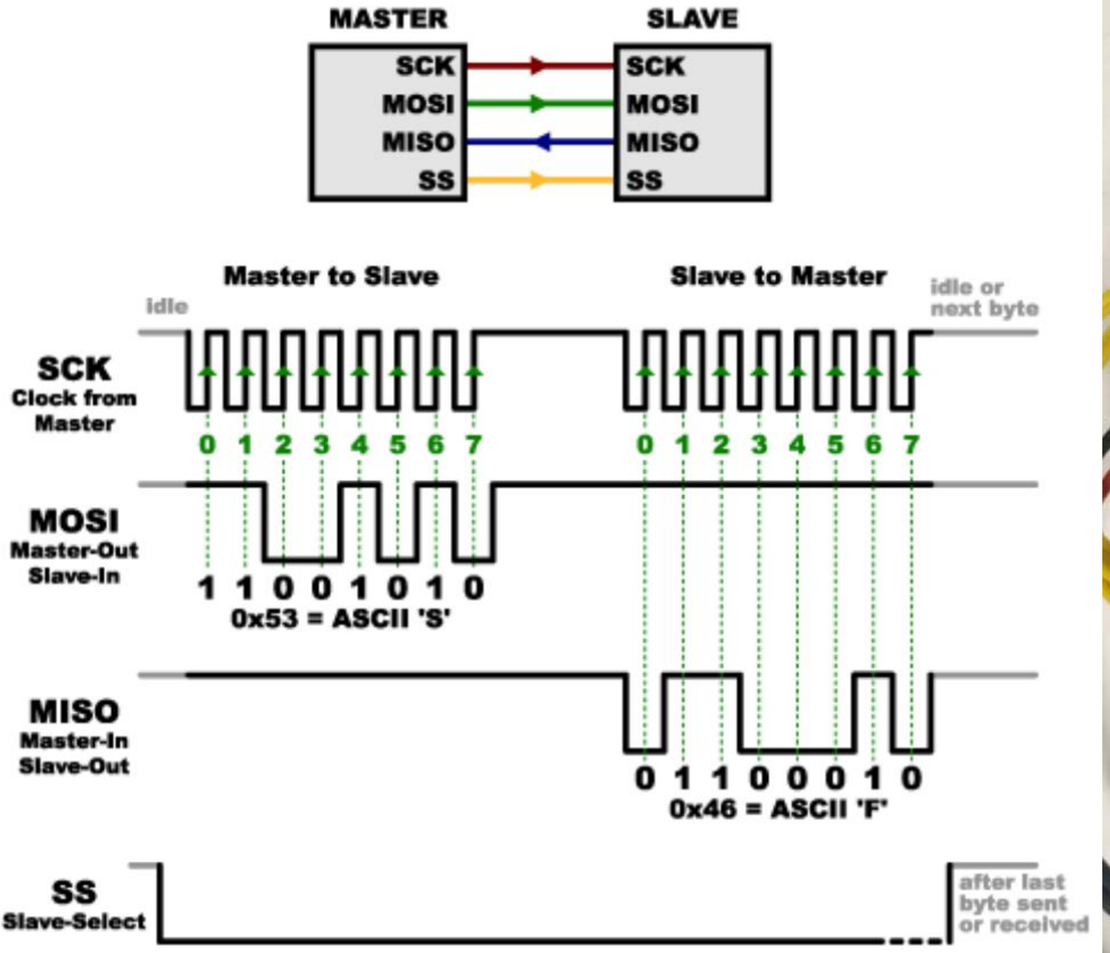
命令窗口 Editor 文档

https://github.com/UnicornTeam/lora-demod

射频芯片SPI嗅探


28 RFO_LF
27 PA_BOOST
26 GND
25 VR_PA
24 VBAT_RF
23 GND
22 GND
1 RFI_LF
2 VR_ANA
3 VBAT_ANA
4 VR_DIG
5 XTA
6 XTB
7 NRESET
0 GND
21 GND
20 RXTX/RFMOD
19 NSS
18 MOSI
17 MISO
16 SCK
15 GND
8 DIO0
9 DIO1
10 DIO2
11 DIO3
12 DIO4
13 DIO5
14 VBAT_DIG
SX1278





Search Protocols

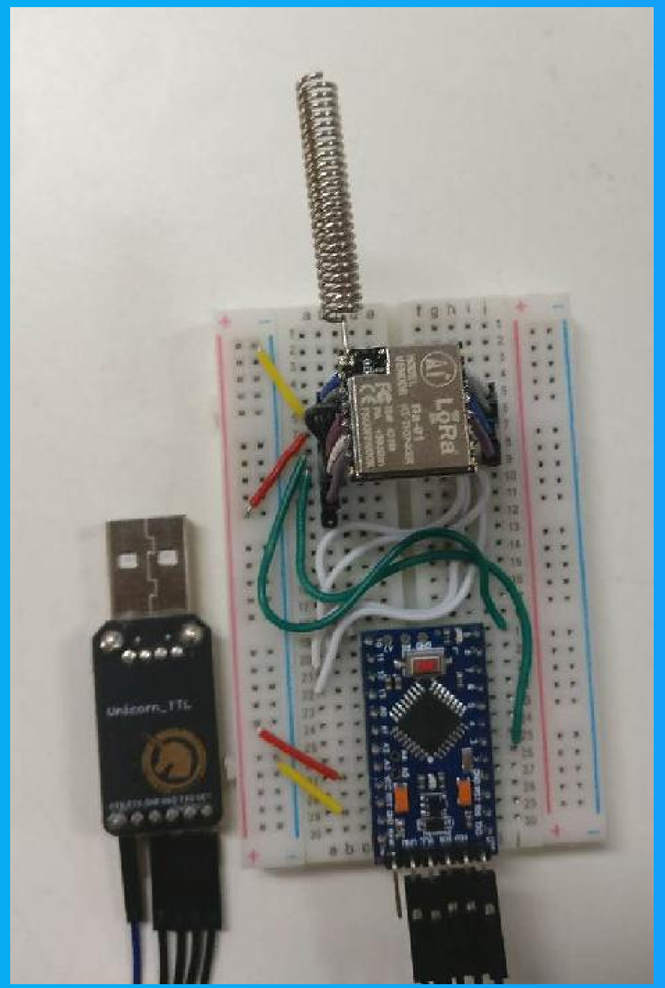
MOSI: 0x92; MISO: 0x18
MOSI: 0x10; MISO: 0x10
MOSI: 0xC0; MISO: 0x18
MOSI: 0x02; MISO: 0x01
MOSI: 0x1B; MISO: 0x18
MOSI: 0x01; MISO: 0x65
MOSI: 0x13; MISO: 0x18
MOSI: 0x01; MISO: 0x2F
MOSI: 0x8D; MISO: 0x18
MOSI: 0x00; MISO: 0x00
MOSI: 0x00; MISO: 0x18
MOSI: 0x2F; MISO: 0x18
MOSI: 0x06; MISO: 0x2C
MOSI: 0x05; MISO: 0x81
MOSI: 0x03; MISO: 0x29
MOSI: 0x01; MISO: 0x01
MOSI: 0x00; MISO: 0x00
MOSI: 0x00; MISO: 0x04
MOSI: 0x0F; MISO: 0x81
MOSI: 0xD8; MISO: 0x94
MOSI: 0x82; MISO: 0x22
MOSI: 0x2E; MISO: 0x8E
MOSI: 0x96; MISO: 0x56
MOSI: 0x40; MISO: 0x80
MOSI: 0x80; MISO: 0x00

射频芯片指令逆向

```
MOSI: 0x00;  MISO: 0x12  //Read VERSION 读取寄存器版本

MOSI: 0x81;  MISO: 0x00//
MOSI: 0x80;  MISO: 0x09// Sleep() writeRegister(REG_OP_MODE, MODE_LONG_RANGE_MODE | MODE_SLEEP);

MOSI: 0x7B;  MISO: 0x6C
MOSI: 0x87;  MISO: 0x68
MOSI: 0x0F;  MISO: 0x80
MOSI: 0x88;  MISO: 0x68
MOSI: 0xFF;  MISO: 0x00//设置射频频率 492.25 Mhz

MOSI: 0x8E;  MISO: 0x68//FifoTxBaseAddr
MOSI: 0x00;  MISO: 0x80//发射缓存区 地址

MOSI: 0x8F;  MISO: 0x68//FifoRxBaseAddr
MOSI: 0x00;  MISO: 0x00//读取缓存区地址

MOSI: 0x0C;  MISO: 0x68//readRegister(REG_LNA));
MOSI: 0x00;  MISO: 0x20

MOSI: 0x8C;  MISO: 0x68//writeRegister(REG_LNA, readRegister(REG_LNA) | 0x03);
MOSI: 0x23;  MISO: 0x20//设置 LNA

MOSI: 0xA6;  MISO: 0x68
MOSI: 0x04;  MISO: 0x04//设置AGC LNA增益

MOSI: 0x89;  MISO: 0x68//writeRegister(REG_PA_CONFIG, 0x70 | level);
MOSI: 0x8F;  MISO: 0x4F//设置PA 17DB

MOSI: 0x81;  MISO: 0x68
MOSI: 0x81;  MISO: 0x80// 进入 IDLE
MOSI: 0xB1;  MISO: 0x68// writeRegister(REG_DETECTION_OPTIMIZE, 0xc3);
MOSI: 0xC3;  MISO: 0xC3// 设置 SF
MOSI: 0xB7;  MISO: 0x68// writeRegister(REG_DETECTION_THRESHOLD, 0x0a);
MOSI: 0x0A;  MISO: 0x0A// 设置 SF
MOSI: 0x1E;  MISO: 0x68// readRegister(REG_MODEM_CONFIG_2) & 0x0f)
MOSI: 0x00;  MISO: 0x70// 设置 SF
MOSI: 0x9E;  MISO: 0x68// writeReg, (readRegister(REG_MODEM_CONFIG_2) & 0x0f) | ((sf << 4) & 0xf0));
MOSI: 0x70;  MISO: 0x70// 设置 SF 7
MOSI: 0x1D;  MISO: 0x68// (readRegister(REG_MODEM_CONFIG_1) & 0x0f)
MOSI: 0x00;  MISO: 0x72// 设置  BW CR Headr
MOSI: 0x9D;  MISO: 0x68// wri..(REG_..._1, (readRegister(REG_MODEM_CONFIG_1) & 0x0f) | (bw << 4));
MOSI: 0x72;  MISO: 0x72// 设置  BW 125Khz CR4/5 显性模式
```

地址	FSK/OOK 模式	LoRa™ 模式	（POR）	（FSK）	FSK 模式	LoRa™ 模式
0x00	RegFifo		0x00		FIFO 读/写访问	
0x01	RegOpMode		0x01		运行模式&LoRa™/FSK 选择	
0x02	RegBitrateMsb	unused	0x1A		比特率设置，最高有效位	
0x03	RegBitrateLsb		0x0B		比特率设置，最低有效位	
0x04	RegFdevMsb		0x00		频率偏移设置，最高有效位	
0x05	RegFdevLsb		0x52		频率偏移设置，最低有效位	
0x06	RegFrfMsb		0x6C		射频载波频率，最高有效位	
0x07	RegFrfMid		0x80		射频载波频率，中间位	
0x08	RegFrfLsb		0x00		射频载波频率，最低有效位	
0x09	RegPaConfig		0x4F		PA 选择和输出功率控制	
0x0A	RegPaRamp		0x09		PA 斜升/斜降时间和低相噪 PLL 的控制	
0x0B	RegOcp		0x2B		过流保护控制	
0x0C	RegLna		0x20		LNA 设置	
0x0D	RegRxConfig	RegFifoAddrPtr	0x08	0x00	AFC、AGC、ctrl	FIFO SPI 指针
0x0E	RegRssiConfig	RegFifoTxBaseAddr	0x02	0x80	RSSI	起始 Tx 数据
0x0F	RegRssiCollision	RegFifoRxBaseAddr	0x0A	0x00	RSSI 冲突检测器	起始 Rx 数据
0x10	RegRssiThresh	FifoRxCurrentAddr	0xFF	不适用	RSSI 阈值控制	最后接收数据包的起始地址
0x11	RegRssiValue	RegIrqFlagsMask	不适用	不适用	RSSI 值（单位：dBm）	可选 IRQ 标志屏蔽
0x12	RegRxBw	RegIrqFlags	0x15	0x00	信道滤波器带宽控制	IRQ 标志
0x13	RegAfcBw	RegRxNbBytes	0x0B	不适用	AFC 信道滤波器带宽	接收到的字节数
0x14	RegOokPeak	RegRxHeaderCntValueMs	0x28	不适用	OOK 解调器	接收到的有效报头数

制作嗅探工具



Sniffer_Watermeter_ESP32_simulation | Arduino 1.8.5

文件 编辑 项目 工具 帮助

Sniffer_Watermeter_ESP32_simulation

```
  SPI.transfer(0x00);
  SPI.transfer(0x00);
  SPI.transfer(0x00);
  SPI.transfer(0x00);
  SPI.transfer(0x7E);
  SPI.transfer(0x00);
  SPI.transfer(0x00);
  SPI.transfer(0xFF);
  SPI.transfer(0x09);
  SPI.transfer(0x29);
  SPI.transfer(0x20);
  //LoRa.writeRegister(0x01, 0x88);
  //LoRa.writeRegister(0x01, 0x88);
}
void setup() {
  Serial.begin(9600);
  while (!Serial); //if just the the basic f
  delay(1000);

  Serial.println("LoRa Receiver");
  //Simulation_SPI();
  SPI.begin(SCK, MISO, MOSI, SS);
  LoRa.setPins(SS, RST, DI00);
  if (!LoRa.begin(BAND, PABOOST)) {
    Serial.println("Starting LoRa failed!");
    while (1);
  }
  LoRa.implicitHeaderMode();
  //LoRa.explicitHeaderMode();
  //LoRa.explicitHeaderMode();
  LoRa.setSpreadingFactor(11);
  LoRa.setCodingRate4(5);
  LoRa.setSignalBandwidth(125E3);
  LoRa.setPreambleLength(7);
  LoRa.setSyncWord(0x12);
  //LoRa.disableCrc();
  LoRa.crc();
  Serial.println("begin");
  LoRa.receive();


}
```

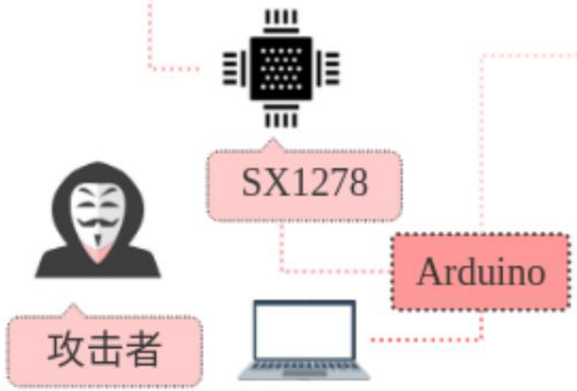
/dev/ttyUSB3

发送

```
LoRa Receiver
begin
Received packet '0x18 0x2C 0x81 0x29 0x01 0x00 0x04 0x81 0x94 0x22 0x8
Received packet '0x18 0x2C 0x81 0x29 0x01 0x00 0x04 0x81 0x94 0x22 0x8
Received packet '0x18 0x2C 0x81 0x29 0x01 0x00 0x04 0x81 0x94 0x22 0x8
```

自动滚屏 | 没有结束符 | 9600 波特率 | Clear output

逆向水表通信协议




```
0x04 0x81 0x94 0x22 0x8E 0x56 0x80 0x00 // UUID
0x00 0x00 0x00 0x00
0x08 0x00 0x01 0x06
0x29 0x0A 0x00 0x00
0xB4 0xDC 0x32 0x00  //正累积水量 //3333300
0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00
0xE6
0x0C //TEMP
0x1E
0x0E //POWER
0x00
0x00 //网关到表计 RSSI
0x00 //网关到表计 SNR
0xBF 0x38 //END
```

安全隐私风险

住户A

住户B

住户C

住户A	住户B	隔壁老王
17号 20:20	17号 21:20	17号 22:20
用量:0.1吨	用量:xx吨	用量:xx吨
•••	•••	•••
•••	•••	•••

```
//住户A
0x04 0x81 ..... 0x80 0x02 //水表ID
....
0x01 0x20 0x00 0x00  //用水量
....
0x0C //TEMP
..
0x0E //POWER
...
```

```
//住户B
0x04 0x81 ..... 0x80 0x01 //水表ID
....
0xB4 0xDC 0x32 0x00  //用水量
....
0x0C //TEMP
..
0x0E //POWER
...
```

SX1278

Arduino

LORA 网关

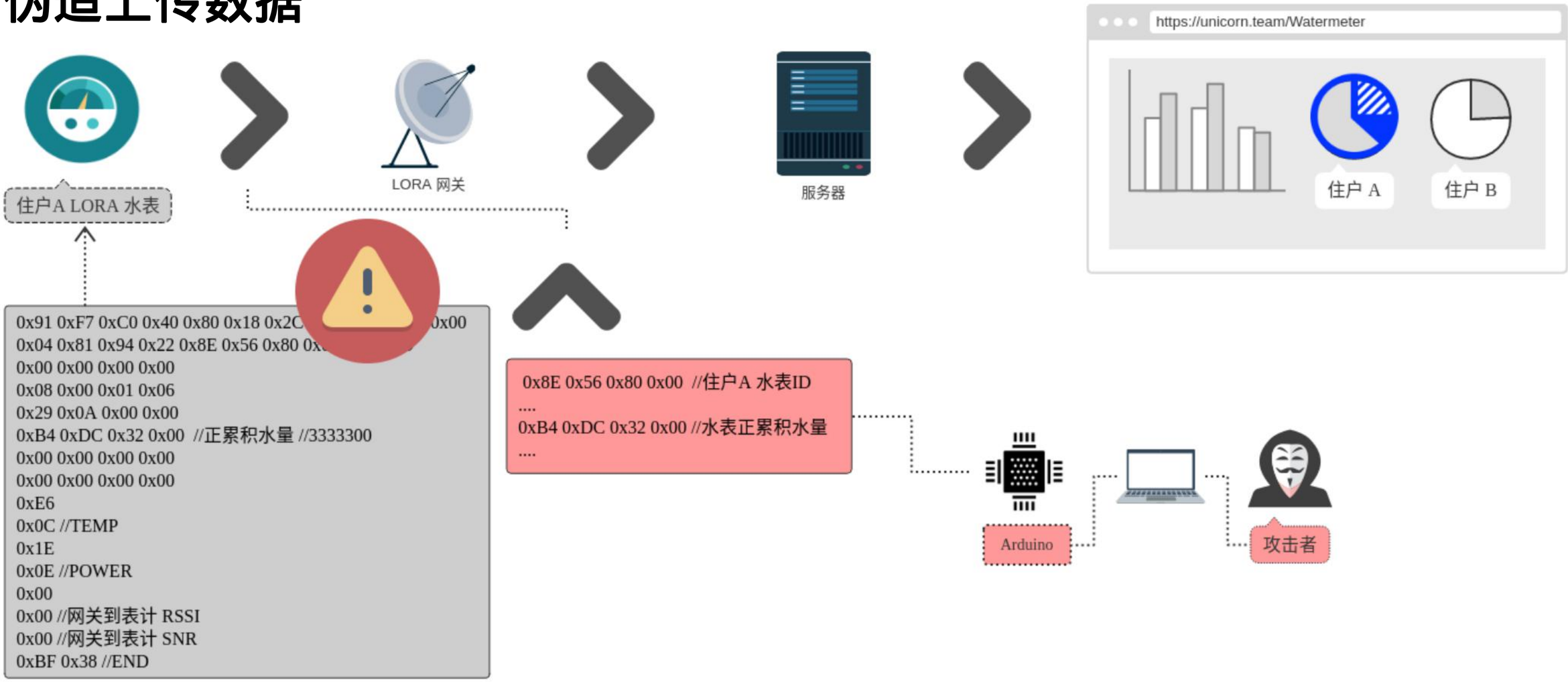
攻击者

昨晚老王家没有用水,反而住户A的用水量多了一倍,明明听说住户A男主出差了

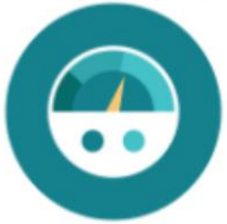
住户B一般 11点洗漱出门了,晚上凌晨一两点才回来洗澡肯定是个程序猿

住户C 这周没任何的用水量,一家人肯定出去旅游了,可以去他家偷东西了

伪造上传数据


住户A LORA 水表
LORA 网关
服务器
https://unicorn.team/Watermeter
住户 A
住户 B
0x91 0xF7 0xC0 0x40 0x80 0x18 0x2C
0x04 0x81 0x94 0x22 0x8E 0x56 0x80 0x
0x00 0x00 0x00 0x00
0x08 0x00 0x01 0x06
0x29 0x0A 0x00 0x00
0xB4 0xDC 0x32 0x00 //正累积水量 //3333300
0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00
0xE6
0x0C //TEMP
0x1E
0x0E //POWER
0x00
0x00 //网关到表计 RSSI
0x00 //网关到表计 SNR
0xBF 0x38 //END
0x8E 0x56 0x80 0x00 //住户A 水表ID
....
0xB4 0xDC 0x32 0x00 //水表正累积水量
....
Arduino
攻击者

煤改气阀门控制



住户A LORA 水表

煤改气阀门

水表ID: 0x8E 0x56 0x80 0x00

阀门ID: 0x8E 0x56 0x80 0x01

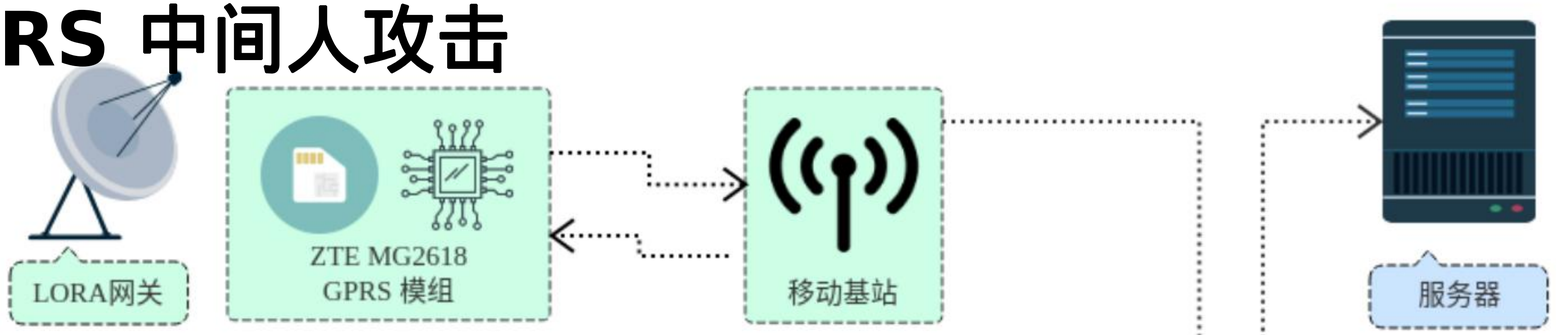
```
将SX1278 进入嗅探模式
....
嗅探LORA 网络中ID 信息
....
//嗅探ID后伪造网关发射恶意指令
....
关闭 .... ID 0x00 阀门
....
关闭 .... ID 0x01 阀门
```

伪造
LORA 网关

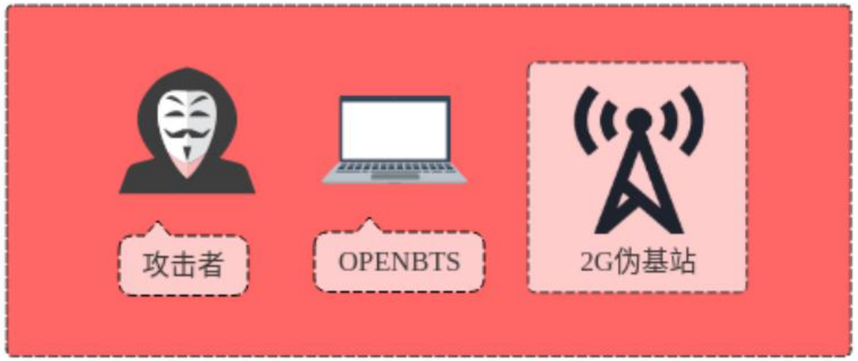
Arduino

攻击者

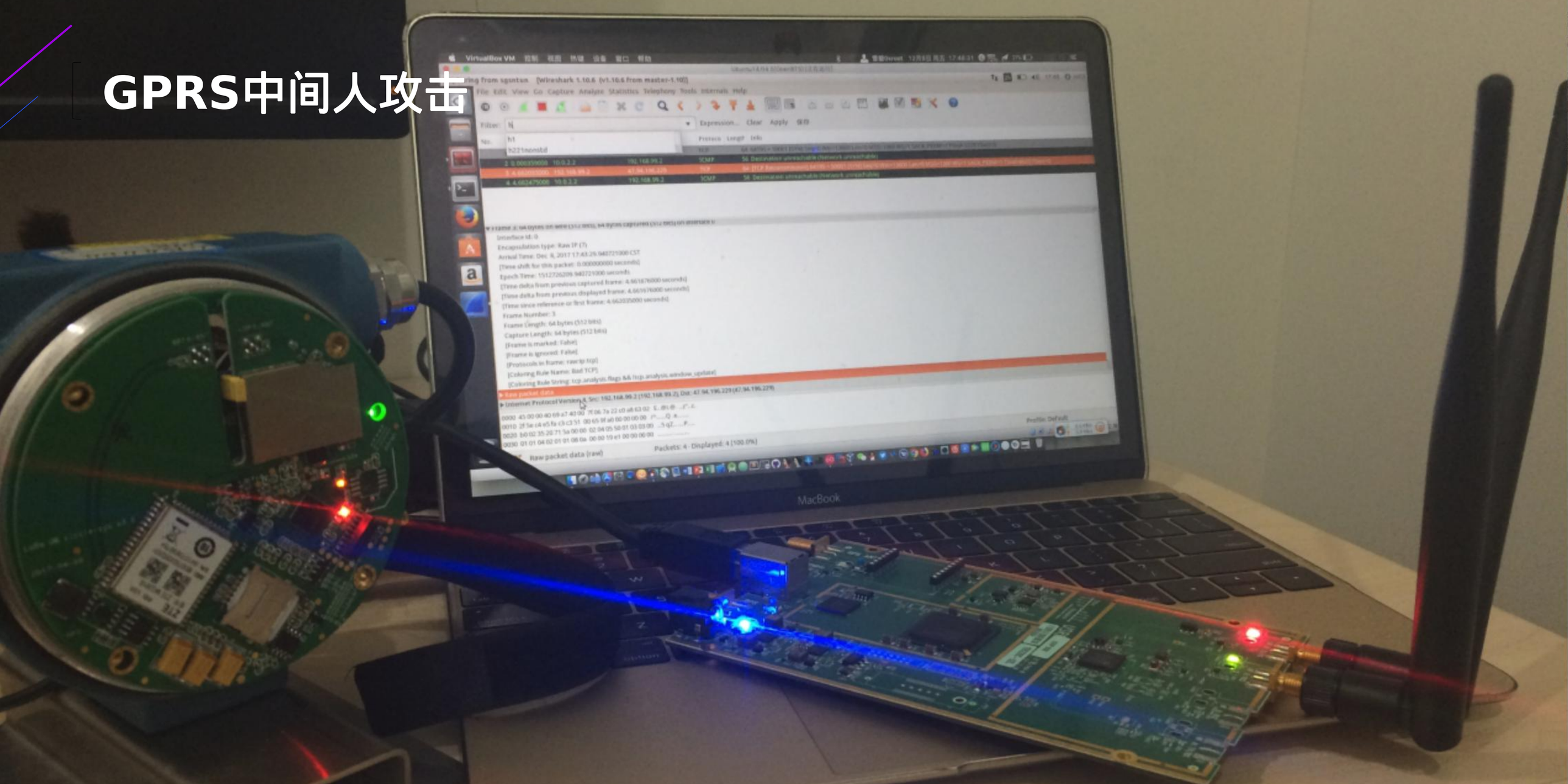
GPRS 中间人攻击



AA 00 28 7A 2C 0B 6E 81 59 02 E0 AA 42 00 1D 00 22 04 81 94 22 8E 56 80 00 00 32 DC B4 00 00 00 00 00 00 00 00 00 0E 0C E6 1E 17 01 19 11 25 65 0B 00 00 84 55
GWID:7A 2C 0B 6E 81 59 02 E0
Header:AA
Cont:42
??00
application:1D
Len:00 22
(8byte)UUID:04 81 94 22 8E 56 80 00 module
(4byte)正累积水量:00 32 DC B4 //3333300
(4byte)负累积水量:00 00 00 00
(2byte)瞬时水量:00 00
(2byte)表计状态:00 00
(2byte)电源电压:00 0E
(1Byte)温度:0C
??: E6 1E
(5Byte)抄表时间:17 01 19 11 25
(1Byte)表计到网关 RSSI:65
(1Byte)表计到网关 SNR:0b
(1Byte)网关到表计 RSSI:00
(1Byte)网关到表计 SNR:00



GPRS中间人攻击



网关GPRS模块数据嗅探

```
OpenBTS Command Line Interface (CLI) utility
Copyright 2012, 2013, 2014 Range Networks, Inc.
Licensed under GPLv2.
Includes libreadline, GPLv2.
Connecting to 127.0.0.1:49300...
Remote Interface Ready.
Type:
 "help" to see commands,
 "version" for version information,
 "notices" for licensing information,
 "quit" to exit console interface.
OpenBTS>
OpenBTS> tmsis
IMSI            TMSI     TMFI            AUTH CREATED ACCESSED TMSI_ASSIGNED
460072[redacted]3311 0xb3652 8657[redacted]9800 2    7m      142s     1
4600[redacted]3010 0x76396 3594[redacted]5190 2    14m     5m       1


OpenBTS> sgsn list
 GMM Context: imsi=4600[redacted]3311 ptmsi=0x69001 tlli=0xc0069001 state=GmmRegist
eredNormal age=86 idle=8 MS#1,TLLI=c0069001,80031001 IPs=192.168.88.1,192.168.88
.2


OpenBTS> gprs list
 MS#1,TLLI=c0069001,80031001 rrmode=PacketIdle Bytes:1225up/1103down Utilization
=162%
        GMM Context: imsi=4600[redacted]3311 ptmsi=0x69001 tlli=0xc0069001 state=G
mmRegisteredNormal age=103 idle=4 IPs=192.168.88.1,192.168.88.2
        TimingError=(-1.46 min=-1.48 max=-0.46 avg=-1.02 N=1313) RSSI=(-30 min=
-34 max=-28 avg=-30.86 N=1313) CV=(54 min=42 max=56 avg=48.89 N=19) ILev=(0) RXQ
ual=(0 min=0 max=7 avg=2.50 N=14) SigVar=(0 min=0 max=63 avg=36.64 N=14) ChCodin
g=(3 min=0 max=3 avg=2.88 N=100)
        dataER:.9% (907) recent:.0% (347) low:1.0% (111) tbfER:.18% (17)
        rrbpER:.5% (131) recent:.7% (40) low:1.0% (9) cchER:0% (0) recent:0% (
0)
 MS#2,TLLI=810cb380 rrmode=PacketIdle Bytes:355up/0down Utilization=0%
        GMM state unknown
        TimingError=(-1.49 min=-1.50 max=-1.31 avg=-1.44 N=48) RSSI=(-44 min=-4
7 max=-16 avg=-41.35 N=48) CV=(49 min=44 max=54 avg=48.20 N=5) ILev=(0) RXQual=(
0) SigVar=(0) ChCoding=(0)
        dataER:0% (33) recent:0% (0) tbfER:0% (5)
        rrbpER:.09% (11) recent:0% (0) cchER:0% (0) recent:0% (0)
 TBF#21  mtMS- MS#1,TLLI-c0069001,80031001 mtDir-RLCDir::Down
        channels: down=( 0:1 0:2 0:3) up=( 0:2,usf=0 0:3,usf=0)
        mtState==TBFState::Dead mtAttached=1 mtTFI=21 mtTlli=0xc0069001 size=0
 PDCH ARFCN=512 TN=1 FER=0%
 PDCH ARFCN=512 TN=2 FER=.3%
 PDCH ARFCN=512 TN=3 FER=0%
```

Filter: Expression... Clear Apply 保存

No.	Time	Source	Destination	Protoco	Length	Info
11	296.45011100	192.168.88.2	117.27.89.185	TCP	40	60325 > 50502 [ACK] Seq=1 Ack=1 Win=10880 Len=0
12	296.49724400	192.168.88.2	117.27.89.185	TCP	65	60325 > 50502 [PSH, ACK] Seq=1 Ack=1 Win=10880 Len=25
13	296.49754700	117.27.89.185	192.168.88.2	TCP	40	50502 > 60325 [ACK] Seq=1 Ack=26 Win=65535 Len=0
14	296.55464400	192.168.88.2	[redacted]96.229	TCP	59	50614 > 50001 [PSH, ACK] Seq=26 Ack=20 Win=10880 Len=19
15	296.55499100	[redacted].229	192.168.88.2	TCP	40	50001 > 50614 [ACK] Seq=20 Ack=45 Win=65535 Len=0
16	296.56053000	[redacted].229	192.168.88.2	TCP	65	50001 > 50614 [PSH, ACK] Seq=20 Ack=45 Win=65535 Len=25
17	296.56865000	117.27.89.185	192.168.88.2	TCP	59	50502 > 60325 [PSH, ACK] Seq=1 Ack=26 Win=65535 Len=19
18	297.13718100	192.168.88.2	[redacted]6.229	TCP	40	50614 > 50001 [ACK] Seq=45 Ack=45 Win=10880 Len=0

- ▶ Frame 14: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
- ▶ Raw packet data
- ▶ Internet Protocol Version 4, Src: 192.168.88.2 (192.168.88.2), Dst: [redacted]6.229 (47.94.196.229)
- ▼ Transmission Control Protocol, Src Port: 50614 (50614), Dst Port: 50001 (50001), Seq: 26, Ack: 20, Len: 19
  - Source port: 50614 (50614)
  - Destination port: 50001 (50001)
  - [Stream index: 1]
  - Sequence number: 26 (relative sequence number)
  - [Next sequence number: 45 (relative sequence number)]
  - Acknowledgment number: 20 (relative ack number)
  - Header length: 20 bytes
  - ▶ Flags: 0x018 (PSH, ACK)
  - Window size value: 10880
  - [Calculated window size: 10880]
  - [Window size scaling factor: -2 (no window scaling used)]
  - ▶ Checksum: 0xb821 [validation disabled]
  - ▼ [SEQ/ACK analysis]
    - [This is an ACK to the segment in frame: 9]
    - [The RTT to ACK the segment was: 1.009809000 seconds]
    - [Bytes in flight: 19]
- ▼ Data (19 bytes)
  - Data: aa00067a2c0b6e815902e0aa4300120000e055
  - [Length: 19]

```
0010 [redacted]                                  ^.....Q ........
0020 50 18 2a 80 b8 21 00 00 aa 00 06 7a 2c 0b 6e 81  P.*..!.. ...z,.n.
```

No.	Time	Source	Destination	Protocol	Length	Info
3	295.181109	[redacted].2	[redacted]	TCP	64	50614 → 50001 [SYN] Seq=0 Win=10880 Len=0 MSS=1360 WS=1 SACK_PERM=1 TSval=22915 TSecr=0
4	295.187401	[redacted]229		TCP	44	50001 → 50614 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5	295.479558	[redacted].2		TCP	40	50614 → 50001 [ACK] Seq=1 Ack=1 Win=10880 Len=0
6	295.538890	[redacted].2		TCP	65	50614 → 50001 [PSH, ACK] Seq=1 Ack=1 Win=10880 Len=25
7	295.539131	[redacted]229		TCP	40	50001 → 50614 [ACK] Seq=1 Ack=26 Win=65535 Len=0
9	295.544835	[redacted]229		TCP	59	50001 → 50614 [PSH, ACK] Seq=1 Ack=26 Win=65535 Len=19
14	296.554644	[redacted].2		TCP	59	50614 → 50001 [PSH, ACK] Seq=26 Ack=20 Win=10880 Len=19
15	296.554991	[redacted]229		TCP	40	50001 → 50614 [ACK] Seq=20 Ack=45 Win=65535 Len=0
16	296.560530	[redacted]229		TCP	65	50001 → 50614 [PSH, ACK] Seq=20 Ack=45 Win=65535 Len=25
18	297.137181	[redacted].2		TCP	40	50614 → 50001 [ACK] Seq=45 Ack=45 Win=10880 Len=0
20	337.461784	[redacted].2		TCP	65	50614 → 50001 [PSH, ACK] Seq=45 Ack=45 Win=10880 Len=25
21	337.462168	[redacted]229				
22	337.462259	[redacted].2				K] Seq=45 Ack=45 Win=10880 Len=25
23	337.462433	[redacted]229				Win=65535 Len=0
24	337.467670	[redacted]229				=25
25	337.518138	[redacted].2				K] Seq=45 Ack=45 Win=10880 Len=25
26	337.518370	[redacted]229				Win=65535 Len=0
27	337.561945	[redacted].2				K] Seq=45 Ack=45 Win=10880 Len=25
28	337.563148	[redacted]229				Win=65535 Len=0
29	338.126089	[redacted].2				
30	358.289074	[redacted].2				=25
31	358.289447	[redacted]229				
32	358.295159	[redacted]229				=25
33	358.771720	[redacted].2				

```
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no
    Checksum: 0xaea5 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▾ [SEQ/ACK analysis]
      [iRTT: 0.298449000 seconds]
      [Bytes in flight: 25]
      [Bytes sent since last PSH flag: 2
    TCP payload (25 bytes)
▾ Data (25 bytes)
```

Wireshark · 追踪 TCP 流 (tcp.stream eq 1) · iot_fuzz

```
00000000  aa 00 0c 7a 2c 0b 6e 81  59 02 e0 aa 41 00 02 00   ...z,.n. Y...A...
00000010  06 6c 78 08 21 01 96 7e  55                       .lx.!..~ U
    00000000  aa 00 06 7a 2c 0b 6e 81  59 02 e0 aa 80 00 00 00   ...z,.n. Y.......
    00000010  00 0b 55                                          ..U
00000019  aa 00 06 7a 2c 0b 6e 81  59 02 e0 aa 43 00 12 00   ...z,.n. Y...C...
00000029  00 e0 55                                          ..U
    00000013  aa 00 0c 7a 2c 0b 6e 81  59 02 e0 aa 81 00 12 00   ...z,.n. Y.......
    00000023  06 17 01 19 11 24 04 94  55                       .....$.. U
0000002C  aa 00 0c 7a 2c 0b 6e 81  59 02 e0 aa 41 00 11 00   ...z,.n. Y...A...
0000003C  06 00 00 00 00 00 00 e9  55                       ........ U
    0000002C  aa 00 0c 7a 2c 0b 6e 81  59 02 e0 aa 80 00 0b 04   ...z,.n. Y.......
    0000003C  7e 94 22 8e 56 80 00 b8  55                       ~.".V... U
00000045  aa 00 0c 7a 2c 0b 6e 81  59 02 e0 aa 41 00 11 00   ...z,.n. Y...A...
00000055  06 00 00 00 00 00 00 e9  55                       ........ U
    00000045  aa 00 0c 7a 2c 0b 6e 81  59 02 e0 aa 80 00 0b 04   ...z,.n. Y.......
    00000055  7e 94 22 8e 56 80 00 b8  55                       ~.".V... U
```

6 客户端 分组, 6 服务器 分组, 9 turn(s).

Entire conversation (188 bytes) | 显示和保存数据为 Hex 转储 | 流 1

查找: | 查找下一个(N)

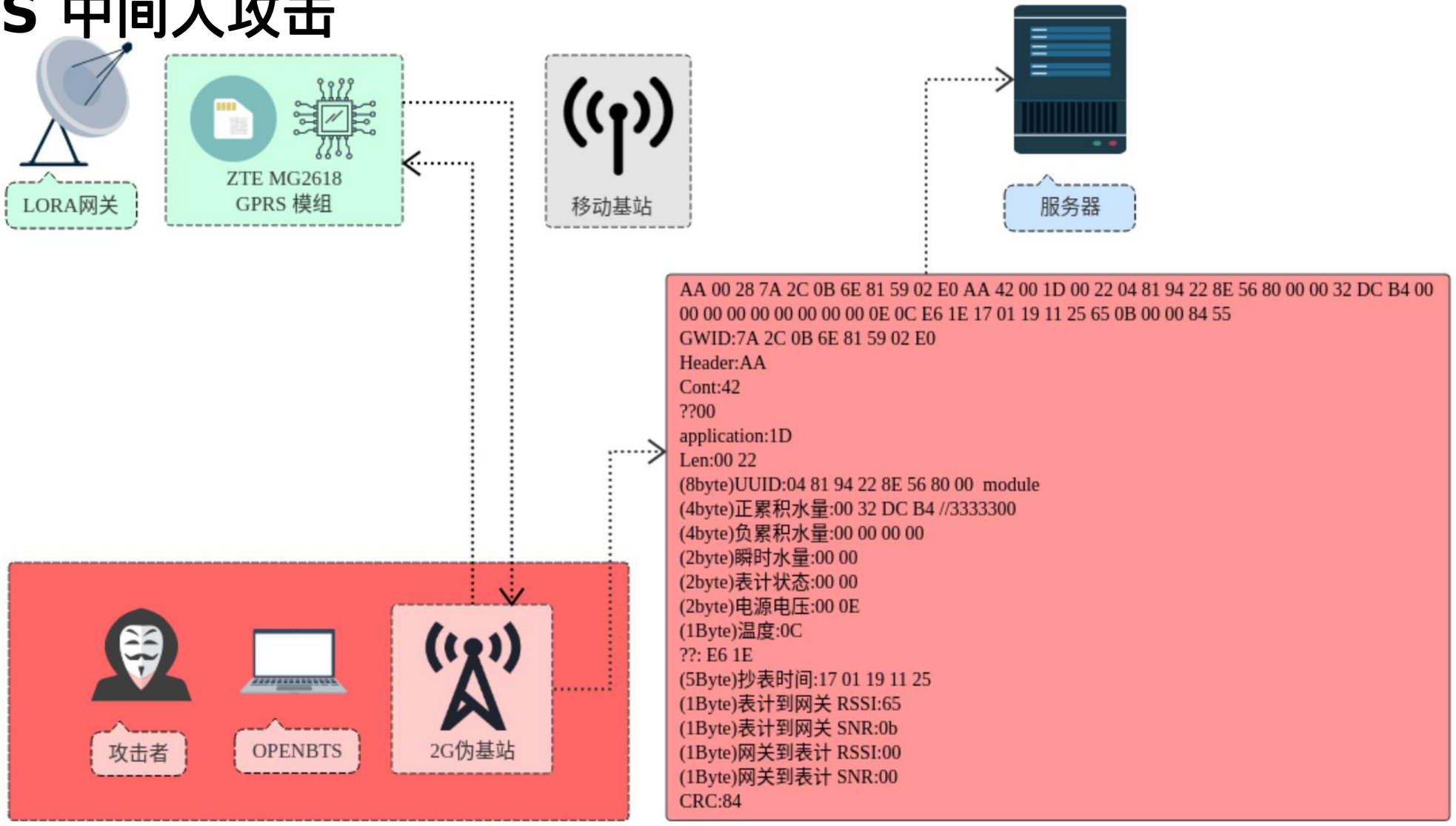
Help | 滤掉此流 | 打印 | Save as... | 返回 | Close

逆向网关上传数据协议

```
recv:AA 00 28 7A 2C 0B 6E 81 59 02 E0 AA 42 00 1D 00 22 04 81 94 22 8E 56 80 00 00 32 DC B4 00 00 00 00 00 00 00 00 00 0E 0C E6 1E 17 01 19 11
25 65 0B 00 00 84 55
GWID:7A 2C 0B 6E 81 59 02 E0 //网关ID
Header:AA
Cont:42 //控制码
??00
application:1D //应用码
Len:00 22 //长度
04 81 94 22 8E 56 80 00  //水表ID (8byte)UUID
00 32 DC B4 //3333300 (4byte)正累积水量
00 00 00 00 //(4byte)负累积水量
00 00 //(2byte)瞬时水量
00 00 //(2byte)表计状态
00 0E //(2byte)电源电压
0C //(1Byte)温度
E6 1E //???
17 01 19 11 25 //(5Byte)抄表时间
65 //(1Byte)表计到网关 RSSI
0b //(1Byte)表计到网关 SNR
00 //(1Byte)网关到表计 RSSI
00 //(1Byte)网关到表计 SNR
84 //(1Byte)CRC
55 //END
```

```
recv:AA 00 0C 7A 2C 0B 6E 81 59 02 E0 AA 41 00 02 00 06 6C 78 08 21 01 96 7E 55 //网关请求注册
Server:aa 00 06 7a 2c 0b 6e 81 59 02 e0 aa 80 00 00 00 00 0b 55 //服务器返回数据包
------------------------------------------------------
recv:AA 00 06 7A 2C 0B 6E 81 59 02 E0 AA 43 00 12 00 00 E0 55  //网关请求服务器 时钟
Server:aa 00 0c 7a 2c 0b 6e 81 59 02 e0 aa 81 00 12 00 06 17 01 19 11 24 04 94 55 //服务器返回时钟 17 01 19 11 24 04
==========================================================================================
Header:AA
len:00 0C //长度
GWID:7A 2C 0B 6E 81 59 02 E0 //网关ID
Header:AA //协议头部
Cont:41 //控制码
??:00
application:02 //应用码
length:00 06 //用户数据长度
data:6C 78 08 21 01 96   mcu version:6C 78 radio mcu:08 21 NID:01 freq:96(150) //网关上传 版本信息
CRC:7E //0c+7a+2c+0b+6e+81+59+02+e0+aa+41+02+06+6c+78+08+21+01+96 //CRC 校验方式
END:55
```

GPRS 中间人攻击

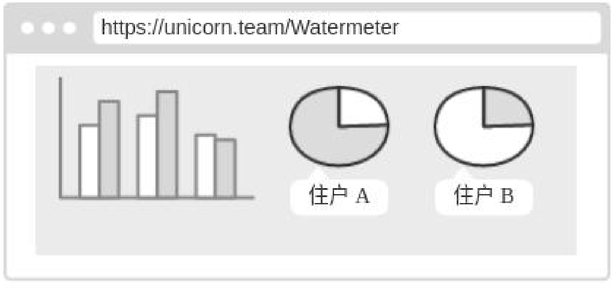

LORA网关
ZTE MG2618
GPRS 模组
移动基站
服务器
攻击者
OPENBTS
2G伪基站
AA 00 28 7A 2C 0B 6E 81 59 02 E0 AA 42 00 1D 00 22 04 81 94 22 8E 56 80 00 00 32 DC B4 00
00 00 00 00 00 00 00 00 0E 0C E6 1E 17 01 19 11 25 65 0B 00 00 84 55
GWID:7A 2C 0B 6E 81 59 02 E0
Header:AA
Cont:42
??00
application:1D
Len:00 22
(8byte)UUID:04 81 94 22 8E 56 80 00 module
(4byte)正累积水量:00 32 DC B4 //3333300
(4byte)负累积水量:00 00 00 00
(2byte)瞬时水量:00 00
(2byte)表计状态:00 00
(2byte)电源电压:00 0E
(1Byte)温度:0C
??: E6 1E
(5Byte)抄表时间:17 01 19 11 25
(1Byte)表计到网关 RSSI:65
(1Byte)表计到网关 SNR:0b
(1Byte)网关到表计 RSSI:00
(1Byte)网关到表计 SNR:00
CRC:84

通信链路

LORA水表

LORA 网关

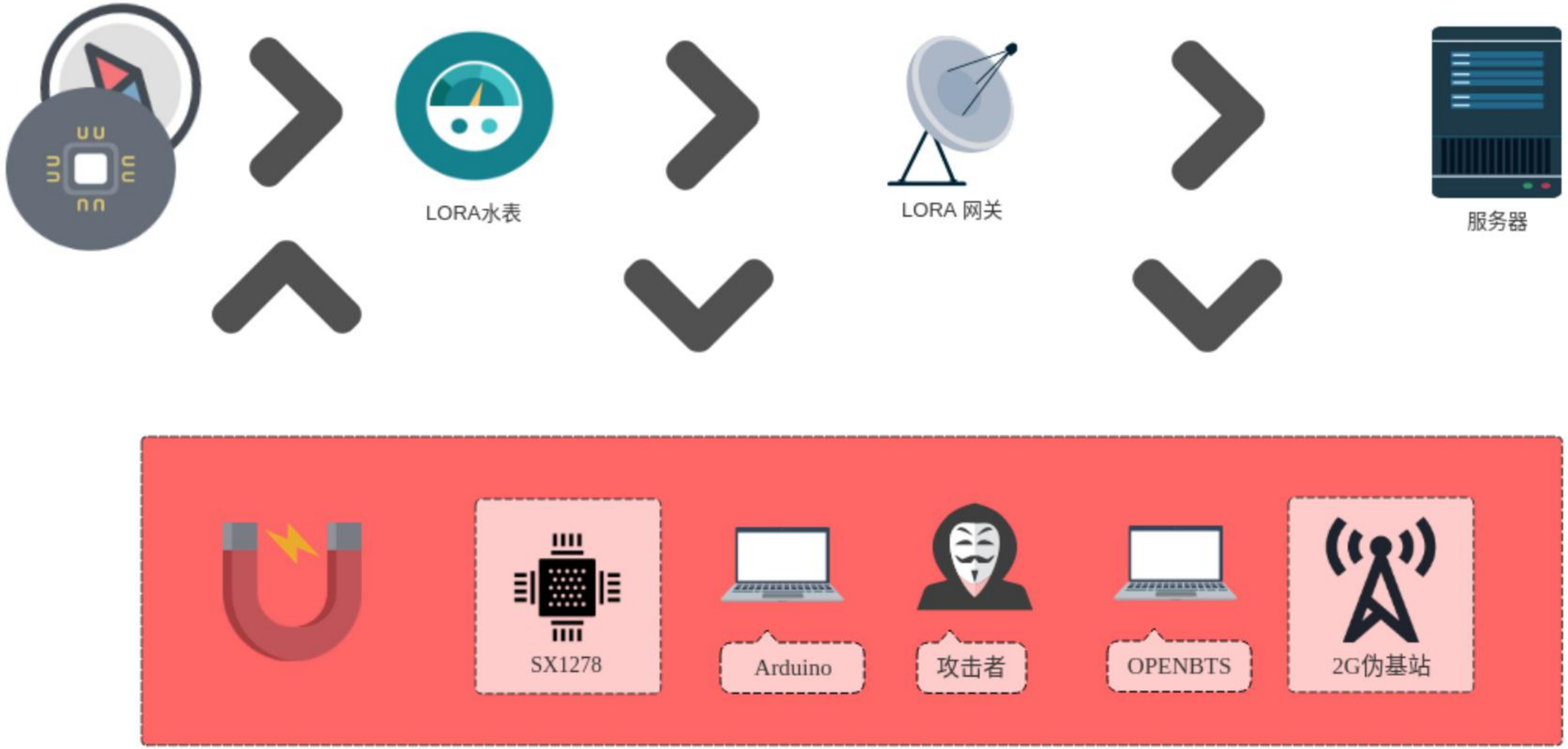
服务器



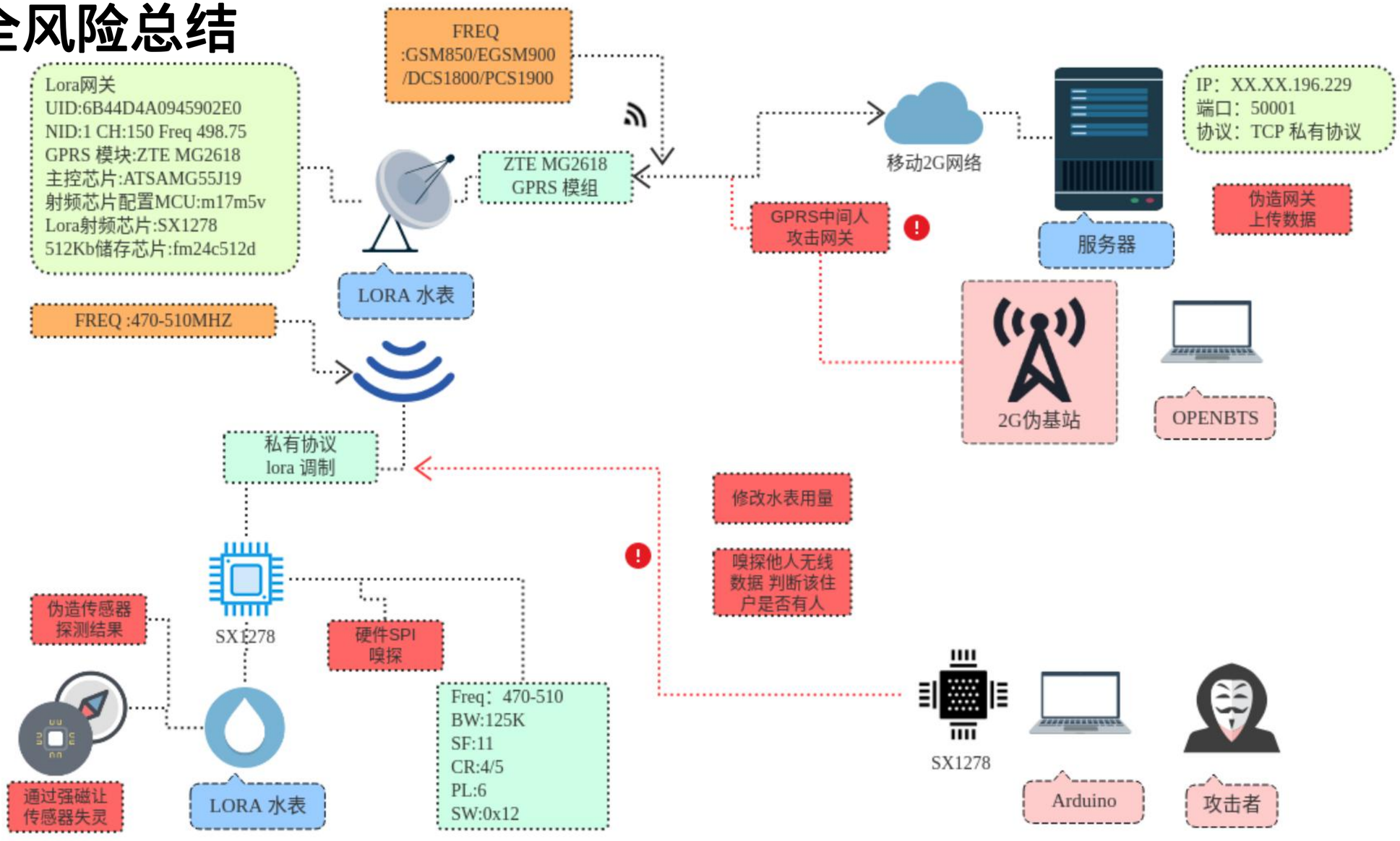
0x91 0xF7 0xC0 0x40 0x80 0x18 0x2C 0x81 0x29 0x01 0x00
0x04 0x81 0x94 0x22 0x8E 0x56 0x80 0x00 // 水表ID
0x00 0x00 0x00 0x00
0x08 0x00 0x01 0x06
0x29 0x0A 0x00 0x00
0xB4 0xDC 0x32 0x00 //正累积水量 //3333300
0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00
0xE6
0x0C //TEMP
0x1E
0x0E //POWER
0x00
0x00 //网关到表计 RSSI
0x00 //网关到表计 SNR
0xBF 0x38 //END

AA 00 28 7A 2C 0B 6E 81 59 02 E0 AA 42 00 1D 00 22 04 81 94 22 8E 56 80 00 00 32
DC B4 00 00 00 00 00 00 00 00 00 0E 0C E6 1E 17 01 19 11 25 65 0B 00 00 84 55
GWID:7A 2C 0B 6E 81 59 02 E0
Header:AA
Cont:42
??00
application:1D
Len:00 22
(8byte)UUID:04 81 94 22 8E 56 80 00 module
(4byte)正累积水量:00 32 DC B4 //3333300
(4byte)负累积水量:00 00 00 00
(2byte)瞬时水量:00 00
(2byte)表计状态:00 00
(2byte)电源电压:00 0E
(1Byte)温度:0C
??: E6 1E
(5Byte)抄表时间:17 01 19 11 25
(1Byte)表计到网关 RSSI:65
(1Byte)表计到网关 SNR:0b
(1Byte)网关到表计 RSSI:00
(1Byte)网关到表计 SNR:00
CRC:84

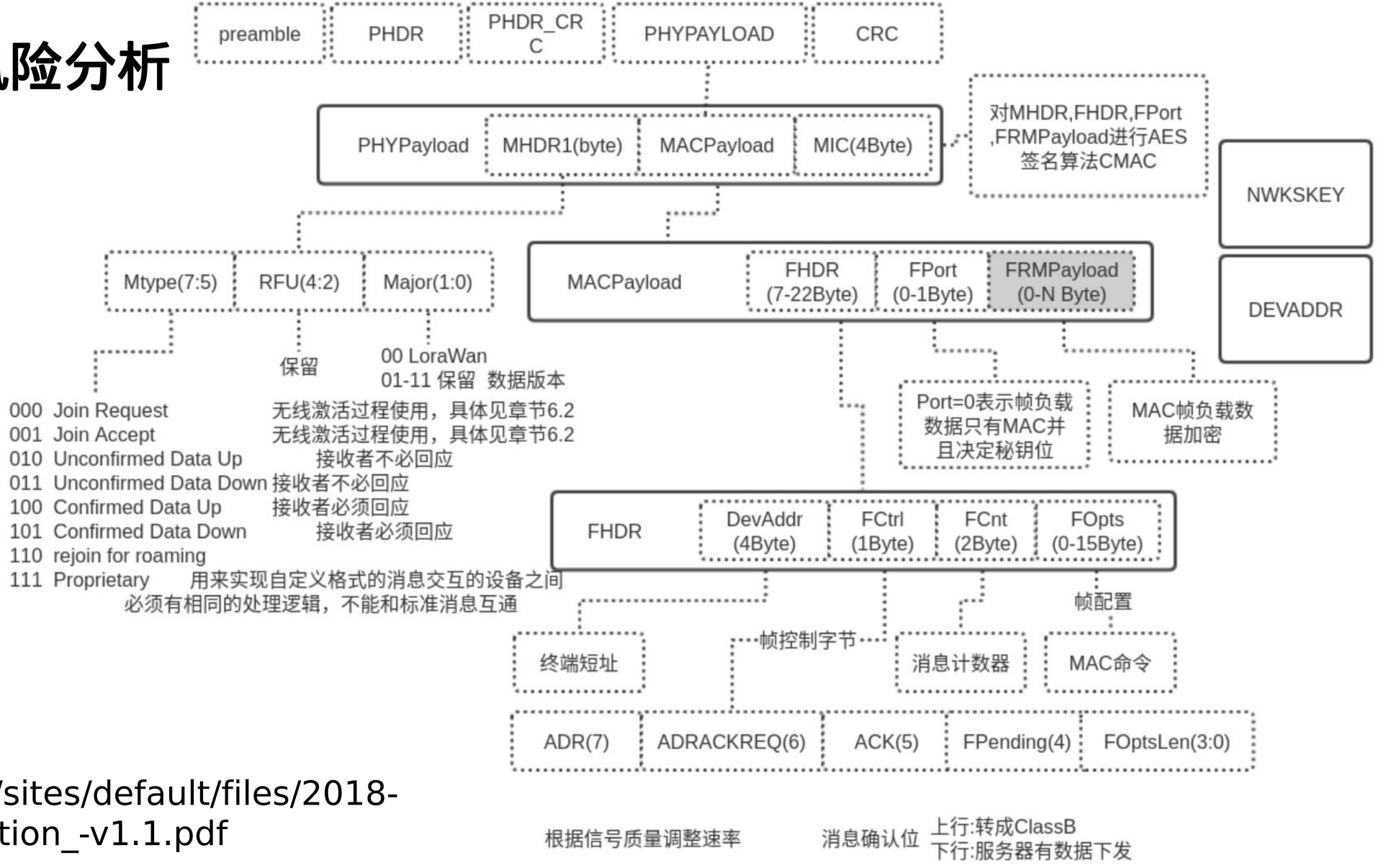
安全测试环境



安全风险总结

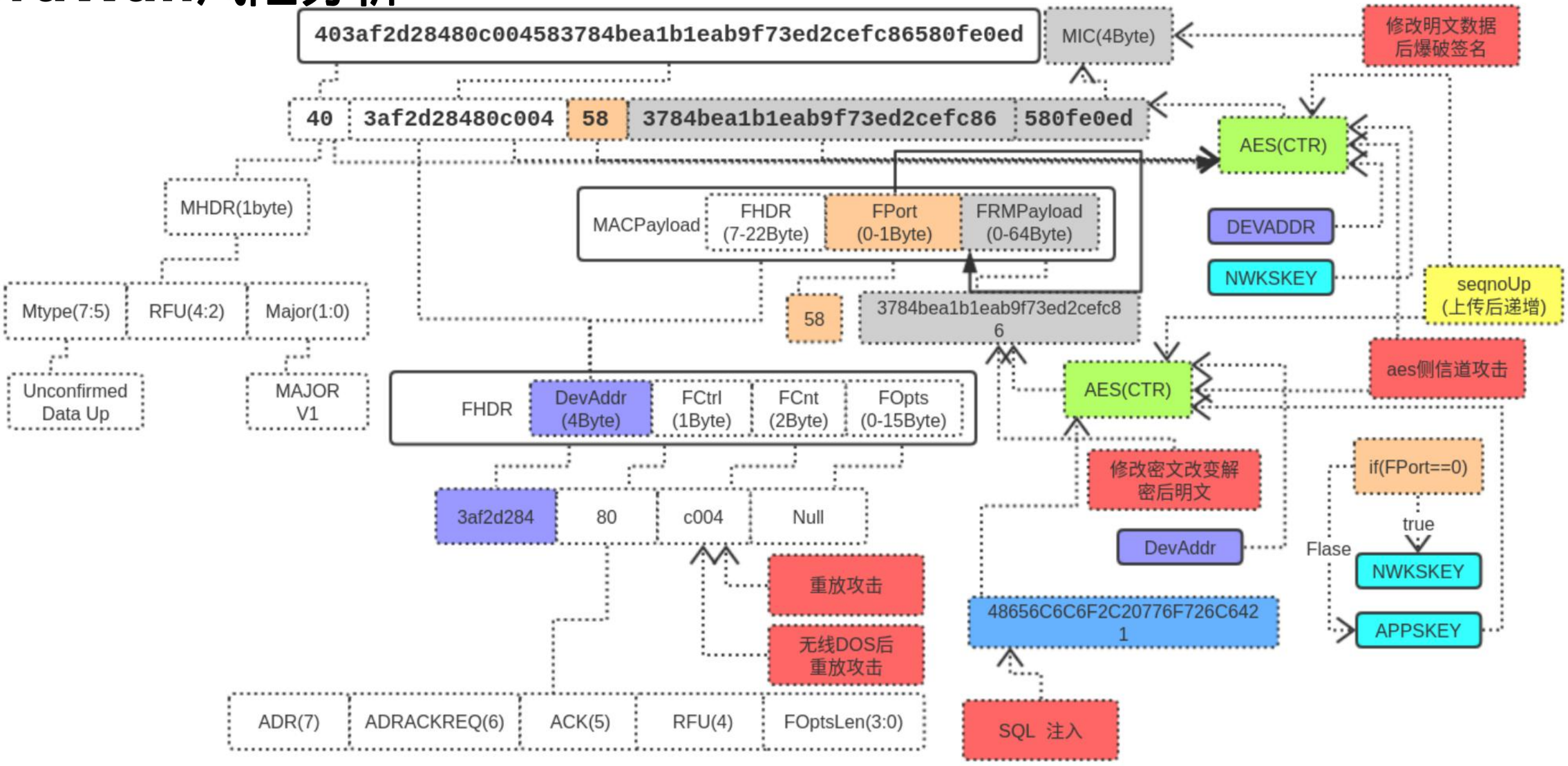

FREQ
:GSM850/EGSM900
/DCS1800/PCS1900
Lora网关
UID:6B44D4A0945902E0
NID:1 CH:150 Freq 498.75
GPRS 模块:ZTE MG2618
主控芯片:ATSAMG55J19
射频芯片配置MCU:m17m5v
Lora射频芯片:SX1278
512Kb储存芯片:fm24c512d
ZTE MG2618
GPRS 模组
LORA 水表
移动2G网络
IP：XX.XX.196.229
端口：50001
协议：TCP 私有协议
服务器
伪造网关
上传数据
GPRS中间人
攻击网关
FREQ :470-510MHZ
2G伪基站
OPENBTS
私有协议
lora 调制
修改水表用量
嗅探他人无线
数据 判断该住
户是否有人
伪造传感器
探测结果
SX1278
硬件SPI
嗅探
Freq：470-510
BW:125K
SF:11
CR:4/5
PL:6
SW:0x12
SX1278
Arduino
攻击者
通过强磁让
传感器失灵
LORA 水表

LoraWan风险分析



Lorawan 协议章节:
https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf

LoraWan风险分析



Thank You !