Long-range and Secure Communication System for Remote Data Logging and Monitoring of Micro-grids

Presented by: Amjad Iqbal
Supervised by: Prof. Tariq Iqbal

March 19, 2019

Contents

Contents

Introduction & Motivation

- Distributed generation and growing renewable energy
- Fermeuse and WEICAN wind farms' communication issues
- Insecure SCADA system and disastrous breach
- Georgian electric grid and Wall Street Journal report
- Communication security algorithm

SCADA System Communication Security Requirements

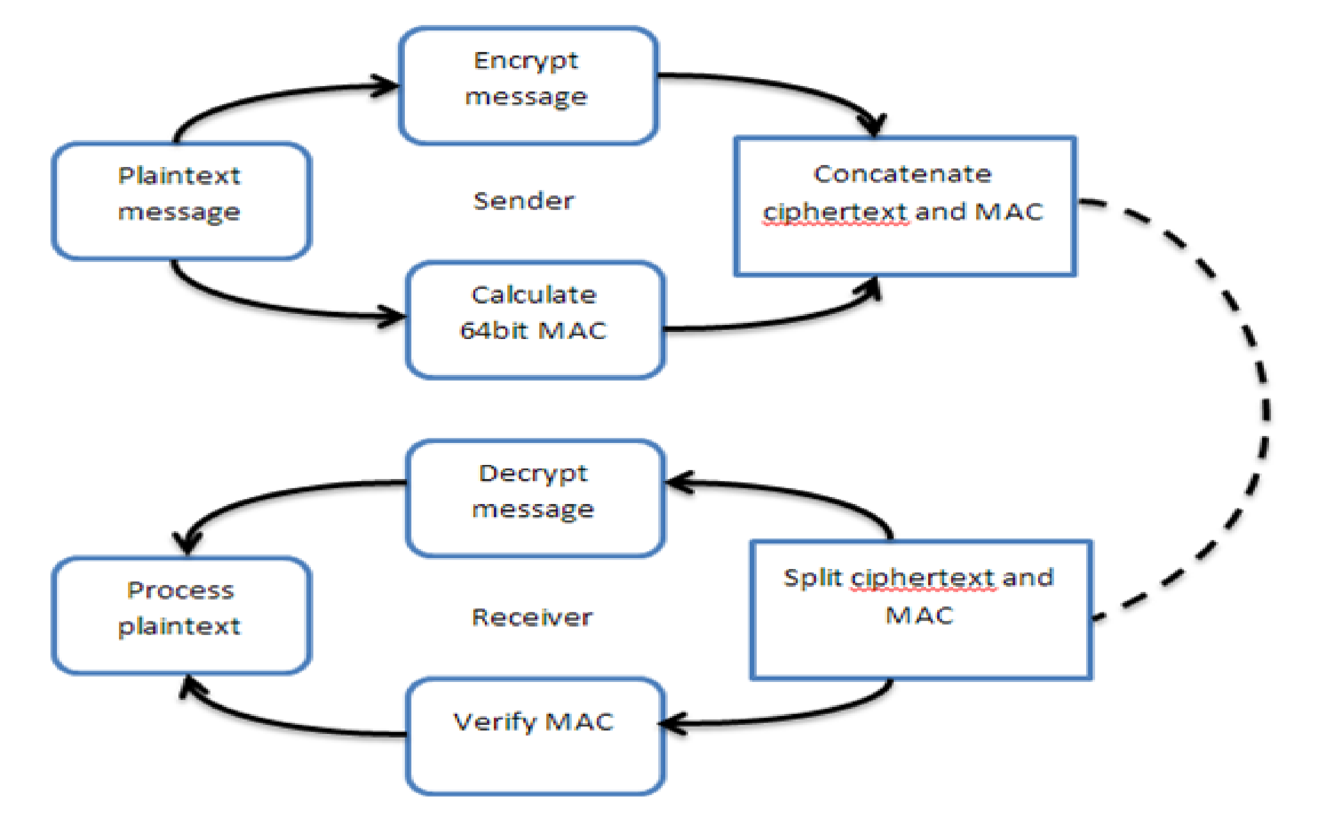
- PRIVACY
- MESSAGE AUTHENTICATION
- INTEGRITY
- NON-REPUDIATION
- LOW-COST
- POWER EFFICIENT

Selection of LoRa Technology and SF (whistle)

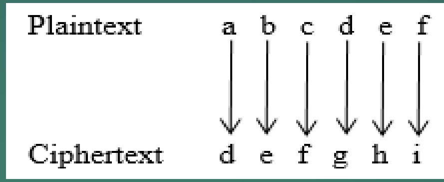
Technology			Data Rate	Coverage	Remarks
Copper Wired PLC			2-3Mb/s	1km to 3 km	Unreliable and noisy due to harmonics
DSL	Wired Internet		Max 1Gb/s	100m	High capital cost for installation and least flexible
DSL	Fiber Optic		Max 14Tb/s	160km	Extremely high capital cost for installation and least flexible for SG
Wireless	Wireless Local Area Network		54Mb/s	200m to 400m	Short Range, Vulnerable to EMI, Easy Installation
Wireless	GSM		14.4kb/s	1km to 10km	Poor Data rate, Monthly cost, Low availability in remote locations
Wireless	BlueTooth		250Mb/s	70-100m	Limited Coverage, Limited number of nodes
Wireless	WifiWLAN		600Mb/s	100m	Small Coverage, Inherent drawbacks of Wireless Mesh Network
Wireless	Radio Teletype		100b/s	Input supply dependent (0.7mV/m)	Outdated and analogue, Uses Electromechanical setup
Wireless	Optical Wireless Communication		622Mb/s	Unlimited	Costly setup, Under experimental phase
Wireless	WiMAX		75Mb/s	10-50km (Line of Sight) 1-5km (OFF LOS)	Poor penetration in obstacles due to HF, Inherent drawbacks of HF
Wireless	Satellite Communication		1Gb/s	Unlimited	High Cost, Signal fading due to snow and rain, Signal latency
Wireless	GPRS		170kb/s	1km to 10km	Poor Data rate, Less reliable due to voice traffic
Wireless	Lora		Depends upon SF	5km to 15km	Low cost, Power saver, Easy Installation, Low data rate
Wireless	Zigbee		250kb/s	30m t0 50m	Short Range, Poor Data rate, Easy Installation
Wireless	SigFox		100b/s	3-10km (Urban)	Low cost, High Scalability, Low data rate, Restricted number of messages per day
Wireless	Cellular	Global Packet Radio System –GPRS- (2G)	170kb/s	1km to 10km	Poor Data rate, Licensed frequency band, Easy Installation
Wireless	Cellular	High Speed Downlink Packet Access-HSDPA- (3G)	384KB/S TO 14.4Mb/s	1-10km	Licensed frequency band, Easy Installation, Limited availability
Wireless	Cellular	Long Term Evaluation-LTE-(4G)	Max 42 Mb/s	1-10km	Licensed frequency band Easy Installation Limited availability

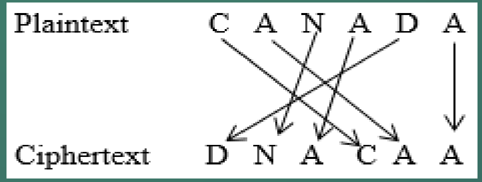
Secure Communication Flow Chart

- From plaintext, calculate unique MAC and encrypt message
- At the receiver end, the received message is decrypted and new MAC is calculated, and is compared with the received MAC to check the message security and authenticity



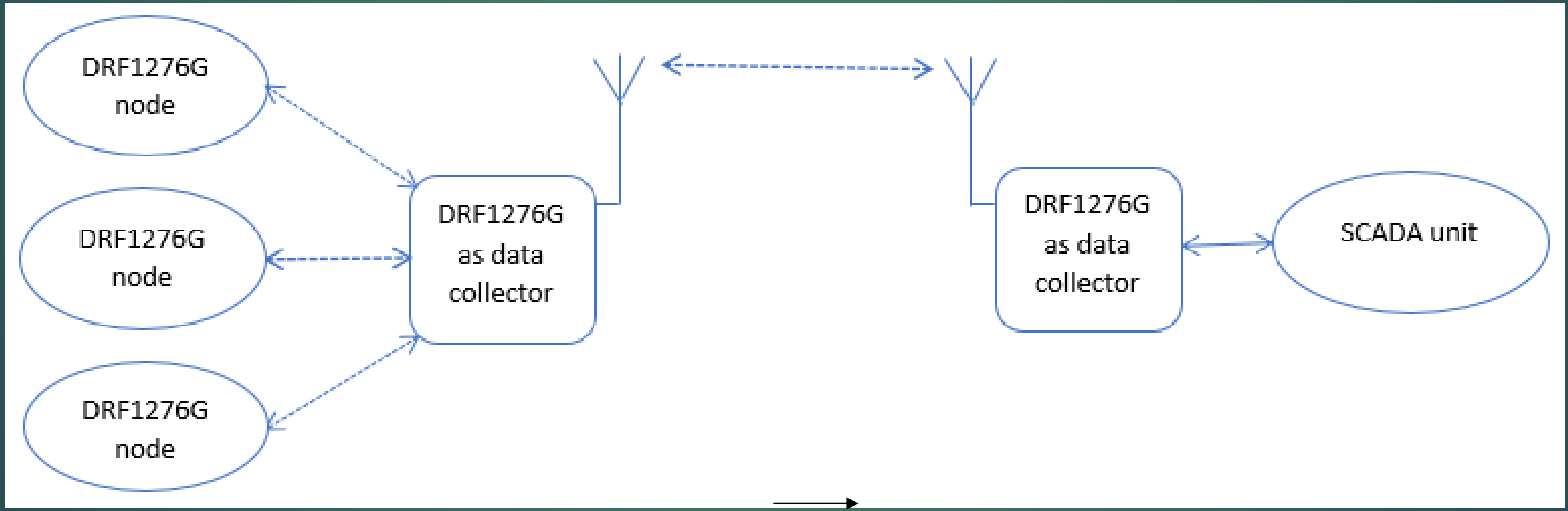
Implementation of Encryption Algorithms

- Shift Cipher
  - 

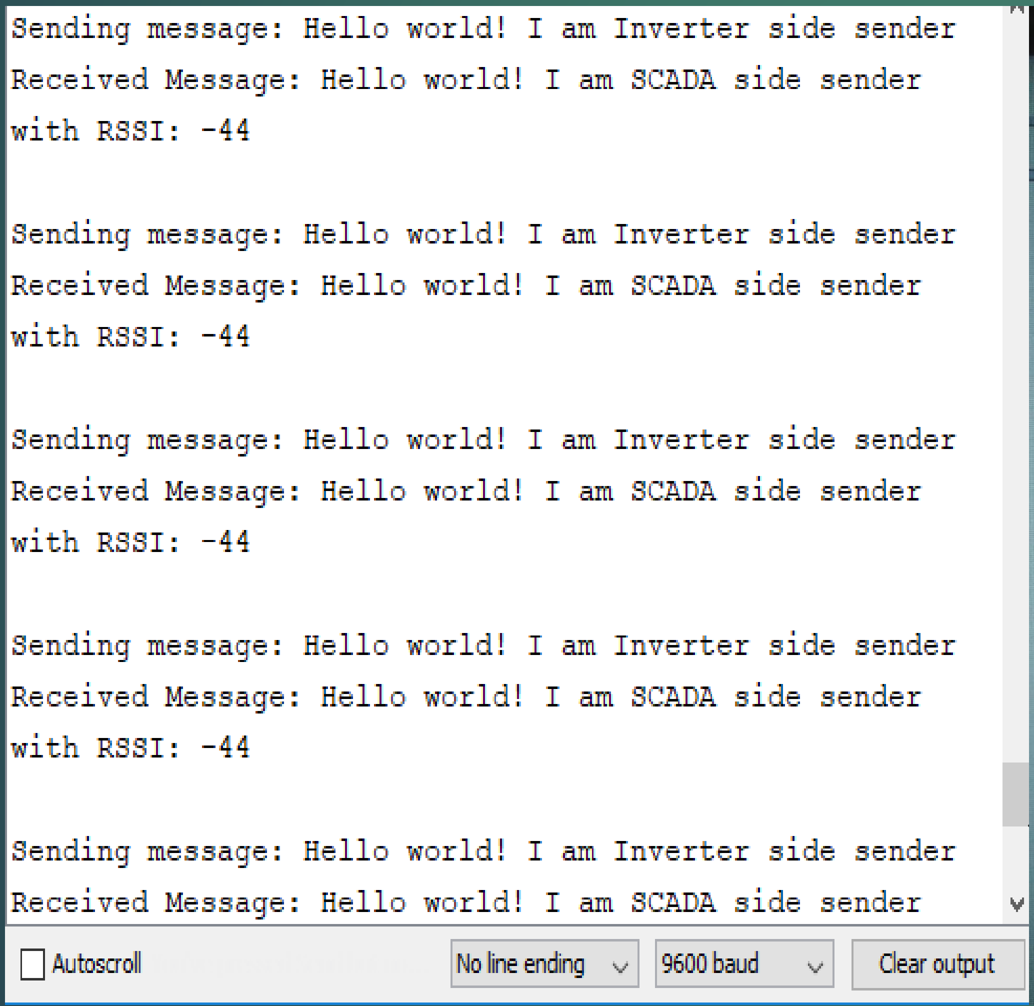
    (key space 26)
- Affine Cipher
  - $y=a*x+b$ (key space p(a)*p(b))
- Substitution Cipher
  - ab → cy (key space N!)
- Transposition Cipher
  - 

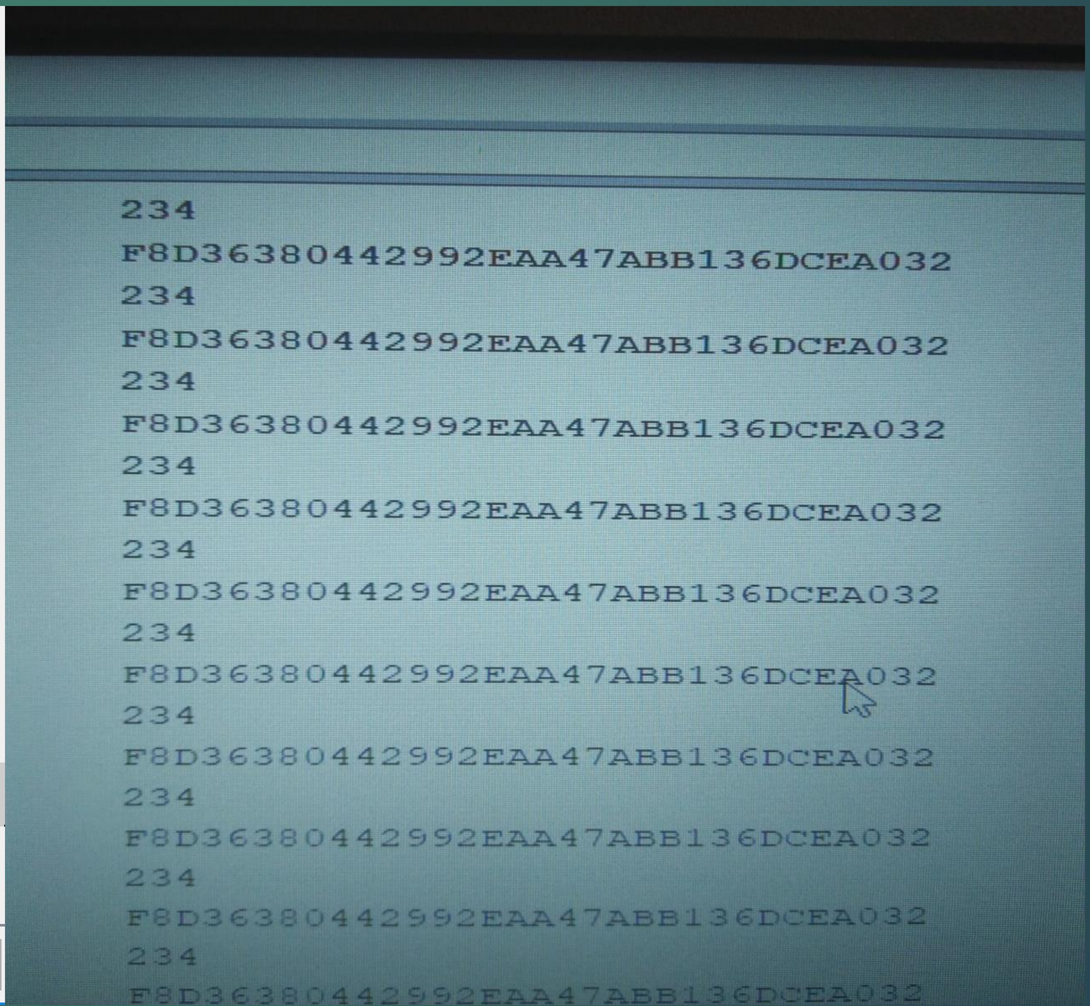
    (key space n!)
- Hill Cipher
  - ab → ci (key space N^n^2)

System Structure Based Upon Arduino with DRF1276G



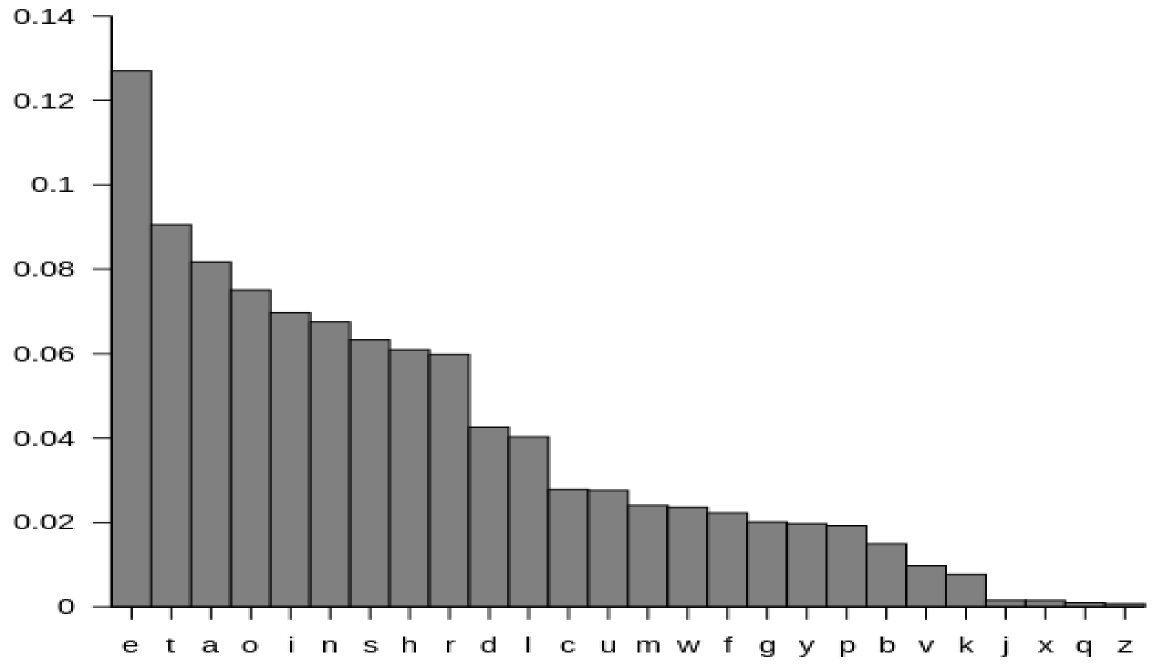
Arduino with DRF1276G based two-way communication and encryption results





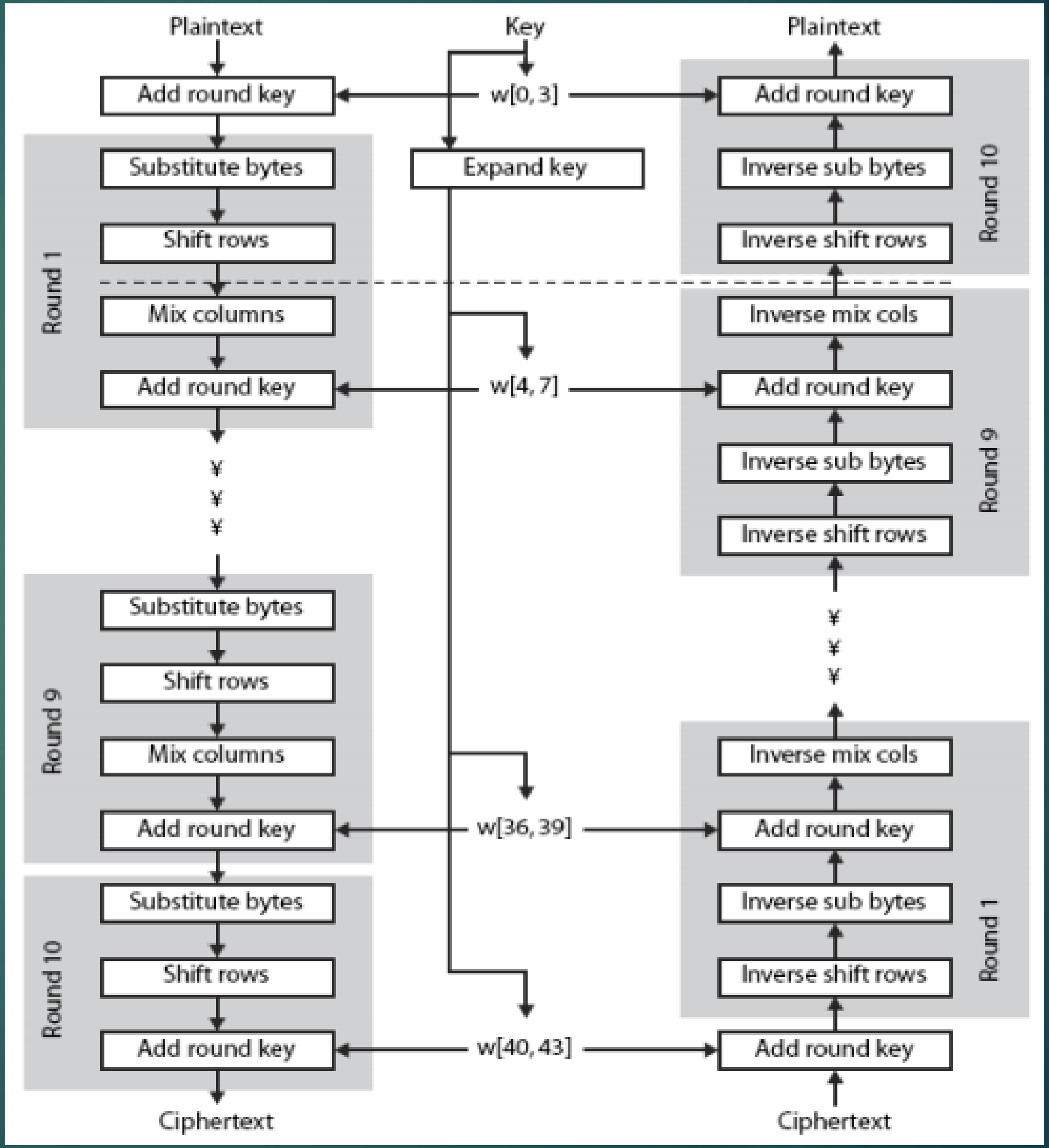
Breaching Encryption Algorithms

- FUGOMRPKWODRDTJHDTHPQTJDADFKLZDTYFWCDLJDALRPNNQV PHZDRF
- **Themonkeyspawpartiwithoutthenightwascoldandwetbutinthe**



- Occurrence frequency of characters/pairs
- Encryption algorithm
- Size of the block
- C++ code

Advanced Encryption Standard (AES) Algorithms key space has 2^128



AES Secrecy

- Perfect secrecy (almost impossible to break regardless of time and resources used but, all known ciphers are relatively secure)
- Enumeration of large numbers

AES key size is 2^128, a glance at 2^128 calculations

2^128 vs 2^100

2^100en≈40,000b years

@ 1encryption/ns)

Time for evolution of a species ≈ 2^{20} years
Age of the earth = 2^{32} years
Bits in a terabyte drive = 2^{43}
Cells in the human body ≥ 2^{46}
Amount of water in the Great Lakes = 2^{53} gallons
Estimate of atoms in observable universe ≈ 2^{265}

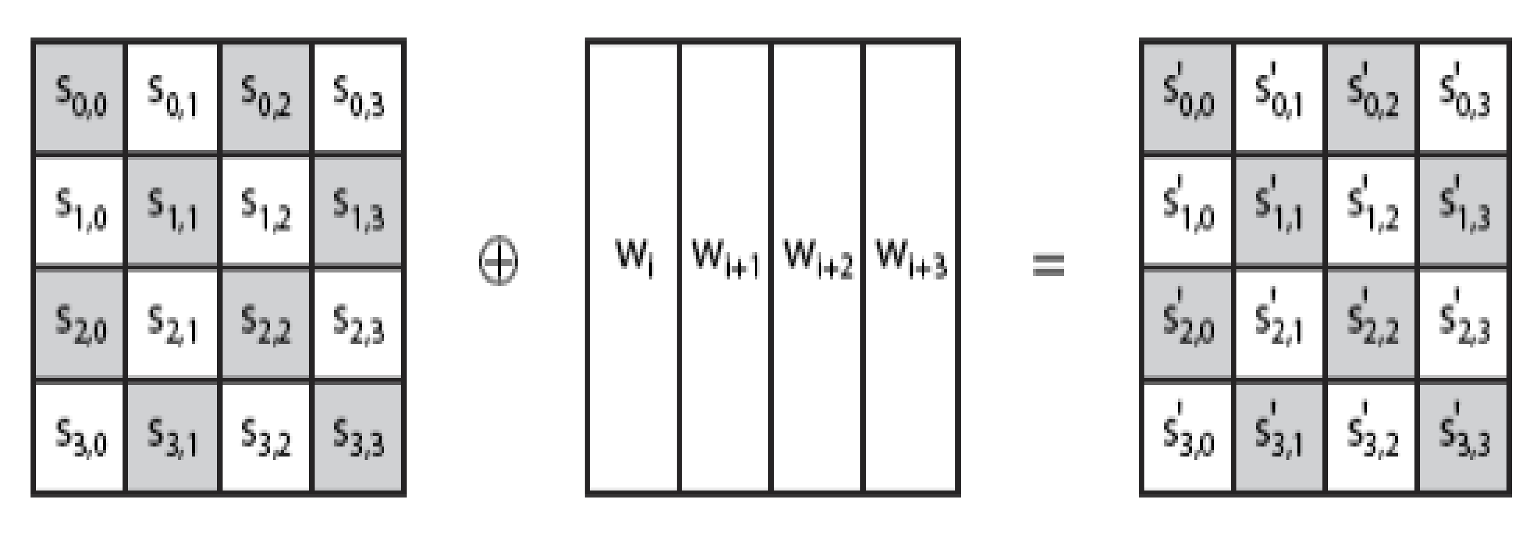
Advanced Encryption Standards (AES) Algorithm

- Flexibility in changing key
- Multiple rounds and increased confusion
- Add round key
- Substitute bytes with Rajindal’s table
- Shift rows
- Mix columns

AES Implementation

Generate and Add Round-key

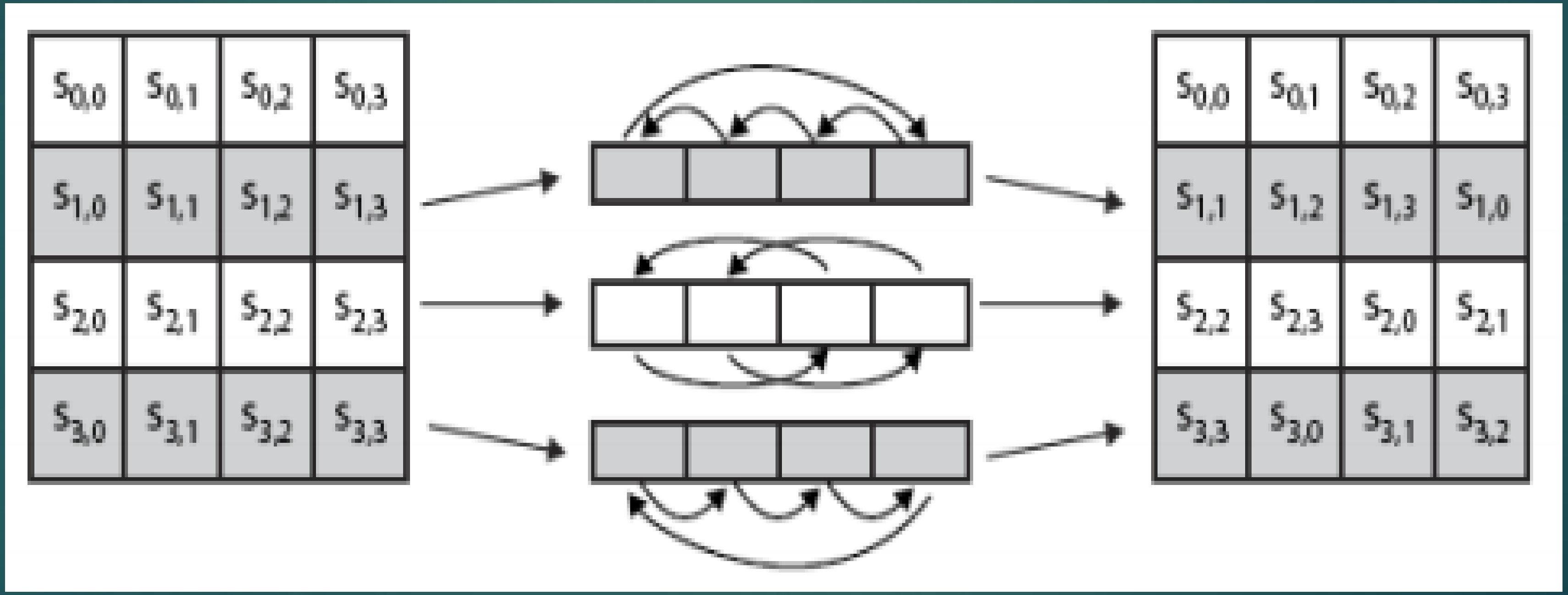
- A 128bit key is generated and XORed with the string of 128bit plaintext before and after each round



- After adding round key, resultant bytes are replaced with respective Rajindal's table

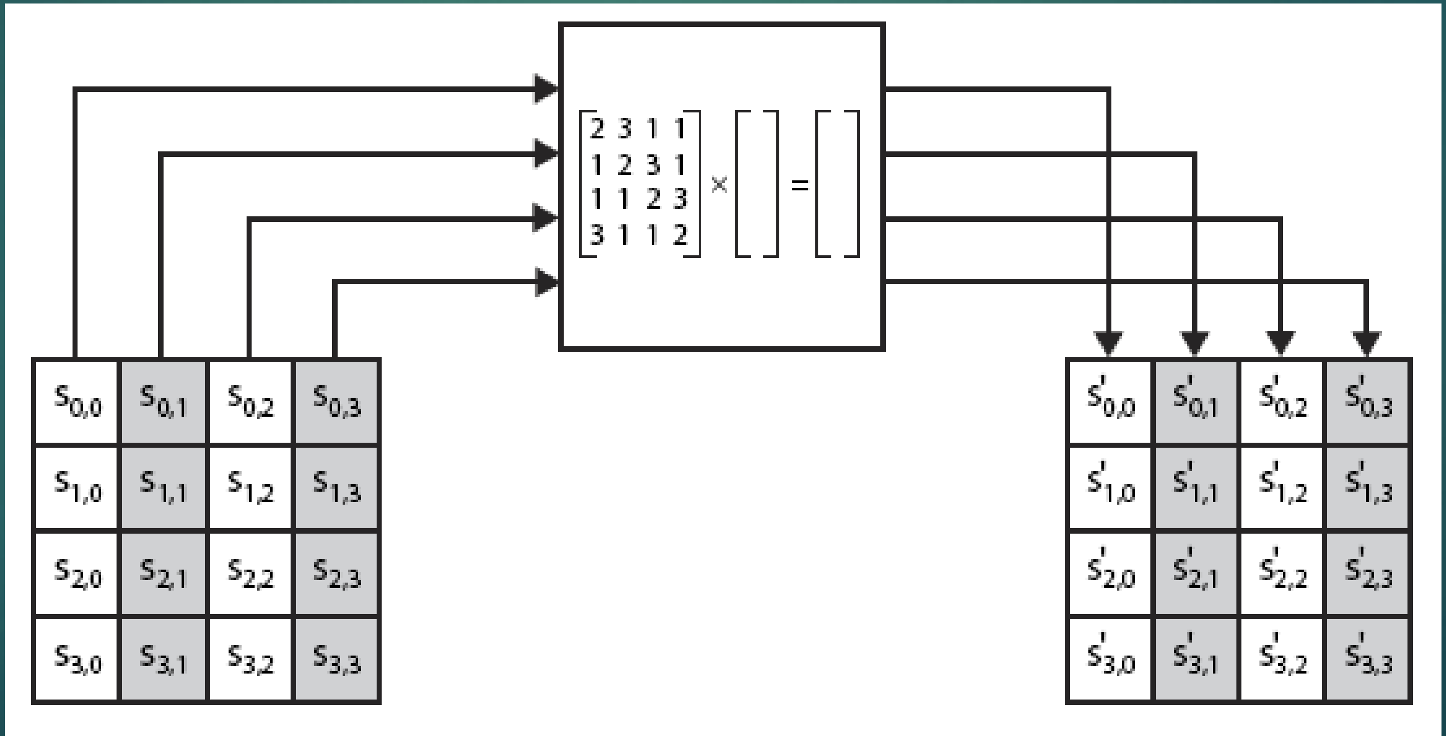
Shift Rows

- Substituted bytes are rotated left/right to increase the confusion within the same round



Mix Columns

- Substitution bytes results undergo through bit-level multiplication (involving 1's and 2's complements) and again results are replaced with Rajindal's inverse matrix



Message Authentication Code (MAC)

- MAC is unique for every message
- Fixed size of 64bits regardless of message length
- Derived from the XOR combination of plaintext and ciphertext bits
- Helpful in detecting a single bit change due to
  - Electromagnetic Interference
  - Eavesdropper
  - Channel Failure
  - Noise

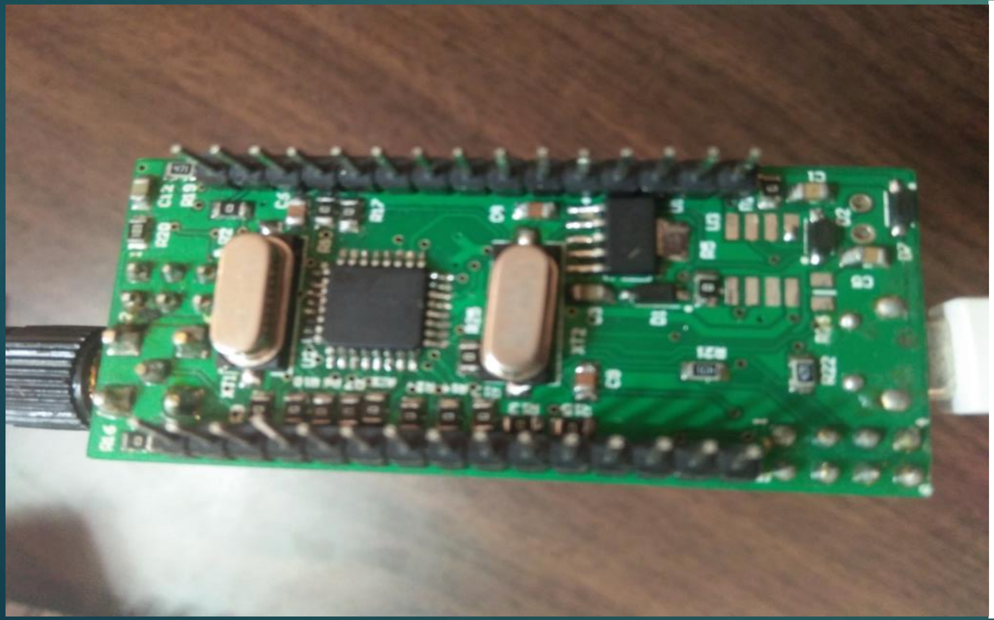
Authenticity and MAC address

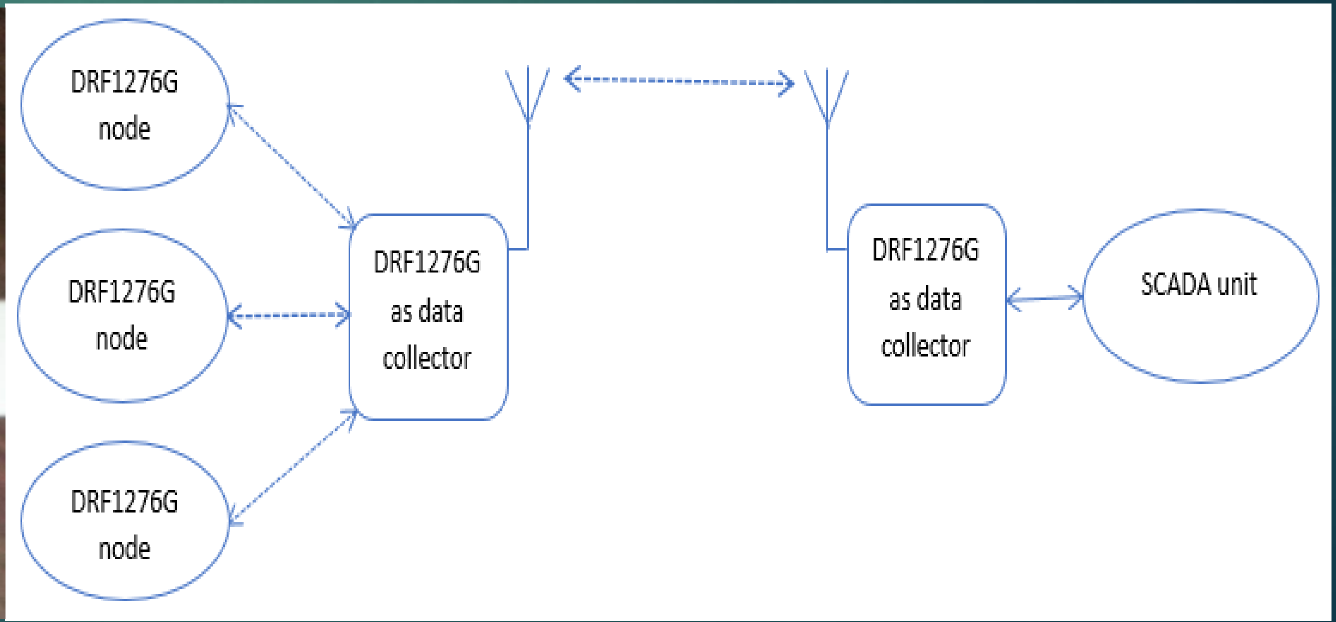
- MAC is concatenated at the end of encrypted string before transmitting the message
- Receiver splits MAC from message and decrypts the message
- From decrypted message again MAC is calculated using secret key and is compared with received MAC to check message authenticity
- Message is processed after ensuring authenticity. In case of mismatch message is discarded assuming fake/eavesdropper involvement

Results

Arduino-uno+LoRa (DRF1276G) based System Structure

- DRF1276G supports relatively simple encryption algorithms in given system structure
- It does not support AES due to flash and processor limitations





Ciphertext with Arduino-uno+LoRa

- Results show that arduni-uno with LoRa (DORJI DRF1276G) does not support 128AES due to flash size and ALU limitations

```
final ciphertext:
pre-encrypt(plain_text):       0123456789ABCDEF0123456789ABCDEF
Ciphet-text after 1
Ciphet-text after 2 rounds:
Ciphet-text after 3 rounds:
Ciphet-text after 4 rounds:
Ciphet-text after 5 rounds:
Ciphet-text after 6 rounds:
Ciphet-text after 7 rounds:
Ciphet-text after 8 rounds:
Ciphet-text after 9 rounds:
final ciphertext:
pre-encrypt(plain_text):       0123456789ABCDEF0123456789ABCDEF
Ciphet-text after 1
Ciphet-text after 2 rounds:
Ciphet-text after 3 rounds:
Ciphet-text after 4 rounds:
Ciphet-text after 5 rounds:
Ciphet-text after 6 rounds:
Ciphet-text after 7 rounds:
Ciphet-text after 8 rounds:
Ciphet-text after 9 rounds:
final ciphertext:
pre-encrypt(plain_text):       0123456789ABCDEF0123456789ABCDEF
Ciphet-text after 1
Ciphet-text after 2 rounds:
Ciphet-text after 3 rounds:
Ciphet-text after 4 rounds:
Ciphet-text after 5 rounds:
Ciphet-text after 6 rounds:
```

Ciphertext with ESP-32

- ESP32 not only supports 10 rounds of AES encryption but also 64 bit MAC calculations

```
pre-encrypt(plain_text):        0123456789ABCDEF0123456789ABCDEF
Ciphet-text after 1 rounds:     4023CABB284333AC463817F42893333D
Ciphet-text after 2 rounds:     4716512657507AE6F0BFB407EBEC5817
Ciphet-text after 3 rounds:     89C5F20861099F9EEB73639A0BE8D3EA
Ciphet-text after 4 rounds:     F1D452604C3119F03577B2790FF6A34D
Ciphet-text after 5 rounds:     92A6C59992FDB6A8A8452D28E3764214
Ciphet-text after 6 rounds:     A0DAD27C43FE5684D8349F6EFA113858
Ciphet-text after 7 rounds:     D71F17D9383AFE1FF08EA6657040EED5
Ciphet-text after 8 rounds:     512E95839F96762F9C544D00A66FFA17
Ciphet-text after 9 rounds:     FF75BAA2661F246560821DBD47D73AB2
final ciphertext:               FF75BAA2661F246560821DBD47D73AB2
pre-encrypt(plain_text):        0123456789ABCDEF0123456789ABCDEF
Ciphet-text after 1 rounds:     4023CABB284333AC463817F42893333D
Ciphet-text after 2 rounds:     4716512657507AE6F0BFB407EBEC5817
Ciphet-text after 3 rounds:     89C5F20861099F9EEB73639A0BE8D3EA
Ciphet-text after 4 rounds:     F1D452604C3119F03577B2790FF6A34D
Ciphet-text after 5 rounds:     92A6C59992FDB6A8A8452D28E3764214
Ciphet-text after 6 rounds:     A0DAD27C43FE5684D8349F6EFA113858
Ciphet-text after 7 rounds:     D71F17D9383AFE1FF08EA6657040EED5
Ciphet-text after 8 rounds:     512E95839F96762F9C544D00A66FFA17
Ciphet-text after 9 rounds:     FF75BAA2661F246560821DBD47D73AB2
final ciphertext:               FF75BAA2661F246560821DBD47D73AB2
pre-encrypt(plain_text):        0123456789ABCDEF0123456789ABCDEF
Ciphet-text after 1 rounds:     4023CABB284333AC463817F42893333D
Ciphet-text after 2 rounds:     4716512657507AE6F0BFB407EBEC5817
Ciphet-text after 3 rounds:     89C5F20861099F9EEB73639A0BE8D3EA
Ciphet-text after 4 rounds:     F1D452604C3119F03577B2790FF6A34D
Ciphet-text after 5 rounds:     92A6C59992FDB6A8A8452D28E3764214
Ciphet-text after 6 rounds:     A0DAD27C43FE5684D8349F6EFA113858
```

Cipher-text with MAC

- Receiver compares received MAC and MAC derived from the received message before processing the message
- Improves data authenticity and integrity

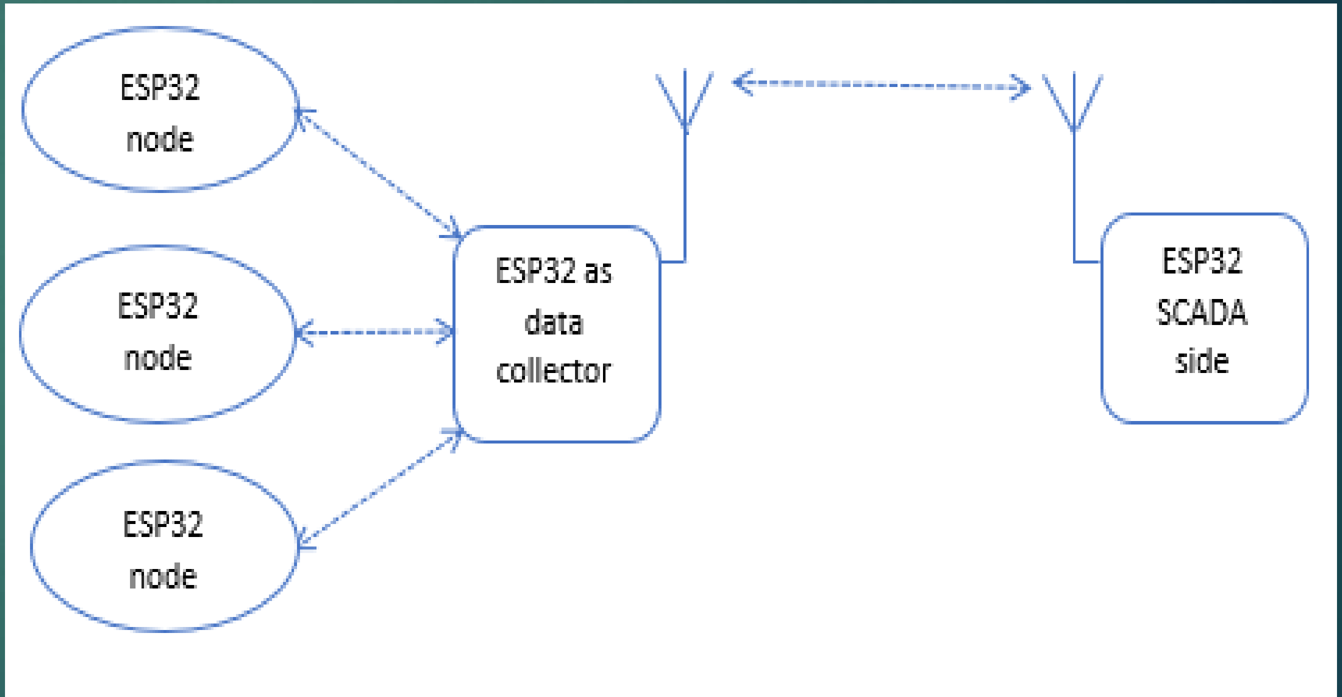
```
pre-encrypt(plain_text):         0123456789ABCDEF0123456789ABCDEF
Ciphertext without MAC is:       F9F026E7CD825F05A559FE74E4656FE9
Decrypted Plaintext:             0123456789ABCDEF0123456789ABCDEF
ciphertext with MAC:             F9F026E7CD825F05A559FE74E4656FE9410DFC5C95DFF8CE
Received_MAC:                    410DFC5C95DFF8CE
Calculated_MAC:                  410DFC5C95DFF8CE
MAC verification status:         Message is authentic.
Verified decrypted message is:   0123456789ABCDEF0123456789ABCDEF
pre-encrypt(plain_text):         0123456789ABCDEF0123456789ABCDEF
Ciphertext without MAC is:       F9F026E7CD825F05A559FE74E4656FE9
Decrypted Plaintext:             0123456789ABCDEF0123456789ABCDEF
ciphertext with MAC:             F9F026E7CD825F05A559FE74E4656FE9410DFC5C95DFF8CE
Received_MAC:                    410DFC5C95DFF8CE
Calculated_MAC:                  410DFC5C95DFF8CE
MAC verification status:         Message is authentic.
Verified decrypted message is:   0123456789ABCDEF0123456789ABCDEF
pre-encrypt(plain_text):         0123456789ABCDEF0123456789ABCDEF
Ciphertext without MAC is:       F9F026E7CD825F05A559FE74E4656FE9
Decrypted Plaintext:             0123456789ABCDEF0123456789ABCDEF
ciphertext with MAC:             F9F026E7CD825F05A559FE74E4656FE9410DFC5C95DFF8CE
Received_MAC:                    410DFC5C95DFF8CE
Calculated_MAC:                  410DFC5C95DFF8CE
MAC verification status:         Message is authentic.
Verified decrypted message is:   0123456789ABCDEF0123456789ABCDEF
```

128bit plain-text

64bit MAC

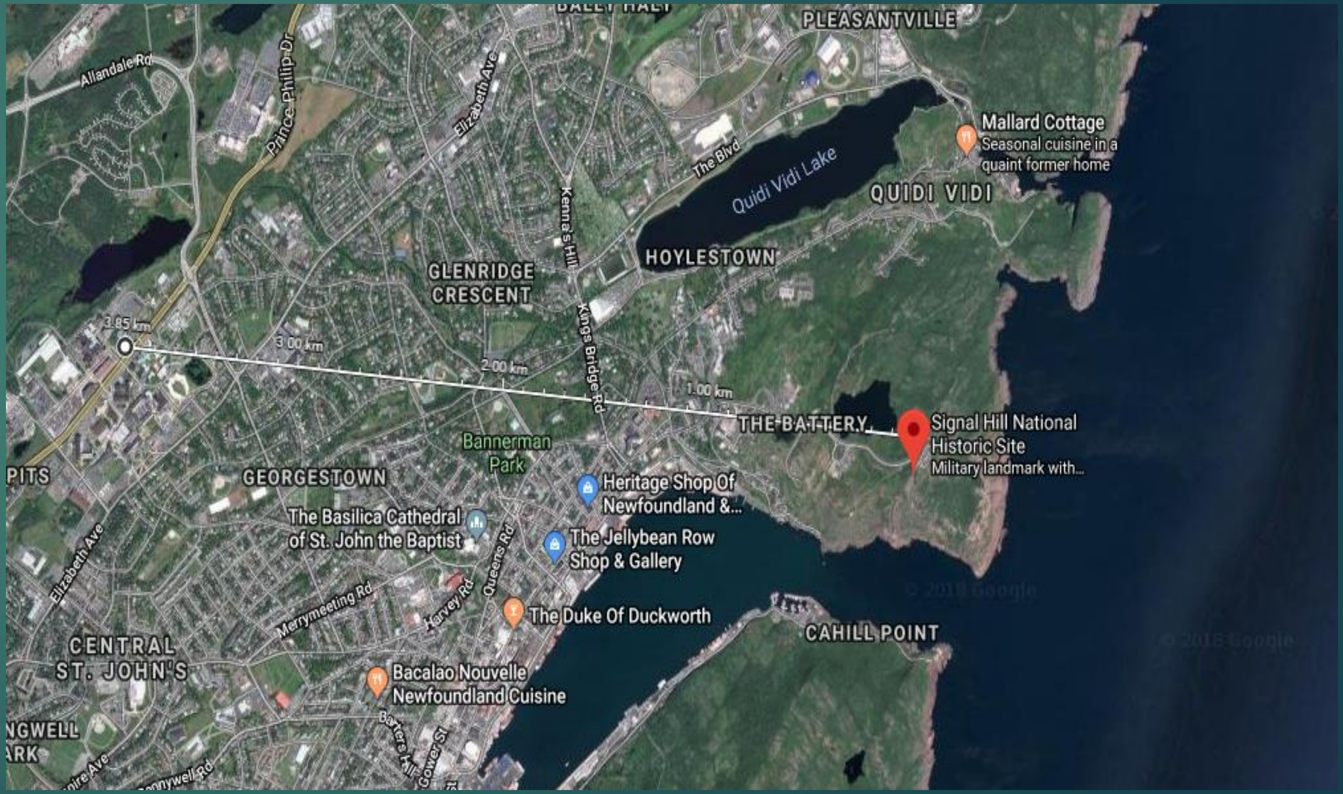
ESP32 Based System Structure with AES and MAC implementation

- AES was successfully implemented in this system topology
- It worked for MAC implementation to authenticate the messages
- It does not cost more than CAD78 (3x26) with power consumption of 500-600mW



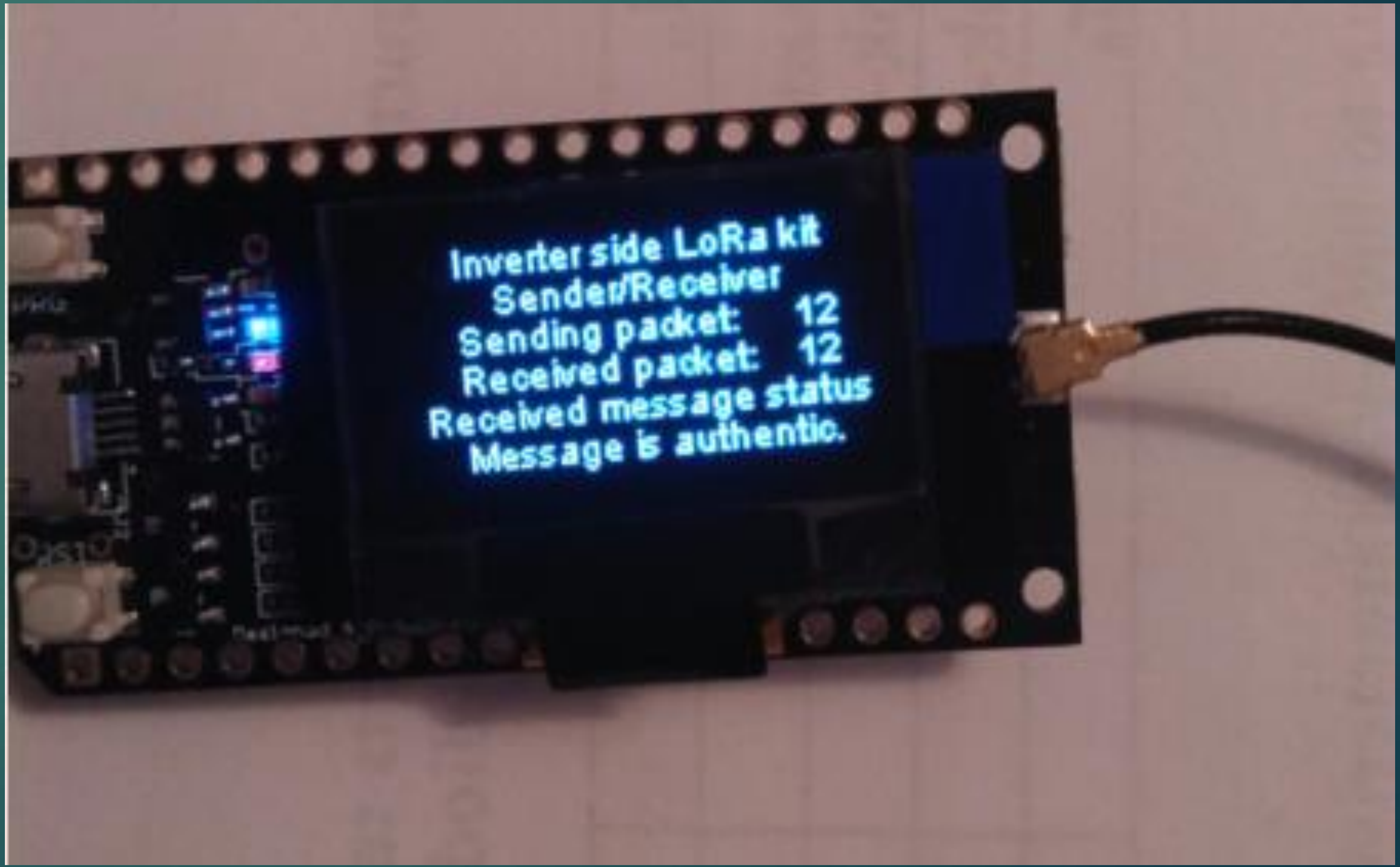
Range Testing (Successful transmission for 3.85km)

- Range Testing (Successful transmission for 3.85km)
- Range is obstacles dependent and site dependent
- Off-site range is 3-5km
- On-site upto 15km (obstacles free)



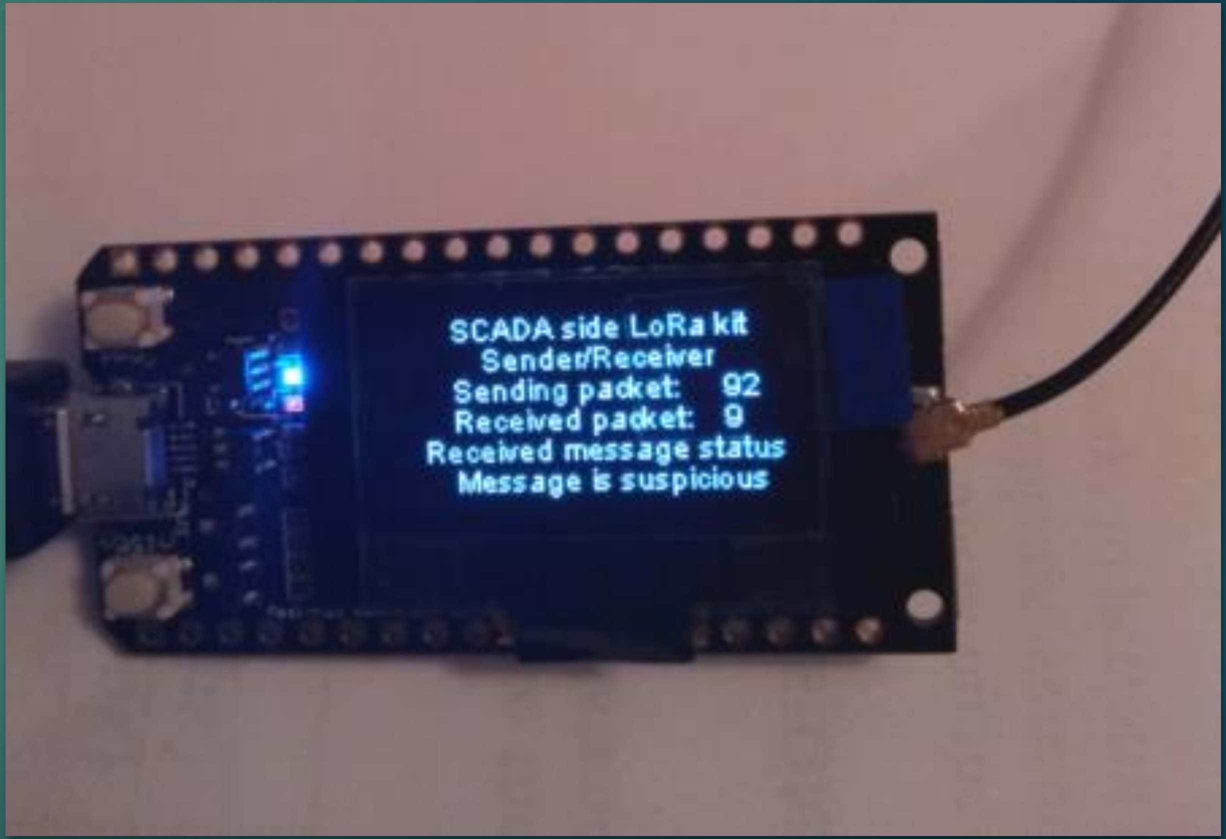
SF7 Affecting Transmission Rate and Authenticity

- Low SF gives better data rate
- Due to smaller time on air data loss decreases
- Loss free data verified through MAC improves reliability



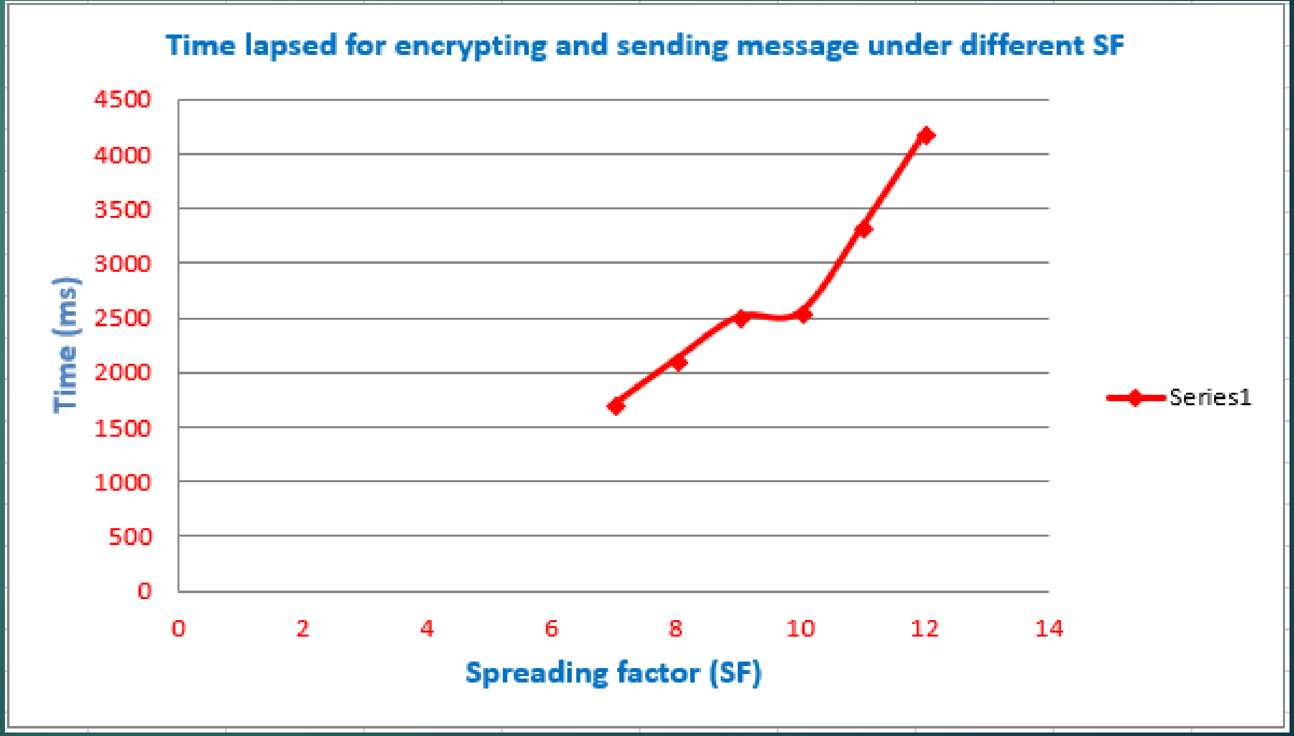
SF12 Affecting Transmission Rate and Authenticity

- Increasing SF causes slow data rate
- Due to increase time on air data loss occurs
- Due to mismatch in received and calculated MAC system perceives that as the intervention of any eavesdropper



SF vs Delay in Encrypting and Sending

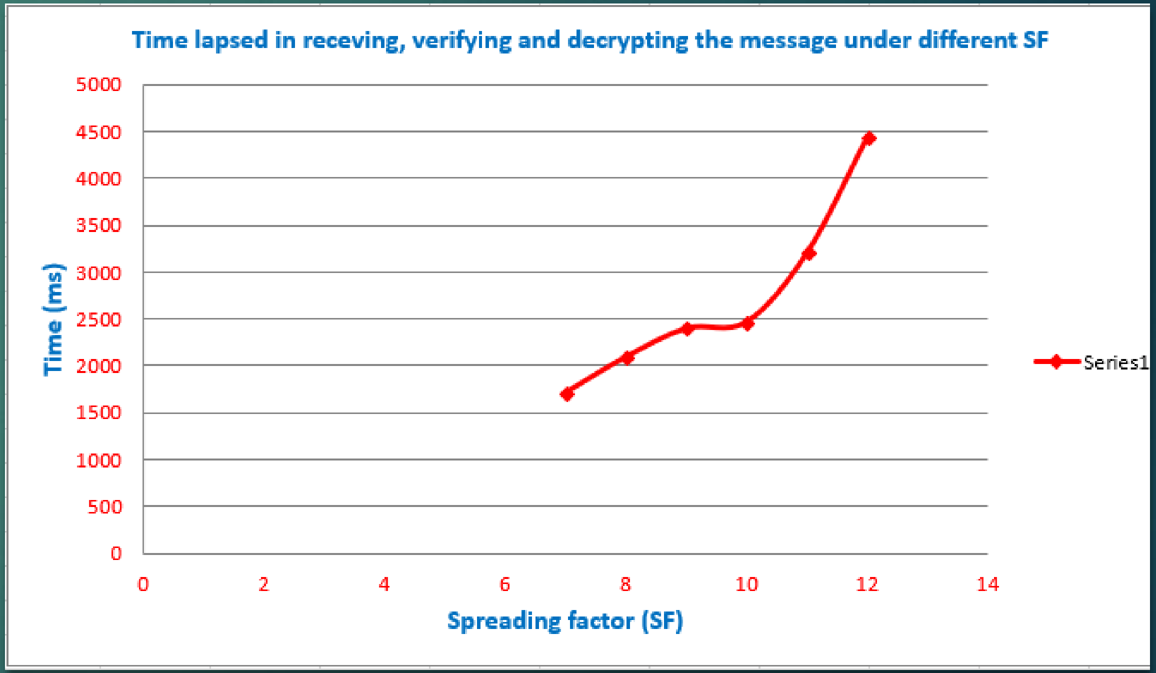
- Higher spreading factor requires more time for
  - Message encryption
  - Verification
  - Decryption



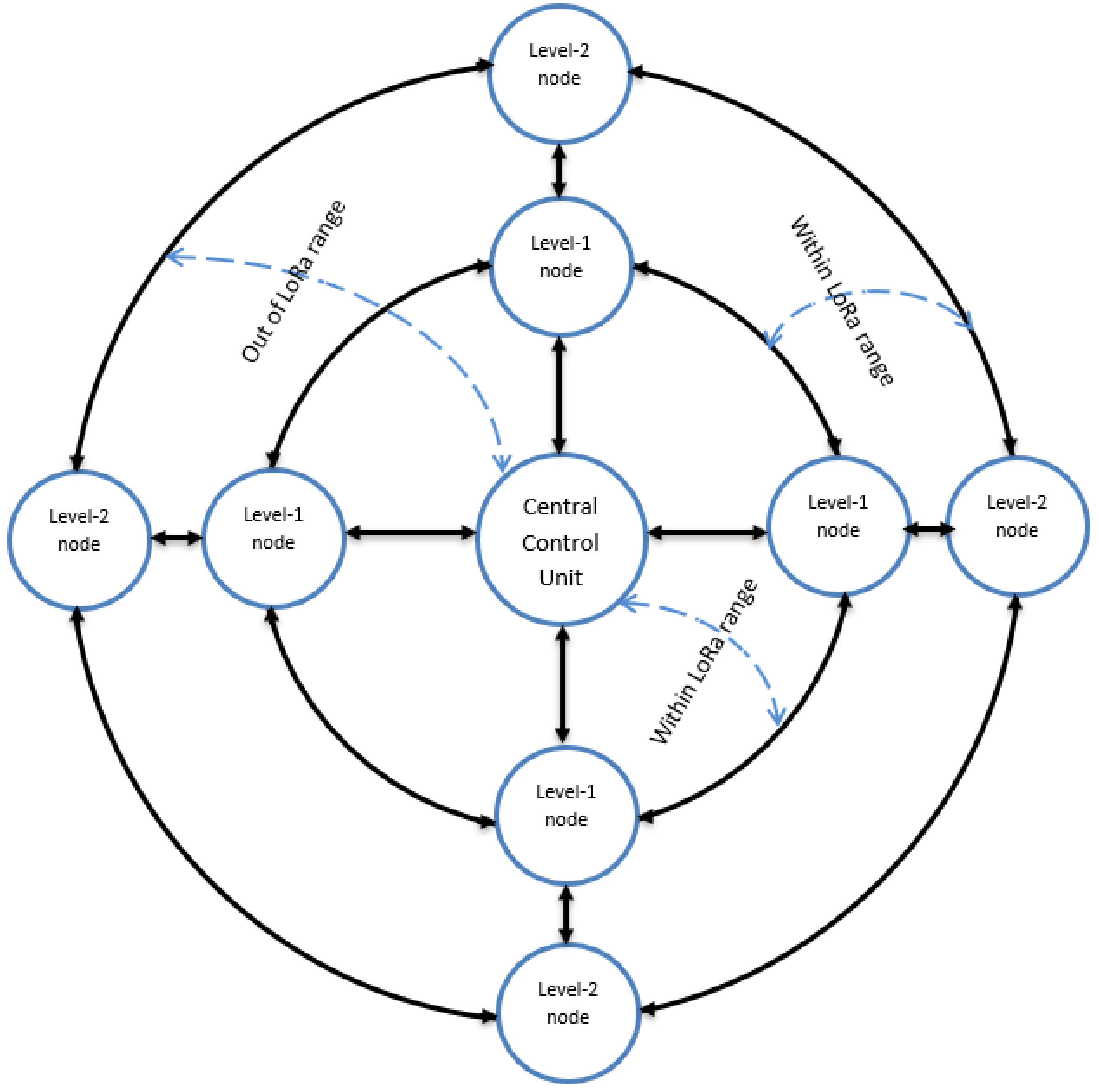
SF vs Delay in Receiving, Verifying and Decrypting

- With increasing spreading factor message on air time increases due to which overall time required for
  - Message receiving
  - Verifying and
  - Decrypting

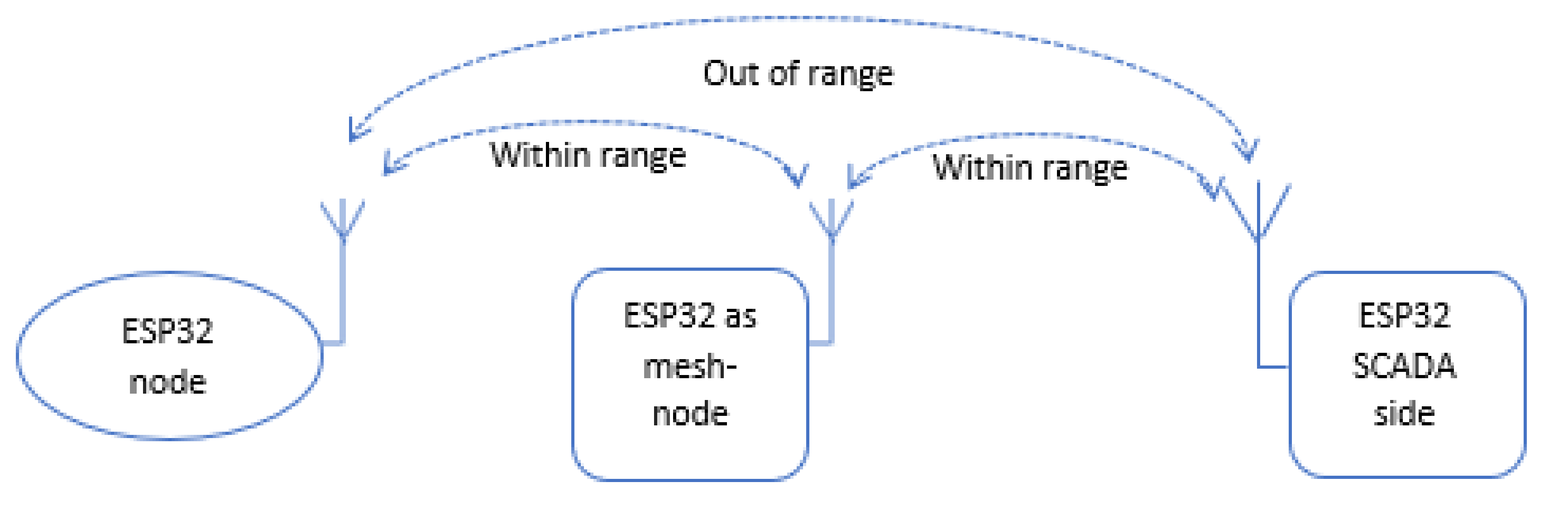
  also increases
- At low spreading factor message on air time is low but, range is shorter as compared to higher spreading factor
- At higher spreading factor data loss/bit error occurs due to increase in air time



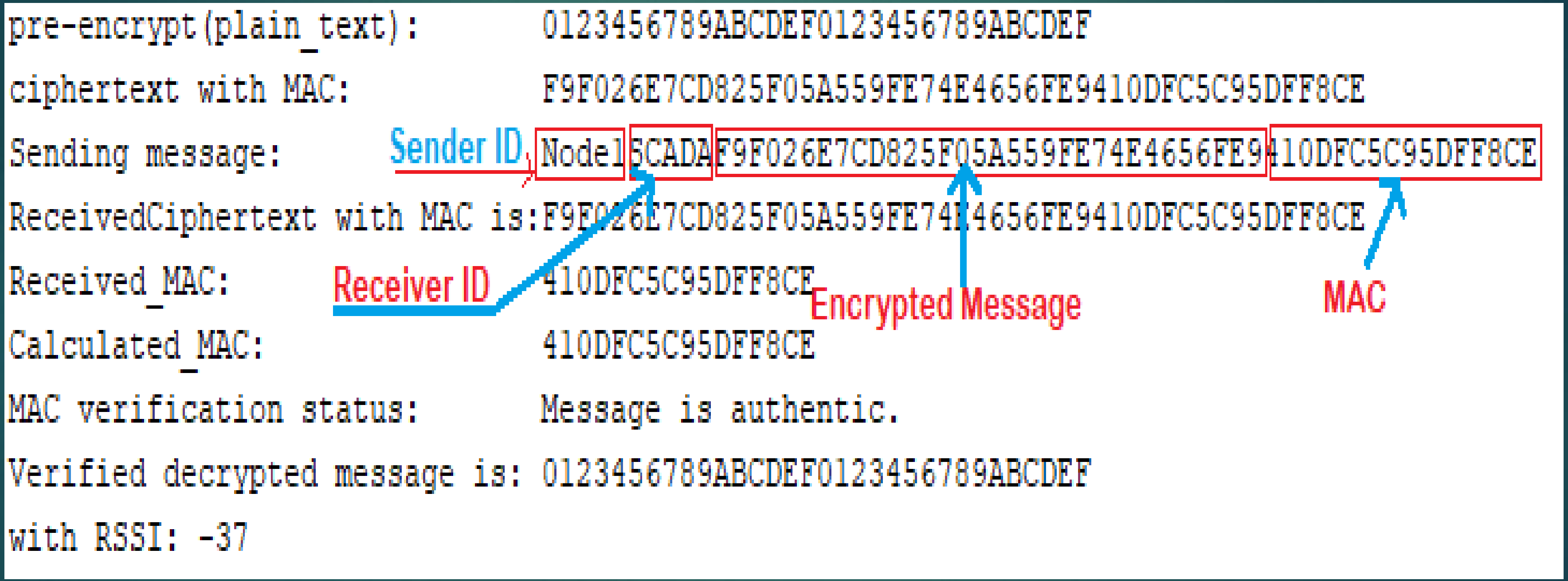
LoRa Mesh-network to Improve Range



Mesh-network Implementation and Testing



Mesh-network Implementation and Testing

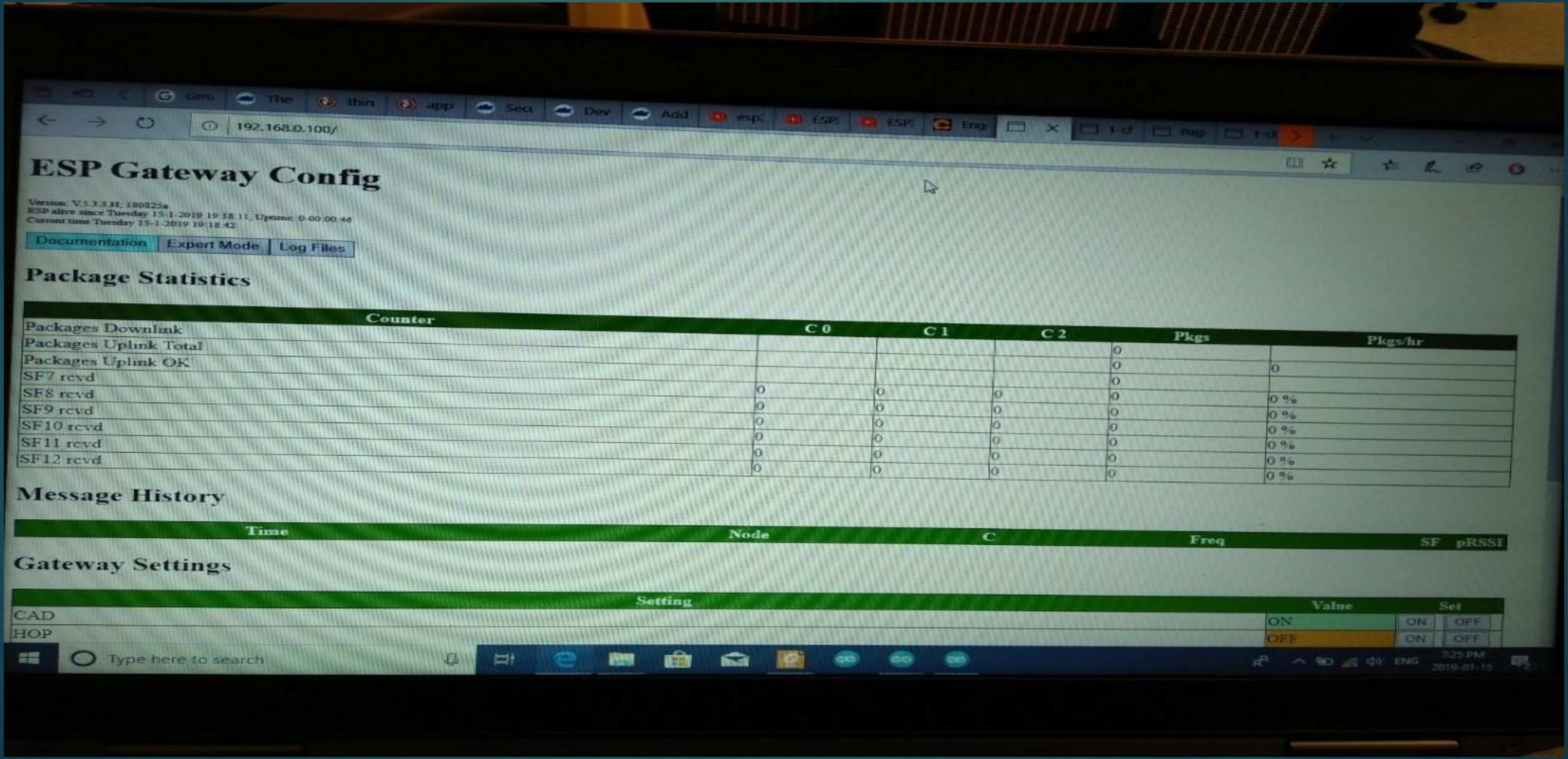


Mesh-network Implementation and Testing

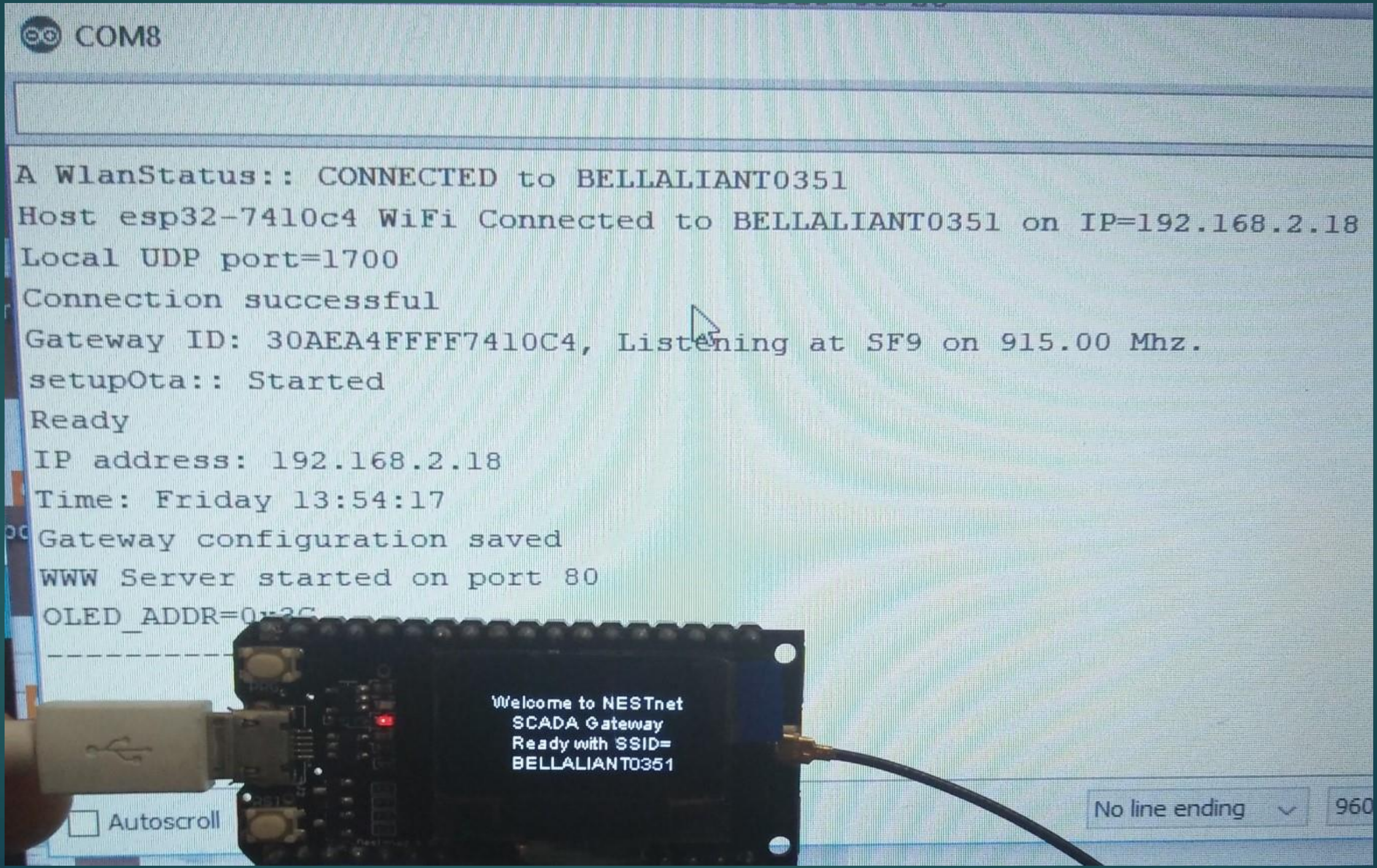
Local Data Logging

```
SD Card Size: 7580MB
Listing directory: /
  FILE: /test.txt  SIZE: 1048576
  FILE: /foo.txt  SIZE: 13
  DIR : /my_new_directory_1
Creating Dir: /mydir
Dir created
Listing directory: /
  FILE: /test.txt  SIZE: 1048576
  FILE: /foo.txt  SIZE: 13
  DIR : /my_new_directory_1
  DIR : /mydir
Removing Dir: /mydir
Dir removed
Listing directory: /
  FILE: /test.txt  SIZE: 1048576
  FILE: /foo.txt  SIZE: 13
  DIR : /my_new_directory_1
Listing directory: /my_new_directory_1
Writing file: /bytes.txt
File written
Appending to file: /bytes.txt
Message appended
1048576 bytes read for 2905 ms
1048576 bytes written for 4913 ms
Total space: 7563MB
```

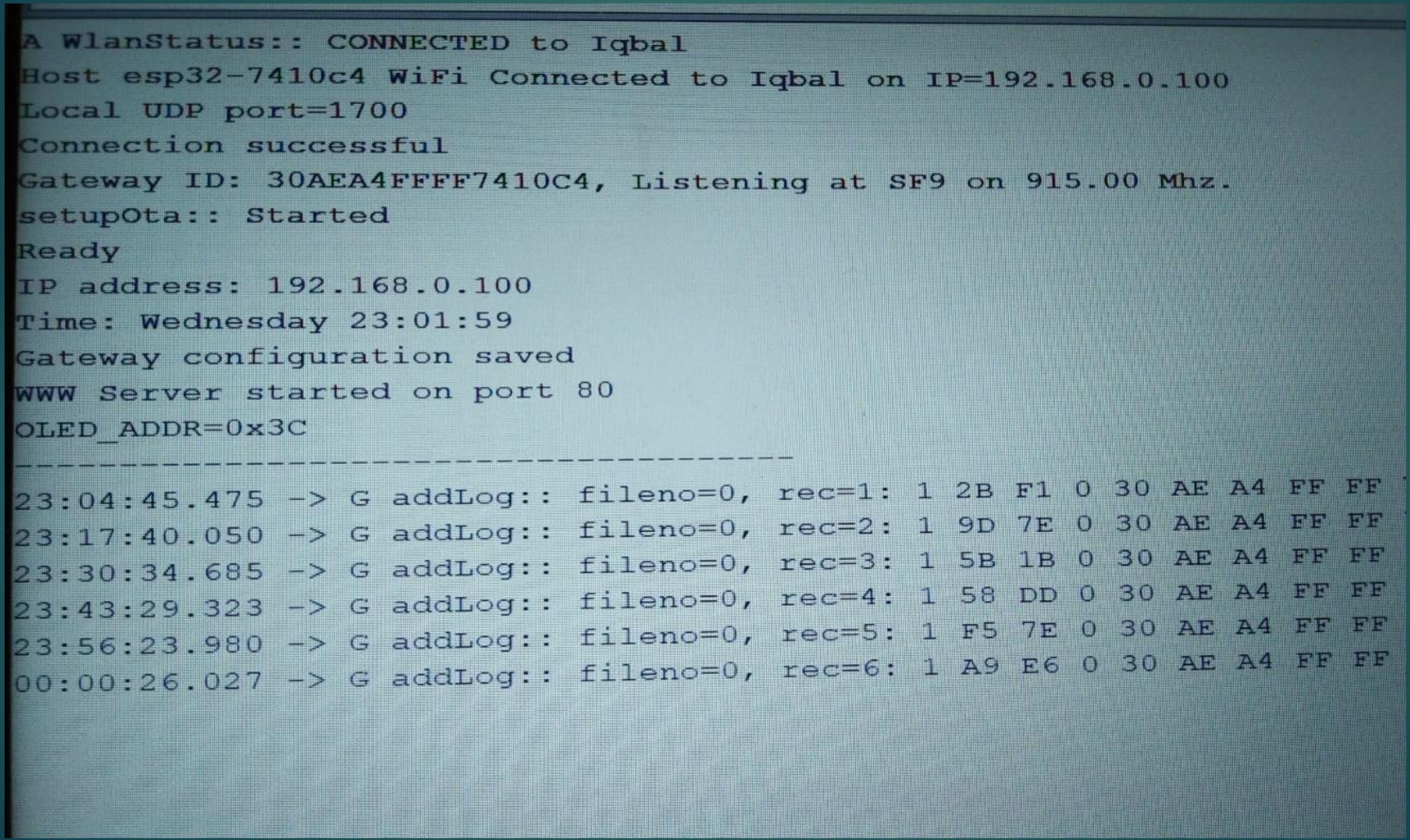
Remote Data Logging (Configuring ESP32 as a Gateway)



ESP32 as a Gateway

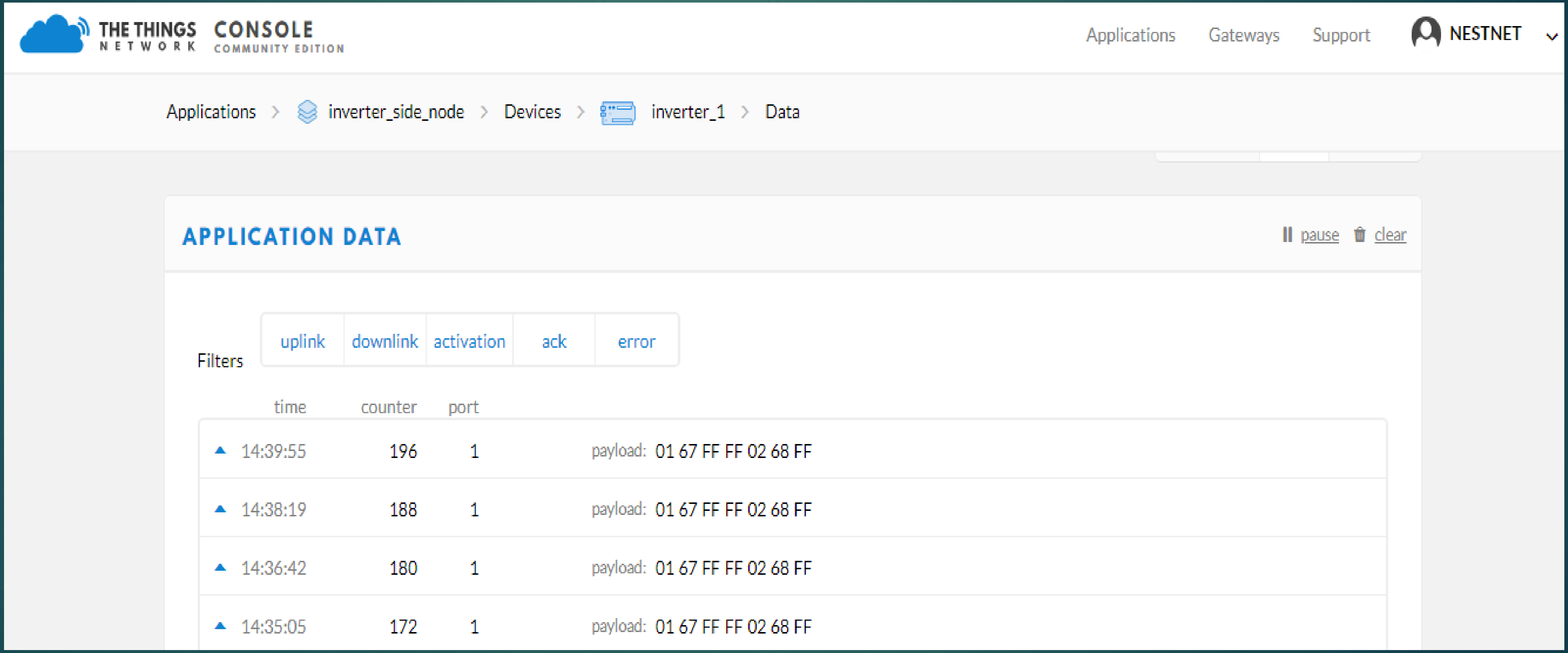


ESP32 as a Gateway

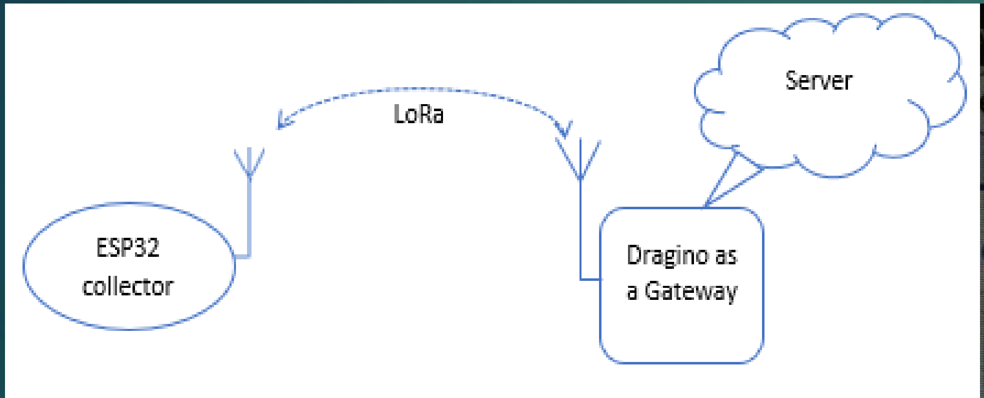


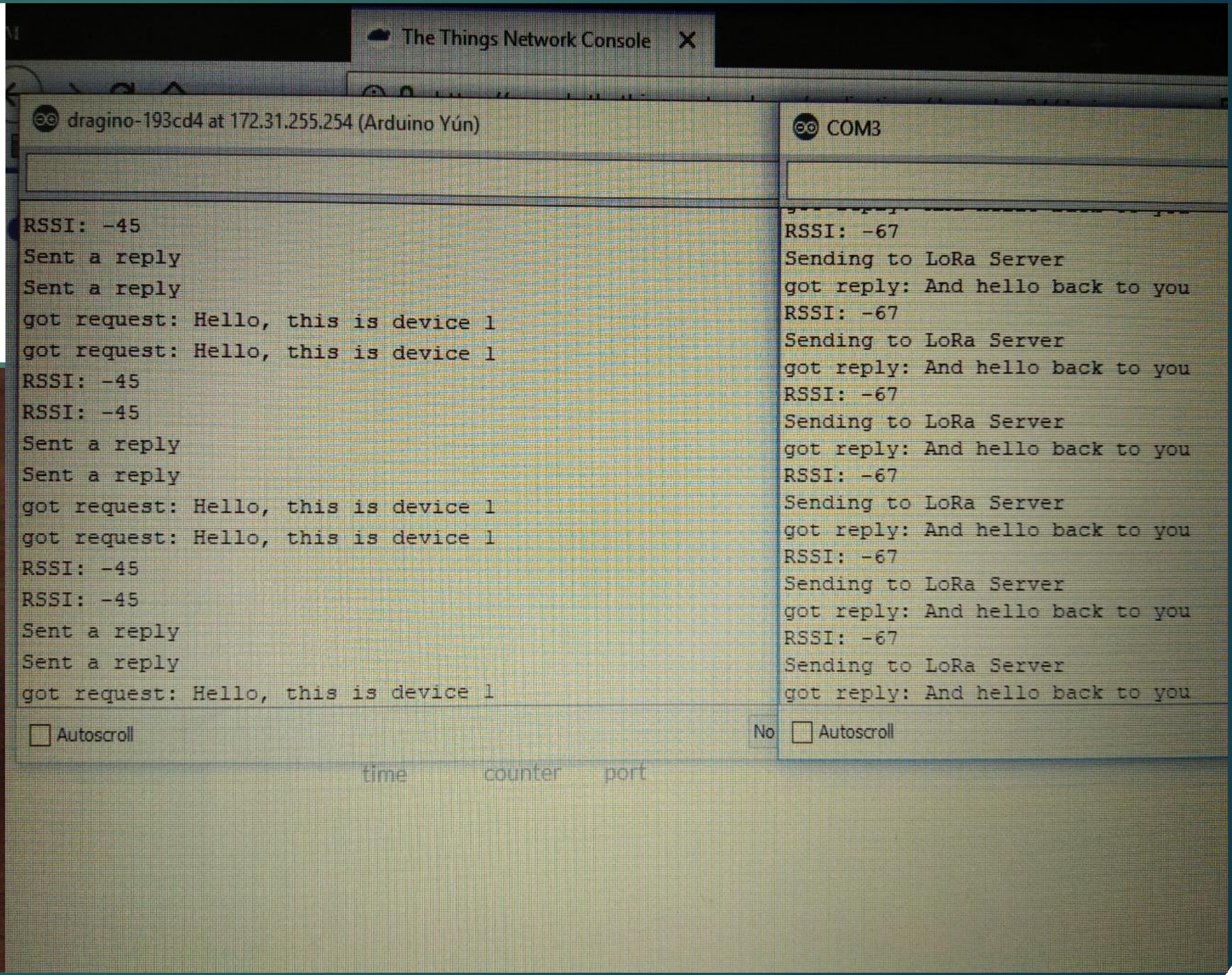
```
A WlanStatus:: CONNECTED to Iqbal
Host esp32-7410c4 WiFi Connected to Iqbal on IP=192.168.0.100
Local UDP port=1700
Connection successful
Gateway ID: 30AEA4FFFF7410C4, Listening at SF9 on 915.00 Mhz.
setupOta:: Started
Ready
IP address: 192.168.0.100
Time: Wednesday 23:01:59
Gateway configuration saved
WWW Server started on port 80
OLED_ADDR=0x3C
--------------------------------------
23:04:45.475 -> G addLog:: fileno=0, rec=1: 1 2B F1 0 30 AE A4 FF FF
23:17:40.050 -> G addLog:: fileno=0, rec=2: 1 9D 7E 0 30 AE A4 FF FF
23:30:34.685 -> G addLog:: fileno=0, rec=3: 1 5B 1B 0 30 AE A4 FF FF
23:43:29.323 -> G addLog:: fileno=0, rec=4: 1 58 DD 0 30 AE A4 FF FF
23:56:23.980 -> G addLog:: fileno=0, rec=5: 1 F5 7E 0 30 AE A4 FF FF
00:00:26.027 -> G addLog:: fileno=0, rec=6: 1 A9 E6 0 30 AE A4 FF FF
```

Logging Data to The Things Network

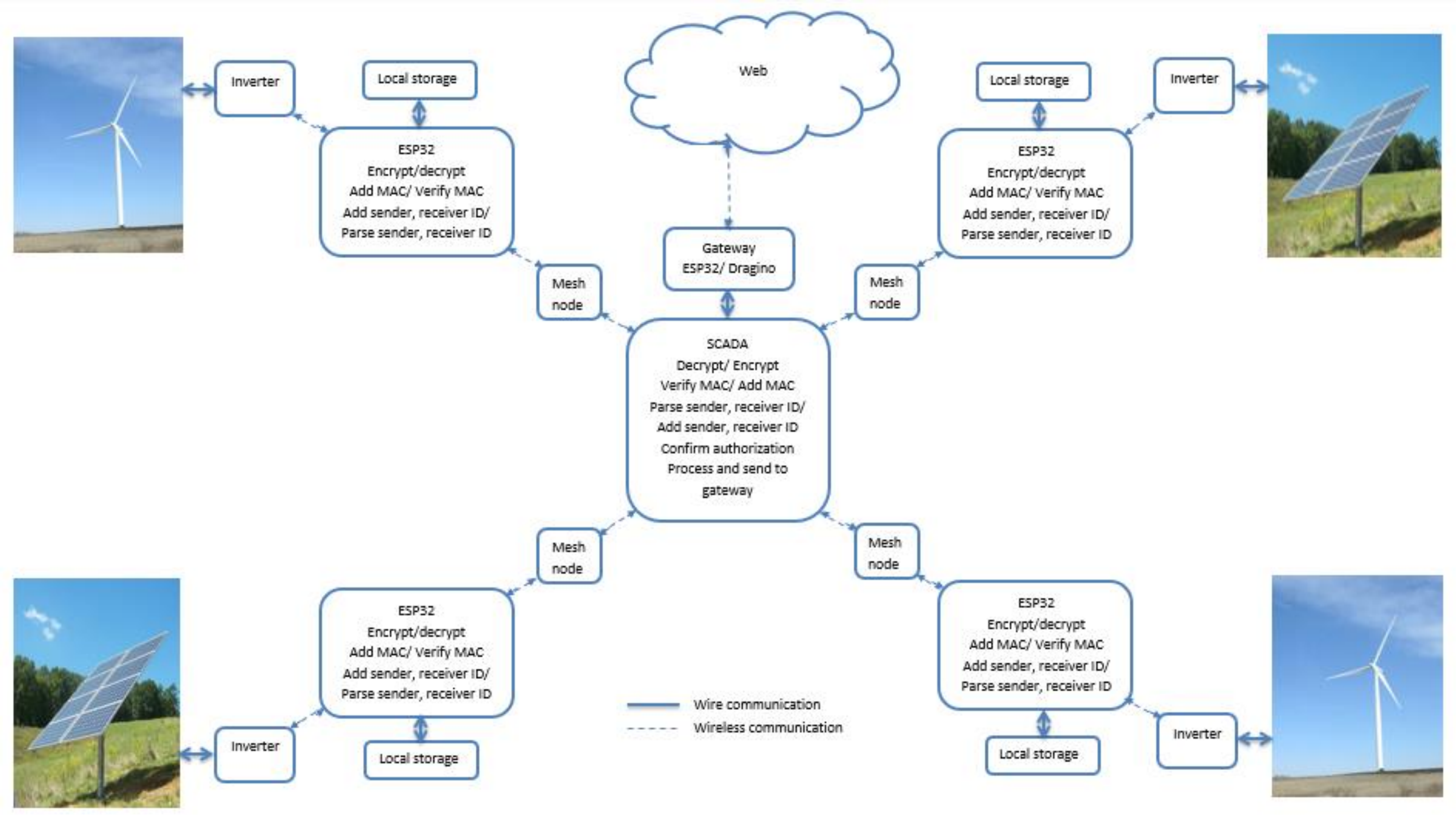


Dragino Gateway for Remote Data Logging

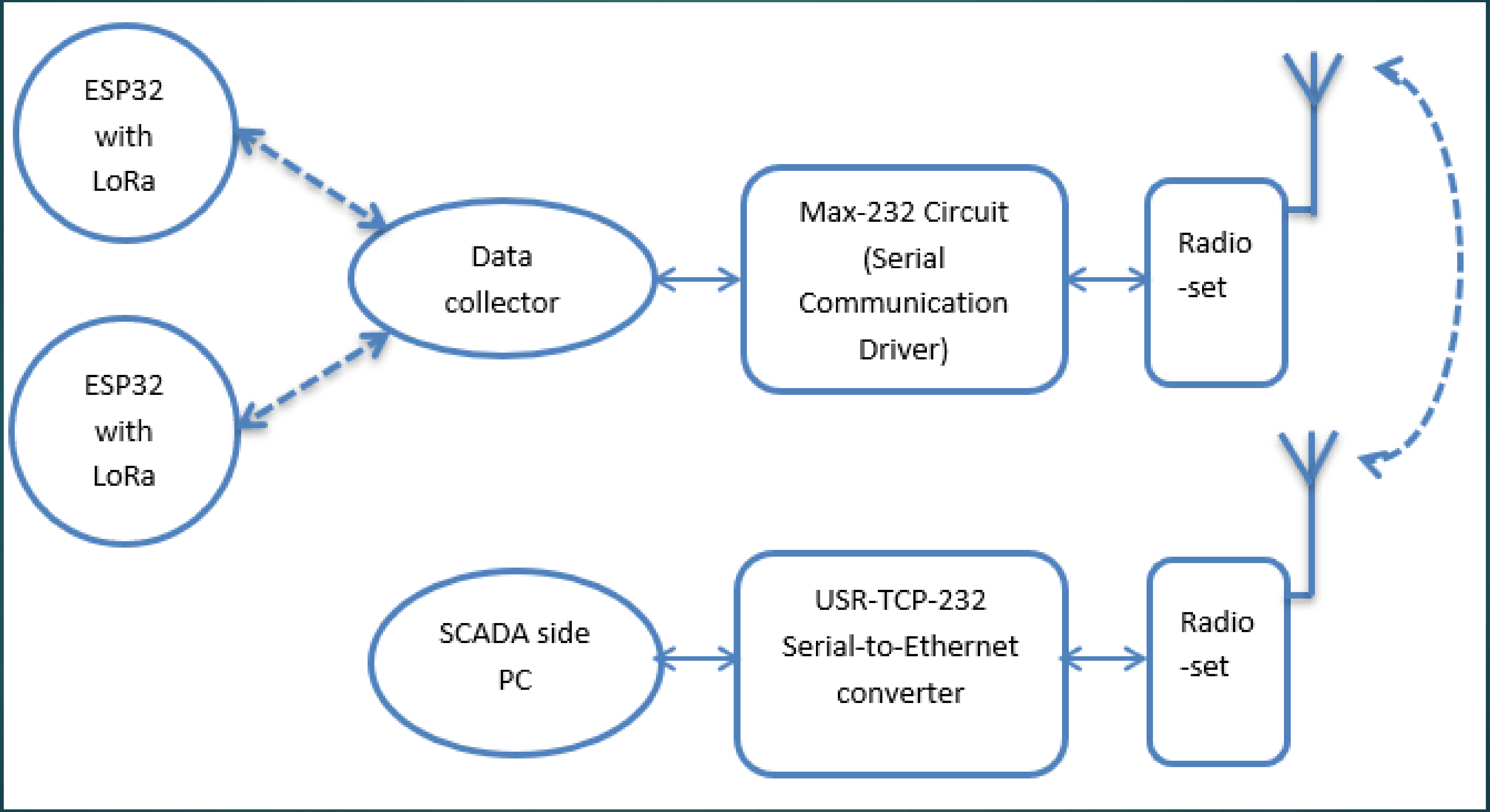




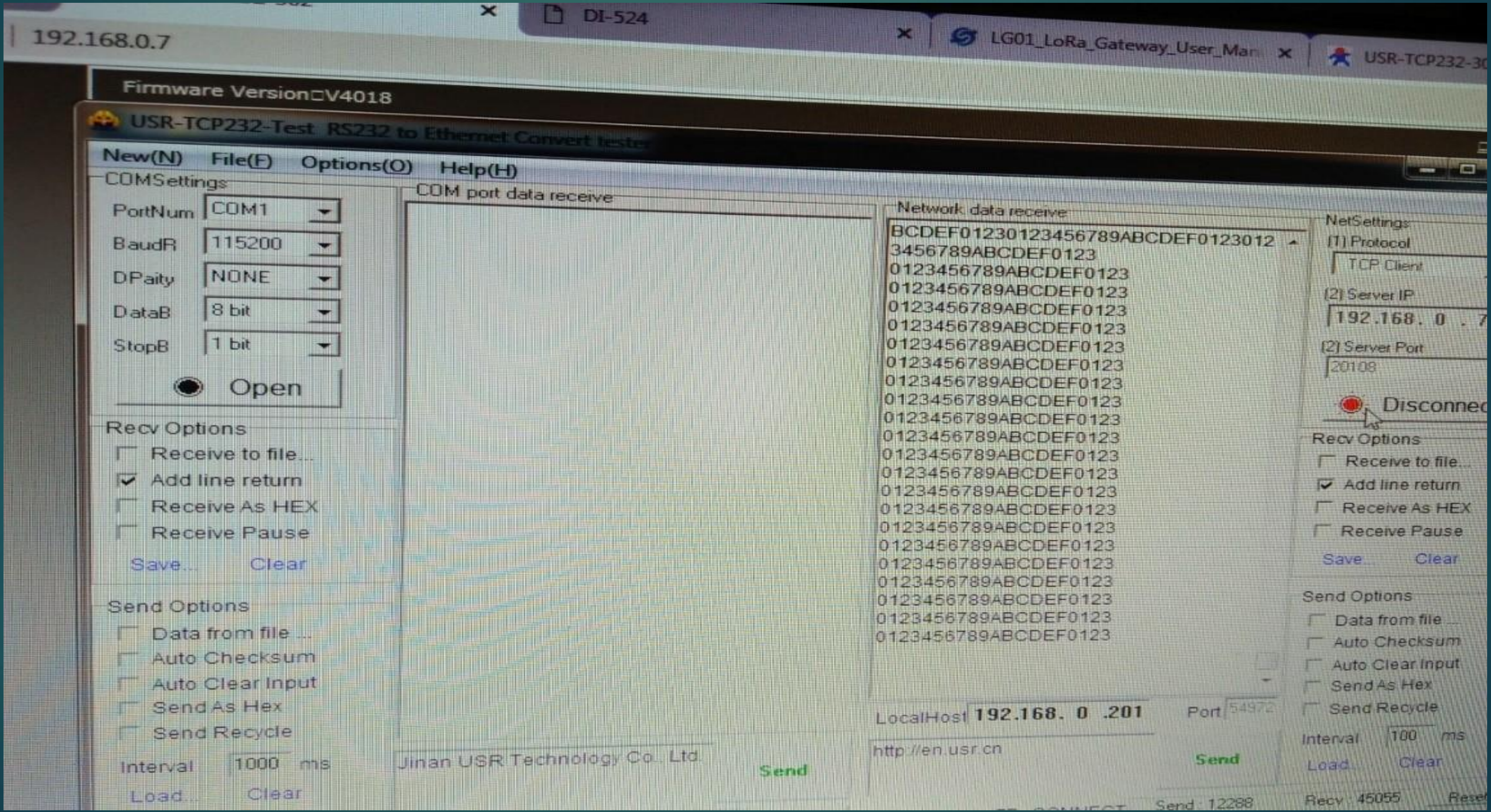
LoRa Based Complete System Diagram



Radio set based System Structure-I

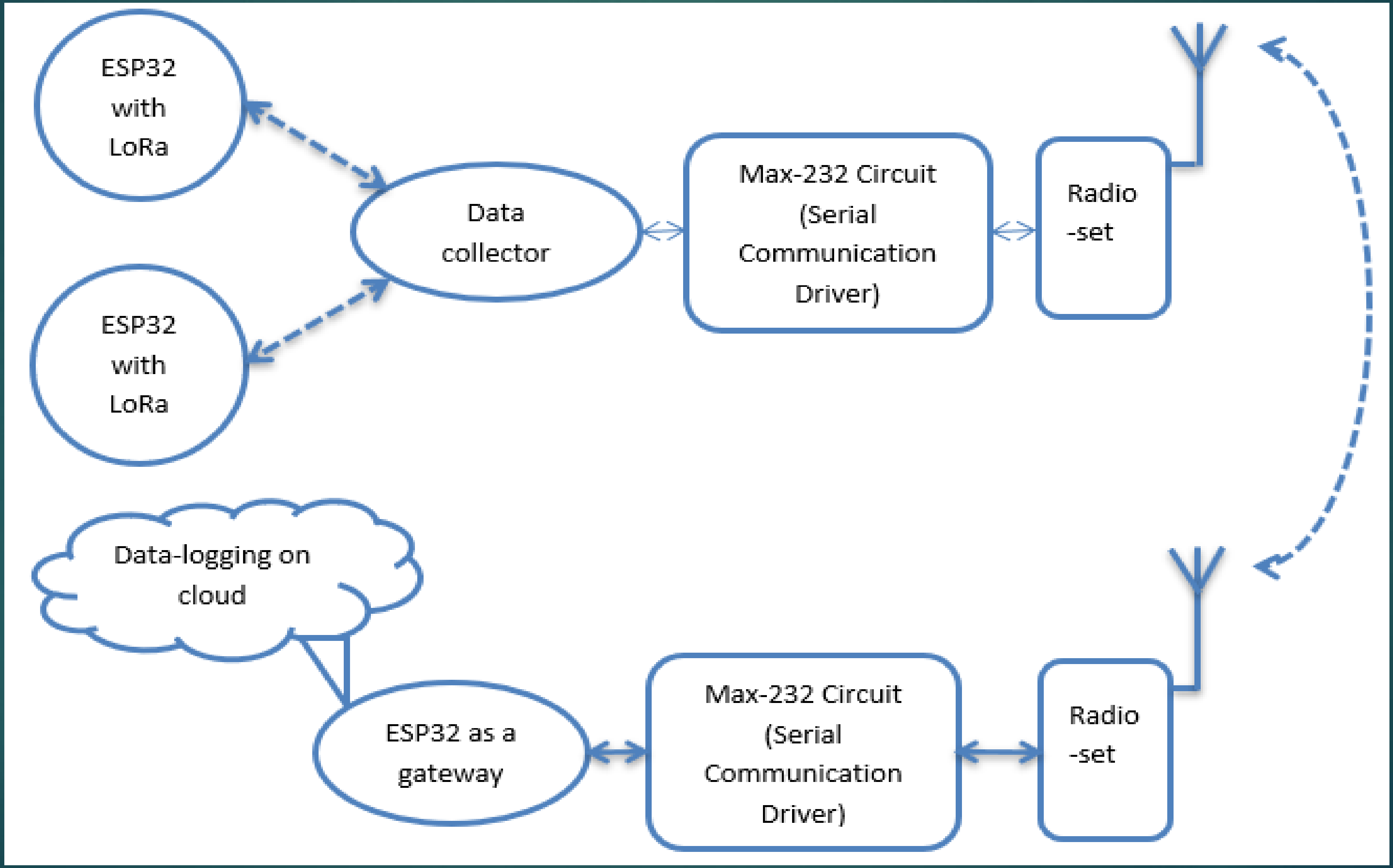


Data Logging in Hybrid System

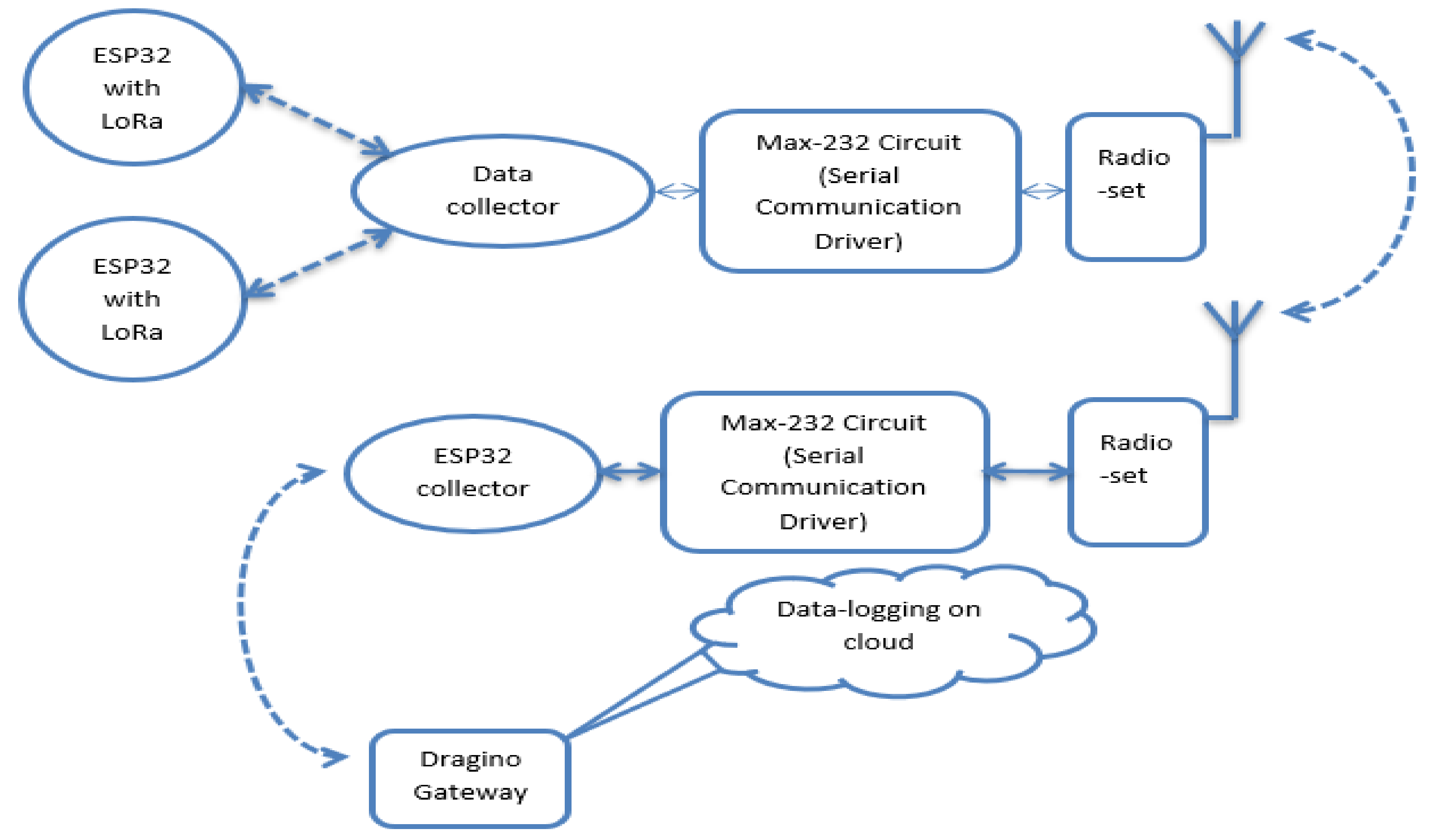


Configuring and Logging Data with Radio-set

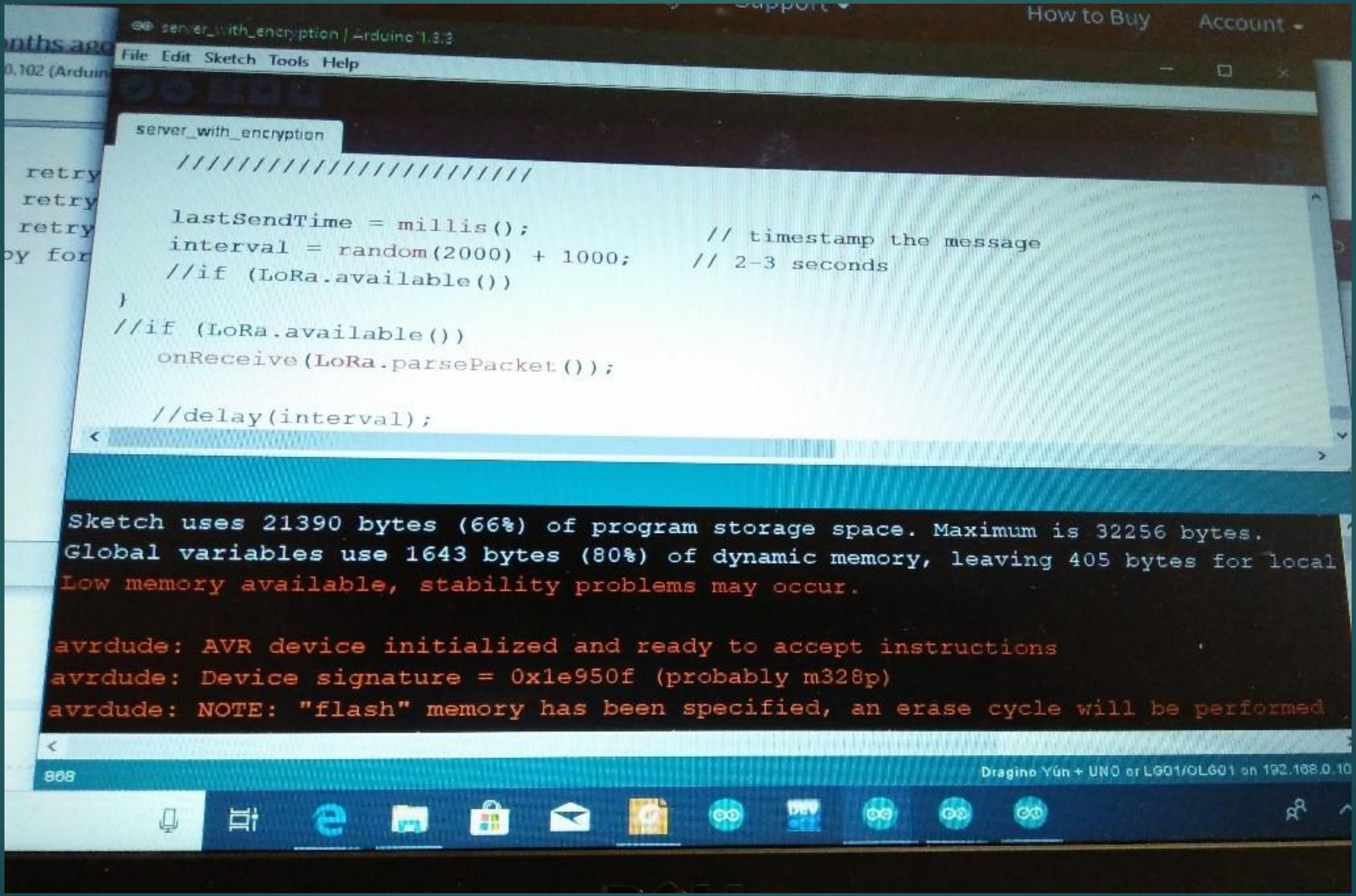
Radio-set based System Structure-II



Radio-set based System Structure-III



Dragino-yun Limitations for Decryption



Power Consumption of Radio-set base System Structure-III

Component	# of pieces used	Watt/piece Max(min)	Cumulative power consumption (W)
ESP32	3	0.2 (0.02)	0.6(0.06)
Dragino-yun	1	4.5 (3)	4.5 (3)
LSR-150-12 with Radio Set	2	22.8 (2.9)	43.6 (5.8)

Power consumption during transmitting/receiving =48.7W

Power consumption during stand-still mode = 9.6W

Cost Calculation of Radio-set based System Structure-III

Component	# of pieces used	$/piece	Cumulative price (CAD)
ESP32	3	26	78
Dragino-yun	1	56	56
LSR-150-12 with Radio-set	2	109.53	219.56

Total capital cost =CAD353.56

Conclusion

1. LoRa based low power, low cost and long range communication system was selected after the literature study of twelve wireless and three wired technologies.
2. Implemented a secure communication system after trying five different encryption algorithms and assessing their strength against any attack.
3. Message authentication was achieved by generating a unique authentication code for each message.
4. Advanced Encryption Standard algorithm was implemented to secure the system against all known attacks.

Conclusion

5. Two different gateways were programmed and configured to access data remotely.
6. LoRa range was improved by implementing ESP32 based LoRa setup in mesh-network
7. A hybrid system of LoRa mesh-network and radio-sets was implemented to achieve the range of above 40km.

Future Work

1. A private server can be developed to eliminate any possible way of intruder’s intervention through server side and internet.
2. Local controllers can be given certain privileges to minimize the communication of critical messages, and rank data based upon the data priority.
3. Local graphical user interfacing (Human Machine Interfacing) and control can be introduced to make the system more user friendly
4. Design a proper housing and power supply for communication link

Publications

Submitted

1. Amjad Iqbal and M. Tariq Iqbal, Low-cost and Secure Communication System for SCADA System of Remote Micro-grids, submitted with the Hindawi International Journal of Communication.

Published/Accepted

2. Amjad Iqbal and M. Tariq Iqbal, Low-cost and Secure Communication System for Remote Micro-grids using AES Cryptography on ESP32 with LoRa Module, presented at IEEE Electrical Power and Energy Conference (EPEC) 2018

3. Amjad Iqbal and M. Tariq Iqbal, Design and Analysis of a Stand-alone PV System for a Rural House in Pakistan, accepted in the Hindawi International Journal of Photoenergy

4. Amjad Iqbal and M. Tariq Iqbal, Thermal Modeling and Sizing of a Stand-Alone PV System for a Rural House in Pakistan, presented at 27th IEEE NECEC Conference 2018

Poster Presentation

5. Amjad Iqbal and M. Tariq Iqbal, Low-cost and Secure Communication System for Remote Micro-grids using AES Cryptography and ESP32 with LoRa, Presented in poster session at Ryerson University, Toronto ON, during NESTNet 2nd Annual Technical Conference, June 19-20, 2018

Questions?

Thank you!