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

- Introduction & Motivation
- SCADA System Communication Requirements
- Selection of LoRa Technology
- Security of Communicated Data for SCADA System
- Implementation of Encryption Algorithms
- System Structure based upon DRF1276G
- Breaching the Encryption Algorithms
- AES Security and Implementation on ESP32
- Inclusion of MAC Address and Results
- Data Rate and Range Testing
Contents

- Local and Remote Data Logging
- ESP32 vs Dragino Gateway
- Mesh-Network Testing and Range Improvements
- System Diagram Based upon only LoRa Network
- Radio-set Based System Topology-I Configuration and Results
- System Structure-II and III
- Cost and Power Analysis
- Conclusion
- Future Recommendations
- Suggestions and Questions
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
<table>
<thead>
<tr>
<th>Technology</th>
<th>Data Rate</th>
<th>Coverage</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copper Wired PLC</td>
<td>2-3Mb/s</td>
<td>1km to 3 km</td>
<td>Unreliable and noisy due to harmonics</td>
</tr>
<tr>
<td>Wired Internet</td>
<td>Max 1Gb/s</td>
<td>100m</td>
<td>High capital cost for installation and least flexible</td>
</tr>
<tr>
<td>Fiber Optic</td>
<td>Max 14Tb/s</td>
<td>160km</td>
<td>Extremely high capital cost for installation and least flexible for SG</td>
</tr>
<tr>
<td>Wireless Local Area Network</td>
<td>54Mb/s</td>
<td>200m to 400m</td>
<td>Short Range, Vulnerable to EMI, Easy Installation</td>
</tr>
<tr>
<td>GSM</td>
<td>14.4kb/s</td>
<td>1km to 10km</td>
<td>Poor Data rate, Monthly cost, Low availability in remote locations</td>
</tr>
<tr>
<td>BlueTooth</td>
<td>250Mb/s</td>
<td>70-100m</td>
<td>Limited Coverage, Limited number of nodes</td>
</tr>
<tr>
<td>WiWLAN</td>
<td>600Mb/s</td>
<td>100m</td>
<td>Small Coverage, Inherent drawbacks of Wireless Mesh Network</td>
</tr>
<tr>
<td>Radio Teletype</td>
<td>100b/s</td>
<td>Input supply dependent (0.7mV/m)</td>
<td>Outdated and analogue, Uses Electromechanical setup</td>
</tr>
<tr>
<td>Optical Wireless Communication</td>
<td>622Mb/s</td>
<td>Unlimited</td>
<td>Costly setup, Under experimental phase</td>
</tr>
<tr>
<td>WiMAX</td>
<td>75Mb/s</td>
<td>10-50km (Line of Sight) 1-5km (OFF LOS)</td>
<td>Poor penetration in obstacles due to HF, Inherent drawbacks of HF</td>
</tr>
<tr>
<td>Satellite Communication</td>
<td>1Gb/s</td>
<td>Unlimited</td>
<td>High Cost, Signal fading due to snow and rain, Signal latency</td>
</tr>
<tr>
<td>GPRS</td>
<td>170kb/s</td>
<td>1km to 10km</td>
<td>Poor Data rate, Less reliable due to voice traffic</td>
</tr>
<tr>
<td>Lora</td>
<td>Depends upon SF</td>
<td>5km to 15km</td>
<td>Low cost, Power saver, Easy Installation, Low data rate</td>
</tr>
<tr>
<td>Zigbee</td>
<td>250kb/s</td>
<td>30m to 50m</td>
<td>Short Range, Poor Data rate, Easy Installation</td>
</tr>
<tr>
<td>SigFox</td>
<td>100b/s</td>
<td>3-10km (Urban)</td>
<td>Low cost, High Scalability, Low data rate, Restricted number of messages per day</td>
</tr>
<tr>
<td>Global Packet Radio System –GPRS- (2G)</td>
<td>170kb/s</td>
<td>1km to 10km</td>
<td>Poor Data rate, Licensed frequency band, Easy Installation</td>
</tr>
<tr>
<td>High Speed Downlink Packet Access-HSDPA- (3G)</td>
<td>384KB/S TO 14.4Mb/s</td>
<td>1-10km</td>
<td>Licensed frequency band, Easy Installation, Limited availability</td>
</tr>
<tr>
<td>Long Term Evaluation-LTE- (4G)</td>
<td>Max 42 Mb/s</td>
<td>1-10km</td>
<td>Licensed frequency band, Easy Installation, Limited availability</td>
</tr>
</tbody>
</table>

Selection of LoRa Technology and SF (whistle)
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**
  - \( y = a \cdot x + b \) (key space \( p(a) \cdot p(b) \))

- **Substitution Cipher**
  - \( ab \rightarrow cy \) (key space \( N! \))

- **Transposition Cipher**
  - (key space \( n! \))

- **Hill Cipher**
  - \( ab \rightarrow ci \) (key space \( N^n \cdot n^2 \))
System Structure Based Upon Arduino with DRF1276G
Arduino with DRF1276G based two-way communication and encryption results

Sending message: Hello world! I am Inverter side sender
Received Message: Hello world! I am SCADA side sender with RSSI: -44

Sending message: Hello world! I am Inverter side sender
Received Message: Hello world! I am SCADA side sender with RSSI: -44

Sending message: Hello world! I am Inverter side sender
Received Message: Hello world! I am SCADA side sender with RSSI: -44

Sending message: Hello world! I am Inverter side sender
Received Message: Hello world! I am SCADA side sender with RSSI: -44

Sending message: Hello world! I am Inverter side sender
Received Message: Hello world! I am SCADA side sender with RSSI: -44

Sending message: Hello world! I am Inverter side sender
Received Message: Hello world! I am SCADA side sender with RSSI: -44
Breaching Encryption Algorithms

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

- FUGOMRPKWODRDTJHDTHPQTDADFKLZDYTEFWCDLJDALRPNQVPHZDRF
- Themonkeyspawpartiwithoutthenightwascoldandwetbutinthe
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 $2^{100}$

  $2^{100} \approx 40,000$ billion years

  @ 1 encryption/ns)
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 64 bits 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

```plaintext
<table>
<thead>
<tr>
<th>Pre-encrypt(plain_text)</th>
<th>0123456789abcdef0123456789abcdef</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphertext after 1</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 2 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 3 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 4 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 5 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 6 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 7 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 8 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 9 rounds</td>
<td></td>
</tr>
</tbody>
</table>
```

```plaintext
<table>
<thead>
<tr>
<th>Pre-encrypt(plain_text)</th>
<th>0123456789abcdef0123456789abcdef</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphertext after 1</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 2 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 3 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 4 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 5 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 6 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 7 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 8 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 9 rounds</td>
<td></td>
</tr>
</tbody>
</table>
```

```plaintext
<table>
<thead>
<tr>
<th>Pre-encrypt(plain_text)</th>
<th>0123456789abcdef0123456789abcdef</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphertext after 1</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 2 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 3 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 4 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 5 rounds</td>
<td></td>
</tr>
<tr>
<td>Ciphertext after 6 rounds</td>
<td></td>
</tr>
</tbody>
</table>
```
Ciphertext with ESP-32

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

<table>
<thead>
<tr>
<th>Pre-encrypt (plain_text):</th>
<th>0123456789ABCDEF0123456789ABCDEF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher-text after 1 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 2 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 3 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 4 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 5 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 6 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 7 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 8 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Cipher-text after 9 rounds:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td>Final ciphertext:</td>
<td>0123456789ABCDEF0123456789ABCDEF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pre-encrypt (plain_text):</th>
<th>FF75BAA2661F246560621ADB47D73AB2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher-text after 1 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 2 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 3 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 4 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 5 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 6 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 7 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 8 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Cipher-text after 9 rounds:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
<tr>
<td>Final ciphertext:</td>
<td>FF75BAA2661F246560621ADB47D73AB2</td>
</tr>
</tbody>
</table>
Cipher-text with MAC

- Receiver compares received MAC and MAC derived from the received message before processing the message.
- Improves data authenticity and integrity.
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
13. 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.
ssetupOta:: 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 5B 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
Radio set based System Structure-I

- ESP32 with LoRa
- Data collector
- Max-232 Circuit (Serial Communication Driver)
- Radio set
- USR-TCP-232 Serial-to-Ethernet converter
Data Logging in Hybrid System
Configuring and Logging Data with Radio-set
Radio-set based System Structure-III
Dragino-yun Limitations for Decryption
# Power Consumption of Radio-set base System Structure-III

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

Power consumption during transmitting/receiving = 48.7W
Power consumption during stand-still mode = 9.6W
Cost Calculation of Radio-set based System Structure-III

<table>
<thead>
<tr>
<th>Component</th>
<th># of pieces used</th>
<th>$/piece</th>
<th>Cumulative price (CAD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP32</td>
<td>3</td>
<td>26</td>
<td>78</td>
</tr>
<tr>
<td>Dragino-yun</td>
<td>1</td>
<td>56</td>
<td>56</td>
</tr>
<tr>
<td>LSR-150-12 with Radio-set</td>
<td>2</td>
<td>109.53</td>
<td>219.56</td>
</tr>
</tbody>
</table>

Total capital cost = CAD353.56
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

Published/Accepted
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

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!