A Secured Smart Grid Network for Advanced Metering Infrastructure

Department of Electronic Engineering
Durban University of Technology
Durban, KZN

Philani Khumalo (Pr Tech Eng)
Student no. 20250262
Email philanipk@gmail.com
Supervisor Prof. B Nleya
A Secured Smart Grid Network for Advanced Metering Infrastructure

Contents
1. Introduction to Power Line Communications (PLC) Smart Grids
2. Purpose of Study Aims and Objectives
3. Methodology
4. Advanced Metering Infrastructure (AMI)
5. PLC Channel
6. PLC Standards
7. Smart Grid Security
8. Encryption and Decryption
9. AES Algorithm Cryptanalysis Resistance
10. Protocols and Algorithm Selection
11. AES Algorithm
12. Modifications
13. Simulation
14. Results
15. Conclusion
A Secured Smart Grid Network for Advanced Metering Infrastructure

1. Introduction to PLC Smart Grids

- What is a Smart Grid?
- What is Power Line Communications?
- Why are We Concerned About Smart Grid Data Security?
- What Is AMI and AMR?
- What is Advance Encryption Standard (AES) or Federal Information Processing Standard FIPS 197?
- What is a Robust Communications Protocol?

Fig.1 Typical AMI Network
2. Purpose of Study, Aim and Objectives

- The purpose of this study is to investigate robust techniques for enhancing data security on PLC Smart Grids.
- The aim and objectives is to implement a secured Smart Grid network by finding the best encryption and authentication scheme to protect Smart Grid network against cyber attacks and any malicious intrusion to the Smart Grid network.
A Secured Smart Grid Network for Advanced Metering Infrastructure

3. Methodology

- Conduct a survey on Advanced Metering Infrastructure (AMI) and Smart Grids.
- Review current available security algorithms and protocols.
- Select the best suitable protocol for Smart Grid network.
- Enhance semantic and physical security for Smart Grids.
- Modification of the selected technology to suit the PLC network Smart Grid design.
- Modelling and Simulation.
A Secured Smart Grid Network for Advanced Metering Infrastructure

4. Advanced Metering Infrastructure (AMI) and Advanced Meter Reading (AMR)

AMI and AMR is a part of Smart Grid

- **AMI and AMR Benefits**
  
  High reliability, avoiding estimate riding, improve energy efficiency and real time consumption.

- **Benefits of Secure Smart Grid**
  
  Network reliability, robustness and trusted data in the purpose of metering data management.
A Secured Smart Grid Network for Advanced Metering Infrastructure

5. Power Line Communication Channel

- The PLC channel is the mostly exposed channel to severe noise interference.
- OFDM is the technology used to mitigate for PLC harsh conditions.
- Zimmermann presented a PLC channel model with \( N \) paths weighing factor \( g_i \) and length \( d_i \), frequency dependent attenuation \( a_0, a_1 \) and \( k \) the signal speed is \( v_p \). Equation 1 below depicts the PLC Channel function equation 1 and Figure 2 shows us the block diagram of noise introduced on the PLC channel.

\[
H(f) = \sum_{i=0}^{N} g_i e^{-(a_0+a_1 f^k) d_i} e^{-j2\pi f \frac{d_i}{v_p}}
\]
A Secured Smart Grid Network for Advanced Metering Infrastructure

6. PLC Standards

The standards used in PLC is IEEE P1901. IEEE P1901 is a high speed data over AC power line. Other standards such as IEEE P1675, PRIME, PLC G3, Home plug and CENELEC are also available.

More standards are still being developed for PLC network by many international organisations. There are few PLC channel model such as MIMO and SISO that can be used but we selected multipath channel model due to it robustness on hash electrical interference resistance using Orthogonal Frequency Division Multiplexing (OFDM) and it also caters for signal attenuation.
7. Smart Grid Security

The following need to be implemented for a secure Smart Grid

- **Cryptography** –
  - Encryption – Data converted to cipher text.
  - Decryption – Cipher text converted back to plain text.

- **Authentication** - Access to the network gained after identifying the user.

- **Integrity Control** - The data sent will be identified if it was modified.

- **Confidentiality** - Data travelling across a network should not be viewed by an intruder.
8. Encryption and Decryption

General block diagram for encryption and decryption of data

![Encryption Decryption Block Diagram](image)

Two types of algorithm:

- **Asymmetric algorithm** - is a public key cryptosystem that uses two different keys for encryption and decryption of data (mostly used in secure shell, web browsing etc.).

- **Symmetric algorithm** - is a private key cryptosystem where one key is used for encryption and decryption of data. (Mostly used in data base, tapes, cards etc.).
A Secured Smart Grid Network for Advanced Metering Infrastructure

9. AES Algorithm Cryptanalysis Resistance.

It can take 1 billion years to crack a 128 bits AES encryption using brute force. With 128 bits AES \(2^{128} = 3.4 \times 10^{38}\) possible keys. A PC that tries \(2^{44}\) keys per second needs 149 000 billion years to break AES.

AES mix column transformation is applied on the state columns one by one. Byte value is changed based on the value of all bytes in columns by multiplying the state in GF \(\mathbb{F}_2^8\) in Equation 3 using polynomial In Equation 2.

\[
m(x) = x^8 + x^4 + x^3 + x + 1 \quad (2)
\]

\[
\begin{bmatrix}
02 & 03 & 01 & 01 \\
01 & 02 & 03 & 01 \\
01 & 01 & 02 & 03 \\
03 & 01 & 01 & 02
\end{bmatrix}
\begin{bmatrix}
s_0,0 & s_0,1 & s_0,2 & s_0,3 \\
s_1,0 & s_1,1 & s_1,2 & s_1,3 \\
s_2,0 & s_2,1 & s_2,2 & s_2,3 \\
s_3,0 & s_3,1 & s_3,2 & s_3,3
\end{bmatrix}
= \begin{bmatrix}
s'_0,0 & s'_0,1 & s'_0,2 & s'_0,3 \\
s'_1,0 & s'_1,1 & s'_1,2 & s'_1,3 \\
s'_2,0 & s'_2,1 & s'_2,2 & s'_2,3 \\
s'_3,0 & s'_3,1 & s'_3,2 & s'_3,3
\end{bmatrix} \quad (3)
\]
10. Protocols and Encryption Algorithm Selection

- The study has been conducted on few encryption protocols such as: RSA, DES, SSH, 3DES, and also five finalists by National Institute of Standards and Technology (NIST) such as AES, MARS, RC6, Two fish and Serpent.

- AES has proven to be more secure and been proven to be the fastest and efficient.

- AES has 3 variations AES 128, AES 192, and AES 256. This keys are arranged in array size if 4x4, 4x6 and 4x8.

- AES 128 bits block data is constructed on a 4x4 matrix called a state. AES is divided into four sequential operations (10, 12 and 14 rounds depending on key size).

- The AES transforms are as follows: Sub Bytes, Shift Row, Mix Column / (Permutation), Add Round key.
A Secured Smart Grid Network for Advanced Metering Infrastructure

11. AES Algorithm Selection

- AES was selected as a better algorithm for PLC Smart Grid due to its robust security flexibility and encryption and decryption speed (software and hardware).
- The AES algorithm utilises 128 bits block and other three different sizes of keys which are: 128, 192 and 256 data bits.
- AES uses symmetric key algorithm that means that the key that is utilized for encryption and decryption of data is the same.
- The cipher text created by AES encryption is of the same size as the plain text.
A Secured Smart Grid Network for Advanced Metering Infrastructure

12. Modifications

- To minimise calculations an AES was modified to lessen the calculation time of encryption and decryption.
- The mix column step is omitted and DES permutation is added. Mix column has high calculation therefore omitted.
- The aim of modifying AES is to lessen computation time but not compromising security of data.
- Modified AES algorithm provides improved encryption speed.
- We selected 128 bits key since it is the most applied in encryption of PLC.
13. Simulation

- We used OPNET and NetBeans 8.0.2 Java compiler to verify the efficiency and speed of the modified AES encryption and decryption.
- A 16 bits data sizes were simulated using AES and Modified AES and the results were compared.
- The program was run on the Java compiler and the results are depicted below.

```
Start program
Java
plain: test text ABC
decrypt: test text ABC
```
14. Results

Simulation of encryption and decryption using Java NetBeans 8.0.2 compiler.

Table 1 Encryption and Decryption Time

<table>
<thead>
<tr>
<th>File size</th>
<th>AES (ms)</th>
<th>Modified AES (ms)</th>
<th>Improvement (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 bit</td>
<td>290</td>
<td>247</td>
<td>43</td>
</tr>
</tbody>
</table>

It can be observed that there is a 43 ms improvement on a 16 bits using on modified AES.
A Secured Smart Grid Network for Advanced Metering Infrastructure

15. Conclusion

- The AES algorithm has proven to provide adequate security for Smart Grids data using simulation tools.
- Due to AES flexibility and variable length block of 128, 192 or 256 bits, it is possible that in future, AES block size be stretched beyond 128, 192 and 256 bit length.
- AES is a modern block cipher and it provides excellent long-term security against brutal force attacks.
- AES is efficient in software and hardware. So far no reported cases of AES algorithm being cracked.
A Secured Smart Grid Network for Advanced Metering Infrastructure

Questions

Plain Data/Text 16 bits = ABC