Analysis of Data Transmission Using RSA Encryption in Power Line Communication

Iago S. Ochôa, Douglas A. Santos, João A. Martins, Valderi R. Q. Leithardt

Laboratory Of Embedded and Distributed Systems – LEDS – Universidade do Vale do Itajaí (UNIVALI)
CEP 88302-202 – Itajaí– SC – Brazil

{iago.ochoa,douglasas,joao_martins}@edu.univali.br, valderi@univali.br

Abstract. *This paper describes a simulation model for transmission of encrypted data in power lines. The model was developed in MATLAB and consists of using asymmetric key cryptography to encode the data to be transmitted. The technique used to perform data transmission was the Power Line Communication technique.*

1. Introduction

Nowadays several organizations manufacture microcontroller units with specific applications of the smart grid segment. These applications must follow rules that govern this segment. The problem of these standards is that they designate the use of symmetric key cryptography in data transmission. With increasing processing power over the years it has been realized that a more secure type of encryption can be used in these systems.

With the emergence of smart grid networks, it has become possible to create more efficient, profitable and sustainable systems. With the advent of these new systems also appear new security breaches that can compromise them. Current literatures show that there is a large gap in security of data transmission in smart grid networks [Ali et al., 2015].

As a simulation scenario, a model of a point-to-point data transmission will be developed using the power line communication technique to send the data through the energy line. The asymmetric key cryptography chosen was RSA [Mathworks, 2012] because it is a widely used type in current days. The system will consist of transmitting an encrypted data from one point to another using the Gaussian Minimum Shift Key modulation. The integrity of received data will be verified after the transmission.

This paper will be structured in the following way: section 2 presents the related works, section 3 shows the proposed project model, section 4 presents the preliminary results obtained and section 5 the conclusions and future works.

2. Related Works

Table 1 shows a comparison of the related works. It is noticed that Lin, Latchman and Lee (2002) used the HomePlug protocol to model their system, the type of encryption described by this protocol is the Default Encryption Standard. Augusto (2011) used the PRIME protocol that describes the use of the Advanced Encryption Standard 128-bits. In the simulation model of Cataliotti, Di Cara, Fiorelli and Tiné (2012) and Chiotellis

and Cotis (2016), no protocol was used in the transmission model, and consequently no encryption.

Author	Characteristics		
	Protocol used	***Type of encryption used***	***Algorithm used.***
Lin, Latchman and Lee. (2002).	HomePlug	Symmetric	DES
Augusto. (2011)	PRIME	Symmetric	128-bit AES
Cataliotti, Di Cara, Fiorelli and Tinè. (2012)	None	None	None
Chiotellis and Cotis. (2016)	None	None	None
Ochôa and Leithardt. (2017)	None	Asymmetric.	RSA

Table 1. Protocol and cryptography comparative.

It is worth mentioning that our work proposes a transmission model without a defined protocol. The cryptography used will be the RSA asymmetric key, it was chosen because the microcontrollers aimed to the smart grid segment supports only symmetric key cryptography due their processing power, and our work intend to verify if it is possible to use asymmetric key cryptography in this microcontroller units. The modulation used to transmit data is the Gaussian Minimum Shift Key [MATLAB, 2016].

3. Suggested Model

The model was implemented in MATLAB because it has a ready-made block of functions for signal modulation in the frequency domain. Two codes were created separately, the first one consists in modulating and transmitting the signal, the second one is responsible for encrypting the data. After validating the two codes, both were integrated in one to make the system. Figure 1 shows the main steps of the proposed system and Figure 2 shows the main algorithm for the suggested model.

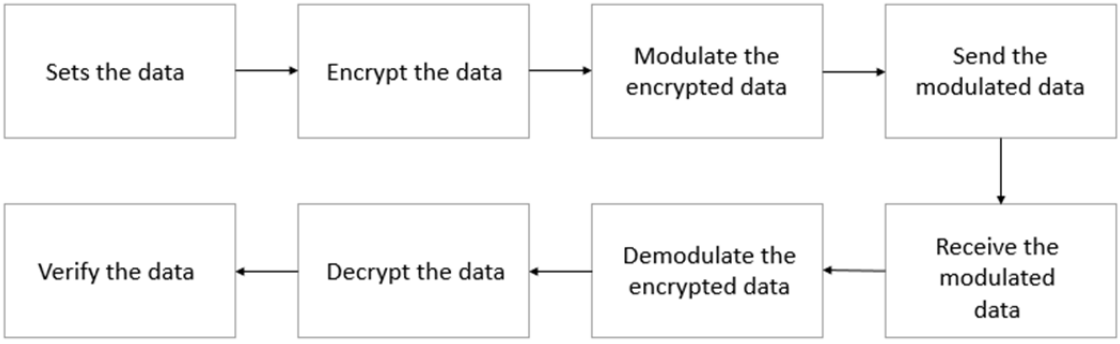

Figure 1. System modeling by author.

```
for i = 1 : 47                                  % 47 transmissions
    for j = 1 : 10                              % 10 bits each value
       aux(j)=(statemod(i,j));
    end
    a = vec2mat(aux,1);                         % vector to matrix
    data = double (a);                          % convert data to double
    modSignal = step(hMod, data);               % modulate signal
    receivedData = step(hDemod, modSignal);     % send data
     for j = 1 : 10
       staterec(i,j)=(receivedData(j));         % decrypt vector
     end
end
```

Figure 2. Main algorithm.

The code consists in transmitting a user-defined random data, after that this data is modulated in the frequency domain (GMSK modulation) – Gaussian Minimum Shift Key [Radio Electronics, 2008]. To simulate the transmission line, a white noise is added on it, to thereby generate a noise in the transmitted signal. Figure 3 shows the block diagram of the algorithm in SIMULINK [Mathworks, 2008].

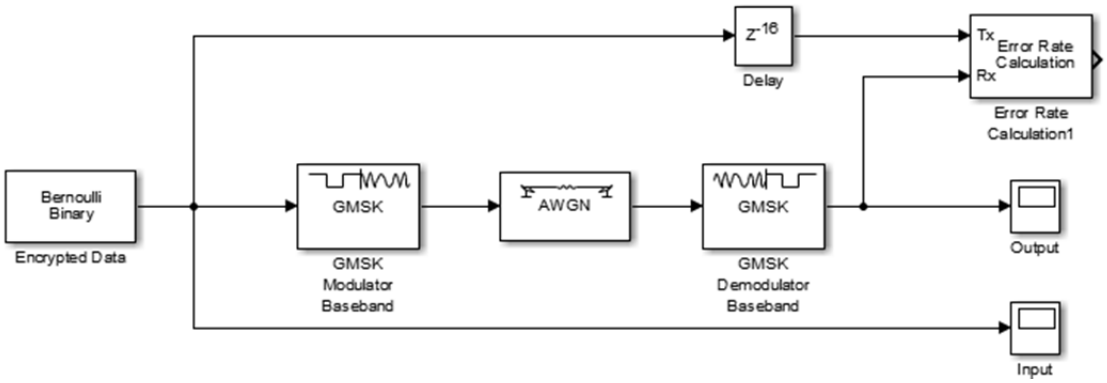

Figure 3. Block diagram of the main algorithm in SIMULINK by author.

4. Preliminary results

Executing the above code, it was obtained an unsatisfactory result for the suggested model. As shown in Figure 4, it is noticeable that the data received is totally different from the one sent. This is due to the integration of encryption and transmission codes. The main reason for this error in the decryption of the transmitted data is the delay generated by the modulation/demodulation process.

```
Public key: 3
Private key: 427
Message: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
Cipher Text of the entered Message:ŏŏ  ęę  íí  ÝÝ  óó  ŒŒ  ıı  ǩǩ  jj  ǨǨ  ǏǏ  òò  KK  ЯЯ  □□  ŶŶ
Decrypted Message is:      □□ □□    □□ □□ □□ □□    □□ □□ □□    □□
```

Figure 4. Transmitted and received data.

5. Conclusions and Future Works

With the development of the work up to the present moment it was noticed that the result obtained was not satisfactory. The delay generated by the modulation/demodulation process compromised the transmission. It was due to this that the data received, and later decrypted, was not the same as the one transmitted.

It was noticed that to fix this problem it is necessary to use a communication protocol that meets the characteristics of the system, only with that will be possible to verify the integrity of the transmitted data.

The cryptography used has a short key due the limited processing power of microcontrollers for the smart grid segment. Extensive keys made the simulations impractical due to data encryption/decryption time.

In future is intended to apply the communication protocol aimed to this segment, to improve the transmission line model to become as close to real as possible and to apply performance characteristics of microcontrollers aimed to this segment to check system performance.

6. References

Ali, H., Amin, F., Hamid, J. and Alireza, G. (2015) "Security and Feasibility of Power Line Communication System". In: International Conference On Global Security, Safety and Sustainability", England.

MATHWORKS. (2012) "Implementation of RSA Algorithm", https://www. mathworks.com/matlabcentral/fileexchange/implementation-of-rsa-algorithm, July 2017.

MATLAB. (2016) "Modulate using GMSK method", https://www.mathworks.com /help/comm/ref/comm.gmskmodulator-class.html, May 2017.

Radio Electronics. (2008) "Gaussian Minimum Shift Key Method", http://www.radio-electronics.com/info/rf-technology-design/pm-phase-modulation/what-is-gmsk-gaussian-minimum-shift-keying-tutorial, April 2017.

MATHWORKS. (2008) "GMSK Mod/Demod", https://www.mathworks.com/ matlabcentral/newsreader/view_thread/169264, May 2017.

Augusto, R. (2011) "Simulation of Powerline Communication (PLC) for Smart Grid in OMNeT++", https://fenix.tecnico.ulisboa.pt/downloadFile/395145996565/resumo.pdf, June 2017.

Lin, Y., Latchman, H. and Lee, M. (2002) "A Power Line Communication Network Infrastructure for The Smart Home". In: IEEE Wireless Communications, p. 104-111, Switzerland.

Cataliotti, A., Di Cara, D., Fiorelli, R. and Tine, G. (2012) "Power-Line Communication in Medium-Voltage System: Simulation Model and Onfield Experimental Tests". In: IEEE Transactions on Power Delivery, p. 90-102, Switzerland.

Sendin, A., Penã, I. and Angueira, P. (2014) "Strategies for Power Line Communication Smart Metering Network Deployment", In: Energies, Switzerland.