Análise de Desempenho na Transmissão de Dados Criptografados Utilizando o Protocolo OSGP

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

Laboratory of Embedded and Distributed Systems – LEDS
Universidade do Vale do Itajaí (UNIVAL)
Caixa Postal 360 – 88.302-202 – Itajaí – SC – Brasil

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

Abstract. *This paper describes an encrypted data transmission simulation model for performance analysis. The model was developed in MATLAB and consists of using symmetric and asymmetric key cryptography to encode the data to be transmitted. The technique used to perform data transmission was the PLC technique. At the end of the simulations it was possible to evaluate the execution time for the tests made.*

Resumo. *Este artigo descreve um modelo de simulação de transmissão de dados criptografados para análise de desempenho. O modelo foi desenvolvido em MATLAB e consiste em usar criptografias de chave simétrica e assimétrica para codificar os dados a serem transmitidos. A técnica utilizada para realizar a transmissão de dados foi a técnica de PLC. Ao fim das simulações foi possível avaliar o tempo de execução para os testes realizados.*

1. Introdução

É importante enfatizar que as redes elétricas estão passando por sua maior transformação desde o seu surgimento. A rede atual está sendo substituída por um conjunto de sistemas digitais denominados *smart grid* [Falcão 2010]. Esses sistemas são mais eficientes, confiáveis e sustentáveis. Um exemplo de aplicação é a medição automatizada da energia elétrica. Com o advento das redes *smart grid* foi possível substituir o ser humano por um sistema de medição automatizado que pode receber e enviar informações às concessionárias responsáveis pelo fornecimento de energia.

Atualmente, várias organizações fabricam microcontroladores com aplicações específicas para o segmento *smart grid*. Essas aplicações devem estar de acordo com as normas que regem a segurança desse segmento. Com o aumento do poder de processamento ao longo dos anos, percebeu-se que um tipo mais seguro de criptografia poderia ser usado nesses sistemas.

Para o cenário de simulação, um modelo de transmissão de dados ponto-a-ponto foi desenvolvido usando a técnica de comunicação PLC com a modulação GMSK (*Gaussian Minimum Shift Key*) para enviar os dados pela linha de energia elétrica. A criptografia de chave assimétrica escolhida foi o RSA sendo amplamente aplicada nos dias atuais [Gomez 2012]. A criptografia simétrica utilizada neste trabalho foi o AES 128 bits, recomendado pelas normas. O sistema consiste na avaliação de desempenho da transmissão de dados criptografados.

Este artigo está estruturado da seguinte forma: a seção 2 apresenta os trabalhos correlatos. A seção 3 descreve o modelo de simulação proposto. A seção 4 apresenta os resultados obtidos com os testes. Por fim, a seção 5 apresenta as conclusões obtidas e os trabalhos futuros.

2. Trabalhos Correlatos

[Uludag et al. 2016] apresenta um protocolo seguro de comunicação de dados que usa criptografia RSA para transmissão de dados que são coletados em dispositivos de medição de energia. Sua conclusão aponta para a criação e uso de um protocolo próprio, pois os protocolos existentes não podem abordar todos os dispositivos que estão emergindo.

[Shijo and Sankaranarayanan 2017], desenvolveram uma análise de desempenho de protocolos de segurança de redes *smart grid.* Foi usado o simulador NS-2 para criar uma rede de medidores inteligentes e realizar os testes. Eles concluem que AES e ECC são válidos para uso. Sua conclusão enfatiza que é necessário transmitir os dados do medidor inteligente através de um *gateway* seguro para fornecer segurança resistente a ataques de DDoS (*Distributed Denial of Service*). Em [Abdallah and Shen 2017] é discutido o uso de *clusters* de dados em vez de relatórios individuais de clientes. Seu esquema provou garantir a comunicação leve e, consequentemente, um bom desempenho computacional.

Fundamentado na literatura pesquisada, este trabalho propõe um modelo de transmissão que usa o protocolo OSPG (*Open Smart Grid Protocol*), que é o mais usado no mundo [OSGP Alliance 2017]. As criptografias utilizadas serão, para chave assimétrica o RSA e para chave simétrica o AES. O AES foi escolhido devido à OSGP padronizar o uso da criptografia RC4, o que provou ser inseguro [Jovanovic and Neves 2015]. O RSA foi escolhido porque a maioria dos microcontroladores voltados para o segmento *smart grid* suporta apenas criptografia de chave simétrica devido ao seu poder de processamento. A modulação usada para transmissão dos dados é a GMSK, que foi escolhida devido às vantagens contra o ruído nas linhas de energia [Santos 2008]. A Tabela 1 apresenta a comparação entre os trabalhos relacionados e este trabalho.

Tabela 1. Comparação dos trabalhos correlatos

Autor	**Características**		
	Protocolo	**Tipo de criptografia**	**Algoritmo**
[Uludag et al. 2016]	Próprio	Assimétrico	RSA
[Shijo and Sankaranarayanan 2017]	Nenhum	Simétrico	AES
[Abdallah and Shen 2017]	Nenhum	Assimétrico	NTRU
Modelo Proposto	OSGP	Assimétrico/Simétrico	RSA/AES

3. Modelo Proposto

O modelo foi implementado em MATLAB devido ao fato de ele possuir blocos de funções prontas para modulação de sinal no domínio da frequência. Dois códigos foram criados separadamente, o primeiro consiste em modular e transmitir o sinal, o segundo é responsável pela criptografia dos dados. Depois de validar os dois códigos, ambos foram integrados em um só para criar o sistema. A Figura 1 ilustra os principais passos do sistema proposto. Primeiramente o dado é criptografado utilizando o modo ECB de cifra de

blocos. Após isso o dado é modulado usando a modulação GMSK, para se assemelhar a um cenário real foi aplicado um ruído branco sobre a rede de transmissão. Após o término da aplicação do ruído é feita a demodulação e decriptação do dado transmitido. O tempo de medição é medido para todo o processo.

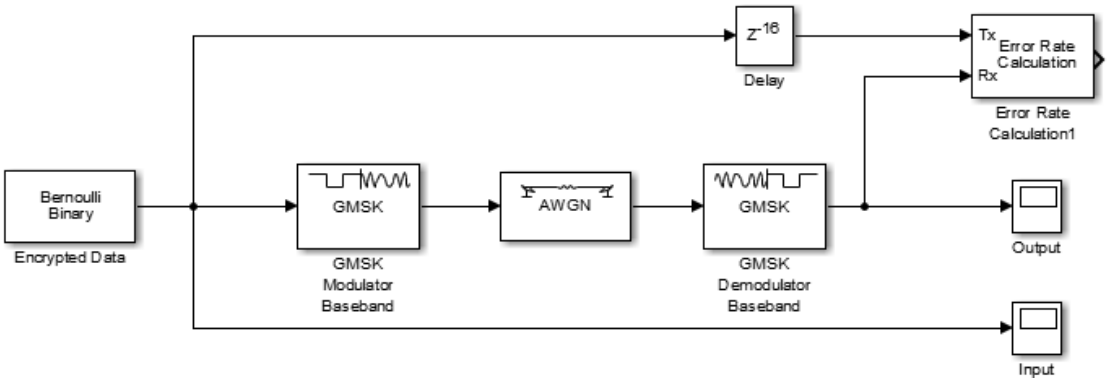

Figura 1. Diagrama de Blocos do algoritmo principal no SIMULINK.

4. Testes e Resultados Preliminares

Quanto ao tempo de execução, o algoritmo AES apresentou melhor desempenho. Mesmo usando uma chave pequena para o algoritmo RSA, é possível perceber que o algoritmo é mais lento do que o AES. A Tabela 2 apresenta a comparação entre os dois códigos executados no MATLAB. Cada código transmitiu os dados cem vezes, com isso foi obtido o tempo de execução mostrado na Tabela 2. O tempo de execução mostrado na Tabela 2 é o tempo total para as cem transmissões, no AES com tamanho de 6 bytes e no RSA com tamanho de 3 bytes.

Tabela 2. Resultados obtidos

Algoritmo	Modo ECB	Tempo de execução
AES 128 bits	16 bits	8,8521 segundos
RSA	8 bits	108,2148 segundos

Os testes foram realizados em um notebook Acer Aspire E1-572-6638 com memória de 8 GB DDR3 1333 MHz. A placa mãe deste modelo é uma Hannstar V5WE2 LA-9532P com processador Intel Core i5 4200U com frequência de operação de 1.6 GHz até 2.3 GHz. O sistema operacional usado na simulação foi o Windows 10 Pro 64 bits com o software MATLAB R2016a.

5. Conclusões e Trabalhos Futuros

O algoritmo AES foi adaptado de uma biblioteca em C disponibilizada pela *Texas Instruments* para os microcontroladores voltados para o segmento *smart grid*. A escolha de usar esse algoritmo específico foi devido ao fato de ser otimizado para rodar de maneira otimizada em microcontroladores voltados para este segmento. A adaptação do algoritmo em C ao MATLAB funcionou corretamente, mas algumas mudanças foram desenvolvidas para funcionar igual, o que pode ter afetado o desempenho.

A criptografia RSA utilizada tem uma chave pequena devido ao poder de processamento limitado dos microcontroladores voltados para o segmento *smart grid*. O uso de chaves extensas tornou as simulações impraticáveis devido ao tempo de encriptação e decriptação de dados. É importante ressaltar que o algoritmo RSA não está otimizado para microcontroladores. Para tanto, foi utilizado um algoritmo geral para realizar a simulação.

Com o desenvolvimento deste trabalho foi possível identificar o tempo de execução de cada algoritmo de criptografia para uma rede PLC simulada. Conforme os valores obtidos referente ao tempo de execução de cada um dos algoritmos, foi possível identificar que o algoritmo de chave simétrica provou ser mais eficiente que o algoritmo de chave assimétrica nesta simulação.

Para trabalhos futuros pretende-se evoluir o modelo de transmissão ponto-a-ponto para uma NAN e uma WAN, para assim, realizar testes de desempenho de criptografia nesses tipos de redes que se assemelham a um cenário prático.

6. Agradecimentos

Os resultados deste trabalho foram possíveis devido ao apoio recebido através do projeto de pesquisa e extensão da Universidade do Vale do Itajaí através do artigo 170 - pesquisa de projetos. Também agradecemos o uso da infra-estrutura fornecida pelo Laboratório de Sistemas Integrados e Distribuídos (LEDS) da UNIVALI.

Referências

Abdallah, A. and Shen, X. (2017). Lightweight security and privacy preserving scheme for smart grid customer-side networks. *IEEE Transactions on Smart Grid*, 8(3):1064–1074.

Falcão, D. M. (2010). Integração de tecnologias para viabilização da smart grid.

Gomez, S. (2012). Implementation of rsa algorithm. Disponível em: http://www.mathworks.com/matlabcentral/fileexchange/38439-implementation-of-rsa-algorithm. Acesso em 17/11/2017.

Jovanovic, P. and Neves, S. (2015). Dumb crypto in smart grids: Practical cryptanalysis of the open smart grid protocol. *IACR Cryptology ePrint Archive*, 2015:428.

OSGP Alliance (2017). Open smart grid protocol. Disponível em: http://www.osgp.org/en/technical. Acesso em 17/11/2017.

Santos, T. L. (2008). Power line communications.

Shijo, M. and Sankaranarayanan, S. (2017). Performance analysis of security protocols in smart energy meter system. 12(19):8294–8315.

Uludag, S., Lui, K. S., Ren, W., and Nahrstedt, K. (2016). Secure and scalable data collection with time minimization in the smart grid. *IEEE Transactions on Smart Grid*, 7(1):43–54.