Smart Grid: uma abordagem sobre os desafios relacionados aos aspectos de segurança

Alexandre Silva Rodrigues, William Dresch Floriano, Tiago Antônio Rizzetti, Murilo Cervi

Colégio Técnico Industrial de Santa Maria – Universidade Federal de Santa Maria (UFSM)
CEP – 97.105-900 – Santa Maria – RS – Brasil

{alexandre.rodrigues,williamdf,murilo}@redes.ufsm.br,
rizzetti@gmail.com

Abstract. *The Smart Grids utilize information technology to facilitate the administration and management of conventional electric network. The process of implementation of this concept finds many challenges, especially regarding the issue of communication between different devices, security and integrity of information.In this paper an approach the issue by analyzing the main scopes of communication and security issues relating to each scope is performed.*

Resumo. *As Smart Grids utilizam tecnologias da informação para facilitar a administração e gerenciamento da rede elétrica convencional. O processo de implementação desse conceito encontra diversos desafios, principalmente quando se refere à questão de comunicação entre diferentes equipamentos, segurança e integridade das informações trafegadas. Neste trabalho é realizada uma abordagem do assunto analisando os principais escopos de comunicação, bem como as questões de segurança relativas a cada escopo.*

1. Introdução

A energia elétrica é utilizada para os mais diversos fins, seja nas residências quanto nas indústrias. Em casos de interrupção no fornecimento da mesma, evidencia-se o quanto ela é importante e necessita de sistemas capazes de automatizar o processo de restabelecimento da mesma. Além disso, a relação entre as distribuidoras de energia elétrica e seus clientes ainda é restrita [GTREI 2010].

Para resolver essas questões, diversas tecnologias têm surgido. Por meio dessas, será possível automatizar o processo de leitura do consumo de energia elétrica do consumidor e aplicar uma diferenciação nas tarifas cobradas de acordo com o horário. Além disso, o consumidor poderá utilizar fontes geradoras de energia em suas residências e assim, vender energia para as concessionárias [Ramos 2012].

Nesse aspecto, as redes elétricas inteligentes (*Smart Grids*) destacam-se por utilizarem as tecnologias da informação para facilitar na administração e gerenciamento da rede elétrica convencional [Ramos 2012]. A automação desse sistema possibilitará ações, em tempo real, em equipamentos presentes na geração até a distribuição da energia elétrica [Moreira 2013].

A primeira ação para tornar a rede elétrica inteligente é a utilização de medidores inteligentes, que além de registrarem o consumo de energia, possibilitam ao

consumidor final ter um controle sobre o seu consumo e obter descontos na fatura em determinados horários. Com esses medidores, casos de falta de energia poderão ser detectados automaticamente pela concessionária, sem necessitar que o consumidor notifique-a [Guimaraes 2013] [GTREI 2010].

Para que as *Smart Grids* possam vir a substituir as redes elétricas convencionais, existe ainda uma série de desafios. Nesse sentido, os principais aspectos a serem analisados é a forma como os equipamentos irão comunicar-se e a segurança das informações que serão trafegadas entre os consumidores e as concessionárias.

Com base nisso, esse artigo tem como objetivo, realizar uma revisão bibliográfica referente ao conceito de *Smart Grid* e as tecnologias utilizadas para prover uma comunicação bidirecional entre consumidores e concessionárias de energia. Além disso, serão abordados alguns aspectos voltados à segurança das informações trafegadas e formas para garantir a confidencialidade e integridade das mesmas.

2. Smart Grid

Uma rede elétrica inteligente (Smart Grid) utiliza tecnologia digital para monitorar e gerenciar o transporte de energia, compreendendo desde a geração até a distribuição. A implementação desse tipo de rede busca otimizar a utilização e operação de equipamentos ativos, minimizar os custos e impactos ambientais e aderir confiabilidade, resiliência e estabilidade ao sistema utilizado até o momento [Avelar 2010].

A *Smart Grid* possui diversos benefícios, dentre eles podemos citar a melhoria de serviço entregue ao consumidor final, através de um sistema de medição que permitirá visualizar maiores detalhes de sua fatura. Este sistema é chamado *Smart-Metering*, onde seu funcionamento baseia-se em medir de forma inteligente, através dos *Smart Meters*, o consumo de energia elétrica, fornecendo assim o cálculo desse consumo de forma mais rápida e eficiente [Ramos 2012].

Para tornar possível a automação da rede elétrica, são utilizados os dispositivos eletrônicos inteligentes (IEDs) que trocam informações de uma maneira eficaz e rápida, tornando simples a implementação de um projeto e automatizando a rede de uma forma confiável [Pereira 2007].

Outro aspecto importante, quando se trata de *Smart Grid,* é contingência em casos de falhas na rede de distribuição. Nesse contexto, aplica-se o conceito de *Self-Healing*, que pode ser visto como uma reconfiguração automática. Para isso, é realizado o monitoramento e análise da rede, buscando por possíveis falhas. Essa funcionalidade permite identificar a falha e o local da ocorrência e assim, facilitar o processo de restabelecimento de energia para os clientes [Aloul 2012].

2.1. Comunicação de Smart Grid

Para prover todas as funcionalidades de uma *Smart Grid*, é necessário que os equipamentos ativos na rede elétrica troquem informações em tempo real. Além disso, é imprescindível integrar os diversos tipos de equipamentos e protocolos utilizados na comunicação e controle do sistema elétrico.

A rede a ser utilizada em uma *Smart Grid* deve permitir uma comunicação bidirecional entre os consumidores e as empresas que atuam na distribuição da energia elétrica. Entre as tecnologias capazes de atender os requisitos de uma *Smart Grid*

podemos destacar as seguintes: Power Line Communication (PLC), ZibBee, redes Mesh, radiofrequência e redes celulares do tipo *General Packet Radio Service* (GPRS) [Ghansah 2009].

A escolha da tecnologia a ser utilizada deve considerar a necessidade de confiabilidade, segurança e integridade das informações. Outro fator importante é o tipo de operação que será realizada. Quando se trata de informações críticas, que podem comprometer o sistema, a tecnologia precisa apresentar robustez, disponibilidade e eficiência no tempo de resposta [GTREI 2010].

Com relação à comunicação de *Smart Grid*, podemos dividir o sistema em quatro camadas, cada uma delas com um tipo de necessidade e formas de implementações diferentes: HAN, LAN, RAN e WAN.

2.1.1. HAN (*Home Area Network*)

Essa camada compreende todos os dispositivos presentes na residência do cliente. Nessa camada destaca-se a utilização de medidores inteligentes. Esses são capazes de processar dados e enviar comandos para outros equipamentos. Com isso, é possível que o cliente possa ter um controle sobre o seu consumo de energia elétrica. Um exemplo disso é desligar equipamentos em determinados horários em que a tarifa cobrada é mais cara. Nesse contexto, a concessionária poderá controlar a carga dentro de cada residência, limitar a demanda e evitar sobrecargas na rede [GTREI 2010].

Para prover a comunicação entre os dispositivos de uma residência e o medidor inteligente, podem ser utilizadas tecnologias de comunicação sem fio, como por exemplo, redes 802.11, ZigBee e 6LoWPAN.

Nessa camada, o medidor inteligente será capaz de interligar a residência ao restante da *Smart Grid*. As informações enviadas por ele serão recebidas por um concentrador. Para enviar esses dados, é possível utilizar a tecnologia de radiofrequência, ZigBee ou PLC [Ghansah 2009].

A tecnologia PLC é uma alternativa às comunicações por meio de redes sem fio. Essa tecnologia utiliza os cabos condutores de eletricidade para trafegar dados, necessitando apenas de dispositivos de comunicação PLC e uma interface para os dispositivos a serem controlados. Entretanto, essa forma de comunicação é viável somente em segmentos onde não existam transformadores, pois os mesmos podem ocasionar a perda de dados. Caso exista algum transformador, é necessário utilizar filtros para eliminar os ruídos causados por ele.

2.1.2. LAN (*Local Area Network*) e RAN (*Regional Area Network*)

Essas camadas são responsáveis por coletarem informações de diferentes concentradores. Nessas camadas existe uma maior preocupação com a segurança das informações e a disponibilidade da rede.

A LAN pode ser vista como uma rede que abrange várias unidades consumidoras e realiza a comunicação entre os medidores inteligentes e pontos centralizadores de dados (concentradores). As tecnologias mais empregadas para prover essa comunicação são: Zigbee, PLC, Wimax, Mesh, ADSL e Rádio Frequência (RF). Uma RAN pode ser compreendida como uma interligação entre os concentradores e pontos mais amplos, como por exemplo, uma subestação. Essa comunicação pode ser

realizada utilizando-se as tecnologias Wimax, Mesh ou fibra óptica [Lamin 2013].

2.1.2. WAN (*Wide Area Network*)

Essa camada recebe informações de dispositivos espalhados em uma grande área geográfica. Por exemplo, vários concentradores de dados e dispositivos presentes em diversas subestações podem enviar informações para uma central de controle.

A tecnologia a ser utilizada nessa camada deve ser altamente confiável, pois nela trafegarão um volume considerável de informações. A disponibilidade deve ser alta, pois, muitas operações de tempo real necessitam de um mínimo tempo de latência. Uma alternativa é o uso de fibra ótica, devido suas especificações que garantem os requisitos mínimos para esse tipo de comunicação.

3. Segurança de *Smart Grid*

A segurança de uma Smart Grid pode ser afetada por atitudes humanas, ou seja, é difícil saber quando uma pessoa age de má-fé ou por engano, e também se seus motivos tratam de benefícios financeiros ou somente a necessidade de afetar o sistema de energia. Assim, torna-se imprescindível a segurança nas redes de comunicação contra esses ataques.

Entres as principais preocupações com segurança de uma *Smart Grid*, podemos destacar os seguintes aspectos: disponibilidade, defesa de integridade e falsificação de dados.

3.1. Disponibilidade

Alguns serviços oferecidos por uma *Smart Grid* necessitam de uma alta disponibilidade, como por exemplo, uma central de monitoramento e controle de uma subestação de distribuição. Nesse contexto, uma possível sobrecarga do sistema, sem a possibilidade de ser controlada, pode gerar um desligamento em toda área de cobertura dessa subestação. Essa funcionalidade necessita que as informações sejam trafegadas em tempo real, para que uma possível anormalidade no sistema seja reconhecida e tratada em tempo hábil, para que não comprometa a disponibilidade da rede elétrica.

Com relação ao cliente, deverá ser considerada a disponibilidade de serviços referentes ao consumo e tarifação da energia. Dessa forma, ele poderá administrar o uso de equipamentos de acordo com os horários que possuem menor tarifação, bem como, receber informações de controle sobre esses equipamentos.

A disponibilidade de uma rede pode ser comprometida por ações de usuários mal intencionados. Dentre as ações que os mesmos podem efetuar, destaca-se uma técnica conhecida como Ataque de Negação de Serviço (*Denial of Service – DoS).* Contudo, existem formas de proteção contra esse ataque [Guimaraes 2013].

3.1.1. Ataque de Negação de Serviço (DoS)

O *DoS* consiste em um atacante utilizar um sistema de rede, ou um conjunto de computadores, para inserir informações falsas que afetam no reconhecimento dos pacotes entre o transmissor e receptor, dessa forma afetando o tráfego normal da rede. Esse tipo de ataque pode causar a indisponibilidade de algum serviço disponível na *Smart Grid* e comprometer a distribuição de energia elétrica em grandes proporções.

Esse ataque pode ser especialmente crítico em redes que utilizam como meio físico de comunicação a transmissão sem fio. Visto que o acesso ao meio não pode ser controlado, há possibilidade de, por exemplo, atacantes utilizarem-se de transmissores que emitam sinais na mesma frequência, deteriorando a capacidade de comunicação do sistema ou mesmo impossibilitando-a.

Em sistemas onde controla-se o meio físico utilizado para transmissão, como o PLC ou fibra óptica, o controle torna-se mais fácil, pois a utilização de filtros e firewalls, se bem utilizados, serão eficazes [Guimaraes 2012].

Para impedir esse tipo de ataque, é importante analisar o tráfego de rede e criar filtros para determinados endereços IPs. Outra forma é adotar um mecanismo de proteção que limite o número de conexões oriundas de um mesmo dispositivo.

3.2. Defesa de integridade

Para garantir a integridade das informações que trafegam na *Smart Grid*, uma técnica utilizada é a criptografia. Aos enviar dados criptografados, esses se tornam menos vulneráveis às ações de usuários mal intencionados. Esse aspecto é mais relevante quando são utilizadas redes sem fio para enviar informações. No caso de uma HAN, a privacidade de um cliente pode ficar exposta a ações de usuários mal intencionados que buscam obter algum tipo de informação.

Por exemplo: em uma residência é utilizada uma rede sem fio para realizar a comunicação entre dispositivos eletrônicos e o medidor inteligente. Se essa rede não utilizar algum método de criptografia, as informações ficam expostas em texto plano. Dessa forma, qualquer pessoa pode vasculhar as mensagens trocadas entre os equipamentos, e assim, tentar burlar o sistema, enviando comandos para um determinado equipamento, bem como, adulterar informações utilizadas na tarifação ou estimação de estado, sendo que esta última pode ocasionar inconsistências no sistema, podendo até mesmo ocasionar uma falha geral.

3.3. Falsificação de Dados

A falsificação de dados representa uma grande ameaça para as redes elétricas inteligentes. Dessa forma, as informações trocadas entre o consumidor e a concessionária, podem ser interceptadas ou manipuladas por terceiros. O primeiro aspecto a ser analisado é a comunicação entre o medidor instalado na residência do cliente e a empresa fornecedora de energia. Assim, o cliente pode tentar modificar os valores de seu consumo para reduzir suas tarifas.

Nesses termos, outra preocupação é com possíveis adulterações nas informações trocadas entre os concentradores e as subestações. Caso alguém tente modificar alguma informação, o controle sobre os níveis de carga poderão ser afetados, e assim, ocasionarão efeitos de indisponibilidade de distribuição de energia elétrica.

A integridade dos dados é garantida através da utilização de chaves criptográficas, de forma similar, para evitar falsificação dos dados deve-se utilizar o processo de assinatura digital. Desta forma poderá assegurar-se que os dados são oriundos dos equipamentos e aplicações que de fato alegam ser [Guimaraes 2013].

4. Conclusões

As redes elétricas inteligentes apresentam uma série de benefícios, entre eles destacam-se as melhorias na relação entre clientes e concessionárias, a automatização dos serviços existentes na rede elétrica convencional e inclusão de novas funcionalidades na mesma. Além disso, as *Smart Grids* oferecerão uma maior confiabilidade e disponibilidade na entrega de energia aos consumidores, bem como, auxiliar na detecção de falhas e roubos de energia elétrica.

Entretanto, muitos desafios precisam ser superados. Para o correto funcionamento de uma *Smart Grid*, ainda é necessário garantir a integridade e a segurança das informações que serão trafegadas na rede. Com isso, é imprescindível a adoção de mecanismos de segurança, a fim de evitar ações de pessoas mal intencionadas. Como alternativa para esses problemas, destaca-se o uso de criptografia nas mensagens trafegadas, a limitação de conexões simultâneas a um dispositivo e a padronização de dispositivos e protocolos de comunicação.

Nesse contexto, será desenvolvido um ambiente virtual para simular ataques a *Smart Grids*. Dessa forma, será utilizado um cenário para analisar a troca de informações entre dispositivos e suas vulnerabilidades, com o objetivo de encontrar soluções que garantam a segurança de uma *Smart Grid*.

Referências

Aloul, F. et al (2012) Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy.

Avelar, M. C. (2010) Perspectivas e Desafios para a Implantação das Smarts Grids: um estudo de caso dos EUA, Portugal e Brasil. Monografia Graduação em Economia. Instituto de Economia, Universidade Federal do Rio de Janeiro.

Ghansah, I. (2009) Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks. California Energy Commission, PIER.

Guimaraes, P. H. V. et al. (2013) Comunicação em Redes Elétricas Inteligentes: Eficiência, Confiabilidade, Segurança e Escalabilidade. In: SBRC – Simpósio Brasileiro de Redes de Computadores.

Grupo de Trabalho de Redes Elétricas Inteligentes (2010) Smart Grid. Relatório.

Lamin H. (2013) Análise de Impacto Regulatório da implantação de redes inteligentes no Brasil. Tese de Doutorado em Engenharia Elétrica, Universidade de Brasília. Brasília.

Moreira, J. A. et al. Aspectos de segurança em Smart Grid. XXXIII Encontro Nacional de Engenharia de Produção. Salvador.

Pereira, A. C. et al. (2007) Automação de Subestações e Usinas – Estado da arte e tendências utilizando a Norma IEC 61850. In: Simpase - Simpósio de Automação de Sistemas Elétricos, 7. Salvador.

Ramos, M. L. C. Proposta de um método de segurança da informação para sistemas de automação em redes elétricas inteligentes. 2012. 107 f. Dissertação de Mestrado. Instituto de Tecnologia para o Desenvolvimento.