PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

Artigo de Revisão

SMART GRID: DESAFIOS EM SEGURANÇA

SMART GRID: SECURITY CHALLENGES

Alan Carlos Santos[1]; Robson Leandro Carvalho Canato[2]

1- Graduado em Ciência da Computação, pela Faculdade Municipal Prof. Franco Montoro (FMPFM/Mogi Guaçu); 2- Mestre em Ciência da Computação, pela Universidade Estadual de Campinas (UNICAMP) e docente/coordenador na FMPFM/Mogi Guaçu.

Contato: canato.fmpfm@gmail.com

RESUMO

Atualmente, as companhias de energia elétrica utilizam-se de um sistema que foi implementado há mais de cem anos atrás, com pouco desenvolvimento tecnológico. Esse cenário começa a mudar com a estruturação das redes inteligentes (*Smart Grid*). São redes que aplicam as tecnologias da informação e comunicação (TIC) às redes elétricas. Espera-se que com essa incorporação, haja o aprimoramento da eficiência e confiabilidade, unindo os conceitos de geração distribuída, comunicação bidirecional, energias renováveis e interconectividade. Com todos esses benefícios provenientes da *Smart Grid*, vem as preocupações em relação à cibersegurança, devido ao imenso número de dispositivos conectados à rede das concessionárias de energia. Esse artigo descreve sobre a Smart Grid e os aspectos de segurança relacionados a sua implantação.
Palavras-chave: Smart grid. Segurança. Geração distribuída. Tecnologias da informação e comunicação.

ABSTRACT

Currently, the electric power companies use a system that was implemented more than a hundred years ago, with little technological development. This scenario began to change with a structuring of Smart Grids. They are networks that apply information and communication technologies (ICT) to the electrical networks. It is hoped that with this incorporation, efficiency and reliability will be improved, combining the concepts of distributed generation, bi-directional communication, renewable energies and interconnectivity. With all these benefits coming from Smart Grid, it comes as a concern for cybersecurity, due to the number of devices connected to the network of the energy

companies. This article describes a Smart Grid and security aspects related to its deployment.
Keywords: Smart grid. Security. Distributed generation. Information and communication technologies.

INTRODUÇÃO

A crescente demanda por energia elétrica na sociedade contemporânea, tem demonstrado ser um verdadeiro desafio para os setores energéticos, que necessitam providenciar formas de ampliação do sistema elétrico encarregado da geração, transmissão e distribuição da energia, evitando possíveis interrupções no fornecimento. Contudo, questões ambientais, econômicas, tecnológicas ou geográficas dificultam a implantação de grandes projetos na área de geração de energia elétrica.

Algumas opções encontradas para evitar tais interrupções englobam condutas de eficiência da rede energética (desde a geração até o consumidor final), uso de fontes alternativas de energia (eólica, solar, biomassa, etc.) e o emprego de pequenas unidades geradoras próximas aos consumidores (geração distribuída). A tecnologia que permite o aprimoramento das atuais redes de energia elétrica é conhecida como *Smart Grid*, que é a união das tecnologias da informação e comunicação (TIC) ao sistema elétrico (SMARTGRIDGOV, 2017).

No sistema de distribuição de energia existente, o fluxo é sempre em sentido único, da distribuidora aos consumidores finais. Com a implementação da *Smart Grid*, o mesmo sistema que era utilizado para transmitir energia, também recebe e envia dados. Através da comunicação bidirecional, o sistema *Smart Grid* viabiliza uma rede elétrica mais eficiente e confiável, facilitando a habilidade dos operadores de gerenciar as operações das redes em tempo real, baseando-se nas informações adquiridas dos consumidores. Alguns benefícios do sistema *Smart Grid* são citados pelo *U.S. Department of Energy* (2017) como sendo:

- ✓ Aumento da eficiência na transmissão e distribuição de energia elétrica.
- ✓ Restabelecimento do fornecimento de energia mais ágil após alterações na rede.
- ✓ Redução nos custos de operações e gerenciamentos da companhia de energia elétrica, resultando em menores custos para consumidores.
- ✓ Demanda de pico reduzida, também auxiliando na diminuição de taxas de eletricidade.
- ✓ Maior integração com sistemas de energias renováveis.
- ✓ Segurança melhorada.

Quando as pessoas ouvem os termos “nova tecnologia”, “interconectividade”, “compartilhamento de dados”, os pensamentos iniciais são referentes as novas funcionalidades e vantagens originárias dessa novidade. Porém, não consideram os novos

riscos que provém desses benefícios. A dependência da rede de comunicação, expõe inevitavelmente, o sistema *Smart Grid* à possíveis vulnerabilidades já enfrentadas por essa rede. Isso aumenta os riscos envolvidos, comprometendo a confiabilidade e segurança do sistema energético, que é o ponto central da *Smart Grid*. O objetivo deste artigo é apresentar conceitos fundamentais sobre a *Smart Grid* e os aspectos de segurança relacionados à sua implementação.

EQUIPAMENTOS DE MEDIÇÃO E COMUNICAÇÃO

Para tornar possível o sistema *Smart Grid*, várias tecnologias são empregadas, como: medidores inteligentes, meios de comunicação (GPRS, GSM, 3G, PLC, WI-FI / Wimax, etc.).

Sistema de Leitura Automática de Medidores (AMR)

A tecnologia AMR (*Automatic Meter Reading)* foi concebida em 1977, evoluindo a partir de um design de Tesla (inventor austríaco), por meio da combinação de tecnologias, incluindo redes com e sem fios. O avanço mais relevante referente ao AMR, foi a capacidade de leitura remota dos medidores pelas companhias elétricas. Com a utilização do AMR, as leituras podem ser realizadas próximas do tempo real, garantindo que as contas dos consumidores sejam baseadas no consumo. Antigamente, as companhias confiavam em uma estimativa de leitura quando tarifavam os consumidores. A partir dessa mudança, as companhias elétricas puderam realizar melhoramentos na produção de energia durante períodos de pico e baixa demanda. Diversas tecnologias foram empregadas para suportar a arquitetura AMR, como notebooks e *handhelds* para coleta de dados e redes com e sem fios para transporta-los (FLICK e MOREHOUSE, 2011).

Power Line Communication (PLC)

Utilizando-se da PLC, os dados são transmitidos através da estrutura de energia existente até as subestações, para só então ser enviadas às companhias de energia elétrica para computação e verificação dos dados. Essa tecnologia fornece um recurso totalmente remoto para obter-se as informações dos medidores.

General Packet Radio Service (GPRS)

O *GPRS* é um aprimoramento da tecnologia *GSM (Global System for Mobile Communication)* que possibilita o trafego das informações utilizando-se a rede de telefonia móvel. Esse sistema permite o envio de dados através de pacotes, em uma taxa de transmissão bem mais elevada que da tecnologia anterior (*GSM*) (SCHETTINO, 2013).

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Artigo de Revisão

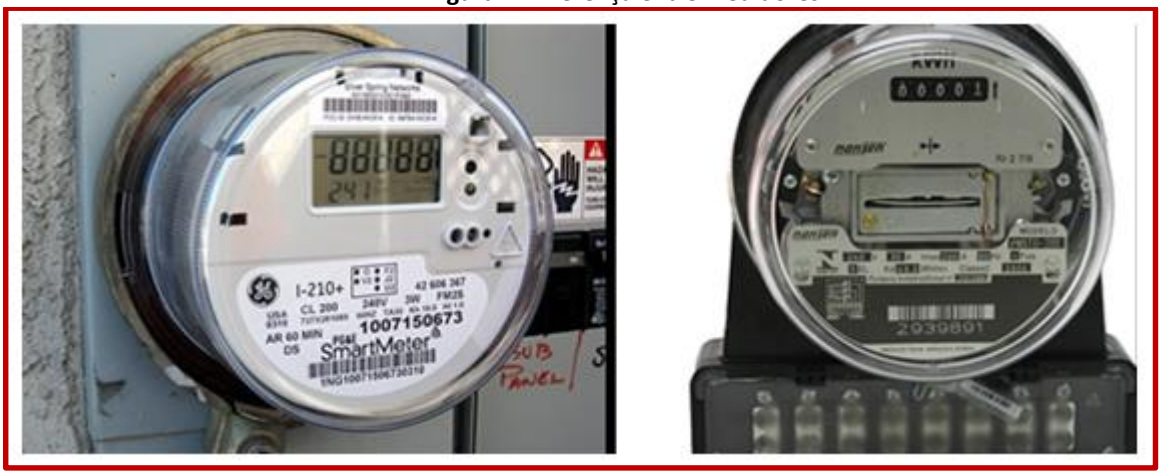
Wi-Fi / Wimax

Wi-Fi é uma tecnologia que permite a conexão de dispositivos (computadores, celulares, *Smart Meters, etc.)* à internet sem a necessidade de uma conexão física (cabeamento). Utilizando o padrão 802.11ac (protocolo de transmissão de dados), pode atingir velocidades de até 1300 Mbps. O Wimax também é uma tecnologia de transmissão de dados sem fio, porém com um alcance muito maior do que o Wi-Fi. Enquanto o Wi-Fi atinge distancias de dezenas de metros, a tecnologia Wimax alcança quilômetros (TELECO, 2008).

Smart Meters

O *Smart Meter* (medidor inteligente) é um equipamento utilizado para medir em tempo real o consumo de energia. Também possibilita a monitoração e controle dos eletrodomésticos e quaisquer dispositivos conectados as instalações elétricas dos consumidores. Com a implantação dos medidores inteligentes, os consumidores passarão a ter acesso as tarifas aplicadas pelas concessionárias antes do final do mês, podendo dessa forma, adaptar os hábitos de consumo e reduzir os gastos. Além desses benefícios, podem ser ressaltados alguns pontos como: tarifação diferenciada (valores distintos dependendo do horário do dia), maior número de informações, tanto para os consumidores quanto para as companhias de energia, monitoração da qualidade da rede (interrupções, tensão) entre outros (SOLARVOLT, 2017). Mesmo com diversas vantagens, a troca dos atuais medidores eletromecânicos pelos *Smart Meters,* ocasiona um elevado custo operacional, levando em consideração as milhões de unidades que devem ser substituídas. Segue abaixo a Figura 1, onde é mostrada a comparação entre um medidor inteligente (à esquerda) e um convencional (à direita):

Figura 1. Diferença entre medidores.



Fonte: Autor (2017).

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Artigo de Revisão

SMART GRID

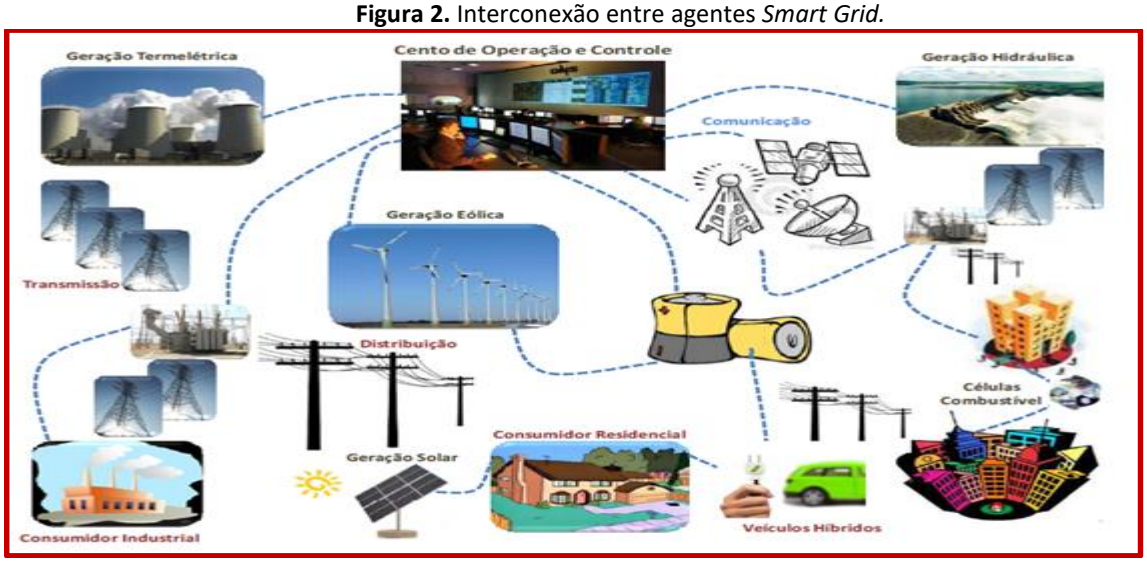
Segundo IEA (*International Energy Agency*, 2015), uma rede de energia inteligente (*Smart Grid*) é um sistema que utiliza as TIC (tecnologia da informação e comunicação) para monitorar e gerenciar a transmissão e distribuição de energia elétrica de todas as fontes geradoras às diferentes demandas dos usuários finais. A rede é capaz de coordenar as capacidades de todos geradores, operadores de redes, usuários finais e *stakeholders* (partes interessadas, como: governo, entidades reguladoras, concessionárias de energia, consumidores, etc.) do mercado de eletricidade, de uma maneira que permita a otimização na utilização dos recursos, operações, e no processo reduzir custos e impactos ambientais ao mesmo tempo em que preserva a confiabilidade, resistência e continuidade do sistema.

Com a implementação da *Smart Grid*, será possível saber em tempo real o consumo de energia, e realizar a emissão a partir da fonte geradora mais economicamente viável e abundante no momento. Do mesmo modo, será possível manipular remotamente todos os equipamentos automatizados que estejam conectados à rede.

Os sistemas elétricos deixaram de introduzir muitos avanços tecnológicos que proporcionariam uma qualidade de vida mais apropriada à era digital em que vivemos, por um investimento relativamente baixo. O homem consegue controlar equipamentos em outros planetas, mas depende, muitas vezes, de ligações dos consumidores alertando sobre quedas de energia ou alterações na rede, para só então enviar uma equipe ao local com a finalidade de reestabelecer o fornecimento de energia.

A Figura 2 a seguir, ilustra a constituição de uma *Smart Grid* e a interconexão entre os mais diversos agentes.

Figura 2. Interconexão entre agentes *Smart Grid.*



Fonte: SCHETTINO, 2013.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Artigo de Revisão

Muitos fatores contribuem para a inabilidade das atuais redes de energia elétrica conhecer a real demanda de energia dos consumidores. Os Quadros 1 e 2, a seguir, comparam algumas características das redes.

Quadro 1. Principais diferenças entre as redes atuais de energia e as redes inteligentes.

Redes Atuais	Smart Grid
Consumidores desinformados e não participativos.	Informados; consumidores envolvidos; reação por demanda e recursos de energia distribuída
Dominado pela central de geração – Muitos obstáculos para a interconexão dos recursos de energia distribuídos.	Muitos recursos de energia distribuída com a conveniência do *plug-and-play* focados na energia renovável
Limitado; pouca integração com os mercados atacadistas; oportunidades limitadas aos consumidores.	Maduro; muita integração com os mercados atacadistas; crescimento de novos mercados de eletricidade aos consumidores.
Foco em interrupções – Lenta reação aos problemas de energia.	Qualidade da energia é prioridade – rápida reação aos problemas de energia
Pouca integração de dados operacionais com gerenciamento de ativos	Aquisição de dados bem expandida dos parâmetros da rede; concentrada em prevenção, minimizando impactos aos consumidores.
Reage para prevenir danos posteriores – Concentra-se em proteger os ativos após as falhas	Automaticamente detecta e reage aos problemas; concentrada em prevenção, minimizando impactos aos consumidores.
Vulnerável à atos terroristas e desastres naturais; Lenta reação	Resistente a ataques cibernéticos e desastres naturais; rápida capacidade de restauração

Fonte: Momoh (2012).

Quadro 2. Principais diferenças entre as redes atuais de energia e as redes inteligentes.

Rede Tradicional	Rede Inteligente
Máquinas Elétricas	Digitais
Comunicação Unidirecional	Comunicação Bidirecional
Geração de Energia Centralizada	Geração de Energia Distribuída
Baixo uso de sensores	Alto uso de sensores
Monitoração Manual	Monitoração Automatizada
Recuperação Manual	Recuperação Automatizada
Poucas opções de usuários	Mais opções de usuários

Fonte (adaptada): Momoh (2012).

Máquinas Elétricas *versus* Digitais

Atualmente, as medições são efetuadas utilizando-se de medidores eletromecânicos. Uma vez por mês, um leiturista é encaminhado as residências e estabelecimentos para realizar a leitura e determinar o consumo de energia total,

podendo-se verificar assim, a conta do consumidor. Com a implementação dos medidores inteligentes, as companhias elétricas têm acesso a quantidade de energia que cada consumidor está utilizando, praticamente em tempo real. Os consumidores por sua vez, através de aplicativos, SMS, agência digital, conseguem obter informações sobre seu gasto também em tempo real, permitindo um maior controle e redução nos gastos.

Comunicação Unidirecional *versus* Comunicação Bidirecional

O atual sistema elétrico é unidirecional, ou seja, os consumidores apenas recebem a energia das concessionárias. Com o uso da *Smart Grid*, a comunicação passa a ser bidirecional, além de receber a energia, os consumidores passam a enviar e receber dados. Também podem produzir energia, enviando o excedente à rede da concessionária.

Geração de Energia Centralizada *versus* Geração de Energia Distribuída

A geração de energia centralizada é referente à energia produzida por grandes centrais elétricas, como hidrelétricas e termoelétricas, além das inúmeras redes de transmissão e distribuição, fazendo com que a energia chegue até o consumidor final. Já a geração distribuída, refere-se à produção de energia descentralizada, geralmente nas imediações de onde ela será consumida. Normalmente utilizam-se de fontes renováveis, como a energia solar, eólica e biomassa. Essa descentralização contribui com a redução nos custos relacionados a implantação de novas centrais elétricas e linhas de transmissão e distribuição, assim como na diminuição de perdas devido ao efeito *joule* (transformação de energia elétrica em energia térmica), e atenuação dos impactos ambientais (VANKS, 2017).

Baixo Uso de Sensores *versus* Alto Uso de Sensores

Na rede tradicional de energia elétrica, a maioria dos sensores utilizados não possui ligação com o sistema de comunicação, sendo assim, a verificação dos dados necessita ser efetuada localmente, o que pode levar muito tempo, devido a incapacidade dos sensores de indicar a localidade da falha precisamente. Diferentemente das redes *Smart Grid*, onde o número elevado de sensores possibilita saber com precisão os locais afetados, muitas vezes resolvendo o problema de forma automática (*self-healing).* Também podem ser integrados ao sistema Smart Grid, os sensores de uma residência, utilizando-se do HAN (*home area network),* conectados ao medidor inteligente, transmitindo informações pela rede.

Monitoração Manual *versus* Monitoração Automatizada

Quando alguma localidade fica sem energia, é necessário que o consumidor entre em contato com a distribuidora, e informe o incidente, para que só então ela envie uma equipe especializada para resolver o problema, levando muitas vezes horas para o reestabelecimento da energia. Com a utilização da rede *Smart Grid*, isso não seria necessário, com os inúmeros sensores da rede, a falha seria prontamente detectada, e em caso de impossibilidade da restauração automática, uma equipe já seria notificada e enviada ao local.

Recuperação Manual *versus* Recuperação Automatizada

Como mencionado na seção anterior, a rede *Smart Grid* possui a capacidade de auto recuperação (*self-healing),* quando possível, diferentemente da rede tradicional, onde os problemas sempre necessitam ser comunicados à concessionária de energia e uma equipe enviada para resolve-los.

Poucas Opções de Usuários *versus* Mais Opções de Usuários

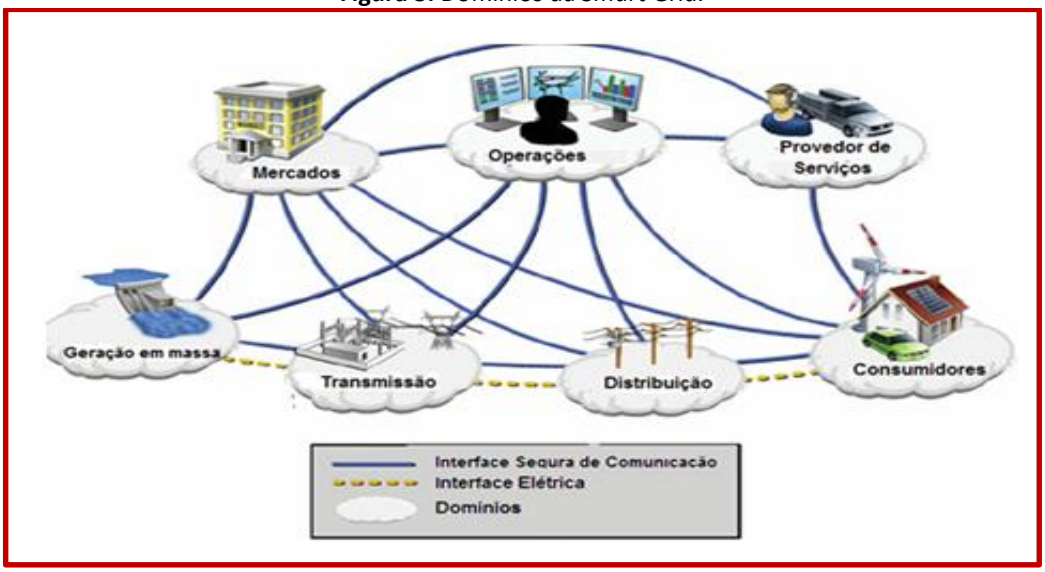
Os atuais usuários possuem pouca ou nenhuma interação com o sistema elétrico, enquanto que os usuários de um sistema *Smart Grid* podem saber em tempo real seu consumo elétrico, programar dispositivos para desligar ou ligar remotamente, sair da condição de apenas consumidor para transformar-se em um prosumidor (além de consumir energia, ele também produz e devolve na rede convencional).

ARQUITETURA *SMART GRID*

A arquitetura da *Smart Grid* foi proposta sendo constituída por sete domínios, conforme podemos conferir na Figura 3. A rede pode ser vista como tendo dois componentes principais, sistema e rede.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Artigo de Revisão

Figura 3. Domínios da *Smart Grid.*



Fonte (Adaptado): NIST, 2017.

Componentes do Sistema

Os principais componentes de uma *Smart Grid* são: medidores inteligentes, eletrodomésticos, recursos de energia renovável, centro de operações de eletricidade e os provedores de serviço.

Os medidores inteligentes são equipamentos que registram periodicamente o consumo de energia e transmitem essas informações as companhias de energia em tempo real. Os consumidores podem ter acesso ao consumo através da agência virtual, smartphones, SMS, e-mail ou aplicativos.

Os eletrodomésticos (inteligentes ou não) serão capazes de comunicar-se com os medidores inteligentes através da HAN (*Home Area Network*), possibilitando assim, um controle mais eficiente do consumo de energia de todos os equipamentos domésticos.

Os Centros de operações de eletricidade comunicam-se com os medidores inteligentes para controlar o consumo de energia. Também coletam informações de uso e notificações sobre possíveis alterações na rede utilizando GPRS (*General Packet Radio Service*).

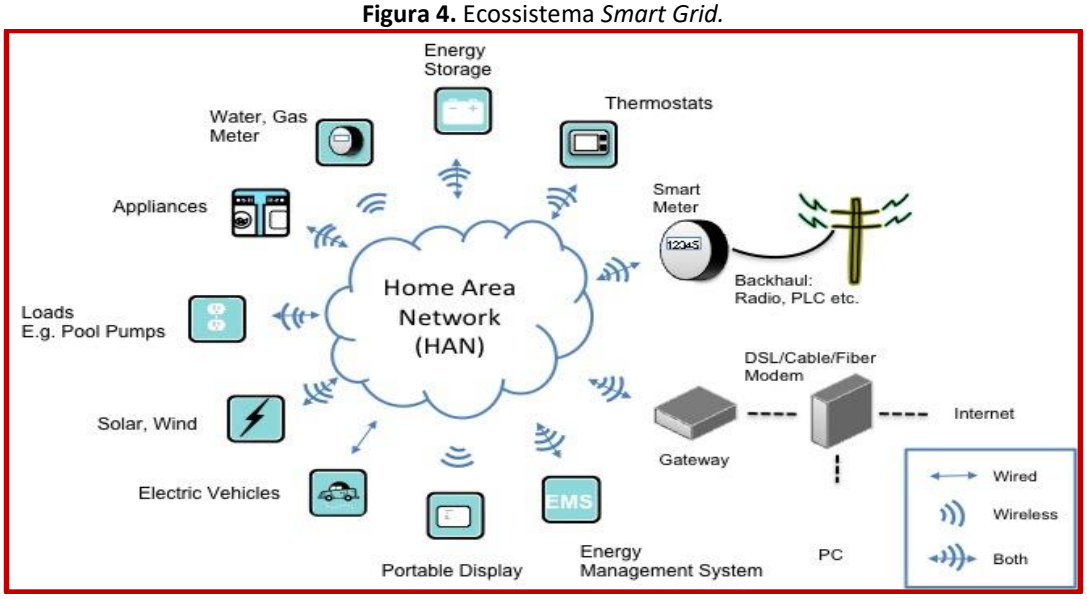
Os provedores de serviço estabelecem contratos para fornecer energia para dispositivos individuais. Eles interagem com os dispositivos internos via mensagens transmitidas pelos medidores inteligentes. Para constituir esse tipo de interação, os provedores de serviços devem obter certificados digitais para suas identidades e chaves públicas registrando-se nas companhias elétricas.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Artigo de Revisão

Componentes da Rede

As redes inteligentes integram dois tipos de comunicação: HAN e WAN (*Wide Area Network*). A HAN conecta os dispositivos da casa utilizando-se dos medidores inteligentes. A HAN pode comunicar-se usando Zigbee (protocolo para comunicação segura utilizando-se de redes sem fio), cabeamento, wireless Ethernet, ou Bluetooth (LEHRBAUM, 2013 e LINUXGIZMOS, 2017). Por outro lado, a WAN é uma rede maior que interconecta os medidores inteligentes, provedores de serviços e companhias de energia. A companhia elétrica gerencia a distribuição de energia dentro da rede, reuni informações sobre o uso da energia dos medidores inteligentes, e envia notificações aos medidores quando necessário. A mensagem enviada pelos dispositivos dentro da HAN é recebida pelos medidores e encaminhadas aos provedores de serviços adequados. A Figura 4, abaixo, retrata os dispositivos conectados através da HAN.

Figura 4. Ecossistema *Smart Grid.*



Fonte: NIST, 2017.

DIFERENÇAS ENTRE SEGURANÇA EM REDES TI E EM *SMART GRID*

Os objetivos primordiais de segurança em TI estão relacionados com os três princípios básicos (confidencialidade, integridade e disponibilidade), à medida que a segurança em redes automatizadas visa proporcionar proteção à vida humana, equipamentos e linhas de energia, e operação do sistema. Além disso, redes de TI utilizam-se de SO's (sistemas operacionais) e protocolos já bem definidos, enquanto que nas redes inteligentes, são empregados diferentes SO's e protocolos específicos de

acordo com o fornecedor. Até mesmo os padrões de qualidades são diferentes, no sentido de que em redes de TI é justificável a reinicialização do sistema em caso de falhas ou atualizações, enquanto que nas redes automatizadas, não é aceitável, considerando-se que os serviços energéticos devem estar disponíveis todo o tempo. Devido à essas diferenças, exige-se a implementação de novas soluções especificas para a *Smart Grid*.

Os desafios que as redes inteligentes devem confrontar no que se refere à cibersegurança, são destacados a seguir como: I) a quantidade de informações sensíveis dos consumidores que se propagam através da rede; II) acréscimo no número de equipamentos inteligentes, com baixa segurança física dos mesmos; III) a insuficiente organização (de forma obrigatória) de padrões; IV) o aumento considerável de *stakeholders* na rede elétrica com influência em sua confiabilidade; V) e a inexistência de um sistema regulatório internacional (MOREIRA e SCHETTINO, 2013).

Em um esforço de reduzir essas iminentes ameaças, o investimento em pesquisa e desenvolvimento (P&D) na área de cibersegurança das *Smart Grids* é imprescindível, assim como a elaboração de técnicas de certificação de segurança para as organizações e produtos. A cibersegurança deve ser reconhecida como fundamental e integrada pelas entidades reguladoras e *utilities* (empresas que trabalham com bens e serviços essenciais como: água, energia, gás) nas políticas energéticas globais e na regulamentação das *Smart Grids* (ALOUL, F et al., 2012).

RISCOS EM CIBERSEGURANÇA

Os riscos em cibersegurança podem aparecer em cada fase do projeto, e abrangem desde riscos gerenciais até operacionais e processos técnicos. Esses riscos são capazes de atingir sistema e equipamentos, gerenciamento e integração da rede, comunicações, controle e operações, e a disponibilidade do sistema (. As primeiras partes que podem estar vulneráveis aos riscos de segurança incluem as aplicações de TI, as redes de comunicações e os equipamentos inteligentes (medidores, termostatos, etc.).

Apesar dos mais variados aperfeiçoamentos do sistema de energia elétrica, a junção do atual sistema com a TIC pode ocasionar diversas possíveis vulnerabilidades, conforme descrito abaixo (GOODRICH e TAMASSIA, 2013):

- *Segurança do consumidor:* os medidores inteligentes automaticamente reúnem numerosas quantidades de dados e os transmitem às companhias de energia, consumidores e provedores de serviços. Informações das quais poderiam ser utilizadas para perceber as atividades dos consumidores, equipamentos em uso, e horários em que a casa ou estabelecimento encontra-se vazio.
- *Quantidade massiva de dispositivos inteligentes:* a *Smart Grid* possui diversos equipamentos inteligentes que possibilitam o gerenciamento do fornecimento de energia elétrica e demanda da rede. Equipamentos dos quais

podem ser usados como pontos de acesso para ataques, levando em consideração que a rede inteligente de energia é de 100 a 1000 vezes maior que a internet, tornando sua fiscalização e gerenciamento extremamente difíceis.

- *Segurança física:* ao contrário da rede tradicional de energia, a *Smart Grid* possui inúmeros dispositivos fora das instalações das companhias elétricas. Isso aumenta o número de locais inseguros, tornando-os vulneráveis à acessos físicos.
- *Tempo de vida dos sistemas elétricos:* como a coexistência das redes elétricas e sistemas TI são relativamente recentes, é inevitável que ainda existam equipamentos desatualizados em funcionamento. Esses dispositivos podem ter sua segurança comprometida mais facilmente, além das possíveis incompatibilidades com o novo sistema.
- *Confiança implícita entre dispositivos tradicionais de energia:* A comunicação entre dispositivos no sistema de controle está sujeita ao *spoofing (*ataque no qual um hacker se passa por outro aparelho ou usuário de uma rede com o objetivo de roubar dados, disseminar malware ou contornar controles de acesso, por exemplo (AVAST, 2017).
- *Equipes com diferentes experiências:* Comunicação ineficiente e desorganizada entre as equipes, pode levar a decisões erradas, contribuindo para o aumento das vulnerabilidades.
- *Usar Internet Protocol (IP):* Existe uma grande vantagem em utilizar-se dos padrões IP em sistemas *Smart Grid*, devido a sua compatibilidade entre os mais variados dispositivos. No entanto, dispositivos usando IP são suscetíveis à vários tipos de ataques baseados em IP, como *IP spoofing (ataque que consiste na falsificação de endereços IP, com intenção de roubos de dados), DoS (denial of service,* ataque que tem por objetivo impedir o acesso legítimo dos usuários a um computador), entre outros (SYMANTEC, 2017).
- *Mais stakeholders:* A quantidade significativa a mais de *stakeholders,* pode levar à um tipo de ataque muito perigoso: ataque interno, que consiste em uma brecha de segurança ocasionada por um integrante da organização que supervisiona ou constrói o sistema a ser protegido (MOREIRA e SCHETTINO, 2013).

CONSIDERAÇÕES FINAIS

Apesar da necessidade de um investimento inicial considerável para a sua implementação, a *Smart Grid* apresenta inúmeras possibilidades de melhorias, desde o aprimoramento da eficiência energética, aumento da confiabilidade, diminuição dos custos operacionais por parte das companhias de energia e uma provável redução nas

contas dos consumidores no decorrer do tempo. A *Smart Grid* aparece como uma alternativa viável e sustentável para a crescente demanda energética, incorporando ao atual sistema elétrico, energias renováveis como a eólica, a solar e a biomassa. Assim, os consumidores passam a ter um controle em tempo real de seu consumo, enquanto as concessionárias de energia gerenciam de forma mais eficiente toda a rede, podendo resolver distúrbios no sistema de modo mais ágil, muitas vezes remotamente.

No entanto, por fazer uso das tecnologias de informação e comunicação para aquisição e transmissão de dados, as questões de segurança são de extrema importância e devem ser consideradas. Neste artigo foram apresentados os principais riscos de segurança associados as redes inteligentes, bem como as diferenças entre essas redes e as redes de tecnologia da informação e comunicação. Como a *Smart Grid* é considerada uma infraestrutura crítica (interrupção pode ocasionar consequências sociais, políticas, econômicas), todas as possíveis vulnerabilidades devem ser detectadas, e as soluções viáveis necessitam ser implementadas para que haja diminuição dos riscos à uma condição admissível.

REFERÊNCIAS

ALOUL, F. et al. Smart Grid Security: Threats, Vulnerabilities and Solutions. **International Journal of Smart Grid and Clean Energy**, Beirute, v. 1, n. 1, set./ 2012.

AVAST. **Spoofing**. Disponível em: <https://www.avast.com/pt-br/c-spoofing>. Acesso em: 19 out. 2017.

FLICK, T.; MOREHOUSE, J. **Securing the smart grid**: Next Generation Power Grid Security. 1 ed. Burlington: Elsevier Inc., 2011. 298 p.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à segurança de computadores**. 1 ed. Internacional: Bookman, 2013. 568 p.

LINUXGIZMOS. **Zigbee-certified software supports smart grid devices**. Disponível em: <http://linuxgizmos.com/zigbee-support-for-smart-grid-apps/>. Acesso em: 17 out. 2017.

MOMOH, J. **Smart grid**: Fundamentals of Design and Analysis. 1 ed. Hoboken: John Wiley & Sons, Inc, 2012. 233 p.

MOREIRA, J. A.; SCHETTINO, S.; SILVA, R. M. Aspectos de segurança em smart grid. **Enegep**, Salvador, v. 1, n. 1, p. 1-12, out. 2013.

NIST - THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Smart grid: a beginner's guide**. Disponível em: <https://www.nist.gov/engineering-laboratory/smart-grid/about-smart-grid/smart-grid-beginners-guide>. Acesso em: 16 out. 2017.

SCHETTINO, S. **Cenários do uso das redes elétricas inteligentes (smart grid):** tendências de sua difusão no Brasil. 2013. 159 f. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal da Paraíba, Paraíba.

SMARTGRIDGOV. **What is the smart grid?**. Disponível em: <https://www.smartgrid.gov/the_smart_grid/smart_grid.html>. Acesso em: 15 out. 2017.

SOLARVOLT. **Entenda as vantagens da geração distribuída de energia**. Disponível em: <http://www.solarvoltenergia.com.br/entenda-as-vantagens-da-geracao-distribuida-de-energia/>. Acesso em: 24 out. 2017.

SYMANTEC. **Dos (denial-of-service) attack (ataque de dos (negação de serviço))**. Disponível em: <https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=d&word=dos-denial-of-service-attack>. Acesso em: 10 nov. 2017.

TELECO. **Wi-fi e wimax II: conceitos do wimax**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialww2/pagina_2.asp>. Acesso em: 15 dez. 1917.

VANKS, E. **O efeito joule: definição do efeito joule**. Disponível em: <http://www.efeitojoule.com/2008/04/efeito-joule.html>. Acesso em: 10 nov. 2017.

Os autores declararam não haver qualquer potencial conflito de interesses referente a este artigo.