Arquitetura de comunicação segura para Smart Grids

Yagor S. Duarte[1], Alexandre Silva Rodrigues[2], Bruno da Silva Alves[2], Tiago A. Rizzetti[1], Luciane Neves Canha[2], Marcio de Abreu Antunes[3]

[1]Colégio Técnico Industrial de Santa Maria - CTISM - UFSM
Av. Roraima, 1000 – 97015-900 – Santa Maria – RS – Brasil

[2]Centro de Tecnologia - UFSM – Santa Maria – RS – Brasil

[3]Companhia Estadual de Energia Elétrica - Distribuição - CEEE-D – RS – Brasil

{yagor,alexandre.rodrigues}@redes.ufsm.br, bdalves@inf.ufsm.br,
{tiago.rizzetti, lucianecanha}@ufsm.br, marcioaa@ceee.com.br

Abstract. *The concept of Smart Grids stands out by integrating new technologies and functionalities to the traditional power system. These new technologies bring with them vulnerabilities that need to be processed to obtain a secure channel for information exchange. Thus, it is proposed in this paper, an architecture for secure communication based on the addition of a self-contained device capable of handling the security features in a transparent way, acting as a bridge of communication between the network and the legacy device. In addition, allowing the gradual inclusion of this technology, without affecting the system in operation and at a reduced cost. Tests carried out demonstrate the feasibility of the idea.*

Resumo. *O conceito de Smart Grids se sobressai pela integração de novas tecnologias e funcionalidades ao sistema elétrico tradicional. Essas novas tecnologias trazem consigo vulnerabilidades que necessitam ser tratadas para que exista um canal seguro de troca de informações. Desta forma, é proposta neste trabalho, uma arquitetura para comunicação segura baseada na adição de um dispositivo autocontido capaz de tratar das funcionalidades de segurança de forma transparente, atuando como uma ponte de comunicação entre a rede e o dispositivo legado, assim, permitindo a inclusão gradativa desta tecnologia sem afetar o sistema em funcionamento e a um custo reduzido. Testes realizados demonstram a viabilidade da ideia.*

1. Introdução

O termo Redes Elétricas Inteligentes (REI), é mundialmente debatido como o futuro do Sistema Elétrico de Potência (SEP) atual. Um sistema novo, capaz de introduzir novas tecnologias e funcionalidades aliadas a um melhor gerenciamento de toda a infraestrutura do sistema de energia. Para obter o efeito esperado, faz-se necessária a implementação de um mecanismo de comunicação confiável.

A incorporação das tecnologias da informação e redes de comunicação bidirecionais também no segmento de distribuição do SEP irá proporcionar um conjunto de novas aplicações, entre elas a infraestrutura de medição e atuação remota denominada *Advanced Metering Infrastructure* (AMI). Muitas mudanças são esperadas com a

implementação da AMI. Dentre elas vale destacar, como exemplo, o gerenciamento de demanda. Com essa nova capacidade de acompanhar e controlar a demanda por energia, possivelmente a curva de carga dos consumidores será mais homogênea, por meio de uma tarifação dinâmica [Brown 2008] [Yan et al. 2013]. Com essas novas possibilidades de medições mais precisas, será possível estabelecer tarifações para diferentes horários do dia, a partir dos níveis de consumo. Isso significa que, em períodos do dia que cotidianamente apresentem um elevado consumo, poderá ser adotada uma tarifa de maior custo. [Rivera et al. 2013] [Yan et al. 2012].

Devido a racionalização da geração e demanda de energia, incluindo novas possibilidades de aplicações, surge a necessidade de evoluções tecnológicas com o objetivo de obter um melhor gerenciamento e evitar falhas. Esse novo sistema deve apresentar um eficiente mecanismo de comunicação digital. Os dispositivos devem poder responder a comandos remotos para recuperar ou melhor distribuir energia elétrica aos consumidores [CGEE 2012].

Falhas de sistema não devem representar grandes impactos aos consumidores, concessionárias e ao sistema elétrico de potência como um todo. Portanto, é imprescindível que o sistema apresente um certo nível de resiliência, sendo capaz de se manter em operação, mesmo na presença de falhas controladas e até mesmo retornar a seu estado estável de operação. Essas particularidades devem estar inclusas nas tecnologias de informação e mecanismos de comunicação de dados presentes neste ambiente. Todo o controle de operações e reconfigurações sobre o SEP é baseado nos dados provindos do sensoriamento, como o dos dispositivos de medição inteligente, que devem trocar informações em um ambiente seguro.

Os recursos computacionais de hardware e software essenciais para a implementação do conceito de REI, estarão incorporados de forma embarcada nos novos dispositivos a serem projetados. Porém, faz-se necessária uma gradativa implementação deste conceito ao SEP, ou seja, adicionar essas tecnologias aos dispositivos legados já presentes no sistema atual. Isso justifica-se devido ao elevado tempo que seria necessário para a substituição imediata de todos os equipamentos do SEP, além do, economicamente inviável, investimento financeiro que teria de ser feito para tais mudanças.

Pensando nisso, este artigo traz uma proposta de uma arquitetura de comunicação segura onde um dispositivo do tipo caixa preta será utilizado na comunicação entre o sistema de supervisionamento e os dispositivos para adicionar algumas funcionalidades aos novos e expandir as capacidades dos legados. Dentre os recursos de software disponibilizados, estará a utilização de plugins para tratamento dos pacotes, como proteções criptográficas, antes de chegarem na rede de comunicação.

Nas próximas seções será apresentada a arquitetura proposta neste artigo, suas motivações e resultados obtidos.

2. Arquitetura proposta

2.1. Sistema SCADA

Um sistema SCADA pode ser visto como um sistema de automação ou controle industrial, que através de protocolos de comunicação pode monitorar, controlar e se comunicar com sensores e atuadores. Desta forma, efetuando leituras de informações, ou

mesmo enviando comandos para estes dispositivos[Strehl 2012]. Em função da diversidade de dispositivos presentes nesse tipo de sistema, os protocolos utilizados são variados. A rede de comunicação utilizada também é heterogênea, abrangendo sistemas legados como o MODDBUS, bem como sistemas mais atuais que utilizam redes baseadas em IP [Ghansah 2009] [Makhija and Subramanyan 2003]. Devido à extrema relevância das informações em uma *Smart Grid*, são essenciais capacidades de segurança em tempo real ao sistema SCADA, como integridade e autenticidade dos pacotes [Aloul et al. 2012] [Ghansah 2009].

O sistema SCADA obtém os dados através de uma rede IP dos seus dispositivos supervisionados [Knapp and Langill 2014]. A adoção de padrões de protocolos abertos, baseados no protocolo IP, expande o contexto de segurança. Possíveis ataques ao sistema SCADA, como ataques de negação de serviço, mascaramento de ip, espionagem e falsificação de dados, seriam de alto impacto ao SEP. Ataques podem fazer com que os dados tornem-se inválidos ou inacessíveis, dessa forma, as aplicações que fazem uso desses dados podem deixar de operar, causando danos ao sistema de energia. Com esse cenário, podem ser verificadas as vulnerabilidades no sistema de comunicação.

Alguns sniffers de rede, como o Wireshark ou TCPDump podem ser utilizados para realizar a análise das informações de tráfego de rede. Informações críticas, como as oriundas dos medidores inteligentes, podem ser interceptadas e adulteradas caso não exista algum tipo de criptografia na mensagem. Além do fato de que ataques de negação de serviço ao sistema de supervisionamento podem torná-lo indisponíveis.

2.2. Arquitetura desenvolvida

Com base nessas vulnerabilidades de segurança, soluções foram desenvolvidas com o objetivo de atenuá-las, utilizando como referência os prazos de tempo de mensagem, estabelecidos pelo padrão IEC61850 [Mackiewicz 2006]. A adição de assinatura digital e criptografia, que exigem um certo poder de processamento, será provida por meio do dispositivo tipo caixa preta. Esse dispositivo contem suporte, via hardware e software, para essas funcionalidades.

Padrões como o IEC 61850 e IEC 62351 apresentam, respectivamente, arquiteturas de mensagens e segurança, visando padronização na implementação de Smart Grids [Baigent et al. 2004] [Cleveland 2012]. Porém, a implementação de segurança não é bem especificada. Existem incompatibilidades de hardwares, que possuem limitada capacidade computacional, mensagens com prazos diferentes, e muitos IEDs implementam ainda protocolos legados como o MODBUS.

Nesse contexto, para prover funcionalidades de segurança aos dispositivos, faz-se necessária a utilização de componentes adicionais na arquitetura. Neste artigo, optou-se pelo uso do Mediador de Pacotes (MEPA) e o uso de plugins de tratamento de pacotes. Esses visam implementar requisitos que supram as normas do padrão de segurança [Hohlbaum et al. 2010]. Com a utilização desses, a comunicação entre o sistema SCADA e os IEDs serão realizadas de forma segura. Passando a solucionar as questões referentes à confidencialidade, integridade, disponibilidade e autenticidade.

2.2.1. Plugins

Para prover as funcionalidades de tratamento dos pacotes, serão utilizados plug-ins de acordo com a necessidade de operação. Um plugin é um elemento de software carregado a partir do software principal, neste caso o MEPA. O plugin é responsável por realizar o tratamento sobre o pacote de rede, não demandando qualquer modificação ou recompilação do código da aplicação principal. Desta forma, cada nova demanda no tratamento de pacotes poderá ser adicionada através da implementação de um plugin apropriado.

Uma vez que o pacote seja tratado, ele é devolvido à aplicação principal que irá deixar que este siga o fluxo normal. Desta forma, para que o tratamento do pacote possa ser efetivo ele deverá ser realizado em ambas as partes comunicantes, ou seja, emissor e receptor. Os elementos envolvidos no caminho da comunicação não sofrem qualquer alteração.

No caso da segurança da comunicação, por exemplo, deverá ser desenvolvido um plugin responsável por implementar um sistema de chaves criptográficas para garantir autenticidade, confidencialidade e integridade dos dados. Junto ao emissor e receptor uma instância deste plugin deve ser executada, permitindo a comunicação entre as partes. Na arquitetura proposta os plugins são carregados pelo MEPA e executam sobre a plataforma de hardware adicionada para tal, no formato de um dispositivo do tipo caixa preta, autocontido e transparente aos elementos finais nos quais se conecta.

2.2.2. MEPA

Mediador de Pacotes ou MEPA, foi construído a partir da utilização do driver TUN/TAP, disponível no Kernel do Linux [Maxim Krasnyansky]. Ele é responsável por realizar a filtragem de pacotes, verificando se está presente no pacote informações que correspondam a algum dos filtros previamente cadastrados. O software MEPA deve ser implementado no dispositivo autocontido, representado junto ao IED e ao sistema SCADA. Caso o MEPA não encontre nenhum filtro que corresponda ao pacote interceptado, ele irá reinserir o pacote no mesmo ponto da pilha TCP/IP do kernel. Essa característica torna a arquitetura flexível, uma vez que somente serão afetados tráfegos específicos de uma aplicação, representada pelo filtro cadastrado.

As funcionalidades a serem providas pelo MEPA são basicamente 3: a) Interceptar pacotes na interface de entrada; b) Verificar se o pacote corresponde a algum filtro pré-cadastro, em caso afirmativo passar ao plugin correspondente e; c) reinserir o pacote na pilha de protocolos TCP/IP para que seja devidamente tratado pela pilha de protocolos disponível no kernel Linux. Nota-se que a reinserção de pacote deverá ser realizada tanto se o pacote foi tratado por um plugin como quando ele não corresponde a nenhum filtro e, portanto, nenhum tratamento é realizado. A figura 1 ilustra esse processo.

As características do MEPA tornam a proposta flexível para poder ser utilizada em qualquer cenário de comunicação entre sistemas SCADA e IEDs. Em dispositivos de softwares que podem ser modificados, o MEPA e os plugins podem ser implementados de maneira embarcada.

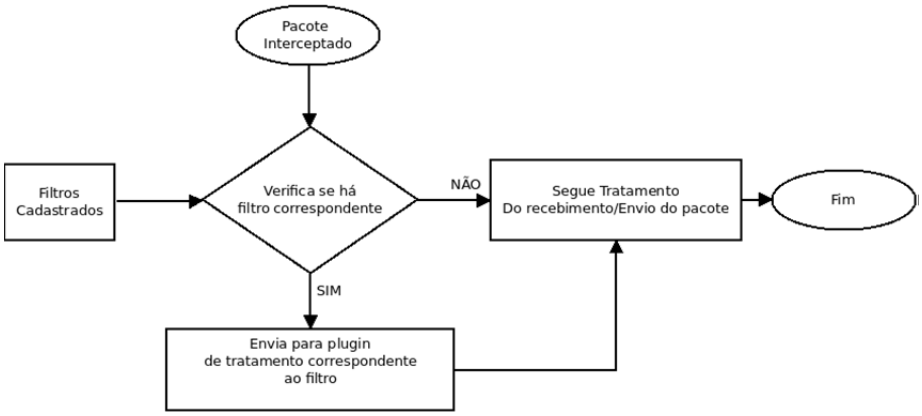

Figure 1. Cenário da arquitetura proposta (Fonte: Acervo pessoal).

A função de interceptação de pacotes do MEPA é proporcionada pela utilização do plugin TUN/TAP, disponível no Linux. TUN/TAP é um driver presente no Kernel do Linux, capaz de criar interfaces de rede virtuais. Tais interfaces permitem que ao invés de receber/enviar pacotes através de um hardware, o dispositivo receba/envie pacotes provenientes de uma aplicação em modo usuário (*user space*).

O driver TUN/TAP provê dois tipos de dispositivos: a) TAP: interface capaz de operar na camada de enlace, enviando/recebendo pacotes da Ethernet; b) TUN: interface capaz de operar na camada de rede, enviando/recebendo pacotes do tipo IP (*Internet Protocol*) [Maxim Krasnyansky]. Assim, através do driver TUN/TAP, uma aplicação é capaz de enviar ou receber pacotes da pilha de protocolos de rede, permitindo que a aplicação presente no MEPA seja capaz de interceptar, repassar, modificar e analisar os pacotes passantes.

3. Resultados parciais obtidos

Para verificar a eficiência e viabilidade da proposta apresentada nesse trabalho, criou-se um ambiente de testes, utilizando-se um cenário real, composto por um sistema SCADA e um painel fotovoltaico. Esse painel possui possibilita o monitoramento e gerenciamento remoto, obtidos através da utilização do sistema SCADA. Nesses termos, para realizar o monitoramento foi utilizado o software *Elipse Power*, que possibilita monitorar as informações referentes à energia gerada pela placa em tempo real.

A troca de mensagens entre a placa fotovoltaica e o sistema SCADA foi realizada por meio do protocolo MODBUS sobre TCP, ou seja, após estabelecer uma comunicação inicial em uma porta específica da placa, o sistema SCADA realiza a sondagem de informações a cada intervalo de tempo preestabelecido. Os dados dessa leitura são apresentados em uma interface HMI (*Human Machine Interface* ? Interface Homem-Máquina), na qual o técnico pode intervir no funcionamento caso esses dados estejam fora do padrão. Também há possibilidade de que o sistema SCADA possa intervir automaticamente, quando programado para tal função, diante de políticas de funcionamento.

Quanto aos aspectos práticos relacionados ao cenário de teste, foram utilizados dois computadores, os quais executavam o MEPA (para interceptar e analisar os pacotes) e um plugin desenvolvido para realizar operações de criptografia e descriptografia de mensagens que estavam de acordo com os padrões definidos nos filtros utilizados no MEPA.

Dos computadores utilizados o primeiro identificado como PC_i5 é constituído de um processador i5 da Intel® de 3320M de cache com *clock* de 2.6GHz, 8 GiB de memória DDR3 de 1600 MHz. O segundo computador identificado como PC_AMD, é constituído de um processador AMD Phenom II X2 B55 de 7256M de cache com *clock* de 1,5GHz, 4 GiB de memória DDR3 de 1333MHz.

Com base no cenário de testes descrito anteriormente, foi realizado um ataque de Homem do Meio, inserindo pacotes modificados, pacotes falsos e aplicando retardos na comunicação. Este ataque consiste na inserção de um novo elemento na comunicação de preferência entre os dispositivos que estão com a comunicação estabelecida e de modo transparente. A medida que os pacotes eram inseridos na comunicação, o MEPA interceptava-os e redirecionava para o plugin verificar os aspectos relacionados à criptografia e assinatura digital. Dessa forma, os pacotes modificados e pacotes falsos foram descartados, já que suas características estavam alteradas, o plugin não conseguiu descriptografar, nem validar sua assinatura digital.

Outro aspecto importante que deve ser abordado para garantir a segurança e disponibilidade de um sistema é a proteção contra ataques de negação de serviço (DoS, *Denial of Service*). Sendo assim, para analisar o comportamento da arquitetura proposta, utilizou-se a ferramenta HPING3 para simular um ataque DoS no sistema SCADA e painel fotovoltaico, efetivando uma inundação de requisição SYN na porta especifica do sistema SCADA. Nesse sentido, como em toda e qualquer comunicação, antes de chegar ao sistema SCADA, essas requisições foram interceptadas pelo MEPA e redirecionadas para a verificação de segurança. Dessa forma, a partir da resposta negativa do plugin, o MEPA descartou todas requisições indevidas. Além disso, todas as mensagens com criptografia incorreta, quebra de integridade do pacote e/ou confidencialidade foram descartadas.

Além disso, optou-se por verificar o tempo necessário para realizar operações de criptografia e descriptografia dos pacotes interceptados pelo MEPA. Os resultados obtidos referem-se ao tempo que cada computador precisou para realizar tais tarefas. Para realizar esse teste, foram realizadas sessões de cem sondagens ao sistema SCADA à placa fotovoltaica, efetuadas 10 vezes em diferentes horários do dia, totalizando 1000 sondagens. A média de tempo que o computador PC_i5 levou em cada sondagem, foi de 4,09 milissegundos para criptografar e descriptografar os dados. A média de tempo que o computador PC_AMD levou foi de 10,97 milissegundos.

Assim sendo, com a utilização do plugin integrado ao MEPA nas duas extremidades realizando a verificação de segurança, os pacotes demoraram em média 15,06 milissegundos a mais em uma sondagem. A Figura 2 apresenta o gráfico que mostra a notável diferença de desempenho de um computador para outro. O computador PC_i5 levou menos tempo para aplicar a segurança à informação do que o computador PC_AMD. Isso acontece porque os computadores utilizados possuem características diferentes, impactando no tempo em que cada um necessita para realizar as tarefas. Pode-se afirmar que no contexto de Redes Elétricas Inteligentes, isso é um problema comum, pois há heterogeneidade de dispositivos com limitações de processamento e memória.

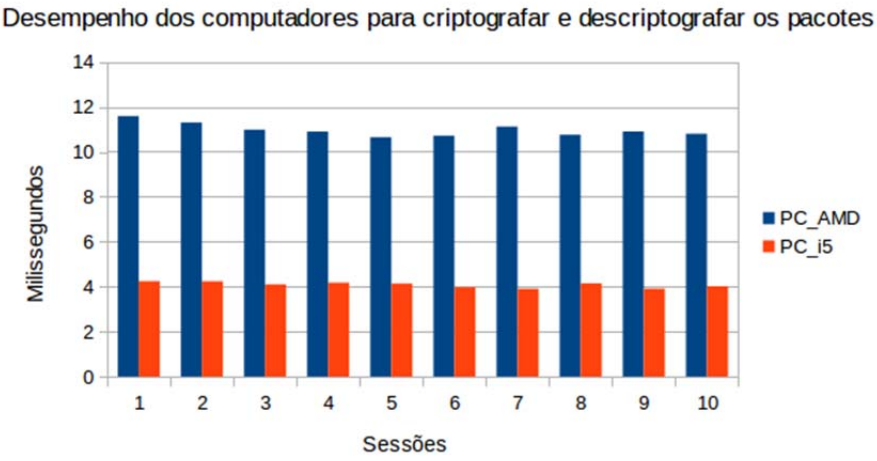

Figure 2. Gráfico de desempenho dos computadores utilizados nos testes (Fonte: Acervo pessoal).

4. Conclusão

A implementação do conceito de REI em sistemas de energia é uma realidade, assim como, as preocupações com a segurança da comunicação desses sistemas. Neste trabalho, as principais tecnologias utilizadas pelo sistema, suas ameaças e vulnerabilidades foram levantadas. Diante disso, para amenizar parte desses problemas, propôs-se a utilização de um Mediador de Pacotes, que possibilita a integração com plugins capazes de realizar operações voltadas a garantir a segurança das informações trocadas entre equipamentos presentes no sistema elétrico e os sistemas supervisórios. Nesses termos, a arquitetura apresentada possibilita implementar tais medidas em qualquer cenário que utilize o sistema SCADA. Com isso, todos os equipamentos dessa rede podem utilizar este serviço.

Desta forma, a comunicação entre o sistema SCADA e IEDs passa a ser assinada digitalmente ou criptografada, provendo integridade, legitimidade e autenticidade das mensagens. Além disso o Mediador de Pacotes controla todas as comunicações de entrada e saída do sistema SCADA e dos IEDs. Nesse contexto, a utilização do Mediador de Pacotes e do plugin desenvolvido demonstraram ser uma solução viável, apresentando resultados promissores, ou seja, por meio da arquitetura proposta é possível garantir que os dados cheguem autênticos e íntegros.

Durante os testes no cenário real, observou-se um discreto retardo nos tempos necessários para aplicar criptografia ou assinatura digital na comunicação. No entanto, pode-se afirmar que diante da diversidade de dispositivos utilizados em Redes Elétricas Inteligentes, é possível implementar segurança em mensagens cuja comunicação acontece através de uma comunicação TCP/IP cliente/servidor e também atender os prazos de tempo, especificados no padrão IEC 61850 em mensagens MMS. Para trabalhos futuros sugere-se a otimização do código do Mediador de Pacotes, para melhorar a performance e modificá-lo para que realize a aplicação de assinatura digital e ou criptografia em mensagens com prazos de tempo reduzido especificadas pelo padrão IEC 61850.

Agradecimentos

Os autores agradecem o apoio da ANEEL P&D Código PD-5707-4301/2015, CEEE-D, UFSM e CNPq (Processo 311516/2014-9).

Referências

Aloul, F., Al-Ali, A., Al-Dalky, R., Al-Mardini, M., and El-Hajj, W. (2012). Smart grid security: Threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy*, 1(1):1–6.

Baigent, D., Adamiak, M., Mackiewicz, R., and SISCO, G. M. G. M. (2004). Iec 61850 communication networks and systems in substations: An overview for users. *SISCO Systems*.

Brown, R. E. (2008). Impact of Smart Grid on Distribution System Design.

CGEE (2012). Centro de gestão e estudos estratégicos (org.). *Redes elétricas inteligentes: contexto nacional. Brasília: Tatiana de Carvalho Pires*.

Cleveland, F. (2012). Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure. *White Paper*.

Ghansah, I. (2009). Smart grid cyber security potential threats, vulnerabilities and risks. *California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047*.

Hohlbaum, F., Braendle, M., and Alvarez, F. (2010). Cyber security practical considerations for implementing iec 62351. In *Proceedings of the PAC World Conference*.

Knapp, E. D. and Langill, J. T. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Mackiewicz, R. (2006). Overview of iec 61850 and benefits. In *Power Systems Conference and Exposition, 2006. PSCE'06. 2006 IEEE PES*, pages 623–630. IEEE.

Makhija, J. and Subramanyan, L. (2003). Comparison of protocols used in remote monitoring: Dnp 3.0, iec 870-5-101 & modbus. *Electronics Systems Group, IIT Bombay, India, Tech. Rep*.

Maxim Krasnyansky, Maksim Yevmenkin, F. T. Universal TUN/TAP device driver. `https://www.kernel.org/doc/Documentation/networking/tuntap.txt`. Accessed: 2017-07-20.

Rivera, R., Esposito, A. S., and Teixeira, I. (2013). Redes elétricas inteligentes (smart grid): oportunidade para adensamento produtivo e tecnológico local. *Revista do BNDES 40*, pages 43–84.

Strehl, L. C. (2012). Prospecção de tecnologias para aumentar a segurança em sistemas scada.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A Survey on Smart Grid Communication Infrastructures : Motivations , Requirements and Challenges. 15(1):1–16.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys Tutorials*, 15(1):5–20.