DINCON 2017
CONFERÊNCIA BRASILEIRA DE DINÂMICA, CONTROLE E APLICAÇÕES
30 de outubro a 01 de novembro de 2017 – São José do Rio Preto/SP

Controlador POX para a detecção de anomalias em redes Smart Grid

Ricardo Cesar Câmara Ferrari[1]
Departamento de Engenharia Elétrica, Unesp, Ilha Solteira, SP
Ailton Akira Shinoda[2]
Departamento de Engenharia Elétrica, Unesp, Ilha Solteira, SP
Christiane Marie Schweitzer[3]
Departamento de Matemática, Unesp, Ilha Solteira, SP

Resumo. O trabalho trata da união das tecnologias *Software Defined Networking* (SDN) e *Smart Grid*, possibilitando que as redes inteligentes consigam usufruir da arquitetura das SDNs, que centralizam todo plano de controle em um controlador, abrindo oportunidades para aplicações de segurança em *Smart Grid*. Após uma análise em trabalhos relacionados à segurança em *Smart Grid*, o trabalho propõem uma aplicação com o uso de desvio padrão para definir limites de máximo e mínimo para detecção de anomalias nos fluxos. Desta forma, foram realizados testes para analisar e monitorar o fluxo de dados de um *OpenVSwitch* (OVS), afim de identificar possíveis anomalias durante a troca de dados entre escravos e mestre.

Palavras-chave. SDN, *Smart Grid*, anomalias, desvio padrão.

1 Introdução

Com o objetivo de aumentar a integração e um uso de energia mais inteligente, com recursos energéticos distribuídos, a *Smart Grid* (detalhada em [8]) foi proposta para substituir o sistema de energia convencional, possibilitando um sistema inteligente de energia e comunicação de dados. Uma diversidade de dispositivos e eletrodomésticos serão interligados e se comunicarão em uma rede inteligente para medição, monitoramento e controle.

Pesquisas recentes com *Smart Grid*, como apresentadas em [9, 11, 12], avaliam a utilização de um novo paradigma para auxiliar em seu gerenciamento, esse novo paradigma é chamado de SDN. Ele atraiu muita atenção devido a um novo conceito de arquitetura de rede que abstrai as

[1] rccferrari@hotmail.com
[2] shinoda@dee.feis.unesp.br
[3] christiane.schweitzer@gmail.com

funcionalidades de controle do hardware para um controlador de *software* externo (plano de controle). Isto coloca a SDN como uma opção extremamente conveniente, possibilitando centralizar o plano de controle da rede em uma única máquina. Pelo fato do controlador ser implementado como *software*, permite o controle do fluxo nos comutadores de rede, deixando qualquer tipo de configuração ou autoconfiguração mais ágil. Desta forma, uma SDN é vista como um grande potencial de utilização na comunicação de uma rede *Smart Grid*.

Com base em uma revisão bibliográfica realizada, várias pesquisas abordam a utilização de SDN para fornecer recursos para redes *Smart Grid*, porém não foi encontrado nenhum estudo que trate do monitoramento no fluxo de uma *Smart Grid* para detecção de anomalias para possíveis tentativas de ataques ou mau funcionamento da rede no fluxo de dados de um *switch* com suporte SDN ou em escravos individuais, levando em conta o cálculo de desvio padrão em intervalos diferentes.

O trabalho apresentado por [8] ilustra 8 arquiteturas, onde são consideradas como candidatas para soluções SDN e *Smart Grid*, sendo que 3 apresentam soluções de segurança, descritas em [7, 1, 10]. A primeira arquitetura trata de sistemas baseados em IEC 61850 (*International Electrotechnical Commission*), capaz de realizar reencaminhamento de tráfego de dados, QoS (*Quality of Service*) e distribuição da carga de tráfego. Utiliza também o coletor de dados *sFlow* (solução pronta) para detecção de limite excedido e o comunica ao controlador. A segunda arquitetura apresenta apenas um protótipo e não apresenta nenhuma implementação ou resultados. Por fim, em [10], a solução proposta apresenta recursos como, estabelecer rotas dinâmicas, restabelecer um roteamento comprometido e troca de canais com cifragem, em possíveis ataques. O IDS está implementado fora do controlador, isso pode gerar maior custo de manutenção em uma atualização, pois são 2 *hosts* diferentes. Também não apresenta uma forma de identificar algum “estranho” na rede ou “derrubar” o atacante. A simulação não apresenta nenhuma forma de aprendizado para que o controlador possa monitorar a rede de forma mais precisa, levando em conta que cada rede pode se comportar de uma forma diferente.

Motivado pelas oportunidades que uma SDN pode trazer para uma *Smart Grid* em relação a sistemas de segurança e pela oportunidade de aplicação de outras técnicas para detecção de intrusos nesta rede, é proposta uma arquitetura capaz de calcular desvios padrão para diferentes momentos e com isso analisar possíveis anomalias de fluxos em diferentes intervalos do monitoramento, além de detectar e derrubar nós que não fazem parte da rede pré-definida.

Para isso, o artigo está organizado da seguinte forma: A Seção 2 examina mais detalhadamente a SDN e a *Smart Grid*. A Seção 3 expõe os materiais e métodos, com o objetivo de apresentar o plano de testes. Em seguida, a seção 4 apresenta os resultados obtidos com base no plano de testes da seção anterior. Por fim, a Seção 5 conclui o artigo.

2 SDN e Smart Grid

Apresentado por [8], uma *Smart Grid* é uma combinação entre redes de energia, redes de comunicação e sistemas de gerenciamento de informações, o que favorece a geração de energia verde e econômica. Geralmente, uma Smart Grid possui uma infraestrutura de comunicação de dados integrada com uma rede elétrica que coleta e analisa dados capturados em tempo de execução sobre a transmissão, distribuição e consumo de energia. Assim, a chave para habilitar um sistema *Smart Grid* é a convergência contínua de sistemas de rede de energia existentes e tecnologias da informação.

O *Distributed Network Protocol* (DNP3) é adequado para aplicação em ambiente SCADA,

incluindo comunicações para *Intelligent Electronic Device* (IED), mestre em comunicações remotas, peer-to-peer e aplicativos de rede. O DNP3 tem a flexibilidade para suportar vários modos de operação, como resposta de leituras e respostas não solicitadas, além de permitir vários mestres e escravos [6].

Já uma SDN, como discutida em [8] é uma arquitetura de rede de próxima geração com serviços de gerenciamento, como filtragem de pacotes, comutação e monitoramento. Em uma SDN, um controlador de rede centralizado gerencia o plano de controle da rede em vez de *switches* de rede individuais. O fluxo de cada *switch* é reportada ao controlador SDN quando essa comunicação não está listada em sua tabela de fluxo. O controlador SDN fornece a nova regra de fluxo ao *switch* através de uma interface (como o *OpenFlow)* para o plano de encaminhamento. Assim, o administrador do serviço gerencia e monitora o sistema de comunicação sem a necessidade de um sistema de gerenciamento de rede adicional.

Foram desenvolvidos diversos controladores para o paradigma SDN. Porém, o controlador utilizado nesse trabalho foi o POX, sendo uma plataforma para o desenvolvimento, além de prototipagem de aplicações para SDNs usando *Python*.

3 Materiais e Métodos

O objetivo principal do trabalho é analisar a quantidade de falsos positivos que podem ocorrer durante a análise de fluxo em um *switch* virtual (OVS), possibilitando identificar os melhores valores para os limites de máximo e mínimo, de pacotes e *bytes*, para que seja considerado anomalia no fluxo.

A Figura 1 apresenta o ambiente utilizado para testes. Para a realização foi utilizado o ambiente GENI (*Global Environment for Network Innovations*), uma infraestrutura aberta afim de proporcionar a pesquisa em redes em escala e sistemas distribuídos, sendo 27 máquinas escravas, 1 OVS, 1 sensor, 1 mestre e 1 controlador POX.

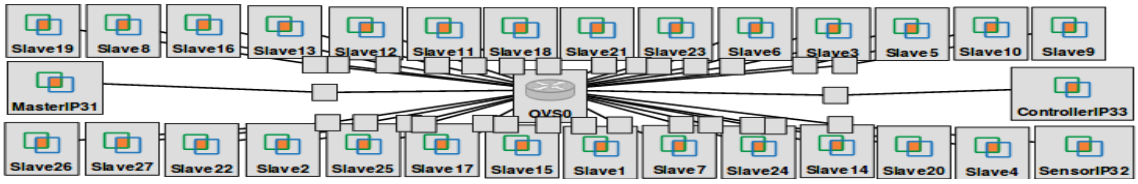

Figura 1: Ambiente de testes no GENI.

Foram utilizados os *softwares*, OVS 2.3.1 [2], GENI [5], *OpenDNP3* 1.1.0-RC1 [3] e o controlador POX 0.1.0-betta [4].

Para realizar os experimentos, foram utilizadas 30 máquinas (número de portas do *switch*) interligadas através do OVS. Com isso, o mestre gera fluxo DNP3 contínuo para cada conexão individual de aproximadamente 62 pacotes/min e 4830 *bytes*/min e as máquinas escravas respondem as solicitações com 31 pacotes/min e 2738 *bytes*/min, com a ferramenta *OpenDNP3*, possibilitando com isso o cálculo dos desvios em 6 intervalos de tempo (6 horas). O controlador da rede SDN está preparado para monitorar os fluxos necessários para as comunicações entre as máquinas escravas e o mestre da *Smart Grid* para os cálculos dos desvios padrão. Por fim, uma máquina sensor verifica se alguma nova máquina entra na rede durante o período de monitoramento (não abordado neste trabalho). No controlador utilizou-se o POX para monitorar o

tráfego entre as máquinas, para que fosse identificada alguma anomalia no fluxo.

Como apresentado na Figura 2, após as finalizações dos cálculos dos desvios D1, D2, D3, D4, D5 e D6, no período entre as 22:54:53 e as 4:54:53, o controlador é capaz de iniciar o monitoramento do fluxo no *switch*, identificando possíveis anomalias.

Para os cálculos dos desvios, foi definido um tempo de leitura da tabela de fluxo do OVS de 1 min., com 60 leituras por intervalo, para determinar os conjuntos de 60 valores de pacotes e *bytes* utilizados para os cálculos dos desvios. Os valores definidos, como tempo de leitura, quantidade de leituras, IP do sensor e número de desvios padrão para os fluxos e *switch* podem ser alterados em um arquivo de configuração.

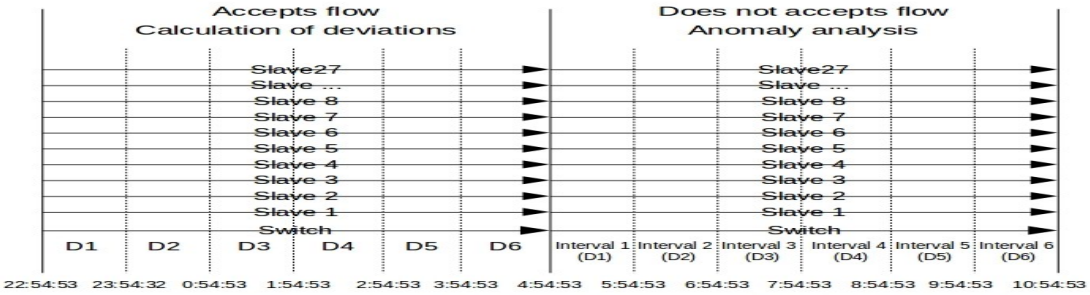

Figura 2: Cálculos dos desvios e monitoramento.

4 Resultados

Após os testes, foram obtidos os resultados das análises realizadas pelo controlador nos intervalos 1, 2, 3, 4, 5 e 6, monitorados no período entre as 4:54:53 e as 10:54:53. Os dados apresentam o comportamento do fluxo total no OVS entre o mestre e os 27 escravos, monitorando possíveis anomalias em cada intervalo, usando os respectivos valores de mínimo e máximo de pacotes e *bytes*, definidos a partir dos desvios calculados, pelo dobro e triplo, tanto para mais como para menos. Os resultados do monitoramento de *bytes* e pacotes podem ser vistos na Tabela 1.

Tabela 1: Monitoramento de *bytes* e pacotes.

Anomalias detectadas pelo OVS												
Intervalos	*Bytes*						Pacotes					
	Dobro do desvio			Triplo do desvio			Dobro do desvio			Triplo do desvio		
	Min.	Max.	Falso positivo	Min.	Max.	Falso positivo	Min.	Max.	Falso positivo	Min.	Max.	Falso positivo
1	190434	216517	0	183913	223037	0	2341	2660	0	2260	2740	0
2	202911	205448	0	202276	206083	0	2494	2524	0	2486	2532	0
3	203882	204790	13	203655	205017	7	2505	2517	13	2501	2521	6
4	203254	205203	2	202767	205690	1	2497	2522	2	2491	2528	1
5	203247	205265	7	202743	205770	6	2498	2522	7	2491	2529	6
6	203395	205024	4	202987	205432	2	2499	2519	6	2494	2525	3

Como podemos observar na Tabela I, apenas nos intervalos 1 e 2 não ocorreram anomalias, já nos demais, foram detectados anomalias. No intervalo 6, tanto para o dobro, como para o triplo do desvio, o número de falsos positivos detectados foram diferentes para *bytes* e pacotes, isso ocorreu pelo fato do controlador analisar anomalias tanto pela quantidade de pacotes como pela quantidade de *bytes*, de forma independente.

Contudo, foram gerados os gráficos apresentados nas Figuras 3 e 4 dos 6 intervalos, apenas para os pacotes, já que o comportamento do fluxo de *bytes* é muito semelhante ao fluxo de pacotes. Assim, pode-se verificar o comportamento do fluxo em todo período de monitoramento e o momento que ocorreram as anomalias. Os gráficos apresentam o número mínimo e máximo de pacotes com o dobro e o triplo do desvio. Os resultados são mostrados nas próximas figuras:

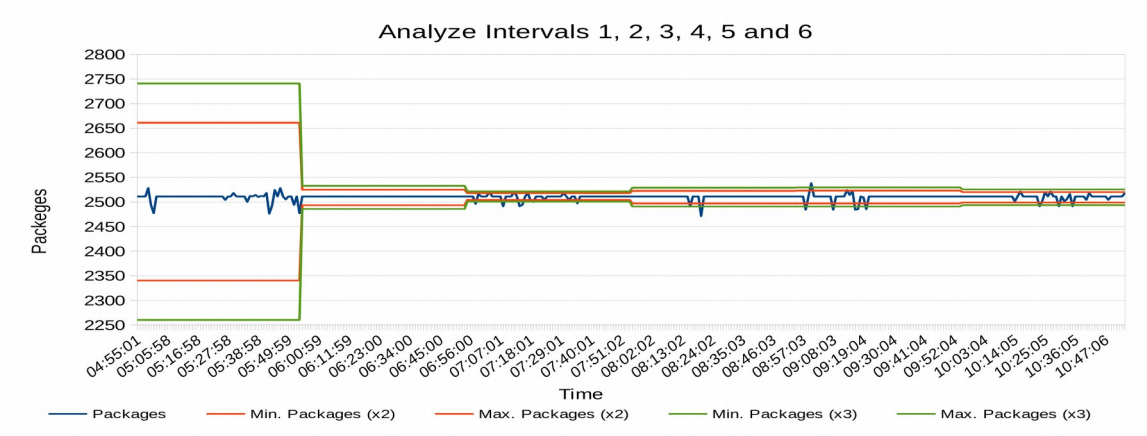

Figura 3: Monitoramento de pacotes nos 6 intervalos.

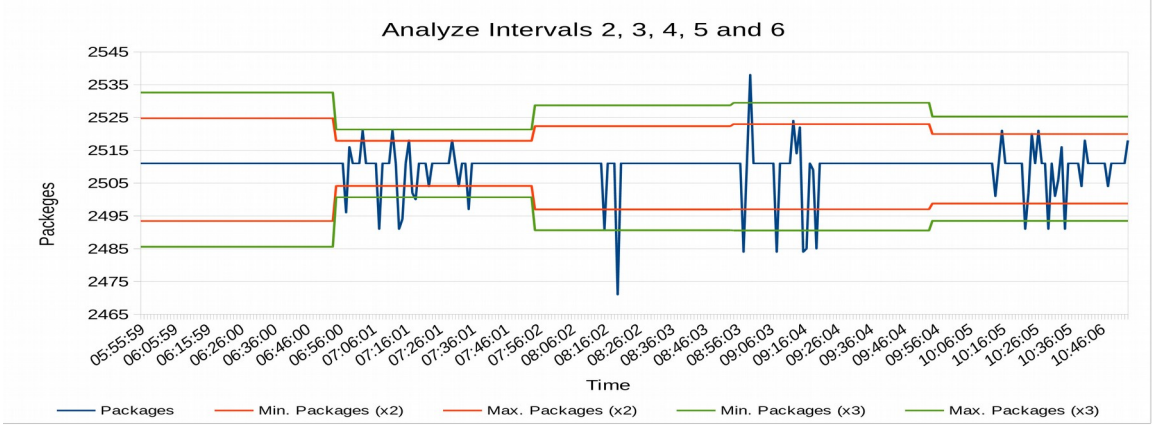

Figura 4: Monitoramento de pacotes nos intervalos 2, 3, 4, 5 e 6.

A Figuras 3 apresenta o comportamento do fluxo no decorrer do tempo, mostrando que no primeiro intervalo os desvios foram maiores que nos demais intervalos. Isso aconteceu em consequência ao maior número de pacotes *Openflow* entre o controlador e o OVS e pacotes TCP de inicialização de conexão, quando as máquinas iniciaram as comunicações, com o propósito de definir as novas regras na tabela de fluxo do OVS e estabelecer as conexões entre os escravos e o

mestre. Desta forma, nenhum falso positivo foi detectado no primeiro intervalo. A partir do segundo intervalo os valores dos desvios são parecidos.

Também podemos observar, que as diferenças entre os mínimos e os máximos dos desvios foram pequenas, isso por causa da comunicação regular entre o mestre e os escravos. Por esse motivo foram detectados os falsos positivos, mesmo com pequenas oscilações do fluxo, como pode ser visto na Figura 4, que apresenta o fluxo nos intervalos 2, 3, 4, 5 e 6.

Por fim, a Figura 5 apresenta o comportamento da função densidade de probabilidade do tempo total de treinamento da rede, ou seja, das 22:54:53 às 4:54:53 horas. A Figura 5 apresenta uma distribuição gaussiana com média de 2510 pacotes e desvio padrão de 6 pacotes. Observe que o gráfico relacionado ao resultado dos pacotes (Figura 3 e Figura 4) apresentam uma média de pacotes próximas da distribuição gaussiana da Figura 5, indicando que a maior parte dos pacotes são das classes de prioridade empregadas no teste e poucos considerados maliciosos.

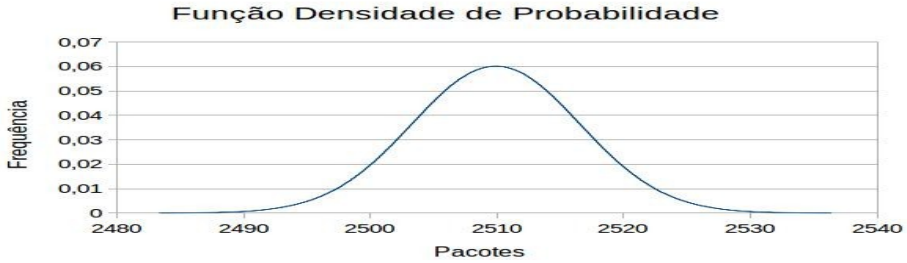

Figura 5: Distribuição de pacotes.

5 Conclusões

Através dos testes realizados foi possível avaliar o comportamento do fluxo em um OVS, onde o controlador POX pôde calcular um desvio padrão para cada intervalo de tempo analisado. Assim, conseguiu monitorar o fluxo com seus respectivos desvios, identificando anomalias quando a quantidade de pacotes e *bytes* eram menores ou maiores que os limites definidos.

Desta forma, obtém-se resultados que apresentaram diferentes características em cada intervalo (mesmo não havendo uma alteração proposital no ambiente), como no primeiro intervalo, com uma maior diferença entre o mínimo e máximo em relação aos demais desvios, devido ao maior número de mensagens para a definição das comunicações entre mestre e escravo.

Os resultados mostram que o controlador deve ser configurado para ser mais ou menos sensível, dependendo do nível de segurança desejado.

Sabendo da importância em preservar a segurança em redes *Smart Grid*, o controlador POX modificado apresenta uma alternativa para complementar a integridade da rede, sendo capaz de monitorar não apenas o fluxo total do *switch*, mas de cada fluxo individualmente, além da arquitetura possuir um sensor para identificação de intrusos na rede, porém não tendo sido o foco nesse trabalho .

Os próximos passos serão para monitorar um número maior de escravos, com o objetivo de analisar o comportamento de fluxo em vários *switches* simultaneamente e nos escravos individualmente. Assim, podemos identificar o limite mínimo e máximo do desvio, definindo limites mais adequados para determinados tamanhos e comportamentos de redes *Smart Grid*.

Desta forma, podemos concluir que um monitoramento detalhado no fluxo total do OVS é necessário, pois não foi encontrada uma arquitetura projetada com tal flexibilidade, sabendo que falsas anomalias podem dificultar no gerenciamento de um sistema de segurança, não identificando ataques reais e podendo causar danos no sistema.

Referências

[1] A. Cahn; Hoyos, J.; Hulse, M.; Keller, E. Software-defined energy communication networks: From substation automation to future Smart Grids. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (Smart GridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 558–563.

[2] Disponível em: http://openvswitch.org/. Acesso em: 10 maio 2017.

[3] Disponível em: https://github.com/gec/dnp3/. Acessado em: 5 julho 2017.

[4] Disponível em: https://github.com/noxrepo/pox. Acesso em: 10 maio 2017.

[5] Disponível em: https://portal.geni.net/. Acessado em: 5 julho 2017.

[6] Disponível em: https://www.dnp.org/Pages/AboutFeatures.aspx. Acessado em: 6 de julho 2017.

[7] E. Molina; Jacob, E.; Matias, J.; Moreira, N.; Astarloa, A. Using software defined networking to manage and control IEC 61850-based systems. Comput. Electr. Eng. 2015, 43, 142–154.

[8] J. Kim; Filali, F.; Ko, Y.-B. Trends and Potentials of the Smart Grid Infrastructure: From ICT Sub-System to SDN-Enabled Smart Grid Architecture. *Appl. Sci.* **2015**, *5*, 706-727.

[9] J. Zhang, B. C. Seet, T. T. Lie, C. H. Foh. Opportunities for software-defined networking in Smart Grid. In Proceedings of the 2013 9th International Conference on Information, Communications and Signal Processing (ICICS), Tainan, Tanwan, 10–13 December 2013; pp. 1–5.

[10] X. Dong, H. L., R. Tan, R. K. Iyer, Z. Kalbarczyk. Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. In Proceedings of The 1st Cyber-Physical System Security Workshop (CPSS), April 14 -17, 2015, Singapore.

[11] X. Dong; Lin, H.; Tan, R.; Iyer, R.K.; Kalbarczyk, Z. Software-defined networking for Smart Grid resilience: Opportunities and challenges. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Singapore, 14–17 April 2015; ACM: New York, NY, USA; pp. 61–68.

[12] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, N. Venkatasubramanian. A Software Defined Networking Architecture for the Internet-of-Things, 2014 IEEE network operations and management symposium (NOMS), 1-9.