Segurança em Redes Definidas por *Software*: Autenticação, Controle de Acesso e Consistência com Plano de Controle Eficientemente Distribuído

Diogo M. F. Mattos[1], **Otto Carlos M. B. Duarte**[1] **e Guy Pujolle**[2]

[1]Grupo de Teleinformática e Automação
Universidade Federal do Rio de Janeiro (UFRJ) – Brasil

[2]Laboratoire d'Informatique de Paris 6
Sorbonne Universities, UPMC Univ Paris 06 – França

{diogo,otto}@gta.ufrj.br, Guy.Pujolle@lip6.fr

Resumo. *A distribuição do controle em Redes Definidas por Software melhora a segurança, o desempenho e a escalabilidade da rede ao custo de novos desafios para a consistência da visão global da rede. Este trabalho apresenta as principais ameaças de segurança às redes definidas por software, propõe um mecanismo de autenticação e controle de acesso de estações finais baseado na credencial da estação, propõe uma arquitetura eficiente de distribuição de controladores e esquemas consistentes para a atualização de políticas em redes com controle centralizado ou distribuído. A avaliação das propostas é realizada através de protótipos, modelos formais e simulações. Os resultados demonstram que a proposta de controlador distribuído é eficiente na instalação e localização das instâncias dos controladores. As simulações dos esquemas de atualização de políticas mostram que o desempenho das propostas são superiores aos literatura nos cenários tanto com controle centralizado como distribuído.*

Abstract. *Control distribution in Software Defined Networking improves network performance and scalability, but incurs new challenges for the consistence of the global view of the network. In this work, we present the main security threats against the software defined networking, we propose an authentication mechanism and access control based on host credentials, we propose an efficient architecture for control distribution, and we also propose two schemes for policy updating on networks with centralized or distributed control. The proposals are evaluated through prototypes, formal models and simulations. The results demonstrate that the distributed controller proposal is efficient in the installation and location of the controller instances. The simulations of the proposed policy-update schemes show that the achieved performance is higher than other previous proposals both in centralized or distributed control scenarios.*

1. Introdução

O paradigma de Redes Definidas por *Software* (*Software Defined Networks* – SDN) desacopla o controle do encaminhamento de dados, oferecendo alta programabilidade e uma visão global da rede. Essa tecnologia permite desenvolver,

Este trabalho foi realizado com recursos da CNPq, CAPES, FINEP, FUNTTEL e FAPERJ.

de forma logicamente centralizada, políticas integradas de segurança [Levin et al. 2012] e, assim, facilitar a solução de problemas complexos de segurança em rede. O controlador de rede SDN, implementando em *software*, executa as funções do plano de controle. O plano de encaminhamento é executado por comutadores de alto desempenho.Contudo, esse novo paradigma apresenta algumas limitações quanto à segurança da rede, pois um componente com comportamento malicioso pode comprometer o funcionamento de toda a rede, realizando, por exemplo, um ataque de negação de serviço no controlador. Dessa forma, a distribuição do controle da rede e o controle de acesso são necessários para garantir maior segurança. A autenticação das estações, o nível de privilégio atribuído a cada estação e a coordenação da aplicação de políticas são essenciais para garantir a segurança da rede definida por *software*.

1.1. Caracterização do Problema e Motivação

A distribuição do controle e a replicação de controladores são as principais técnicas para aumentar a resiliência das Redes Definidas por *Software*. No entanto, a adoção de controladores que agem como um sistema distribuído ou a simples replicação de controladores não é suficiente para garantir a segurança, o desempenho e a escalabilidade, pois dependem ainda do mapeamento otimizado entre comutadores e controladores, criando domínios de controle [Mattos et al. 2016c]. Outro desafio que desponta da distribuição do controle é manutenção da consistência da visão global unificada [Levin et al. 2012, Schmid e Suomela 2013]. A visão global inconsistente acarreta em perda de desempenho e erros na execução de aplicações de controle da rede [Schmid e Suomela 2013].

A mudança da configuração de uma Rede Definida por Software pode levar a instabilidades da rede, como a interrupção do funcionamento, a degradação do desempenho e, até mesmo, a estados vulneráveis de segurança [Reitblatt et al. 2012]. O desafio de manter a consistência das políticas durante as atualizações é presente mesmo quando os estados iniciais e finais da configuração da rede são consistentes e corretos, pois não há garantias que os estados intermediários, que ocorrem durante o processo de atualização, sejam consistentes. No cenário de SDN, a transição entre configurações da rede deve ocorrer em uma sequência de instalações e desinstalações de regras, comutador a comutador, que garanta que a rede apresente o comportamento esperado, mesmo durante o transiente de ocorrência da atualização. A hipótese de que cada aplicação em uma SDN deva ser responsável pelo seu próprio processo de atualização de políticas não é suficiente, pois as aplicações de controle da rede estão comumente sujeitas a erros quando tratam das atualizações de políticas [Perešíni et al. 2013].

1.2. Objetivos e Contribuições

O objetivo deste trabalho é prover soluções de segurança para as Redes Definidas por Software. A segurança da rede é definida em relação a três desafios fundamentais em redes definidas por *software*: vulnerabilidade a ataques de negação de serviço, ausência de confiança entre componentes e a vulnerabilidade de componentes. Assim, é necessário que o controle das redes definidas por software seja fisicamente distribuído em diferentes instâncias de controladores, enquanto também apresente uma interface única e consistente de controle logicamente centralizado. A consistência em SDN é composta por duas vertentes principais: a consistência de tratamento do fluxo durante a sua existência e a

consistência das políticas de encaminhamento ou tratamento de fluxos entre controladores. O trabalho formaliza o problema de consistência em SDN com base na literatura existente e propõe um mecanismo de autenticação e controle de acesso para SDN, assim como também propõe um controlador distribuído com consistência forte de políticas entre controladores. A ideia central é usar o teorema do CAP (Consistência, Disponibilidade e Tolerância a Partições) para balizar a proposta do controlador distribuído e garantir consistência local e disponibilidade, mesmo em cenários em que haja partições da rede.

Mecanismo de Autenticação e Controle de Acesso. O trabalho apresenta a proposta e o desenvolvimento do mecanismo de autenticação e controle de acesso para redes definidas por *software*, o AuthFlow. O mecanismo AuthFlow apresenta duas contribuições principais: (i) a autenticação das estações finais diretamente na camada de enlace e (ii) a associação das credenciais de acesso de uma estação aos fluxos pertencentes a essa estação. A autenticação da estação final na camada de enlace é realizada através do padrão IEEE 801.X que garante que as informações de autenticação sejam trocadas de forma padronizada entre a estação e o autenticador e, portanto, não requer qualquer alteração nas estações finais. O mecanismo de autenticação encapsula as mensagens no formato *Extensible Authentication Protocol* (EAP), o que permite a adoção de diferentes métodos de autenticação. A autenticação do mecanismo AuthFlow, direto na camada de enlace, tem a vantagem de prover uma baixa sobrecarga de controle quando comparada a uma autenticação na camada rede, ou na camada de aplicação, que dependem da atribuição de um IP à estação que está se autenticando e dependem da troca de informações da aplicação para a autenticação.

Distribuição do Controle e Resiliência. O trabalho modela o desempenho de um controlador para Rede Definida por *Software*, baseado na teoria de filas, e propõe uma arquitetura eficiente para a distribuição do controle. Para tanto, o trabalho aborda a distribuição do controle sob a ótica das duas vertentes. Primeiro, desenvolve-se um controlador distribuído para SDN. A proposta consiste em criar zonas de controle independentes com um controlador responsável. Os controladores das zonas se reportam a um controlador designado responsável por manter a consistência da visão global conhecida pelos controladores. Na arquitetura proposta, todos os controladores exercem o controle plano da rede, isto é, não há uma hierarquia em que controladores locais se reportem a controladores globais. O controle plano depende somente da propagação das informações de atualização da visão global através dos controladores. Na arquitetura proposta, adota-se a ideia de um controlador designado que recebe as atualizações e repassa aos demais, reduzindo a sobrecarga de propagação de informações.

Atualização de Políticas Consistente. O tratamento consistente dos fluxos em uma rede definida por *software* requer que os pacotes de um fluxo sempre sejam processados pela visão global mais recente da rede. Para tanto, ao se fazer uma atualização nas políticas de encaminhamento e tratamento de pacotes na rede, essas atualizações devem ser orquestradas de forma a garantir que nenhum pacote possa ser processado por configurações mais antigas da rede, mesmo que durante um curto transiente de instalação das novas políticas. Os estados intermediários de transição entre configurações da rede podem causar laços, perda de conectividade, vulnerabilidades ou, até mesmo, parada no funcionamento da rede. Este trabalho propõe a Atualização Reversa, um esquema de atualização de políticas de processamento, encaminhamento e segurança em Redes Definidas por Software. A

ideia central do esquema proposto se baseia no relaxamento do conceito de consistência por pacote para executar a atualização das políticas no caminho inverso do fluxo na rede. Em um cenário com o controle distribuído da rede, o desafio de se garantir a consistência no tratamento dos fluxos é ainda maior, pois atualizações das políticas que definem a visão global da rede podem ser emitidas concomitantemente por diferentes controladores. Assim, antes de se instalar uma nova política na rede, há a necessidade de se definir uma ordem entre as políticas que chegam aos controladores, garantir que haja um acordo entre os controladores sobre quais políticas devem ser instaladas e, só então, proceder a instalação consistente da política na rede. Este trabalho propõe, então, um protocolo simples e eficiente para a serialização da instalação de atualizações de políticas em Rede Definidas por Software com um plano de controle distribuído. A ideia principal é garantir o consenso entre os controladores quanto à aplicação de uma nova política sobre a rede. Quando atualizações de política chegam concomitantemente a diferentes controladores, esses devem concordar sobre a ordem de instalação de todas as atualizações requisitadas e, também, se a nova política gera conflito com as demais.

2. Trabalhos Relacionados

A noção de um plano de controle logicamente centralizado é parte essencial do paradigma de Redes Definidas por *Software* [Levin et al. 2012]. Contudo, a realização do controle através de nós controladores com implementação centralizada não provê os níveis requeridos de disponibilidade, tempo de resposta e escalabilidade [Canini et al. 2013]. Dessa forma, um importante desafio em SDN é como realizar a distribuição do controle da rede, atendendo as relações de compromisso entre robustez, modelos de consistência, disponibilidade e desempenho.

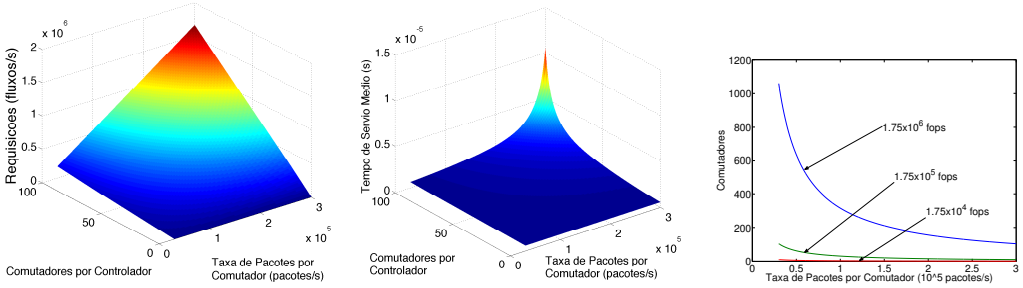
A distribuição do controle e a localização de controladores também são abordadas por outras propostas. Müller *et al.* propõem uma estratégia de localização de controladores, chamada *Survivor*, que considera a diversidade de caminhos desconexos entre si para o controlador, os recursos dos controladores e os mecanismos de recuperação de desastres [Muller et al. 2014]. Bari *et al.* também propõem um esquema de otimização de localização de controladores de acordo com a carga da rede [Bari et al. 2013]. Por sua vez, Ros e Ruiz propõem a formulação do problema de Localização de Controladores Tolerantes a Falhas (*Fault Tolerant Controller Placement* - FTCP) [Ros e Ruiz 2016].

As principais propostas para a atualização de políticas em SDN baseiam-se nas ideias de atualização atômica [Perešíni et al. 2013] ou atualização em duas fases [Reitblatt et al. 2012, Canini et al. 2013]. A atualização atômica considera que todos os nós da rede são atualizados simultaneamente em uma operação atômica. No entanto, a operação de atualização dos comutadores em uma rede SDN não pode ser realizada de forma atômica e, consequentemente, os pacotes em trânsito, que estão atravessando a rede no momento da implantação da atualização, podem ser processados por configurações da rede anteriores ou posteriores à atualização, sem garantias de consistência para estes pacotes em trânsito. Para assegurar a consistência foi proposta a Atualização de Duas Fases, que se baseia na marcação de uma etiqueta de versão da configuração nos pacotes e, consequentemente, no processamento dos pacotes segundo a versão que carregam. Assim, esse esquema de atualização consistente depende de um sistema de identificação de configurações no qual as regras da nova configuração sejam designadas com número de versão diferente das anteriores e, portanto, dependem da instalação das novas regras

nos comutadores. Além disso, os comutadores passam a ter diferentes regras nas tabelas para o mesmo fluxo, que diferem pela versão, o que pode gerar uma grande sobrecarga nas tabelas de fluxos em função da implantação de regras mais elaboradas com campos coringas [Luo et al. 2015, Fogel et al. 2015]. Já a proposta deste artigo reduz a sobrecarga, quando comparada à Atualização de Duas Fases, e provê garantias de consistência, quando comparara à atualização atômica.

3. Resultados Obtidos

A implantação do plano de controle de uma Rede Definida por *Software* deve considerar quantos controladores são necessários para manter a disponibilidade, o baixo tempo de resposta e a robustez do plano de controle [Heller et al. 2012]. Nesse sentido, uma proposta desse trabalho é um modelo para o controlador SDN em que modela-se o tempo de tratamento de cada pacote em função do número de comutadores que um determinado controlador é responsável. O modelo proposto é simples e baseado em teoria de filas. Assim, assume-se que o tráfego que chega a cada comutador da rede segue uma distribuição de Poisson para a frequência de chegada de novos pacotes e a taxa de tratamento de eventos em um controlador segue uma distribuição exponencial.



(a) Carga agregada de requisições no controlador.

(b) Tempo médio de serviço para cada requisição no controlador.

(c) Comutadores por controlador para o sistema em equilíbrio.

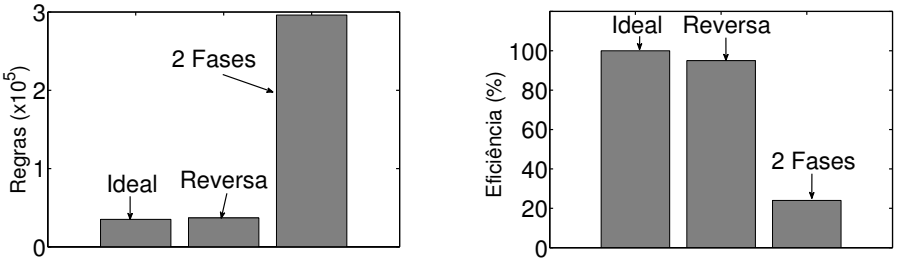
Figura 1. Aplicação do modelo de controlador SDN em uma rede com um controlador com taxa de serviço $\mu_c = 1.75 * 10^6$ `fops`, número de comutadores variando de 1 a 100 e taxa de chegada de pacotes por comutador de até 0.3 `Mpps`.

A Figura 1 mostra a aplicação do modelo proposto em uma rede com até 100 comutadores sendo controlada por um nó controlador. A aplicação do modelo considera um controlador de alto desempenho, com capacidade de responder até $1.75 * 10^6$ eventos por segundo [Azodolmolky et al. 2013]. A taxa de chegada de fluxos por comutador varia de 0,03 a 0,3 milhões de pacotes por segundo, de acordo com os resultados de desempenho máximo de comutadores [Rotsos et al. 2012]. A probabilidade de um pacote ser encaminhado para o controlador foi estimada no inverso do número de pacotes por fluxo. A estimativa foi realizada com base nos dados reportados pela CAIDA (*Center for Applied Internet Data Analysis*) para o ponto de medidas passivas `chicago (dirA)` no período do ano de 2014 [1]. Com base nesses dados, definiu-se a probabilidade $p = 0,0276$. Da mesma forma, os dados validam as taxas de chegada de pacote por comutador na medida em que a taxa de chegada de pacotes média em `chicago (dirA)`, para o período

[1] Dados disponíveis em http://www.caida.org/data/passive/trace_stats/.

avaliado, é 0,374 milhões de pacotes por segundo. A Figura 1(a) mostra que a carga do controlador, com 100 comutadores e cada um gerando tráfego de 300 mil pacotes por segundo, é próxima do limite suportado pelo controlador. O limite de 100 comutadores é evidenciado pela Figura 1(c), na qual valores acima da curva tendem s tirar o sistema da situação de equilíbrio.

Outros resultados obtidos concentram-se na avaliação da proposta da Atualização Reversa para a atualização de políticas em redes com controle centralizado. O relaxamento da consistência por pacote proposto na tese prevê que basta garantir que o pacote, após ser encaminhado por uma configuração global mais atual, não volte a ser encaminhado por uma configuração anterior. Assim, a simulação da proposta de Atualização Reversa mostra que há um percentual de pacotes afetados pela atualização muito próxima de uma atualização ideal. Mostra-se também que o esquema proposto apresenta o mesmo número de fluxos atualizados na rede que a atualização ideal. Quando comparado ao esquema de atualização proposto na literatura, atualização de duas fases, o número de fluxos que são tratados pela configuração mais atual é menor que do esquema proposto.

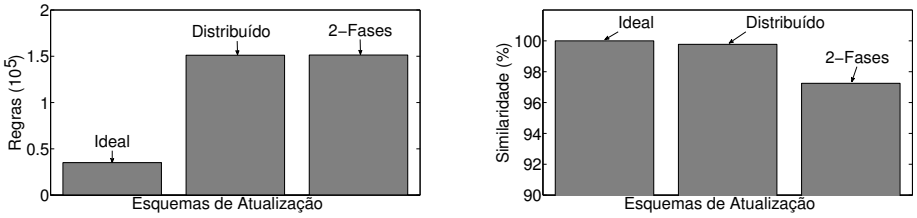


(a) Número de Regras na rede após a simulação.

(b) Similaridadeem relação ao Ideal.

Figura 2. A Atualização Reversa introduz menor sobrecarga de regras geradas que a Atualização de Duas Fases. A Atualização Reversa apresenta maior similaridade em relação ao ideal que a Atualização de Duas Fases.

A Figura 2(a) compara o número de regras instaladas por cada esquema durante toda a execução da simulação. É possível perceber que o número de regras instaladas pela Atualização de Duas Fases é muito superior ao dos outros esquemas de atualização. Isso ocorre devido à adição de novas regras nas portas do núcleo da rede, enquanto a Atualização Reversa apenas atualiza as regras já existentes, assim como a Atualização Ideal. Avaliou-se a similaridade de cada esquema de atualização em relação ao ideal. A similaridade é o percentual de pacotes encaminhados pelos esquemas de atualização que estão em correspondência àqueles encaminhados pela atualização ideal, durante a ocorrência de atualizações. Nesse sentido, verifica-se que a Atualização Reversa alcança uma similaridade de 94%, enquanto a Atualização de Duas Fases apresenta similaridade de 24%, mostrado na Figura 2(b). No cenário de controle distribuído, o trabalho propõe um esquema de atualização coordenado entre os controladores através de algoritmo de consistência [Mattos et al. 2017]. A atualização por controladores distribuídos age mais prontamente na rede do que a atualização de duas fases com controle centralizado, apresentando um resultado mais próximo ao ideal. O esquema distribuído atualiza 42% mais de fluxos do que o centralizado de atualização de duas fases.



(a) Número de regras instaladas na rede. (b) Similaridade com o ideal.

Figura 3. Comparação do número de regras e do efeito no destino causado pelo uso dos esquemas de atualização. a) Número total de regras instaladas na rede. b) A similaridade das propostas em relação ao esquema ideal.

O número total de regras instaladas nos comutadores da rede com controle distribuído é evidenciado na Figura 3(a). Como os esquemas de atualização distribuído e de atualização de duas fases centralizado instalam regras no núcleo da rede para garantir a consistência por pacote, o número de regras instalado por esses esquemas chega a ser 4x superior ao do ideal[2]. Por sua vez, a Figura 3(b) compara o resultado do encaminhamento no destino dos pacotes. A similaridade mede o quão próximo o encaminhamento dos pacotes em cada esquema de atualização está do ideal. Essa medida fornece uma estimativa da qualidade de cada esquema de atualização. Verifica-se que o esquema de duas fases já apresenta um desempenho muito próximo do ideal. Contudo, a proposta do esquema distribuído alcança um resultado ainda mais próximo do ideal devido à coordenação eficiente de ações entre os controladores com o uso do protocolo de consistência proposto.

4. Considerações Finais

As propostas discutidas nessa tese apresentam contribuição na área de Segurança em Redes Definidas por *Software*. O trabalho apresentou os principais vetores de ameaça e discutiu a segurança e a distribuição de controle em SDN e trabalho propôs o AuthFlow [Mattos e Duarte 2014, Mattos e Duarte 2016], um mecanismo de autenticação e controle de acesso para Redes Definidas por Software que permite a definição de fluxos baseada na identidade de um usuário. Como a realização do controlador de rede como um servidor centralizado implica desafios para a segurança, o desempenho e a escalabilidade da rede, esse trabalho propôs um controlador de rede distribuído [Mattos et al. 2016b, Mattos et al. 2015, Mattos et al. 2016a]. O trabalho apresentou a modelagem de Redes Definidas por Software. Esse trabalho, por sua vez, propôs um novo esquema de atualização de políticas em Redes Definidas por *Software* com controle centralizado, que se prova ser consistente e não depende de marcação de pacotes, mas da ordem como as atualizações são realizadas na rede [Mattos e Duarte 2015, Mattos et al. 2016c]. O trabalho propôs um protocolo de consistência para controladores distribuídos, em que o conflito entre políticas é verificado localmente e a ordem global de instalação é garantida pela coordenação entre controladores [Mattos et al. 2017]. A tese obteve como resultado direto a publicação de quatro artigos em congressos nacionais, dois artigos em congressos internacionais, duas revistas indexadas internacionais e, ainda, a submissão em andamento de duas revistas internacionais.

[2]Há fluxos não expiraram na tabela de fluxos dos comutadores e são afetados por mais de uma atualização, gerando um aumento ainda maior no número de regras instaladas do que a instalação de uma regra a mais por fluxo em cada comutador.

5. Referências

[Azodolmolky et al. 2013] Azodolmolky, S., Nejabati, R., Pazouki, M., Wieder, P., Yahyapour, R. e Simeonidou, D. (2013). An analytical model for software defined networking: A network calculus-based approach. Em *2013 IEEE Global Communications Conference (GLOBECOM)*, páginas 1397–1402.

[Bari et al. 2013] Bari, M., Roy, A., Chowdhury, S., Zhang, Q., Zhani, M., Ahmed, R. e Boutaba, R. (2013). Dynamic controller provisioning in software defined networks. Em *9th International Conference on Network and Service Management (CNSM), 2013*, páginas 18–25.

[Canini et al. 2013] Canini, M., Kuznetsov, P., Levin, D., Schmid, S. et al. (2013). The case for reliable software transactional networking. Relatório Técnico CKLS-CRSTN-13, Internet Network Architectures - Department of Telecommunication Systems - Technische Universität Berlin.

[Fogel et al. 2015] Fogel, A., Fung, S., Pedrosa, L., Walraed-Sullivan, M., Govindan, R., Mahajan, R. e Millstein, T. (2015). A general approach to network configuration analysis. Em *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI'15)*, Berkeley, CA, USA. USENIX Association.

[Heller et al. 2012] Heller, B., Sherwood, R. e McKeown, N. (2012). The controller placement problem. Em *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, HotSDN'12, páginas 7–12, New York, NY, USA. ACM.

[Levin et al. 2012] Levin, D., Wundsam, A., Heller, B., Handigol, N. e Feldmann, A. (2012). Logically centralized?: state distribution trade-offs in software defined networks. Em *Proceedings of the First workshop on Hot topics in software defined networks*, HotSDN'12, Helsinki, Finland. ACM.

[Luo et al. 2015] Luo, S., Yu, H. e Li, L. (2015). Consistency is not easy: How to use two-phase update for wildcard rules? *Communications Letters, IEEE*, 19(3):347–350.

[Mattos et al. 2017] Mattos, D., Duarte, O. C. M. B. e Pujolle, G. (2017). Um protocolo simples e eficiente para atualização consistente de políticas em redes definidas por software com controle distribuído. Em *XXXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC'2017*.

[Mattos et al. 2015] Mattos, D. M. F., Andreoni Lopez, M., Ferraz, L. H. G. e Duarte, O. C. M. B. (2015). Controlador resiliente com distribuição eficiente para redes definidas por software. Em *XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC'2015*.

[Mattos e Duarte 2014] Mattos, D. M. F. e Duarte, O. C. M. B. (2014). AuthFlow: Um mecanismo de autenticação e controle de acesso para redes definidas por software. Em *XXXII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC'2014*.

[Mattos e Duarte 2015] Mattos, D. M. F. e Duarte, O. C. M. B. (2015). Atualização reversa: Garantindo consistência de estados em redes definidas por software. Em *SBSeg 2015 - XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, Florianópolis, SC - Brasil.

[Mattos e Duarte 2016] Mattos, D. M. F. e Duarte, O. C. M. B. (2016). AuthFlow: authentication and access control mechanism for software defined networking. *Annals of Telecommunications*, 71(11):607–615.

[Mattos et al. 2016a] Mattos, D. M. F., Duarte, O. C. M. B. e Pujolle, G. (2016a). Profiling software defined networks for dynamic distributed-controller provisioning. Em *2016 7th International Conference on the Network of the Future (NOF)*, páginas 1–4.

[Mattos et al. 2016b] Mattos, D. M. F., Duarte, O. C. M. B. e Pujolle, G. (2016b). A resilient distributed controller for software defined networking. Em *IEEE ICC 2016 - Next Generation Networking and Internet Symposium (ICC'16 - NGN)*, Kuala Lumpur, Malaysia.

[Mattos et al. 2016c] Mattos, D. M. F., Duarte, O. C. M. B. e Pujolle, G. (2016c). Reverse update: A consistent policy update scheme for software-defined networking. *IEEE Communications Letters*, 20(5):886–889.

[Muller et al. 2014] Muller, L. F., Oliveira, R. R., Luizelli, M. C., Gaspary, L. P. e Barcellos, M. P. (2014). Survivor: an enhanced controller placement strategy for improving sdn survivability. Em *Global Communications Conference (GLOBECOM), 2014 IEEE*, Austin, Texas, USA.

[Perešíni et al. 2013] Perešíni, P., Kuzniar, M., Vasić, N., Canini, M. e Kostiū, D. (2013). Of.cpp: Consistent packet processing for openflow. Em *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN'13, páginas 97–102, New York, NY, USA. ACM.

[Reitblatt et al. 2012] Reitblatt, M., Foster, N., Rexford, J., Schlesinger, C. e Walker, D. (2012). Abstractions for network update. Em *Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM'12, páginas 323–334, New York, NY, USA. ACM.

[Ros e Ruiz 2016] Ros, F. J. e Ruiz, P. M. (2016). On reliable controller placements in software-defined networks. *Computer Communications*, 77:41 – 51.

[Rotsos et al. 2012] Rotsos, C., Sarrar, N., Uhlig, S., Sherwood, R. e Moore, A. (2012). Oflops: An open framework for openflow switch evaluation. Em Taft, N. e Ricciato, F., editors, *Passive and Active Measurement*, volume 7192 of *Lecture Notes in Computer Science*, páginas 85–95. Springer Berlin Heidelberg.

[Schmid e Suomela 2013] Schmid, S. e Suomela, J. (2013). Exploiting locality in distributed sdn control. Em *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN'13, páginas 121–126, New York, NY, USA. ACM.