Mobility-Flow: Solução para Handover Transparente e com Suporte à Autenticação 802.1x em Redes OpenFlow

Edivaldo C. de A. Junior, Edson A. M. Avelar, Kelvin L. Dias, Paulo R. F. Cunha

Centro de Informática – Universidade Federal de Pernambuco (UFPE)
CEP: 50740-540 – Recife – PE – Brasil

{ecaj,eama,kld,prfc}@cin.ufpe.br

Abstract. *User authentication is an essential element to ensure adequate levels of security in accessing the strategic corporate services. However, this procedure can lead to the degradation of the quality perceived by the user upon handover executions between access points since reauthentication is required. Despite that numerous mobility management strategies exist in the literature, user authentication is neglected and it is not taken into account as part of the solution design. This article proposes an OpenFlow-based mobility management solution for Wi-Fi networks, considering 802.1x authentication. The results from testbed experiments show the benefits of the proposed solution to best effort and video traffics.*

Resumo. *Autenticação do usuário é um elemento primordial para garantir níveis adequados de segurança no acesso aos serviços corporativos estratégicos. Contudo, este procedimento pode acarretar degradação da qualidade percebida pelo usuário quando das execuções de handover entre pontos de acesso, uma vez que a reautenticação é requerida. Apesar de inúmeras soluções presentes na literatura para o gerenciamento de mobilidade, a autenticação do usuário é negligenciada. Este artigo propõe uma solução de gerenciamento mobilidade baseada no OpenFlow para redes Wi-Fi, considerando autenticação 802.1x. Os resultados mostram os benefícios da solução proposta para tráfego de melhor esforço e de vídeo.*

1. Introdução

Com a crescente utilização de tecnologias de redes sem fio e o aumento no acesso à Internet vias *smartphones*, *tablets* e *notebooks* em qualquer lugar e a qualquer momento, bem como a convergência de várias tecnologias para redes IP, cada vez mais, o usuário faz uso de dispositivos móveis para dispor de serviços e aplicações em seu dia-a-dia.

A ampliação dos pontos de acesso de rede sem fio gera novas questões e desafios quanto ao gerenciamento eficiente e centralizado, bem como ao provimento de vários requisitos atuais, tais como: continuidade do serviço enquanto o usuário se desloca entre pontos de acesso, procedimento denominado de *handover*, e também aspectos de Qualidade de Serviço/Experiência (QoS – *Quality of Service*/QoE – *Quality of Experience*), aliado à necessidade do cumprimento de requisitos de segurança, como

a autenticação do usuário, um elemento primordial para garantir níveis adequados de segurança no acesso aos serviços estratégicos da organização. Apesar das inúmeras soluções existentes na literatura para o gerenciamento de mobilidade e *handover* (Ferretti, et al., 2016), o suporte à autenticação do usuário é um aspecto negligenciado nesses cenários, fazendo com que requisitos de QoS e QoE não possam ser garantidos devido aos atrasos inerentes ao processo de reautenticação quando o dispositivo migra para um novo ponto de acesso ou rede.

Com o advento do paradigma SDN (*Software-Defined Networking*) e com penetração cada vez maior no mercado de equipamentos com a tecnologia OpenFlow(OF), tornou-se possível prover soluções inovadoras. SDN baseia-se no princípio da separação entre os planos de controle e dados e esse controle é totalmente programável (McKeown et al., 2008). Nesta arquitetura temos a vantagem da simplificação dos ativos de rede, pois o plano de controle deste é transferido para o controlador SDN, no qual são executadas as aplicações que podem atribuir aos ativos, funcionalidades de roteadores e/ou protocolos diversos para o funcionamento de rede. Estas aplicações podem ser desenvolvidas em uma linguagem de propósito geral, viabilizando a inovação e soluções antes apenas permitidas e implementadas pelos próprios fabricantes.

Nesse contexto, soluções baseadas no protocolo IP, que não foram amplamente difundidas pelos fabricantes que utilizam suas próprias soluções fechadas, podem ser redesenhadas considerando os benefícios do emprego do paradigma SDN. Assim, a gerência de mobilidade pode utilizar-se desta filosofia de rede aberta e programável, para viabilizar a implementação de ideias promovidas pela abordagem baseada em NetLMM (*Network-based Localized Mobility Management*) (Internet Engineering Task Force, 2010), tais como PMIP (*Proxy Mobile IP*), onde a gerência de mobilidade é realizada com a isenção de sinalização nos dispositivos clientes, ficando esta sinalização a cargo do núcleo da rede.

Este artigo propõe, implementa e avalia o desempenho de uma estratégia de *handover* que reduz a latência do processo de reautenticação utilizando técnica de transferência de contexto de informações de segurança, bem como, considera uma arquitetura SDN para programar dinamicamente o tratamento da mobilidade com suporte dos ativos pertencentes ao núcleo da rede, o que viabiliza a continuidade do serviço e requisitos de QoS/QoE das aplicações, além de evitar o envolvimento do dispositivo móvel na sinalização para troca de ponto de acesso.

Este artigo está organizado da seguinte forma. Na Seção 2, os trabalhos relacionados serão discutidos. Em seguida, na Seção 3, a arquitetura da proposta, denominada *Mobility-Flow*, será detalhada. Na Seção 4, será apresentada a avaliação da proposta e a Seção 5 mostra as considerações finais deste trabalho.

2. Trabalhos Relacionados

Esta Seção aborda trabalhos relacionados no que concerne o gerenciamento de mobilidade baseado em redes definidas por software.

Devido à demanda crescente de gerenciamento de mobilidade em redes sem fio, o paradigma SDN tem recebido cada vez mais a atenção também nessa área. A plataforma OpenRoads (Yap *et al.*, 2009) foi a primeira abordagem criada para

manipular redes sem fio definidas por software no padrão OpenFlow. Foi projetada para fornecer suporte às novas abordagens de gerenciamento de mobilidade que antes eram difíceis de testar em ambientes de produção.

A abordagem CloudMAC (Dely et al., 2012) foi criada para gerenciar redes públicas do padrão IEEE 802.11, sem perder a capacidade de ser extensível, permitindo que novos serviços possam ser implementados facilmente em linguagens de programação de alto nível. No CloudMAC, os pontos de acesso físicos apenas encaminham pacotes até os dispositivos móveis. Processamento e gerenciamento dos pacotes são realizados em pontos de acesso virtuais localizados em nuvem computacional. As ligações entre os pontos de acesso físicos e virtuais são gerenciadas através de um controlador OpenFlow, que redireciona a transmissão dos fluxos. A desvantagem dessa abordagem é que o handover pode ser prejudicado devido ao alto atraso decorrente do processamento dos pacotes nos pontos de acesso virtuais nos datacenters.

O trabalho proposto em (Avelar et al., 2013) propõe o PMIPFlow, solução para o gerenciamento de mobilidade baseada em SDN. Um mecanismo de antecipação de handover baseado em lógica fuzzy para a redução das quedas de conexões durante o handover é elaborado e avaliado. Apesar de sua contribuição, o PMIPFlow como outras iniciativas, também não considera aspectos de segurança e suporte à autenticação. Além disso, os pontos de acesso precisam embarcar parte do protocolo para desempenhar as funções específicas para o provimento da mobilidade. A proposta utiliza uma versão de *software switch* que é executado no espaço do usuário, o que contribui para um baixo desempenho em relação à vazão máxima nominal dos pontos de acesso utilizados.

Em (Tantayakul et al., 2016), os autores defendem a não utilização de uma implementação baseada em protocolos legados como o PMIP e sim uma estratégia puramente baseada em SDN (SDN *Mobility*), que pode utilizar uma de suas características, a visão global da rede, para tratar e encaminhar fluxos de forma a entregar o serviço de mobilidade. Para avaliação da proposta foi criado um cenário simulado no mininet e [1]realizado comparativo entre PMIPv6 padrão e a solução proposta, demonstrando ao fim que a solução SDN *Mobility* é mais vantajosa em termo de perdas de pacotes.

O OpenSWDN (J. S. Zender et al., 2015), introduz uma arquitetura Wi-Fi baseada em uma abordagem SDN/NFV, e permite o controle programável e a virtualização de recursos físicos do WiFi através do uso do LVAP (light virtual access point). A estratégia adotada tem como desvantagem o fato do handover ser prejudicado caso haja alto atraso decorrente do processamento dos pacotes nos pontos de acesso virtuais nos datacenters. No Mobility-Flow apenas as primeiras mensagens são enviadas ao controlador, que instala regras de fluxo, responsáveis pelo encaminhamento do trafego.

Em suma, os trabalhos relacionados apresentados não consideram o processo de autenticação em suas propostas ou o fazem com grande custo computacional. A maioria das propostas baseiam-se em ambiente emulado, modelagem analítica ou solução com baixo desempenho usando OpenFlow como aplicação no espaço do usuário. A

[1] Mininet é um emulador de redes - links http://www.mininet.org/

abordagem de virtualização dos roteadores sem fio na nuvem ainda requer mecanismos visando garantir a QoS para aplicações de tempo real. Além disso, o trabalhos não exploram avaliações de métricas de QoE.

3. Arquitetura proposta

A Figura 1 apresenta a proposta de arquitetura para gerenciamento de mobilidade.

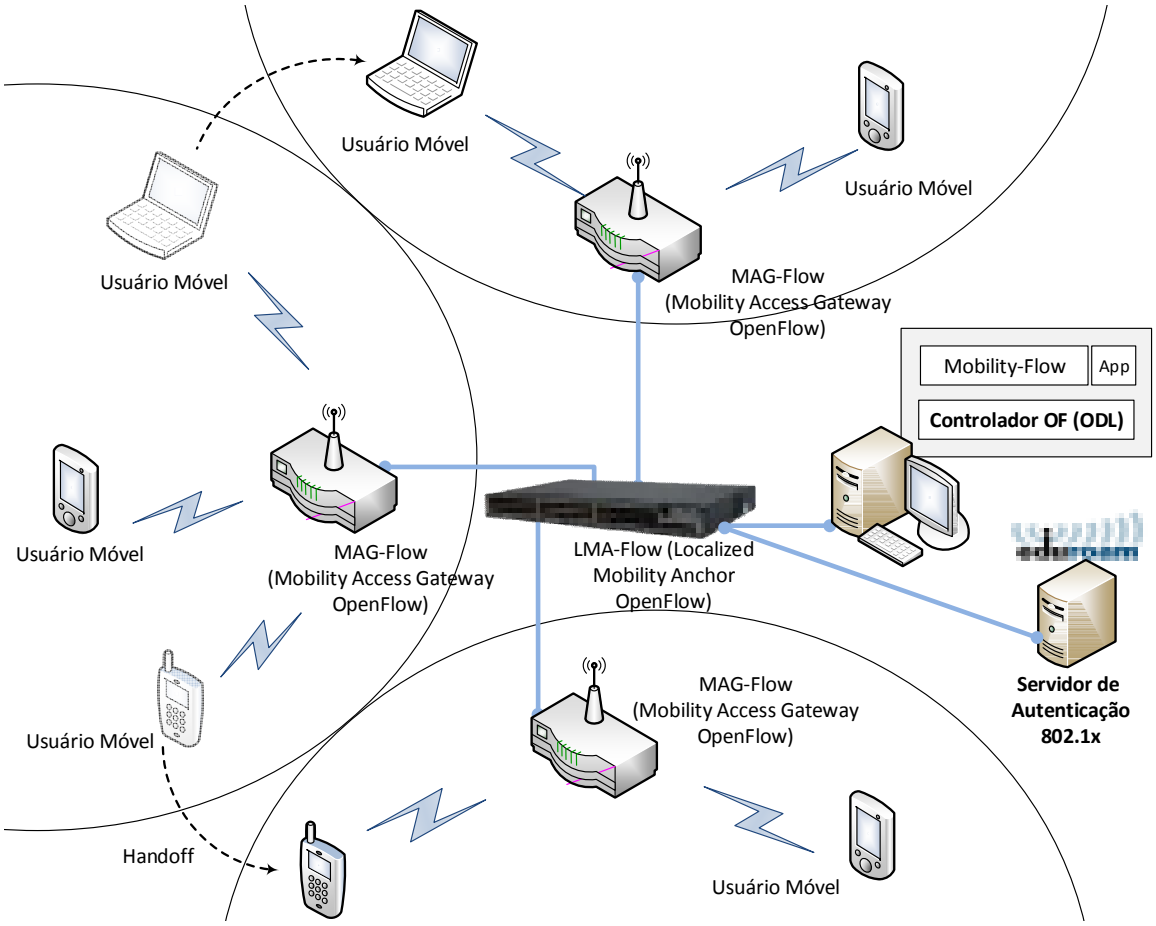


Figura 1. Arquitetura Mobility-Flow

O MAG-Flow (*Mobility Access Gateway - OpenFlow)* é o elemento responsável por monitorar e gerenciar a mobilidade dos usuários e possui duas representações: física e lógica. A parte física do MAG-Flow corresponde aos roteadores comerciais modificados. Nesses roteadores, o *firmware* original é substituído pelo OpenWRT,[2] que é um sistema linux para dispositivos com limitações de recursos computacionais. Além do firmware, é acrescentada uma versão OpenFlow instalada no espaço do *kernel*. Foi escolhida a versão 1.3 do OpenFlow, pois as versões anteriores não dão suporte a funcionalidades de QoS, que poderão ser utilizadas em trabalhos futuros da proposta.

Os elementos denominados de LMA-Flow (*Localized Mobility Anchor* – OpenFlow) são gateways dos elementos MAG-Flow, cuja responsabilidade é gerenciar

[2] Distribuição GNU/Linux para pontos de acesso sem fio - https://openwrt.org/

todo o tráfego, além de manter estruturas de dados que permitem saber se o usuário está se movendo entre MAG-Flows distintos, isto é, executando *handover*.

3.1 Sinalização de Conexão

A sinalização de conexão, mostrada na Figura 2, possui quatro etapas: autenticação, mobilidade, fornecimento de IP e implementação de regras OpenFlow, como detalhado nas trocas de mensagens:

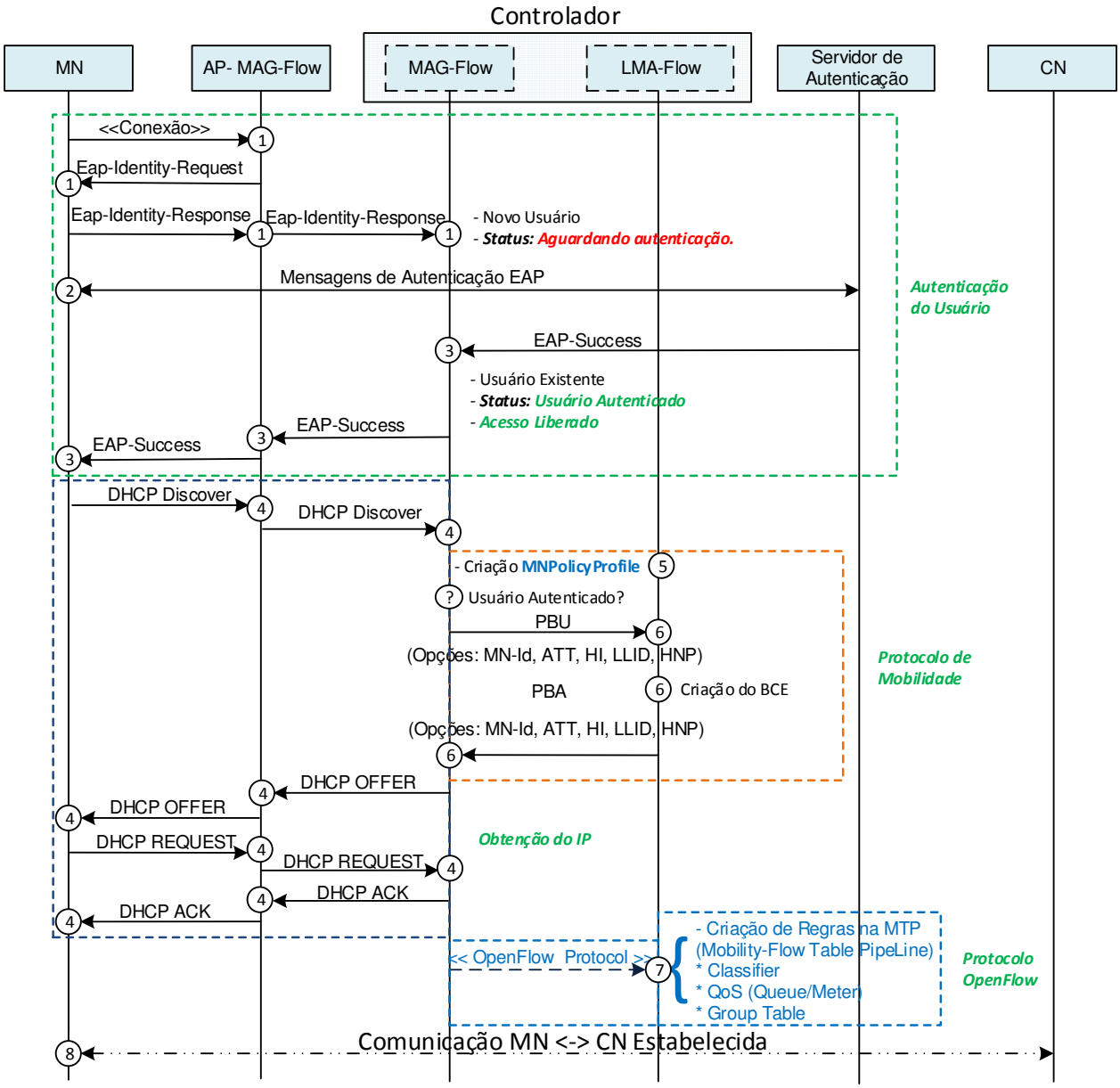


Figura 2. Sinalização de Conexão

[1]: Solicitação de Conexão a Rede Sem Fio: O MN (*Mobile Node*) conecta-se à rede autenticada, fornecendo nome de usuário e senha. No protótipo, a rede autenticada usa o protocolo EAP (*Extensible Authentication Protocol*) com autenticação TTLS (*Tunneled Transport Layer Security*). A comunicação entre o

cliente e o MAG-Flow é feita através do protocolo EAP e o protocolo RADIUS é usado para a troca entre o roteador e o servidor de autenticação.

[2]: Monitoramento de mensagens de Autenticação: A aplicação MAG-Flow executada no Controlador SDN, monitora toda a troca de mensagens entre cliente e servidor de autenticação, até a confirmação da autenticação do usuário.

[3]: Obtenção de *status* da autenticação: O servidor de Autenticação informa à aplicação MAG-Flow residente no controlador o sucesso na autenticação do usuário e este informa para o MN.

[4]: Processo de obtenção de IP: Nessa etapa o MN troca mensagens com o servidor DHCP implementado no controlador, para obtenção de endereço IP. Esta comunicação é gerenciada pelo protocolo de mobilidade do MAG-Flow.

[5]: Criação da Estrutura de dados de autenticação e controle de acesso: Nesta etapa é criada a estrutura de dados *MNPolicyProfile* no controlador, com informações de autenticação e permissões de acesso do MN, para serem utilizadas pelos MAG-Flow e LMA-Flow para autorização e controle dos MNs durante o Handover.

[6]: Troca de Mensagens do protocolo de Mobilidade: As mensagens PBU (*Proxy Binding Update)* e PBA (*Proxy Binding Ack*) são trocadas entre MAG-Flow e LMA-Flow com objetivo de verificar permissões e possíveis ocorrências de *handover* e criação e atualização do BCE.

[7]: Implementação de Regras OpenFlow: Nessa etapa, as regras OpenFlow para roteamento e encaminhamento são implementadas nos switches para provimento da comunicação.

[8]: Estabelecimento da comunicação entre MN e CN: Por fim, a comunicação entre o nó móvel (MN) e o nó correspondente (CN) é estabelecida.

3.2 Sinalização de *Handover*

A sinalização de handover, destacada na Figura 3, é semelhante à de conexão. A diferença é que quando o MN tentar migrar do MAG-Flow1 para o MAG-Flow2, o protocolo de mobilidade verifica que o usuário requisitante já estava conectado à outra rede. Então o MAG-Flow2 consulta o LMA-Flow para verificar se a solicitação trata-se de uma *handover*. Em caso positivo, o LMA-Flow verifica na estrutura de armazenamento MNPolicyProfile, os identificadores utilizados na primeira conexão do MN solicitante, e autoriza a migração do cliente sem a necessidade de uma reautenticação, pois a identificação é realizada a partir dos identificadores repassados por meio da transferência destes, dentro do mesmo contexto de segurança, conforme preceitua a RFC3374 (*Context Transfer Problem Statement - Internet Engineering Task Force*, 2002), o que corrobora para um *handover* suave, sem quebras decorrentes do tempo gasto no processo de reautenticação.

Durante o handover, o endereço obtido pelo usuário é o mesmo utilizado na rede anterior. Isso faz com que não haja quebra de conexão devido à mudança de endereçamento do MN na nova rede, desse modo, mantendo a conexão nas camadas superiores.

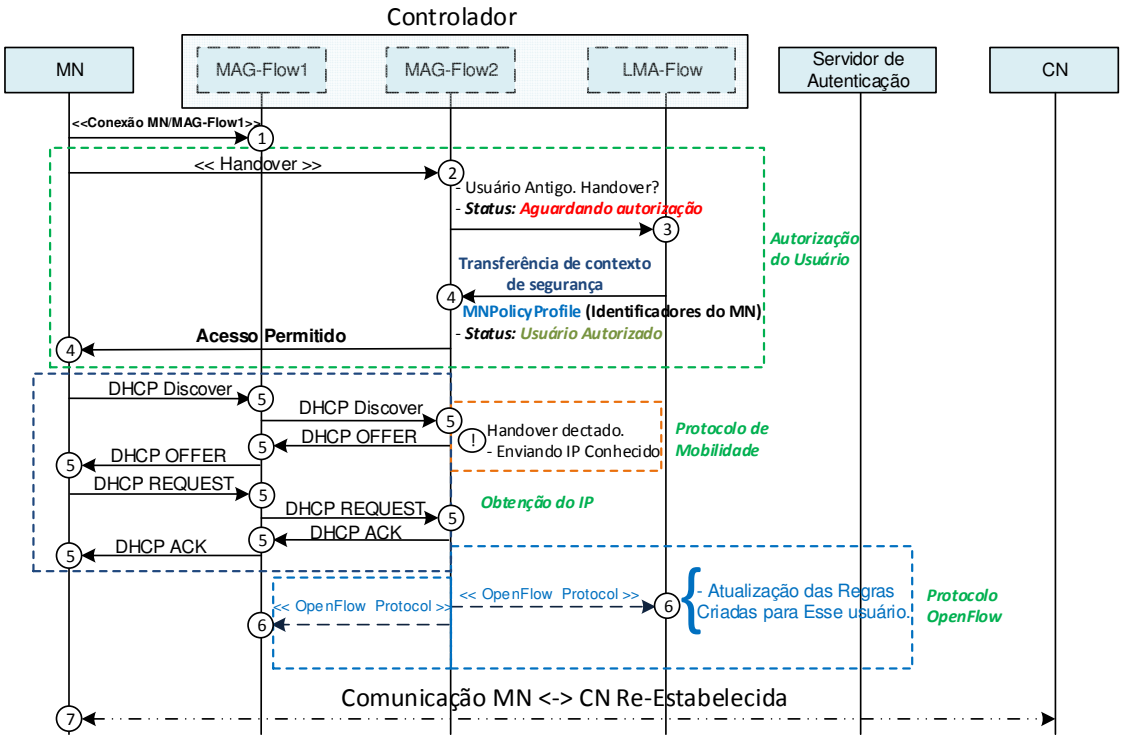


Figura 3. Sinalização de Handover

Todo processo de handover é detalhado nas trocas de mensagens abaixo:

[1]: Estado inicial do MN: O nó móvel (MN) inicialmente está conectado no MAG-Flow1, e segue em deslocamento aproximando-se do próximo ponto de acesso sem fio, o MAG-Flow2.

[2]: Solicitação de troca de ponto de acesso (*Handover*) devido à mobilidade: O nó móvel(MN) conectado no MAG-Flow1, solicita conexão para MAG-Flow2.

[3]: Verificação de nova conexão ou Handover: Ao receber a solicitação de conexão, o MAG-Flow2 envia uma mensagem ao LMA-Flow, para consultar se a solicitação trata-se de uma Handover.

[4]: Transferência de contexto de segurança: O LMA-Flow verifica que o MN estava conectado no MAG-Flow1 e que a solicitação de conexão para o MAG-Flow2 não refere-se a uma nova conexão e sim um handover, assim este consulta a estrutura de dados MNPolicyProfile para verificação das informações de autenticação e permissões de acesso do MN e informa ao MAG-Flow2 sobre a autorização do MN, sem a necessidade da realização de novo processo de autenticação. Por fim, o MAG-Flow2 de posse da autorização repassada pelo LMA-Flow, aceita a solicitação do MN.

[5]: Processo de obtenção de IP: Nessa etapa o MN troca mensagens com o servidor DHCP implementado no controlador, para obtenção de endereço IP. Esta comunicação é gerenciada pelo protocolo de mobilidade do MAG-Flow. Durante o processo de *handover,* o endereço obtido pelo MN é o mesmo utilizado na rede anterior. Isso faz com que a quebra de conexão da camada 3 decorrente da mudança de endereçamento não ocorra, mantendo a conexão nas camadas superiores.

[6]: Implementação e atualização de Regras OpenFlow: Nessa etapa, as regras de roteamento e encaminhamento correspondentes ao conexão MN/MAG-Flow1 são

retiradas e são implementadas regras OpenFlow nos switches para provimento da comunicação do MN/MAG-Flow2.

[7]: Estabelecimento da comunicação entre MN e CN: Por fim a comunicação entre o nó móvel(MN) e o nó correspondente(CN) é estabelecida.

4. Avaliação da Proposta

Nesta seção é realizada a avaliação da proposta em um testbed 802.11ac. Na subseção 4.1 é apresentado todo ambiente de teste e as funções desempenhadas pelos equipamentos durante os experimentos. Em seguida, na subseção 4.2, são apontados os resultados obtidos nos experimentos com a utilização da estratégia de gerenciamento de mobilidade com transferência de contexto de segurança implementada na proposta.

4.1 Ambiente de Teste

O testbed possui três pontos de acesso *Mobility-flow*, que são roteadores sem fio com OpenvSwitch (Openvswitch, 2016) instalado para suportar OpenFlow no nível do kernel. O ambiente possui também um comutador *Mobility-Flow*, que possui a função do LMA (*Localized Mobility Anchor*) do protocolo PMIP, ou seja, funciona como ponto de ancoragem e saída dos APs. O comutador Mobility-Flow é um roteador modificado para, assim como os Mobility-Flow-APs, suportar o protocolo OpenFlow. O Controlador é o elemento mais importante da rede e gerencia toda a rede OpenFlow. O último elemento da rede é o Gateway, responsável por redirecionar o tráfego da rede OpenFlow para a Internet. Nos experimentos, o gateway também funciona como servidor de autenticação. A Figura 4 mostra a planta baixa do ambiente onde o testbed foi implantado.

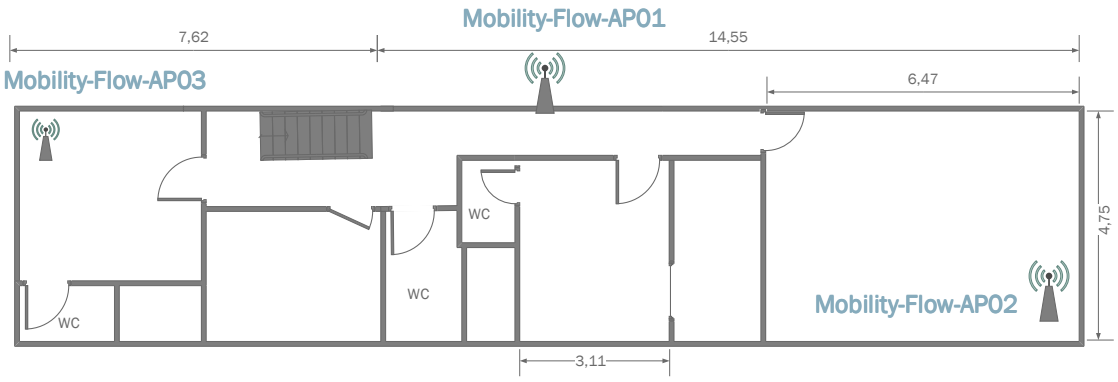


Figura 4. Ambiente do Testbed

Todos os testes foram realizados com um usuário movendo-se a uma velocidade média de um metro por segundo (1m/s). A Figura 5 mostra o padrão de movimentação usado em todos os testes. Escolheu-se esse padrão para comparar de forma justa as diferentes soluções apresentadas. Um percurso completo da Figura 5 leva em média 120 segundos. Por isso, todos os testes foram ajustados para durarem 200 segundos.

Para cada teste foram realizadas 30 repetições, como forma de obter resultados com relevância estatística.

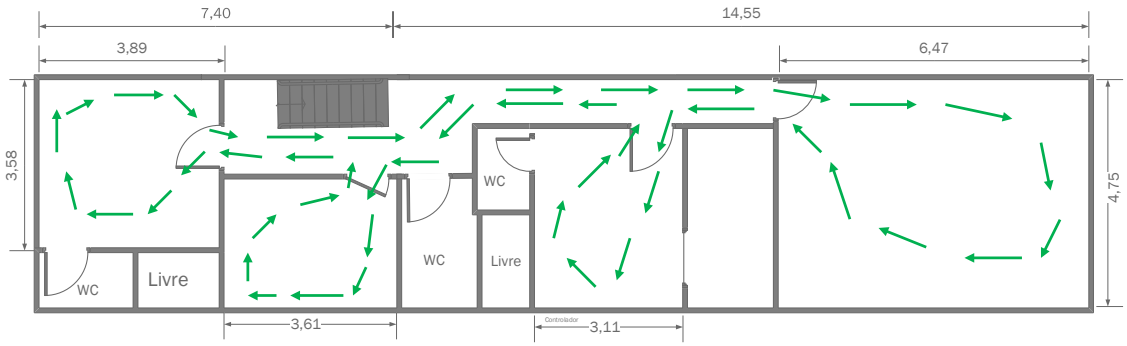


Figura 5. Padrão de movimentação pelo Ambiente

A Figura 6 mostra o mapa de força de sinal dos três pontos de acesso sem fio. O mapa foi feito com auxílio da ferramenta Heat mapper[3] da Ekahau, e mostra como está a distribuição do sinal no testbed. Quanto mais próximo do verde maior a intensidade do sinal, quanto mais próximo do vermelho, menor a intensidade. As potências das antenas dos pontos de acesso foram levemente reduzidas para permitir o cenário mostrado na Figura 6, caso contrário, devido ao espaço limitado, o usuário poderia se manter conectado mesmo estando no cômodo mais afastado. Como mostrado na Figura 6, quando o usuário migra de um cômodo ao outro ele é forçado a mudar de rede, do contrário a conexão é perdida.

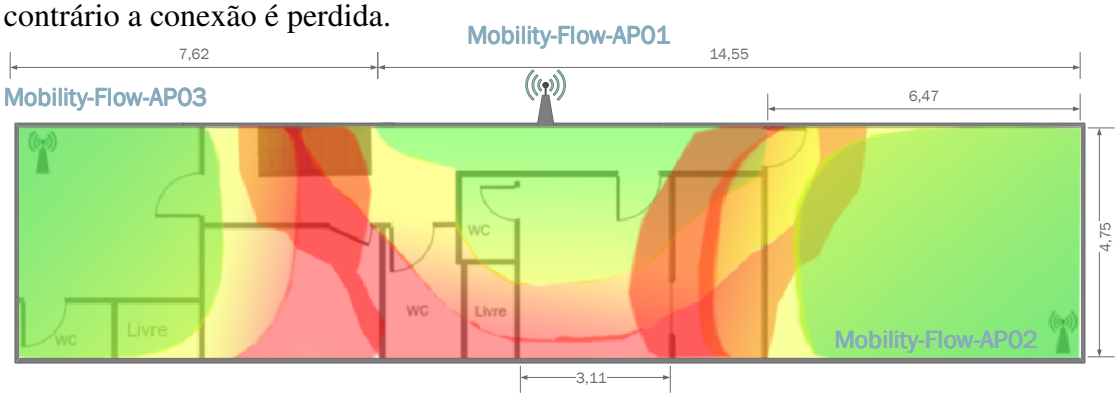


Figura 6. Mapa de Força do Sinal do Testbed

4.2 Resultados

4.2.1 Avaliação de QoS: Vazão e Atraso médio

Para a obtenção dos resultados das avaliações de vazão e atraso médio, foram realizados dois experimentos:

- **Vazão:** O experimento consistiu na execução de um fluxo sintético UDP de 100 Mbps entre o gateway e o cliente em deslocamento e realização da coleta dos resultados das vazões alcançadas. A Figura 7 mostra a média da vazão do switch do OpenvSwitch nos experimentos, onde, sem a proposta de transferência de contexto, a média da vazão foi de 64,24Mbps e com a proposta o valor médio da vazão aumenta para 74,43 Mbps, equivalente a um ganho de 15,8% em relação

[3] http://www.ekahau.com/wifidesign/ekahau-heatmapper

aos resultados alcançados na avaliação sem a adição da proposta de transferência de contexto de segurança.

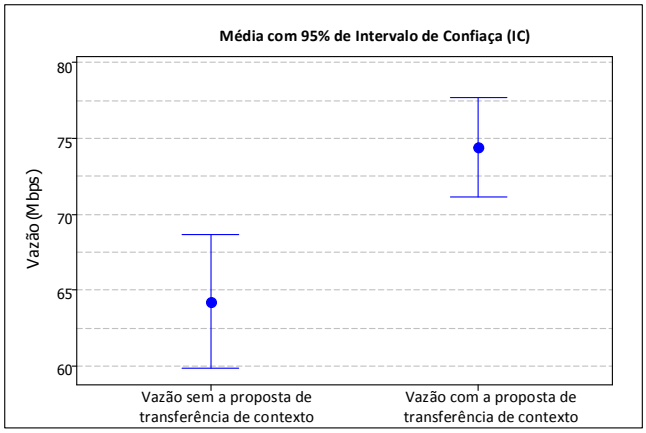


Figura 7. Vazão UDP com e sem transferência de contexto de segurança

- **Atraso Médio:** Para o segundo experimento foi enviado um *streaming* de vídeo do gateway para o cliente em deslocamento, para verificação do atraso entre os frames do vídeo. Quanto menor o atraso, melhor é a qualidade do vídeo recebido. A Figura 8 compara o atraso médio em 30 repetições, onde verifica-se que, sem a utilização da proposta de transferência de contexto de segurança, as perdas de pacotes devido à mobilidade do usuário são mais acentuadas, com isso o atraso médio da entrega dos pacotes fica em torno de 40ms. Já com a utilização da proposta de transferência de contexto de segurança, o valor de atraso médio cai para 30ms, o que representa um ganho de 25% nos resultados que utilizam a proposta. Os resultados de atraso médio apresentados na Figura 8 foram calculados usando a ferramenta Evalvid (Evalvid, 2016).

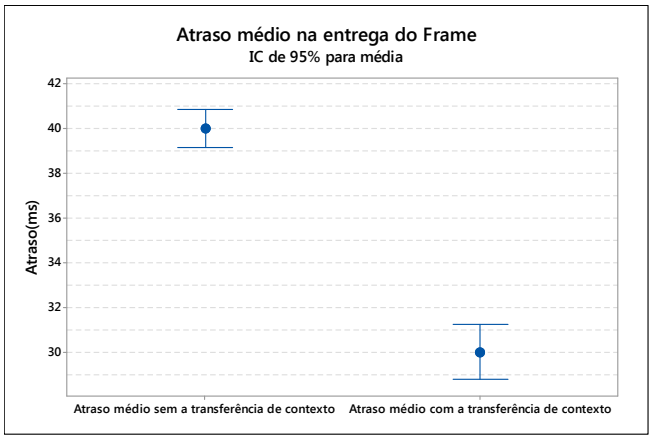


Figura 8. Atraso médio na entrega do Frame

4.2.2 Avaliação de QoE: PSNR

O PSNR (*Peak Signal-to-Noise Ratio*) é uma métrica de QoE que estima a qualidade do vídeo em decibéis, comparando o vídeo original com o vídeo recebido pelo usuário. Para cada faixa de valores de PSNR, há uma qualificação para o vídeo que foi recebido pelo usuário.

Para este experimento os vídeos foram enviados um de cada vez. Durante a transmissão do vídeo, assim como na avaliação de QoS, o usuário permanece em constante movimento de um ponto de acesso para outro. Após o recebimento do vídeo foi utilizada a versão gratuita da ferramenta MSU (*Video Quality Measurement Tool*), (MSU, 2013), para avaliar e extrair as informações para avaliação do vídeo recebido.

A Figura 9 mostra que o valor médio do PSNR sem a proposta de transferência de contexto de segurança foi de 26,7, considerado ACEITÁVEL, já com a adição da transferência de contexto de segurança o resultado de PSNR foi de 32,2, considerado BOM. Na comparação entre os intervalos de cada cenário, com 95% de confiança. É possível notar que com a proposta o PSNR é visivelmente superior ao cenário sem a proposta de transferência de contexto.

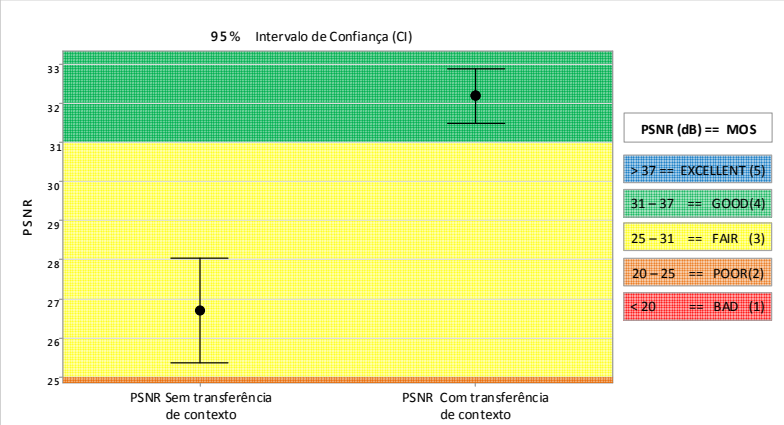


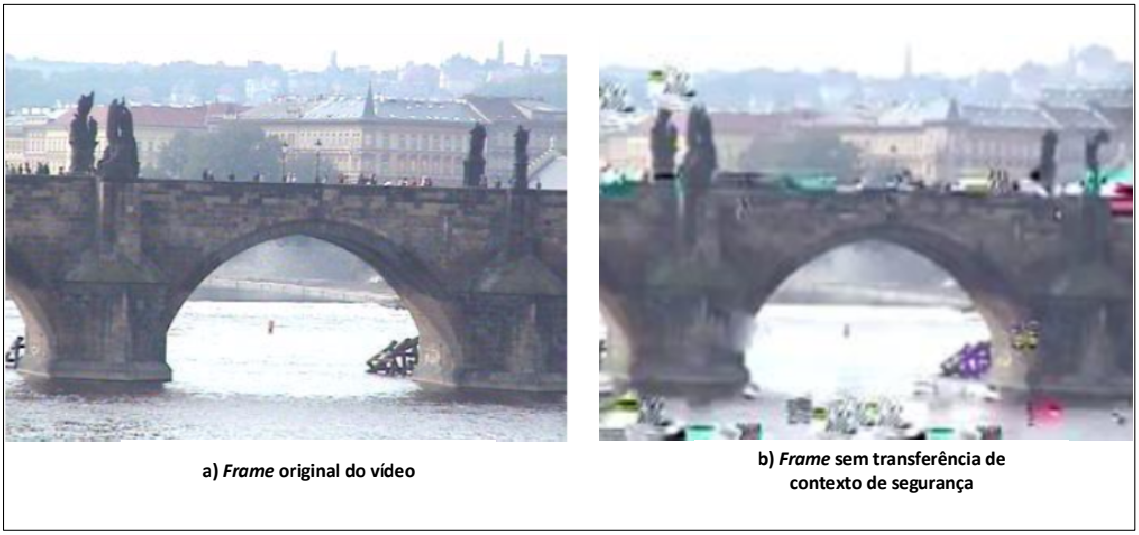
Figura 9. Atraso médio na entrega do Frame

a) Respaldo Visual PSNR

A Figura 10 apresenta um *frame* original do vídeo usado na avaliação do PSNR. O vídeo utilizado dura 30 segundos e 2000 frames. Esse vídeo foi escolhido por durar mais do que os outros vídeos disponíveis em (Bridge, 2016). Como um percurso completo dura 120 segundos em média (ver Figura 5), o mesmo vídeo foi repetido 5 vezes, para gerar uma duração de 150 segundos.

Figura 10. *Frame* original do vídeo

A Figura 11 apresenta uma comparação para respaldo visual do *frame* original do vídeo (a), *frame* no momento do handover sem a proposta de transferência de contexto de segurança (b). É possível observar que o quadro mostrado na Figura 11b está com uma qualidade bem inferior, se comparado com o *frame* original mostrado na Figura 11a. Isso ocorre porque houve perdas de pacotes durante o handover, que foram acentuadas pelo processo de reautenticação, o que culminou na reconstrução incompleta do *frame* no receptor.

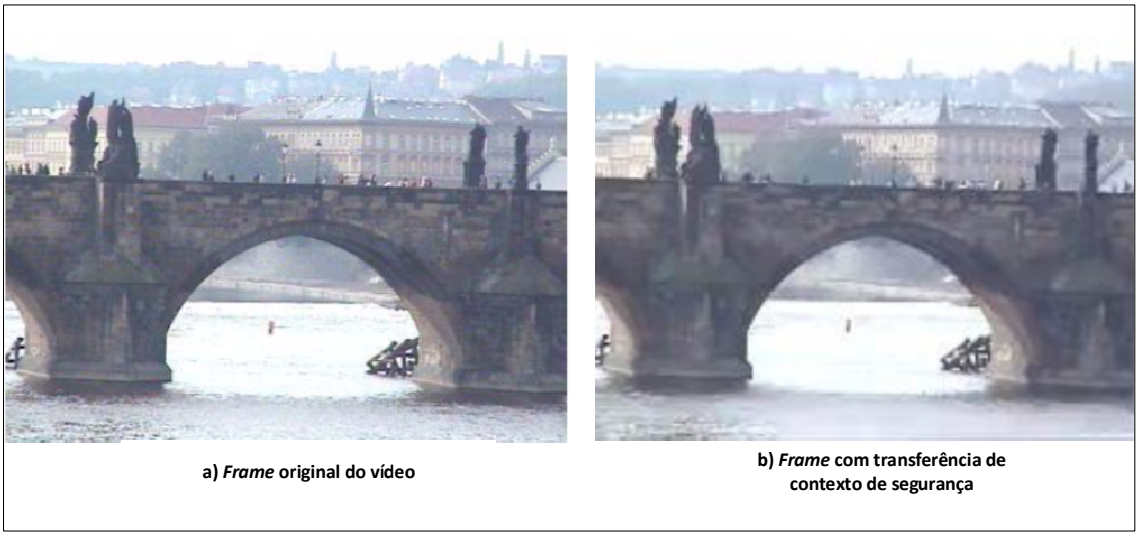


a) *Frame* original do vídeo

b) *Frame* sem transferência de contexto de segurança

Figura 11. *Frame* original (a) e *frame* sem a transferência de contexto (b)

Por outro lado, a Figura 12, é uma comparação para respaldo visual do *frame* original do vídeo (a), e o *frame* capturado no momento do handover com a proposta de transferência de contexto de segurança (b). Percebe-se que nesse caso, o *frame* capturado está com qualidade melhor que na Figura 11b, pois poucos pacotes são perdidos com a proposta, o que resulta em um *frame* de vídeo mais completo. Mesmo com perdas da camada L2, o vídeo resultante do cenário com a proposta é muito superior ao vídeo sem a proposta.



a) *Frame* original do vídeo

b) *Frame* com transferência de contexto de segurança

Figura 12. *Frame* original (a) e *frame* com transferência de contexto (b)

5. Conclusão

Este trabalho implementou e avaliou uma proposta de estratégia de transferência de contexto de segurança para o *Mobility-Flow*, que suaviza a degradação do processo de reautenticação decorrente do handover entre redes e assim fornece níveis aceitáveis de QoE. Foram discutidas diversas iniciativas na literatura voltadas a prover o serviço mobilidade, com destaque para a lacuna no aspecto referente ao suporte à segurança nas soluções de *handover*.

A avaliação foi realizada em um ambiente de experimentação e a proposta obteve como resultados os seguintes ganhos: 15,8% na vazão, 25% no atraso médio e 20,5% no PSNR em relação ao cenário de não utilização da proposta de transferência de contexto de segurança. Os resultados obtidos demonstram a aplicabilidade da proposta no gerenciamento mobilidade seguro, bem como sua eficácia no suporte aos requisitos de QoS/QoE para sessões de tráfego de vídeo de usuários móveis.

6. Referências

Avelar, E. A. M., Marques, L., Dias, K. L.. PMIPFlow: *Uma Proposta para Gerenciamento de Mobilidade em Redes Definidas por Software*. In: WPerformance, 2013, Maceió. WPerformance, 2013. p. 1-14.

Bridge (close) (2016). http://www2.tkn.tu-berlin.de/research/evalvid/cif.html

Dely, P., Vestin, J., Kassler, A., Bayer, N., Einsiedler, H., and Peylo, C. (2012). *"CloudMAC – An OpenFlow based Architecture for 802.11 MAC Layer Processing in the Cloud."* In Globecom Workshops (GC Wkshps), 2012 IEEE, pages 186–191. IEEE.

Evalvid 2016. A Video Quality Evaluation Tool-set, http://www2.tkn.tu-berlin.de/research/evalvid/EvalVid/docevalvid.html

Ferretti, S., Ghini, V. and Panzieri, F.. "A survey on handover management in mobility architectures." Computer Networks 94 (2016): 390-413.

Internet Engineering Task Force (2010). Network-based Localized Mobility Management. http://datatracker.ietf.org/doc/charter-ietf-netlmm/

Internet Engineering Task Force (2002). Context Transfer Problem Statement. https://www.ietf.org/rfc/rfc3374.txt

J. S. Zander, C. Mayer, B. Ciobotaru, S. Schmid, A. Feldmann, OpenSDWN: programmatic control over home and enterprise WiFi, in: Proceedings of the ACM SIGCOMM SOSR, Santa Clara, CA, USA, 2015.

K. Tantayakul, R. Dhaou and B. Paillassa, "Impact of SDN on Mobility Management," *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Crans-Montana, 2016, pp. 260-265.

MSU Video Group (2013). Video Quality Measurement Tool. http://compression.ru/index_en.htm.

N. McKeown, T. Anderson, H. Balakrishnan,G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. "*OpenFlow : enabling innovation in campus networks*". ACM SIGCOMM Computer Communication Review. April de 2008, Vol. 38, 2, pp. 69-74.

OpenvSwitch (2016). OpenFlow 1.3 kernel Switch. Disponível em: http://openvswitch.org/download/.

Yap, K.-K., Kobayashi, M., Underhill, D., Seetharaman, S., Kazemian, P., and McKeown, N. (2009). The Stanford OpenRoads Deployment. In Proceedings of the 4th ACM International Workshop on Experimental Evaluation and Characterization, WINTECH '09, pages 59–66, New York, NY, USA. ACM.

Wang, Y., & Bi, J. "*A Solution for IP Mobility Support in Software Defined Networks*." Computer Communication and Networks (ICCCN), 2014 23rd International Conference on, pages 1 – 8.