Decisão de Transição em Redes Heterogêneas Ciente do Nível de Segurança

Alisson Puska, Aldri Santos, Michele Nogueira

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2)
Universidade Federal do Paraná (UFPR)
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brazil

{aapuska,aldri,michele}@inf.ufpr.br

Abstract. *The process of handoff in wireless heterogeneous networks allows the maintenance of the mobile user connectivity in order to keep it continuously connected and in the best network available. This maintenance depends on the selection of an access point for connection transference. The decision methods analyze the performance, quality of service and security characteristics of access points in order to select one for the handoff. However, the methods presented in literature consider security superficially and does not analyze its distinct properties, which may lead to risky choices and prejudice the user. Besides, the lack of information about the decision criteria may cause failures in the transition process. This work presents a method that assists the decision making in the transition process to provide safe decisions based on the confidentiality risk to the communications through the access points and the lack of information. The evaluation results show the precision of the method on the less risky choices and it is insignificant impact on the transition performance.*

Resumo. *O processo de transição em redes heterogêneas sem fio possibilita a manutenção da conectividade do usuário móvel afim de mantê-lo conectado continuamente e na melhor rede disponível. Esta manutenção depende da escolha de um ponto de acesso para transferência da conexão. Os métodos de decisão analisam as características de desempenho, qualidade de serviço e segurança dos pontos de acesso a fim de selecionar um para a transição. Entretanto, os métodos presentes na literatura consideram a segurança superficialmente e não analisam as suas propriedades distintas, podendo levar a decisões arriscadas. Isto, juntamente com a falta de informações sobre os critérios de decisão podem gerar escolhas inadequadas e falhas no processo de transição. Este trabalho apresenta um método que auxilia a tomada de decisão no processo de transição em redes heterogêneas para proporcionar decisões seguras com base no risco à confidencialidade das comunicações e da falta de informações. Os resultados da avaliação mostram a precisão do método quanto às escolhas menos arriscadas e o seu impacto insignificante no desempenho na transição.*

1. Introdução

O constante desenvolvimento das tecnologias de comunicação sem fio e o aumento no número de usuários com intensa demanda pela melhor conexão têm instigado uma mudança de paradigma na forma como as redes de comunicação são implantadas [Erews 2013]. Este novo paradigma prevê a interoperabilidade entre as diferentes

tecnologias de comunicação (802.11, 3G, etc.) com o objetivo de fornecer melhores conexões, e assim manter a conectividade do usuário móvel em um ambiente heterogêneo repleto de pontos de acesso. Esta interação entre tecnologias permite a integração de redes com características distintas de Qualidade de serviço, desempenho e segurança.

As redes sem fio heterogêneas (HetNets, do inglês, *Heterogeneous Networks*) representam esta mudança de paradigma e preveem mecanismos para o gerenciamento da mobilidade dos dispositivos. Os mecanismos de detecção dos pontos de acesso no ambiente, de mensuração da capacidade das redes, de avaliação das suas características, de escolha e de transferência de conexão entre os pontos de acesso, entre outros, proveem quando necessária a transição (*handoff*) do dispositivo entre as redes [Rao et al. 2013]. Esta transferência ocorre por diferentes motivos, como a degradação na qualidade da conexão ou a detecção de um ponto de acesso com melhor capacidade de atender as necessidades do dispositivo móvel. Logo, o controle de mobilidade permite a manutenção da conectividade do dispositivo móvel, transferindo de modo transparente a sua conexão. A tarefa de selecionar a rede mais adequada para transferência da conexão é o ponto mais importante do processo de transição [Ahmed et al. 2014]. Particularmente, o processo de decisão na transição entre HetNets compara as redes disponíveis para determinar aquela que seja adequada às necessidades do dispositivo móvel. Esta escolha acontece de forma automática e transparente ao usuário. A seleção dos critérios de decisão, a classificação da importância relativa de cada critério, o tempo de decisão e a eficácia das decisões estão entre os desafios do processo de decisão em HetNets.

Apesar da existência de vários métodos de decisão propostos para as HetNets, não há estudos sobre as propriedades de segurança dos pontos de acesso. Alguns trabalhos apontam a importância de considerar este critério no processo de decisão, porém não realizam um estudo aprofundado do uso das propriedades que compõem a segurança na decisão [Ahmed et al. 2014, Rajule et al. 2013, Zekri et al. 2012]. Tais métodos usam o critério segurança como um atributo simples, não considerando as suas principais propriedades: confidencialidade, integridade e disponibilidade. Ignorar as diferenças destas propriedades e as técnicas que procuram garanti-las pode levar à decisões inadequadas as necessidades do dispositivo. Por exemplo, um dispositivo pode escolher uma rede que possua mecanismos que garantam à disponibilidade das comunicações, porém ele também necessite de confidencialidade nas transmissões. Assim, o impacto da falta de informações sobre os critérios usados na escolha prejudica o processo de decisão e diminui a acurácia das escolhas [Beresford and Sloper 2008]. Em um ambiente de HetNets não existem garantias de que todas as informações necessárias na comparação dos pontos de aceso estarão sempre disponíveis. Portanto, o impacto da ausência de informações deve ser considerado na tomada de decisões em HetNets.

Um modo de definir a segurança de uma rede de acesso consiste da determinação do seu risco, onde [Pfleeger 2012], [Avizienis et al. 2004]. O modelo prospectivo de decisão considera fatores como o risco das alternativas e a falta de informações para efetuar escolhas [Kahneman and Tversky 1979]. Este modelo da área de economia descreve como seres humanos tomam decisões envolvendo risco e fatores como a falta de informações. Assim, a adaptação deste modelo pode auxiliar o processo de decisão de *handoff* em redes heterogêneas a aferir o risco de segurança e a executar escolhas menos arriscadas quando faltam informações dos critérios de comparação.

Este trabalho apresenta um método autônomo de apoio a decisão no *handoff* em HetNets, chamado SDHet. Este método considera os aspectos de segurança oferecidos pelos pontos de acesso, em particular a confidencialidade na transmissão dos dados, buscando a autopreservação do anonimato e da privacidade do usuário. A eficácia e a eficiência do SDHET foram avaliadas através de simulações, e os resultados comparados com outro método considerando diferentes ambientes de redes heterogêneas.

O restante do artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados a. A Seção 3 especifica o método proposto de apoio a decisão. A Seção 4 apresenta uma avaliação da eficácia do métdo. A Seção 5 conclui o trabalho.

2. Trabalhos Relacionados

Os trabalhos encontrados na literatura têm destacados a importância de considerar a segurança como um critério de seleção no processo de decisão de *handoff* em HetNets [Ahmed et al. 2014, Khanum and Islam 2014, Li and Chen 2013]. No entanto, a maioria dos trabalhos que consideram segurança como um critério de seleção no processo de decisão analisam apenas o seu desempenho. Os poucos trabalham sobre o processo de decisão de *handoff* que analisam a segurança de modo adequado desconsideram as propriedades de segurança de fato ou as consideram de modo superficial.

Li e Cheng [Li and Chen 2013] propõem um método simples que utiliza uma função objetivo para classificação dos pontos de acesso e uma função de valoração adaptativa para ponderação dos critérios de decisão. Apesar de usar a segurança como critério de seleção, os autores avaliam apenas o desempenho do processo de decisão. A proposta deles assume a segurança como um critério único e não a analisam de maneira adequada, podendo levar a decisões inadequadas. A simplicidade da solução torna o desempenho do método um ponto forte juntamente com flexibilidade quanto ao número de critérios de decisão e de considerar as informações do contexto do dispositivo na função de ponderação. Kahnum et al. [Khanum and Islam 2014] utilizam uma estratégia baseada na teoria difusa e nas preferências do usuário. A lógica difusa trata a imprecisão das medições dos critérios, porém, o custo para o desempenho é alto além de comprometer a dinamicidade das decisões quando o ambiente se altera constantemente. Eles não analisam a segurança de maneira adequada, não respeitando as diferentes características de cada principio. Além disso, a solução requer uma fase de calibração dos valores medidos, o que aumenta o tempo do processo de decisão. A forma adaptativa de ponderar os critérios com base nas preferências do usuário é eficaz.

Os autores em [Nasser et al. 2007] e [Bakmaz et al. 2012] empregam o Nível de Segurança (LoS, do inglês Level of Security) na avaliação das redes disponíveis. O valor deste nível considera a força dos algoritmos de criptografia presentes nas redes, determinando a rede mais segura. Entretanto, a força do algoritmo de criptografia por si só não indica a segurança de uma rede. Outras técnicas, como ocultação de informações (esteganografia, anonimato) e controle de acesso (autenticação, autorização e filtragem), devem ser considerados na avaliação da confidencialidade das transmissões. Ma et al. [Ma et al. 2012] propõe a avaliação do critério segurança através da inferência do nível de risco do ambiente. Porém, os autores não especificam como realizar a aferição e quais aspectos da segurança são considerados.

O processo de decisão em HetNets deve realizar escolhas com segurança de ma-

neira adequada, analisando os princípios de segurança separadamente. Assim, este trabalho propõe um método de decisão que analisa e quantifica as propriedades de confidencialidade para classificação das redes de acesso. O método objetiva a manutenção da confidencialidade da conectividade na transição de dispositivo móvel em HetNets.

3. Método de Apoio a Decisão

O método proposto, chamado de SDHet, tem como objetivo auxiliar o processo de decisão na transição (*handoff*) em HetNets para a escolha de pontos de acesso (APs) através da análise da confidencialidade das transmissões. Ele determina o risco à confidencialidade (CR) de cada rede disponível, suplementando as informações de desempenho e qualidade de serviço (QoS, do inglês *Quality of Service*) comumente usadas para decisão [Ahmed et al. 2014]. O CR estabelecido baseia-se na avaliação das propriedades de confidencialidade dos APs e na inferência de um valor representativo através da observação da presença de mecanismos de segurança que tentam garantir este principio.

As HetNets integram tecnologias de comunicação com características diferentes [Zekri et al. 2012]. Essas tecnologias possuem propriedades específicas de desempenho, QoS e segurança que tornam complexa a avaliação dos APs para a tomada de decisão. O SDHet foca nas propriedades de segurança, em particular nos tipos de mecanismos oferecidos por cada rede de acesso que tentam garantir a confidencialidade das transmissões, para avaliar e classificar o nível de segurança das redes de acesso. Este valor classificatório corresponde ao principal critério para decisão e seleção de uma rede para a transferência da conexão do dispositivo móvel.

Os componentes das HetNets compreendem os dispositivos móveis, os pontos de acesso e suas redes centrais [Cavalcanti et al. 2005]. Os dispositivos móveis podem ser heterogêneos quanto a suas características, possuindo diferentes capacidades de processamento, mobilidade e suporte à tecnologias de comunicação. Estas características influenciam o tempo de decisão, podendo prejudicar o processo de transição. Por exemplo, se o grau de mobilidade do dispositivo for alto e o processo de decisão levar muito tempo, o dispositivo corre o risco de transitar para uma rede fora de alcance quando o processo termina. O SDHet considera a simplicidade a fim de obter um tempo de decisão que não prejudique a transição. Os APs podem ser heterogêneos quanto a suas configurações, suportando tecnologias de comunicação com características de segurança diferentes. Cada AP emprega apenas uma tecnologia de comunicação, e a rede central representa o *backbone* para os APs e oferece serviços e conectividade com a internet [MELO et al. 2013].

O SDHet assume que a rede heterogênea corresponde a um conjunto N composto por ap (ponto de acesso) identificados por $\{ap_1, ap_2, ap_3, ..., ap_i\}$, onde $ap_i \in N$. Cada ponto de acesso ap_i possui um único identificador e pertence a uma rede central diferente. Como cada rede central pertence a um domínio diferente, o *handoff* ocorre verticalmente, alterando o sistema de comunicação mesmo quando a tecnologia à qual se transita se mantém. O valor de ap_i corresponde a um número único de identificação usado na escolha e no controle do *handoff*. A Figura 1 ilustra uma rede heterogênea onde ocorre o handoff.

Cada tecnologia de comunicação pode possuir diferentes mecanismos que buscam garantir a confidencialidade das comunicações. Estes mecanismos empregam técnicas de confidencialidade classificadas como controle de acesso (AC, do inglês *Access Control*) e ocultação de dados (DH, do inglês *Data Hiding*) [Stamp 2011,

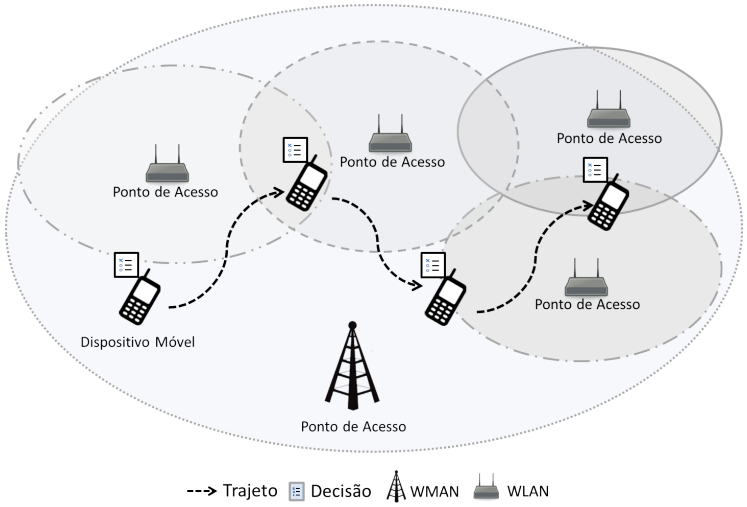

Figura 1. Cenário de uma Rede Heterogênea

Pfitzmann 1996, Cacciaguerra and Ferretti 2003]. As técnicas de AC englobam mecanismos de autenticação, autorização e filtragem, tais como senhas (autenticação), listas de permissão (autorização) e *proxys* (filtragem). As técnicas de DH empregam mecanismos de criptografia e esteganografia, tais como criptografia simétrica (criptografia) e *fingerprinting* (esteganografia) O SDHet determina os conjuntos de AC e DH, compostos por t_{ac} e t_{dh} técnicas identificadas por $\{t_{ac_1}, t_{ac_2}, t_{ac_3}, ..., t_{ac_i}\}$ e $\{t_{dh_1}, t_{dh_2}, t_{dh_3}, ..., t_{dh_i}\}$, onde $t_{ac_i} \in AC$ e $t_{dh_i} \in IO$. O SDHet assume que as informações sobre o número de mecanismos que empregam cada tipo de técnica de confidencialidade são fornecidas pela fase de coleta de dados. Além disso, cada dispositivo móvel possui necessidades diferentes, podendo considerar uma determinada técnica mais importante do que outra. Assim, as técnicas de confidencialidade podem ser ponderadas de acordo com a sua importância ou a necessidade do dispositivo móvel. O valor ponderativo corresponde ao elemento α.

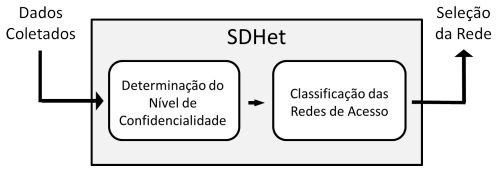

Figura 2. Arquitetura do Método de Apoio a Decisão

O SDHet classifica as redes de acordo com o nível do risco à confidencialidade e da falta de informações, sendo dividido em duas fases: a fase de determinação do nível de confidencialidade e a fase de classificação dos pontos de acesso. Estas fases são inseridas entre a fase de coleta de dados e a fase de transição do processo de *handoff*. A Figura 2 ilustra a arquitetura do método. A primeira fase infere os valores do risco à confidencialidade (CR), o nível de confiança (L_c) e o nível de possibilidade (L_p) para os pontos de acesso. O (CR) se baseia na quantidade de técnicas de confidencialidade em cada ponto de acesso. O nível de confiança considera a quantidade de mecanismos que implementam as técnicas de confidencialidade presentes nas redes e o nível de possibilidade se baseia na falta de informações sobre a presença ou ausência dos mecanismos. A segunda fase

infere um valor classificatório para ordenação das redes, e emprega os valores de CR, L_c e L_p para determinar a rede de acesso com o maior nível de confidencialidade.

3.1. Cálculo do Risco, do Nível de Confiança e do Nível de Possibilidade

O cálculo do CR, Equação 1, emprega a técnica de probabilidade subjetiva [Triola et al. 2005] que utiliza conhecimentos circunstanciais para estimar a probabilidade do evento. A presença ou ausência de uma determinada técnica de confidencialidade correspondem as informações circunstanciais que servem de base para o cálculo. O CR na rede ap_i corresponde à probabilidade subjetiva inicial de exposição das transmissões P_i (50%) adicionada da diferença entre a probabilidade subjetiva de exposição das transmissões ($V_{am}(ap_i)$) e a probabilidade subjetiva de proteção das transmissões ($V_{pm}(ap_i)$).

$$CR_{ap_i} = P_i + (V_{am}(ap_i) - V_{pm}(ap_i)) \tag{1}$$

A Equação 2 define o valor final do risco à confidencialidade das comunicações de uma rede. Onde $F_a(t_{ac_j})$ e $F_a(t_{dh_j})$ identificam a ausência (0) de uma técnica de AC e DH em ap_i respectivamente. O valor N corresponde ao total de técnicas de confidencialidade consideradas pelo SDHet. O α_j representa o valor de ponderação da respectiva técnica de confidencialidade. O somatório de todos os pesos deve ser obrigatoriamente 0.5 , que corresponde ao valor máximo da probabilidade subjtiva de proteção de cada técnica, obedecendo a Equação 3. Desta forma, V_{am} corresponde ao somatório da probabilidade subjetiva de exposição de cada técnica ausente ($P_i * \alpha_j$). A ponderação das técnicas não são consideradas no escopo deste trabalho, podendo ser realizada por diferentes métodos [Martinez-Morales et al. 2010]. A soma dos valores referentes aos dois conjuntos representa a probabilidade subjetiva das técnicas de segurança ausentes.

$$V_{am}(ap_i) = \sum_{j=1}^{N}(F_a(t_{ac_j}) * (P_i * \alpha_j)) + \sum_{j=1}^{N}(F_a(t_{dh_j}) * (P_i * \alpha_j)) \tag{2}$$

$$\sum_{j=1}^{N} \alpha_j * P_a = 0,5 \tag{3}$$

Do mesmo modo, a função ($V_{pm}(ap_i)$) calcula a probabilidade subjetiva de proteção das comunicações em ap_i. A Equação 4 define a presença das técnicas na rede. Onde $F_p(t_{ac_j})$ e $F_p(t_{dh_j})$ identificam a presença (1) de uma técnica de AC e DH em ap_i respectivamente. N corresponde ao total de técnicas de confidencialidade consideradas pelo SDHet. A quantidade total de técnicas presentes em cada conjunto multiplica o valor da probabilidade subjetiva de proteger as comunicações de cada tipo de técnica. A soma dos valores referentes aos dois conjuntos resulta no total que representa a probabilidade subjetiva das técnicas protegerem os dados na rede ap_i.

$$V_{pm}(ap_i) = \sum_{j=1}^{N}(F_p(t_{ac_j}) * (P_i * \alpha_j)) + \sum_{j=1}^{N}(F_p(t_{dh_j}) * (P_i * \alpha_j)) \tag{4}$$

Caso não existam informações sobre a presença ou ausência de uma técnica, o valor da probabilidade da respectiva técnica resulta em 0. Nestes casos, registra-se a falta de

informações para a posterior utilização do valor na fase de escolha. A falta de informações define o valor do nível de possibilidade nas redes disponíveis e a troca da regra de escolha. Este valor influencia o comportamento da decisão na segunda fase, onde ao invés de selecionar a rede mais confidencial, o SDHet seleciona a rede de maior confiança. O SDHet assume que o valor do risco à confidencialidade não deve ultrapassar o limiar inferior de 10% e o limiar superior de 90%. Devido a inevitável presença ou ocorrência de falhas, nenhum sistema pode ser considerado 100% seguro [Avizienis et al. 2004]. Da mesma forma, nenhum sistema pode ser considerado 100% vulnerável.

O valor de L_c, dada pela Equação 5, representa o impacto do número de mecanismos de uma mesma técnica no valor do CR. Este fator é inspirado na função de ponderação do impacto de um evento da teoria da prospecção e mapeia o impacto de um evento para o decisor. O SDHet baseia-se nesta função para definir um função que auxilie a ponderar e selecionar o ponto de acesso quando ocorre a falta de informações de um critério. O cálculo de L_c se baseia na quantidade de mecanismos presentes em uma rede. A soma do número de mecanismos de cada técnica multiplicados pelo valor base do tipo do mecanismo retorna o nível de confiança L_c. O L_c determina a confiança do dispositivo no risco à confidencialidade calculado para um ponto de acesso. As funções $F_t(t_{ac_j})$ e $F_t(t_{dh_j})$ identificam a quantidade total de mecanismos que aplicam uma mesma técnica de AC e DH em ap_i respectivamente. O somatório do número de mecanismo nos conjuntos AC e DH é multiplicado pelo valor base de cada técnica para designar o L_c.

$$L_c(ap_i) = \sum_{j=1}^{N}(F_t(t_{ac_j}) * (P_i * \alpha_j)) + \sum_{j=1}^{N}(F_t(t_{dh_j}) * (P_i * \alpha_j)) \tag{5}$$

O valor possibilidade (L_p), dada pela Equação 6, corresponde à quantidade de técnicas sem nenhuma informação a respeito da presença ou ausência de mecanismos em uma rede de acesso. Este valor baseia-se na função que mapeia o impacto de fatores como a incerteza e a falta de informações para o decisor no modelo definido pela teoria da prospecção. No SDHet, ele corresponde ao impacto da falta de informações na escolha. A soma do número de técnicas sem informações multiplicado pelo valor base de cada técnica de técnicas resulta no nível de possibilidade.

$$L_p(ap_i) = \sum_{j=1}^{N}(F_i(t_{ac_j}) * (P_i * \alpha_j)) + \sum_{j=1}^{N}(F_i(t_{dh_j}) * (P_i * \alpha_j)) \tag{6}$$

As funções $F_i(t_{ac_j})$ e $F_i(t_{dh_j})$ identificam a ausência de informações sobre uma técnica de AC e DH em ap_i. O valor da técnica sem informações multiplica o valor da probabilidade subjetivo proteger a rede. A soma dos valores referentes aos dois conjuntos resulta no total que representa a probabilidade subjetiva das técnicas sem informações.

3.2. Classificação dos Pontos de Acesso

O valor do CR é o principal critério para classificação. O SDHet assume que é mais importante a presença de técnicas diferentes do que a quantidade de mecanismos de um mesma técnica em uma rede de acesso. Como as diferentes técnicas protegem aspectos diferentes da confidencialidade, quanto mais técnicas presentes na rede menor o risco para o dispositivo. O número de mecanismos de uma mesma técnica é usado como um fator

de desempate. Os APs podem possuir o mesmo valor de risco à confidencialidade devido ao número limitado de técnicas. A quantidade de mecanismos de um mesma técnica age como um ponderador que diminui o impacto do risco oferecido pelas redes. Quanto mais mecanismos de uma mesma técnica, menor o valor do risco. O nível de possibilidade determina o impacto da incerteza na decisão. Este valor representa a insegurança ao se escolher uma rede com falta de informações. Ele pondera positivamente o risco à confidencialidade apresentado por uma rede e age como um fator de desempate.

$$N_c(ap_i) = RC_{(ap_i)} - (L_c(ap_i) - L_p(ap_i)) \tag{7}$$

A Equação 7 determina o valor classificatório de uma rede de acesso, considerando o risco à confidencialidade e os fatores de impacto de confiança. Nesta equação N_c corresponde ao nível de confidencialidade da rede ap_i. A diferença entre o nível de confiança L_c e o nível de possibilidade L_p subtrai o valor do risco à confidencialidade CR da rede ap_i. O resultado é então ordenado do menor para o maior, sendo que quanto menor o valor classificatório, menor os fatores de risco e de possibilidade, impactando na melhor rede a ser selecionada. Caso o nível de possibilidade da existência das informações (L_p) seja maior que o nível de confiança nas informações (L_c), o valor classificatório tende a aumentar. Caso contrário, este valor tende a diminuir, enfatizando o menor risco apresentado pelo ponto de acesso.

4. Avaliação

O SDHet foi implementado no simulador NS3 com base nos módulos existentes de WiFi, de LTE e no MIHF (do inglês Media *Indepedent Handoff Function*). Os módulos de WiFi e LTE fornecem as plataformas para a criação dos ambientes de redes heterogêneas. O MIHF proporciona a intercomunicação entre redes WiFi e LTE e os mecanismos para transição vertical. A implementação do MIHF utilizada foi desenvolvida por [Salumu Munga 2014] e não possui um módulo de decisão. Assim, um módulo de classificação e escolha de HetNets foi criado para coordenar o processo de decisão, implementando o SDHet. Além disso, o método proposto por Li e Cheng [Li and Chen 2013], chamado de MLC, foi também implementado no NS3 para comparação com o SDHet. Ele foi escolhido por empregar uma função objetivo que é a mesma técnica utilizada pelo SDHet.

Os cenários usados na avaliação consideram dois ambientes: local e metropolitano. Cada cenário possui propriedades específicas de mobilidade do nó móvel e do número de redes com áreas de cobertura sobrepostas. O ambiente local corresponde a um cenário de 30mx40m de área onde a variação de velocidade representa um pedestre que se move a aproximadamente $1,5m/s$ [Zinonos et al. 2013]. O número de redes sobrepostas neste cenário corresponde a uma rede WiFi e uma rede LTE. O ambiente metropolitano corresponde a um cenário urbano em uma área de 400mx400m representando o caminho que um usuário móvel faz quando se locomove de casa até o trabalho [Vegni and Natalizio 2014]. A velocidade do nó móvel representa a de um veículose movimentando a aproximadamente $11.5m/s$. O número de redes sobrepostas corresponde a 20 redes, onde 16 delas são WiFi e 4 são LTE distribuídas em uma área de 400mx400m. O padrão de mobilidade é aleatório, baseado em [Jailton et al. 2013].

Os pontos de acesso (APs) em cada cenário foram agrupados respeitando três configurações de sobreposição de área de cobertura, conforme [Zinonos et al. 2013]: *sobreposição baixa, média* e *alta*. A baixa sobreposição ocorre quando há de 2 a 4 APs cobrindo a mesma área. A média sobreposição quando há uma variação de 5 a 10 APs sobrepostos. A alta sobreposição representa um número de redes maior que 10 APs em uma mesma região. O ambiente local possui somente a baixa sobreposição. O ambiente urbano possui áreas onde a proporção vária entre baixa, média e alta. Os agrupamentos são distribuídos aleatoriamente pelos cenários [Vegni and Natalizio 2014]. Os APs WiFi foram configurados com um raio de alcance de 70m, os APs LTE foram ajustados para cobrir totalmente a área de cada cenário.

O SDHet analisa as propriedades de força de sinal (RSS do inglês, *Radio Signal Strenght*) e de confidencialidade (técnicas de controle de acesso e ocultação da informação) dos APs para classificação das redes e indicação ao *handoff*. O RSS é medido a cada 2 segundos para garantir que o nó não fique sem conectividade e determinará necessidade de transição e execução o método. Ademais, a detecção de um AP que ainda não teve o risco à confidencialidade avaliado também aciona o SDHet. Desta forma, sempre que uma de rede acesso desconhecida pelo nó móvel surge, o método infere o seu valor do risco à confidencialidade. A Tabela 1 resume os parâmetros dos cenários avaliados.

Tabela 1. Parâmetros da simulação do método de tomada de decisão

Parâmetros	**Valores**	
Áreas	Local	$30m$x$40m$
	Urbano	$400m$x$400m$
Sobreposição	Baixa	2-4 Redes
	Média	5-10 Redes
	Alta	¡10 Redes
Tecnologia	WiFi	70 m^2
	LTE	1500 m^2
Velocidade	1 m/s; 11.5 m/s	
Critérios de decisão	RSS	
	Risco à confidencialidade	

Os APs possuem duas configurações quanto à segurança: Baixo Risco à Confidencialidade (LCR) e Alto Risco à Confidencialidade (HCR). A LCR configura os pontos de acesso com mecanismos de controle de acesso e de ocultação de informação que tentam garantir a confidencialidade das comunicações. A HCR configura cada pontos de acesso 30 % a menos do número de mecanismos de confidencialidade que a LCR e com 30% a mais para o valor RSS. O número de pontos de acesso do tipo ARC é 30% do número total de pontos de acesso em cada cenário. Desta forma, os cenários representam situações de risco em que o dispositivo móvel pode tomar decisões prejudiciais.

Tabela 2. Associação das técnicas de confidencialidade com os mecanismos

Controle de Acesso			**Ocultação a Informação**	
Autenticação	*Autorização*	*Filtragem*	*Criptografia*	*Esteganografia*
Senha	Acordo de confiança	Firewall de rede	Hash	Salto de freq.
Cartão de acesso	Tokens	Detecção intrusão	Simétrica	Watermarking
Digitais	Com base em atributos	Proxy	Assimétrica	Fingerprinting
Assinatura	Com base em compor.	Captcha	Curva elíptica	Ocultar eco

O SDHet não verifica a eficiência e a eficácia das técnicas de confidencialidade,

mas sim o número de mecanismos que as utilizam. O número de mecanismos de confidencialidade definidos na LCR e HCR variam entre 0 (nenhum mecanismo daquele tipo) e 4 (até quatro mecanismos de um mesmo tipo) para cada técnica (autenticação, autorização, filtragem, criptografia, etc.). Esta variação foi definida com base na quantidade de mecanismos, que aplicam alguma técnica de confidencialidade, presentes na literatura [Stamp 2011, Pfitzmann 1996, Cacciaguerra and Ferretti 2003]. Este parâmetro pode ser variado conforme o contexto ou a necessidade da avaliação. Nesta avaliação, o número total de mecanismos de uma mesma técnica foi limitado para quatro. A Tabela 2 apresenta a associação das técnicas com exemplos dos seus respectivos mecanismos.

O SDHet e o MLC foram avaliados através de três métricas de eficácia e uma de eficiência. As métricas de eficácia correspondem a acurácia da seleção de redes confidenciais (**CNSA**), impacto do método na confidencialidade das transmissões (**TCI**) e exatidão dos valores classificatórios inferidos (**CVT**) para a confidencialidade. A métrica CNSA foi inspirada em [Aliakbary et al. 2015] e avalia o número de vezes em que o SDHet seleciona o ponto de acesso com maior nível de confidencialidade. Ela representa a confiabilidade do método nas decisões pelo nível de confidencialidade das redes. A métrica TCI verifica o impacto do uso do SDHet para selecionar pontos de acesso com confidencialidade nas suas transmissões. A métrica CVT afere o efeito da falta de informações na inferência dos valores dos níveis de confidencialidade pelo SDHet em comparação com os valores reais nas redes [Swartz and Joshi 2014]. A avaliação de eficiência usou a métrica de velocidade de decisão (**DV**), que averígua o tempo necessário para classificação e escolha da rede com maior confidencialidade [Bisio et al. 2014]. Está métrica determina se o tempo de uma decisão é suficiente para não afetar o processo de transição. Os resultados apresentados são a média de 30 simulações e um intervalo de confiança de 95%.

4.1. Resultados

A CNSA afere a eficácia das decisões quanto a escolha da rede menos arriscada com base no nível de confidencialidade de cada uma. Esta métrica representa a precisão do SDHet ao escolher a rede de acesso com maior confidencialidade. Ela foi aferida para o SDHet em comparação com o MLC nos dois cenários definidos.A Figura 3 mostra a acurácia alcançada pelo SDHet e o MLC nos cenários propostos. O SDHet obteve 100% de acurácia ao selecionar as redes de acesso de maior confidencialidade. Isto ocorreu porque ele avalia as propriedades de confidencialidade de cada ponto de acesso, permitindo a inferência com precisão do valor do risco à confidencialidade de cada ponto. Logo, a quantidade de redes em cada decisão não tem impacto sobre a acurácia das escolhas. Já o MLC obteve taxas de acerto menores, pois ele não separa as diferentes propriedades da segurança no processo de escolha, prejudicando a acurácia. Assim, quanto maior o numero de redes menor a acurácia do MLC.

O impacto do SDHet na confidencialidade das transmissões pode ser verificado na Figura 4, que mostra o tempo de transmissão ocorrido através de redes com menor risco à confidencialidade. Esta figura refere-se a uma amostra de tempo em cada cenário. Em comparação ao MLC, as escolhas do SDHet proporcionam um menor risco à confidencialidade nas transmissões do dispositivo. Este comportamento porque o SDHet seleciona as redes que possuem uma maior quantidade de técnicas de confidencialidade, diferenciando com maior precisão as redes que podem expor as transmissões do dispositivo móvel. Por outro lado, o efeito ping-pong, caracterizado por sucessivas transições com poucos se-

gundos de intervalo, pôde ser observado no cenário urbano atráves do número de trocas entre os pontos de acesso com poucos segundos de intervalo. Isto ocorre devido ao maior número de pontos de acesso ao alcance do dispositivo móvel e da falta de um mecanismo que determine a necessidade de transição.

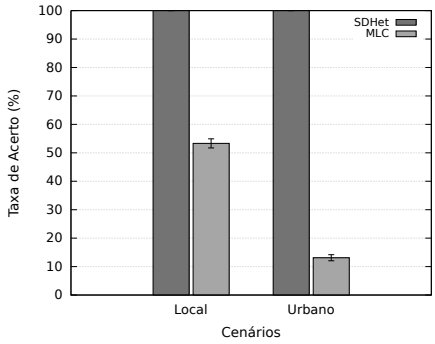

Figura 3. Comparação da Acurácia das Decisões dos Métodos

A avaliação da acurácia do SDHet quanto a falta de informações dos critérios de decisão foi realizada pela métrica CNSA variando a quantidade de critérios sem informações (NUC). O número de vezes em que o método escolhe a rede com menor risco, levando em consideração a falta de informações a respeito de algum critério, representa a acurácia do método em situações adversas nas quais existem incertezas nas medições. A Figura 5(a) mostra as taxas de acerto do método quanto a variação do NUC.

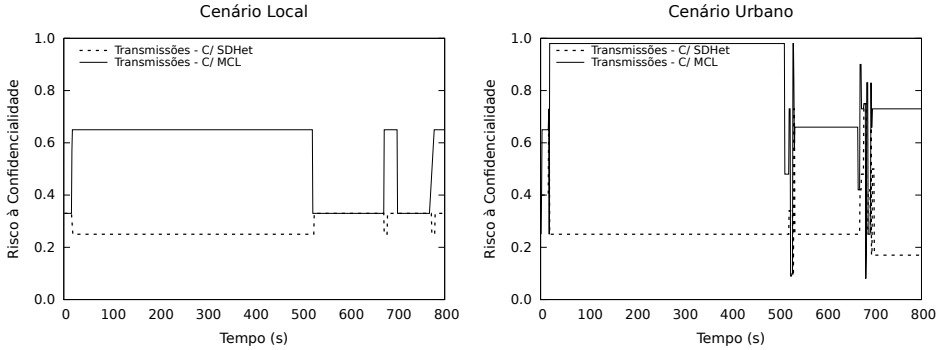

Figura 4. Impacto das Decisões na Confidencialidade das Transmissões

O SDHet apresenta uma variação na taxa de acerto conforme o NUC aumenta. Quanto maior o NUC, maior o erro na inferência do nível de confidencialidade das redes. Como as decisões tem como base as informações coletadas sobre o número de mecanismos de confidencialidade em cada rede, a falta dessas informações prejudica a acurácia do SDHet. Apesar de a precisão ser afetada, o que era esperado, o método mantém suas operações mesmo quando ocorre a falta de todas as informações necessárias para o seu funcionamento. O resultado são escolhas que consideram a rede menos arriscada e com o maior número critérios conhecidos. Além do número de NUCs, a quantidade de redes disponíveis para analise também influencia a acurácia do SDHet. Quanto mais redes, maior probabilidade de erro na seleção. Isto ocorre devido a falta de informações que

causa a imprecisão das inferências do SDHet. Com o maior número de redes com valores imprecisos, maior a probabilidade de selecionar as redes que não sejam as de maior confidencialidade que estejam ao alcance.

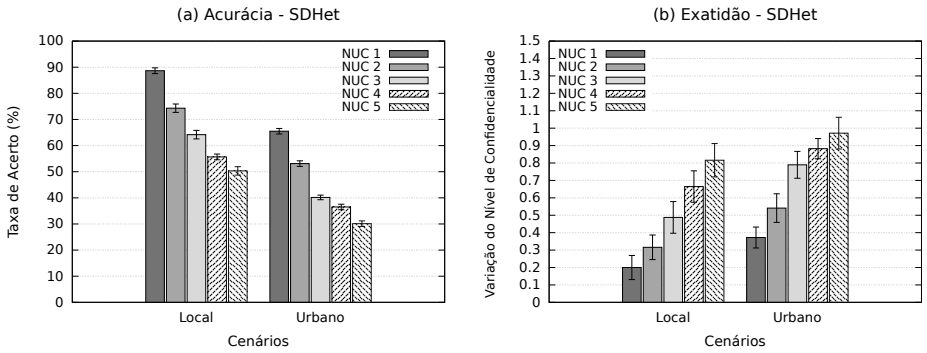

Figura 5. Acurácia e Exatidão das Decisões com Ausência de Informações

A Figura 5(b) mostra a diferença entre os valores do nível de confidencialidade calculados pelo SDHet com a variação dos NUCs em comparação com os valores realmente existentes nas redes, variando o número de critérios sem informações. Conforme o NUC cresce a diferença entre os valores também cresce, resultando em escolhas imprecisas. Apesar das escolhas não serem ótimas (a rede real de maior confidencialidade), o SDHet seleciona a rede com maior confiabilidade no valor calculado. Os resultados mostram escolhas por redes com o nível de confidencialidade próximo ao nível das rede com maior confidencialidade. Este comportamento se deve a escolha realizada com base na probabilidade de ocorrer a exposição das comunicações e da confiança no valor calculado. A quantidade de critérios sem informação gera um impacto negativo na exatidão das inferências do SDHet.

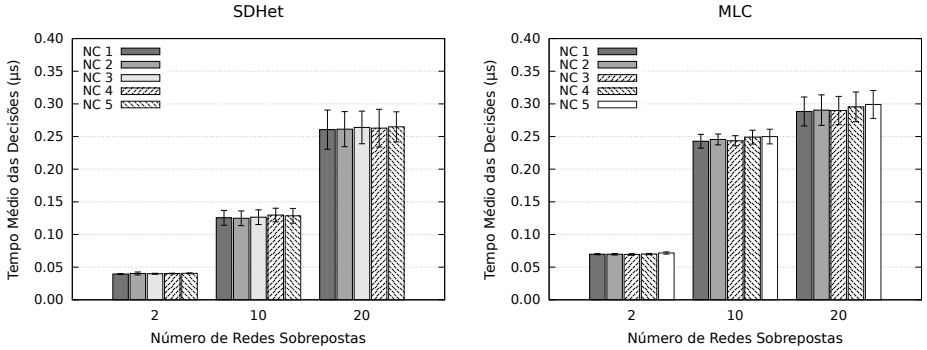

Figura 6. Comparação das Velocidades das Decisões

A avaliação do tempo de decisão verifica a eficiência do método em classificar os pontos de acesso pelo nível de confidencialidade e determinar aquele que oferece o menor risco de exposição das transmissões. Esta métrica determina se as decisões ocorrem em tempo hábil para a transição do nó móvel. Se o grau de mobilidade do dispositivo for alto e o processo de decisão levar muito tempo para avaliar os pontos de acesso, o dispositivo corre o risco de transitar para uma rede que está fora de alcance quando o processo

termina. Por este motivo, o tempo de decisão deve ser adequado ao *handoff* para evitar escolhas inapropriadas ou falhas na transição.

O tempo de decisão foi aferido em dois casos distintos: variando o número de critérios de decisão avaliados simultaneamente e variando o número de redes avaliadas simultaneamente. Os resultados no gráfico da Figura 6 indicam uma pequena variação nos tempos das decisões quando a quantidade de critérios varia. Isto significa que o número de critérios de decisão interfere de maneira pouco significativa no tempo de decisão. Em comparação com a variação do número de redes, os resultados mostram uma variação maior nos tempos de decisões entre as sobreposições de baixa, média e alta proporção. Isto significa que o número de redes para comparação influencia o tempo de decisão significativamente, onde, quanto maior o número de redes para coletar e analisar as informações maior o tempo gasto. Estes resultados comprovam a eficiência do método e seu impacto insignificante para o tempo de transição total do *handoff*, considerando a variação de mobilidade e de sobreposição de redes definidas nos cenários.

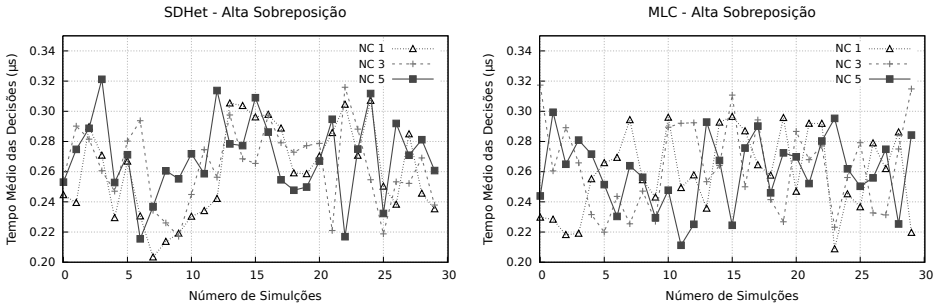

Figura 7. Variação das Velocidades das Decisões (Alta Sobreposição)

A Figura 7 mostra uma comparação da variação dos tempos de decisão para o cenário com alta sobreposição de redes. Ambos os métodos obtiveram um comportamento variável na escala de microssegundos para o tempo médio gasto por decisões. Isto ocorre porque se mede o tempo em função da avaliação dos critérios e da inferência dos valores classificatórios. Apesar dos valores variarem de simulação para simulação, o impacto desta variação é insignificante no tempo total do *handoff*.

5. Conclusão

O processo de decisão na transição entre HetNets demanda por segurança para evitar a perda de conectividade, bem como a exposição das transmissões dos dispositivos. O método SDHet colabora nas decisões de transições baseado em propriedades de confidencialidade e tempo hábil de escolha de rede. Os resultados obtidos sob diferentes cenários de HetNets mostram os ganhos de conectividade e segurança obtidos pelos dispositivos móveis ao considerar os aspectos de segurança de forma separada na transição entre redes.

Referências

Ahmed, A., Boulahia, L. M., and Gaïti, D. (2014). Enabling vertical handover decisions in heterogeneous wireless networks: A state-of-the-art and a classification. *Communications Surveys & Tutorials, IEEE*, 16(2):776–811.

Aliakbary, S., Motallebi, S., Rashidian, S., Habibi, J., and Movaghar, A. (2015). Noise-tolerant model selection and parameter estimation for complex networks. *Physica A: Statistical Mechanics and its Applications*, 427:100–112.

Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on*, 1(1):11–33.

Bakmaz, B., Bojkovic, Z., and Bakmaz, M. (2012). Traffic parameters influences on network selection in heterogeneous wireless environment. In *Systems, Signals and Image Processing (IWSSIP), 2012 19th International Conference on*, pages 292–295. IEEE.

Beresford, B. and Sloper, P. (2008). *Understanding the dynamics of decision-making and choice: A scoping study of key psychological theories to inform the design and analysis of the Panel Study*. Social Policy Research Unit, University of York York.

Bisio, I., Braccini, C., Delucchi, S., Lavagetto, F., and Marchese, M. (2014). Dynamic multi-attribute network selection algorithm for vertical handover procedures over mobile ad hoc networks. In *Communications (ICC), 2014 IEEE International Conference on*, pages 342–347. IEEE.

Cacciaguerra, S. and Ferretti, S. (2003). Data hiding: steganography and copyright marking. *Department of Computer Science, University of Bologna, Italy. http://www.cs.unibo.it/-people/phdstudents/scacciag/home/files/-teach/datahiding. pdf*, page 12.

Cavalcanti, D., Agrawal, D., Cordeiro, C., Xie, B., and Kumar, A. (2005). Issues in integrating cellular networks wlans, and manets: a futuristic heterogeneous wireless network. *Wireless Communications, IEEE*, 12(3):30–41.

Erews, J. G. (2013). Seven ways that hetnets are a cellular paradigm shift. *Communications Magazine, IEEE*, 51(3):136–144.

Jailton, J., Carvalho, T., Valente, W., Natalino, C., Frances, R., and Dias, K. (2013). A quality of experience handover architecture for heterogeneous mobile wireless multimedia networks. *Communications Magazine, IEEE*, 51(6):152–159.

Kahneman, D. and Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, pages 263–291.

Khanum, S. and Islam, M. M. (2014). An enhanced model of vertical handoff decision based on fuzzy control theory & user preference. In *Electrical Information and Communication Technology (EICT), 2013 International Conference on*, pages 1–6. IEEE.

Li, X. and Chen, R. (2013). Adaptive vertical handover algorithm based on user experience for heterogeneous network.

Ma, B., Liao, X., and Xie, X. (2012). Risk-aware vertical handoff algorithm for security access support in heterogeneous wireless networks. In *Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on*, pages 1515–1519. IEEE.

Martinez-Morales, J. D., Pineda-Rico, U., and Stevens-Navarro, E. (2010). Performance comparison between madm algorithms for vertical handoff in 4g networks. In *Electrical Engineering Computing Science and Automatic Control (CCE), 2010 7th International Conference on*, pages 309–314. IEEE.

MELO, R. G., SANTOS, A., NOGUEIRA, M., and MEDHI, D. (2013). Modelagem e projeto de redes sem fio heterogêneas resilientes e sobreviventes. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 31:01–50.

Nasser, N., Guizani, S., and Al-Masri, E. (2007). Middleware vertical handoff manager: A neural network-based solution. In *Communications, 2007. ICC'07. IEEE International Conference on*, pages 5671–5676. IEEE.

Pfitzmann, B. (1996). Information hiding terminology-results of an informal plenary meeting and additional proposals. In *Proceedings of the First International Workshop on Information Hiding*, pages 347–350. Springer-Verlag.

Pfleeger, S. L. (2012). Security measurement steps, missteps, and next steps. *IEEE Security & Privacy*, 10(4):0005–9.

Rajule, N., Ambudkar, B., and Dhee, A. (2013). Survey of vertical handover decision algorithms. *Inter. Journal of Innovations in Engineering and Tech*, 2(1):362–368.

Rao, K., Bojkovic, Z. S., and Bakmaz, B. M. (2013). Network selection in heterogeneous environment: A step toward always best connected and served. In *Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference on*, volume 1, pages 83–92. IEEE.

Salumu Munga (2014). Overview. Data de acesso: Nov. 2014.

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Swartz, C. and Joshi, A. (2014). Identification in encrypted wireless networks using supervised learning. In *Military Communications Conference (MILCOM), 2014 IEEE*, pages 210–215. IEEE.

Triola, M. F. et al. (2005). *Introdução à estatística*, volume 10. Ltc Rio de Janeiro.

Vegni, A. M. and Natalizio, E. (2014). A hybrid (n/m) cho soft/hard vertical handover technique for heterogeneous wireless networks. *Ad Hoc Networks*, 14:51–70.

Zekri, M., Jouaber, B., and Zeghlache, D. (2012). A review on mobility management and vertical handover solutions over heterogeneous wireless networks. *Computer Communications*, 35(17):2055–2068.

Zinonos, Z., Vassiliou, V., and Chrysostomou, C. (2013). Handoff triggering for wireless sensor networks with performance needs. In *Computers and Communications (ISCC), 2013 IEEE Symposium on*, pages 000982–000988. IEEE.