ALISSON A. PUSKA

DECISÃO NO HANDOFF VERTICAL CIENTE DA CONFIDENCIALIDADE DAS REDES DE ACESSO

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador:Prof.Aldri Luiz dos Santos
Coorientadora:Profa. Michele Nogueira Lima

CURITIBA

2015

ALISSON A. PUSKA

DECISÃO NO HANDOFF VERTICAL CIENTE DA CONFIDENCIALIDADE DAS REDES DE ACESSO

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador:Prof.Aldri Luiz dos Santos
Coorientadora:Profa. Michele Nogueira Lima

CURITIBA

2015

P987d

Puska, Alisson A.
Decisão no handoff vertical ciente da confidencialidade das redes de acesso/ Alisson A. Puska. – Curitiba, 2015.
75 f. : il. color. ; 30 cm.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em Informática, 2015.

Orientador: Aldri Luiz dos Santos – Co-orientador: Michele Nogueira Lima.
Bibliografia: p. 63-70.

1. Redes de computadores. 2. Processo decisório. 3. Incerteza - Modelos matemáticos. 4. Avaliação de riscos. 5. Confidencialidade. I. Universidade Federal do Paraná. II.Santos, Aldri Luiz dos. III. Lima, Michele Nogueira . IV. Título.

CDD: 004.6

Ministério da Educação
Universidade Federal do Paraná
Programa de Pós-Graduação em Informática

PARECER

Nós, abaixo assinados, membros da Banca Examinadora da defesa de Dissertação de Mestrado em Informática, do aluno Alisson Andrey Puska, avaliamos o trabalho intitulado, "Decisão no Handoff Vertical Ciente da Confidencialidade das Redes de Acesso", cuja defesa foi realizada no dia 21 de agosto de 2015, às 09:00 horas, no Departamento de Informática do Setor de Ciências Exatas da Universidade Federal do Paraná. Após a avaliação, decidimos pela:

(X)**aprovação** do candidato. ( )**reprovação** do candidato.

Curitiba, 31 de agosto de 2015.

Prof. Dr. Aldri Luiz dos Santos
PPGInf - Orientador

Prof. Dr. Michele Nogueira
PPGInf – Coorientadora

MINISTÉRIO DA EDUCAÇÃO - UNIVERSIDADE FEDERAL DO PARANÁ - Setor de Ciências Exatas - Coordenação de Pós-Graduação em Informática

Prof. Dr. Kelvin Lopes Dias
UFPE – Membro Externo

Prof. Dr. Mauro Sérgio Pereira Fonseca
UTFPR – Membro Interno

AGRADECIMENTOS

Gostaria de começar os agradecimentos pela minha família que sempre foram e serão minha fortaleza nos momentos de turbulência. Tenho muito orgulho e admiração por vocês. Obrigado por todo apoio e amor dedicados a mim.

Quero agradecer ao meu mentor Aldri Luiz dos Santos pelas orientações que me auxiliaram no caminho árduo de me tornar um mestre. Muito obrigado pela confiança (e paciência) depositados em mim. Agradeço a Michele Nogueira Lima pelos ensinamentos, esclarecimentos e pelos esforços dedicados ao meu aprimoramento.

Aos colegas de laboratório deixo aqui meu muito obrigado. Muito obrigado mesmo, pela parceria, amizade, descontração, zoeiras, geladas, pela erva mate, o café, os concelhos, modelos, metodologias, livros, artigos, ideias, exemplos e pela força. Ao Chicó (Danilo), A mi hermano de otra madre (Christian), ao Bulbasauro (Ricardo), ao George da Floresta (Cládio), Ao Filinho (Rodrigo), ao Robinho (Robson), ao Benê (Benevide), ao Ganso (Jefferson), Ao adi (Anonymous). Ao Meu Pupilo (Luiz), ao Grande Arthur, a Andressa, ao Otto "Machi..."(Otto), ao Rafael, ao Ursinho (Metuzalem), ao Cunhado (Renato Melo), ao Tio San (Santiago), ao Ivan e ao Edgar.

Brincadeiras a parte, vocês fizeram o meu caminhar mais leve nestes anos. Vou carregar um pedaço de vocês sempre. Aqueles que esqueci, me desculpem. Mas acreditem, todos que fizeram parte da minha vida durante os anos deste trabalho e me ajudaram a amadurecer eu sinto gratidão.

Agradeço a todos que me influenciaram direta e indiretamente durante estes dois anos e meio. Muito obrigado pela paciência e compreensão nos momentos de stress. Pela mão firme nas horas de insegurança. Pelos ouvidos nos momentos de desabafo, reclamação e cansaço extremo. Agradeço as palavras de sabedoria, os conselhos que perdi na confusão do caminho, mas que ei de reencontrá-los. Deixo aqui meu humilde muito obrigado, na certeza de que sem vocês não chegaria até aqui.

RESUMO

A diversidade das tecnologias de comunicação sem fio existentes e o constante aumento do número de pontos de acessos resultaram em ambientes repletos de redes sem fio com diferentes características de desempenho e segurança. Estes avanços, em conjunto com o desenvolvimento de dispositivos móveis com mais de uma interface para comunicação sem fio e a proliferação do uso da comunicação no dia a dia das pessoas, instigaram o desenvolvimento da interoperabilidade entre as diferentes tecnologias. A interoperabilidade tem como objetivo alcançar maiores áreas de cobertura, melhorar a qualidade dos serviços oferecidos para o usuário, bem como mantê-lo conectado em todo lugar e a todo momento, resultando no paradigma das redes heterogêneas. Este novo paradigma demanda o gerenciamento da mobilidade do usuário para manter a sua conectividade, transferindo a conexão do dispositivo móvel quando necessário e sem perdas nos serviços. Este processo é chamado de *handoff* em redes heterogêneas e depende da escolha automática de um ponto de acesso adequado às necessidades do usuário móvel. Com esta finalidade, vários métodos de decisão propostos na literatura avaliam as características de desempenho, qualidade de serviço e segurança das redes de acesso para classificá-las de acordo com estes conjuntos de propriedades. Entretanto, os métodos encontrados na literatura analisam a segurança de maneira genérica, ignorando os aspectos distintos de suas propriedades de confidencialidade, integridade e disponibilidade. Este problema pode gerar decisões inadequadas e que colocam o usuário em risco, como quando o dispositivo requer confidencialidade nas transmissões e o processo de decisão seleciona uma rede cuja à segurança se refere à disponibilidade das transmissões, conectando-o a uma rede inadequada. Além disso, nenhum método considera a falta de informações a respeito dos critérios de comparação na escolha dos pontos de acesso, o que diminui a precisão das decisões, levando a escolhas inadequadas ou até falhas do processo de transição. Portanto, este trabalho apresenta um método de decisão, chamado SDHet, que seleciona a rede de acesso com base no seu nível de confidencialidade. Ele é inspirado na teoria da prospecção, que modela a tomada de decisão por seres humanos quando em risco e falta de informações, para selecionar as redes quando nestas situações. O SDHet foi avaliado através de simulações e os resultados mostram a sua eficácia em escolher as redes considerando o nível de confidencialidade e a falta de informações dos critérios de comparação. Além disso, a utilização do método não interfere de maneira significativa no desempenho do processo de transição.

Palavras-chave: Redes Heterogêneas, *handoff*, método de decisão, teoria da prospecção, análise de risco, confidencialidade.

ABSTRACT

The diversity of wireless communication technologies and the steady increase in the number of access points resulted in full of wireless networks with different performance characteristics and safety environments. This advances, together with the development of mobile devices with more than one interface for wireless communication and the proliferation of the use of communication in day-to-day lives instigated the development of interoperability between different technologies. The interoperabolity aims to achieve greater coverage areas, improve the quality of services offered to the user, as well as keep him connected everywhere and at all times resulting in the paradigm of heterogeneous networks. This new paradigm provides the mobility management for the user to maintain its connectivity, transferring the mobile connection when required and no with loss in service. This process is called vertical handoff and depends on the automated choice of a suitable access point for user needs. To this end, various decision methods proposed in the literature evaluate performance characteristics, quality of service and safety of access networks to classify them according to these sets of properties. However, the methods in the literature analyze the safety of the networks in a generic way, ignoring the different aspects of their confidentiality, integrity and availability properties. This problem can lead to inappropriate decisions and put the user at risk, such as when the device requires confidentiality in transmissions and the decision making process selects a network whose security criteria refers to the availability of transmissions. Furthermore, no method considers the absence of information about the comparison criteria in the choice of access points, which decreases the accuracy of the decisions, leading to inappropriate choices or to the transition faults. Therefore, this paper presents a decision method, called SDHet, which selects the access network based on their level of confidentiality. He is inspired by the prospect theory, modeling decision making by humans when at risk and lack of information, to select the networks on these situations. The SDHet method was evaluated through simulation and the results shows its effectiveness in choosing the networks considering the level of confidentiality and the lack of information of the comparison criteria. Furthermore, the use of the method does not interfere significantly the performance of the transition.

Keywords: Heterogeneous networks, handoff, decision method, prospect theory, risk analysis, confidentiality.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

QoS	Quality of Service
HetNet	Heterogeneous Network
AP	Access Point
MD	Mobile Device
ABC&S	Always Best Connected and Served
MADM	Multi Attribute Decision Method
SAW	Simple Addictive Weighting
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
MEW	Multiplicative Exponent Weighting
AHP	Analytic Hierarchy Process
OF	Objective Function
AI	Artificial Intelligence
LOS	Level Of Security
RSS	Radio Signal Strength
SINR	Signal to Interference plus Noise Ratio
MIH	Midia Independent Handover
CR	Confidentiality Risk
AC	Access Control
DH	Data Hiding
LP	Level of Possibility
LC	Level of Confidence
CR	Confidentiality Risk
MIHF	Midia Independent Handover Function
LCR	Low Confidentiality Risk
HCR	High Confidentiality Risk
ASRC	Acurácia da Seleção de Redes Confidenciais
IMCT	Impacto do Método na Confidencialidade das Transmissões
VD	Velocidade de Decisão
NUC	Number of Unknown Criteria
NC	Número de Critérios
MLC	Método de Decisão Le e Cheng

NOTAÇÃO

N	Conjunto de pontos de acessos
ap	Ponto de acesso
ID	Identificador do ponto de acesso
AC	Conjunto de técnicas de controle de acesso
IO	Conjunto de técnicas de ocultação de informação
n_{ac}	Quantidade de técnicas de controle de acesso analisadas
n_{io}	Quantidade de técnicas de ocultação de informação analisadas
t_{ac}	Quantidade de mecanismos de uma técnica de controle de acesso
t_{io}	Quantidade de mecanismos de uma técnica de ocultação de informação
k	Total de técnicas de confidencialidade consideradas
R_c	Risco à confidencialidade
L_c	Nível de confiança
L_u	Nível de incerteza
α	valor ponderativo corresponde ao elemento
P_e	Probabilidade subjetiva inicial de exposição das transmissões
V_{at}	Valor da probabilidade dos mecanismo ausentes no ponto de acesso
V_{pt}	Valor da probabilidade dos mecanismo presentes no ponto de acesso
$F_v()$	Função que determina as técnicas de CA e OI ausentes ou presentes
$F_v()$	Função que determina a quantidade de técnicas repetidas de CA e OI ausentes ou presentes
$F_u()$	Função que determina as técnicas de CA e OI sem informação
Nc	Valor classificatório
Tx_r	Taxa de acerto
NrA	Número de vezes em que se selecionou a rede de maior NC
N_rDecs	Número total de decisões
E	Número de simulações
V_nc	Variação do nível de Confidencialidade
$I_{sdhet}(NUC)$	NC inferido pelo SDHet com NUC
I_{valor_real}	NC inferido pelo SDHet sem NUC
T_m	Tempo médio
T_i	Tempo inicial de decisão
T_f	Tempo final de decisão

CAPÍTULO 1

INTRODUÇÃO

O constante desenvolvimento das tecnologias de comunicação sem fio e o aumento no número de usuários com intensa demanda pela melhor conexão instigaram uma mudança de paradigma na forma como as redes de comunicação são implantadas [1]. Este novo paradigma prevê a interoperabilidade entre 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 (APs, do inglês, *Access Point*). A interação entre diferentes tecnologias de comunicação sem fio permite a integração de redes heterogêneas sem fio com características distintas de Qualidade de Serviço (QoS, do inglês, *Quality of Service*), desempenho e segurança.

As redes heterogêneas sem fio (HetNets, do inglês, *Heterogeneous Networks*) representam a convergência de tecnologias de comunicação diferentes e a integração de domínios de redes diferentes [2]. Elas são compostas por dispositivos móveis, pontos de acesso (APs, do inglês, *Access Points*) e redes centrais que interagem com o objetivo de satisfazer o usuário final [3]. Os dispositivos móveis (MD, do inglês, *Mobile Device*) como *smartphones*, *PDAs*, *tablets*, *notebooks*, entre outros, se conectam aos APs para usufruir de serviços da rede central ou obter conectividade com a internet. Juntamente com as redes centrais, os APs possuem características como área de cobertura, qualidade do sinal, largura de banda, entre outras, que variam conforme a tecnologia empregada pela rede. Estas redes podem atender as necessidades dos MDs que variam dependendo do tipo do dispositivo, do contexto e dos usuários. Assim, as HetNets tentam prover uma infraestrutura capaz de atender as distintas demandas dos usuários.

As HetNets preveem mecanismos para gerenciamento da mobilidade dos dispositivos. Por exemplo, os mecanismos de detecção dos APs 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, possibilitam a manutenção da conectividade do MD quando necessário [4]. Esta manutenção ocorre por diferentes motivos, como a degradação na qualidade da conexão atual ou a detecção de um ponto de acesso com melhor capacidade de atender a demanda do dispositivo móvel. Neste ambiente ímpar, o gerenciamento de mobilidade realiza a manutenção da conectividade do dispositivo, transferindo a conexão de maneira transparente para o usuário quando necessário.

Diversos serviços e aplicações se beneficiam com a integração das redes heterogêneas e os serviços de gerenciamento de mobilidade e conectividade. Por exemplo, os serviços de voz, videochamadas e *media streaming* em tempo real necessitam de alta largura de

banda, são sensíveis ao atraso fim-a-fim (*delay*) e ao atraso entre pacotes (*jitter*) [5]. Estes serviços, quando usados em dispositivos móveis como *smartphones*, podem usufruir de uma qualidade maior ao gerenciar a conectividade de maneira inteligente e adaptável e utiliza-los por mais tempo enquanto ele se move por diferentes redes. O acesso a *e-mails*, redes sociais, e outros serviços que necessitam de qualidade da conectividade e garantias na entrega pode ser feito de maneira inteligente, utilizando redes com menor largura de bande, menor custo e maior qualidade de conectividade. A melhor utilização de recursos e o aumento da qualidade de serviço e de experiência são algumas das vantagens de se gerenciar a mobilidade dos MDs.

Os mecanismos de gerenciamento de conectividade permitem a transferência da conexão do MD entre redes de acesso heterogêneas conforme a necessidade. Por redes de acesso entende-se o conjunto AP e sua rede central que fornecem serviços e conectividade para o MD. O serviço de *handoff* gerencia a transição entre as redes de acesso [6, 7]. A detecção de redes de acesso no ambiente [8], a determinação do momento correto para a transição [8], a aferição de suas características [9], a classificação e a escolha da rede de acesso à ser transferida a conexão do dispositivo móvel [10], são os principais desafios do *handoff* em HetNets [11]. A escolha de uma rede adequada para transferência da conexão é o ponto mais importante do processo de transição [10]. Este processo compara as redes disponíveis a fim de determinar uma rede adequada às necessidades do dispositivo móvel. A escolha acontece de forma automática e segue um método de decisão. A seleção dos critérios de decisão, a classificação da importância relativa à cada critério, o tempo de decisão e a eficácia das decisões estão entre os desafios de pesquisa do processo de decisão.

Os métodos de decisão objetivam melhorar o desempenho do processo de escolha, o que inclui otimizar o tempo e o uso de recursos utilizados nas decisões, e escolher a rede mais adequada a necessidade do dispositivo. Para isto, eles empregam estratégias como funções de minimização do custo, maximização da utilidade, inteligência artificial, cadeias de Markov, lógica difusa, entre outras, que comparam os critérios de escolha e classificam as redes de acesso [10, 12, 13]. Quanto menor o tempo gasto na decisão e maior a precisão das escolhas, melhor é o desempenho do método de decisão. Desta forma, cada técnica possui características específicas que as tornam interessantes para o seu emprego em métodos de decisão.

As decisões acorrem através de comparações das redes de acesso. As comparação são feitas pela analise de critérios que correspondem as características das redes de acesso. Dentro do grupo de características mais usadas como critérios de comparação, se destacam na literatura os que pertencem às classes de desempenho e QoS [10, 12, 11]. A classe de desempenho engloba critérios como área de cobertura, força do sinal de transmissão e qualidade do enlace estão entre os mais estudados desta classe. A largura de banda, capacidade de transmissão, *delay* e *jitter* encontram-se entre os critérios de QoS mais empregados nos métodos de decisão.

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 [10, 12, 11, 14]. 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. Neste exemplo, o dispositivo acredita estar protegido nas suas necessidades quando na verdade não está. Sendo assim, classificar os APs separando os princípios de segurança como critérios de decisão pode tornar a decisão mais inteligente e eficaz.

Uma forma de considerar a segurança de uma rede de acesso é a determinação do risco apresentado por ela [15]. A aferição do risco determina o quão segura uma rede é, e pode ser realizado considerando para cada um de seus princípios: confidencialidade, integridade e disponibilidade. A aferição do risco deve ser realizada para cada princípio individualmente, considerando suas propriedades específicas. Neste sentido, a mensuração do risco de segurança é essencial para a decisão entre redes de acesso heterogêneas, uma vez que isto representa a medida de um critério importante para a escolha. Medir o risco de segurança de uma rede aumenta a precisão no processo de decisão, diminuindo o número de escolhas por redes de acesso com potencial para prejudicar os usuários.

Outro aspecto não considerado pelos métodos encontrados na literatura é o impacto da falta de informações sobre o processo de escolha. As informações necessárias para tomada de decisão nem sempre podem estar disponíveis em um ambiente tão vulnerável a interferências como os das comunicações sem fio. A falta de informações prejudica o processo de decisão e diminui a precisão das escolhas [16]. Este é um ponto importante a ser considerado no processo de decisão, uma vez que em um ambiente onde redes de acesso sem fio com características distintas nem sempre as informações necessárias para a comparação estarão disponíveis.

Um modelo de decisão que considera a incerteza para efetuar escolhas é o modelo prospectivo [17]. A teoria da prospecção descreve um modelo de tomada de decisão que demonstra como seres humanos tomam decisões envolvendo risco e falta de informações. Desta forma, a adaptação deste modelo pode auxiliar o processo de decisão na transição em rede heterogêneas a escolher quando faltam informações dos critérios de comparação.

1.1 Motivação

O princípio da confidencialidade determina que a visualização de informações privadas deve ser feita somente por entidades autorizadas [18, 19]. No âmbito das comunicações sem fio, este princípio tem importância, visto que o meio de transmissão das informações é aberto e compartilhado, tornando fácil a visualização não autorizada das mensagens transmitidas. Certamente, considerar a confidencialidade oferecida pelas redes de acesso no processo de decisão do *handoff* em redes heterogêneas oferece benefícios ao usuário. Por exemplo, escolher uma rede que oferece confidencialidade aumenta as garantias de que os dados enviados por ela estão protegidos contra visualizações indevidas.

Alguns método de decisão encontrados na literatura definem a segurança como um critério importante para a comparação das redes de acesso no *handoff* em redes heterogêneas, porém desconsideram a complexidade deste critério na formulação dos métodos de decisão. Existem métodos que comparam somente as características de desempenho e QoS [20, 21] que são inadequados para as decisões que necessitam de segurança. Outros métodos tem como objetivo aperfeiçoar a eficiência do processo de decisão, diminuindo o tempo e o número de decisões através da variação do número, do peso e dos critérios [22, 23]. Nestes, a segurança é somente mencionada e não utilizada para seleções, além de a considerarem de forma simples, unificando suas propriedades. Alguns métodos resolvem o problema de determinar a importância da segurança ao compará-la com outros critérios [24, 25, 26], estudando a segurança de maneira superficial e sem considerar a falta de informações. Somente um método utiliza o risco de segurança apresentado pela rede de acesso para efetuar a escolha [27], porém não descreve como este risco é obtido, ou quais aspectos de segurança são considerados, além de não considerar a falta de informações.

A teoria da prospecção foi proposta na área da economia comportamental e define um modelo de tomada de decisão descritivo, o qual explica como seres humanos tomam decisões envolvendo risco e falta de informações [17, 28]. Este modelo avalia as consequências das alternativas em termos de ganhos e perdas e considera como o agente decisor (ser humano) age na presença de risco e incerteza (falta de informações). Assim, adaptar a análise subjetiva de riscos e incerteza para o processo de decisão automático (*handoff* em redes Heterogêneas) pode propiciar um comportamento adaptativo para o agente decisor, devido à subjetividade de suas decisões (ora buscando o risco, ora evitando), reduzindo o prejuízo e certificando-se do ganho nas escolhas do dispositivo.

Portanto, é necessário desenvolver um método de apoio a decisão no *handoff* em redes heterogêneas que considere de maneira adequada os aspectos de segurança das redes de acesso, em particular a confidencialidade na transmissão dos dados, buscando a autopreservação do anonimato e da privacidade do usuário. Sendo as características essenciais para a eficácia do processo de decisão a autopreservação, para evitar redes de acesso com potencial para expor as informações do usuário e, a autonomia para tomar decisões mesmo

quando faltam informações a respeito dos critérios de comparação.

1.2 Objetivos

Este trabalho tem como objetivo propor um método para auxiliar o processo de decisão no *handoff* em redes heterogêneas para escolha de redes de acesso com menor potencial de expor os dados privados do usuário. Para alcançar este objetivo, um método é proposto para determinar o nível de confidencialidade de cada rede disponível, suplementando as informações de desempenho e QoS comumente usadas para decisão. O método deve ser capaz de classificar as redes com base no valor da confidencialidade das comunicações de cada uma mesmo quando faltam as informações necessárias para o seu funcionamento.

O método proposto aplica a análise probabilística de risco para determinar o nível de confidencialidade apresentado por uma rede. Ele baseia-se na avaliação subjetiva dos mecanismos de confidencialidade nas redes de acesso para inferir um valor representativo através da observação da presença destes mecanismos. Desta forma, a presença dos mecanismos permite identificar o risco de confidencialidade apresentado por uma rede antes de utilizá-la ou escolhê-la.

A presença de mecanismos que aplicam estas técnicas determina o risco da quebra de confidencialidade na transmissão de mensagens em uma rede de acesso. O método não trata da detecção de atacantes ou da aferição da capacidade de um mecanismo de segurança em uma determinada rede, mas sim da possibilidade de ter a privacidade invadida ao utilizar uma rede de acesso para comunicação.

1.2.1 Contribuições

As contribuições deste trabalho são as seguintes:

- Um estudo sobre métodos de tomada de decisão na transição em redes heterogêneas que consideram a segurança como critério. O levantamento bibliográfico permitiu a classificação dos métodos em grupos, compreendendo diferentes abordagens do uso de segurança e de técnicas de decisão de multi atributos. Neste estudo foram levantados os requisitos para um método de tomada de decisão que quantifique o nível de segurança das redes de acesso a serem escolhidas e que consiga tomar decisões quando faltam informações a respeito dos critérios de escolha para transição em redes heterogêneas.

- A especificação e implementação de uma técnica para quantificação da confidencialidade apresentada pelas redes de acesso. Esta técnica determina o nível de confidencialidade de cada rede de acesso através da regra de probabilidade subjetiva, que considera as informações sobre os mecanismos de confidencialidade usados

nas redes para inferência do valor de tal nível. Ela possibilita a escolha de redes de acesso para transição da conectividade do nó móvel que sejam menos arriscadas a expor os dados privados do usuário.

- A especificação de uma técnica para efetuar escolhas quando faltam informações a respeito dos critérios usados na decisão. Tal técnica foi inspirada na teoria da prospecção, que determina como seres humanos tomam decisões na presença de risco e com fatores adversos como a falta de informações. Ela adapta as funções que ponderam o impacto do risco e o impacto do valor inferido para a probabilidade de ocorrência um evento, presentes na teoria da prospecção, em duas funções que ponderam o impacto da falta de informações e da confiança no valor de segurança calculado. Com estes fatores, a técnica utiliza a falta de informações, ponderando e selecionando as redes de acesso.

- A especificação e implementação de um método de apoio a decisão para escolha de redes que possuam menor risco a confidencialidade mesmo quando faltam informações para decisão adequada. O método emprega as duas técnicas explorando suas vantagens para analisar e inferir um valor classificatório para as redes de acesso.

- A avaliação do método proposto, no NS3, utilizando cenários baseados na literatura. Foi implementado um módulo específico para o método de decisão proposto, bem como para um outro método da literatura, para comparação de alguns aspectos de desempenho. Por fim, foi feita a análise dos resultados que estabeleceu padrões entre as métricas avaliadas e os parâmetros de simulação.

1.3 Estrutura da dissertação

Esta dissertação está organizada em cinco capítulos. O Capítulo 2 apresenta os fundamentos necessários ao entendimento da proposta, descrevendo as características gerais das redes heterogêneas, dos esquemas de decisão, da segurança e da teoria da prospecção. O Capítulo 3 apresenta vários trabalhos da literatura que tratam do processo de decisão no *handoff*, bem como trabalhos relacionados a quantificação da segurança. O Capítulo 4 detalha o método de apoio à tomada de decisão inspirado na teoria da prospecção considerando os riscos e as incertezas. O Capítulo 5 demonstra a avaliação do método e a discussão dos resultados. O Capítulo 6 conclui o trabalho, apresentando as considerações finais e atividades futuras.

CAPÍTULO 2

FUNDAMENTOS

Este capítulo apresenta os fundamentos necessários para o entendimento do contexto, do problema, bem como da proposta desenvolvida neste trabalho. A Seção 2.1 descreve as características gerais das redes heterogêneas sem fio e do processo de *handoff* entre as redes, especificando a fase de decisão. A Seção 2.3 introduz os princípios de segurança importantes para transição entre redes. A Seção 2.4 apresenta a teoria da prospecção e as características relevantes do modelo de decisão prospectivo.

2.1 Redes heterogêneas sem fio

As HetNets representam uma mudança de paradigma na operação das redes de telecomunicações atuais [1]. Este paradigma compreende a integração entre redes de comunicação sem fio com diferentes características, por exemplo, área de cobertura, segurança, qualidade de serviço, largura de banda, custo e tecnologia [29]. Esta integração proporciona uma melhor capacidade e cobertura dos sistemas de comunicação, atendendo a crescente demanda do usuário móvel por melhores conexões.

As redes heterogêneas sem fio são compostas basicamente por estações móveis (MDs), APs (estações base ou pontos de acesso) e uma rede central [3]. Os dispositivos móveis possuem diferentes níveis de mobilidade, além de uma ou mais interfaces de comunicação que suportam uma ou mais tecnologias de acesso ao meio (3G, 802.11, etc.). Os APs gerenciam os recursos (largura de banda, QoS, entre outros) usados por um dispositivo móvel e são responsáveis pela entrada deles na rede. A rede central proporciona a conectividade com a Internet e representa o *backbone* para os pontos de acesso. As estações móveis se conectam a rede central por meio de um AP (modo infraestruturado) ou através de outra estação móvel (modo ad hoc). A Figura 2.1 ilustra um cenário com a disposição destes componentes.

O modelo de redes heterogêneas sem fio prevê a interoperabilidade entre redes distintas. Esta interoperabilidade consiste na interação entre redes e tecnologias heterogêneas através da definição de padrões, procedimentos, políticas e regras que possibilitam a comunicação entre as redes (operadoras e sistemas diferentes) e as tecnologias (*WiFi*, *LTE*, *Bluetooth*, etc.) [30, 31]. Isto permite que sistemas de telecomunicação heterogêneos troquem informações e otimizem a utilização de seus recursos ao gerenciarem a mobilidade do usuário móvel.

A interação entre redes heterogêneas permite estender a funcionalidade de gerenciamento da conexão de uma estação móvel para além da rede em que se encontra conec-

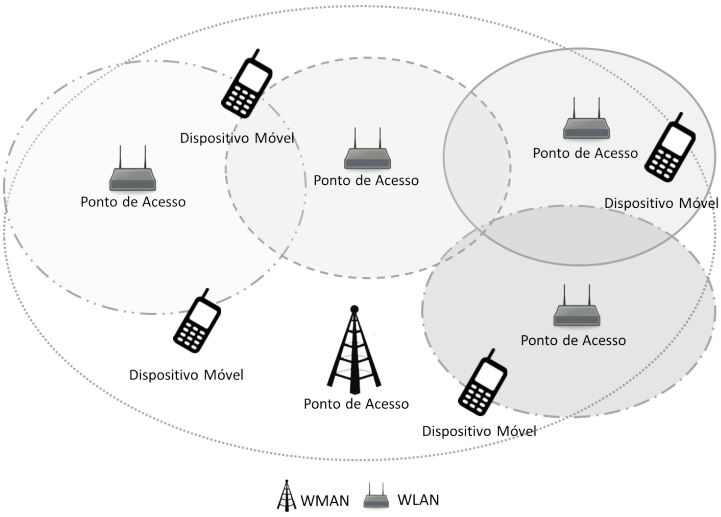

Figura 2.1: Exemplo de cenário de uma HetNet

tada [32]. O gerenciamento da conexão em HetNets garante a continuidade da conectividade de uma estação móvel com um determinado destino enquanto transita por uma área com redes de diferentes tecnologias e coberturas. Este processo transfere as rotas dos pacotes e a ligação do dispositivo móvel entre os diferentes APs disponíveis no meio quando necessário. O procedimento de transferência de conexão é conhecido como **processo de transição ou *handoff*** e acontece de modo transparente para o usuário, sem perdas no serviço. Portanto, um usuário móvel em uma rede celular (3G) assistindo a um vídeo ao vivo da Internet em seu *smartphone* migra automaticamente para um AP de uma rede local (WiFi) com mais recursos e sem custos, sem perdas no serviço.

2.1.1 Transição em redes heterogêneas

O objetivo do processo de transição reside no paradigma "Sempre Melhor Conectado e Servido" (ABC&S, do inglês, *Always Best Conected & Served*). Este paradigma define que além do usuário desejar a conectividade ubíqua, ele deseja se conectar a tecnologia de acesso disponível mais adequada às suas necessidades [4]. Desta forma, o processo de transição deve avaliar as redes disponíveis e escolher a que melhor atende as necessidades do usuário baseando-se nas suas preferências e nos requisitos das aplicações usadas por ele.

O *handoff* realiza a manutenção da conectividade do usuário móvel e a migração transparente entre as redes [11]. Os APs podem pertencer a mesma tecnologia (sistema homogêneo) ou tecnologias diferentes (sistema heterogêneo). Este processo considera características da estação móvel, como mobilidade e capacidade de processamento, do ambiente, como a quantidade de dispositivos móveis e das redes disponíveis, como a capacidade e desempenho de cada uma, a fim de determinar o momento de transição, a rede mais adequada para conexão do dispositivo e o modo de execução da transição.

Um dispositivo móvel transita entre redes de duas formas: horizontalmente ou verticalmente [33]. O *handoff* horizontal acontece entre APs de uma mesma rede e usando uma mesma tecnologia como a transição de um usuário móvel entre pontos de acessos de uma rede celular de mesma operadora. A *handoff* vertical ocorre entre APs de redes diferentes e/ou tecnologias diferentes, por exemplo, a transferência da conexão de uma interface 3G para uma interface WiFi no mesmo dispositivo.

O *handoff* pode ser controlado pela rede ou pelo dispositivo [10]. Quando controlado pela rede, o AP determina quando e para onde a conexão da estação móvel será transferida. Neste modelo a escalabilidade torna-se um desafio, pois a rede deve gerenciar a transição de vários dispositivos simultaneamente. Se controlado pelo dispositivo, a rede não interfere diretamente nas decisões do dispositivo. A medição das características, a avaliação e a escolha de uma rede são desafios deste modelo de transição.

O *handoff* consiste em três fases: coleta de informações, decisão e execução [33]. A fase de coleta de informações determina o momento do início do processo e se encarrega da detecção das redes disponíveis no meio e da aquisição de informações sobre essas redes. A fase de decisão analisa as informações coletadas sobre as redes disponíveis, classifica cada rede comparando estas informações e determina a melhor alternativa dentre as redes candidatas. A fase de execução se encarrega da conexão, autenticação e o acesso a rede escolhida, além do encerramento da conexão com o ponto antigo. Após a fase de execução ocorre a finalização da transição na qual recalcula-se as rotas e altera-se o caminho dos pacotes, passando pelo novo ponto de acesso. A Figura 2.2 demonstra a relação entre estas fases.

Figura 2.2: Fases do *handoff*

A fase inicial do *handoff* é caracterizada pela coleta de informações. O dispositivo móvel constantemente monitora as propriedades da comunicação com o AP ao qual está conectado e detecta qualquer oscilação na qualidade do sinal ou do serviço utilizado que ultrapassem um limiar previamente definido [34]. Além disso, nesta fase a estação móvel checa periodicamente o meio em busca das redes disponíveis e identifica as suas características.

A fase de execução finaliza o *handoff*. Nesta fase a rede atual e a rede escolhida trocam informações para a transferência do nó móvel e a alteração de rotas dos pacotes [35]. Alguns esquemas encontrados na literatura, preveem a transferência de credenciais e a pré-autenticação da estação móvel para realizar uma transição segura.

2.2 Fase de tomada de decisão

A fase de decisão é o passo principal no processo de transição em redes heterogêneas. Ele infere os valores de cada rede com base nas informações coletadas, chamadas de critérios de comparação, para escolher uma adequada as necessidades do dispositivo. Este processo tem o objetivo de satisfazer os requisitos do ABC&S, atender as necessidades do dispositivo, respeitar os desejos do usuário e otimizar o uso dos recursos das redes. A escolha de um procedimento de decisão adequado, a determinação das métricas e critérios para comparação e a definição do responsável pela escolha estão entre os desafios de pesquisa do processo de decisão [10].

Os métodos de decisão podem ser classificados de duas formas: pelas estratégias de decisão utilizadas ou pelos critérios empregados na comparação das redes [13, 36]. A classificação por estratégia de decisão é dividida em : função objetivo (OF, do inglês, *Objective Function*), inteligência artificial, teoria dos jogos e decisão com múltiplos atributos (MADM do inglês, *Multiple Atribute Decision Method*). A classificação por critérios engloba as características de QoS, desempenho e segurança das redes, sendo os critérios de QoS os mais utilizados. A Figura 2.3 apresenta uma representação do processo de transição e decisão.

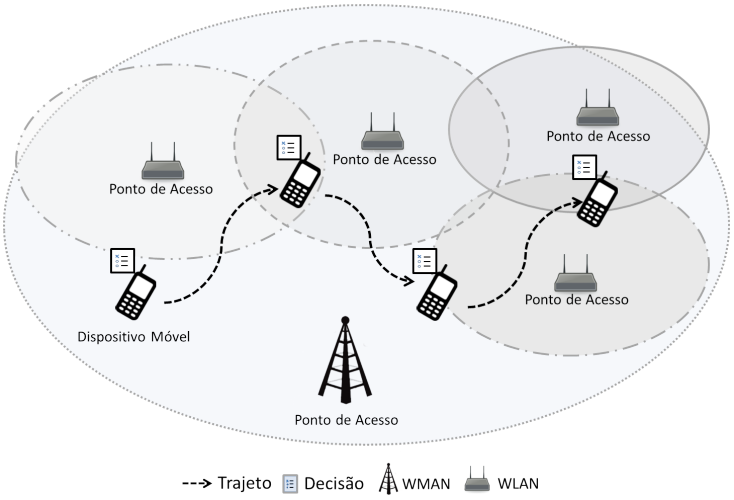

Figura 2.3: Transição e decisão em HetNets

2.2.1 Esquemas de decisão

Os esquemas de decisão baseados em OF tem a finalidade de encontrar um conjunto de parâmetros que maximizem ou minimizem um resultado [10, 12]. Esta estratégia verifica diferentes agrupamentos de parâmetros que representam as características da rede e as preferências do usuário em busca de um objetivo determinado previamente (uma rede de menor custo, uma rede com maior largura de banda, uma rede segura, entre outros). Os

métodos que utilizam a técnica de OF possuem o melhor desempenho comparada com os outros esquemas [11].

Os esquemas baseados em inteligência empregam redes neurais artificiais, protocolos inteligentes e lógica *fuzzy* para decidir quando e em qual rede se dará a conexão [10]. Estes esquemas possuem uma fase de treinamento, onde dados de entrada e configurações são testadas para resolver o problema de decisão. As estratégias baseadas em inteligência possuem flexibilidade quanto aos critérios que serão avaliados. O objetivo destas estratégias são decisões inteligentes e adaptáveis ao contexto do dispositivo decisor. Os métodos que utilizam a técnicas inteligentes são os mais precisos e conseguem trabalhar com medições imprecisas, porém possuem o desempenho prejudicado pela fase de aprendizado de comportamento, fase de calibração dos pesos dos critérios ou pela necessidade de informações prévias [11].

As estratégias de MADMs inferem os valores das alternativas através de funções que comparam os critérios. Tais estratégias funcionam através da atribuição de valores de importância para cada critério em funções que determinam os valores classificatórios das redes. Entre as estratégias MADMs mais utilizadas estão SAW (do inglês, *Simple Additive Weighting*), TOPSIS (do inglês, *Technique for Order Preference by Similarity to Ideal Solution*) [37], MEW (do inglês, *Multiplicative Exponent Weighting) e AHP (do inglês, Analytic Hierarchy Process*) [38, 39].

A estratégia SAW determina pesos diferentes para cada critério e soma os valores para determinar o valor classificatório. Os valores são ordenados do maior para o menor, onde a escolha é realizada dependendo da regra de decisão (maximizar ou minimizar um objetivo). A TOPSIS tenta determinar qual o conjunto de critérios e seus valores que mais se aproximam da "solução ideal" ou um limiar desejado. O valor escolhido é o que mais se aproxima da solução ideal. A MEW determina pesos variáveis para cada critério e multiplica seus valores para classificá-los do maior para o menor. A AHP determina de forma dinâmica o peso para cada critério e procura encontrar o grupo de critérios que maximiza o objetivo. Os métodos que utilizam alguma técnicas MADM são flexíveis, possuem um bom desempenho e precisão, no entanto gastam tempo na busca pelo conjunto de critérios mais relevantes para maximizar o objetivo da decisão [11].

2.2.2 Critérios

A classificação por critérios de comparação possui três grupos: orientados à rede, orientados ao serviço e orientados ao usuário [36]. Os orientados à rede exprimem características de desempenho das redes, por exemplo, área de cobertura, qualidade do enlace, largura de banda, capacidade da rede, segurança, entre outras. Estes critérios determinam as qualidades e as capacidades da rede analisada.

Os critérios orientados ao serviço expressam as características referentes a qualidade

de serviço. Tais critérios englobam propriedades como *jitter*, atraso, taxa de pacotes perdidos, vazão, taxa de erro, etc. Estas métricas influenciam o serviço entregue ao usuário e são as mais utilizadas em métodos de seleção automática de redes. Os critérios orientados ao usuário são subjetivos e determinam as preferências do usuário. Nesta classe estão contidos aspectos como o custo, a preferência por operadora, a qualidade de experiência, entre outros. Estes critérios determinam a satisfação do usuário.

A classe de critérios orientados ao QoS é a mais utilizada pelos métodos de decisão na transição em redes heterogêneas. A mesma emprega como principais critérios a largura de banda disponível, o *jitter*, o *delay* e a taxa de perda de pacotes [10]. Tais critérios são aplicados nos esquemas de decisão em conjunto com critérios secundários como, mobilidade, área de cobertura, requisitos de aplicação, RSS e custo monetário. Desta forma, o dispositivo móvel descobre a rede que possui melhor capacidade de atendê-lo, considerando diversas características importantes para manter a qualidade de serviço.

O critério segurança faz parte dos critérios orientados à rede. Na literatura, alguns trabalhos o determinam como um fator importante na escolha de uma rede, calculando o peso deste atributo na fase de decisão [40, 10, 41, 22, 33]. Ele é tratado de forma genérica, como uma única métrica que representa a quantificação dos aspectos de segurança das redes de acesso e desconsidera as propriedades distintas de confidencialidade, integridade e disponibilidade. Estas propriedades e as técnicas que procuram garanti-las são importantes para escolha eficaz de redes seguras, e ignora-las pode levar à decisões inadequadas as necessidades do dispositivo. Por exemplo, se um dispositivo esta utilizando um serviço que necessita de garantias da confidencialidade das transmissões, ele precisa escolher uma rede de acesso que possua mecanismos de segurança que procurem garantir este principio, porém ao considerar a segurança de maneira genérica uma rede que possua mecanismos que somente garantam à disponibilidade das comunicações pode ser selecionada, colocando o dispositivo em uma situação de risco.

2.2.3 Desafios da fase de decisão

Aferir o critério segurança é um desafio para fase de decisão. Nem sempre existirão informações prévias sobre a segurança da rede, e mesmo se existirem, estas informações podem estar desatualizadas, tendo em vista a dinamicidade do ambiente de redes heterogêneas sem fio [10]. Outro desafio é a necessidade de se obter o nível de segurança antes de transitar de fato para a rede escolhida, objetivando evitar a utilização dos recursos de uma rede insegura. Além disso, poucos métodos consideram este critério na comparação das redes de acesso e apenas ponderam a sua importância perante os critérios de desempenho e QoS [10, 12, 11]. A segurança tem diferentes propriedades que são garantidas por diferentes mecanismos e técnicas [19]. Ignorar estas diferenças pode causar problemas como escolher redes que colocam o dispositivo móvel em risco. Por isso, é necessário um

método de decisão que análise a segurança de forma adequada, separando cada propriedade e avaliando suas características próprias e em tempo hábil para o *handoff*.

A mobilidade dos usuários pode variar em diferentes níveis. A fase de decisão precisa ser rápida o suficiente para não escolher uma rede de acesso que não esteja mais ao alcance do dispositivo móvel. Os diferentes graus de mobilidade apresentam um desafio para a fase de decisão, sendo o tempo de decisão um importante fator de desempenho [10, 42]. Dessa forma, existe a necessidade de se obter um valor para segurança em tempo adequado, onde o nó móvel deve quantificar a segurança de maneira adequada e com um desempenho adequado para não prejudicar o *handoff*.

A fase de decisão analisa as informações coletadas pela fase de coleta de dados e infere valores para cada rede. Estas informações nem sempre estão completas, ou disponíveis. Por este motivo, a falta de informações apresenta um desafio para eficácia da fase de decisão, sendo que a precisão da escolha depende da qualidade das informações coletadas [16].

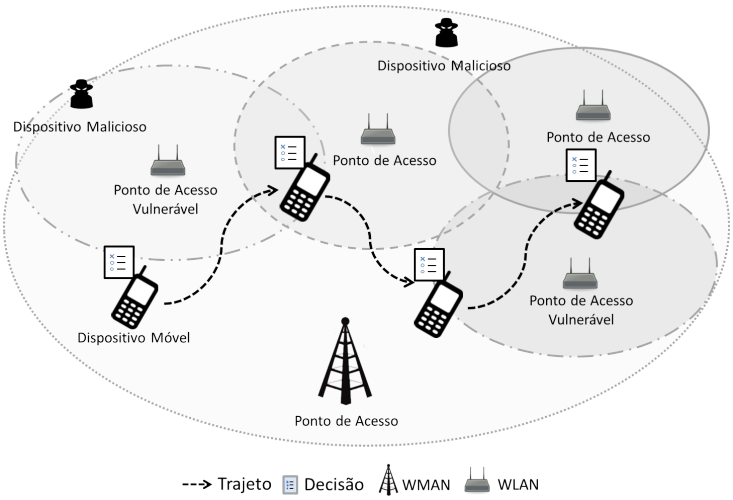

Figura 2.4: Cenário de risco em HetNets

2.3 Princípios da segurança importantes para a fase de decisão

Em seu trabalho Laprie et al. [19], definem a segurança com três atributos principais: confidencialidade, integridade e disponibilidade. A confidencialidade significa que a informação deve ser visualizada apenas por indivíduos com autorização. A integridade determina que a informação deve ser alterada somente por indivíduos autorizados. A disponibilidade define que a informação/serviço deve estar disponível sempre que um indivíduo autorizado precise acessá-la.

A confidencialidade previne que as informações importantes do usuário (dados bancários, logins, senhas, etc.) sejam roubadas e utilizadas de maneira prejudicial. Devido as características das redes sem fio (meio de transmissão comum e de fácil acesso, comunicação

em *broadcast*), os dados podem ser roubados por usuários maliciosos de diversas formas (sybil, homem-no-meio, entre outros) [43, 44]. A confidencialidade deve ser avaliada a fim de evitar decisões automáticas prejudiciais que levem o dispositivo a se conectar em redes sem mecanismos de proteção adequados às necessidades do dispositivo na transição em redes heterogêneas.

As redes de comunicação sem fio garantem a confidencialidade dos dados transmitidos através de mecanismos de Controle de Acesso (AC, do inglês, *Access Control*) e de Ocultação de Informação (DH, do inglês, *Data Hiding*) [44, 45, 46, 47]. Os mecanismos de AC previnem o acesso não autorizado aos dados privados do usuário. Os mecanismos de DH evitam que os dados sejam interceptados e entendidos. Sendo assim, estas duas classes de mecanismos podem ser avaliadas na quantificação do nível de confidencialidade de uma rede.

A classe de CA emprega técnicas de autenticação, autorização e filtragem para gerenciar o acesso à informação [44]. As técnicas de autenticação confirmam a identidade de um usuário de quatro formas diferentes: algo que ele sabe (Ex: senha), algo que ele possui (Ex: *token*, cartão, etc.), algo que ele é (Ex: Análise da iris, digitais, biometria), e algo que ele faz (Ex: modo de fala ou escrita, etc.). As técnicas de autorização verificam e liberam o acesso aos dados que o usuário tem permissão através de mecanismos de verificação, listas (acesso, permissão). As técnicas de filtragem (*captchas*, *firewalls*, *proxys*, etc.) são usadas na prevenção de acessos não autorizados às informações privadas [48, 44, 45, 46, 47].

A Classe de DH agrupa técnicas de criptografia e esteganografia para evitar que as informações sejam detectadas, entendidas ou visualizadas [46]. As técnicas de criptografia são usadas para codificar a informação, impedindo um indivíduo sem autorização de decifrar a mensagem. A estenografia tem como objetivo a ocultação da existência de uma informação, usando técnicas que escondem uma mensagem dentro de outra mensagem ou que ocultam o canal de comunicação.

Os mecanismos de AC e DH presentes nas redes de acesso podem ser analisados para determinar o nível de confidencialidade oferecido pela rede. Entretanto, medir a segurança não é uma tarefa fácil. Entre as dificuldades, Pfleeger et. al. [15] citam a necessidade de testar os mecanismos de segurança, a incerteza nas medições (informações imprecisas) e a falta de informações. O processo de decisão na transição em redes heterogêneas deve considerar estes requisitos. A Figura 2.5 apresenta uma organização dos princípios, técnicas e mecanismos de confidencialidade.

O modelo prospectivo de decisão considera a incerteza e a falta de informações na tomada de decisão. Este modelo pode ser utilizado para determinar o valor de confidencialidade de uma rede e selecioná-la. Sendo assim, a próxima sessão introduz o modelo prospectivo de tomada de decisão e suas características.

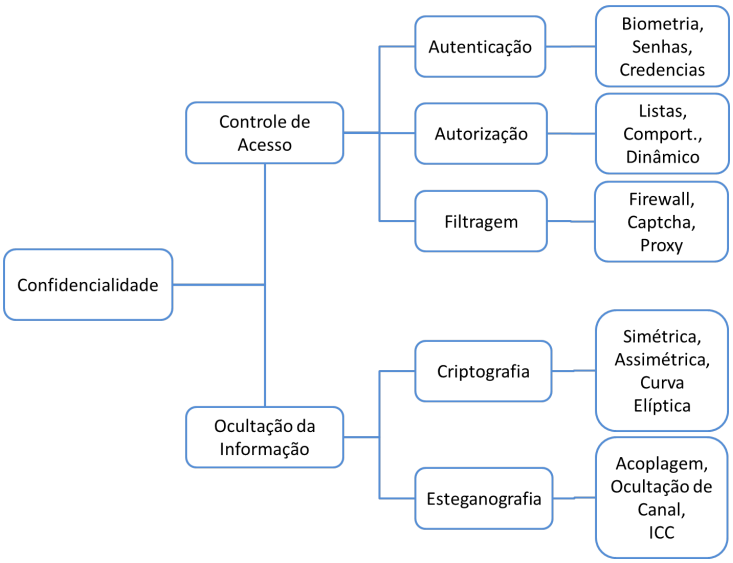

Figura 2.5: Organograma das técnicas de confidencialidade

2.4 Modelo prospectivo

A teoria da prospecção ou teoria do prospecto, é uma teoria da área de economia comportamental que define um modelo de tomada de decisão descritivo, o qual explica como seres humanos tomam decisões envolvendo risco e falta de informações [28]. Este modelo avalia as consequências das alternativas em termos de ganhos e perdas e considera a forma com que o agente decisor (ser humano) as compreende durante o processo de decisão. A perspectiva da teoria da prospecção possibilita a tradução das vontades, expectativas e da importância dada por um agente humano às alternativas de um problema de decisão, incorporando a subjetividade do usuário na forma como ele escolhe entre alternativas.

O modelo prospectivo de decisão demonstra como o ser humano reage na presença de incerteza e risco quando enfrenta um problema de decisão [17]. A incerteza significa a imprecisão ou falta das informações a respeito dos critérios de comparação das alternativas e o risco representa a probabilidade de ocorrência de eventos caso escolha uma dada alternativa [49]. Este modelo traduz a incerteza e risco das alternativas através de uma função que mapeia a importância de um evento, positivo ou negativo, e a chance deste evento ocorrer para o agente. Para isso, calcula-se a probabilidade de um determinado evento ocorrer para uma dada alternativa e determina-se a importância deste evento e de sua probabilidade para o usuário. Desta forma, tal modelo pode ser usado em problemas de decisão onde existam a imprecisão das informações (incerteza) e da falta de informações (ignorância) sobre as alternativas como, por exemplo, na avaliação do nível de confidencialidade de um sistema.

A tomada de decisão na teoria da prospecção possui duas fases: a edição e a avaliação [17]. A fase de edição realiza a organização e reformulação das alternativas através de regras e operações, simplificando a fase de avaliação subsequente. A fase de avaliação

determina o valor das alternativas e escolhe a mais apropriada com base no risco de cada alternativa e na percepção e "sentimento" sobre o risco para o agente.

2.4.1 Fase de edição

A fase de edição possui seis operações: codificação, segregação, combinação, cancelamento, simplificação e detecção de dominância. Estas operações objetivam a identificação correta das consequências relevantes as alternativas e simplifica o problema de decisão. As operações desta fase melhoram a eficiência e eficácia da decisão, além de fornecer informações necessárias para determinar o valor das alternativas. Com exceção da operação de codificação, todas as outras operações são executas quando existe mais de uma consequência analisada em cada alternativa.

A operação de codificação identifica o ponto de referência e codifica cada consequência de cada alternativa determinando situações de ganho ou de perda. O ponto de referência corresponde a um limiar que serve para comparação das consequências. Se uma consequência apresenta um valor menor que o ponto de referência então o modelo a considera como perda. Se uma consequência possui um valor maior que o ponto de referência, o modelo prospectivo considera-a como ganho. Na teoria da prospecção o ponto de referência e a codificação de ganho e perda são influenciados pelas aspirações do agente decisor.

O procedimento de combinação identifica consequências idênticas em uma alternativa e une suas probabilidades, simplificando a avaliação da alternativa. Isto ocorre quando o problema de decisão apresenta alternativas que possuem mais de uma consequência, sendo desnecessário em problemas com somente uma consequência. Este procedimento auxilia a avaliação eliminando equívocos na formulação das alternativas. A segregação identifica consequências que são certas de ocorrerem em todas as alternativas. Existem consequências comuns a todas às alternativas, se a chance de ocorrência for 100% em todas as alternativas então tal consequência não faz parte dos critérios que diferenciam as alternativas. Isto diminui a complexidade do processo de avaliação, pois retira as consequências que não precisam ser avaliadas.

A operação de cancelamento descarta consequências com probabilidades comuns entre as alternativas. Por exemplo, consequências com probabilidades iguais para as duas alternativas podem ser ignoradas no processo de decisão considerando que a probabilidade que ocorram é a mesma para as duas alternativas não tendo impacto na avaliação. Este procedimento segue o mesma lógica da segregação com a diferença da probabilidade de ocorrência ser menos de 100% e a consequência ser comum as alternativas comparadas. A simplificação corresponde ao ajuste dos valores das probabilidades e da desconsideração de consequências pouco prováveis. A operação de detecção de dominância identifica alternativas com consequências irrelevantes ou que possuem probabilidades inferiores excluindo estas alternativas da avaliação subsequente. Este procedimento diminuí a complexidade

da comparação e torna o processo mais eficiente. Estas operações servem para identificar as consequências e simplificar o problema de decisão [50].

2.4.2 Fase de avaliação

A fase de avaliação determina os valores das alternativas e escolhe a de maior valor. Esta fase utiliza duas funções para avaliar cada alternativa: a função de valoração e a função de ponderação da probabilidade [17]. Estas funções resultam na escolha da alternativa mais adequada ao contexto do agente decisor, considerando a falta de informações e a imprecisão dos critérios de comparação.

A função de valoração define o impacto das possíveis consequências relacionadas a perspectiva do decisor. Isto é, a forma com que o agente avalia a consequência de uma alternativa, considerando o ponto de referência. O ponto de referência representa o estado equilibrado do ambiente do ponto de vista do agente (a visão do agente do que é um ambiente ideal). O valor definido por esta função indica a importância de uma consequência e é influenciado por fatores subjetivos ao seu contexto como as informações disponíveis sobre a alternativa, a probabilidade de ocorrência de uma consequência, entre outras. A adaptação desta função para o processo de decisão no *handoff* pode auxiliar o processo de decisão a lidar com aspectos aversos e imprevisíveis como a falta de informação sobre os critérios de comparação das alternativas (no contexto de HetNets, as redes de acesso disponíveis para escolha).

A função de ponderação da probabilidade estabelece um valor para o impacto das probabilidades de cada consequência de uma alternativa. Este valor representa a importância da ocorrência da consequência em uma determinada alternativa. A ponderação de uma consequência tem como base as informações a respeito da alternativa. Se as informações forem precisas e completas o valor do peso da probabilidade é maior que o valor do peso da consequência. Desta forma, o peso de uma probabilidade determina a confiança de um agente decisor em uma alternativa. Aplicar um peso par a confiança nos valores calculados pode aumentar a precisão da decisão quando em situações adversas como na falta de informações dos critérios de comparação das alternativas.

O modelo prospectivo usa a técnica de função objetivo e explica de forma simples como a utilização dessas duas funções de valoração e ponderação avaliam o risco e a incerteza presente em cada alternativa e consideram o contexto do agente decisor. A Equação 2.1 infere o valor de prospecção de uma alternativa:

$$U = \sum_{i=1}^{n} (w(p_i)v(x_i)) \tag{2.1}$$

Na equação x_i representa as possíveis consequências (eventos), p_i representa as respectivas probabilidades para cada consequência. A função v atribui o valor de uma con-

sequência e w é a função que atribui o valor das probabilidades. A variável U representa o valor da utilidade esperada das alternativas (prospecções).

A teoria da prospecção expõe dois comportamentos presentes na decisão executada por seres humanos: o efeito **certeza** e o efeito **possibilidade**. Estes efeitos ocorrem em duas possíveis situações: quando as consequências são favoráveis e quando não são. As situações favoráveis correspondem a problemas de decisão onde todas as alternativas apresentam ganhos. Os ganhos são resultados onde o valor da alternativa é maior que o valor do ponto de referência do usuário (que é o que ele entende como resultado aceitável). Situações de perda correspondem a situações onde todas as alternativas apresentam perdas. As perdas são resultados onde o valor da alternativa é menor que o valor do ponto de referência do usuário.

O efeito certeza ocorre quando o valor das alternativas é muito próximo. Quando as consequências são favoráveis e a variação dos valores das alternativas consideradas maiores que o ponto de referência é pequena, o agente decide com base no valor da probabilidade, escolhendo a alternativa de maior chance de ocorrência. Nestes casos o agente procura evitar o risco de se desapontar, preferindo uma alternativa que é certa de ocorrer a uma alternativa que possa não ocorrer. Este comportamento é chamado de **aversão ao risco**, pois o agente tende a evitar perdas. Quando as consequências são desfavoráveis e a variação dos valores destas alternativas é pequena, em uma situação de perda garantida, o agente escolhe com base na probabilidade. A alternativa com a menor probabilidade de ocorrência é preferível ao invés da alternativa com menor valor de perda. Este comportamento chama-se de **busca de risco**, onde o agente escolhe a probabilidade menor com o objetivo de evitar maiores perdas e ocorre quando os valores das perdas tem um impacto auto considerado pelo usuário. Ao considerar que o valor das alternativas de ganhos ou perdas variam muito pouco em seus grupos, este efeito leva a decisões menos valiosas (onde o valor ganho é menor ou o valor da perda é maior), porém mais inteligentes no sentido de tentar minimizar as perdas e maximizar os ganhos, optando pela probabilidade.

Exemplo	**Situação Favorável (Ganho)**	**Situação Desfavorável (Perda)**
Certeza	70% de chance de ganhar uma viagem de 3 semanas pela Europa ou outra onde existe 100% de chance de ganhar uma viagem de dois dias ao Equador. Neste caso, o medo de perder faz com que o agente seja evasivo ao risco, aceitando a aposta de viajar ao Equador ao invés da chance de ganhar uma viagem pela Europa	Uma aposta onde existe 85% de chance de perder R$4.000,00 ou outra onde existe 100% de chance de perder R$3.300,00. Neste caso, o agente espera evitar a perda e assume um o risco de perder menos, aceitando a aposta desfavorável de 85% chance de perder R$4.000,00.
Possibilidade	15% de chance de ganhar uma viagem de 3 semanas pela Europa ou outra onde existe 92% de chance de ganhar um livro sore a Europa. Neste caso o agente espera um ganho maior e busca o risco, aceitando a chance de 15% de viajar.	Uma aposta onde existe 15% de chance de perder R$3.000,00 ou outra onde existe 100% de chance de perder R$100,00. Neste caso, o agente espera perder menos e admite perder menos, aceitando a certeza de perder R$100,00

Tabela 2.1: Exemplo de ocorrência dos efeitos de certeza e possibilidade

O efeito possibilidade ocorre quando o valor das alternativas é muito diferente. Quando as consequências são favoráveis, o agente decide com base no valor da alternativa, escolhendo aquela que mais vale, mesmo que a probabilidade seja muito baixa. Este comportamento recebe o nome de **busca de risco**, pois o agente escolhe a possibilidade de *maior ganho* ao invés da certeza de ganhar. Quando as consequências são desfavoráveis e os valores de perda possuem uma variação considerada pelo agente muito grande, ele decide baseado no valor menor, escolhendo a alternativa de menor valor ao invés da possibilidade menor de perder. Este comportamento tende a evitar o risco de perder muito, sendo chamado de **aversão ao risco**.

A Tabela 2.1 demonstra um exemplo onde os efeitos de certeza e possibilidade ocorrem. O exemplo é inspirado nas experiências de Kahneman [17]. O exemplo ilustra de o comportamento das decisões de um ser humano. O modelo prospectivo pode ser adaptado para o problema de decisão automático na transição em redes heterogêneas. A vantagem de utilizar este modelo é decidir com base no risco de ocorrência de um evento e considerar a falta de informação para a tomada de decisões.

2.5 Resumo

Este capítulo apresentou os fundamentos sobre as redes heterogêneas, destacando o funcionamento do processo de *handoff* vertical e as principais propriedades da fase de decisão contida neste processo. Foram ressaltadas as principais características das redes de acesso usadas para comparação entre elas, bem como as principais estratégias de analise e classificação destas características. Além disso, foram levantados os requisitos necessários para se considerar a segurança de maneira adequada no processo de decisão, separando suas principais propriedades e a necessidade de tratar a falta de informações sobre os critérios de comparação. Por fim foi demonstrada a abordagem da teoria da prospecção e seu modelo para tomada de decisões baseadas no comportamento do ser humano quando enfrentam problemas de decisão com situações adversas como a falta de informações sobre as alternativas.

CAPÍTULO 3

MÉTODOS DE DECISÃO COM SEGURANÇA NO *HANDOFF*

Este capítulo apresenta os principais trabalhos existentes na literatura que propõe métodos para a fase de decisão na transição em redes heterogêneas e também os trabalhos que apresentam técnicas de aferição do nível de segurança de sistemas e redes de comunicação. A Seção 3.1 apresenta e analisa as propriedades dos métodos de decisão que consideram a segurança como um critério de seleção. A Seção 3.2 apresenta as principais técnicas de quantificação de segurança.

3.1 Métodos de decisão baseados em segurança

Os métodos de decisão para *handoff* em Hetnets procuram determinar a rede de acesso que melhor atende as necessidades do MD [4]. Para tal, estes métodos analisam as características das redes para classificá-las e selecionar a mais adequada para o *handoff* [10, 12, 51, 52]. Entre estes métodos existem alguns que consideram as características de segurança das redes como critérios importantes nas decisões de *handoff* [25, 41, 53, 54]. Esta seção apresenta uma classificação sobre estes métodos, dividindo-os em métodos que utilizam estratégias MADM de decisão e métodos baseados em aprendizado que aplicam redes neurais, inteligencia artificial e lógica *fuzzy*. A seguir são apresentados os métodos de cada uma destas classes, detalhando suas vantagens e desvantagens para o *handoff*.

3.1.1 Métodos baseados em MADM

Esta subseção apresenta os métodos de decisão relacionados a ponderação dos critérios de acordo com sua importância relacionada as necessidades do dispositivo móvel. Tais métodos foram separados em dois grupos que reúnem os trabalhos que empregam estratégias com funções objetivo e trabalhos que empregam estratégias de analise de multi atributos.

Alguns trabalhos utilizam uma estratégia baseada em funções objetivo (OF) [26, 25]. Tais trabalhos ponderam os critérios de comparação das redes em busca da rede cujo conjunto de critérios possua o melhor valor. Dependendo da regra de seleção, a primeira (maximizar um conjunto de critérios como melhor valor) ou a última (minimizar um conjunto de critérios como melhor valor) rede é selecionada. Funções objetivo possuem desempenho e acurácia adequadas ao processo de de decisão em *handoffs* [38]. A Figura 3.1 mostra as fases do funcionamento do método usando função objetivo.

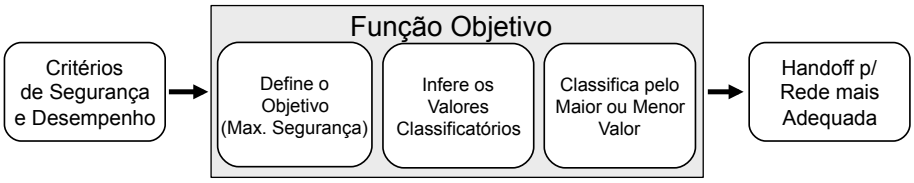

Figura 3.1: Funcionamento das estratégias com OF

Entre os métodos de decisão para o *handoff* que ponderam o critério segurança, Li e Cheng [25] se destacam ao propor uma abordagem simples para classificação dos PAs através de uma função objetivo e da ponderação adaptativa dos critérios. A OF aplica a ponderação de cada critério e soma os resultados para resultar no valor classificatório da rede. A função adaptativa se baseia em informações relativas ao contexto do dispositivo móvel, como por exemplo, o nível de bateria para determinar a importância dos critérios. Os critérios utilizados são força do sinal, atraso fim-a-fim, segurança, bateria e custo da rede. A simplicidade da solução e o emprego do esquema de OF torna o desempenho do método e a flexibilidade quanto a quantidade de critérios os pontos mais fortes. Além disso, o método considera as informações do contexto do dispositivo na ponderação dos critério, o que aumenta a satisfação do usuário. Apesar de considerar as características de segurança como critério de seleção, os autores avaliam apenas o desempenho do processo de decisão, assumindo a segurança como um critério único e não a analisam de maneira adequada. A analise da segurança de modo genérico feita pelo método, pode levar a decisões inadequadas que colocam o dispositivo móvel em risco.

Alguns trabalhos utilizam estratégia baseadas em MADMs para selecionar as redes. Entre elas estão o TOPSIS, o SAW e o AHP. O SAW é estratégia mais simples de seleção, onde os critérios são multiplicado por pesos e os valores somados para determinar a melhor rede. A rede com o maior valor deste somatório é selecionada. O TOPSIS utiliza limiares para selecionar a rede mais adequada. Os critérios são ponderados e somados. A rede com o valor que mais se aproxima do limiar definido é selecionada. O AHP determina importâncias relativas para cada critério. O valor da importância relativa, que pondera cada critério, se baseia em informações do contexto do MD. As Figuras 3.2 e 3.3 apresentam as fases de funcionamento dos métodos usando estas estratégias, respectivamente.

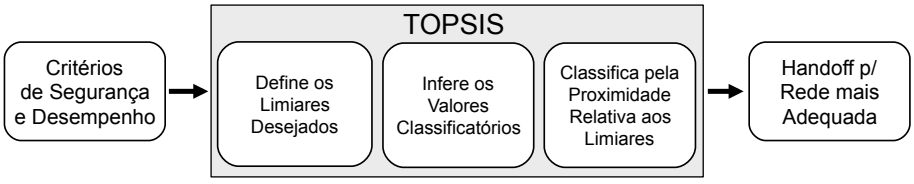

Figura 3.2: Funcionamento das estratégias com TOPSIS

Em [55], os autores analisam a influência dos parâmetros do tráfego do MD na seleção da rede de acesso. O trabalho emprega a estratégia TOPSIS para determinar o conjunto

de critérios que melhor representa a necessidade do MD e avaliá-os para determinar a rede de acesso para o *handoff*. O TOSIS seleciona a rede que possuir a valor da soma dos critérios mais próxima de um limiar que é definido dinamicamente com base nas características do tráfego do MD. Os critérios selecionados para decisão são baseados no tipo de tráfego usado pelo MD. Os autores propõe utilizar o Nível de Segurança (LoS, do inglês, Level of Security) como um critério de decisão quando as transmissões do MD necessitam ser confidenciais. O LoS é apresentado de forma genérica por Bakmaz [56] onde os aspectos de segurança importantes são levantados para serem considerados na quantificação do LoS, sendo o principal aspecto a força do algoritmo de criptografia. 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), são importantes para a confidencialidade das transmissões [44, 46, 57]. Negligenciar as diferentes características da segurança podem levar o MD a uma situação de risco, onde suas necessidades reais de segurança podem não ser atendidas.

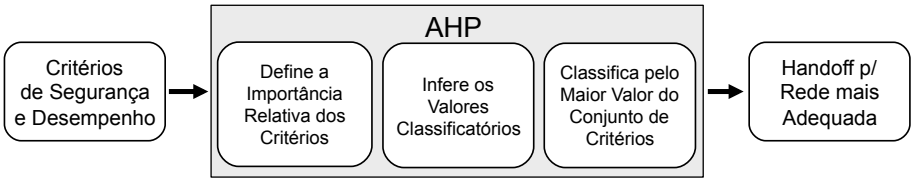

Figura 3.3: Funcionamento das estratégias com AHP

Lahby et al. [22] propõe um método híbrido com base no E-TOPSIS e no E-AHP. A solução é flexível quanto aos critérios avaliados, baseando-se no contexto do dispositivo para determinar quais características serão empregadas na comparação. O E-AHP pondera os critérios com base nesta analise do contexto do MD. O E-TOPSIS escolhe a rede analisando limiares calculados dinamicamente com base na importância relativa para o contexto do dispositivo. Os autores consideram a segurança das redes de forma genérica, desconsiderando suas propriedades distintas. Sun-lei et al. [41], Radhika et al. [58]. propõem métodos MADM para seleção de redes sem fio que aplicam AHP na ponderação dos critérios e SAW na classificação e escolha das redes. Ambos os métodos são flexíveis quanto aos critérios empregados na comparação das alternativas e possuem baixo tempo de execução quando comparados com outras estratégias [38]. Entretanto, estes trabalhos avaliam a segurança como um atributo único, não especificando quais propriedades nem como elas são consideradas na comparação das redes. A abordagem genérica da segurança pode levar a decisões equivocadas com potencial para prejudicar o dispositivo, por exemplo, expondo dados confidenciais.

3.1.2 Métodos baseados em aprendizado

Os métodos que apresentam fases de calibração ou aprendizagem de padrões se encontram nesta subseção. Tais métodos foram separados em dois grupos que reúnem os trabalhos que empregam estratégias com lógica fuzzy, inteligencia artificial e redes neurais na analise e classificação das redes.

Alguns métodos de decisão aplicam a lógica fuzzy para calibrar as medições dos critérios de comparação. Com isso obtém-se resultados precisos ao inferir os valores classificatórios das redes. As estratégias baseadas em lógica fuzzy possuem melhor acurácia das decisões. A Figura 3.4 mostra as fases do funcionamento do método usando OF.

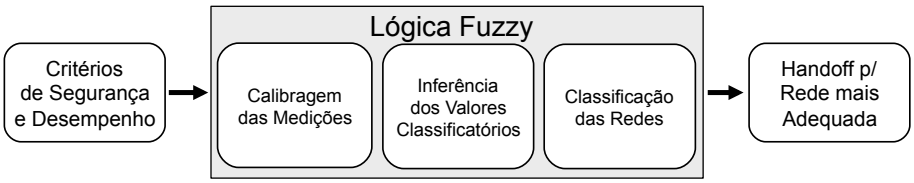

Figura 3.4: Funcionamento das estratégias com lógica fuzzy

Kahnum et al. [26] utilizam uma estratégia híbrida de seleção das redes no *handoff*, baseando-se na teoria difusa, nas preferências do usuário e em uma OF. A lógica fuzzy trata a imprecisão das medições dos critérios e as preferências do usuário são usadas para determinar a importância dos critérios usados na OF. No trabalho, a OF é usada como uma função de pertinência, que determina em qual rede o MD se encaixa. O critério segurança é considerado de maneira superficial, onde suas principais características de integridade, confidencialidade e disponibilidade não são analisadas ou separadas. Isto pode levar a decisões equivocadas e prejudiciais ao MD.

Os autores em Batich et al. [59] combinam a lógica fuzzy na avaliação do critério SINR (do inglês, *Signal to Interference and Noise Ratio*) com uma plataforma para transições baseada na Transição Independente de Mídia (MIH, do inglês, *Midia Independet Handover*) [60]. O MIH permite a transferência de sessões IP de uma tecnologia de acesso para outra, gerenciando a mobilidade dos dispositivos e o handoff. O método aplica logica fuzzy para tratar a imprecisão dos valores medidos. O critério segurança é usado de forma inadequada na comparação, desconsiderando suas propriedades distintas e não especificando detalhadamente a sua aplicação. A fase de calibração feita com a lógica fuzzy aumenta o tempo de decisão o que pode resultar em decisões não adequadas como transitar para um rede que não está mais ao alcance. Além disso, se os critérios empregados forem dinâmicos, mudando com o passar do tempo e com os diferentes padrões de tráfego usados pelo usuário, a calibração consecutiva pode se tornar um problema e aumentar ainda mais o tempo de decisão.

Kaleem e Yen [24] propõem um método de decisão que emprega um esquema AHP, um esquema TOPSIS e lógica fuzzy. A solução é flexível quanto aos critérios emprega-

dos, possibilitando o uso inteligente de critérios de comparação. O método executa no dispositivo sem interferências da rede, o que garante a autonomia nas escolhas. Além disso, a aplicação da lógica fuzzy para normalizar os valores dos atributos melhora a precisão dos resultados e o uso do AHP analisando informações do contexto do usuário aumentam a satisfação. Entretanto, o método não trata a falta de informações a respeito dos critérios analisados. Ademais, o uso de estratégias inteligentes aumenta o tempo de resposta da decisão, apesar de melhorar a precisão da escolha. Por fim, o trabalho apenas pondera o critério segurança sem considerar suas diferentes características ou apresentar uma forma de calcular o nível de segurança oferecido pelas redes, podendo levar a escolhas inadequadas as necessidades do dispositivo.

Alguns métodos aplicam estratégias baseadas em redes neurais e inteligencia artificial (AI, do inglês, *Artificial intelligence*) nas decisões de *handoff*. As estratégias de redes neurais e inteligencia artificial são centradas na rede, o que aumenta a precisão das escolhas e diminui a autonomia das escolhas do dispositivo móvel. A Figura 3.5 mostra as fases do funcionamento do método usando OF.

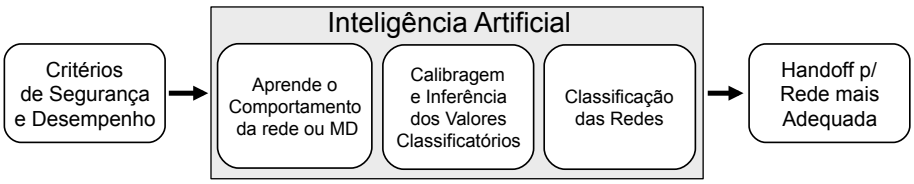

Figura 3.5: Funcionamento das estratégias com AI

Os autores em [53] empregam o LoS no processo de decisão. A estratégia usada para inferência e classificação das rede tem como base as redes neurais artificiais. Os esquemas baseados em inteligência artificial possuem uma maior precisão nas decisões e inferências em comparação com os demais esquemas [11]. Entretanto, a fase de aprendizado existente nesse método aumenta o tempo de decisão. Ademais, a dinamicidade das medições podem prejudicar o desempenho do processo de decisão em caso de um ambiente que varie rapidamente suas condições, executando sucessivas inferências e adaptações a cada alteração nas medições. Ma et al. [27] propõe a utilização do nível de risco do ambiente empregado juntamente com outros critérios de desempenho em um modelo de inferência através de um sistema em uma nuvem para classificação das redes. O uso de um esquema de inteligência artificial melhora a precisão das inferências e das escolhas, além de permitir lidar com situações adversas onde ocorre a imprecisão das medições. O objetivo do método é garantir a satisfação do usuário final, porém as decisões são determinadas pela rede, retirando a autonomia do MD. O desempenho de métodos baseados em inteligência é prejudicado pelo fase de calibração e aprendizado. Além disso, o nível de risco no ambiente não separa os diferentes aspetos da segurança na avaliação do critério, o que diminui a precisão das escolhas podendo levar o MD a se conectar com redes arriscadas.

Tabela 3.1: Propriedades dos métodos que consideram segurança

Método	Confidencialidade	Incerteza	Acurácia	Tempo	Autônomo
Sun-Lei [41]			Baixa	Sim	Sim
Xiaobin Liu [25]			Media	Sim	Sim
Radika [58]			Baixa	Sim	Sim
Lahby [22]			Baixa	Sim	Sim
Kaleem [24]			Média	Sim	Sim
Khanum [26]			Média	Sim	
Bathich [59]			Média	Sim	
Bakmas [55]			Baixa	Sim	
Nasser [53]			Baixa	Sim	
MA [27]			Média	Sim	Sim
Zekri [11]			Média	Sim	

A Tabela 3.1 apresenta a comparação dos trabalhos relacionados. Ela mostra um resumo dos requisitos considerados importantes para determinação de uma rede confidencial. O requisito de confidencialidade corresponde se o respectivo método trata de maneira adequada esta propriedade, considerando as técnicas que tentam garanti-lo. A acurácia diz respeito ao método ser eficaz em decidir entre as redes de acesso com segurança, classificando-os com baixa, média e alta acurácia, onde baixa considera se o método não é adaptável a dinamicidade das medições e não trata a segurança de maneira adequada, média se o método trata as variações das medições ou se considera segurança adequadamente, e alta se trata as variações e considera a segurança de maneira adequada. O tempo diz respeito a velocidade das decisão, se são executadas em tempo hábil para o *handoff*. A autonomia do método quer dizer se o dispositivo móvel toma as decisões ou se é a rede. A incerteza corresponde se o método trata ou não a falta de informações.

3.2 Técnicas de quantificação de risco de segurança

A quantificação da segurança pode ser realizada de diversos modos [61, 62, 63, 64, 65], sendo uma destas formas a análise de risco. A análise de risco é usada para detectar possíveis ameaças e para prevenir situações inseguras e danosas [15, 66]. Desta forma, esta estratégia de quantificação de segurança pode ser usada em um método de decisão para o *handoff*, podendo prevenir que o MD transite para uma rede arriscada e pouco segura.

O LoS é apresentado por Bakmaz et. al [56], onde os autores reúnem os aspectos considerados mais relevantes para o desenvolvimento e integração de soluções de segurança de redes sem fio heterogêneas. Os aspectos de segurança mais importantes para o *handoff* seguro por redes móveis, WLAN e redes ad-hoc são apresentados. Entre estes aspectos encontram-se a descoberta das vulnerabilidades e riscos de segurança conhecidas, a classificação de mecanismos de criptografia de acordo com seus desempenhos, a localização dos

mecanismos de segurança na rede e custo dos mecanismos. Entretanto, o trabalho não especifica como considerar os aspectos levantados na quantificação de segurança, apenas desenha perfis de segurança específicos para cada tipo de rede.

Os autores em [67] analisam as vulnerabilidades de segurança nas redes de comunicação pontuando cada vulnerabilidade para gerar um valor que represente o nível de segurança. De acordo com os pesquisadores, este nível é modelado em um grafo de ataques, onde quanto mais relacionamentos uma vulnerabilidade possui, maior é a sua importância. Nesta abordagem existe a necessidade de obter informações prévias, como as informações sobre a força das vulnerabilidades conhecidas, além da necessidade de avaliar quais dessas vulnerabilidades estão presentes nas redes. Por esse motivo, esta abordagem não é interessante para o *handoff* controlado pelo MD, considerando a necessidade de entrar na rede para testar suas vulnerabilidades, além do tempo gasto para avaliar a segurança da rede e quantificá-la. No trabalho de Bhattacharya et al. [68] existem os mesmos problemas apesar da abordagem para quantificação de risco utilizar grafos de dependência de vulnerabilidades. Do mesmo modo em [69], os autores propõe a análise de risco considerando fatores subjetivos de cada sistema, como o tipo e os serviços em uso e o tipo do tráfego na rede para determinar a probabilidade de que vulnerabilidades sejam exploradas. A estratégia proposta também requer o acesso as informações de dentro da rede para quantificar a segurança através do risco.

Em [68], os autores propõe a avaliação do risco de segurança das informações se baseando no julgamento de diferentes especialistas. As análises são realizadas por sistemas computacionais diferentes que compartilham seus resultados para determinar o valor do risco, gerando resultados mais precisos Porém, existe a necessidade de obter informações prévias, além da possibilidade de se confiar nas informações de um sistema comprometido, sendo prejudicial em um ambiente de redes heterogêneas. Outras abordagens como detecção de anomalias [70] e uso de métricas como k-anonimo e L-diversidade [71, 72], foram propostos para aferir o risco de segurança em redes. Porém, estas abordagens também não são adequadas ao *handoff* pois necessitam que o MD entre na rede para inferir o risco. Desta forma, um técnica que possa quantificar o risco de segurança antes da entrada do nó na rede e que seja rápida e eficaz se faz necessária para o processo de decisão seguro no *handoff*.

3.3 Resumo

Este capítulo apresentou os métodos e soluções propostos na literatura para decisão automática da seleção de redes de acesso que consideram a segurança como um critério de comparação. Foi realizada uma breve contextualização dos métodos de decisão e suas vantagens e desvantagens foram apresentadas. As técnicas de quantificação de segurança também foram classificadas e suas vantagens e desvantagens apresentadas. O próximo

capitulo especifica um método de apoio a decisão que quantifica a confidencialidade das redes e toma decisões mesmo quando não existem informações sobre os critérios de comparação.

CAPÍTULO 4

UM MÉTODO DE DECISÃO CIENTE DA CONFIDENCIALIDADE

Este capítulo apresenta um método autônomo de apoio à decisão na transição em redes heterogêneas que classifica os pontos de acesso com base no nível de confidencialidade de cada uma. O método considera a existência de técnicas de confidencialidade nas redes de acesso para aferir o nível de confidencialidade e auxiliar o processo de escolha. Ele determina o nível de confidencialidade mesmo quando faltam informações sobre a existência de técnicas de confidencialidade nos pontos de acesso. A Seção 4.1 apresenta uma visão geral do método proposto e seus componentes. A Seção 4.2 especifica o método e suas fases. A Seção 4.3 descreve o seu funcionamento.

4.1 Visão geral

O método proposto, chamado de SDHet, tem como objetivo auxiliar o processo de decisão na transição (*handoff*) em redes heterogêneas para escolha de pontos de acesso (PA) com menor potencial de expor os dados privados do usuário. Para isso, ele determina o nível de segurança de cada PA, suplementando as informações de desempenho e Qos comumente usadas para decisão [10]. O nível de segurança baseia-se na avaliação da confidencialidade das redes de acesso e na inferência de um valor representativo através da observação da presença de técnicas de segurança que garantem este princípio. Este método opera entre a fase de coleta e a fase de escolha do processo de decisão no *handoff*. o SDHet consegue determinar o nível de segurança mesmo quando faltam as informações necessárias para o seu funcionamento.

A integridade, a confidencialidade e a disponibilidade das informações são os três principais pilares da segurança e cada um deles possui características próprias que precisam ser garantidas [19]. Os método de decisão encontrados na literatura definem a segurança como um critério importante para a comparação das redes de acesso no *handoff* em HetNets ao considera-lo nas decisões. Porém, nenhum dos métodos na literatura considera a complexidade deste critério em suas formulações [24, 25, 26], não analisando a segurança de maneira adequada ao considerá-la de forma genérica. Sendo assim, considerar a segurança genericamente, como um critério único, pode levar a escolha e a transição para redes que não atendem os requisitos de segurança do dispositivo. Por exemplo, se o critério segurança baseia-se em mecanismos de disponibilidade, e o dispositivo móvel necessita de mecanismos de confidencialidade, a sua escolha se baseará em um critério

com pouca importância para ele, levando-o o a uma situação de risco.

O princípio da confidencialidade determina que a visualização de informações privadas deve ser feita somente por entidades autorizadas [19]. No âmbito das comunicações sem fio, este princípio tem importância, visto que o meio de transmissão das informações é aberto e compartilhado, tornando fácil a visualização não autorizada das mensagens transmitidas. Por esse motivo, o SDHet avalia a propriedade de confidencialidade das redes de acesso como o principal critério na decisão do processo de *handoff*.

As técnicas de segurança que objetivam garantir a confidencialidade das comunicações são classificadas em: Controle de Acesso (AC) e Ocultação de Informações (DH). A presença destas técnicas auxilia a determina o Nível de Confidencialidade (Nc) nas transmissões de mensagens em um PA. O SDHet não trata da detecção de atacantes ou da aferição da capacidade de uma técnica de confidencialidade em um PA, mas sim da possibilidade de se ter a privacidade comprometida ao utilizar uma AP para comunicação.

O SDHet utiliza informações referentes aos mecanismos de confidencialidade presentes nas redes de acesso. Estas informações são provenientes da fase de coleta de dados do processo de decisão. A coleta de informações não faz parte das funções do SDHet.

O $N_c$se baseia no risco a confidencialidade e na falta de informações necessárias para decisão A avaliação de segurança pode ser feita através da técnica de análise de risco [15]. O SDHet proposto aplica a análise probabilística de risco para determinar o risco à confidencialidade apresentado por uma rede. Esta análise utiliza informações subjetivas sobre a existência de mecanismos de confidencialidade em cada rede para determinar a probabilidade de ocorrer a visualização não autorizada das comunicações.

A incerteza representa a falta de informações para tomada de decisão. Este fator prejudica o processo de decisão e diminui a precisão das escolhas [16]. O SDHet consegue determinar o $N_c$dos APs mesmo quando faltam informações a respeito dos critérios de confidencialidade nelas presentes. Para isso, ele assume que a fase coleta de informações do processo de *handoff* informa-o quando ocorre a falta de informações sobre algum critério, independente se a falta é natural ou causada por humanos [19]. Além disso, este método quantifica a incerteza e a utiliza para determinar a importância do $R_c$apresentado por uma rede. Este valor representa a sensibilidade do dispositivo móvel ao valor do risco calculado, auxiliando à classificar as redes. O objetivo consiste em melhorar a precisão do palpite do dispositivo móvel, levando em conta que a escolha quando sem todas as informações necessárias é uma aposta feita pelo dispositivo.

O SDHet classifica as redes de acordo com o $N_c$oferecido por elas com base na sua confidencialidade e na incerteza dos dados coletados. Estas funções são divididas em duas fases: a fase determinação do N_ce a fase de classificação dos PAs, que são inseridas entre a fase de coleta de dados e a fase de transição do *handoff*. A Figura 4.1 demonstra as fases do SDHet.

O SDHet possui as seguintes propriedades: A auto-preservação e a autonomia na

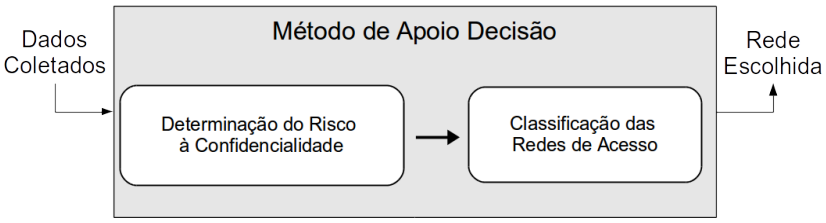

Figura 4.1: Fases do método

decisão quanto a falta de informações. A auto-preservação é a capacidade do dispositivo móvel de não se colocar em situação de risco. Ela visa a utilização do N_c de um AP para minimizar as escolhas prejudiciais ao dispositivo quanto a confidencialidade das transmissões neste PA. A autonomia relativa a falta de informações garante que o SDHet auxilie a decisão mesmo quando não possui todas as informações necessárias.

4.1.1 Modelo da rede

As HetNets integram tecnologias de comunicação com diferentes características [11]. Cada tipo de tecnologia possuí características específicas de desempenho, QoS e segurança que tornam complexa a avaliação das redes de acesso para tomada de decisão. O SDHet proposto foca nas propriedades de segurança, em particular nas características que garantem a confidencialidade das redes de acesso, para auxiliar a decisão de *handoff*.

As HetNets são compostas por dispositivos móveis, APs e redes centrais [3]. Os dispositivos móveis são heterogêneos quanto a suas características, possuindo capacidades de processamento, mobilidade e suporte à tecnologias de comunicação diferentes. Estas características influenciam o tempo gasto pelo processo de decisão. Este efeito pode gerar decisões que não atingem as necessidades do dispositivo, sendo que o processo de decisão pode utilizar valores não representativos da realidade no momento da decisão. Além disso, o grau de mobilidade dos dispositivos também é uma característica importante. Se o grau de mobilidade do dispositivo for alto e o processo de decisão levar muito tempo para avaliar os PAs, o dispositivo corre o risco de transitar para uma rede que está fora de alcance quando o processo termina. Desse modo, esta característica também influencia nas decisões de *handoff*. Por isso, o SDHet foca na simplicidade a fim de obter um tempo de decisão que minimize estes prejuízos ao dispositivo.

Os APs são heterogêneos quanto a suas configurações, suportando tecnologias de comunicação com características de segurança diferentes. Cada AP emprega somente uma tecnologia de comunicação em interface direta com a tecnologia dos dispositivos móveis. Independente da tecnologia de comunicação e dos seus mecanismos específicos de confidencialidade [73, 74], o SDHet considera as técnicas empregadas por estes mecanismos e o seu número presente nos APs para inferir o risco.

O SDHet assume que a rede heterogênea corresponde a um conjunto N composto por

ap APs identificados por $\{ap_1, ap_2, ap_3, ..., ap_i\}$, onde $ap_i \in N$. Cada AP ap_i possui um único identificador e pertence a uma rede central diferente. Como cada *ap* pertence a uma rede central diferente o *handoff* é sempre vertical, pois altera o sistema de comunicação mesmo quando a tecnologia para a qual se transita é a mesma. O identificador ap_i único é um número $\mathbb{N}$ e é usado na escolha e no controle do *handoff* entre os pontos de acesso.

A quantidade de dispositivos móveis com capacidade para transitar entre redes de diferentes tecnologias influencia no desempenho do processo de decisão. Os métodos de decisão centrados na rede podem perder em desempenho quando o número de dispositivos transitando excede a sua capacidade. Além disso, as informações usadas para comparação são de origens independentes para cada AP, como por exemplo, os desejos do usuário, a área de cobertura dos pontos de acesso, e o desempenho da rede central, dificultando a coleta de informações. Além disso, a autonomia do dispositivo deve ser respeitada na decisão do *handoff*, onde ele deve ser o responsável por escolher para qual rede transitar, evitando a transição para um PA não desejado. Por estes motivos, uma abordagem para tomada de decisão auxiliada pela rede e centrada no dispositivos torna-se mais interessante, considerando o tempo de decisão e a precisão na determinação de uma rede de acesso. Assim, o SDHet assume que o dispositivo decide para qual rede transitar auxiliado pelas informações fornecidas pelos PAs.

Cada tecnologias possui seus mecanismos que tentam garantir a confidencialidade. Estes mecanismos seguem os mesmos princípios da confidencialidade e empregam as técnicas que garantem estes princípios. Independente do tipo de tecnologia, cada AP possui mecanismos de confidencialidade de dois tipos: CA e DH. Os mecanismos de CA implementam as técnicas de autenticação, autorização e filtragem. Os mecanismos de DH empregam as técnicas de criptografia, esteganografia e ocultação de canal de comunicação.

4.1.2 Análise do risco nas decisões do processo de *handoff*

Os métodos de decisão para o processo de *handoff* propostos na literatura avaliam as propriedades de QoS e desempenho das redes de acesso. As características mais comuns são, RSS, *jitter*, *delay*, largura de banda. Estas características servem de critérios para comparação e classificação das redes disponíveis. Alguns métodos consideram a segurança como um critério importante de comparação e propõe uma maneira de pondera-lo. Porém, a segurança é abordada de maneira superficial, não sendo considerada as suas diferentes propriedades.

Os dispositivos móveis utilizam serviços e aplicativos com necessidades diferentes de segurança. Alguns serviços necessitam de disponibilidade da rede e serviços, outros de integridade dos dados, e outros de confidencialidade. Logo, selecionar a rede de acesso considerando a segurança como um único critério pode ser prejudicial, principalmente quando os requisitos de segurança de um dispositivo são diferentes do que o AP ou a

rede oferecem. Por exemplo, quando o dispositivo necessita de uma rede que oferece confidencialidade, mas a rede possui somente disponibilidade.

As características da comunicação sem fio, o meio de transmissão compartilhado e a possibilidade de dispositivos móveis interceptarem os dados sendo transmitidos no meio representam fatores de risco para o usuário da rede de acesso. Ao decidir por uma rede para transição, o dispositivo pode conectar-se em uma rede que possibilita a visualização não autorizada dos dados privados sendo transmitidos pelo dispositivo. Por este motivo, faz-se necessário uma abordagem detalhada da segurança, em especial da confidencialidade oferecida pelas redes de acesso, no processo de escolha. Este trabalho aborda a propriedade de confidencialidade como um critério de decisão.

A segurança pode ser aferida pela análise do risco presente em um sistema ou rede de acesso [15]. No contexto deste trabalho, a análise de risco aborda a probabilidade dos dados em transmissão serem interceptadas e entendidas. O SDHet propõe analisar o risco considerando a presença ou ausência de técnicas que garantem a confidencialidade para determinar a probabilidade subjetiva que se baseia neste fator de presença ou ausência. Para efetuar a análise, verifica-se a presença e a quantidade de técnicas que garantem a confidencialidade nas redes de acesso. Assim, o nível de confidencialidade é definido pelo risco de ocorrer o acesso indevido aos dados em transmissão enquanto transita pelas redes de acesso heterogêneas. O risco permite a avaliação da confidencialidade, quantificando-a para escolha de uma rede segura.

O SDHet predetermina para cada AP ap_i dois conjuntos AC e DH que reúnem as técnicas de controle de acesso e ocultação de informação que são consideradas. Cada conjunto é composto por t_{ac} e t_{dh} técnicas identificadas por, onde $AC = \{\, t_{ac_i} \mid 0 \leq i \leq k-1 \,\}$ e $DH = \{\, t_{dh_i} \mid 0 \leq i \leq l-1 \,\}$, sendo $|AC| = k$; $|DH| = l$. O SDHet assume que as informações sobre a presença ou ausência das técnica de confidencialidade em cada AP estão disponíveis sempre que o dispositivo móvel necessite e são adquiridos por ele na fase de coleta de dados. Além disso, cada dispositivo móvel pode possuir 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. A Figura 4.2 apresenta um cenário de risco.

Outro ponto observado nos principais trabalhos da literatura diz respeito a falta de informação. Nenhum dos métodos encontrados detalha seu funcionamento em casos onde faltam informações relacionadas aos critérios usados na decisão. Esta falta de informações pode gerar escolhas inconsistentes ou até falhas nos métodos de decisão. Como o SDHet assume a presença ou ausência de técnicas de confidencialidade nas redes de acesso, existe a possibilidade de não se saber nada a respeito da presença ou ausência deste técnicas. Por este motivo, o modelo de decisão da teoria da prospecção é adaptado para permitir a tomada de decisões no *handoff* sem informações das rede, possibilitando a melhor escolha

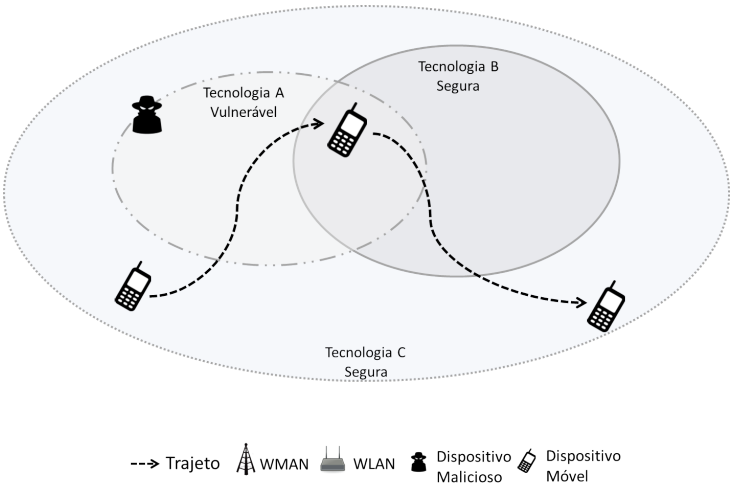

Figura 4.2: Cenário de risco

possível com as informações existentes sobre cada PA.

A não avaliação da segurança sem considerar suas propriedades distintas resulta em escolhas de redes inadequadas as necessidades dos dispositivos. Ademais, a falta de informações utilizadas na decisão também prejudica a eficiência e eficácia do processo. Sendo assim, este trabalho propõe um método de decisão para o *handoff* em redes heterogêneas que avalia a confidencialidade das redes de acesso e que consegue decidir quando faltam informações.

4.2 O método SDHet

Esta seção especifica o SDHet, um método de apoio à decisão que classifica as redes de acesso de acordo com o seu nível de confidencialidade e da falta de informações. O SDHet possui duas fases: a fase de determinação do N_c e a fase de classificação dos APs. Estas duas fases são especificadas nas subseções seguintes juntamente com o funcionamento do SDHet.

4.2.1 Determinação do nível de confidencialidade

O nível de confidencialidade N_c representa o valor classificatório dos APs. A determinação do N_c utiliza os valores do Risco à Confidencialidade (R_c, do inglês, Risk for Confidentiality), o Nível de Confiança (L_c, do inglês, *Level of Confidence*) e o Nível de Incerteza (L_u, do inglês, *Level of Uncertainty*) para cada ap_i. O (R_c) se baseia na presença ou ausência de alguma técnica de confidencialidade em cada ponto de acesso e quantifica o risco das transmissões de dados serem interceptadas e entendidas. O (L_c) considera o número de vezes que uma mesma técnica de confidencialidade está presente e representa o impacto do risco calculado. O (L_u) se baseia na falta de informações sobre a presença ou ausência

das técnicas e representa o impacto da falta de informações nas decisões. Os fatores de impacto são usados para decidir quando não existem todas as informações necessárias para decisão. O N_c é dado pela Equação 4.1 que considera o R_ce os fatores de impacto de confiança (L_c) e incerteza (L_u) e é realizado para cada ap_i.

$$N_c = C_r - (L_c - L_u) \tag{4.1}$$

Onde N_c corresponde ao nível de confidencialidade da rede ap_i. A diferença entre o nível de confiança L_c e o nível de incerteza L_u subtrai o valor do R_cR_c 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 incerteza, impactando na melhor rede a ser selecionada. Caso o nível de incerteza da existência das informações (L_u) 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.

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) e ocultação de dados (DH) [44, 46, 57]. Os mecanismos de AC englobam as técnicas de autenticação, autorização e filtragem, tais como senhas (autenticação), listas de permissão (autorização) e *proxys* (filtragem). Os mecanismos de DH empregam técnicas de criptografia e esteganografia, tais como criptografia simétrica (criptografia) e *fingerprinting* (esteganografia).

O SDHet assume que a fase de coleta executa sempre que uma decisão é necessária. Isto é, sempre que o *handoff* for iniciado. Toda vez que o SDHet é chamado, o cálculo recebe novos valores dos conjuntos AC e DH da fase de coleta e infere novos valores de classificação para cada AP ap_i. Assim, as decisões são tomadas com informações atualizadas a respeito das redes.

As informações provenientes da fase de coleta correspondem a presença, ausência ou falta de informações dos mecanismos de confidencialidade nas redes disponíveis. A presença designa a existência de um dos tipos de mecanismos e determina o número de mecanismos existentes que empregam aquele tipo de técnica. A ausência significa a certeza da falta de um tipo mecanismo e influencia no aumento do risco. A falta de informações representa a incerteza da presença ou ausência de um tipo de mecanismo. Estas informações são a base para a inferência dos fatores utilizados no SDHet.

4.2.1.1 Risco à confidencialidade

O risco à confidencialidade é a probabilidade de ocorrer alguma a espionagem dos dados sendo transmitidos. Como o processo de decisão no *handoff* precisa ser rápido e a aferição do risco precisa ser feita antes de transitar para uma rede, se faz necessária uma forma

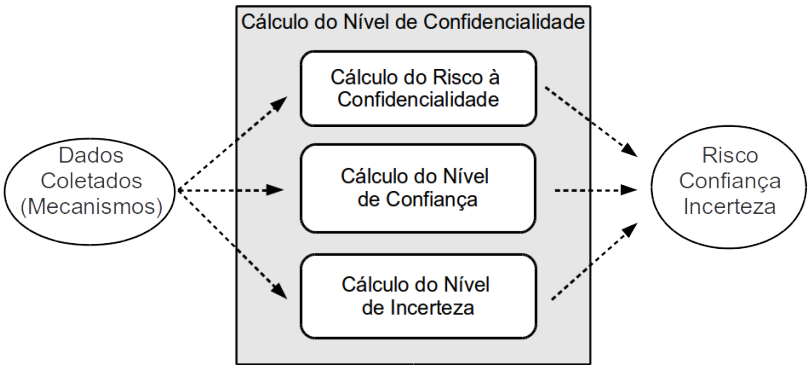

Figura 4.3: Fase de determinação do Nível à Confidencialidade

de aferir o a probabilidade de exposição das comunicações do dispositivo de maneira simples e eficaz. Entre as três regras mais simples de calculo de probabilidade (Frequência relativa, abordagem clássica e probabilidade subjetiva) [75], a técnica de probabilidade subjetiva se enquadra nos requisitos desejados para o *handoff*. Como não existem dados anteriores a respeito do evento (regra da frequência relativa) e a exposição dos dados do usuário depende de um número de fatores desconhecidos e que possuem probabilidades não igualmente prováveis (regra de abordagem clássica), aplica-se a regra subjetiva com o objetivo de alcançar a velocidade adequada de decisão pela simplicidade. A abordagem subjetiva utiliza conhecimentos circunstanciais para estimar a probabilidade do evento, neste caso, a presença ou ausência de um mecanismo de confidencialidade. Assim, o cálculo do valor do $R_c$se da pela Equação 4.2:

$$R_c = \{\, P_e + V_{at} - V_{pt} \mid \forall ap_i \in N, 0 \leq i \leq |N| - 1\} \tag{4.2}$$

O P_e corresponde à probabilidade subjetiva inicial de exposição das transmissões (50%) que é adicionada da diferença entre o impacto da ausência das técnicas de confidencialidade (V_{at}) e do impacto da existência das técnicas de confidencialidade(V_{pt}) no AP. Para facilitar o entendimento do método proposto, a Tabela 4.1 reúne a notação matemática utilizada para formulação das equações a seguir.

4.2.1.2 Probabilidade de exposição e probabilidade de proteção

Inicialmente, estima-se que P_e é de 0.5. Ou seja, inicialmente, sem nenhuma informação, o MD considera que cada rede apresenta 0.5 de chances de expor seus dados e 0.5 de chances de proteger os dados. O valor base P_b do impacto de qualquer técnica é $0,5/N$ de chances de proteger os dados, onde $N = |AC| + |DH|$. O SDHet assume que todos os mecanismos possuem a mesma importância e capacidade de proteger as informações. Este valor corresponde ao peso de um mecanismo de confidencialidade no cálculo do risco na rede.

O SDHet avalia a presença ou ausência de mecanismos de uma das classes (CA ou

Tabela 4.1: Notação empregada na especificação do SDHet

Notação	**Significado**
N_c	Nível de Confidencialidade
R_c	Risco à confidencialidade
L_c	Nível de confiança
L_u	Nível de incerteza
α	Valor de ponderação correspondente as técnicas de AC
β	Valor de ponderação correspondente as técnicas de DH
P_e	Probabilidade subjetiva inicial de exposição das transmissões
V_{at}	Impacto das técnicas ausentes no ponto de acesso
V_{pt}	Impacto das técnicas presentes no ponto de acesso
$F_v()$	Função que determina as técnicas de CA e OI ausentes ou presentes
$F_v()$	Função que determina as técnicas repetidas de CA e OI presentes
$F_u()$	Função que determina as técnicas de CA e OI sem informação

OI) em cada ap_i. A Equação 4.3 define o valor do impacto de cada mecanismo ausente no valor de P_e. Onde, a função $F_v()$ resulta em um valor booleano 0,1, que identifica presença (1) ou a ausência (0) de uma técnica de AC e DH em ap_i. Esta função verifica os k elementos de AC e os l elementos de DH. O valor base das técnicas P_b multiplica um fator ponderativo α ou β que depende do tipo da técnica. Isto é feito pois cada técnica pode possuir um peso diferente para o dispositivo móvel, por exemplo, uma técnica de criptografia pode ser mais útil do que um técnica de esteganografia. O valor final de cada técnica deve respeitar a Equação4.4.A ponderação das técnicas não é considerada no escopo deste trabalho, podendo ser realizada por diferentes métodos [38]. O resultado de $F_v()$ é multiplicado pelo respectivo valor de cada técnica e somado. A soma dos valores referentes aos dois somatórios representa impacto das técnicas de confidencialidade ausentes ausentes.

$$V_{at} = \sum_{i=0}^{k-1} F_v(t_{ac_i}) * (P_b * \alpha_{t_i}) + \sum_{i=0}^{l-1} F_v(t_{dh_i}) * (P_b * \beta_{t_i}) \tag{4.3}$$

$$\sum_{i=0}^{k-1} (\alpha_{t_i} * P_b) + \sum_{i=0}^{l-1} (\beta_{t_i} * P_b) = 0.5 \tag{4.4}$$

Do mesmo modo, a Equação 4.5 determina o impacto da presença das técnicas de confidencialidade em cada ap_i. Onde, a função $F_v()$ identifica a presença (1) ou ausência de uma técnica de AC e DH em ap_i. O valor base das técnicas P_b multiplica um fator ponderativo α ou β que depende do tipo da técnica. Este valor é multiplicado pelo resultado de F_v e depois somado. A soma dos valores referentes aos dois somaorios resulta no total que representa impacto das técnicas de confidencialidade presentes na rede ap_i.

$$V_{pt} = \sum_{i=0}^{k-1} F_v(t_{ac_i}) * (P_b * \alpha_{t_i}) + \sum_{i=0}^{l-1} F_v(t_{dh_i}) * (P_b * \beta_{t_i}) \quad (4.5)$$

Caso não existam informações sobre a presença ou ausência de um tipo de mecanismo, o valor do respectivo tipo de mecanismo não é adicionado a probabilidade subjetiva de exposição e nem a probabilidade subjetiva de proteção. Nestes casos, registra-se a falta de informações para a posterior utilização do valor na fase de escolha. A presença da incerteza define o valor do **nível de incerteza** nas redes disponíveis. Este valor influencia o comportamento da decisão na segunda fase.

O SDHet assume que o valor do $R_c$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 [19]. Da mesma forma, nenhum sistema pode ser considerado 100% vulnerável. Este valor influencia na classificação das redes de acesso.

4.2.1.3 Fatores de impacto: confiança e incerteza

Outros valores que influenciam na decisão são: nível de confiança (L_c) e nível de incerteza (L_u). O valor de L_c representa o impacto do número de técnicas de um mesmo tipo no valor do R_c. Este fator é inspirado na função de ponderação do impacto de um evento da teoria da prospecção que mapeia o impacto de um evento para o decisor. O SDHet baseia-se nesta função para definir um valor que auxilie a ponderar e selecionar o AP quando ocorre a falta de informações de algum critério.

O cálculo deste valor se baseia na quantidade de técnicasrepetidas presentes em um ap_i. A soma do número de técnicas de cada tipo multiplicados pelo valor base do tipo do mecanismo ponderado retorna o nível de confiança L_c. O cálculo deste valor dado pela Equação 4.6:

$$L_c = \sum_{i=0}^{k-1} F_c(t_{ac_i}) * (P_b * \alpha_{t_i}) + \sum_{i=0}^{l-1} F_c(t_{dh_i}) * (P_b * \beta_{t_i}) \quad (4.6)$$

Onde $L_c()$ representa o impacto do nível de confiança da rede ap_i. O somatório do número de técnicas nos conjuntos AC e DH é multiplicado pelo valor base ponderado de suas técnicas para designar o L_c. O L_c determina a confiança do dispositivo no R_c calculado para um ponto de acesso.

O nível de incerteza corresponde a quantidade de técnicas sem nenhuma informações a respeito da presença ou ausência em cada ap_i. Este valor é inspirado na função que mapeia o impacto de fatores como a incerteza 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 tipos de mecanismos sem informações multiplicados pelo valor base ponderado da técnica resulta o valor incerteza. O cálculo deste valor ocorre da

seguinte maneira:

$$L_u = \sum_{i=0}^{k-1} F_u(t_{ac_i}) * (P_b * \alpha_{t_i}) + \sum_{i=0}^{l-1} F_u(t_{dh_i}) * (P_b * \beta_{t_i}) \quad (4.7)$$

Onde as funções $F_u()$ determinam o número de técnicas de AC e DH sem informações na rede ap_i. A quantidade de cada conjunto é multiplicada pelo valor base ponderado de cada técnica. A soma dos valores referentes aos dois conjuntos resulta no total que representa a probabilidade subjetiva dos mecanismos sem informações.

4.2.2 Classificação das redes de acesso

A fase de classificação das redes de acesso ordena o valor classificatórios em N para ordenação das redes. O valor do R_c é o principal critério na comparação. O SDHet considera que é mais importante a existência de tipos diferentes de mecanismos do que a quantidade de mecanismos de um mesmo tipo em uma rede de acesso. Como as diferentes classes de mecanismos protegem aspectos diferentes da confidencialidade, quanto mais classes de mecanismos presentes na rede menor o risco para o dispositivo.

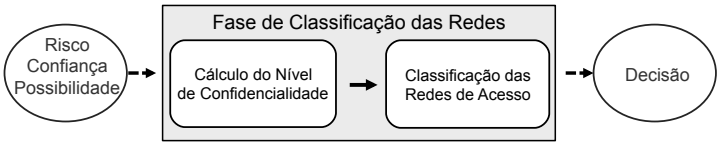

Figura 4.4: Fase de classificação das redes

A quantidade de mecanismos de um mesmo tipo é usada como um fator de desempate. As redes de acesso podem possuir o mesmo valor de $R_c$devido ao número limitado de técnicas consideradas. Por isso, usa-se a quantidade de mecanismos de um mesmo tipo como um ponderador que diminui o impacto do risco oferecido pelas redes. Quanto mais mecanismos de um mesmo tipo, menor o valor do risco. O grau de incerteza determina o impacto da incerteza na decisão. Este valor representa a insegurança ao escolher um rede com falta de informações. Ele pondera positivamente o $R_c$apresentado por uma rede e serve como um fator de desempate. Com isto em perspectiva, o comportamento de decisão do SDHet corresponde, em partes, o comportamento modelado na teoria da prospecção e seleciona a rede considerando a incerteza de perder ou ganhar. Mesmo que a rede selecionada não seja a rede que oferece o menor risco ao dispositivo, a escolha sempre será por uma rede que apresenta um baixo risco e uma menor incerteza das informações. A Figura 4.5 apresenta o fluxograma que resumo o funcionamento do SDHet e suas fases.

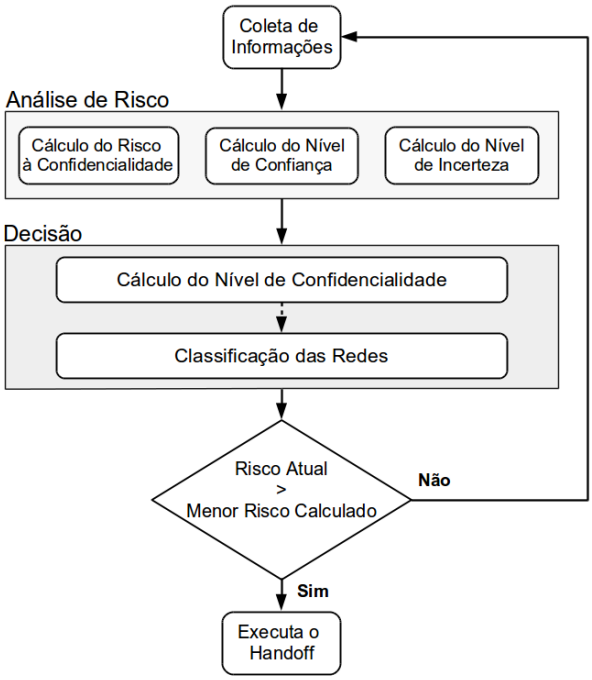

Figura 4.5: Funcionamento do SDHet

4.3 Funcionamento do SDHet

Esta seção demonstra o funcionamento do SDHet proposto e suas operações. Inicialmente são apresentados os cálculos do risco à confidencialidade (R_c), seus elementos (V_{at} e V_{pt}) e a inferência dos níveis de confiança (L_c) e incerteza (L_u). Em seguida, a fase de classificação é detalhadas na seção.

4.3.1 Estrutura dos dados coletados

Como base no método SDHet, o dispositivo móvel recebe dois conjuntos de dados AC e DH contendo as informações dos mecanismos de controle de acesso e ocultação de informação detectados no AP ap_i. A Figura 4.6 ilustra uma topologia simples e a estrutura dos dados coletados usados pelos dispositivos na definição do *handoff*. Os dispositivos transitam por uma área contendo três redes de tecnologias diferentes, e os dados recebidos pelo método estão representados na caixa pontilhada, onde a rede de ID A possui os conjuntos $CA = \{1, -1, 2\}$ e $DH = \{1, 0\}$, a rede de ID B possui os conjuntos $CA = \{0, 0, -1\}$ e $DH = \{-1, -1\}$ e rede de ID C possui os conjuntos $CA = \{2, 1, 3\}$ e $DH = \{2, 0\}$. Os valores representam respectivamente as técnicas de autenticação (AC), autorização (AC), filtragem (AC), criptografia (DH) e esteganografia (DH). Os valores variam de -1 (sem informações), 0 (nenhum mecanismo), 1, 2 e 3 (número de mecanismos presentes).

4.3.2 Cálculo do R_c, L_c e L_u

Com as informações a respeito dos mecanismo encontrados nas redes de acesso, o próximo passo é calcular o valor do $R_c$utilizando a equação 4.2. Para isso, primeiro calcula-se o valor de $V_{pt}(ap_i)$ e $V_{pt}(ap_i)$, usando as Equações 4.3 e 4.5, que determinam a probabilidade subjetiva de exposição e a probabilidade subjetiva de proteção. A Figura 4.6 apresenta um cenário referenciando a especificação do funcionamento do SDHet.

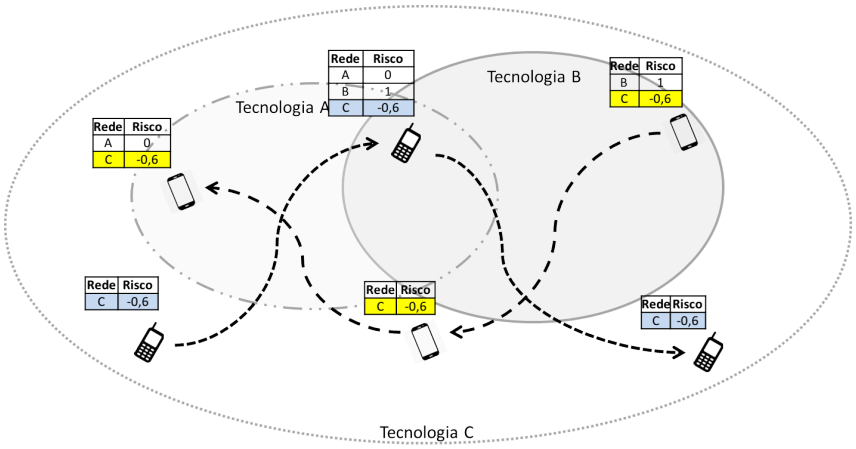

Figura 4.6: Exemplo de funcionamento do SDHet

Para utilizar estas equações é preciso primeiro identificar o valor base de cada tipo mecanismo ($P_i * \alpha$). Como o valor da probabilidade de proteção é 0,5 (50%) e o valor de α, que representa o peso de cada mecanismo, foi ajustado para considerar que todas as técnicas tem importancia igual, o valor base de cada técnica de segurança consiste de $0,1$ devido ao cálculo da Equação 4.3 onde ($P_i * \alpha = 0,5 * 0,2$) para cada mecanismo em cada grupo.

Em seguida, a Equação 4.3 infere o valor dos mecanismos ausentes nas redes. O valor base de $0,1$ multiplicado pelo número de tipos de mecanismos ausentes nos dois conjuntos. Na rede de ID A, $V_{at}(A) = F_v(AC) * 0,1 + F_v(DH) * 0,1 = 0 * 0,1 + 1 * 0,1 = 0,1$. Cálculo similar ocorre na rede B e C. Na rede de ID B, $V_{at}(1) = F_v(AC) * 0,1 + F_v(DH) * 0,1 = 2 * 0,1 + 0 * 0,1 = 0,2$. Na rede de ID C, $V_{at}(1) = F_v(AC) * 0,1 + F_v(DH) * 0,1 = 0 * 0,1 + 1 * 0,1 = 0,1$.

O próximo passo é determinar o valor de V_{pt} pela equação 4.5. Para isso, o valor base da técnica presente $0,1$ multiplicado pelo número de técnicas com mecanismos presentes nos dois conjuntos. Na rede de ID A, $V_{at}(A) = F_v(AC) * 0,1 + F_v(DH) * 0,1 = 2 * 0,1 + 1 * 0,1 = 0,3$. Na rede de ID B, $V_{at}(1) = F_v(AC) * 0,1 + F_v(DH) * 0,1 = 0 * 0,1 + 0 * 0,1 = 0$. Na rede de ID C, $V_{at}(1) = F_v(AC) * 0,1 + F_v(DH) * 0,1 = 3 * 0,1 + 1 * 0,1 = 0,4$.

Com os valores de $V_{pt}(ap_i)$ e $V_{pt}(ap_i)$ inferidos é possível calcular o valor de R_c. Aplicando a equação 4.2 obtém-se para a rede de ID A o valor de $CR_{(A)} = 0,3$, para rede de ID B o valor $CR_{(B)} = 0,7$ e para rede de ID C o valor $CR_{(C)} = 0,2$. Em seguida,

a equação 4.6 calcula o nível de confiança L_c das redes. Para a rede de ID A o valor $L_c(A) = 0,04$. Na rede de ID B, $L_c(B) = 0$ e na rede de ID C, $L_c(C) = 0.8$. A equação 4.7 calcula o nível de incerteza L_u das redes. Para a rede de ID A consegue-se o $L_u(A) = 0,1$. Na rede de ID B o valor de $L_u(B) = 0,3$ e na rede de ID B o valor de $L_u(B) = 0$.

4.3.3 Cálculo do valor classificatório

O passo final é a classificação das redes pelo valor de N_c 4.1. Para a rede de ID A o valor classificatório resulta em $N_c(A) = 0,3 - (0,4 - 0,1) = 0$. Para a rede de ID B o valor classificatório resulta em $N_c(B) = 0,7 - (0 - 0,3) = 1$. Para a rede de ID C o valor classificatório resulta em $N_c(C) = 0,2 - (0,8 - 0) = -0,6$. Assim, o dispositivo móvel transita para a rede com mais confidencialidade e confiança. Na Figura 4.6, a seleção é representada pela linha da tabela que está marcada.

4.4 Resumo

Este capítulo apresentou a descrição do SDHet, um método de apoio a tomada de decisão no *handoff* em redes heterogêneas que tenta prevenir a transferência da conexão do MD para redes com risco à confidencialidade das transmissões. O SDHet considera as características de confidencialidade das redes e a falta de informações sobre os critérios de comparação para classificá-las. O funcionamento do SDHet é baseado em duas fases, sendo elas, a fase de determinação do R_ce a fase de classificação das redes. A primeira fase determina o valor do risco à confidencialidade oferecido por uma rede, considerando as informações coletadas a respeito dos mecanismos de confidencialidade. Por fim, a fase de classificação ordena as redes do menor nível de confidencialidade para o maior.

CAPÍTULO 5

AVALIAÇÃO DO SDHET

Este capítulo apresenta a avaliação de desempenho do SDHet nas decisões de *handoff* em HetNets, considerando a eficiência e a eficácia das decisões em evitar as redes com maior risco à confidencialidade das transmissões do dispositivo móvel. A Seção 5.1 apresenta o ambiente de simulação, os cenário utilizados na avaliação e seus parâmetros. A Seção 5.2 descreve as métricas de eficiência e eficácia usadas na avaliação de desempenho. As Seções 5.3 e 5.4 apresentam e discutem os resultados da avaliação de eficácia e eficiência, respectivamente.

5.1 Ambiente de avaliação

A avaliação de desempenho do SDHet foi realizada através de simulações. O SDHet foi implementado no simulador NS3 utilizando a linguagem C++. A implementação teve como base os módulos existentes de WiFi, de LTE e no MIHF (*Media Indepedent Midia 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. O NS3 é largamente utilizado para avaliação de desempenho pela comunidade acadêmica e foi escolhido por possuir um conjunto recursos que possibilitam a simulação de redes heterogêneas.

A implementação do MIHF utilizada foi desenvolvida por [76]. O MIHF gerencia a transferência da conectividade através da desconexão do dispositivo móvel da rede atual antes de iniciar a conexão com o novo ponto de acesso, existindo um intervalo de interrupção do serviço em uso. Esta interrupção afeta o *handoff*, mas não tem impacto sobre a avaliação de desempenho do processo de decisão.

O MIHF [76] não possui um módulo de decisão. Por isso, um módulo de classificação e escolha de HetNets foi criado para coordenar o processo de decisão, implementando o SDHet na linguagem C++. O módulo recebe como entrada as informações coletadas pela primeira fase do processo de *handoff*. Como esta fase não foi implementada, a coleta foi simulada através de um gerador de números aleatórios que produz os valores referentes a quantidade de mecanismos de cada técnica de confidencialidade considerada pelo SDHet em cada rede. Os valores são gerados e analisado uma vez para cada rede por simulação.

O método proposto por Li e Cheng [25], chamado de MLC, foi implementado no NS3 com o objetivo de comparar os resultados com o SDHet. Este método foi escolhido pela sua simplicidade e pelo seu desempenho alcançados ao utilizar uma função objetivo para classificação das rede. A função objetivo é considerado a estratégia com o melhor

desempenho [38] entre as mais utilizadas para a decisão, sendo aplicada também no modelo de decisão prospectivo. O MLC considera a segurança como critério de comparação, porém não analisa seus diferentes aspectos e propriedades. Ele foi usado para comparação de desempenho e para mostrar a relevância de analisar adequadamente a segurança.

5.1.1 Cenários e parâmetros

Os cenários usados na avaliação consideram dois ambientes: local e metropolitano. Os cenários possuem propriedades particulares de mobilidade para nó móvel, da área de disposição das entidades 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 $1,5m/s$ [77], representando um ambiente pequeno como uma casa ou uma rua, onde o usuário é um pedestre. O número de redes sobrepostas neste cenário correspondem a uma rede WiFi e uma rede LTE. O ambiente metropolitano corresponde a um cenário urbano com uma área de 400mx400m, representando o caminho que um usuário móvel faz quando se locomove de casa até o trabalho. A velocidade do nó móvel representa a de um veículo se 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 [78]. O padrão de mobilidade do dispositivo móvel é aleatório, baseado em [79].

Os APs em cada cenário foram agrupados respeitando três configurações para sobreposição da área de cobertura, conforme [77]: *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 e menor que 20 APs em uma mesma região. O ambiente local possui somente a baixa sobreposição. O ambiente metropolitano possui áreas onde a proporção vária entre baixa, média e alta. Os agrupamentos são distribuídos aleatoriamente pelos cenários [78]. 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 RSS e de confidencialidade (técnicas de controle de acesso e ocultação da informação) dos APs para classificação das redes. O RSS é medido a cada 2 segundos para garantir que o nó não fique sem conectividade, além de determinar a necessidade de transição e execução o método de decisão. Ademais, a detecção de um AP que ainda não teve o risco à confidencialidade avaliado também aciona a execução do módulo de decisão. Desta forma, sempre que uma de rede de acesso ainda não conhecida pelo nó móvel é detectada, o método infere o seu nível de confidencialidade. A Tabela 5.1 resume os parâmetros dos cenários avaliados.

Os APs possuem duas configurações quanto à segurança: Baixo Risco à Confidencialidade (LCR, do inglês, *Low Confidentiality Risk*) e Alto Risco à Confidencialidade

Tabela 5.1: Parâmetros da simulação do método de tomada de decisão

Parâmetros	**Valores**	
Áreas	Local	$30mx40m$
	Metropolitano	$400mx400m$
Sobreposição	Baixa	2-4 Redes
	Média	5-10 Redes
	Alta	10-20 Redes
Tecnologia	WiFi	70 m^2
	LTE	1500 m^2
Velocidade	1 m/s; 11.5 m/s	
Nr. Critérios de Decisão	5	
Variação d0 NUC	[0:5]	

(HCR, do inglês, *High Cinfidentiality Risk*). 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, variando sua quantidade entre 1-4 para cada técnica. A HCR configura cada ponto de acesso 30 % a menos do número de mecanismos de confidencialidade que a LCR e com 30% a mais para o valor RSS. Esta configuração corresponde a pontos de acesso com risco à confidencialidade. O número de pontos de acesso do tipo HCR é 30% do número total de pontos de acesso em cada cenário. Desta forma, os cenários representam uma situação de risco em que o dispositivo móvel pode tomar decisões prejudiciais. Além disso, os pontos de acesso podem possuir outros mecanismos de segurança que garantem os princípios de integridade e disponibilidade. Desta forma, os dois métodos devem decidir por pontos de acesso com e sem confidencialidade, além de existirem pontes de acesso que garantem os outros princípios de segurança.

O SDHet não verifica a eficiência e a eficácia das técnica 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, criptografia, etc.). Esta variação foi definida com base na quantidade de mecanismos, que aplicam alguma técnica de confidencialidade, presentes na literatura [44, 46, 57]. Este parâmetro pode ser variado conforme o contexto ou a necessidade. Nesta avaliação, o número total de mecanismos de uma mesma técnica foi limitado para quatro. A Tabela 5.2 apresenta a associação das técnicas com exemplos dos seus respectivos mecanismos.

Tabela 5.2: Associação das técnicas de confidencialidade com os mecanismos

Técnicas	**Controle de Acesso**			**Ocultação a Informação**	
	Autenticação	*Autorização*	Filtragem	*Criptografia*	*Esteganografia*
Mecanismos	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

5.2 Métricas

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, impacto do método na confidencialidade das transmissões e exatidão dos valores classificatórios inferidos para a confidencialidade. A acurácia da seleção de redes confidenciais foi baseada em [80] 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 impacto do método na confidencialidade das transmissões verifica o impacto do uso do SDHet para selecionar pontos de acesso com confidencialidade nas suas transmissões. A exatidão dos valores classificatórios inferidos para a confidencialidade foi inspirada em [81] e 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. Esta métrica representa o erro do SDHet ao inferir o nível de confidencialidade dos APs quando sem todas as informações dos critérios. A avaliação de eficiência usou a métrica de velocidade de decisão, que averígua o tempo decorrido na classificação e escolha da rede com maior confidencialidade [23]. 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%.

Acurácia da seleção de redes confidenciais (ASRC): Esta métrica afere a eficácia das decisões quanto a escolha da rede menos arriscada com base no nível de confidencialidade de cada uma. Ela representa a acurácia do SDHet ao escolher a rede de acesso com maior confidencialidade. Ela foi aferida para o SDHet em duas situação diferentes: quando se tem todas as informações e variando o número de critérios sem informação. A Equação 5.1 calcula esta métrica.

$$Tx_r = \sum_{j=1}^{E} (NrA/N_rDecs) \tag{5.1}$$

Onde Tx_r representa a taxa média de acerto do método avaliado (SDHet ou MLC). NrA representa o número de vezes que o o método escolheu a rede disponível que apresentava o maior nível de confidencialidade. N_rDecs corresponde ao número total de decisões realizadas. E é o número de simulações feitas. O resultado corresponde a taxa média de acerto entre todas as decisões realizadas.

Impacto do método na confidencialidade das transmissões (IMCT): Está métrica mede o tempo de transmissão do MD utilizando um rede de acesso avaliada e o seu respectivo valor de nível de confidencialidade. Através dela é possível detectar se avaliar a segurança de maneira composta é vantajoso. Durante uma simulação, o tempo de transmissão em cada rede é armazenado junto com o identificador da rede e com o nível

de confidencialidade dela. Os dados dos dois métodos são comparados par determinar qual deles proporcionou mais tempo de transmissão pela rede com maior confidencialidade.

Exatidão dos valores classificatórios inferidos (VCI): Esta métrica verifica a diferença média entre os valores do nível de confidencialidade calculados pelo SDHet em comparação com os valores realmente existentes nas redes. Ela estima a diferença média entre dos valores inferidos quando o número de critérios sem informações (NUC, do inglês, *Number of Unknown Criteria*) varia. A métrica é calculada através da Equação 5.2.

$$V_nc = \frac{\sum_{j=1}^{E} |(|I_{sdhet}(NUC)| - |I_{ValorReal}|)|}{N_rDecs} \tag{5.2}$$

Onde V_nc representa a variação média do nível de confidencialidade. $I_{sdhet}(NUC)$ corresponde ao valor de NC inferido pelo SDHet com a variação do NUC. $I_{ValorReal}$ corresponde ao número valor da inferência para a mesma rede, porem considerando todas as informações. Neste caso, para avaliar esta métrica, conforme aumenta o número de critérios sem informação, para cada NUC é gerado um valor aleatório correspondente ao número real de mecanismos. O SDHet avalia o conjunto de critérios com os valores considerando o NUC, e um outro modulo também executando o SDHet avalia a mesma rede, sob as mesmas condições, porém para cada NUC, o valor dinamicamente gerado para os mecanismos sem informação é usado. Desta forma, esta métrica representa o quão preciso e confiável são as inferências do SDHet.

Velocidade de uma decisão (VD): Ela afere 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. A métrica é calculada pela Equação 5.3.

$$T_m = \frac{\sum_{j=1}^{E}(T_f - T_i))}{N_rDecs} \tag{5.3}$$

Onde T_m representa o tempo médio de decisão. T_f corresponde ao tempo final de decisão, ou seja, o momento em que o método selecionou uma rede. T_i representa o tempo inicial da decisão, ou seja, o momento em que o método foi chamado. N_rDecs corresponde ao número total de decisões realizadas.

A métrica ASRC foi mensurada na avaliação dos dois métodos e os resultados foram analisados e comparados para os dois cenários definidos. Ela aferiu o tempo de decisão variando o número de critério ($NC = |AC| + |DH| = 5$) usados pelos métodos em função do número de redes para comparação. A Figura 5.1 apresenta um representação dos ambientes ondes as métricas foram aferidas.

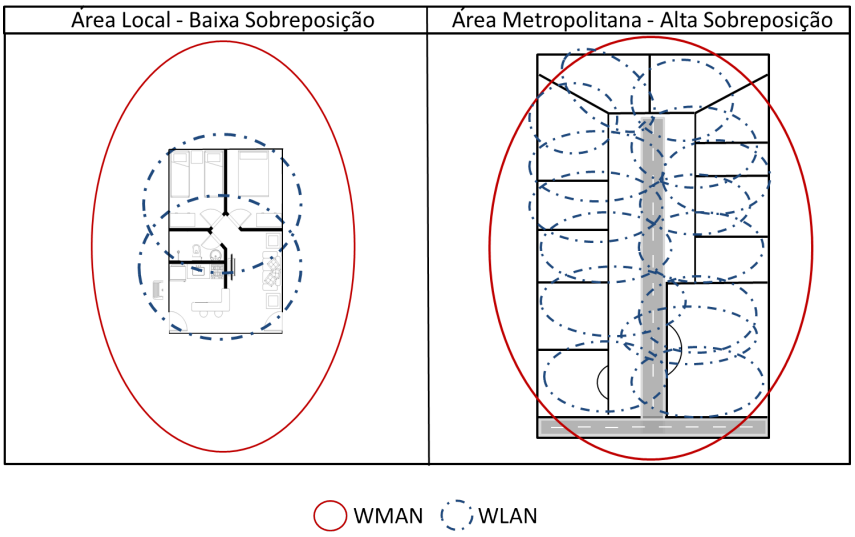

Figura 5.1: Representação dos cenários da avaliação

5.3 Resultados de eficácia

Esta seção apresenta os resultados da avaliação da eficácia do SDHet ao inferir o nível de confidencialidade e selecionar os pontos de acesso com base neste nível. A eficácia do SDHet foi avaliada pelas métricas ASRC, IMCT e VCI, variando a quantidade de critérios sem informação (NUCs). A eficácia do MLC foi avaliada somente pelas métricas ASRC e IMCT, onde ambas foram aferidas sem a falta de informações, pois MLC não foi projetado para lidar com esse fator. Ambos os métodos foram avaliados considerando que a necessidade do dispositivo móvel é somente de confidencialidade nas transmissões, desconsiderando os outros princípios de segurança por nãos ser o foco deste trabalho.

A acurácia do SDHet e do MLC (ASRC) correspondem as taxas de acertos de suas escolhas. A Figura 5.2 mostra a acurácia alcançada pelo SDHet e pelo MLC nos cenários propostos, sem variar a quantidade de critérios de decisão sem informação. O SDHet obteve 100% de acurácia ao selecionar as redes de acesso de maior confidencialidade, como era esperado. Isto ocorreu porque as propriedades de confidencialidade de cada ponto de acesso são avaliadas separadamente, permitindo a inferência com precisão do valor do risco à confidencialidade e a seleção precisa da rede que oferece maior confidencialidade nas transmissões. Como a avaliação é feita com base na propriedade de confidencialidade das redes, o SDHet possui melhor eficácia. Nota-se que a quantidade de redes comparadas em cada decisão não tem impacto sobre a acurácia das escolhas do SDHet, não variando a taxa de acerto. O MLC avalia a segurança de forma genérica, o que resulta na obtenção de taxas de acerto menores quando se avalia a necessidade especifica do principio de confidencialidade. Este fator prejudica a sua acurácia e a seleção da rede de maior confidencialidade. Para o MLC quanto maior o numero de redes, maior a possibilidade do nível de segurança inferido ser relacionado aos princípios de integridade e disponibilidade,

além de ter de decidir entre redes com um nível de confidencialidade diferente.

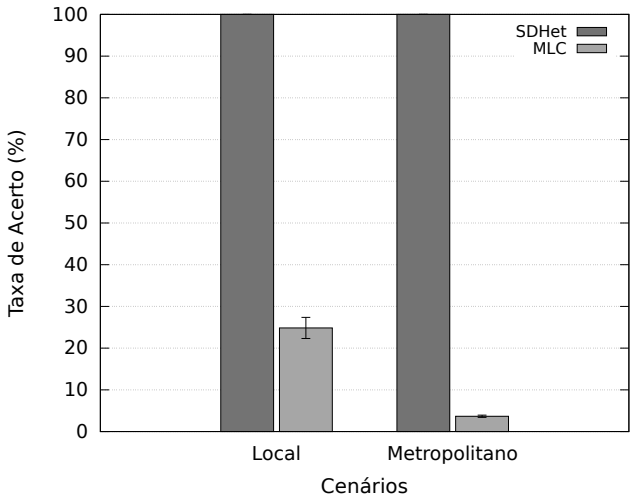

Figura 5.2: Comparação da acurácia das decisões dos métodos (ASRC)

Os resultados alcançados comprovam que a avaliação da segurança de maneira composta, através da separação e analise das características de um princípio, aumenta a acurácia das escolhas quando a necessidade do dispositivo móvel. No contexto desta avaliação, a analise do critério segurança de forma genérica leva o dispositivo a assumir que uma rede segura seja necessariamente uma rede confidencial. Este fator pode colocar o dispositivo móvel em situações de risco, expondo seus dados transmitidos em casos de necessidade de confidencialidade, como ocorre como as escolhas executadas pelo MLC. Assim, o SDHet possui um impacto relevante na segurança da conectividade do dispositivo móvel por atender a necessidade de escolher com base na confidencialidade das transmissões.

O impacto do SDHet na confidencialidade das transmissões foi verificado para o ambiente local com baixa sobreposição de redes (2-4 redes) e para o ambiente metropolitano variando as áreas de sobreposição em média (5-10 redes) e alta (10-20 redes). Os resultados apresentados pelos gráficos na Figura 5.3 mostram o tempo decorrido das transmissões do dispositivo móvel através de redes em função do valor do nível de confidencialidade inferido. A avaliação do impacto refere-se a uma amostra de tempo em cada cenário. Como o SDHet decide por redes com pouca ou nenhuma confidencialidade (quando o principio de segurança do AP é integridade ou disponibilidade) algumas transmissões ocorrem por redes sem nenhuma confidencialidade. Os resultados são referentes a amostras de tempo de algumas simulações.

Em comparação ao MLC, as escolhas do SDHet proporcionam um maior nível de confidencialidade nas transmissões do dispositivo móvel em todos os cenários de avaliação. Este comportamento ocorre porque o SDHet seleciona as redes que possuem a maior quantidade de mecanismos que aplicam técnicas de confidencialidade, diferenciando com

maior precisão as redes que podem expor as transmissões do dispositivo móvel. Dessa forma, quanto mais redes disponíveis com mecanismos de confidencialidade maior é o tempo de transmissão por redes que oferecem maior confidencialidade.

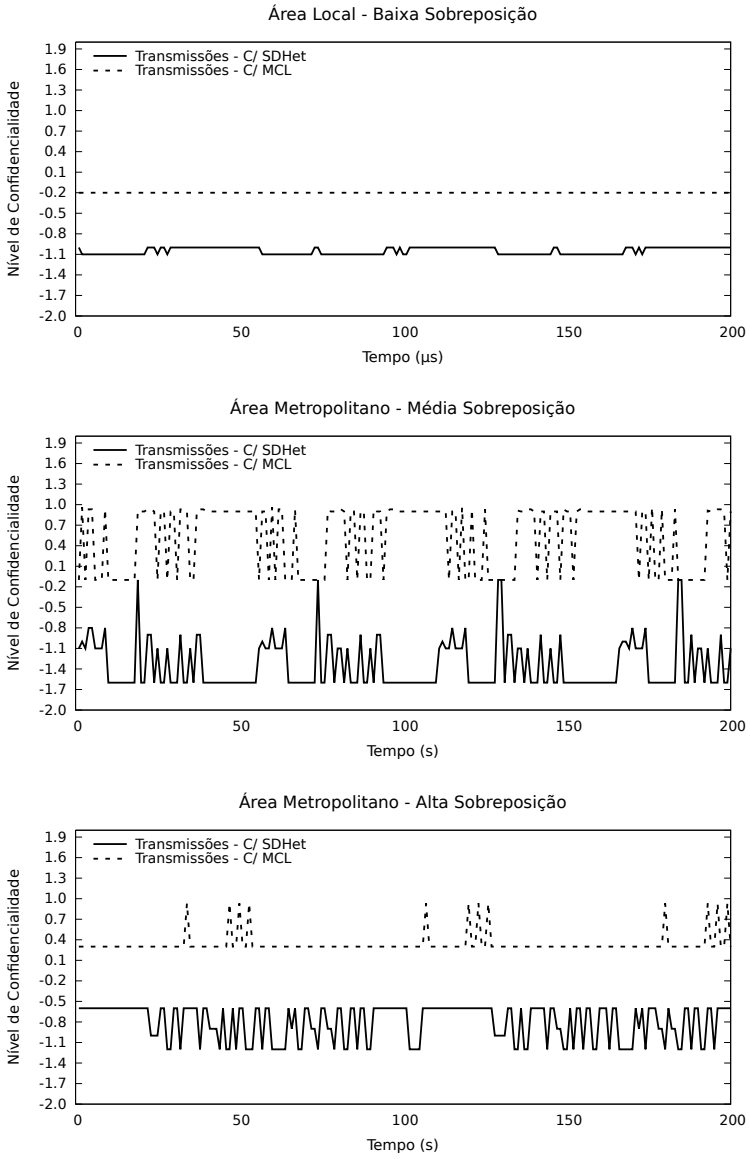

Figura 5.3: Impacto das decisões na confidencialidade das transmissões (IMCT)

Os resultados apresentados mostram o aumento da confidencialidade das transmissões ao empregar o SDHet para decisões baseadas em confidencialidade. O impacto das escolhas que consideram a confidencialidade previne a exposição dos dados sendo transmitidos através da previsão de qual das redes de acesso oferece a maior garantia de transmissões confidencias. O número de redes não teve impacto na confidencialidade das transmissões, porém, vale a observação de que se caso as redes de acesso disponíveis no ambiente possuam poucos ou nenhum mecanismo de confidencialidade, o SDHet sempre escolherá a que tiver maior quantidade de mecanismos, o que neste caso levará indiferentemente ao

uso de uma rede com poucos mecanismos ou nenhum. Por outro lado, é possível verificar a ocorrência do efeito ping-pong, que é caracterizado por sucessivas transições com poucos segundos de intervalo. Isto ocorre devido a quantidade de número de pontos de acesso ao alcance do dispositivo móvel, da sua mobilidade enquanto transita na borda de um rede e da falta de um mecanismo que gerencie a necessidade de transição.

O efeito da falta de informações a respeito dos critérios foi verificada pela métrica ASRC através da variação da quantidade de critérios sem informação (NUC) presentas na decisão. Está variação corresponde a [1:NC] onde NC é o número total de critérios de comparação. Para calcular a taxa média de acerto, o nível de confidencialidade foi inferido através de dois módulos de decisão presentes no mesmo dispositivo móvel simulado. Cada taxa corresponde a uma simulação diferente. Os dois módulos utilizaram o SDHet para as inferências, com a diferença de que um módulo recebeu todas as informações sobre os mecanismos de confidencialidade nas redes e outro módulo recebia a variação na quantidade de critérios com informações. Dessa forma, um módulo inferiu o NC com informações de todos os critérios e o outro inferiu variando o quantidade de critérios com informações.

O número de vezes que o SDHet escolhe a rede disponível com o melhor nível de confidencialidade representa a acurácia do método em situações adversas, como quando faltam informações sobre os critérios de comparação. A avaliação foi realizada nos dois cenários, onde o ambiente local foi configurado com a sobreposição baixa e o ambiente metropolitano foi configurado variando o número de redes sobrepostas em médio e alto. A Figura 5.4 mostra as taxas de acerto do método quanto a variação do NUC para os cenários definidos.

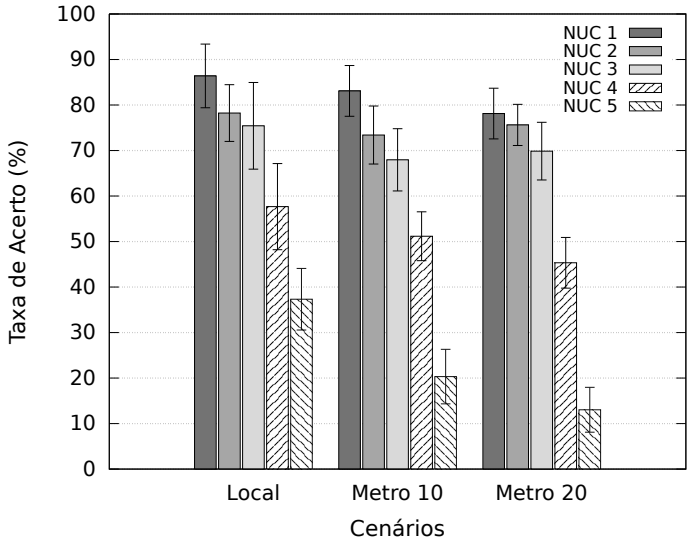

Figura 5.4: Exatidão das decisões com ausência de informações (VCI)

Os resultados mostram que a acurácia do SDHet varia conforme o NUC aumenta. Quanto maior o NUC, maior o erro na inferência do nível de confidencialidade das redes,

resultando em escolhas inadequadas baseadas em informações imprecisas. Dessa forma, o impacto da falta de informações é negativo nas escolhas do SDHet, aumentando o número de escolhas por redes com maior potencial de expor as transmissões dos usuários. Entretanto, apesar da acurácia 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, além de manter uma taxa de acerto acima de 50%. Isto comprova a eficácia da adaptação do modelo de decisão prospectivo nas decisões de handoff.

As escolhas do SDHet consideram o CR, o número de critérios conhecidos e o número de mecanismos de confidencialidade, garantindo que as redes escolhidas possuam algum tipo de mecanismo de confidencialidade. No entanto, quando faltam informações de todos os critérios avaliados, estas escolhas se tornam arbitrárias, seguindo o RSS para o *handoff*, podendo resultar em escolhas por redes totalmente inseguras. Por outro lado, no caso anterior ao pior dos casos, que ocorre quando existe somente informações de um critério apenas, o SDHet obteve uma taxa de acerto próxima de 40% para ambiente metropolitano de alta sobreposição. Isto quer dizer que, mesmo sobre condições adversar extremas, o SDHet pode decidir de forma a evitar APs de risco.

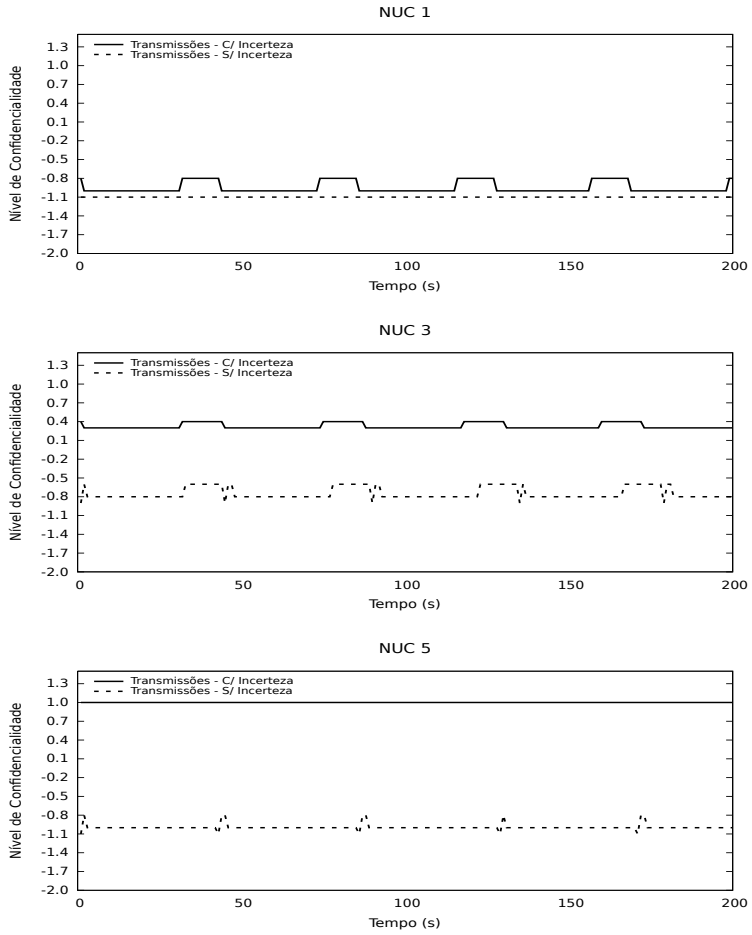

Figura 5.5: Impacto dos NUCs na confidencialidade das transmissões - Área local (IMCT)

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. Os resultados apresentados mostram que o SDHet procura manter o seu funcionando próximo do melhor possível, considerando as adversidades das faltas de informações.

O efeito da falta de informações no impacto da confidencialidade das transmissões pode ser verificado nas Figuras 5.5 e 5.6 que mostram a influência da falta de informações nas escolhas do SDHet. Os tempos decorridos das transmissões através de redes com menor risco à confidencialidade correspondem a uma amostra de tempo em cada cenário. A avaliação do impacto da falta de informações na confidencialidade das transmissões foi realizada no cenário local com a sobreposição baixa e no ambiente metropolitano variando o número de redes sobrepostas em médio e alto para apresentar o comportamento das transições.

Ao variar o NUC o SDHet executa escolhas com base na quantidade de mecanismos conhecidos e o número de critérios sem informação. Os resultados mostram que a confidencialidade das transmissões podem ser comprometidos quando a quantidade de NUCs se aproxima da quantidade total de critérios de comparação. Este comportamento ocorre porque o SDHet busca a melhor opção dentre as disponíveis com base nas informações que ele possui, o que leva a escolhas de redes com o nível de confidencialidade próximos ao da melhor rede disponível dependendo da variação. Dessa forma, quanto mais informações disponíveis sobre os mecanismos de confidencialidade nas redes, tende a ser maior o tempo de transmissão por redes que oferecem maior confidencialidade.

Os resultados apresentados mostram que o efeito da falta de informações sobre os critérios de decisão nas escolhas do SDHet tem um impacto negativo na confidencialidade das transmissões. Ao selecionar as redes com base em informações imprecisas, como o não conhecimento da presença dos mecanismos de confidencialidade, a acurácia das escolhas é prejudicada e como consequência seleciona-se uma rede que não é a de maior confidencialidade real. Por outro lado, pode ser visto um padrão na diferença dos valores de nível de confidencialidade das redes escolhidos e os valores do nível de confidencialidade das melhores redes naquele momento. Tal diferença corresponde ao comportamento das decisões do SDHet, de que quanto maior o NUC, maior é a diferença entre os níveis de confidencialidade inferidos. Os resultados demonstram o comportamento do SDHet busca a auto preservação do MD ao minimizar os possíveis prejuízos. Mesmo em situações adversas como quando faltam informações, quando o SDHet erra ao selecionar uma rede que não é a de maior nível de confidencialidade, suas escolhas são por redes que possuem um nível de confidencialidade próximo ao da melhor rede.

Também é possível verificar o efeito ping-pong, caracterizado por sucessivas transições

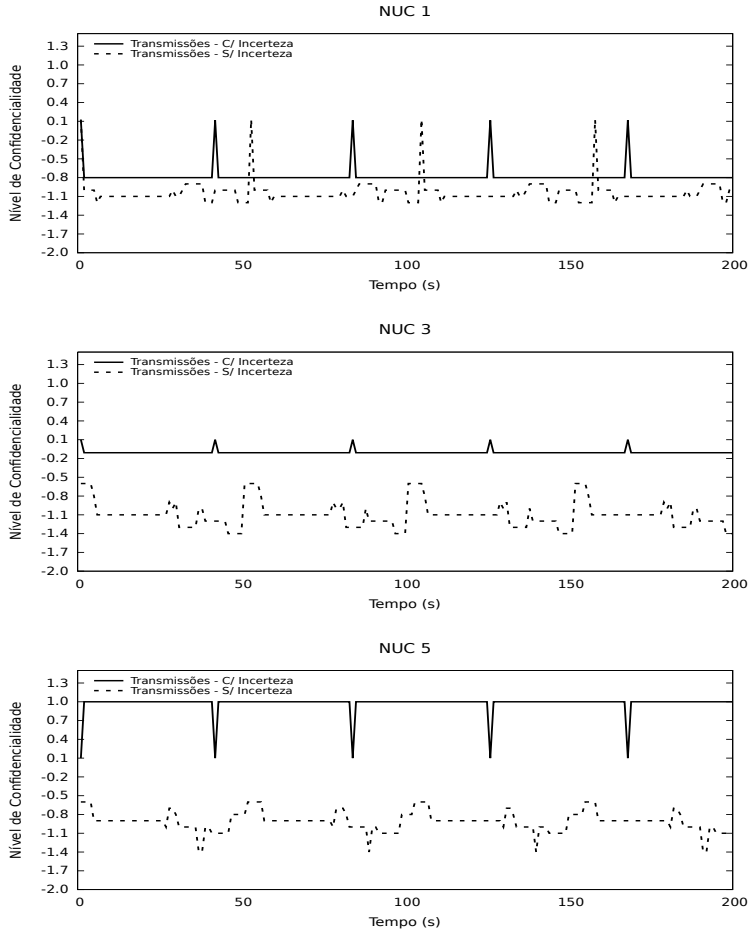

Figura 5.6: Impacto dos NUCs na confidencialidade das transmissões - Área metropolitana (IMCT)

com poucos segundos de intervalo. No ambiente metropolitano, que sofre mais impacto devido ao maior número de redes sobrepostas, observa-se através do número de trocas entre os pontos de acesso com poucos segundos de intervalo. Isto ocorre devido a falta de um mecanismo que gerencie a necessidade de transição.

A variação dos valores inferidos para o nível de confidencialidade das redes pode ser verificado na Figura 5.7 que mostra a exatidão do SDHet, considerando a variação dos NUCs. Conforme o NUC aumenta o erro entre os valores inferidos também aumenta, refletindo as taxas de acerto observadas na Figura 5.7. Apesar das escolhas não serem sempre ótimas, considerando como ótima a escolha pela rede de maior confidencialidade real, o SDHet escolha a rede com maior confiabilidade no valor calculado. Este fator controla o comportamento do SDHet, que o faz escolher sempre a melhor rede disponível com as informações disponíveis. Os resultados mostram escolhas por redes com o nível de confidencialidade próximo ao nível das rede com maior confidencialidade e que estes valores vão se afastando do valor da melhor rede conforme o NUC aumenta. Ademais, o método apresenta taxas de acerto a cima de 50% para a maioria das variações dos NUCs

em todos os cenários.

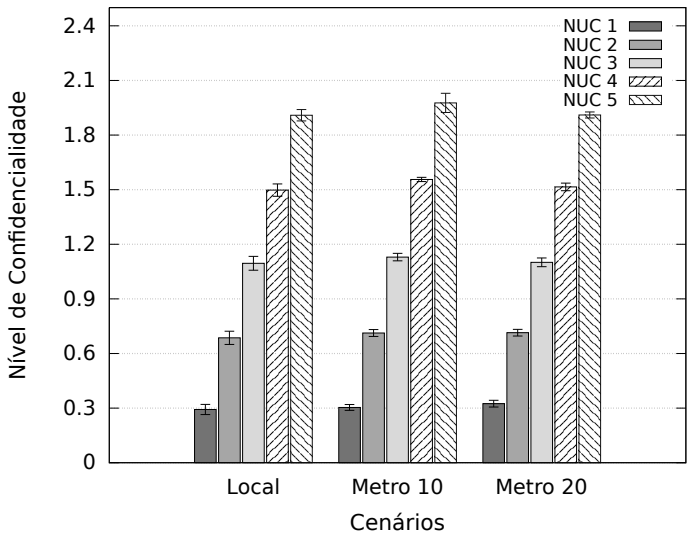

Figura 5.7: Exatidão das inferências com ausência de informações (VCI)

Os resultados mostram o impacto da falta de informações nas inferências do SDHet do nível de confidencialidade presentes nas redes de acesso disponíveis. A quantidade de critérios sem informação gera um impacto negativo na exatidão das inferências do SDHet. Este resultado complementa os resultados obtidos pela ASRC referentes a acurácia quanto a falta de informações, demonstrando que as escolhas do SDHet podem ser pouco confiáveis quando o NUC é próximo do valor total. Da mesma forma, conforme o NUC se aproxima de 0, a confiança das escolhas também aumenta, permitindo o funcionamento próximo do ideal nestes casos.

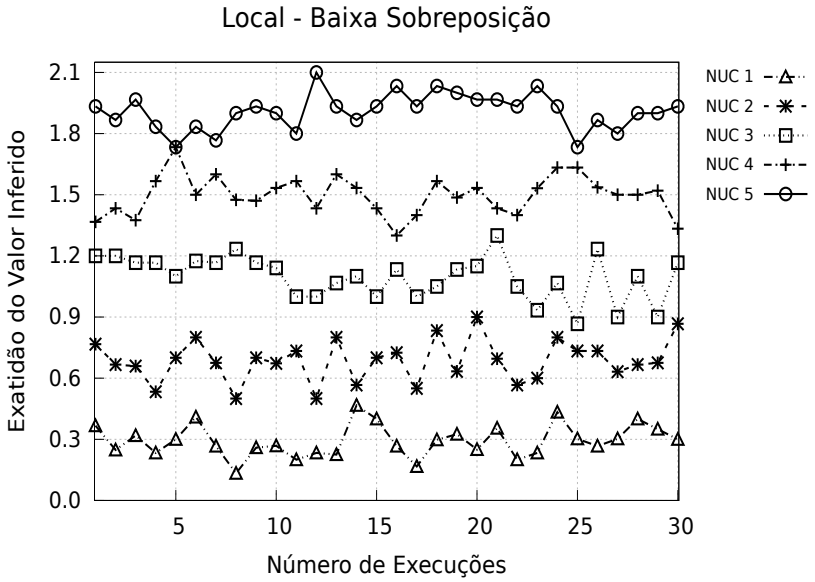

Figura 5.8: Variação das inferências com ausência de informações - Área local

O comportamento das variações da exatidão do SDHet pode ser verificado nós gráficos das Figuras 5.8 e 5.9. Estes gráficos representam a diferença entre o valor de confidencialidade inferido pelo SDHet com NUCs e o valor real inferido pelo SDHet sem NUCs para a mesma rede. Estes valores são referentes a 30 simulações para cada NUC em cada cenário.

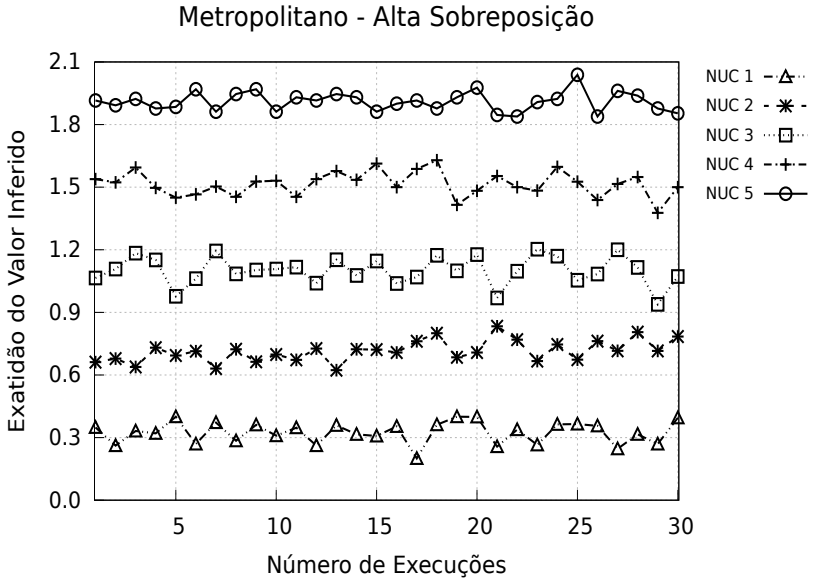

Figura 5.9: Variação das inferências com ausência de informações - Área Metropolitana

Os valores inferidos seguem um comportamento constante para cada cenário com cada NUC. Os resultados complementam as informações do gráfico da Figura 5.7, demonstrando a variação dos valores do nível de confidencialidade. O comportamento segue o esperado, mantendo-se entre os valores médios referentes a cada NUC, comprovando a variação baixa e a confiança nos valores inferidos.

5.4 Resultados de eficiência

A avaliação de eficiência das escolhas do SDHet verificou o tempo que o método gasta para tomar decisões. Esta avaliação foi feita através de simulações e medida por uma função no módulo desenvolvido para decisão. Como o módulo é integrado ao simulador, as medições foram realizadas externamente ao simulador, apresentando algumas variações entre as simulações. Estas variações não são significativas para o resultado da avaliação.

O 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 verifica 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.

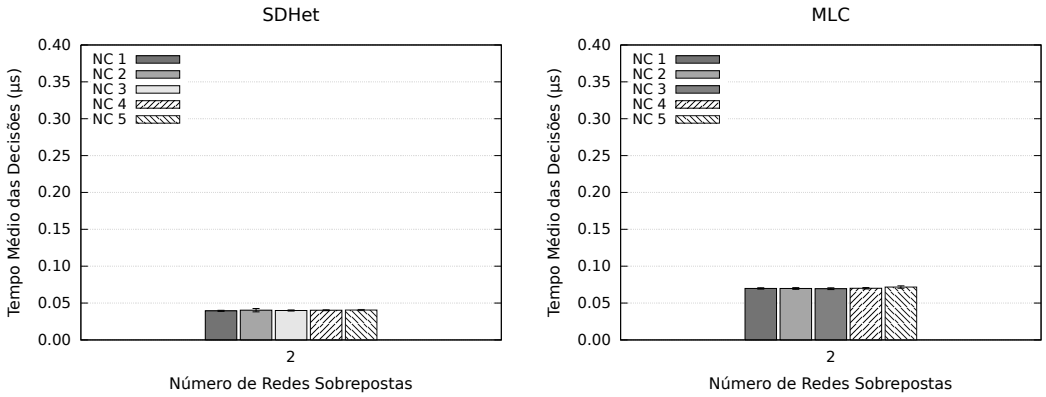

Figura 5.10: Comparação das velocidades das decisões (VD) - 2 Redes

A avaliação do tempo de decisão foi realizada em dois casos: variando o NC de decisão avaliados simultaneamente e variando o número de redes avaliadas simultaneamente. A quantidade de critérios foi variada de 1 até 5 critérios para três grupos de redes diferentes. O tempo foi avaliado para agrupamentos de 2, 10 e 20 redes. Além disso, a avaliação verificou o impacto da variação destes parâmetros no tempo de decisão dos métodos SDHet e MLC, comparando seus resultados.

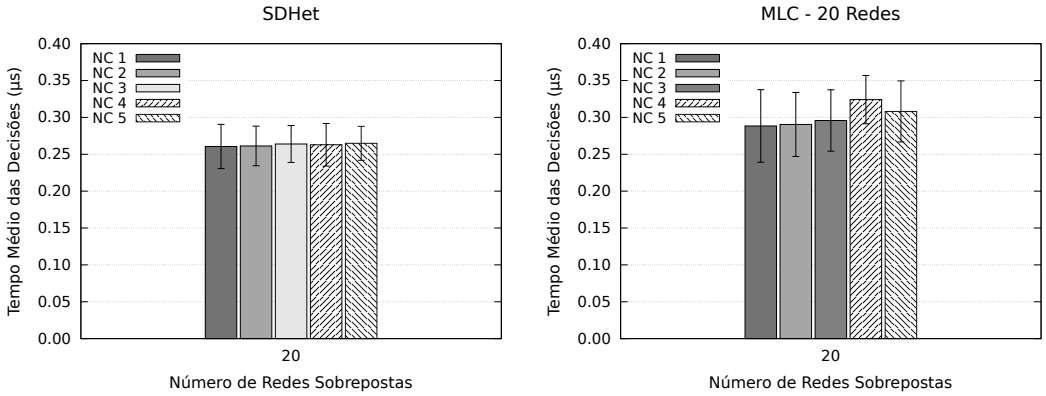

Figura 5.11: Comparação das velocidades das decisões (VD) - 20 Redes

As Figuras 5.10 e 5.11 apresentam a comparação dos resultados da avaliação da VD para os dois métodos. Os resultados indicam uma variação quase imperceptível 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 relação aos tempos de decisão dos dois métodos, os resultados mostram que ambos alcançam tempos de decisão muito próximos. Como o MLC toma decisões dentro em tempo hábil para o *handoff*, concluiu-se que o SDHet também pode ser aplicado neste processo com eficiência.

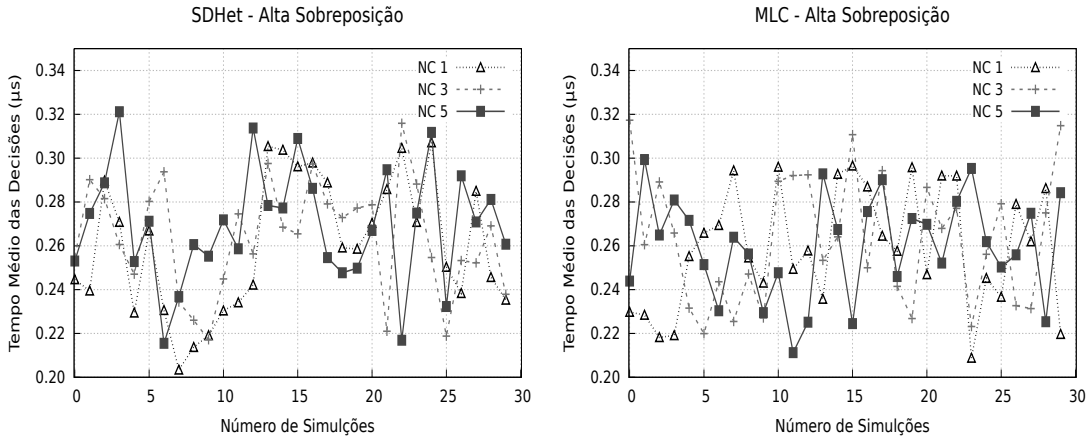

Figura 5.12: Variação das velocidades das decisões (alta sobreposição)

Em relação a variação do número de redes, os resultados mostram uma mudança 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.

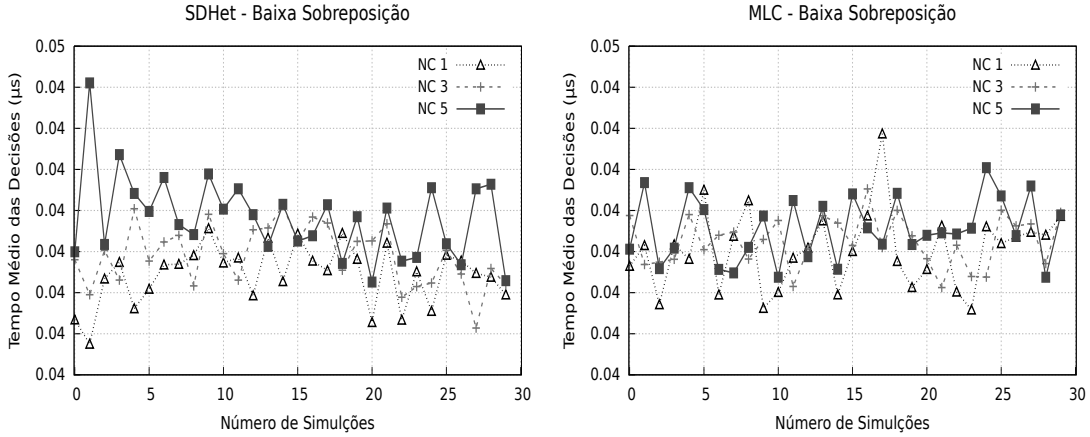

Figura 5.13: Variação das velocidades das decisões (alta sobreposição)

A Figura 5.13 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*.

5.5 Resumo

Este capítulo apresentou a avaliação da eficácia e da eficiência do método SDHet, comparando o seu desempenho com o método MLC na escolha de redes pelo nível de confidencialidade apresentado. Foi constatado o aumento na acurácia das escolhas com base na confidencialidade como critério quando utilizando o SDHet. A avaliação do critério segurança de maneira adequada, analisando seus principais princípios separadamente, provou o aumento da eficacia das escolhas ao atender usuários que necessitam de especificidade na segurança. O SDHet foi eficiente no *handoff* ao executar em tempo insignificante para o tempo total do processo, igualando-se a métodos simples que utilizam função objetivo como o MLC.

CAPÍTULO 6

CONCLUSÃO

O serviço de *handoff* vertical em redes heterogêneas proporciona a manutenção da conectividade dos dispositivos móveis, buscando a ubiquidade na utilização de serviços *online* e a melhora na conectividade do MD. Este mecanismo transfere a conexão do dispositivo móvel, escolhendo uma rede de acesso entre as redes disponíveis para transição quando necessário. Dessa forma, o processo de decisão avalia as características das redes, quando necessário, em busca da rede mais adequada as necessidades do dispositivo.

A segurança das comunicações do dispositivo móvel é um preocupação relevante para a transição, principalmente se os serviços em uso necessitam de proteção. Entre os aspectos de segurança importantes, destacam-se os seus três principais princípios de confidencialidade, integridade e disponibilidade. O processo de decisão escolhe com base nos valores quantificados destes aspectos de segurança de cada rede e na necessidade do dispositivo móvel em determinar a rede adequada. Por isso, considerar a segurança das redes de acesso no processo de decisão evita que o dispositivo móvel execute o *handoff* para redes arriscadas e prejudiciais.

Os métodos de decisão para *handoff* em Hetnets procuram determinar a rede de acesso que melhor atende as necessidades do MD, analisando suas características e classificando-as de acordo com a necessidade. Entre eles existem alguns métodos que consideram as características de segurança das redes como critérios importantes nas decisões de *handoff*. No entanto, estes métodos consideram a segurança de modo genérico, ignorando o impacto de suas diferentes propriedades na acurácia das escolhas e não especificando quais aspectos da segurança são tratados. Neste contexto, ainda existe a necessidade de levar em conta as diferentes propriedades da segurança, analisando separadamente suas características de confidencialidade, integridade e disponibilidade a fim de selecionar a rede adequada com maior precisão.

O método de decisão SDHet foi proposto para auxiliar a escolha de redes de acesso baseado na confidencialidade das comunicações. Ele infere um valor, que é chamado de nível de confidencialidade, para cada rede de acesso considerando de maneira adequada este princípio. O nível de confidencialidade se baseia nas técnicas que procuram garantir a confidencialidade e que são empregadas em mecanismos de segurança presentes nas redes. O método emprega a regra de probabilidade subjetiva, utilizando as informações dos mecanismos existentes em cada rede como informações subjetivas para inferir o valor do nível de confidencialidade e classificar as rede de acesso. Além da quantificação da confidencialidade das redes, o SDHet possibilita a tomada de decisões mesmo quando faltam

informações a respeito dos critérios de decisão. Para tanto, o modelo de decisão prospectivo foi empregado na classificação das redes por representar como um ser humano toma decisões na presença de risco (quantificação da confidencialidade) e de situações adversas como a presença de incerteza (falta de informações dos critérios). O modelos prospectivo possui duas funções que mapeiam a importância de uma consequência e a importância da chance dessa consequência ocorrer. As duas funções foram adaptadas como o nível de confiança e o nível de incerteza, que se baseiam na falta de informações e auxiliam na classificação das redes pelo nível de confidencialidade. Assim, o SDHet combina a analise de uma única propriedade de segurança (a confidencialidade das transmissões do MD) através de uma técnica de quantificação baseada em probabilidade subjetiva, com um método de decisão inspirado nas funções de mapeamento de importância do modelo de decisão da teoria da prospecção para classificar as redes eficientemente.

O SDHet foi implementado no simulador NS3 e sua eficácia e eficiência foram avaliadas em cenários que representam ambientes reais. Ele foi comparado com o MLC, método de decisão para o *handoff*, também implementado no simulador NS3 e que utiliza a mesma forma de classificação de redes que o SDHet, uma função objetivo. As simulações demonstram que o SDHet é eficaz em classificar e selecionar as redes de acesso com base no seu nível de confidencialidade. Os resultados comprovaram a eficácia das decisões, que atingiram 100% de acurácia quando existem todas as informações a respeito dos critério necessários para comparação. Ao variar o número de critérios com informações, notou-se uma queda nas taxas de acerto conforme a quantidade destes critérios aumentava. Entretanto, o SDHet consegue manter seu funcionamento mesmo quando faltam todas as informações, preservando da melhor maneira possível a confidencialidade das transmissões do MD. Dessa forma, o impacto da falta de informações na exatidão das inferências do nível de confidencialidade é significativo para a acurácia do SDHet. Ademais, o SDHet permite ao MD auto-preservar a confidencialidade de suas transmissões e se adaptar a situação adversa quando faltam informações para decisão.

Quando comparado ao MLC, um método de decisão que considera a segurança de maneira genérica e não leva em conta a falta de informações, o SDHet foi significativamente mais preciso em suas decisões. Tal diferença reflete a necessidade de analisar a segurança separadamente, verificando seus princípios adequadamente. Além disso, a falta de informações é um aspecto muito importante que deve ser tratado para melhorar o desempenho das decisões e garantir a satisfação do usuário. Em relação ao tempo de decisão, os dois métodos possuem tempos aceitáveis para o *handoff*, considerando as velocidades de movimento dos MDs. Ademais, o tempo de decisão é impactado de forma significativa pelo número de redes comparadas, quanto mais redes mais perceptível é o impacto do processo de decisão. O número de critérios de comparação possuí um impacto quase imperceptível no tempo de decisão, onde a variação da quantidade entre 1 e 5 critério simultâneos não apresentou variações no tempo de decisão. O SDHet consolida um novo

uso para métodos de decisão que modelam o comportamento humano na tentativa de lidar com situações adversar durante o *handoff* em HetNets.

A adaptação do modelo de decisão prospectivo pelo SDHet apresenta uma forma de auto-preservar o MD em situações adversas no *handoff*, em especial quando faltam informações dos critérios. Ao selecionar uma rede de acesso, quando não se tem todas as informações necessárias para a comparação, que mantém a confidencialidade das transmissões o método garante a adaptabilidade e a sobrevivência das transmissões com confidencialidade. Assim, o MD pode confiar que a rede de acesso que está utilizando atende o princípio de segurança desejado.

6.1 Trabalhos futuros

Os resultados alcançados e as conclusões deste trabalho proporcionam novas abordagens para trabalhos futuros. A adaptação da técnica de quantificação das propriedades de integridade e de disponibilidade pode ser realizada utilizando a mesma técnica de quantificação da confidencialidade. A utilização da probabilidade subjetiva baseada em informações relacionadas as técnicas destas propriedades pode ser útil na analise e classificação das redes de acesso para o *handoff*. Além disso, o método pode ser expandido para analisar outras técnicas de confidencialidade e mecanismos na determinação do nível de segurança das redes.

Em consideração a adaptação do modelo de decisão prospectivo, a acurácia das escolhas em situações adversas pode ser melhorada. O ponto principal a ser investigado reside na melhor ponderação da função de custo/benefício e de utilizar conhecimentos de experiencias anteriores para refinar as escolhas, baseando-se nas decisões já realizadas pelo MD. Além disso, a inspiração e adaptação da teoria da prospecção abre novos caminhos para a tomada de decisão adaptativa. O desenvolvimento de funções de impacto de outros tipos de situações adversas como, por exemplo, o uso de informações falsas, pode melhorar ainda mais a precisão das decisões e agregar novas caracteristicas a auto-preservação dos MDs. Ademais, a adaptação destes modelos de decisão baseados no comportamento humano não é limitada exclusivamente ao *handoff* em redes heterogêneas, podendo ser utilizada em outros contextos que não o de redes sem fio heterogêneas.

A integração do SDHet com outros métodos que analisem as características de desempenho e qualidade das redes, como a Qualidade de Experiência, pode trazer benefícios para o handoff. A qualidade de experiência pode sofrer impacto da quantidade de mecanismos de segurança usados numa rede como por exemplo, técnicas de manipulação dos dados transmitidos, como criptografia e esteganografia, podem aumentar o *delay* de transmissão das partes de um vídeo. sendo interessante a investigação da agregação de métricas de qualidade de experiencia com métricas de segurança. Como o SDHet possuí um tempo de decisão insignificante para o *handoff*, está adaptação tem prospecções de

não impactar significativamente no tempo de transição. Esta integração pode gerar um sistema de decisão completo com maior eficiência e eficacia nas escolhas. Além disso, uma avaliação estendida da eficiência também pode ser feita, como por exemplo, utilizando métricas que aferem o consumo energético e o uso de recursos no processo de decisão [82].

Outro ponto importante condiz com o problema do efeito ping-pong. O método proposto sofre com este problema quando o MD está próximo da borda de uma rede ou detectando novas redes com menos de 1s de intervalo. Um mecanismo de controle pode ser desenvolvido para mitigar os efeitos do problema ping-pong. Ademais, novas avaliações de desempenho do método utilizando parâmetros mais extremos e cenários diferentes podem ser realizadas para testar o método e descobrir seus limites de utilização.

Um dos objetivos do método SDHet era a autonomia do dispositivo móvel para efetuar decisões. Por este motivo, ele foi proposto centrado no dispositivo. No entanto, uma de suas limitações é a aquisição de informações na fase de coleta e descoberta de redes, que pode sofrer falhas. A investigação a dinamicidade na aplicação do SDHet pode ser feita implementando-o centrado na rede, onde os pontos de acesso poderiam fazer as inferências dos níveis de confidencialidade com menor impacto da falta de informações.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Jeffrey Gerews. Seven ways that hetnets are a cellular paradigm shift. *Communications Magazine, IEEE*, 51(3):136–144, 2013.

[2] R. Berezdivin, R. Breinig, and R. Topp. Next-generation wireless communications concepts and technologies. *Communications Magazine, IEEE*, 40(3):108–116, Março 2002.

[3] Dave Cavalcanti, Dharma Agrawal, Carlos Cordeiro, Bin Xie, and Anup Kumar. Issues in integrating cellular networks wlans, and manets: a futuristic heterogeneous wireless network. *Wireless Communications, IEEE*, 12(3):30–41, 2005.

[4] K.R. Rao, Z.S. Bojkovic, and B.M. Bakmaz. 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 01, pages 83–92, Outubro 2013.

[5] Reiner Ludwig, Hannes Ekstrom, Per Willars, and Niklas Lundin. An evolved 3gpp qos concept. In *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, volume 1, pages 388–392. IEEE, 2006.

[6] S. Fernandes and A. Karmouch. Vertical mobility management architectures in wireless networks: A comprehensive survey and future directions. *Communications Surveys Tutorials, IEEE*, 14(1):45–63, Primeiro 2012.

[7] Jiannong Cao, Weigang Wu, and Xuan Liu. Seamless mobility support for adaptive applications in heterogeneous wireless networks. In *Ubiquitous Intelligence Computing and 7th International Conference on Autonomic Trusted Computing (UIC/ATC), 2010 7th International Conference on*, pages 217–222, Outubro 2010.

[8] A. Dutta, S. Madhani, and Tao Zhang. Network discovery mechanisms for fast-handoff. In *Broadband Communications, Networks and Systems, 2006. BROADNETS 2006. 3rd International Conference on*, pages 1–11, Outubro 2006.

[9] Joanna Abraham, Thomas Kannampallil, and Vimla L Patel. A systematic review of the literature on the evaluation of handoff tools: implications for research and practice. *Journal of the American Medical Informatics Association*, 21(1):154–162, 2014.

[10] Atiq Ahmed, Leıla Merghem Boulahia, and Dominique Gaïti. Enabling vertical handover decisions in heterogeneous wireless networks: A state-of-the-art and a classification. *Communications Surveys & Tutorials, IEEE*, 16(2):776–811.

[11] Mariem Zekri, Badii Jouaber, and Djamal Zeghlache. A review on mobility management and vertical handover solutions over heterogeneous wireless networks. *Computer Communications*, 35(17):2055–2068, 2012.

[12] Nilakshee Rajule, Bhavna Ambudkar, and A.P. Dhee. Survey of vertical handover decision algorithms. *Inter. Journal of Innovations in Engineering and Tech*, 2(1):362–368, 2013.

[13] Meriem Kassar, Brigitte Kervella, and Guy Pujolle. An overview of vertical handover decision strategies in heterogeneous wireless networks. *Computer Communications*, 31(10):2607–2620, 2008.

[14] Daojing He, Chun Chen, Jiajun Bu, S. Chan, and Yan Zhang. Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects. *Communications Magazine, IEEE*, 51(2):142–150, Fevereiro 2013.

[15] Shari Lawrence Pfleeger. Security measurement steps, missteps, and next steps. *IEEE Security and Privacy*, 10(4):0005–9, 2012.

[16] Bryony Beresford and Patricia Sloper. *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, 2008.

[17] Daniel Kahneman and Amos Tversky. Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, pages 263–291, 1979.

[18] Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann. Confidentiality and integrity: A constructive perspective. In Ronald Cramer, editor, *Theory of Cryptography*, volume 7194 of *Lecture Notes in Computer Science*, pages 209–229. Springer Berlin Heidelberg, 2012.

[19] Algirdas Avizienis, J.C. Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on*, 1(1):11–33, 2004.

[20] Sanjay Dhar Roy and S Reddy Vamshidhar Reddy. Signal strength ratio based vertical handoff decision algorithms in integrated heterogeneous networks. *Wireless personal communications*, 77(4):2565–2585, 2014.

[21] Bo Hu, Ning Li, and Jingjing Zhang. Iass: An intelligence access selection scheme for heterogeneous networks. In *Information Networking (ICOIN), 2015 International Conference on*, pages 531–536. IEEE, 2015.

[22] Mohamed Lahby, Leghris Cherkaoui, and Abdellah Adib. Hybrid network selection strategy by using m-ahp/e-topsis for heterogeneous networks. In *Intelligent Systems: Theories and Applications (SITA), 2013 8th International Conference on*, pages 1–6. IEEE, 2013.

[23] Igor Bisio, Carlo Braccini, Stefano Delucchi, Fabio Lavagetto, and Mario Marchese. 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, 2014.

[24] Faisal Kaleem. *VHITS: vertical handoff initiation and target selection in a heterogeneous wireless network*. PhD thesis, Florida International University, 2012.

[25] Xiaobin Li and Renfeng Chen. Adaptive vertical handover algorithm based on user experience for heterogeneous network. In *Image and Signal Processing (CISP), 2013 6th International Congress on*, volume 3, pages 1540–1544. IEEE, 2013.

[26] Snigdha Khanum and Mohammad Mahfuzul Islam. 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, 2014.

[27] Bin Ma, Xiaofeng Liao, and Xianzhong Xie. 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, 2012.

[28] George Wu, Jiao Zhang, and Richard Gonzalez. Decision under risk. *Blackwell handbook of judgment and decision making*, 399, 2004.

[29] Shu-Ping Yeh, Shilpa Talwar, Geng Wu, Nageen Himayat, and Kerstin Johnsson. Capacity and coverage enhancement in heterogeneous networks. *Wireless Communications, IEEE*, 18(3):32–38, 2011.

[30] Kyeong-Deok Moon, Young-Hee Lee, Chang-Eun Lee, and Young-Sung Son. Design of a universal middleware bridge for device interoperability in heterogeneous home network middleware. *Consumer Electronics, IEEE Transactions on*, 51(1):314–318, 2005.

[31] Djamal-Eddine Meddour, Usman Javaid, Nicolas Bihannic, Tinku Rasheed, and Raouf Boutaba. Completing the convergence puzzle: a survey and a roadmap. *Wireless Communications, IEEE*, 16(3):86–96, 2009.

[32] Filippo Cacace and Luca Vollero. Managing mobility and adaptation in upcoming 802.21 enabled devices. In *Proceedings of the 4th international workshop on Wireless mobile applications and services on WLAN hotspots*, pages 1–10. ACM, 2006.

[33] Johann Márquez-Barja, Carlos T Calafate, Juan-Carlos Cano, and Pietro Manzoni. An overview of vertical handover techniques: Algorithms, protocols and tools. *Computer Communications*, 34(8):985–997, 2011.

[34] Azita Laily Yusof, Norsuzila Ya'acob, and Mohd Tarmizi Ali. Handover initiation across heterogeneous access networks for next generation cellular network. In *Wireless Technology and Applications (ISWTA), 2011 IEEE Symposium on*, pages 78–83. IEEE, 2011.

[35] Ane R Prasad, Alf Zugenmaier, and Peter Schoo. Next generation communications and secure seamless handover. In *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on*, pages 267–274. IEEE, 2005.

[36] Dhanaraj Cheelu, M. Rajasekhara Babu, and P. Venkata Krishna. A study of vertical handoff decision strategies in heterogeneous wireless networks. *International Journal of Engineering and Technology*, 5(3):2541–2554, 2013.

[37] Wenhui Zhang. Handover decision using fuzzy madm in heterogeneous networks. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, volume 2, pages 653–658. IEEE, 2004.

[38] Jose D Martinez-Morales, Ulises Pineda-Rico, and Enrique Stevens-Navarro. 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, 2010.

[39] Enrique Stevens-Navarro and Vincent WS Wong. Comparison between vertical handoff decision algorithms for heterogeneous wireless networks. In *Vehicular technology conference, 2006. VTC 2006-Spring. IEEE 63rd*, volume 2, pages 947–951. IEEE, 2006.

[40] Ahmed Hasswa, Nidal Nasser, and Hossam Hassanein. Tramcar: A context-aware cross-layer architecture for next generation heterogeneous wireless networks. In *Communications, 2006. ICC'06. IEEE International Conference on*, volume 1, pages 240–245. IEEE, 2006.

[41] Lei Sun, Jianquan Wang, and Zhaobiao Lv. An adaptive network selection scheme in 4g composite radio environments. In *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on*, pages 1–4. IEEE, 2012.

[42] B. Ahlgren, P.A. Aranda, P. Chemouil, S. Oueslati, L.M. Correia, H. Karl, M. Sollner, and A. Welin. Content, connectivity, and cloud: ingredients for the network of the future. *Communications Magazine, IEEE*, 49(7):62–70, Julho 2011.

[43] Angelo Bannack, Eduardo da Silva, Michele Nogueira Lima, Aldri L dos Santos, and Luiz Carlos Pessoa Albini. Segurança em redes ad hoc. *Anais do XXVI Simpósio Brasileiro de Telecomunicaçoes (SBRT'08)*, pages 19–20, 2008.

[44] Mark Stamp. *Information security: principles and practice*. John Wiley & Sons, 2011.

[45] Stallings William and William Stallings. *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.

[46] Birgit Pfitzmann. 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, 1996.

[47] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35(3.4):313–336, 1996. Ultima Edição 2010.

[48] Atul Kahate. *Cryptography and network security*. Tata McGraw-Hill Education, 2013.

[49] Ken Manktelow. *Thinking and reasoning: An introduction to the psychology of reason, judgment and decision making*. Psychology Press, 2012.

[50] Dongxu Li and Jose B Cruz Jr. Information, decision-making and deception in games. *Decision Support Systems*, 47(4):518–527, 2009.

[51] Mahmood Adnan, Hushairi Zen, and Al-Khalid Othman. A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks. *World Applied Sciences Journal*, 28(5):629–635, 2013.

[52] Jyoti Madaan and Indu Kashyap. An overview of vertical handoff decision algorithm. *International Journal of Computer Applications*, 111(3), 2015.

[53] Nidal Nasser, Sghaier Guizani, and Eyhab Al-Masri. Middleware vertical handoff manager: A neural network-based solution. In *Communications, 2007. ICC'07. IEEE International Conference on*, pages 5671–5676. IEEE, 2007.

[54] M.M. Alkhawlani, K.A. Alsalem, and A.A. Hussein. Multi-criteria vertical handover by topsis and fuzzy logic. In *Communications and Information Technology (ICCIT), 2011 International Conference on*, pages 96–102, Março 2011.

[55] Bojan Bakmaz, Zoran Bojkovic, and Miodrag Bakmaz. 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, 2012.

[56] Bojan Bakmaz, Zoran Bojkovic, and Miodrag Bakmaz. Elements of security aspects in wireless networks: Analysis and integration. volume 1, pages 70–75, 2007.

[57] Stefano Cacciaguerra and Stefano Ferretti. 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, 2003.

[58] K. Radhika and K.A. Reddy. Vertical handoff decision algorithm for heterogeneous wireless networks based on 2-level analytic hierarchy process. In *India Conference (INDICON), 2011 Annual IEEE*, pages 1–6. IEEE, 2011.

[59] Ammar A. Bathich, Mohd Dani Baba, and R.A. Rahman. Sinr based media independent handover in wimax and wlan networks. In *Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE International Conference on*, pages 331–334. IEEE, 2011.

[60] Kenichi Taniuchi, Yoshihiro Ohba, Victor Fajardo, Subir Das, Miriam Tauil, Y.H. Cheng, Ashutosh Dutta, Donald Baker, Maya Yajnik, and David Famolari. Ieee 802.21: Media independent handover: Features, applicability, and realization. *Communications Magazine, IEEE*, 47(1):112–120, 2009.

[61] M. Barrere, R. Badonnel, and O. Festor. Vulnerability assessment in autonomic networks and services: A survey. *Communications Surveys Tutorials, IEEE*, 16(2):988–1004, Segunda 2014.

[62] Anis Ben Aissa, Latifa Ben Arfa Rabai, Robert K. Abercrombie, Ali Mili, and Frederick T. Sheldon. Quantifying availability in scada environments using the cyber security metric mfc. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, pages 81–84, 2014.

[63] Michael R Clarkson and Fred B Schneider. Quantification of integrity. *Mathematical Structures in Computer Science*, 25(02):207–258, 2015.

[64] Nikhat Parveen, M.D. Rizwan Beg, and M.H. Khan. Model to quantify confidentiality at requirement phase. In *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015)*, page 52. ACM, 2015.

[65] A. Mukherjee, S.A.A. Fakoorian, Jing Huang, and A.L. Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *Communications Surveys Tutorials, IEEE*, 16(3):1550–1573, Terceira 2014.

[66] Wayne Jansen. *Directions in security metrics research*. DIANE Publishing, 2010.

[67] Mahsa Keramati. Novel security metrics for ranking vulnerabilities in computer networks. In *Telecommunications (IST), 2014 7th International Symposium on*, pages 883–888. IEEE, 2014.

[68] Pallab Bhattacharya and Soumya K Ghosh. Analytical framework for measuring network security using exploit dependency graph. *Information Security, IET*, 6(4):264–270, 2012.

[69] N. Poolsappasit, R. Dewri, and I. Ray. Dynamic security risk management using bayesian attack graphs. *Dependable and Secure Computing, IEEE Transactions on*, 9(1):61–74, Janeiro 2012.

[70] M.H. Bhuyan, D.K. Bhattacharyya, and J.K. Kalita. Network anomaly detection: Methods, systems and tools. *Communications Surveys Tutorials, IEEE*, 16(1):303–336, Primeira 2014.

[71] Alessandro Armando, Michele Bezzi, Nadia Metoui, and Antonino Sabetta. Risk-aware information disclosure. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pages 266–276. Springer, 2015.

[72] Cándido Caballero-Gil, Jezabel Molina-Gil, Juan Hernández-Serrano, Olga León, and Miguel Soriano-Ibañez. Providing k-anonymity and revocation in ubiquitous vanets. *Ad Hoc Networks*, 2015.

[73] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. A survey on security aspects for lte and lte-a networks. *Communications Surveys & Tutorials, IEEE*, 16(1):283–302, 2014.

[74] Dejan Simic and Radomir Prodanovic. A survey of wireless security. *CIT. Journal of Computing and Information Technology*, 15(3):237–255, 2007.

[75] Mario F. Triola et al. *Introdução à estatística*, volume 10. Ltc Rio de Janeiro, 2005.

[76] Salumu Munga. Overview on mih and mihf modules for ns3. http://www.worldcommunitygrid.org/help/viewTopic.do?shortName=acah. Data de acesso: Nov. 2014.

[77] Zinon Zinonos, Vasos Vassiliou, and Charalambos Chrysostomou. Handoff triggering for wireless sensor networks with performance needs. In *Computers and Communications (ISCC), 2013 IEEE Symposium on*, pages 000982–000988. IEEE, 2013.

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

[79] Jose Jailton, Tereza Carvalho, Warley Valente, Carlos Natalino, Renato Frances, and Kelvin Dias. A quality of experience handover architecture for heterogeneous mobile wireless multimedia networks. *Communications Magazine, IEEE*, 51(6):152–159, 2013.

[80] Sadegh Aliakbary, Sadegh Motallebi, Sina Rashidian, Jafar Habibi, and Ali Movaghar. Noise-tolerant model selection and parameter estimation for complex networks. *Physica A: Statistical Mechanics and its Applications*, 427:100–112, 2015.

[81] Christopher Swartz and Akanksha Joshi. Identification in encrypted wireless networks using supervised learning. In *Military Communications Conference (MILCOM), 2014 IEEE*, pages 210–215. IEEE, 2014.

[82] G. Coskun, I. Hokelek, and H.A. Cirpan. Energy efficient handover in hetnets using ieee 802.21. In *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, pages 349–353, Maio 2014.

ANEXO

Este anexo apresenta os resultados da avaliação de desempenho do método de decisão SDHet quanto a varição da quantidade de redes sobrepostas. Estes resultados são referentes as simulações em um cenário com área metropolitana utilizando um alta sobreposição de rede, considerando até 40 redes sobrepostas, com o objetivo de compreender melhor os limites de desempenho do SDHet. Ademais, são exibidos os resultados complementares das métricas de impacto do método na confidencialidade das transmissões, exatidão dos valores classificatórios inferidos e velocidade de decisão considerando até 6 critérios de decisão.

Acurácia da seleção de redes confidenciais

Esta seção apresenta os resultados complementares da avaliação da eficácia do SDHet ao inferir o nível de confidencialidade. A eficácia do SDHet foi avaliada pelas métricas ASRC, IMCT e VCI, especificadas no Capítulo 5, variando a quantidade de critérios sem informação (NUCs). A eficácia do MLC foi avaliada somente pelas métricas ASRC e IMCT, onde ambas foram aferidas sem a falta de informações, pois MLC não foi projetado para lidar com esse fator.

A métrica ASRC mede a acurácia do SDHet e do MLC na seleção de redes confidenciais. Os resultados desta métrica apresentados no Capítulo 5 correspondem a amostras selecionadas dos resultados de cada simulação para cada cenário onde foi variada quantidade de critérios sem informações. As figura apresentadas nesta subseção condizem com os resultados das demais simulações que complementam os resultados do Capítulo 5.

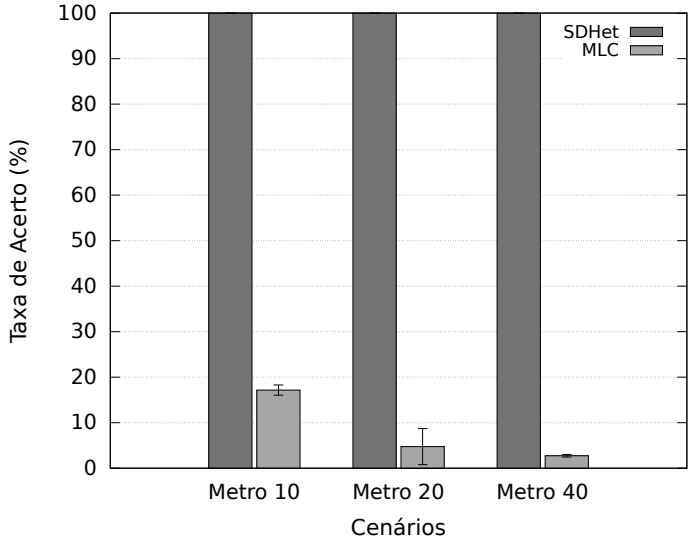

Figura 6.1: Comparação da acurácia das decisões dos métodos (ASRC)

A Figura 6.1 mostra o resultado da avaliação da acurácia do SDHet comparada com a do MLC. Os cenário utilizado foi o mesmo ambiente metropolitano descrito no Capítulo 5, onde foi variado somente o grau de sobreposição de redes em 10 e 40 redes sobrepostas. Para facilitar a analise os resultados obtidos no mesmo cenário com 20 redes sobrepostas também são mostrados.

Como pode ser observado, com o aumento da quantidade de redes diminuí-se a precisão das escolhas do MLC. Seguindo a tendencia apresentada no Capítulo 5, o MLC sofre o impacto do aumento do número de redes sobrepostas. Quanto mais redes para comparação e escolha, maior a possibilidade de selecionar uma rede inadequada.

Impacto das decisões na confidencialidade das transmissões

Nesta seção são apresentados os resultados complementares da métrica IDCT. Os resultados apresentados no Capítulo 5 correspondem a amostras selecionadas referentes aos NUCs 1, 3 e 5 em cada cenário. As figuras apresentadas nesta subseção demonstram os resultados das demais variações intermediárias, de NUC 2 e 4, nos ambientes local e metropolitano, que não estão no Capítulo 5.

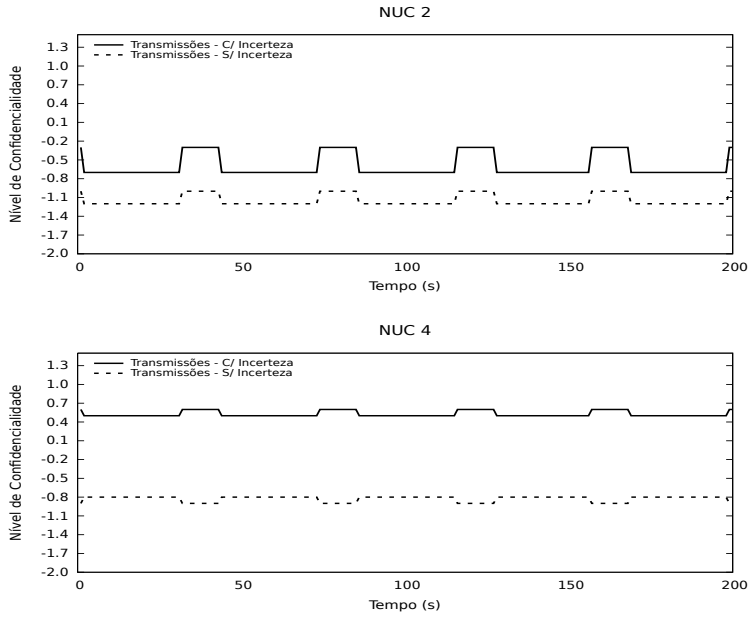

Figura 6.2: Impacto dos NUCs na confidencialidade das transmissões - Área local (IMCT)

As Figuras 6.2 e 6.3 apresenta os resultados para o cenário local. Os resultados apresentados mostraram que o efeito da falta de informações sobre os critérios de decisão nas escolhas do SDHet tem um impacto negativo na confidencialidade das transmissões. O impacto para os NUCs 2 e 4 pode ser percebido como o intervalo entre os valores do nível de confidencialidade das redes escolhidas pelo SDHet e utilizadas para transmissão.

A acurácia das escolhas é prejudicada conforme o NUC aumenta e como consequência seleciona-se uma rede não adequada.

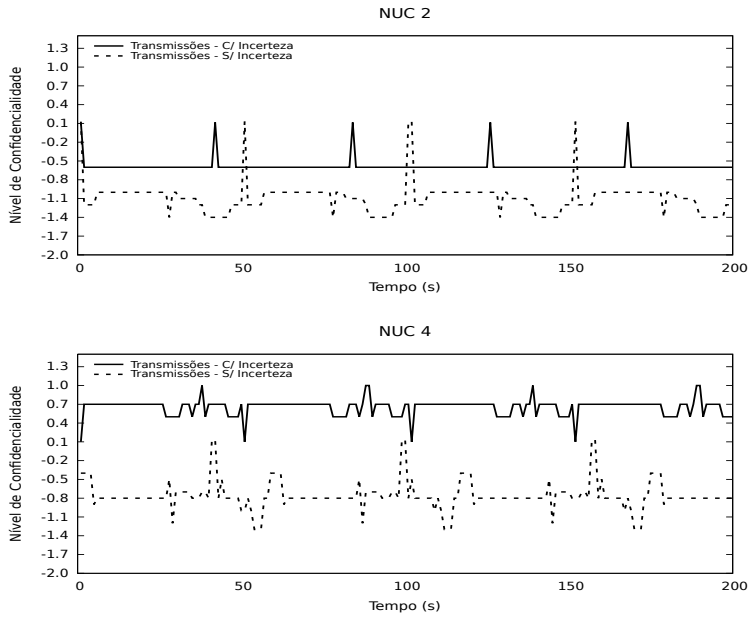

Figura 6.3: Impacto dos NUCs na confidencialidade das transmissões - Área metropolitana (IMCT)

A aumento do NUC aumenta também a variação das inferências, podendo ser notada no nível de confidencialidade das redes selecionadas em cada situação. Este comportamento, onde a distancia entre os valores da confidencialidade das seleções com e sem incerteza, pode ser melhor observado ao comprar todos os NUCs juntos. A Figura 6.4 apresenta os gráficos das variações de todos os NUCs agrupados.

O efeito ping-pong pode ser observado na variação, com poucos segundos de diferença, das redes utilizadas para transmissão. A intensidade da variação depende de dois fatores, o raio de cobertura das redes e o padrão de mobilidade utilizado. A mobilidade influencia na entrada e saída do MD na área de cobertura das redes. O raio de cobertura interfere quando o MD está entrando e saindo de uma área onde a intersecção de diferentes redes está no limite do raio. Ao entrar e sair da área de cobertura de um rede com alto nível de confidencialidade o MD executa o *handoff*, caracterizando o efeito ping-pong.

Impacto das decisões na confidencialidade das transmissões

Nesta seção são apresentados os resultados complementares da métrica VD. Os resultados apresentados no Capítulo 5 correspondem a avaliação da velocidade de decisão com até 5 NC em cada cenário. A Figura 6.5 apresentada os resultados da simulação de um cenário com 40 redes sobrepostas e até 6 critérios de decisão comparados simultaneamente.

A variação do número de redes tem o impacto mais significativo sobre o tempo de

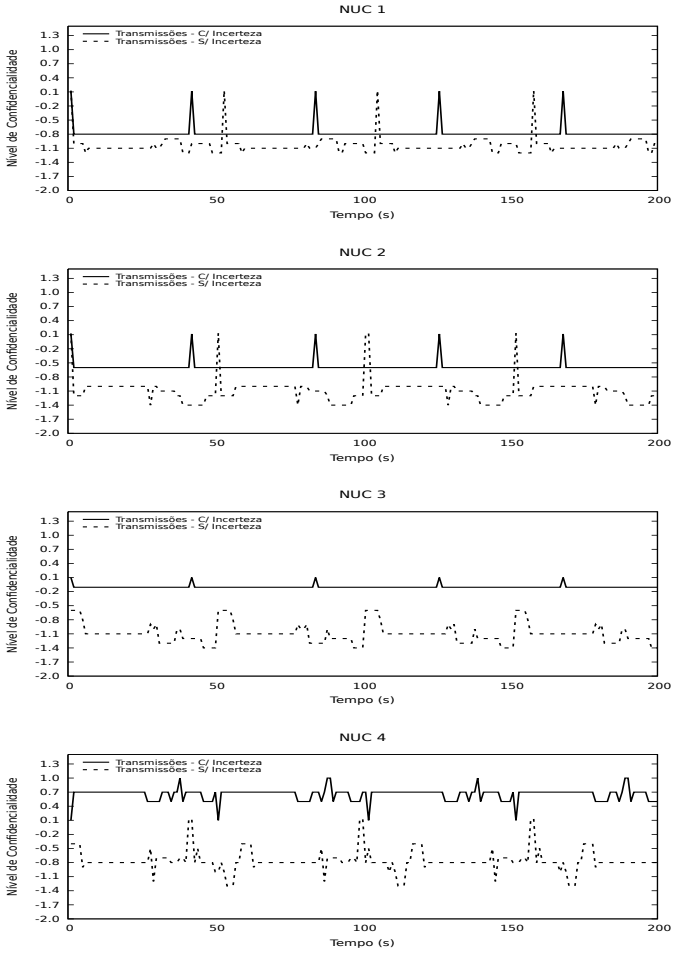

Figura 6.4: Impacto dos NUCs na confidencialidade das transmissões - Área metropolitana (IMCT)

decisão. Isto significa que quanto maior o número de redes para inferir e classificar maior o tempo gasto. Em contra partida, mesmo considerando um critério adicional na comparação, o tempo de decisão com 1 critério ou com 6 critérios tem uma variação insignificante na operação do método. Estes resultados comprovam a eficiência do método e seu impacto insignificante para o tempo de transição total do *handoff*, considerando a variação da quantidade de redes com até 40 redes sobrepostas.

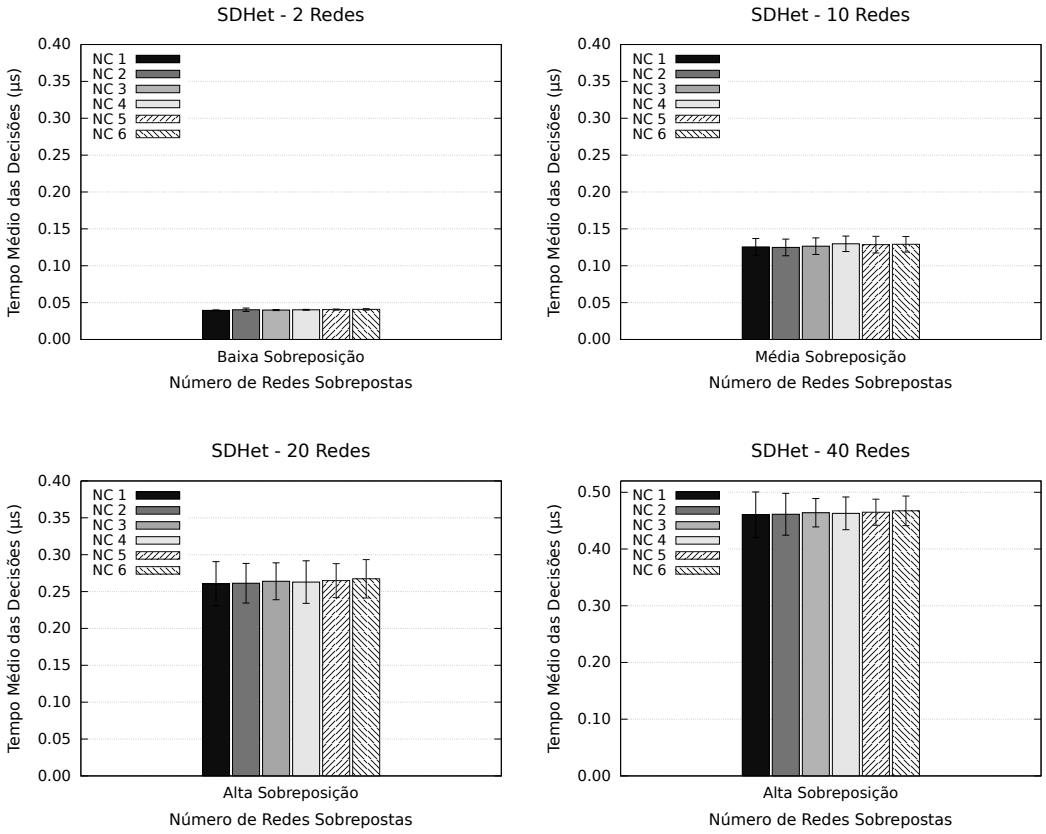

Figura 6.5: Velocidade das decisões do SDHet - (VD)