UNIVERSIDADE FEDERAL FLUMINENSE

Igor Cesar Gonzalez Ribeiro

THOR: Um Framework para Infraestrutura de Medição Avançada Resiliente a Falhas de Agregadores nas Redes Elétricas Inteligentes

NITERÓI

2018

UNIVERSIDADE FEDERAL FLUMINENSE

Igor Cesar Gonzalez Ribeiro

THOR: Um Framework para Infraestrutura de Medição Avançada Resiliente a Falhas de Agregadores nas Redes Elétricas Inteligentes

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Doutor em Computação. Área de concentração: Sistemas de Computação

Orientador:
Célio Vinicius Neves Albuquerque

Co-orientador:
Antônio Augusto de Aragão Rocha

NITERÓI

2018

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

R484t Ribeiro, Igor Cesar Gonzalez
Thor: um framework para infraestrutura de medição avançada resiliente a falhas de agregadores nas redes elétricas inteligentes / Igor Cesar Gonzalez Ribeiro ; Célio Vinicius Neves de Albuquerque, orientador ; Antônio Augusto de Aragão Rocha, coorientador. Niterói, 2018.
96 f. : il.

Tese (doutorado)-Universidade Federal Fluminense, Niterói, 2018.

DOI: http://dx.doi.org/10.22409/PGC.2018.d.11429539712

1. Redes elétricas inteligentes. 2. Redes em malha sem fio. 3. Infraestrutura de medição avançada. 4. Resiliência a falhas. 5. Produção intelectual. I. Albuquerque, Célio Vinicius Neves de, orientador. II. Rocha, Antônio Augusto de Aragão, coorientador. III. Universidade Federal Fluminense. Escola de Engenharia. IV. Título.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

Igor Cesar Gonzalez RIbeiro

THOR: Um Framework para Infraestrutura de Medição Avançada Resiliente a Falhas de Agregadores nas Redes Elétricas Inteligentes

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Doutor em Computação. Área de concentração: Sistemas de Computação

BANCA EXAMINADORA

Prof. Célio Vinicius Neves Albuquerque - Orientador, UFF

Prof. Antônio Augusto de A. Rocha - Coorientador, UFF

Prof. Diego Passos, UFF

Prof.ª Débora Christina Muchaluat Saade, UFF

Prof. José Ferreira de Rezende, UFRJ

Prof. Flávia Coimbra Delicato, UFRJ

Niterói

2018

Dedico este trabalho a minha companheira de vida Gabriela Rebello Martins.

Agradecimentos

Eis que chega o momento de agradecer a todos que tornaram possível, suportável e vitoriosa a minha trajetória ao longo desses muitos anos de estudo. De fato, a lista de pessoas que contribuíram para a conclusão desse trabalho não é pequena e provavelmente é muito maior do que a minha memória, que a essa altura já mostra seus sinais de cansaço. Mesmo assim, prometo fazer um esforço para lembrar de todos.

Sem sombra de dúvidas, esse trabalho nunca teria sido possível sem os ensinamentos, os conselhos, as conversas e a força que me foi dada pelos meus orientadores Célio Albuquerque e Antônio Rocha. Na realidade, em diversas situações, esses dois excederam suas funções institucionais e foram verdadeiros amigos, não só comigo, mas com todos os seus orientados. Foi um privilégio e uma honra ter conhecido e trabalhado com vocês. Espero que um dia eu consiga retribuir um pouco do que me foi dado sendo um professor para outros quase tão bom quanto vocês foram para mim. Por tudo isso, o meu muito obrigado.

Gostaria de agradecer também a maravilhosa equipe do laboratório Midiacom, que me permitiu desenvolver o meu trabalho em um ambiente confortável e propício ao desenvolvimento de novas ideias. Em especial, eu gostaria de agradecer a incrível Marister Outão pelo imenso carinho com que me acolheu no laboratório dês do meu primeiro dia até hoje. Também gostaria de agradecer ao Diego Passos, uma das pessoas mais inteligentes, didáticas e disponíveis que já conheci. Muito obrigado pelas dicas e pelas ideias que, sem dúvidas, então presentes nos capítulos deste trabalho.

Dedico ainda o meu muito obrigado aos professores e funcionários do Instituto de Computação da UFF, os quais foram sempre solícitos para me ajudar quando eu precisei.

Agradeço também aos professores Débora Saade, Flávia Delicato e José Rezende por aceitarem fazer parte da minha banca.

Mesmo com orientadores excepcionais, por incontáveis vezes eu desanimei e achei que não iria conseguir. Cheguei em casa chateado, cansado e sem vontade de continuar. Para a minha sorte, em casa eu tinha uma companheira, uma amiga, uma conselheira, uma

coaching acadêmica persistente que nunca me deixou jogar a toalha. Gabriela, em todos esses anos juntos você sempre me ajudou a crescer e se hoje eu sou quem sou e conquistei o que conquistei é, em grande parte, graças a você. Obrigado por ter desempenhado as tarefas da casa que me competiam, além de ter passeado com o Romeu, para que eu tivesse tempo para trabalhar nesta tese. Acima de tudo, obrigado por ter escutado pacientemente toda a minha ladainha interminável sobre Smart Grids, mesmo sem entender nada do que eu dizia. Esse trabalho é uma realização minha, mas sem dúvida é sua também.

Eu também preciso agradecer aos meus pais pelo apoio, carinho e dedicação que sempre me dispensaram. Durante minha criação, a educação sempre foi prioridade e essa tese nada mais é do que o resultado das bases sólidas que eles me proporcionaram.

Agradeço também aos meus amigos, John Edson, Sérgio Telles, Flávio Queiroz e tantos outros que sempre me deram força pra continuar firme nessa ideia de ser doutor. Em especial, gostaria de agradecer a Rafaelle Castro por me incentivar a todo momento e por ter servido de inspiração (tendo ela também alcançado o doutorado) no final desta maratona.

Por fim, agradeço a CAPES por ter financiado a minha jornada no doutorado, permitindo que eu me dedicasse mais à minha pesquisa. Nos anos tempestuosos que se aproximam, onde a ignorância é cultuada e a educação é perseguida, eu realmente espero que outros possam ter as mesmas oportunidades que eu tive.

Resumo

As Redes Elétricas Inteligentes representam uma evolução do sistema elétrico atual e são projetadas para atender, de forma segura e confiável, a crescente demanda por energia. Para tanto, além de uma infraestrutura de transmissão e distribuição de energia, as Redes Elétricas Inteligentes também implementam uma rede de comunicação de dados, utilizada para coletar informações e enviar comandos para os diversos componentes do sistema elétrico. Um desses componentes, conhecido como Infraestrutura de Medição Avançada (IMA), é responsável por garantir a comunicação entre os medidores de energia, agora conhecidos como medidores inteligentes, e o restante da rede de dados. Diferentes tecnologias de comunicação foram propostas para a implementação da IMA, mas dentre elas as Redes em Malha Sem Fio (RMSF) oferecem uma maior flexibilidade e capacidade de recuperação de falhas, garantindo maior resiliência. Entretanto, mesmo com esses benefícios, quando um *gateway* falha na IMA, a rede pode levar algumas dezenas de segundos para se recuperar, provocando a perda de diversos pacotes possivelmente críticos. Em alguns casos, principalmente quando a falha é maliciosa, a rede pode nunca se recuperar, interrompendo a comunicação de certos medidores por um período indeterminado. Visando aumentar a resiliência da rede, este trabalho propõe o *framework* THOR, que utiliza proativamente um conjunto de *gateways*, de forma que se um deles falhar, as mensagens poderão continuar a ser entregues através dos demais, sem a necessidade de esperar o tempo de recuperação da rede. Além do *framework* em si, este trabalho também apresenta algumas propostas de implementação. Uma delas, denominada MDSA, foi capaz de entregar aproximadamente 100% das mensagens enviadas por todos medidores mesmo em cenários com falha de *gateways* sem causar uma sobrecarga significativa na latência das mensagens, como ocorre em propostas existentes.

Palavras-chave: Redes Elétricas Inteligentes, Infraestrutura de Medição Avançada, Resiliência, Redes em Malha Sem Fio, Roteamento, Falha de DAPs.

Abstract

Smart Grids represent an evolution of the current electrical power system. They are designed to supply the growing energy demands in a secure and reliable way. Besides a power grid infrastructure, Smart Grids also implement a data communication network, used to collect information and to send commands to several components of the power system. One of these components, called Advanced Metering Infrastructure (AMI), is responsible for enabling the communication between electric meters, now called smart meters, and the remaining devices of the data network. Some different network technologies have been proposed to implement AMI, but among them the Wireless Mesh Network (WMN) technology offers higher flexibility and resilience to failures. However, even with these benefits, when a gateway fails, the AMI may take several seconds to recover, resulting in the loss of some potentially critical packets. Even worse, if the failure is intentional and malicious, the network may never recover, breaking the communication to some meters for an undefined period of time. In order to increase network resilience, in this work we propose the THOR framework, which proactively uses a subset of reachable gateways, instead of just one (the best one). As a consequence, if one of these gateways fails, the messages can still be delivered through the remaining ones. Besides the framework, this thesis also presents some implementation proposals. One of them, called MDSA, enabled the delivery of approximately 100% of the messages sent by all meters even in scenarios with a gateway failure and without imposing a significant latency overhead, as it happens to some related works.

Keywords: Smart Grids, Advanced Metering Infrastructure, Resilience, Wireless Mesh Networks, Routing, DAP Failure.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

AMI	:	Advanced Metering Infrastructure;
IMA	:	Infraestrutura de Medição Avançada;
REI	:	Rede Elétrica Inteligente;
DAP	:	Data Aggregation Point;
RAV	:	Rede de Área de Vizinhança;
PLC	:	Power Line Communication;
RLA	:	Rede de Longo Alcance;
RMSF	:	Rede em Malha Sem Fio;
ETX	:	Expected Transmission Count;
OLSR	:	Optimized Link State Routing Protocol;
UDSA	:	Uniform DAP Selection Algorithm;
DDSA	:	Dynamic DAP Selection Algorithm;
MDSA	:	MultiDAP Selection Algorithm;
NIST	:	National Institute of Standards and Technology;
PRP	:	Parallel Redundancy Protocol;
HRP	:	High-availability Seamless Redundancy;
DANP	:	Doubly Attached Nodes with PRP;
SAN	:	Single Attached Node;
LRE	:	Link Redundancy Entity;
RCT	:	Edundancy Control Trailer;
SCP	:	Set Covering Problem;
SDR	:	Sucessful Delivery Rate;

Sumário

Capítulo 1

Introdução

É indiscutível que a vida em uma sociedade moderna se tornou totalmente dependente da disponibilidade de energia elétrica. A grande maioria dos serviços que utilizamos hoje são dependentes, em algum sentido, desse recurso, como comunicação, transporte, segurança, saúde, educação, dentre outros. Como consequência, a confiabilidade do sistema elétrico de uma nação tornou-se fundamental para garantir a continuidade do seu modo de vida.

1.1 O sistema elétrico atual e seus desafios

O sistema elétrico tradicional foi desenvolvido a partir de 1890, tendo sofrido atualizações ao longo das décadas seguintes para acompanhar a evolução tecnológica. Como resultado, a infraestrutura atual desse sistema é extremamente complexa, composta por milhares de dispositivos elétricos utilizados para controlar o fluxo de energia das plantas de geração até as linhas de transmissão e, em seguida, até os consumidores finais através das linhas de distribuição. Todos esses equipamentos, assim como o transporte da energia em si, precisam ser monitorados constantemente para evitar – e, caso ocorram, se recuperar de – falhas e desbalanceamentos, que podem levar a interrupções pontuais no fornecimento de energia ou, em casos mais graves, a grandes apagões.

De 1890 até os dias atuais, a população mundial cresceu consideravelmente. Entre 1900 e 2015, o número de indivíduos no planeta mais do que quadruplicou [48]. A partir da Figura 1.1 também é possível notar que para 2100 estima-se uma população mundial com 9,2 bilhões de habitantes. Soma-se a isso o fato de que, ao longo dessas décadas, o número de equipamentos movidos à energia elétrica cresceu ainda mais, criando uma enorme demanda não prevista na época do projeto do sistema elétrico tradicional.

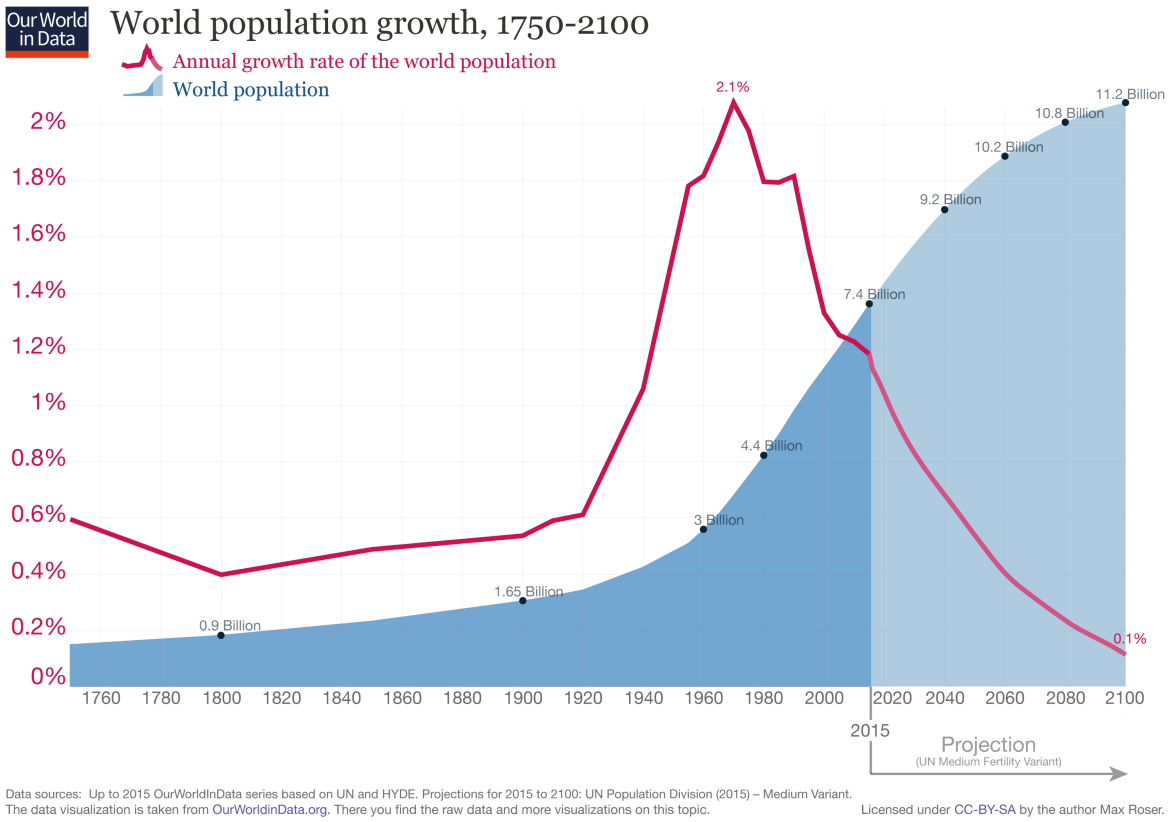


Figura 1.1: Crescimento da população mundial entre 1760 e 2100 (Fonte: [48]).

Como resultado, na última década ocorreram mais problemas (sobrecargas, apagões, etc.) do que nos quarenta anos anteriores [17]. Essas interrupções no fornecimento de energia causam impactos importantes na sociedade, incluindo grandes prejuízos sociais e econômicos. Como exemplo, segundo relatório do Tribunal de Contas da União (TCU), o custo do apagão ocorrido em 2001 no Brasil foi de $45,2$ bilhões de reais, dos quais 60% foram pagos pelos consumidores através de repasses tarifários [58]. Entretanto, esse problema não é exclusividade do Brasil. Em 2003, a região nordeste dos Estados Unidos e a região sul do Canadá sofreram o maior apagão da história, onde aproximadamente 50 milhões de pessoas foram afetadas [38].

É possível dividir a causa das interrupções de fornecimento de energia em dois grupos: a) interrupções devido a escassez de energia e b) interrupções devido a falhas operacionais e de controle. No cenário brasileiro, como mostrado na Figura 1.2, o processo de geração de energia elétrica é predominantemente baseado em hidrelétricas. Devido a sua natureza, a geração de energia depende fortemente do volume de água nos rios onde as usinas são instaladas. Em períodos prolongados de falta de chuva, o volume dos rios pode diminuir, dificultando, ou até mesmo impedindo, a geração de energia. Como contramedida, outras fontes de energia podem ser utilizadas, como por exemplo a térmica e a nuclear.

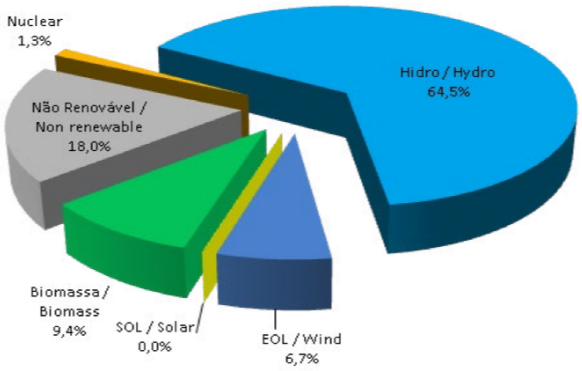


Figura 1.2: Matriz energética brasileira em 2016 [14].

Entretanto, a utilização dessas fontes de energia pode aumentar o custo para o consumidor final, além de, possivelmente, não atender toda a demanda. Como consequência, em períodos de grande estiagem é comum ocorrer a necessidade do racionamento de energia e, em cenários mais graves, a interrupção do seu fornecimento. Por outro lado, ainda que a geração de energia seja compatível com a demanda, a infraestrutura utilizada para transportá-la das plantas de geração até o usuário final é complexa e engloba diversos componentes que, por sua vez, podem falhar.

Em um sistema que implementa um fluxo unidirecional de energia e que possui baixa ou nenhuma participação do consumidor final, a única estratégia possível para compatibilizar oferta e demanda é o aumento da produção. Entretanto, fica claro que em algum momento as plantas de geração já em operação não serão capazes de suprir a demanda, levando à instalação de novas usinas hidrelétricas, termelétricas, nucleares, etc. No caso das usinas hidrelétricas, sua construção exige a inundação de grandes áreas, causando grandes prejuízos à fauna, à flora e à população que vive na região. As termelétricas consomem grandes quantidades de combustível fóssil, contribuindo para o aquecimento global e todos os problemas associados a ele (nos Estados Unidos o sistema elétrico é responsável por 40% das emissões de carbono em toda a nação [22]). Já as usinas nucleares podem causar acidentes de grande magnitude devido a falhas ou descarte incorreto de rejeitos. Em qualquer um desses casos, a criação de novas plantas de geração causa impactos importantes e deve ser evitada. Por outro lado, temos atualmente a disponibilidade de fontes alternativas de energia consideradas limpas como, por exemplo, a solar, a eólica e a maremotriz. A integração dessas fontes no sistema elétrico constitui um importante passo no caminho para reduzir a emissão de carbono e, consequentemente, reduzir problemas ambientais, como o aquecimento global.

A partir do exposto, podemos questionar como será possível lidar com a crescente

demanda por energia sem recorrer (ou ao menos recorrer o mínimo possível) à criação de novas plantas de geração. A resposta para essa pergunta exige uma atualização completa de toda a infraestrutura da rede elétrica, permitindo um fluxo bidirecional de energia e geração distribuída, onde um consumidor que produza localmente sua própria energia (através de painéis solares, por exemplo) possa devolver para a rede elétrica seu excedente e ser remunerado por isso. Além disso, essa nova infraestrutura também precisa ampliar o controle e a automação em todas as etapas do transporte da energia, permitindo uma recuperação de falhas ainda mais rápida. Para que isso seja possível, os diversos equipamentos do sistema elétrico precisam ser capazes de se comunicar, incluindo os medidores de energia que hoje operam de forma isolada.

Com a evolução da tecnologia, cada vez mais dispositivos utilizados na infraestrutura da rede elétrica têm ganhado capacidade de processamento e comunicação, permitindo que a rede se torne cada vez mais autônoma, inteligente e resiliente a falhas. Com base nisso, diversas aplicações têm sido propostas para as redes elétricas, incluindo a adoção de novas fontes renováveis de energia, a descentralização da distribuição de energia através das chamadas Microgids [43] e a maior participação dos consumidores no processo de distribuição de energia através de sistemas de resposta à demanda [44]. A implementação de todas essas novas funcionalidades conduz a rede elétrica atual a um novo patamar, conhecido como Rede Elétrica Inteligente - REI [1].

1.2 Visão Geral das Redes Elétricas Inteligentes - REI

Segundo o *National Institute of Standards and Technology* - NIST, as características que definem as REI incluem [40]:

- Aumento da utilização de tecnologias de controle e informação para aumentar a resiliência, segurança e eficiência da rede elétrica;
- Otimização dinâmica das operações e recursos da rede elétrica, tudo com uma cibersegurança completa;
- Implementação e integração de geração distribuída de energia, incluindo fontes renováveis;

[1] O conceito de Rede Elétrica Inteligente é mais conhecido na comunidade científica pelo seu nome em inglês *Smart Grid*. Entretanto, para fins de padronização, a sigla em português será utilizada no restante do texto.

- Implementação e integração de resposta à demanda;
- Instalação de tecnologias inteligentes de medição, comunicações relacionadas às operações da rede elétrica e automação do domínio de distribuição;
- Fornecimento de informações em tempo real e opções de controle aos consumidores;
- Desenvolvimento de padrões de comunicação e interoperabilidade entre equipamentos conectados à rede elétrica.

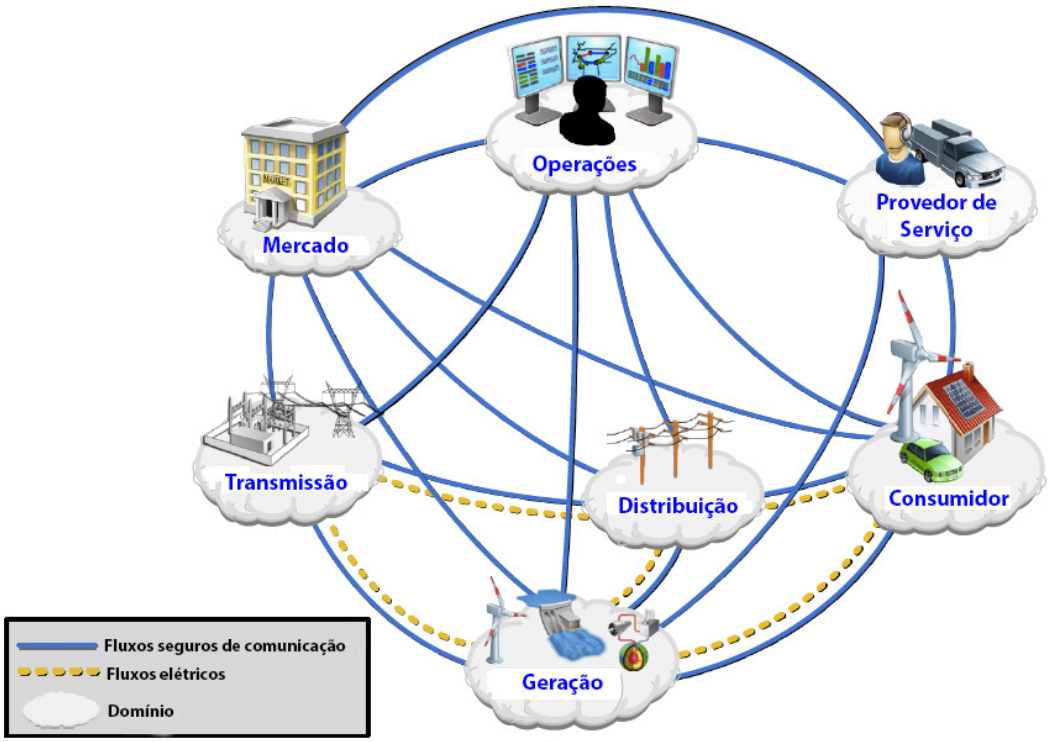


Figura 1.3: Interação entre os diferentes domínios das Redes Elétricas Inteligentes através de conexões seguras (Adaptado de [40]).

Para que todos os objetivos e benefícios pretendidos para as REI sejam alcançados, é necessário que os diversos agentes envolvidos nesse complexo sistema, como desenvolvedores de equipamentos e provedores de serviço, possam manter a interoperabilidade de seus produtos e serviços. Assim, é importante que seja desenvolvido um conjunto de documentos arquiteturais que possibilitem que cada *stakeholder* se mantenha focado no seu próprio negócio, mas de tal forma que o produto ou serviço gerado possa interagir sem problemas com os demais. Com esse objetivo, foi desenvolvido pelo NIST um modelo

conceitual que divide o complexo conjunto de redes e tecnologias que compõem a infraestrutura das Redes Elétricas Inteligentes em sete domínios, como ilustrado na Figura 1.3. A seguir são apresentadas as definições de cada domínio.

- **Consumidor:** refere-se aos usuários finais de energia elétrica, podendo ser residenciais, industriais ou comerciais. Nesse domínio são previstas atividades de geração, armazenamento e gerenciamento do uso de energia elétrica;
- **Mercado:** refere-se aos operadores e participantes responsáveis pela comercialização da energia elétrica;
- **Provedor de Serviços:** inclui as organizações responsáveis por prover serviços para os consumidores e para as companhias de energia;
- **Operações:** inclui as entidades responsáveis por gerenciar o processo de transmissão e distribuição da energia elétrica;
- **Geração:** esse domínio inclui as fontes de geração de energia como nuclear, térmica e hidráulica, usualmente conectadas às linhas de transmissão. Além disso, a geração distribuída de energia também se encontra neste domínio, mas precisa estabelecer associações com os domínios Consumidor, Distribuição e Provedor de Serviço;
- **Transmissão:** engloba as entidades responsáveis por transportar a energia elétrica através de grandes distâncias;
- **Distribuição:** engloba as entidades responsáveis por distribuir a energia elétrica de/para os consumidores.

Além dos domínios, a figura também mostra as linhas de condução de energia elétrica e de comunicação. É possível notar que as linhas de energia conectam os domínios Consumidor, Geração, Transmissão e Distribuição e representam um fluxo bidirecional entre os mesmos. Uma vez que todo o processo de geração, transmissão e distribuição de energia precisa ser monitorado e controlado, as linhas de comunicação interligam todos os domínios das REI.

De maneira geral, as REI podem ser divididas em duas partes: Infraestrutura e Aplicações, conforme ilustrado na Figura 1.4. A Infraestrutura contempla uma rede elétrica com fluxo bidirecional de energia e um sistema de comunicação de dados responsável por interligar os diferentes dispositivos da rede elétrica. Por outro lado, as aplicações utilizam a infraestrutura e as informações obtidas através dela para implementar aplicações

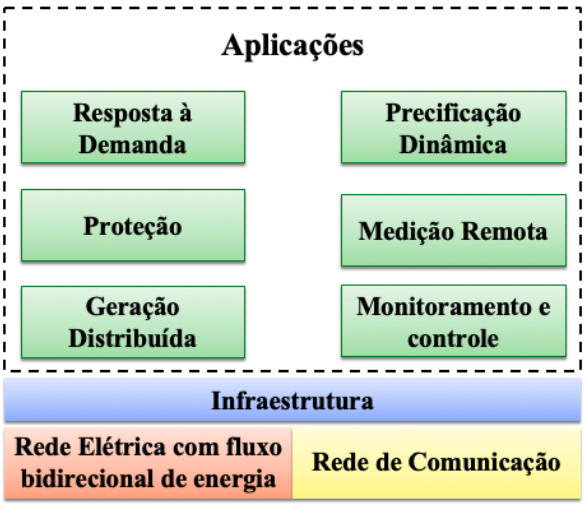


Figura 1.4: Estrutura das Redes Elétricas Inteligentes.

que aumentem a eficiência e a confiabilidade do sistema elétrico e reduzam seus impactos ambientais.

1.2.1 Geração Distribuída

Em contraste ao modelo tradicional que permitia apenas um fluxo unidirecional de energia das plantas de geração até o consumidor final, nas REI esse fluxo se torna bidirecional, o que permite uma geração de energia muito mais flexível. Uma possibilidade bastante interessante é o aproveitamento de diversas fontes de energia, em sua maioria renováveis, para complementar a geração principal. Esse modelo de geração distribuída traz diversos benefícios. Em primeiro lugar, uma vez que as fontes distribuídas de energia estão mais próximas aos consumidores finais (painéis solares, carros elétricos, etc.), os prejuízos financeiros e ambientais resultantes das perdas de energia nas linhas de transmissão são mitigados [22]. Em algumas situações, a produção de energia por essas fontes distribuídas pode se tornar maior do que a demanda local, o que permite que os consumidores vendam o excedente de volta para as companhias de energia ou para outros consumidores [15].

Outro benefício importante trazido pela geração distribuída é a formação das chamadas Microgrids. A ideia é conectar algumas dessas pequenas fontes distribuídas de energia de forma que elas operem como uma grande fonte, fornecendo energia para os consumidores locais. A utilização de Microgrids permite que regiões, chamadas de ilhas, continuem recebendo energia mesmo quando a distribuição originária da rede elétrica principal é interrompida. Adicionalmente, as Microgrids também podem ser utilizadas para suprir o crescimento da demanda, sem a necessidade de construir novas plantas de geração. O

conceito de Microgrids tem sido bastante discutido na literatura ([21, 43, 33, 55, 51]) e diversos desafios foram levantados, como a imprevisibilidade das fontes distribuídas de energia, a necessidade de construir sistemas de recuperação de falhas que protejam as Microgrids de falhas na rede elétrica principal e ainda que protejam as fontes individuais em uma Microgrid em caso de falha de uma delas. Outro desafio importante é a integração de veículos elétricos na rede, tanto por conta do seu consumo, quanto pela possibilidade de utilização desses veículos como fonte de energia em caso de alta demanda.

1.2.2 Precificação Dinâmica e Resposta à Demanda

Uma vez que nas REI os consumidores estão conectados à rede elétrica e de comunicação através dos medidores, as companhias de energia podem enviar, em tempo real, informações sobre o preço da energia naquele momento. Ou seja, com as REI o preço da energia passa a ser reajustado de uma forma muito mais granular do que é feito atualmente. De posse dessa informação, o consumidor pode ajustar o seu perfil de consumo, reduzindo a utilização de equipamentos não essenciais durante períodos de pico e, portanto, com energia mais cara. Como consequência, a companhia de energia é capaz de estabelecer um sistema de resposta à demanda com a participação dos consumidores, de forma a evitar racionamentos ou outros problemas devido ao desbalanceamento entre oferta e consumo. Abordagens para precificação dinâmica e resposta à demanda têm recebido bastante atenção da comunidade científica ao longo dos últimos anos. Exemplos de trabalhos podem ser observados em [34, 49, 63, 29, 50, 13, 20, 54, 31, 62].

1.2.3 Monitoramento, Controle e Proteção

Para que a rede elétrica seja capaz de fornecer um serviço de distribuição de energia eficiente e confiável, os diversos equipamentos envolvidos em todo o processo de transmissão e distribuição devem ser constantemente monitorados. Para tanto, diversas propostas na literatura sugerem a implantação de uma rede de sensores nas REI, como em [7, 57, 24]. Adicionalmente, atuadores também podem ser instalados, de forma a permitir que, de forma autônoma ou semiautônoma, a rede possa se recuperar de eventuais falhas elétricas ou mecânicas, como falha de condutores, queda de torres de transmissão e condições severas anormais, como focos de incêndio próximos às linhas de transmissão.

Apesar de seus possíveis benefícios, a implantação de uma Rede de Sensores Sem Fio nas REI também traz desafios, como discutido em [6]. Em primeiro lugar, o ambiente

onde os sensores devem ser instalados apresenta condições bastante variadas e adversas, como alta umidade, grande quantidade de vibrações, poeira, etc. Além disso, devido à criticidade das informações geradas e transmitidas pelos sensores, a rede deve garantir restrições mínimas de qualidade de serviço, permitindo que as mensagens sejam entregues com a confiabilidade adequada. Pela mesma razão, os sensores também serão alvos de ataques, o que significa que a rede deve ser projetada para permitir uma comunicação segura entre os sensores e a entidade que processa essas mensagens [3].

1.2.4 Medição Inteligente

Com a disponibilização de uma rede de comunicação que integra os consumidores através de medidores inteligentes com o restante das entidades participantes do sistema elétrico, o processo de medição de vários parâmetros relacionados ao domínio de distribuição de energia se tornou muito mais eficiente. Com isso, informações importantes para a geração de faturas e para a proteção da rede elétrica podem ser obtidas em tempo real pelos operadores. Ademais, os medidores inteligentes podem trocar informações com os diversos dispositivos presentes nas residências dos usuários, permitindo diversas aplicações como, por exemplo, a verificação do consumo de cada dispositivo em tempo real, ações de resposta a demanda que permitam a companhia de energia desligar alguns equipamentos em horários de pico, entre outros [56].

Devido ao seu caráter crítico, o sistema de Medição Inteligente precisa ser seguro, garantindo a privacidade dos dados dos usuários, impedindo fraudes e ataques com o objetivo de derrubar todo o sistema elétrico [59]. Violações de segurança no sistema de Medição Inteligente podem causar bilhões de dólares em prejuízo financeiro para os consumidores, para a companhia de energia e para a nação como um todo [66]. A implementação do sistema de Medição Inteligente requer que os medidores inteligentes sejam conectados ao restante da rede de dados do sistema elétrico, o que é feito através da Infraestrutura de Medição Avançada (IMA), assunto discutidao na próxima seção.

1.2.5 Infraestrutura de Medição Avançada - IMA

Atualmente, a rede elétrica não conta com qualquer participação dos consumidores em seus processos. As informações coletadas a partir dos usuários finais resumem-se a dados de consumo e são obtidas, em geral, de forma manual pelos funcionários de campo. Esse cenário tem se mostrado cada vez mais ineficiente, pois gera gastos com o deslocamento

de técnicos e impede que controles e serviços mais granulares sejam implementados. Com o passar dos anos, um grande esforço foi feito com o objetivo de desenvolver e instalar medidores mais inteligentes, com poder de processamento e comunicação. Além do consumo de energia, esses medidores são capazes de medir um conjunto muito mais amplo de parâmetros periodicamente, como o valor instantâneo da voltagem, valor instantâneo da corrente, etc.

Para que os dados coletados pelos medidores inteligentes possam ser enviados até a Central de Controle da companhia de energia e para que esta possa enviar comandos até os medidores, uma infraestrutura de comunicação precisa ser utilizada. Essa infraestrutura é denominada Infraestrutura de Medição Avançada - IMA.

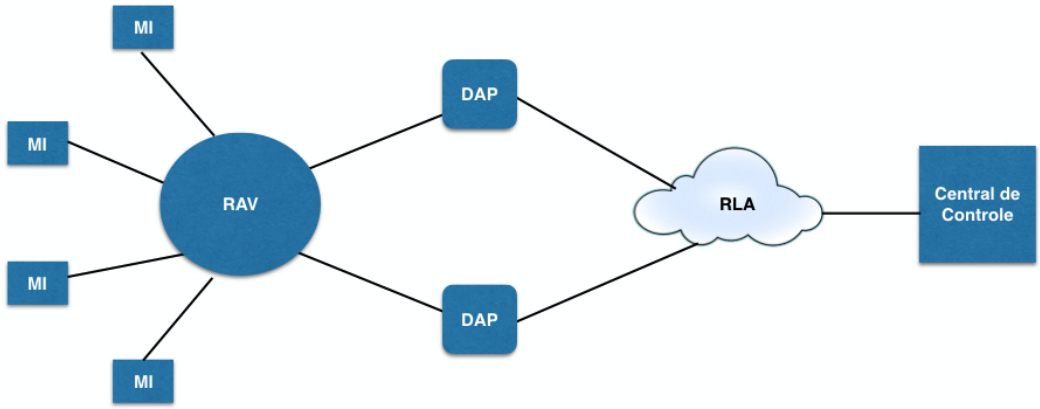


Figura 1.5: Estrutura típica de uma IMA.

De maneira geral, as implementações da IMA vêm sendo baseadas em uma estrutura similar à mostrada na Figura 1.5. As mensagens geradas pelos Medidores Inteligentes - MIs são enviadas para os *gateways*, também conhecidos como Pontos de Agregação de Dados (PAD), ou do inglês *Data Aggregation Points* - DAPs[2], através da Rede de Área de Vizinhança - RAV. Por sua vez, os DAPs agregam as mensagens dos medidores e as encaminham para Central de Controle através da Rede de Longo Alcance - RLA. Da mesma forma, comandos podem ser enviados a partir da Central de Controle para um MI específico, sendo recebidos primeiramente pelo DAP e, então, repassados para os medidores especificados.

Para que a IMA possa funcionar corretamente, os MIs e os DAPs precisam trocar mensagens utilizando alguma tecnologia de comunicação disponível. Duas tecnologias comumente adotadas são o *Power Line Communication* - PLC [16] e as Redes em Malha

[2]No restante deste trabalho, a sigla DAP será utilizada ao invés de PAD, já que o termo em inglês é mais comum na literatura do que o em português.

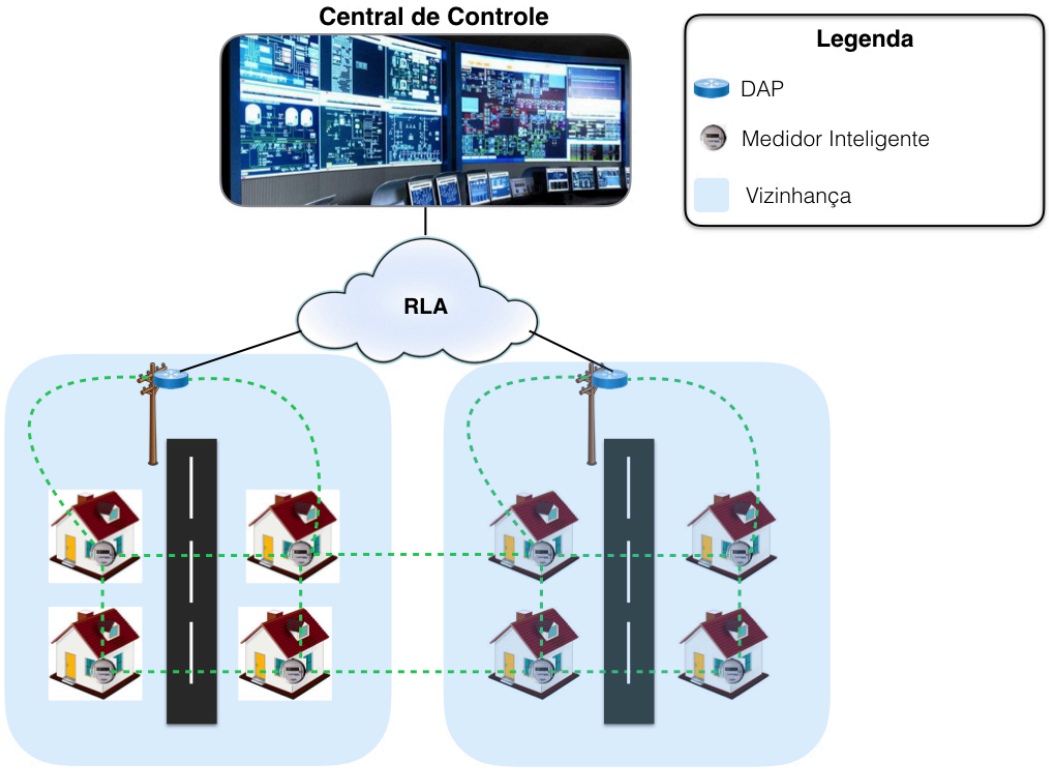


Figura 1.6: Cenário de uma IMA onde os medidores inteligentes e os DAPs formam uma RMSF.

Sem Fio - RMSF [1, 53, 12, 19, 42]. O protocolo PLC permite que sejam enviados dados pelos cabos elétricos de distribuição que são utilizados para alimentar residências e industrias em uma região. Diversos projetos reais, principalmente na Europa, utilizam o PLC para comunicação entre os medidores inteligentes e os DAPs. Por exemplo, o projeto executado pela companhia elétrica italiana Enel instalou, até o fim de 2013, 32 milhões de medidores inteligentes na Itália. Outros exemplos incluem a Suécia, Áustria e Holanda [18].

Apesar de apresentar vantagens como a possibilidade de transmissão através de longas distâncias (utilizando baixa frequência) e a redução dos custos de implantação, o PLC sofre de problemas de largura de banda reduzida e interferência [10], além de representar um ponto único de falha, uma vez que se a rede elétrica parar de funcionar, a rede de comunicação também ficará inoperante.

Por outro lado, a utilização de RMSF torna a rede mais flexível, permitindo que ela se auto-organize e se recupere de falhas automaticamente. Devido a esses benefícios, a implementação da IMA como uma RMSF tem recebido considerável atenção da comunidade acadêmica, além de estar sendo utilizada em diversos projetos reais nos EUA e

na Ásia [25, 60]. Nesse sentido, este trabalho segue esta linha e considera a IMA como mostrada na Figura 1.6.

1.3 Problema Estudado

Para que as aplicações que dependem da IMA funcionem corretamente, dentro dos critérios de qualidade de serviço estabelecidos [32], a rede deve garantir a comunicação dos medidores inteligentes com o restante da rede, mesmo em caso de falha de equipamentos. Devido às suas características naturais, as RMSF permitem auto-recuperação em caso de falhas de nós e enlaces. Entretanto, esse processo não é imediato, podendo levar a uma perda massiva de pacotes (dependendo do tráfego da rede) e, para aqueles que são entregues, um aumento da latência. Em outras aplicações, como no caso das Redes de Sensores Sem Fio (RSSF), esse pode não ser um problema sério, tendo em vista que em muitos casos as RSSF são tolerantes a atraso e perda de pacotes. Porém, no caso da AMI, as restrições de latência e disponibilidade são mais estritas, e os efeitos causados pela falha podem inviabilizar aplicações críticas, como a Resposta à Demanda e a Precificação Dinâmica.

Dentre os possíveis problemas que podem ocorrer em uma AMI, a falha de um DAP tem grande potencial de prejudicar as aplicações, a medida que é por meio desses equipamentos que os medidores inteligentes se comunicam com o restante da rede. Para compreender as implicações causadas pela falha, considere a IMA simplificada mostrada na Figura 1.7, onde um medidor inteligente M pode enviar suas mensagens através do DAP D_1 ou do DAP D_2. Como pode ser observado, o custo do caminho $(M - D_1)$ é menor que o custo do caminho $(M - D_2)$, uma vez que o enlace $E(M, D_1)$ tem qualidade superior a do enlace $E(M, D_2)$. Como consequência, M envia todas as suas mensagens através do DAP D_1.

Suponha que em determinado instante de tempo t_f, o DAP D_1 passe a apresentar uma falha onde, além de não processar e encaminhar pacotes recebidos, ele também pare de enviar as mensagens periódicas de *hello* geradas pelo protocolo de roteamento. Com o tempo, dependendo da métrica de roteamento, o custo do caminho $(M - D_1)$ começará a aumentar até que, em um instante de tempo t_{rec}, o custo do caminho $(M - D_1)$ se tornará maior do que o do caminho $(M - D_2)$. Nesse instante, o protocolo de roteamento em M passará a selecionar o DAP D_2 como próximo salto para todas as mensagens enviadas pelo medidor e, consequentemente, a rede terá se recuperado da falha. Apesar dessa recu-

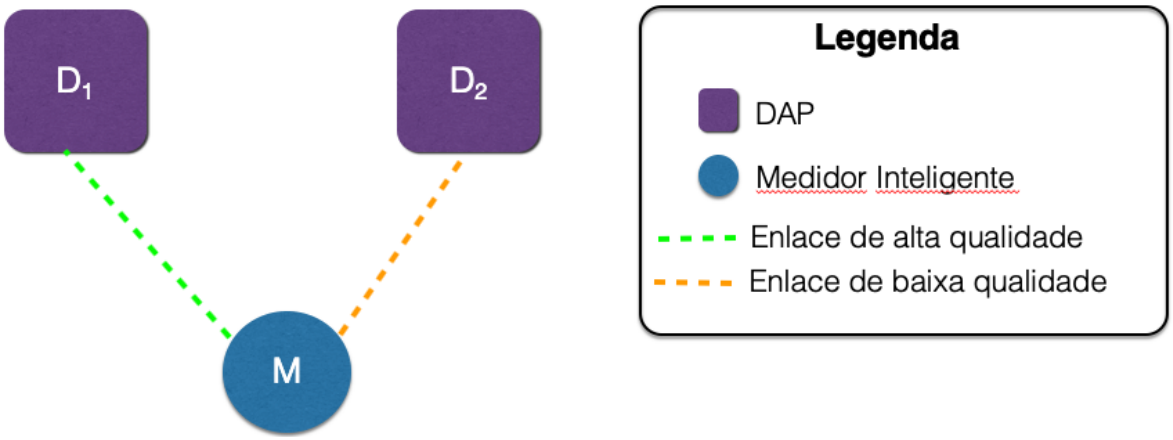


Figura 1.7: IMA simples onde o MI pode enviar suas medições tanto para o DAPA quanto para o DAPB através de uma rede em malha sem fio 802.11. O enlace para o DAPA possui qualidade superior ao enlace para o DAPB.

peração, durante o intervalo de tempo $[t_f, t_{rec}]$ o medidor M se manteve enviando todas mensagens através do DAP D_1 que, por sua vez, continuou descartado todas elas devido à falha. No trabalho publicado em [41], é proposto um modelo matemático que descreve precisamente este comportamento. A partir desse modelo, os autores geraram o gráfico mostrado na Figura 1.8, que descreve como a probabilidade de entrega das mensagens varia com o tempo. A linha correspondente ao Best_ETX representa justamente o comportamento que descrevemos, enquanto que a linha DDSA representa o comportamento da proposta dos autores, que será explicada no Capítulo 2. Note que o DAP D_1 passa a apresentar a falha no instante 20s, quando a probabilidade de entrega do Best_ETX cai a zero, se mantendo assim até o instante 75s, ponto onde ocorre a recuperação da rede.

Um problema ainda mais sério poderia ser causado se a falha do DAP D_1 fosse decorrente de um ataque cibernético e, portanto, maliciosa. Nesse caso, o atacante poderia reconfigurar o DAP para que este passasse a se comportar como um Buraco Cinza [27], atraindo o tráfego para si (através de mensagens de roteamento falsas), descartando as mensagens de aplicação enviadas pelos (ou para os) medidores, mas mantendo o comportamento normal do ponto de vista do protocolo de roteamento. Sendo assim, uma vez que a rede não é mais capaz de detectar a falha, ela não se recupera, fazendo com que o medidor M se mantenha indisponível por um tempo indeterminado.

A partir do exposto, o problema estudado nesta tese é como utilizar a redundância de DAPs trazida pela implementação da IMA como uma RMSF para que esta infraestrutura seja robusta e resiliente a falhas de DAPs, sendo elas maliciosas ou não.

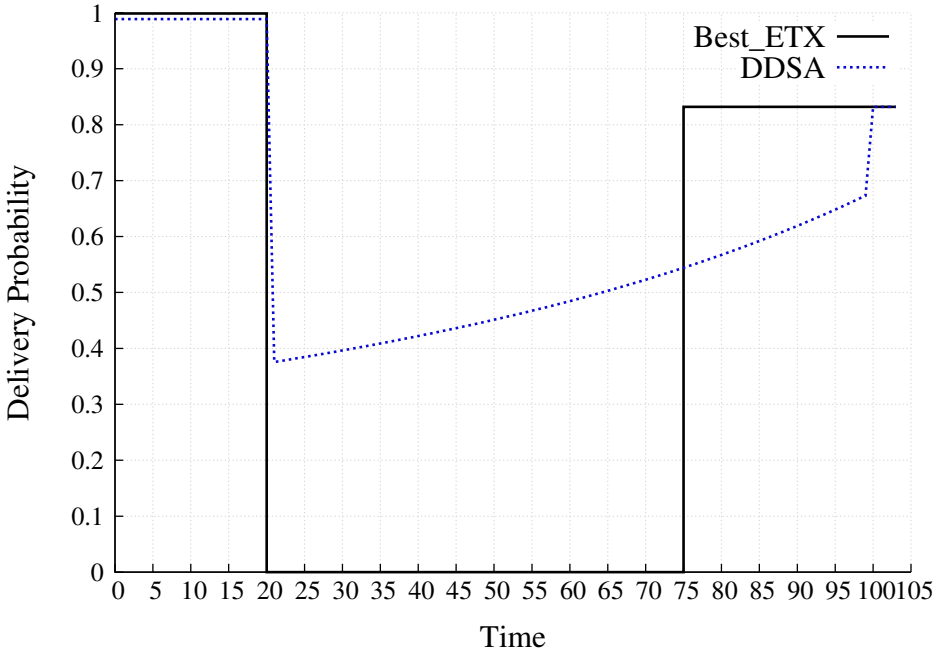


Figura 1.8: Variação da probabilidade de entrega em uma IMA com falha (não maliciosa) de um DAP, de acordo com o modelo matemático proposto em [41].

1.4 Objetivos da Tese

O principal objetivo desta tese é desenvolver uma solução que mitigue os efeitos causados na IMA pelo comportamento anormal de um DAP, seja esse comportamento uma Falha Total do dispositivo ou uma falha causada por um ataque de Buraco Negro com Repasse Seletivo. Neste sentido, a solução desenvolvida deve garantir uma alta taxa de entrega de pacotes, porém sem contribuir para o aumento desnecessário da latência na entrega desses pacotes. Também é objetivo deste trabalho propor um *Framework* que guie o desenvolvimento de propostas que aproveitem a redundância de DAPs disponíveis em uma IMA a fim de permitir que a rede se recupera na ocorrência de uma falha nesses dispositivos.

1.5 Principais Contribuições

Durante a elaboração desta tese, as seguintes contribuições foram alcançadas:

1. Proposta do *framework* THOR, utilizado como base para soluções que se consideram a redundância de DAPs em uma IMA para permitir que a rede se recupere de falhas nesses dispositivos;

2. Proposta do *Uniform DAP Selection Algorithm* (UDSA), uma solução baseada no *framework* THOR, que realiza um número pré-definido de retransmissões pró-ativas e, a cada uma, escolhe um DAP de acordo com sua probabilidade de seleção que, nesse caso, é uniformemente distribuída entre todos os DAPs elegíveis;

3. Proposta do *Dynamic DAP Selection Algorithm* v2 (DDSA v2), o qual é similar ao DDSA [41], mas nesse caso o número de retransmissões pró-ativas é calculado dinamicamente, de acordo com a probabilidade de entrega pretendida;

4. Proposta do *MultiDAP Selection Algorithm* (MDSA). Assim como as demais propostas, o MDSA também realiza retransmissões pró-ativas, mas o número de retransmissões é calculado dinamicamente e individualmente para cada DAP elegível, de acordo com a métrica de roteamento. Nessa proposta, todos os DAPs elegíveis são sempre selecionados para cada mensagem, aumentando a utilização da redundância de DAPs disponível;

5. Implementação no simulador NS3 de uma versão modificada do protocolo OLSR, para permitir a utilização de métricas cientes de qualidade;

6. Implementação no simulador NS3 de uma versão da métrica ETX baseada em [45].

1.6 Organização do Texto

O restante do texto está organizado da seguinte forma: O Capítulo 2 apresenta uma visão geral sobre trabalhos relacionados a esta tese. No Capítulo 3 é apresentado o *framework* THOR para o projeto e implementação de uma IMA baseada em Redes em Malha Sem Fio resiliente a falha de DAPs. No Capítulo 4, são apresentadas algumas propostas para implementação dos módulos do *framework* THOR. No Capítulo 5, é realizada uma comparação entre os resultados de simulação das propostas apresentadas no Capítulo 4 quanto às métricas Taxa de Entrega de Mensagens e Latência Média. Por fim, no Capítulo 6, são apresentadas as conclusões obtidas neste trabalho e propostas para trabalhos futuros.

Capítulo 2

Trabalhos Relacionados

Resiliência e confiabilidade são duas propriedades fundamentais que devem ser consideradas ao se construir uma infraestrutura de comunicação para sistemas críticos. Enquanto confiabilidade está relacionada à capacidade do sistema manter seus serviços disponíveis de acordo com os parâmetros acordados, resiliência é a habilidade que o sistema tem de se recuperar de falhas. Consequentemente, um sistema resiliente é um sistema mais confiável. Como discutido em [61], uma IMA baseada em uma Rede em Malha Sem Fio (RMSF) provê comunicação de dados de forma robusta e relativamente confiável, devido à existência de caminhos redundantes entre uma origem e um destino, permitindo uma recuperação rápida na ocorrência de falhas de enlace ou de nós da rede.

Devido a requisitos estritos impostos ao tempo de recuperação de falhas pela norma IEC 61850-5, sistemas de tele-proteção instalados em subestações implementam protocolos que auxiliam no pronto reestabelecimento da comunicação em caso de falhas de dispositivos ou enlaces. Dois desses protocolos são o *Parallel Redundancy Protocol* - PRP e o *High-availability Seamless Redundancy* - HSR. O PRP [4] utiliza uma abordagem proativa onde cada mensagem gerada é duplicada e, em seguida, é encaminhada através de componentes redundantes distintos. Uma vez que os benefícios introduzidos pelo PRP dependem da disponibilidade desses componentes redundantes, o protocolo estabelece que toda a infraestrutura de rede deve ser duplicada, conforme ilustrado na Figura 2.1.

No jargão do PRP, dispositivos conectados diretamente às duas redes da topologia são chamados de *Doubly Attached Nodes with PRP* - DANP. Por outro lado, dispositivos que são conectados diretamente a somente uma das redes são chamados de *Single Attached Nodes* - SAN. Um SAN pode se conectar às duas redes através dos chamados *RedBoxes*. Como pode ser observado na figura, quando um dispositivo origem (*source* deseja enviar uma mensagem para um dispositivo destino (*destination*), o PRP na origem deve duplicar

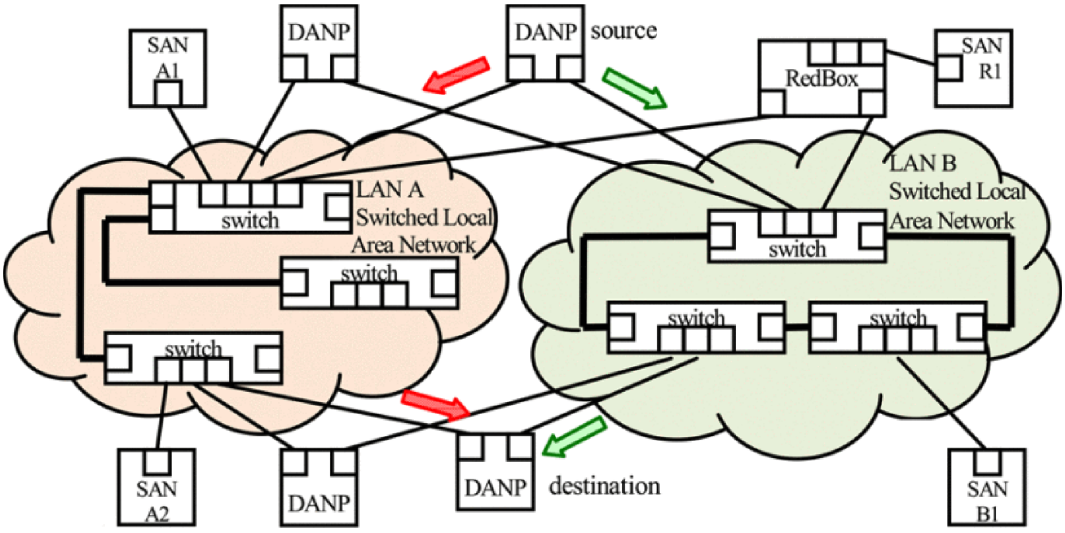


Figura 2.1: Topologia PRP utilizando duas redes para prover redundância [4].

a mensagem e enviar cada cópia por uma rede diferente. Se uma falha ocorrer em uma das duas redes, a mensagem ainda poderá ser recebida através da outra rede. Caso nenhuma falha ocorra, o destino irá receber a mensagem de forma duplicada, o que precisa ser tratado de forma apropriada.

Para permitir o tratamento das mensagens duplicadas sem a necessidade de modificar os demais serviços de rede, o PRP introduz uma camada adicional entre a camada de enlace e a camada física dos dispositivos, chamada *Link Redundancy Entity* - LRE. Quando uma mensagem é gerada, a camada de enlace entrega o *frame* correspondente para a camada LRE, que introduz o chamado *Redundancy Control Trailer* - RCT ao final do cabeçalho do *frame*, conforme mostrado na Figura 2.2.

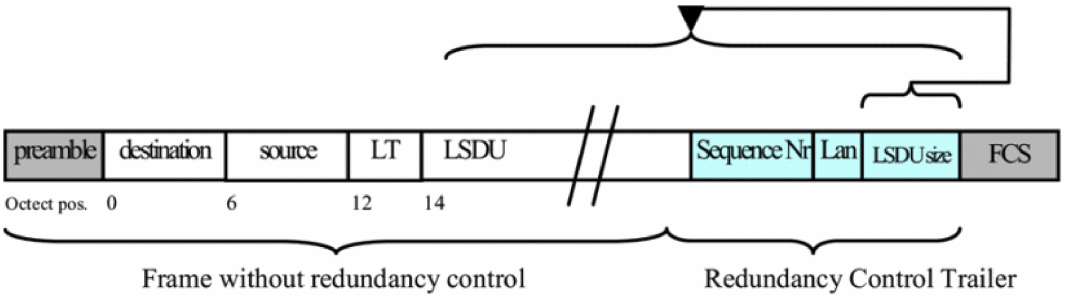


Figura 2.2: Estrutura do *Redundancy Control Trailer* - RCT [4]

O primeiro componente do RCT é um número de sequência que deve ser único para cada mensagem (mas duas cópias da mesma mensagem possuem o mesmo número de sequência). Uma característica do PRP é que as interfaces conectadas as duas redes possuem o mesmo endereço MAC. Sendo assim, o RCT também possui o campo LAN, utilizado para identificar por qual rede o *frame* foi enviado. O último campo do RCT,

LSDU *Size*, guarda o tamanho do campo LSDU do cabeçalho Ethernet mais o tamanho do RCT, incluindo o campo LSDU *Size*.

Apesar das vantagens introduzidas pelo PRP, alguns problemas também podem ser identificados. Em primeiro lugar, a necessidade de se duplicar praticamente toda a infra-estrutura de rede eleva consideravelmente os custos de implantação do sistema de tele-proteção [30]. Além disso, o PRP só é capaz de se recuperar imediatamente de uma falha por vez (em uma rede). Se duas falhas ocorrerem ao mesmo tempo, uma em cada rede, a mensagem enviada pela origem não será recebida no destino. Essa característica torna a capacidade de recuperação de falhas do PRP não escalável.

Assim como o PRP, o protocolo HSR também procura garantir a pronta recuperação de falhas através da utilização de redundância na rede. Entretanto, ao invés de utilizar duas redes LAN duplicadas, o HSR opera sobre uma única rede com topologia em anel, como ilustrado na Figura 2.3.

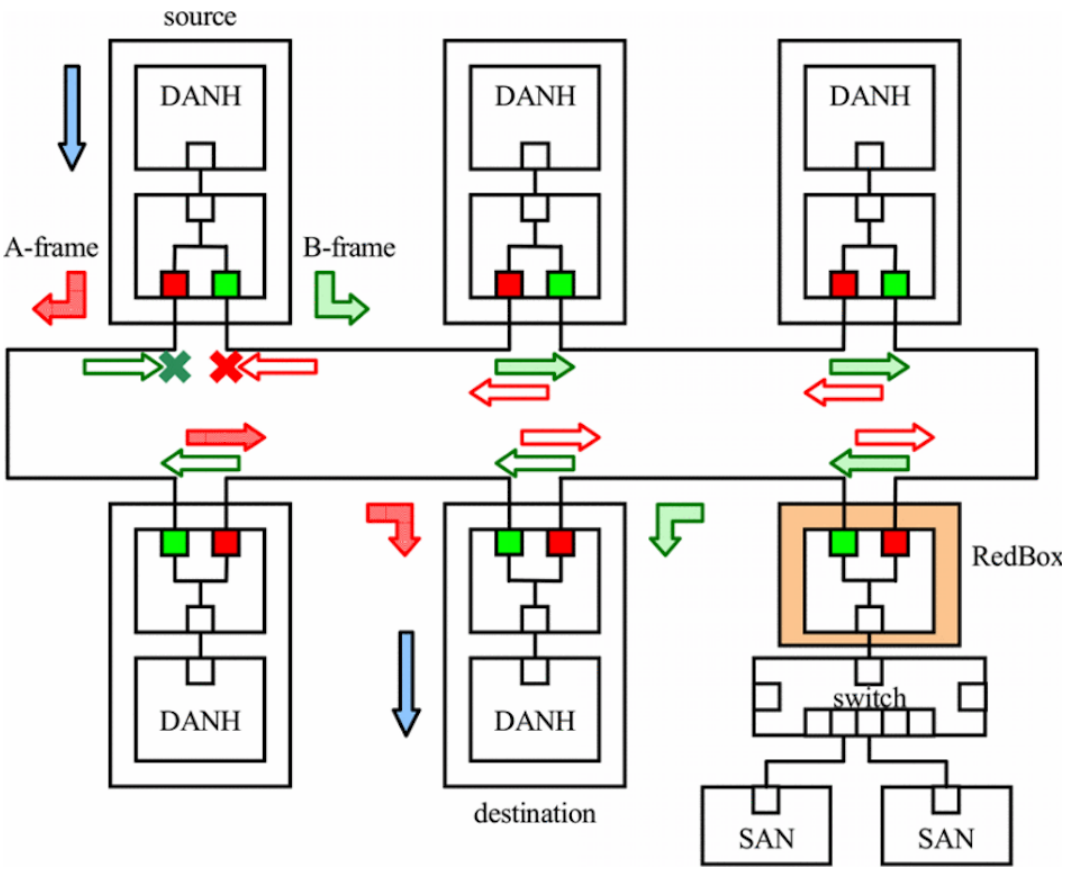


Figura 2.3: Topologia em anel utilizada pelo HSR [4].

Os dispositivos DANH são similares aos dispositivos DANP, mas habilitados para o HSR ao invés do PRP. No HSR, dispositivos SAN só podem se conectar à rede através da utilização de *RedBoxes*. Quando uma mensagem precisa ser enviada por um dispositivo

origem, ela é duplicada e cada cópia é transmitida em um sentido diferente do anel. Os nós na rede HSR também implementam uma camada LRE, responsável por tratar duplicatas, encaminhar e descartar *frames*, etc. Ao contrário do LRE do PRP, que adiciona o RCT ao final do *frame* Ethernet, o LRE do HSR adiciona uma *tag* HSR de 6 *bytes* logo após o campo de endereço de destino do *frame*, conforme mostrado na Figura 2.4.

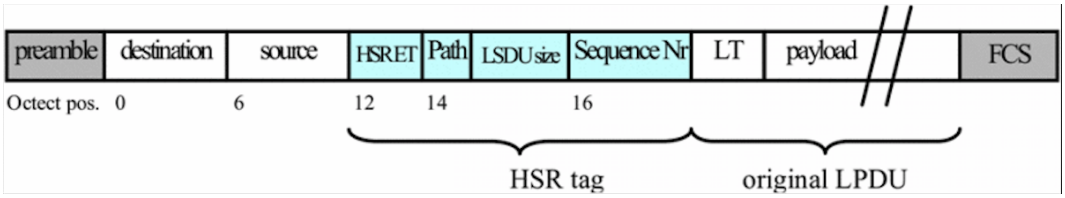


Figura 2.4: Estrutura da *tag* HSR [4].

Apesar desses protocolos permitirem que a rede se recupere de falhas prontamente, eles são propostos para utilização em redes Ethernet, o que representa um cenário bastante distinto daquele encontrado nas IMAs que utilizam RMSF. Dessa forma, apesar de relacionados a este trabalho no propósito, o PRP e o HSR não são soluções viáveis para tolerância a falhas na IMA.

Em uma IMA baseada em RMSF, a disponibilidade de DAPs redundantes alcançáveis pelos medidores é muito importante para que a rede possa se recuperar de falhas. Essa disponibilidade depende fortemente da estratégia adotada para o posicionamento de DAPs e medidores inteligentes durante a implantação da rede. Nesse sentido, Rolim et al. propõem em [47] um modelo capaz de realizar o posicionamento de DAPs na IMA de forma que cada medidor seja coberto por ao menos um DAP, ao mesmo tempo em que minimiza o número total de DAPs na rede. A proposta reduz o problema de posicionamento de DAPs ao conhecido problema *Set Covering Problem*, que é NP-Completo. Os autores estabelecem que DAPs são sempre instalados em postes das companhias de energia e a qualidade de enlaces entre os medidores e os DAPs são estimadas utilizando o *Successful Delivery Rate* - SDR, que por sua vez foi calculado com base no modelo de propagação *Extended Hata SRD*. No trabalho, somente enlaces com SDR superior a 90% foram considerados pelo modelo. Os autores argumentam que esse valor pode ser reduzido, por exemplo, o que aumentaria o raio de cobertura dos DAPs, reduzindo a quantidade necessária desses equipamentos. Por outro lado, isso acarretaria em enlaces muito ruins entre medidores e DAPs e, possivelmente até impedindo a comunicação entre os dispositivos.

Para resolver o SCP associado ao problema de posicionamento de DAPs, os autores propõem uma heuristica baseada na abordagem dividir para conquistar. Quando o ta-

manho da instância (número de postes e medidores) é médio (no trabalho foi utilizado um total de 9997 medidores e 750 postes), é possível utilizar *sovers* para encontrar a solução ótima do problema em um tempo bastante razoável (com a instância utilizada no trabalho, o tempo para a solução foi de 31,56s. Entretanto, para instâncias muito grandes, os autores relatam problemas de estouro de memória, não sendo possível, portanto, encontrar a solução.

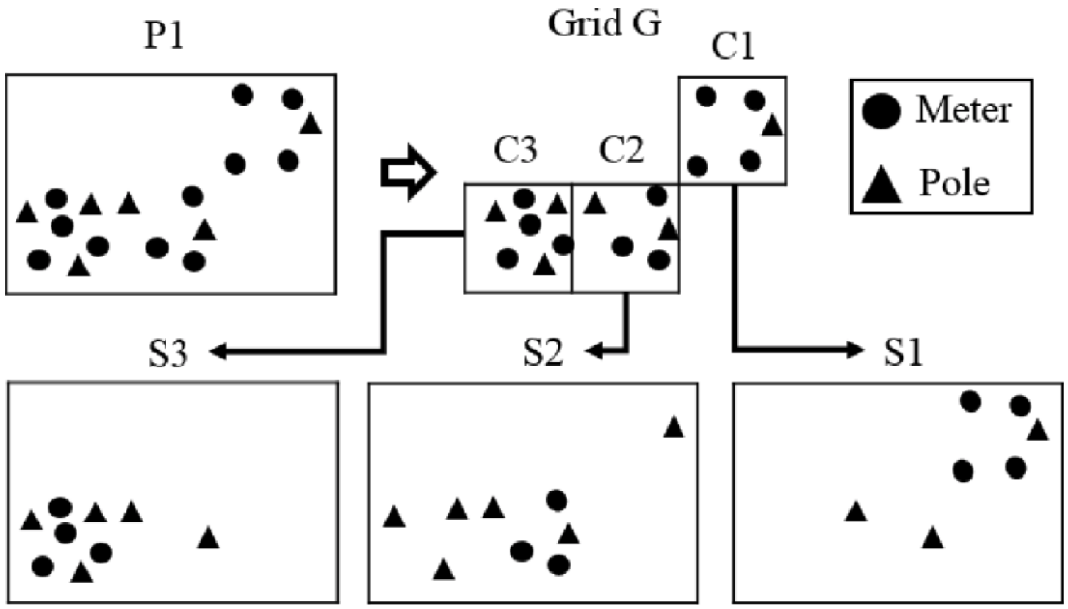


Figura 2.5: Divisão do problema SCP inicial em subproblemas [47].

A primeira parte para a solução do problema consiste em dividir a instância inicial formando uma matriz. Cada célula da matriz mais os postes das células vizinhas formam um subproblema a ser resolvido pelo *sover*. Na figura, as células C1, C2 e C3 formaram os subproblemas S1, S2 e S3, respectivamente. A composição das soluções dos subproblemas S1, S2 e S3 forma a solução do problema inicial P1. Entretanto, a solução ótima para um subproblema não faz parte, necessariamente, da solução ótima do problema inicial. Por essa razão, a solução encontrada passa ainda por um processo de pós-processamento, onde se tenta encontrar posições de postes capazes de substituir dois ou mais DAPs. Como resultado, os autores concluem que a utilização da heurística proposta reduz os requisitos de memória e processamento em relação a utilização de *sovers* para resolver o problema com um todo. Entretanto, a qualidade da solução final depende do tamanho das células geradas pela heurística. Quanto maior o tamanho das células, mais próxima do ótima a solução fica, mas também crescem o tempo de processamento e a utilização de memória. Por fim, os autores também apresentam em [46] uma extensão do trabalho, onde uma redundância mínima é adicionada ao problema, permitindo gerar IMAs mais tolerantes à

falhas.

Outra estratégia para buscar tolerância à falhas em uma IMA é a utilização de protocolos de roteamento multicaminho para redes em malha sem fio. Diversos protocolos com esse objetivo podem ser encontrados na literatura, incluindo [65, 23, 64, 8, 36, 37]. Em linhas gerais, o objetivo desses protocolos é encontrar dois ou mais caminhos, disjuntos ou não, entre uma origem e todos os outros nós da rede. Entretanto, no contexto de uma IMA a origem dos dados é, geralmente, um medidor inteligente na rede sem fio, enquanto que o destino é um nó em uma rede externa, que neste trabalho chamamos de central de controle. Uma vez que a origem dos dados e o destino estão em redes diferentes (tipicamente com tecnologias diferentes), os protocolos de roteamento não são capazes de encontrar múltiplos caminhos entre esses dois nós. Para lidar com esse problema, os autores propõem uma heurística que divide uma instância grande em instâncias menores. Cada histância menor é então aplicada ao *sover*, gerando um conjunto de soluções intermediárias. A composição das soluções intermediárias formam então a solução do problema original. A Figura 2.5 ilustra esse processo.

Por outro lado, os protocolos de roteamento MMESH [37] e ASMRP [36] utilizam uma estratégia diferente. Eles constroem múltiplos caminhos, mas somente entre os nós da rede e os *gateways*, o que representa uma estratégia mais adequada no contexto de uma IMA. Infelizmente, esses algoritmos foram desenvolvidos com o objetivo de reduzir o tráfego em um único caminho e não distribuir o tráfego através dos *gateways*, o que seria mais indicado para aumentar a resiliência da rede. Diferentemente das propostas MMESH e ASMRP que encontram múltiplos caminhos para um mesmo *gateway*, o 2CPR [8] encontra sempre dois caminhos, um para cada *gateway*, onde ambos podem ser utilizados simultaneamente com interferência reduzida.

Por fim, o DDSA, proposto em [41], segue uma estratégia diferente e funciona como um complemento do protocolo de roteamento tradicional (aquele que sempre utiliza um único caminho para enviar dados). O DDSA em um medidor mantêm uma lista de DAPs alcançáveis e quando uma mensagem precisa ser enviada por um medidor, ele seleciona um desses DAPs para encaminhá-la para a central de controle, de acordo com a probabilidade de seleção de cada um. Para aumentar a utilização de múltiplos DAPs por cada mensagem e aumentar a confiabilidade da entrega, o DDSA realiza retransmissões proativas. O DDSA é explicado mais detalhadamente na Seção 4.

Capítulo 3

THOR: Um Framework Para IMA com Tolerância a Falha de DAPs

Um dos grandes benefícios da implementação da IMA sob a forma de uma Rede em Malha Sem Fio é a possibilidade que um medidor tem de alcançar DAPs através de múltiplos saltos. Essa característica permite que cada medidor possa estar associado a um conjunto de DAPs sem que isso implique em um aumento de custo da rede. Nesse sentido, o objetivo do *framework* THOR é estruturar técnicas que visem aproveitar a disponibilidade de DAPs redundantes na IMA para mitigar os problemas decorrentes de falhas desses equipamentos.

3.1 Pré-requisito: IMA Projetada com DAPs Redundantes

É importante ressaltar que todos os benefícios trazidos pelo *framework* THOR e suas implementações dependem da disponibilidade de DAPs redundantes na IMA. Sendo assim, o projeto adequado da IMA é extremamente importante para garantir resiliência à falha de DAPs. Nesse contexto, Rolim et al. propõem em [47] uma ferramenta que realiza o planejamento de uma IMA com base na localização dos medidores e o grau de redundância pretendido. A ferramenta tem o objetivo de garantir os parâmetros especificados enquanto minimiza o número de DAPs necessários na rede.

3.2 Estrutura do Framework

O *framework* THOR, projetado para operar entre as camadas de transporte e rede nos medidores inteligentes, segue o paradigma Orientado à Objetos e é composto por uma classe concreta, duas classes abstratas e três interfaces, conforme ilustrado na Figura 3.1. A classe concreta Dap é utilizada para agregar informações úteis sobres os DAPs, as quais são manipuladas pelos demais componentes do *framework*. Cada implementação pode estender a classe Dap com o objetivo de incorporar novas informações úteis, mas no mínimo é necessário saber o endereço IP do DAP e se o DAP é ou não elegível para o envio de mensagens. As demais classes que compõem o *framework* são descritas nas subseções a seguir.

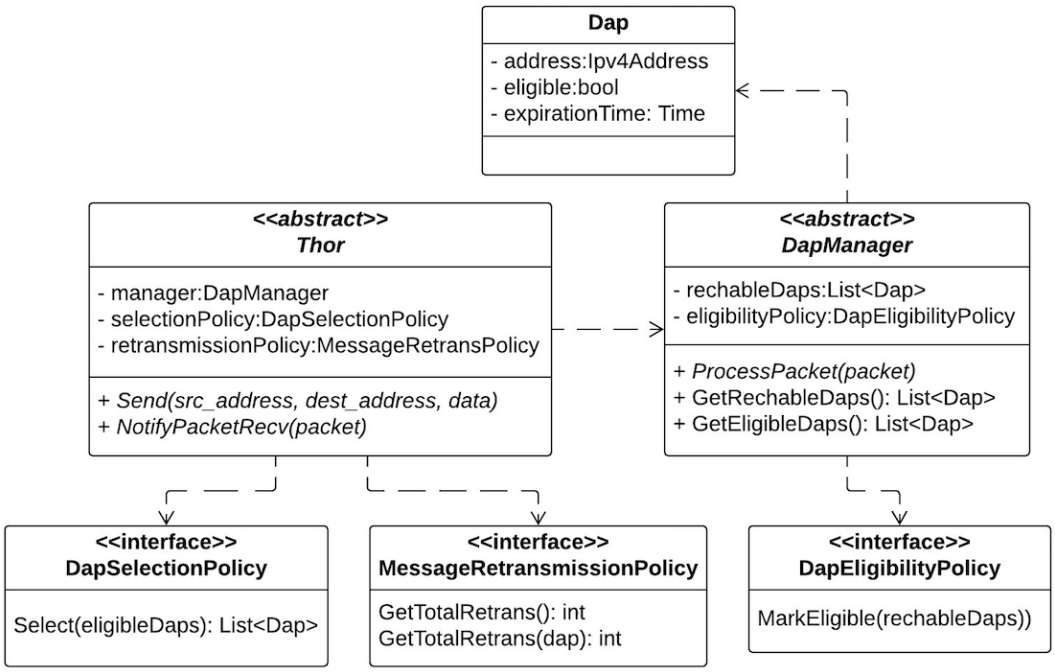


Figura 3.1: Estrutura do *framework* THOR.

3.2.1 Descoberta e Manutenção de DAPs com a Classe DapManager

No contexto do *framework* THOR, cada medidor deve manter uma lista de DAPs alcançáveis (aqueles com os quais o medidor consiga se comunicar através de um ou mais saltos). Essa lista pode ser pré-carregada de forma estática, mas devido às condições variáveis dos canais sem fio, é mais interessante permitir que ela seja construída dinamicamente. Essa é precisamente a função da classe abstrata DapManager, que consiste nas seguintes tarefas:

1. Descoberta e atualização de DAPs alcançáveis;

2. Exclusão de DAPs que deixaram de ser alcançáveis.

O processo de descoberta e atualização de DAPs alcançáveis no *framework* THOR ocorre de forma passiva e pró-ativa. Ou seja, o framework supõe a existência de um protocolo onde cada DAP anuncia a si mesmo na rede através de uma mensagem de *DAP_HELLO*. Toda vez que a camada de rede em um medidor inteligente recebe um novo pacote, esta deve notificar a classe DapManager através de uma chamada ao método ProcessPacket. Por sua vez, o método ProcessPacket verifica se o pacote recebido corresponde a uma mensagem DAP_HELLO, descartando o pacote e retornando caso contrário. Caso o pacote corresponda a uma mensagem DAP_HELLO, o método ProcessPacket cria uma instância da classe Dap (ou de uma classe filha da classe DAP) contendo o endereço IP de origem do pacote e possíveis informações adicionais trazidas junto à mensagem DAP_HELLO. Adicionalmente, o método ProcessPacket também ajusta o tempo de expiração (*expirationTime*) da instância para um valor apropriado. Se já houver uma entrada na lista de DAPs alcançáveis (*reachableDaps*) com o mesmo endereço IP que a instância recém criada, esta entrada é atualizada. Caso contrário, a instância recém criada é adicionada à lista.

Por outro lado, o processo de exclusão de DAPs que deixaram de ser alcançáveis ocorre por meio de temporizadores e do tempo de expiração das entradas da lista de DAPs alcançáveis. Quando um medidor permanece sem receber mensagens DAP_HELLO de um DAP alcançável por um tempo considerável, o tempo de expiração da entrada correspondente a este DAP na lista de DAPs alcançáveis será atingido, o que resultará na sua exclusão. Nesse ponto, o DAP será então considerado não alcançável. Os processos de Descoberta e atualização de DAPs alcançáveis e de Exclusão de DAPs que deixaram de ser alcançáveis são ilustrados na Figura 3.2.

É importante observar que, sendo o THOR um *framework*, não é sua função estabelecer parâmetros de implementação, como o formato real das mensagens de *DAP_HELLO* ou o tempo de expiração das entradas da lista de DAPs alcançáveis. Na verdade, o *framework* sequer requer que o protocolo de Descoberta e Manutenção de DAPs seja especialmente projetado para essa finalidade, sendo possível utilizar qualquer protocolo que tenha uma semântica compatível com aquela estabelecida pelo THOR. Como será explicado no Capítulo 4, a implementação da classe DapManager realizada neste trabalho utiliza mensagens *Host and Network Association*-HNA, definidas na RFC 3626 [9], como mensagens de *DAP_HELLO* para a descoberta e manutenção de DAPS.

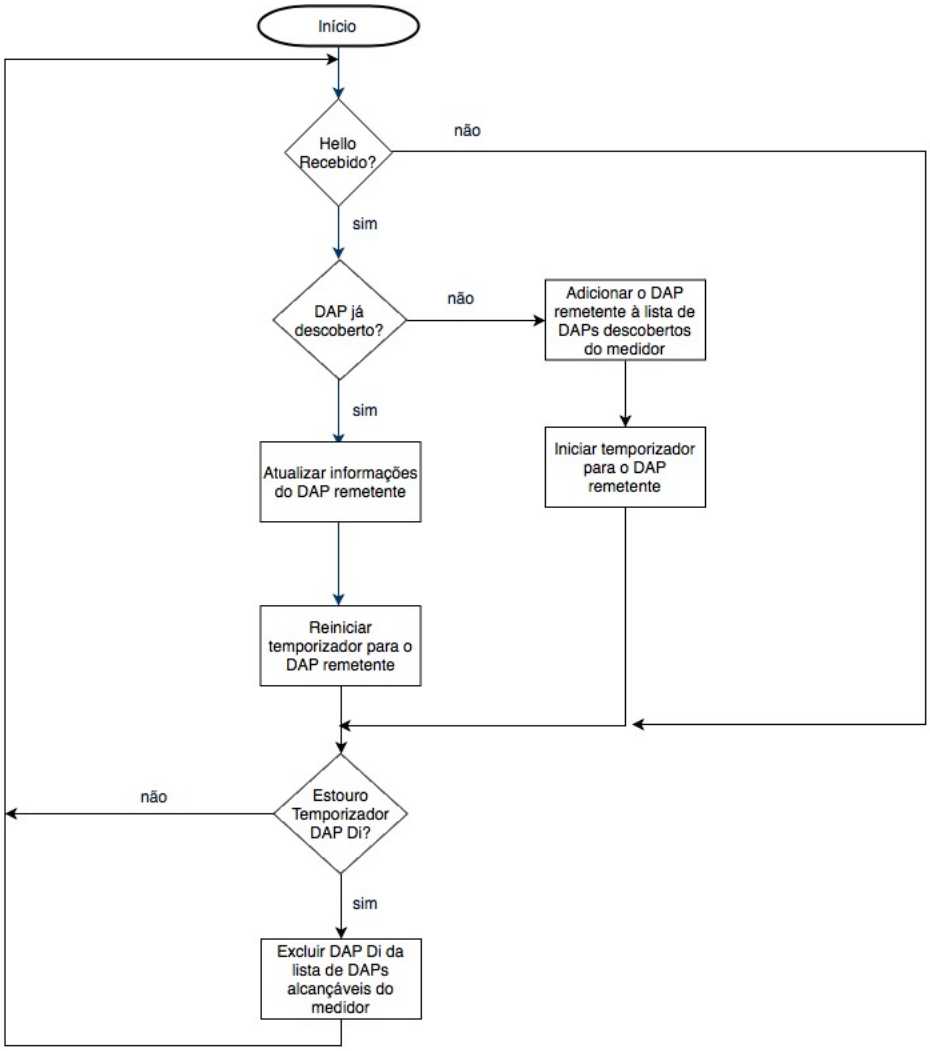


Figura 3.2: Fluxograma que ilustra o funcionamento do módulo de Descoberta e Manutenção de DAPs.

Apesar de algumas informações sobre o DAP poderem ser enviadas ao medidor através das mensagens de *DAP_HELLO*, outras precisam ser obtidas sob o ponto de vista do medidor e, portanto, devem ser acessadas através de interações entre o *framework* THOR e outros protocolos e serviços presentes no medidor. Por exemplo, pode ser interessante classificar os DAPs descobertos de acordo com o custo do melhor caminho em relação ao medidor. Nesse caso, é importante que o protocolo de roteamento forneça meios para que o THOR obtenha essa informação. Além disso, quando a tabela de roteamento é recalculada, o custo dos caminhos para cada DAP pode ser alterado, sendo necessário, portanto, que o THOR seja notificado sobre esse evento. Para maiores detalhes sobre a implementação do *framework* THOR, consulte o Capítulo 4.

3.2.2 Política de Elegibilidade de DAPs com a Interface DapEligibilityPolicy

Ao analisar a Figura 3.1 é possível notar que a classe DapManager possui um componente do tipo DapEligibilityPolicy, sobre o qual nada foi dito até este momento. Ocorre que a classe DapManager é responsável por construir a lista de DAPs alcançáveis, mas em alguns casos, nem todos os DAPs alcançáveis devem ser elegíveis para encaminhar as mensagens enviadas pelo medidor até a Central de Controle. Por exemplo, alguns DAPs podem ser alcançáveis, mas o melhor caminho até eles pode possuir um custo muito alto e, consequentemente, eles não deverão ser utilizados. Sendo assim, o que define se um DAP é ou não elegível é a Política de Elegibilidade, definida como uma implementação da interface DapEligibilityPolicy.

Quando um novo DAP é descoberto ou quando suas informações são atualizadas, a classe DapManager chama o método MarkEligible em sua instância *eligibilityPolicy*. Este método, por sua vez, verifica, para cada entrada na lista de DAPs alcançáveis, se o DAP alcançável deve ou não ser considerado elegível, definindo sua propriedade *eligible* apropriadamente.

3.2.3 Política de Seleção de DAPs com a Interface DapSelectionPolicy

Sem o *framework* THOR, uma vez que o endereço IP de destino das mensagens é o da Central de Controle, o DAP utilizado para encaminhar as mensagens é aquele contido no caminho de menor custo até a Central de Controle. Como visto no Capítulo 1, esse comportamento pode apresentar problemas caso este DAP apresente falhas. Uma vez que o medidor já conhece sua lista de DAPs alcançáveis, ele pode utilizá-la para escolher um ou mais DAPs através dos quais suas mensagens serão encaminhadas à Central de Controle. Dessa forma, quando um DAP falha, a mensagem ainda poderá ser entregue ao MDMS através de outro DAP. Apesar de aparentemente simples, existem diversas possibilidades de políticas para a seleção de DAPs e, como será visto no Capítulo 5, a escolha por um deles traz impactos consideráveis no desempenho da IMA. A interface DapSelectionPolicy provê o método Select que recebe como parâmetro a lista de DAPs elegíveis e retorna uma lista de DAPs selecionados para encaminhar a mensagem até a Central de Controle.

É importante notar que o destino final das mensagens ainda é a Central de Controle e não o DAP. Consequentemente, para permitir que a mensagem seja enviada primeiramente

aos DAPs selecionados e em seguida até a Central de Controle, é necessário implementar um túnel IP sobre IP, onde um pacote IP contendo o endereço da Central de Controle com endereço de destino é encapsulado em outro pacote IP onde o endereço de destino é o do DAP selecionado. Os medidores irão então utilizar o cabeçalho IP mais externo para encaminhar a mensagem até o DAP selecionado que, por sua vez, usará o cabeçalho IP mais interno para encaminhar a mensagem até a Central de Controle.

3.2.4 Política de Retransmissão de Mensagens com a Interface MessageRetransmissionPolicy

Quando a camada de aplicação em um medidor gera uma mensagem, ela pode fazer uso dos protocolos TCP e UDP para realizar a entrega da mesma até o destino pretendido. A escolha pelo TCP traz a garantia de entrega, o que é importante para diversas aplicações da IMA. Entretanto, o TCP também traz consigo mecanismos de controle de fluxo e de congestionamento que podem aumentar de forma significativa a latência na entrega das mensagens. Por outro lado, se o protocolo UDP for escolhido, nenhuma garantia de entrega é estabelecida. Uma vez que em meios sem fio perdas são comuns, o *framework* THOR faz uso de retransmissões proativas, assim como em protocolos como GOOSE, PRP e HSR [39, 5], onde para cada mensagem gerada pela camada de aplicação, são transmitidas n cópias.

A utilização de retransmissões proativas traz ainda um benefício secundário importante caso a Política de Seleção de DAPs implementada seja probabilística. Como nesse caso a seleção dos DAPs é feita a cada transmissão, duas cópias da mesma mensagem podem seguir em direção à DAPs diferentes para serem encaminhadas até a Central de Controle. Dessa forma, se um desses DAPs falha, a outra cópia ainda pode ser recebida corretamente no destino. Sem as retransmissões proativas, cada mensagem é encaminhada por apenas um DAP (só existe uma cópia de cada mensagem). Em caso de falha do DAP, a mensagem será perdida.

A interface MessageRetransmissionPolicy é utilizada pelo *framework* THOR para permitir diferentes implementações para o cálculo do número de cópias que devem ser enviadas para cada mensagem. Existem duas possibilidades de cálculo. No primeiro caso, o método GetTotalRetrans é chamado e calcula o número total de cópias com base na rede como um todo e de acordo com a política implementado. No segundo caso, o método GetTotalRetrans(dap) é chamado e calcula o número total de cópias com base na qualidade do caminho até um DAP específico, passado como parâmetro.

3.2.5 A classe Thor

A classe Thor representa a coluna dorsal do *framework*, conectando os demais componentes e interagindo com as camadas superiores e inferiores, conforme ilustrado na Figura 3.3. Quando um medidor precisa enviar uma mensagem para a Central de Controle, a camada de transporte deve entregar o segmento, juntamente com o endereço de destino, para o *framework* THOR através de uma chamada ao método Send da classe Thor. O método Send deve então utilizar as propriedades selectionPolicy e retransmissionPolicy, que representam, respectivamente, implementações das interfaces DapSelectionPolicy e MessageRetransmissionPolicy, para selecionar um ou mais DAPs que encaminharão a mensagem até a Central de Controle e enviar uma ou mais cópias da mensagem até esses DAPs.

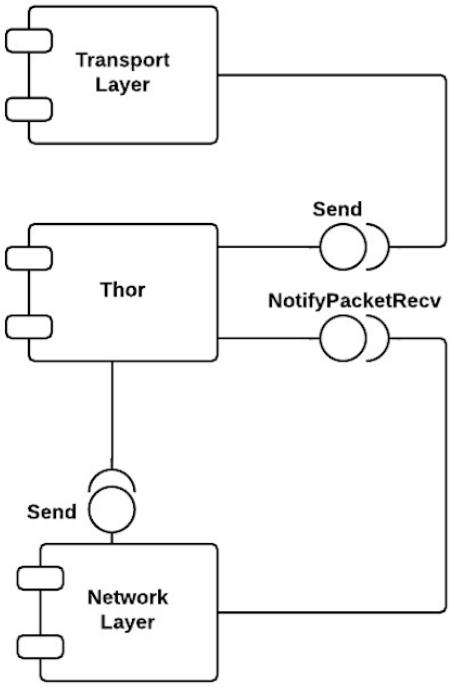


Figura 3.3: Interação do *framework* THOR com as camadas inferiores e superiores.

3.3 Conclusão do Capítulo

Este capítulo apresentou o THOR, um *framework* que objetiva auxiliar o processo de desenvolvimento de estratégias que aproveitem a existência de DAPs redundantes na IMA para permitir que mensagens enviadas pelos medidores sejam recebidas pela Central de Controle mesmo na presença de falhas de DAPs. Como visto, o *framework* é baseado no paradigma de orientação a objetos e possui uma classe concreta, duas classes abstratas

e três interfaces que representam seus quatro módulos principais: um protocolo para Descoberta e Manutenção de DAPs, uma Política de Seleção de DAPs, uma Política de Retransmissão de Mensagens e uma Política de Elegibilidade de DAPs. Existem diversas possibilidades de implementação para cada um desses componentes e no Capítulo 4 serão discutidas algumas delas.

Capítulo 4

Propostas Baseadas no Framework THOR

O *framework* THOR, apresentado no Capítulo 3, serve como base para o desenvolvimento de propostas que visem utilizar a disponibilidade de múltiplos DAPs alcançáveis na IMA para aumentar a robustez da rede contra falhas nesses equipamentos. Neste capítulo, são apresentadas algumas dessas propostas.

4.1 Descoberta e Manutenção de DAPs

Diferentemente da Política de Seleção de DAPs, da Política de Retransmissão de Mensagens e da Política de Elegibilidade de DAPs, que tem diferentes implementações para as diferentes propostas apresentadas, o processo de Descoberta e Manutenção de DAPs apresentado neste trabalho é comum para todas as propostas.

Ao invés de desenvolver um protocolo sob medida para a descoberta e manutenção de DAPs, neste trabalho foi utilizado o próprio protocolo de roteamento para esse fim. Para compreender como isso funciona, é preciso notar que uma IMA baseada em uma Rede em Malha Sem Fio (RMSF) é conectada à Central de Controle através de uma rede infraestruturada, sendo o DAP o responsável por fazer a comunicação entre essas duas tecnologias, como mostrado na Figura 1.6. Para que um medidor possa enviar mensagens para a Central de Controle, o protocolo de roteamento utilizado na RMSF precisa ser capaz de anunciar rotas para a rede infraestruturada dentro da rede sem fio, em um processo conhecido como Redistribuição de Rotas. O mesmo acontece com as rotas da rede sem fio, que devem ser anunciadas na rede infraestruturada.

Neste trabalho, foi utilizado o Optimized Link State Routing Protocol (OLSR) [26, 9], um protocolo de roteamento de estado de enlace que troca mensagens de `HELLO` e `TC` para

construir sua tabela de topologia e, consequentemente, de roteamento. Entretanto, as implementações realizadas neste trabalho não foram feitas em equipamentos reais, mas sim no simulador NS3, o qual é comumente adotado pela comunidade científica. Originalmente, apenas a primeira versão do protocolo OLSR estava disponível no simulador, o que permitia apenas a utilização da métrica *hop count*. Essa limitação não é interessante em uma RMSF devido à constante variação na qualidade dos enlaces sem fio, sendo, portanto, necessário utilizar uma métrica de roteamento que considere essa característica. Para contornar esse problema, foram realizadas adaptações no protocolo OLSR original, de forma a permitir que esse protocolo interaja com métricas cientes de qualidade.

Uma funcionalidade opcional do protocolo OLSR é a utilização de mensagens de *Host and Network Association* (HNA) para comunicar aos nós internos à RMSF sobre a existência de redes externas, que não implementam o protocolo OLSR. A Figura 4.1 mostra o formato de uma mensagem HNA, que deve estar contida no campo de dados de um pacote geral do OLSR. É possível notar que uma mensagem HNA representa uma lista de tuplas, cada uma com um campo para o endereço de rede e outro para a máscara de sub-rede das redes anunciadas.

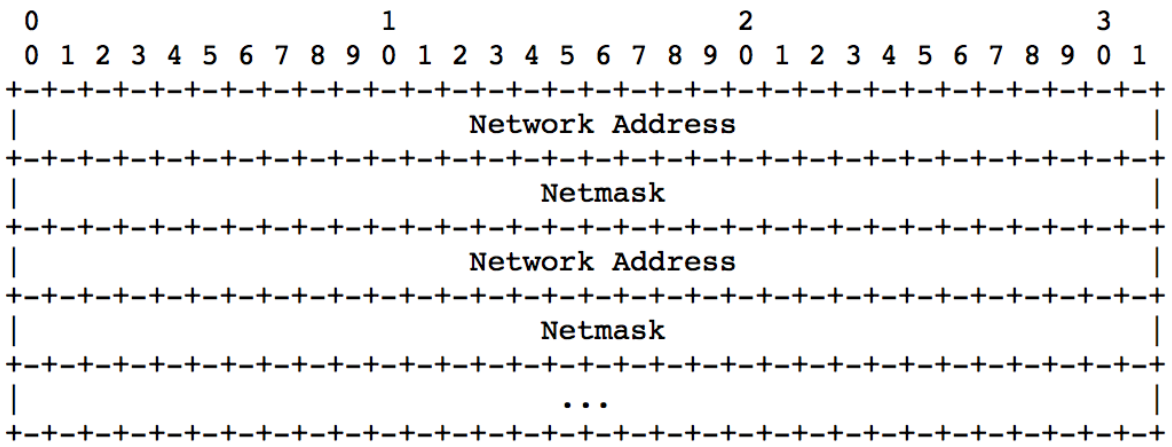


Figura 4.1: Formato de uma mensagem HNA (Retirado de [9]).

Mensagens HNA são criadas com o campo TTL definido como 255, o que significa que elas devem ser reencaminhadas através de múltiplos saltos na rede. Quando um nó recebe uma mensagem HNA, ele deve extrair o endereço do originador (*gateway*) contido no campo *Originator Address* do pacote geral do OLSR e armazenar, em uma lista de associações, que a rede anunciada através da mensagem HNA pode ser alcançada através do seu originador. Uma vez que vários nós podem anunciar a mesma rede externa, o protocolo em cada nó precisa decidir qual deles compõe o caminho de menor custo (do ponto de vista da rede sem fio) até a rede anunciada. Dessa forma, uma segunda tabela

de roteamento é computada especificamente para redes externas ao OLSR.

Quando um nó precisa enviar uma mensagem para uma rede externa à rede sem fio, o protocolo OLSR primeiro verifica a tabela de roteamento HNA, encontrando o *gateway* g_i para o qual a mensagem deve ser encaminhada. Em seguida, o protocolo consulta a tabela de roteamento original para verificar quem é o próximo salto no melhor caminho até o *gateway* g_i. Esse processo é repetido em cada nó no caminho, até que a mensagem chegue a um *gateway* e, consequentemente, seja encaminhada até a rede externa.

No caso de uma IMA, temos que os *gateways* são os DAPs e os demais nós da rede sem fio são medidores. Sendo assim, somente DAPs podem gerar mensagens HNA, o que significa que quando um medidor recebe uma mensagem HNA ele pode inferir que ela foi enviada por um DAP. Essa abordagem para descoberta de DAPs traz uma vulnerabilidade intrínseca, já que, a princípio, qualquer nó poderia se passar por um DAP na rede. Esse problema pode se agravar se o medidor confiar que a rede anunciada através de uma mensagem HNA é, de fato, a rede real conectada à Central de Controle. Para mitigar esse problema, poderíamos recorrer a um processo de autenticação utilizando, por exemplo, certificados digitais. Entretanto, neste trabalho essa estratégia não foi adotada, sendo proposta como trabalho futuro no Capítulo 6. Mesmo sem mecanismos de autenticação, é possível reduzir os efeitos de um ataque de um DAP falso evitando confiar nos endereços de rede anunciados através das mensagens de HNA. Para tanto, o endereço da Central de Controle pode ser pré-instalado em cada medidor. Quando uma mensagem HNA é recebida, o medidor verifica se o endereço da Central de Controle faz parte da rede anunciada, descartando a mensagem em caso negativo.

Uma vez que o módulo de Descoberta e Manutenção de DAPs - DMD depende de mensagens geradas e processadas pelo protocolo de roteamento, tal módulo foi implementado como uma extensão deste. Sendo assim, toda vez que o protocolo de roteamento recebe e identifica uma mensagem HNA, o controle é passado para o DMD, que identifica o originador da mensagem e o adiciona como um DAP à lista de DAPs alcançáveis (se já não tiver feito isso), retornando o controle para o protocolo de roteamento em seguida. Cada DAP alcançável possui um conjunto de informações associadas que são especificadas pelas diferentes implementações da Política de Seleção de DAPs, como o custo do melhor caminho até ele e sua probabilidade de seleção. Além disso, cada DAP também possui um tempo de expiração, após o qual é descartado da lista de DAPs alcançáveis. Sempre que o medidor recebe uma mensagem HNA cujo originador já fora adicionado à lista de DAPs alcançáveis, o tempo de expiração do DAP é reiniciado.

Note que, uma vez que mensagens HNA são utilizadas para a descoberta de DAPs, nenhuma informação adicional sobre eles (além do seu endereço) pode ser obtida através da recepção dessas mensagens. Ao invés disso, todas as informações necessárias sobre o DAP descoberto devem ser obtidas a partir de outros protocolos executados no medidor, como é o caso do protocolo de roteamento. Nesse sentido, sempre que a tabela de roteamento precisa ser recalculada, o controle é novamente passado para o DMD, que, por sua vez, atualiza o custo e outras informações sobre os DAPs alcançáveis.

Nas próximas seções serão apresentadas algumas propostas para os demais módulos do *framework* THOR. Todas essas propostas se apoiam no módulo de Descoberta e Manutenção de DAPs, descrito nesta seção, para a criação e gerenciamento da lista de DAPs alcançáveis.

4.2 Propostas Baseadas em Seleção Probabilística de DAPs

Uma maneira de implementar a Política de Seleção de DAPs do *framework* THOR, e portanto a interface DapSelectionPolicy, é fazer com que um único DAP seja selecionado pelo método Select de acordo com determinada probabilidade. Para tanto, é necessário implementar duas funcionalidades: uma para calcular e atribuir uma probabilidade de seleção a cada DAP na lista de DAPs elegíveis e outra para selecionar um DAP de acordo com sua probabilidade de seleção. A Figura 4.2 mostra a extensões necessárias aplicadas ao *framework* para permitir essas duas funcionalidades.

Como pode ser observado, a classe ProbabilisticDapSelPolicy implementa a interface DapSelectionPolicy e possui dois métodos. O método Select realiza a seleção probabilística de DAPs e o método DefineProbabilities calcula e atribui uma probabilidade de seleção a cada DAP elegível. Além disso, a classe ProbabilisticDap estende a classe DAP para incluir a propriedade selectionProbability, a qual é utilizada por ambos os métodos da classe ProbabilisticDapSelPolicy.

O algoritmo de cálculo e atribuição de probabilidades é particular de cada proposta e pode ser implementado de maneiras diferentes por cada uma delas, razão pela qual o método DefineProbabilities é definido como abstrato na classe ProbabilisticDapSelPolicy. Por outro lado, o Algoritmo 1, utilizado para realizar a seleção probabilística de DAPs, é comum a todas as propostas dessa categoria. É importante notar que o algoritmo utiliza a notação de ponto (*dot notation*) para representar um acesso a uma propriedade ou método

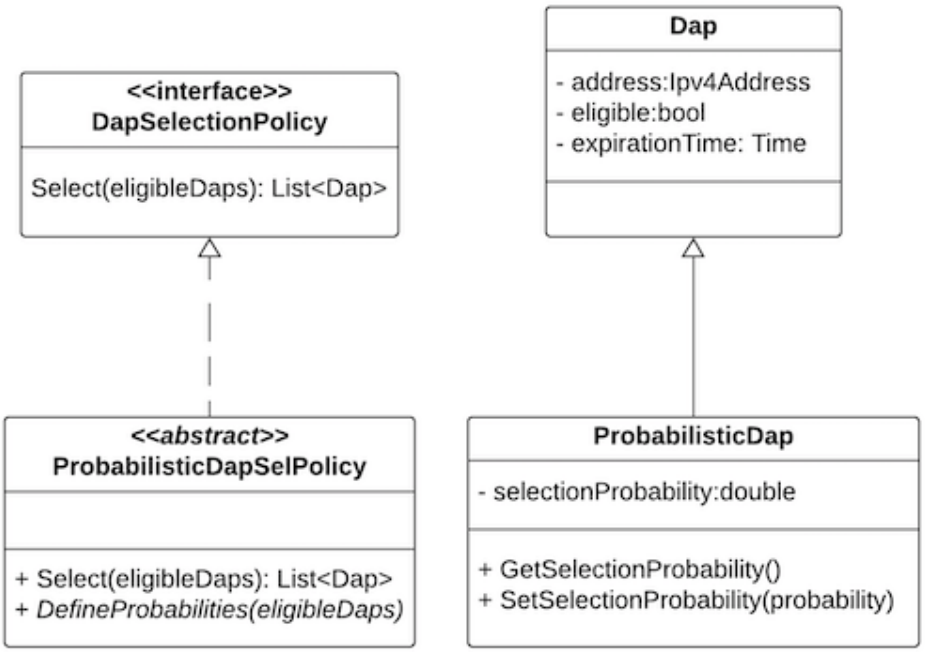


Figura 4.2: Componentes necessários para a implementação da seleção probabilistica de DAPs.

de uma entidade. Assim, na linha 4 do Algoritmo 1, o trecho $d_i.GetSelectionProbability()$ representa uma chamada ao método GetSelectionProbability na instância d_i da classe ProbabilisticDap, resultando no retorno do valor da probabilidade de seleção do DAP d_i. Além disso, apesar do algoritmo sempre selecionar apenas um DAP, uma vez que a assinatura do método Select requer o retorno de uma lista de DAPs, o algoritmo retorna uma lista de DAPs, mas sempre contendo apenas um elemento, como pode ser observado na linha 6 do Algoritmo 1.

Para que as propostas baseadas em seleção probabilística de DAPs possam aproveitar ao máximo a disponibilidade de múltiplos DAPs alcançáveis, é importante que o método Select seja chamado para cada cópia gerada pela Política de Retransmissão de Mensagens. Dessa forma, duas cópias podem ser enviadas a Central de Controle através de DAPs distindos, aumentando assim a resiliência a falhas nesses equipamentos. Por essa razão, todas as propostas baseadas em seleção probabilística de DAPs implementam o método Send da classe Thor seguindo as seguintes etapas:

1. Calcula o número de cópias com base na Política de Retransmissão de Mensagens;
2. Chama o método DefineProbabilities derivado da classe ProbabilisticDapSelPolicy para definir a probabilidade de seleção dos DAPs elegíveis;

Algoritmo 1: Método Select da classe ProbabilisticDapSelPolicy

input : Conjunto $D = \{d_1, d_2, ..., d_n\}$ de DAPs elegíveis (instâncias da classe ProbabilisticDap)
output: Conjunto de DAPs selecionados S contendo apenas um elemento.

```
1 rand ← GetRandom()
2 soma ← 0
3 foreach d_i ∈ D do
4 |   soma ← soma + d_i.GetSelectionProbability()
5 |   if soma ≥ rand then
6 |   |   S ← {d_i}
7 |   |   Break
8 |   end
9 end
```

3. Para cada cópia: seleciona probabilisticamente um dos DAPs elegíveis e envia a cópia através do DAP selecionado utilizando um tunel Ip sobre IP.

4.2.1 Uniform DAP Selection Algorithm - UDSA

Como visto na seção anterior, as propostas baseadas em seleção probabilística de DAPs precisam implementar um modelo de distribuição de probabilidades para o conjunto de DAPs elegíveis. O UDSA utiliza a abordagem mais simples, onde todos os DAPs recebem a mesma probabilidade de seleção $1/n$, onde n é o número de DAPs elegíveis. Para a implementação do UDSA foi criada uma classe que estende ProbabilisticDapSelPolicy, chamada UDSADapSelPolicy, uma classe que implementa a interface MessageRetransmissionPolicy, chamada StaticMessageRetransPolicy e uma classe que implementa a interface DapEligibilityPolicy, chamada NullEligibilityPolicy, conforme ilustrado na Figura 4.3.

As duas versões sobrecarregadas do método GetTotalRetrans da classe StaticMessageRetransPolicy possuem a mesma implementação e sempre retornam um valor k, que representa um parâmetro ajustável da proposta. Por outro lado, os métodos Select e DefineProbabilities dá classe UDSADapSelPolicy são implementados de acordo com os algoritmos 1 e 2, respectivamente. Uma vez que o UDSA não define nenhuma política específica para avaliar a elegibilidade de DAPs, o método MarkEligible da classe NullEligibilityPolicy simplesmente marca todos os DAPs alcançáveis como elegíveis.

Um ponto positivo do UDSA é a sua simplicidade de implementação. Todo o seu funcionamento depende apenas de informações disponibilizadas pelos componentes do

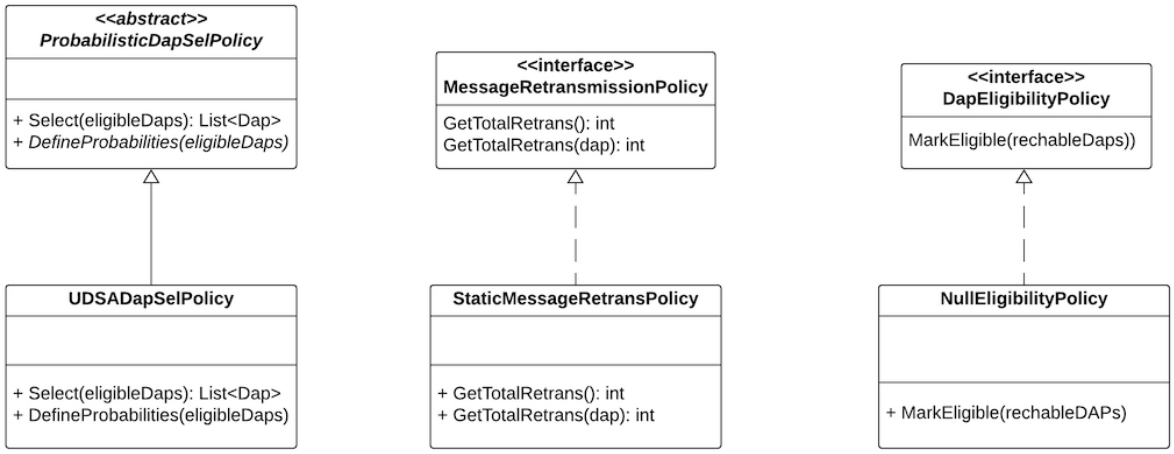


Figura 4.3: Componentes necessários para a implementação do UDSA

Algoritmo 2: Método DefineProbabilities da classe UDSADapSelPolicy

input : Conjunto $D = \{d_1, d_2, ..., d_n\}$ de DAPs elegíveis (instâncias da classe ProbabilisticDap)

1 **foreach** $d_i \in D$ **do**
2 $\quad selProb \leftarrow \frac{1}{n}$
3 $\quad d_i.SetSelectionProbability(selProb)$
4 **end**

framework e por um parâmetro ajustável k. Não há a necessidade de estabelecer interações entre o UDSA e outros serviços de rede, como o protocolo de roteamento. Por outro lado, o UDSA trata da mesma maneira DAPs com alta e baixa qualidades, o que leva a resultados menos eficientes, como será visto no Capítulo 5.

4.2.2 Dynamic DAP Selection Algorithm - DDSA v1

O DDSA, proposto em [41], chamado neste trabalho de DDSA v1, também seleciona um DAP probabilisticamente a partir da lista de DAPs elegíveis utilizando o Algoritmo 1. Assim como o UDSA, o DDSA v1 também utiliza uma Política de Retransmissão de Mensagens estática, baseada no parâmetro configurável k e implementada pela classe StaticMessageRetransPolicy.

Ao analisar a proposta do UDSA é possível notar um problema importante no Algoritmo 2: a probabilidade de seleção do DAP d_i, calculada no medidor m, não depende do custo do caminho entre m e d_i. Se consideramos que a métrica de roteamento utilizada reflete a probabilidade de entrega de um pacote, isso significa que um DAP cujo caminho tem baixa probabilidade de entrega seria escolhido com a mesma probabilidade de um

DAP cujo caminho tem alta probabilidade de entrega, o que poderia resultar em uma taxa de entrega de pacotes sub-ótima na IMA.

Para solucionar esse problema, O DDSA v1 utiliza um algoritmo que atribui probabilidades de seleção proporcionais a qualidade do caminho até determinado DAP. Além disso, para reduzir as chances de escolher um DAP com custo alto, o DDSA v1 também emprega uma Política de Exclusão de DAPs que torna inelegíveis aqueles DAPs cujo melhor caminho apresenta baixa qualidade (custo alto). A Figura 4.4 mostra as classes necessárias para a implementação dessas funcionalidades e as subseções seguintes explicam cada uma delas.

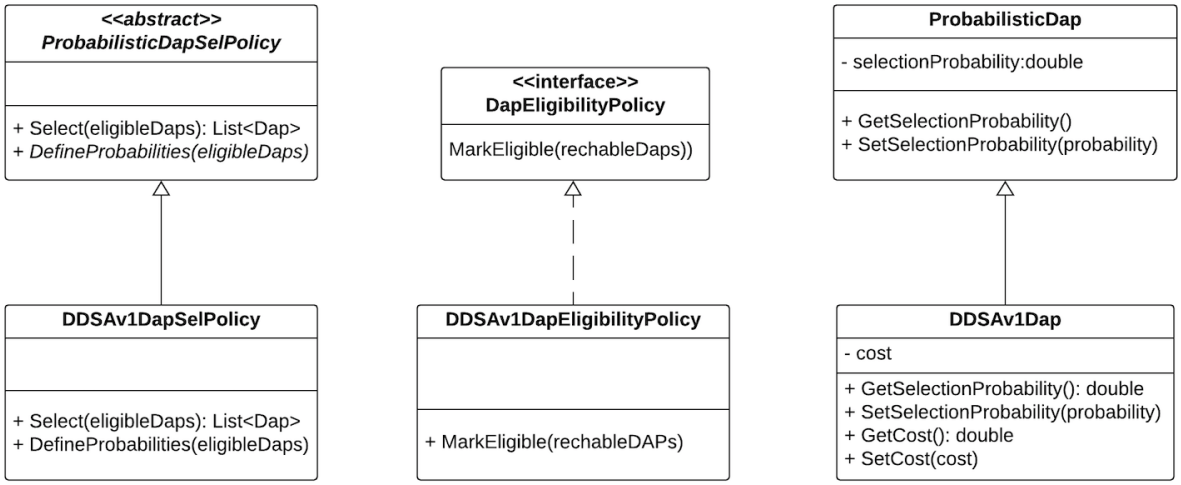


Figura 4.4: Componentes necessários para a implementação do DDSA v1

4.2.2.1 Cálculo das Probabilidades de Seleção

Para evitar os problemas decorrentes da maneira como o UDSA realiza o cálculo e atribuição de probabilidades aos DAPs elegíveis, o DDSA v1 realiza esse processo associando o cálculo da probabilidade de seleção de um DAP d_i em um medidor m ($P_m^{d_i}$) ao custo do melhor caminho entre esse medidor e o DAP, definido como $c(m, d_i)$. A necessidade de conhecer o custo do melhor caminho até cada DAP introduz uma nova complexidade à implementação da classe DapManager, que agora precisa interagir com o protocolo de roteamento para obter tal informação. Além disso, como pode ser observado na Figura 4.4, o DDSA v1 precisa estender a classe ProbabilisticDap, gerando a classe DDSAv1Dap, para incorporar a propriedade que guarda o custo dos DAPs.

Supondo que a classe DapManager foi capaz de obter o custo do melhor caminho entre o medidor e cada um dos DAPs elegíveis, o método DefineProbabilities da classe

DDSAv1DapSelPolicy pode fazer uso dessas informações para calcular as probabilidades de seleção. Entretanto, a maneira como esse cálculo é executado depende do tipo da métrica de roteamento utilizada. Para métricas que assumem valores maiores para representar enlaces de melhor qualidade, chamadas doravante de métricas de Tipo 1, a probabilidade de seleção pode ser calculada de acordo com a Equação 4.1.

$$P_m^{d_i} = \frac{c(m, d_i)}{\sum_{j=1}^{n} c(m, d_j)} \text{ onde } d_i,\, d_j \in D \tag{4.1}$$

Na equação, o custo do caminho de menor custo do medidor m até o DAP d_i é dividido pelo somatório dos custos dos caminhos de menor custo do medidor m até cada um dos DAPs elegíveis em m. Se, por outro lado, a métrica de roteamento utilizada assumir valores menores para enlaces de melhor qualidade, chamada doravante de métrica de Tipo 2, então a Equação 4.2 deve ser utilizada no lugar da Equação 4.1. Nesse caso, o inverso do custo do caminho de menor custo do medidor m até o DAP d_i é dividido pelo somatório do inverso dos custos dos caminhos de menor custo do medidor m até cada um dos DAPs elegíveis em m.

$$P_m^{d_i} = \frac{1/c(m, d_i)}{\sum_{j=1}^{n} 1/c(m, d_j)} \text{ onde } d_i,\, d_j \in D \tag{4.2}$$

Existem duas maneiras de implementar o processo de cálculo e atribuição de probabilidades. No primeiro caso, seria necessário ter duas classes derivadas de ProbabilisticDapSelPolicy, uma para cada tipo de métrica. Assim, ao configurar o *framework* THOR no medidor a classe correta deve ser escolhida para a métrica utilizada. A segunda possibilidade é utilizar uma única classe derivada de ProbabilisticDapSelPolicy, assim como mostrado na Figura 4.4, onde o método DefineProbabilities precisa interagir com o protocolo de roteamento para descobrir o tipo de métrica em utilização. Consequentemente, o método poderia escolher qual equação utilizar (4.1 ou 4.2) de acordo com a informação obtida.

O Algoritmo 3 utiliza a segunda possibilidade de implementação. Nas linhas 2 a 9, dependendo do tipo da métrica, o algoritmo acumula na variável $Soma\_Custo$ o somatório do custo do melhor caminho entre o medidor m e cada DAP d_i (métrica Tipo 1) ou o somatório do inverso do custo do melhor caminho entre o medidor m e cada DAP d_i (métrica Tipo 2). Note que novamente é utilizada a notação de ponto (*dot notation*) para

representar o acesso a um membro (método ou propriedade) da classe DDSAv1Dap. Em seguida, o algoritmo calcula a probabilidade de seleção utilizando a Equação 4.1 (linha 13) ou a Equação 4.2 (linha 16), dependendo do tipo da métrica de roteamento utilizado. Por fim, na linha 18, a probabilidade calculada é atribuída ao DAP.

Algoritmo 3: Método DefineProbabilities da classe DDSAv1DapSelPolicy

input : Conjunto $D = \{d_1, d_2, ..., d_n\}$ de DAPs elegíveis (instâncias da classe DDSAv1Dap)
Result: As probabilidades de seleção são calculadas e associadas a cada DAP elegível

```
1  Soma_Custo ← 0
2  foreach d_i ∈ D do
3  |  if Métrica Tipo 1 then
4  |  |  Soma_Custo ← Soma_Custo + d_i.GetCost()
5  |  end
6  |  else
7  |  |  Soma_Custo ← Soma_Custo + 1/d_i.GetCost()
8  |  end
9  end
10 foreach d_i ∈ D do
11 |  probability ← 0.0
12 |  if Métrica Tipo 1 then
13 |  |  probability ← d_i.GetCost()/Soma_Custo
14 |  end
15 |  else
16 |  |  probability ← 1/(d_i.GetCost() × Soma_Custo)
17 |  end
18 |  d_i.SetSelectionProbability(probability)
19 end
```

Uma vez que a probabilidade de seleção de um DAP depende do custo do caminho do medidor até cada um dos DAPs elegíveis, quando uma alteração de topologia que afete esses custos ocorre, todas as probabilidades de seleção precisariam ser recalculadas. Entretanto, dado que as probabilidades de seleção são sempre recalculadas quando uma nova mensagem é gerada pelo medidor, contanto que a classe DapManager mantenha os custos sempre atualizados, não há necessidade da classe DDSAv1DapSelPolicy ser notificada sobre alterações nos custos até os DAPs. Por fim, é importante observar que o bom funcionamento do DDSA v1 depende da utilização de uma métrica de roteamento que seja capaz de refletir com boa precisão a probabilidade do enlace sem fio entregar os

pacotes enviados.

4.2.2.2 Política de Elegibilidade de DAPs

Dado que no DDSA v1 a probabilidade de seleção de um DAP reflete o custo do melhor caminho do medidor até ele, é correto afirmar que DAPs com probabilidade de seleção baixa, se selecionados, irão influenciar negativamente na performance da IMA (baixa probabilidade de entrega, alta latência, etc). Para evitar esse tipo de problema, o DDSA v1 utiliza uma política de exclusão de DAPs, implementada na classe DDSAv1DapEligibilityPolicy, que torna inelegíveis aqueles DAPs que possuem menos do que uma fração α da maior probabilidade de seleção entre todos os DAPs. O Algoritmo 4 mostra como o método MarkEligible realiza essa tarefa.

Da linha 1 a linha 13, o algoritmo encontra o melhor DAP e o armazena na variável d_{best}. O significado de melhor DAP depende do tipo da métrica de roteamento. Para métricas do Tipo 1, o melhor DAP é aquele que apresenta o maior custo. Por outro lado, para métricas do Tipo 2, o melhor DAP é aquele que apresenta o menor custo. Nas linhas 14 a 19 é calculado o limiar γ como sendo o produto de *alpha* pelo custo de de d_{best}, no caso da métrica de roteamento ser do tipo 1 (linha 15), ou pelo inverso do custo de d_{best}, no caso da métrica ser do tipo 2 (linha 18). Note que *alpha* é uma propriedade da classe DDSAv1DapEligibilityPolicy e, portanto, é acessada diretamente no algoritmo. Nas linhas 20 a 37 o algoritmo marca todos os DAPs cujo custo (métrica do tipo 1) ou inverso do custo (métrica do tipo 2) é menor que γ como inelegíveis (linhas 23 e 31) ou, caso contrário, como elegíveis (linhas 26 e 34). Note que o método GetCost pertence à classe DDSAv1Dap e o método SetEligible foi herdado da classe DAP pela classe DDSAv1Dap.

O Algoritmo 4 sugere um funcionamento um pouco diferente para a Política de Eligibilidade de DAPs do que o originalmente proposto em [41]. O algoritmo original utiliza a probabilidade de seleção como parâmetro para definir o melhor DAP (aquele que tem a maior probabilidade), para calcular o limiar γ e para verificar se um DAP deve ou não ser elegível, comparando γ com a probabilidade de seleção de cada DAP alcançável. Essa abordagem gera alguns problemas:

1. Seria necessário calcular a probabilidade de seleção para cada DAP alcançável e não somente para os DAPs elegíveis, já que a verificação da elegibilidade dos DAPs depende da probabilidade de seleção dos mesmos;

2. Alterações no custo dos DAPs exigem uma nova verificação de elegibilidade, que

Algoritmo 4: Método MarkEligible da classe DDSAv1DapEligibilityPolicy

input : Conjunto $R = \{d_1, d_2, ..., d_n\}$ de DAPs alcançáveis (instâncias da classe DDSAv1Dap)

Result: Todos os DAPs alcançáveis são marcados como elegíveis ou inelegíveis

```
1  d_best ← d_1
2  foreach d_i ∈ R do
3      if Metrica Tipo 1 then
4          if d_i.GetCost() > d_best.GetCost() then
5              d_best ← d_i
6          end
7      end
8      else
9          if d_i.GetCost() < d_best.GetCost() then
10             d_best ← d_i
11         end
12     end
13 end
14 if Métrica Tipo 1 then
15     γ ← alpha × d_best.GetCost()
16 end
17 else
18     γ ← alpha × 1 / d_best.GetCost()
19 end
20 foreach d_i ∈ R do
21     if Métrica Tipo 1 then
22         if d_i.GetCost() < γ then
23             d_i.SetEligible(FALSE)
24         end
25         else
26             d_i.SetEligible(TRUE)
27         end
28     end
29     else
30         if 1 / d_i.GetCost() < γ then
31             d_i.SetEligible(FALSE)
32         end
33         else
34             d_i.SetEligible(TRUE)
35         end
36     end
37 end
```

so pode ser feita após o cálculo das probabilidades de seleção. Dessa forma, a politica de elegibilidade de DAPs passaria a depender da política de seleção de DAPs, dificultando a troca dessas políticas de forma independente.

Além de gerar problemas, fazer com que o Algoritmo de verificação de elegibilidade dependa das probabilidades de seleção é desnecessário. Para entender, suponha o limiar γ sela calculado como o produto de *alpha* pela probabilidade de seleção do melhor DAP, resultando em $\gamma = alpha \times d_{best}.GetSelectionProbability()$. Nesse caso, para saber se um DAP d_i é elegível, seria feita a seguinte comparação: $d_i.GetSelectionProbability \geq \gamma$. Supondo que a métrica de roteamento seja do Tipo 1, podemos substituir as chamadas a GetSelectionProbability pela maneira como as probabilidades são calculadas, resultando na seguinte inequação: $\frac{d_i.GetCost()}{\sum_{j=1}^{n} c(m,d_j)} \geq alpha \times \frac{d_{best}.GetCost()}{\sum_{j=1}^{n} c(m,d_j)}$. É simples notar que os denominadores dos dois lados da inequação são cancelados e a verificação de eligibilidade passa a depender somente do custo do melhor DAP e do custo de cada DAP sendo verificado, razão pela qual o Algoritmo 4 faz uso apenas dessas informações.

A utilização de uma Política de Elegibilidade de DAPs introduz um *trade-off* importante no DDSA v1 e nas demais propostas. Por um lado, tornar inelegível um DAP cujo caminho tem baixa qualidade pode melhorar o desempenho da IMA, pois evita que mensagens sejam enviadas por caminhos com baixa taxa de entrega ou com alta latência. Por outro lado, dependendo do valor escolhido para *alpha*, o Algoritmo 4 pode acabar eliminando toda redundância de DAPs. Essa é uma situação muito ruim, já que o as propostas baseadas no *framework* THOR dependem da existência de DAPs redundantes para se recuperar de falhas nesses equipamentos. Para evitar esse problema, na implementação do DDSA v1 realizada neste trabalho, um DAP só é definido como inelegível se isso não tornar a lista de DAPs elegíveis menor do que um valor mínimo configurável.

4.2.3 Dynamic DAP Selection Algorithm - DDSA v2

O DDSA v2 introduz uma proposta de melhoria da Política de Retransmissão de Mensagens do DDSA v1. Ao invés de utilizar um valor estático, definido empiricamente, para o número de retransmissões, como faz o DDSA v1, o DDSA v2 calcula esse valor dinamicamente, permitindo que o número de retransmissões se adapte às condições atuais da rede. O funcionamento dos demais componentes do DDSA v2 (Política de Seleção de DAPs, Cálculo da Probabilidade de Seleção e Política de Elegibilidade de DAPs) é análogo ao do DDSA v1. A Figura 4.5 mostra o novo componente introduzido pela implementação

do DDSA v2.

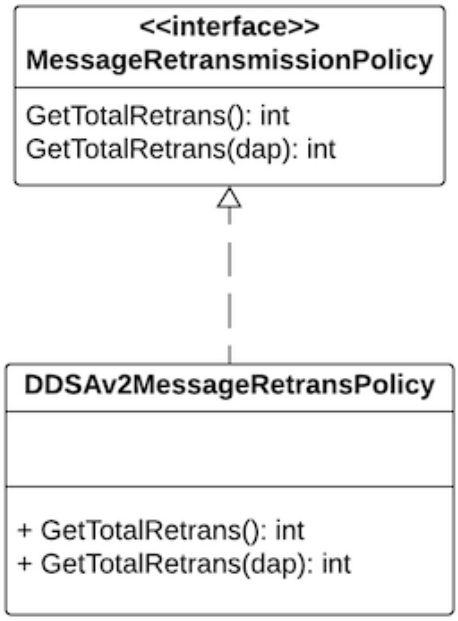


Figura 4.5: Componentes necessários para a implementação do DDSA v2.

Para compreender o funcionamento da Política de Retransmissão de Mensagens do DDSA v2, observe a Figura 4.6. Um medidor M precisa enviar uma mensagem para a Central de Controle e, para tanto, ele tem a possibilidade de selecionar tanto o DAP D1 quanto o DAP D2. Note que as linhas tracejadas representam os caminhos de menor custo entre o medidor M e os DAPs.

Suponha que a probabilidade da mensagem enviada pelo medidor M através de D1 ser efetivamente recebida por D1 é denotada por $P^{D1}_{sucesso}$. Da mesma forma, a probabilidade da mensagem enviada por M através de D2 ser efetivamente recebida por D2 é denotada por $P^{D2}_{sucesso}$. Suponha também que as probabilidades de D1 e de D2 serem selecionados pelo Algorítimo de Seleção de DAPs são denotadas por P^{D1}_{sel} e P^{D2}_{sel}, respectivamente.

Considere que, uma vez que a mensagem é recebida por D1 ou por D2, então a probabilidade dela ser entregue à Central de Controle é aproximadamente 1. A partir dessas considerações, podemos calcular a probabilidade de uma mensagem ser corretamente recebida pela Central de Controle quando apenas uma cópia é enviada (P^{C}_{rec}) através da Equação 4.3. Supondo que o medidor M possui uma lista de DAPs elegíveis com n DAPs, então a Equação 4.3 pode ser generalizada pela Equação 4.4

$$P^{C}_{rec} = P^{D1}_{sel} \cdot P^{D1}_{sucesso} + P^{D2}_{sel} \cdot P^{D2}_{sucesso} \tag{4.3}$$

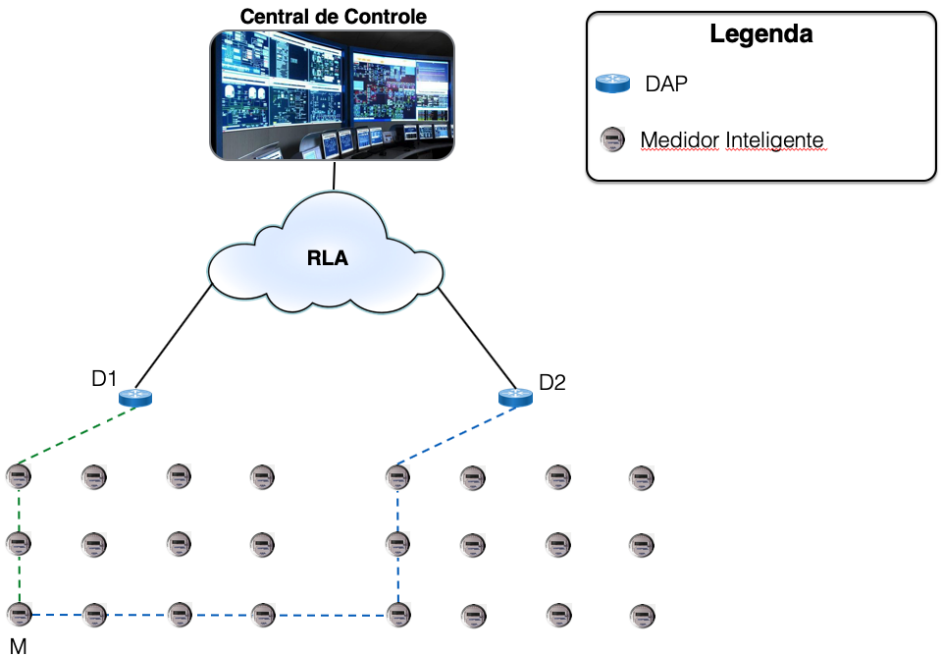


Figura 4.6: Exemplo de uma AMI, onde o medidor M quer enviar uma mensagem para a central de controle e pode fazê-lo através do DAP D1 ou do DAP D2.

$$P_{rec}^{C} = \sum_{i=1}^{k} P_{sel}^{Di} \cdot P_{sucesso}^{Di} \tag{4.4}$$

Agora, imagine que a Política de Retransmissão de Mensagens do DDSA v2 envie Y cópias da mensagem de forma pró-ativa. Nesse caso, basta que uma cópia chegue até a Central de Controle para que a mensagem seja considerada como recebida. Por outro lado, uma mensagem não é considerada como recebida se nenhuma de suas cópias chegar até a Central de Controle.

Sendo assim, suponha que A é o evento onde uma das Y cópias da mensagem, enviada por M, foi recebida com sucesso pela Central de Controle e B é o evento onde nenhuma das cópias da mensagem foi recebida pela Central de Controle. Nesse caso, temos que $P_r[A] = 1 - P_r[B] = 1 - (1 - P_{rec}^{C})^{Y}$ e, consequentemente, conseguimos chegar a Equação 4.5.

$$Y = \frac{\log(1 - P_r[A])}{\log(1 - P_{rec}^{C})} \tag{4.5}$$

Para calcular o valor de Y na Equação 4.5, precisamos, primeiramente, definir o valor desejado para $P_r[A]$. Apesar de querermos maximizar a probabilidade de entrega de mensagens, definir $P_r[A] = 1$ não irá funcionar, pois, nesse caso, P_{rec}^{C} também deverá ser igual a um, o que é pouco provável de acontecer devido a variabilidade das condições

da rede e a limitação de recursos financeiros para aquisição de novos DAPs. Mesmo que P_{rec}^{C} pudesse ser igual a um, a Equação 4.5 não faria sentido, já que, nesse caso, só precisaríamos enviar uma cópia da mensagem e teríamos a certeza da entrega. Ao invés disso, neste trabalho definiremos $P_r[A] = 0,99$, ou seja, queremos que uma mensagem enviada por um medidor chegue até a Central de Controle com 99% de probabilidade.

Além de definir o valor de $P_r[A]$, também precisamos calcular o valor de P_{rec}^{C} de acordo com a Equação 4.3. O valor da probabilidade de seleção de cada DAP é calculado segundo o Algoritmo 3, restando apenas definirmos uma maneira de calcular a probabilidade de entrega no caminho de menor custo entre o medidor M e cada DAP alcançável. Ao utilizar o *Expected Transmission Count* - ETX [11] como métrica de roteamento, nós já temos uma estimativa da probabilidade de entrega em um enlace, dada pelo inverso do valor da métrica nesse enlace. Na realidade, para conseguirmos uma estimativa real, precisamos também considerar as retransmissões realizadas pela camada de enlace no cálculo da probabilidade de entrega.

Seja $P_m^{Di} = \{E_1, E_2, ..., E_n\}$ um caminho entre o medidor M e um DAP Di qualquer, onde $E_i \in P_m^{di}$ representa um enlace nesse caminho. Suponha que A_i é o evento onde uma mensagem enviada através do enlace E_i é recebida corretamente do outro lado e B_i é o complemento de A_i. Considere também que a camada de enlace realize até W retransmissões do frame no enlace. Nesse caso, temos que $P_r[B_j] = (1 - \frac{1}{ETX_i})^W$ e, consequentemente, $P_r[A_i] = 1 - P_r[B_i] = 1 - (1 - \frac{1}{ETX_i})^W$, onde ETX_i é o valor da métrica no enlace E_i. Uma vez que já temos a probabilidade de entrega em um enlace, podemos calcular a probabilidade de entrega no caminho P_m^{di} fazendo o produtório de $P_r(A_i)$ para todo enlace E_i em P_m^{di}. Esse resultado é mostrado na Equação 4.6.

$$P_{sucesso}^{DAPi} = \prod_{i=1}^{n} \left[1 - \left(1 - \frac{1}{ETX_i} \right)^W \right] \tag{4.6}$$

Em suma, ambos os métodos GetTotalRetrans da classe DDSAv2MessageRetransPolicy aplicam as equações 4.4 e 4.6 à Equação 4.5, fazendo $P_r[A] = 0,99$, sendo assim capazes de calcular, de forma dinâmica e adaptativa, o número de retransmissões necessárias para que uma mensagem enviada pelo medidor M possa ser recebida pela Central de Controle com 99% de probabilidade.

Por fim, é importante observar que caso P_{rec}^{C} tenha um valor baixo, o número de retransmissões calculado pode se tornar muito alto. Nesse caso, o parâmetro α utilizado pelo Algoritmo 4 para realizar a exclusão de DAPs da lista de DAPs elegíveis deve ser ajustado

de forma a estabelecer uma boa relação entre o valor de P_{rec}^{C} e o nível de redundância de DAPs resultante. Uma outra estratégia seria reduzir o valor de $P_r[A]$ com o objetivo de estabelecer uma boa relação entre o número de retransmissões e a probabilidade de entrega das mensagens.

4.3 MultiDAP Selection Algorithm - MDSA

Ao analisar o funcionamento das propostas que utilizam seleção probabilística de DAPs, onde a probabilidade de seleção é proporcional à qualidade do enlace, é possível notar que os DAPs cujo caminho apresentam os menores custos são aqueles selecionados mais vezes durante as retransmissões. Apesar de fazer sentido selecionar o melhor DAP com maior probabilidade quando se analisa uma única transmissão, quando se consideram as n retransmissões essa escolha passa a apresentar problemas.

Por exemplo, se um medidor dispõe de três DAPs elegíveis, sendo d_1 com probabilidade 0,7, d_2 com probabilidade 0,2 e d_3 com probabilidade 0,1, onde dez retransmissões são utilizadas, então, em média, d_1 será selecionado sete vezes, d_2 será selecionado duas vezes e d_3 será selecionado uma única vez. Como d_1 tem uma probabilidade de seleção alta, então é possível supor que o caminho entre ele e o medidor apresenta alta qualidade. Sendo assim, é muito provável que uma única cópia da mensagem seja suficiente para garantir a entrega à Central de Controle através do DAP d_1. Apesar disso, sete cópias foram enviadas através dele, gerando um *overhead* de tráfego na rede.

Para atenuar esse problema, o MDSA utiliza uma abordagem diferente para as políticas de seleção de DAPs, de retransmissão de mensagem e de elegibilidade de DAPs, conforme ilustrado na Figura 4.7. Diferentemente das propostas baseadas em seleção probabilística de DAPs, o método Select da classe MDSADapSelectionPolicy simplesmente retorna todos os DAPs elegíveis. Quando uma mensagem precisa ser enviada à Central de Controle, ao menos um cópia dela sera encaminhada através de cada um dos DAPs elegíveis.

Assim como no DDSA v2, a política de retransmissão de mensagens do MDSA também é dinâmica, mas calcula o número de retransmissões de maneira diferente. Enquanto que no DDSA v2 o número de retransmissão é calculado de forma a maximizar a probabilidade de entrega da mensagem na Central de Controle, considerando assim todos os DAPs elegíveis, o MDSA calcula o número de retransmissões individualmente para cada DAP, procurando maximizar a probabilidade de entrega no caminho até esse DAP. Ou

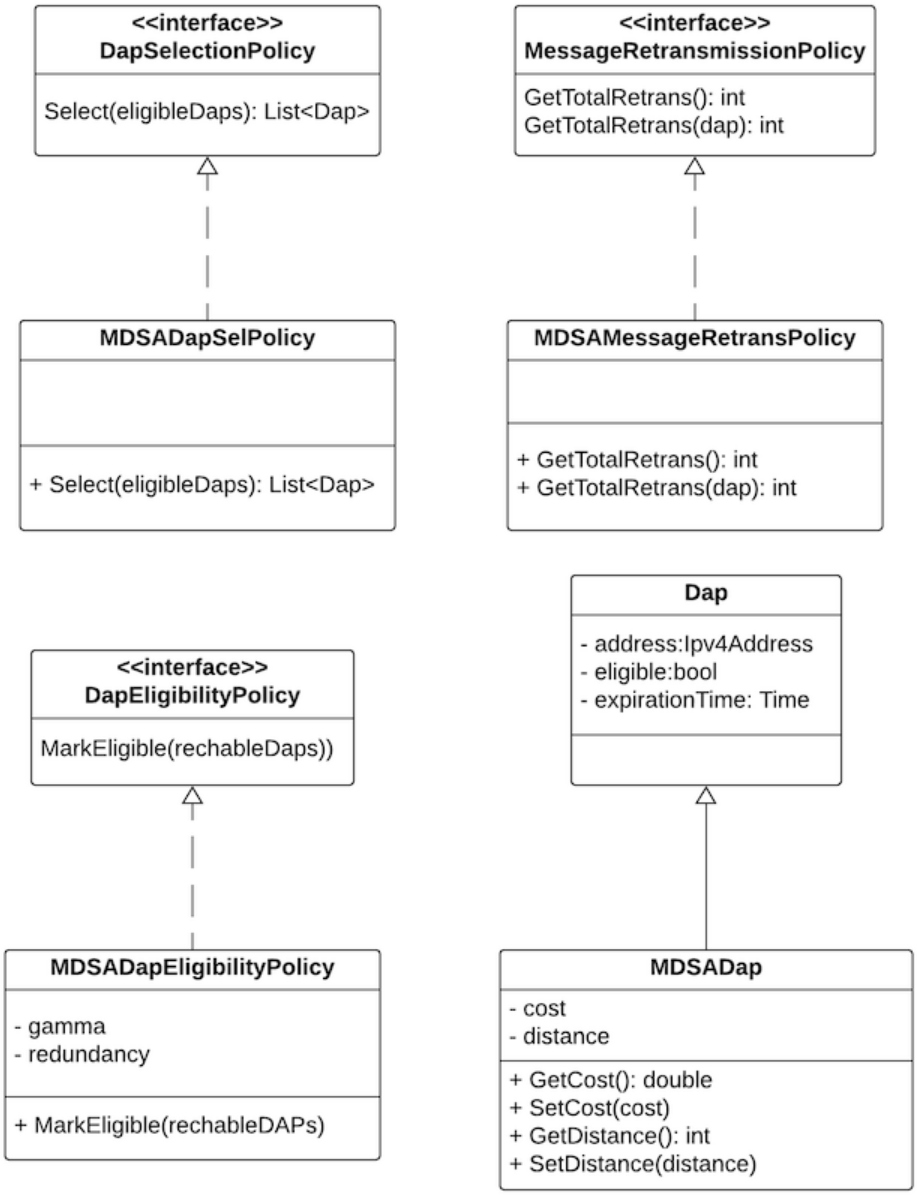


Figura 4.7: Componentes necessários para a implementação do DDSA v2.

seja, para cada DAP selecionado, o MDSA obtém o número total de retransmissões k através de uma chamada ao método GetTotalRetransmissions(dap) da classe MDSAMessageRetransPolicy e envia k cópias através desse DAP. O Algoritmo 5 mostra como o método GetTotalRetrans(dap) é implementado.

Como pode ser observado, o algoritmo calcula o número de retransmissões como sendo o custo(ETX) médio no caminho entre o DAP d_i e o medidor. Para tanto, além da informação sobre o custo do DAP, a classe MDSADap também mantém a distância em número de saltos do caminho entre o DAP e o medidor. Mais uma vez, a informação sobre essa distância deve ser obtida pela classe DapManager a partir do protocolo de roteamento.

Algoritmo 5: Método GetTotalRetrans da classe MDSAMessageRetransPolicy

input : Dap d_i para o qual se quer calcular o número de retransmissões (instância da classe MDSADap

output: Número de retransmissões k para o DAP d_i.

1 $k \leftarrow \frac{d_i.GetCost()}{d_i.GetDistance}$

Entretanto, normalmente os protocolos de roteamento utilizam apenas uma métrica para montar definirem o melhor caminho entre dois nós. A utilização do MDSA introduz uma complexidade adicional, pois requer que o protocolo de roteamento mantenha informações sobre duas métricas: o ETX e a distância em saltos.

Como já discutido, o melhor caminho para alguns DAPs pode apresentar um custo muito alto, fazendo com que o número de retransmissões aumente demasiadamente, gerando um *overhead* muitas vezes desnecessário. Para mitigar esse problema, o MDSA implementa uma política que torna DAPs inelegíveis de acordo com o número de retransmissões k calculado pela Política de Retransmissão de Mensagens, como mostra o Algoritmo 6.

Algoritmo 6: Método MarkEligible da classe MDSADapEligibilityPolicy

input : Conjunto $R = \{d_1, d_2, ..., d_n\}$ de DAPs alcançáveis (instâncias da classe MDSADap)

Result: Todos os DAPs alcançáveis são marcados como elegíveis ou inelegíveis

```
1  nEligible ← |R|
2  foreach d_i ∈ R do
3      k ← retransPolicy.GetTotalRetrans(d_i)
4      if k > gamma e redundancy > nEligible − 1 then
5          d_i.SetEligible(FALSE)
6          nEligible ← nEligible − 1
7      end
8      else
9          d_i.SetEligible(TRUE)
10     end
11 end
```

Na linha 1 o algoritmo inicializa a variável *nEligible*, que guarda o número de DAPs elegíveis até o momento, com o número total de DAPs alcançáveis passados ao método MarkEligible como parâmetro. Na linha 3 o método GetTotalRetrans é chamado através

Tabela 4.1: Tabela comparativa entre as propostas apresentadas.

erle

	UDSA	DDSA v1	DDSA v2	MDSA
Descoberta e Manutenção de DAPs	Baseada em HNA	Baseada em HNA	Baseada em HNA	Baseada em HNA
Política de Seleção de DAPs	Probabilístico com distribuição uniforme	Probabilístico com distribuição inversamente proporcional ao custo	Probabilístico com distribuição inversamente proporcional ao custo	Seleciona todos os elegíveis
Política de Elegibilidade de DAPs	Não exclui nenhum DAP	Exclusão baseada na probabilidade de seleção	Exclusão baseada na probabilidade de seleção	Exclusão baseada no número de retransmissões
Política de Retransmissão de Mensagens	Número de retransmissões estático e configurável	Número de retransmissões estático e configurável	Número de retransmissões dinâmico, calculado a partir das equações 4.4, 4.6 e 4.5	Número de retransmissões dinâmico, definido como a média do ETX no caminho até o DAP

da propriedade retransPolicy presente na classe MDSADapEligibilityPolicy e retorna o número de retransmissões k para o DAP d_i. o DAP é marcado como inelegível (linha 5) se seu número de retransmissões for superior a um limiar *gamma* e se tornar esse DAP inelegível não reduzir o número de DAPs elegíveis a uma valor mais baixo que a redundância mínima *redundancy*. Caso contrário, o algoritmo marca o DAP d_i como elegível na linha 9. Note que *gamma* e *redundancy* são propriedades configuráveis da classe MDSADapEligibilityPolicy.

4.4 Conclusão do Capítulo

Neste capítulo foram apresentadas algumas propostas baseadas no *framework* THOR. Essas propostas se diferenciam pela maneira com que realizam a seleção de DAPs elegíveis, com que marcam como inelegíveis DAPs alcançáveis e, por fim, com que calculam e realizam as retransmissões de mensagens. A Tabela 4.1 resume o comportamento das quatro propostas (UDSA, DDSA v1, DDSA v2 e MDSA), com relação à Descoberta e Manutenção de DAPs (linha 1), Política de Seleção de DAPs (linha 2), Política de Elegibilidade de DAPs (linha 3) e Política de Retransmissão de Mensagens (linha 4).

Capítulo 5

Avaliação das Propostas de Implementação do Framework THOR

Neste capítulo, é apresentada a avaliação experimental das quatro propostas discutidas no Capítulo 4. Todos os resultados analisados neste capítulo foram gerados através de simulações realizadas com o *software* NS3, amplamente utilizado pela comunidade científica.

5.1 Topologia Avaliada

A topologia avaliada neste trabalho representa uma IMA com quatro vizinhanças, onde cada uma possui um total de nove medidores inteligentes. Essas quatro vizinhanças são cobertas por um total de seis DAPs, os quais se conectam à Central de Controle através de enlaces cabeados de longa distância, como ilustrado na Figura 5.1. Os medidores inteligentes e os DAPs formam entre si uma Rede em Malha Sem Fio configurada com o protocolo de roteamento OLSR (modificado para operar com métricas cientes de qualidade) e uma implementação da métrica ETX baseada no número de sequência de pacotes [45].

Os links sem fio utilizados no cenário foram divididos em dois grupos: aqueles com potência de recepção de -95 dbm e os com potência de recepção de -97 dbm. A distribuição desses enlaces pode ser observada na Figura 5.1. Note que quando não há um enlace entre dois nós na figura, significa que eles só poderão se comunicar através de múltiplos saltos.

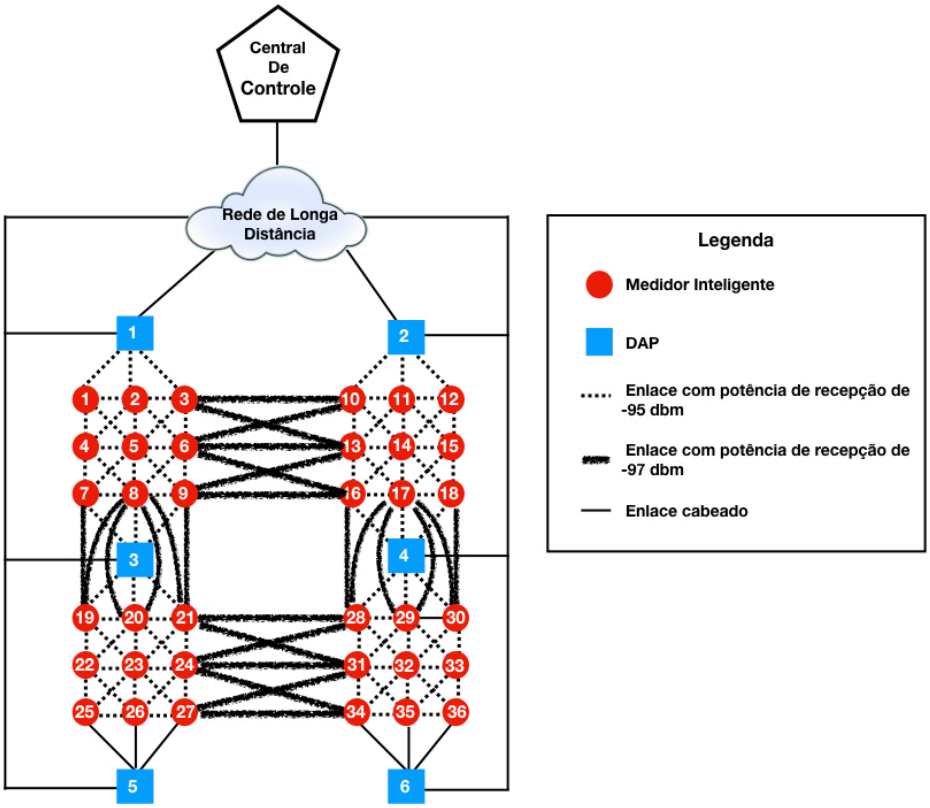


Figura 5.1: Cenário de uma AMI com quatro vizinhanças cobertas por seis DAPs no total.

5.2 Aplicação Utilizada

Uma das principais funções da IMA é permitir a coleta de dados gerados pelos medidores inteligentes, que são então encaminhados para a central de controle para análise e processamento. Essa coleta pode ser ativada periodicamente, em reação a um evento local ou de acordo com a demanda da operadora. Além disso, os dados coletados podem ser enviados individualmente para a central de controle ou podem ser agregados nos DAPs para reduzir o *overhead* gerado pelos cabeçalhos dos protocolos e, consequentemente, a utilização da rede [28, 52]. Tendo em vista que o objetivo principal deste trabalho é garantir que a AMI seja resiliente à falha de DAPs, a maneira pela qual a coleta de dados é iniciada e o formato no qual os dados são enviados dos DAPs para a central de controle são irrelevantes.

Sendo assim, todos os medidores da IMA foram configurados com uma aplicação de coleta de dados periódica, onde a cada três segundos (essa frequência de envio é igual a usada em [41]) uma mensagem é enviada para a Central de Controle. Além dos dados

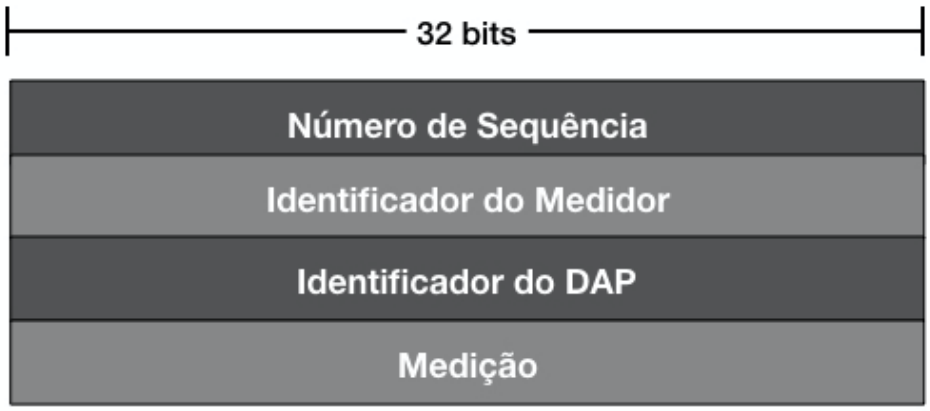


Figura 5.2: Cabeçalho das mensagens enviadas pelos medidores inteligentes.

propriamente ditos, cada mensagem também contém um cabeçalho, como mostrado na Figura 5.2. Uma vez que essas mensagens utilizam o protocolo UDP para transporte e podem ser duplicadas pela Política de Retransmissão de Mensagens, é preciso estabelecer um número de sequência que permita a Central de Controle diferenciar mensagens originais e duplicatas. Outra informação importante para a Central de Controle é o identificador do medidor que enviou a mensagem. Esse campo poderia ser excluído do cabeçalho da mensagem caso os medidores inteligentes fossem configurados com endereços IP públicos. Por fim, a mensagem também carrega o identificador do DAP que a encaminhou até a Central de Controle. Essa informação pode ser interessante para, por exemplo, identificar DAPs com problema ou mal posicionados (DAPs que não estão encaminhando qualquer mensagem).

É importante ressaltar que mecanismos de segurança devem ser incluídos na comunicação entre o medidor, o DAP e a central de controle. Caso contrário, um atacante poderia, por exemplo, se passar por um medidor e fornecer informações incorretas para a Central de Controle. Outra ameaça importante é a violação da privacidade dos usuários, através da análise dos seus padrões de consumo [35, 2]. Apesar se serem fundamentais para o correto funcionamento da AMI, tais mecanismos não são implementados neste trabalho, já que não interferem na capacidade de resiliência à falhas de DAPs da rede.

5.3 Modelo de Falha de DAP

O objetivo principal deste trabalho é propor uma solução para a IMA que permita aos medidores manter a comunicação com a Central de Controle mesmo no caso de falha de DAPs. Sendo assim, para que seja possível avaliar o impacto das propostas de imple-

mentação do *framework* THOR, faz-se necessário definir o que se entende por falha de DAP neste trabalho.

O tipo mais simples de falha, definido neste trabalho como **Falha Total - FT**, é aquele onde, devido a um problema de *hardware* ou *software*, o DAP para de enviar e receber, de forma inesperada e aleatória, qualquer tipo de pacote, incluindo os pacotes de controle gerados pelo protocolo de roteamento. Como consequência, todas as mensagens de medição que precisarem passar por esse DAP para serem encaminhadas à Central de Controle serão perdidas após a falha.

Na Falha Total, o problema ocorre de forma não intencional, resultante de uma falha real no equipamento. Por outro lado, uma vez que DAPs são dispositivos críticos instalados em ambientes com pouca ou nenhuma proteção, é possível supor que estes equipamentos são alvos em potencial para possíveis ataques cibernéticos. Neste contexto, o segundo tipo de falha considerado, chamado de **DAP Malicioso - DM**, é aquele onde um atacante altera o funcionamento do *hardware* ou do *software* do DAP e este passa a se comportar de forma maliciosa.

O comportamento malicioso implementado e avaliado foi aquele conhecido como **Buraco Cinza** [27], onde o DAP tenta atrair para si a maior parte possível das mensagens e executa um encaminhamento seletivo, onde todas as mensagens de aplicação (mensagens de medição periódica) são descartadas, mas todas as mensagens de controle são processadas e encaminhadas normalmente. Para atrair o tráfego para si, o DAP malicioso envia informações falsas sobre a métrica ETX, dando a entender que, do ponto de vista do DAP malicioso, todos os enlaces que chegam até ele têm custo mínimo. Além disso, o DAP malicioso ignora uma configuração realizada no protocolo de roteamento que evita a formação de caminhos entre um medidor e um DAP que contenha outros DAPs.

5.4 Métricas Avaliadas

Durante as simulações, quatro métricas foram utilizadas para avaliar o desempenho das propostas baseadas no *framework* THOR. São elas:

- **Taxa de Entrega de Mensagens:** representa a fração de mensagens corretamente recebidas pela Central de Controle. Uma mensagem é considerada corretamente recebida quando ao menos uma de suas cópias é recebida pela Central de Controle;
- **Latência:** tempo entre o envio da primeira cópia de uma mensagem e a recepção

de qualquer uma das cópias desta mensagem pela Central de Controle. Note que mensagens que não são corretamente recebidas pela Central de Controle não têm sua latência considerada;

- **Número de Mensagens Enviadas:** representa o número total de cópias de mensagens enviadas considerando-se todos os medidores;
- **Número de Colisões Internas:** representa o número total de colisões internas geradas durante toda a simulação. Do ponto de vista do simulador NS3, colisões internas são causadas exclusivamente pela geração e envio de uma mensagem em um nó enquanto ele está transmitindo outra mensagem.

5.5 Metodologia de Execução das Simulações

Considere como um cenário de simulação o conjunto formado por:

- uma topologia de rede para a AMI;
- uma proposta de implementação do *framework* THOR;
- um modelo de falha.

Em todos os cenários de simulação avaliados, a topologia da AMI foi mantida como aquela descrita na Seção 5.1. Além das propostas de implementação do *framework* THOR, apresentadas no Capítulo 4, também foram avaliados cenários de simulação onde o *framework* THOR não foi utilizado. Nesse caso, a AMI opera apenas com o protocolo de roteamento OLSR e a métrica ETX, sem quaisquer mecanismos adicionais para aumentar a resiliência. Para fins de nomenclatura, chamamos a ausência de implementação do *framework* THOR de **BestDAP**, pois as mensagens são encaminhadas através do DAP que pertence ao caminho de menor custo entre o medidor e a Central de Controle.

O último componente de um cenário de simulação, o modelo de falha, é opcional. Quando um modelo de falha não é fornecido, todos os DAPs se comportam normalmente, sem apresentar qualquer problema. Por outro lado, se um modelo de falha for configurado, então o DAP que deve falhar passará a apresentar o comportamento característico do modelo de falha após um instante de tempo especificado. Nas simulações realizadas neste trabalho, foram analisadas as falhas de dois DAPs diferentes (DAPS 4 e 5), um por vez.

Tabela 5.1: Cenários de simulação avaliados no presente trabalho. Para cada cenário é mostrada a proposta de implementação do *framework* THOR, o DAP que apresenta falha e o modelo de falha

	Proposta	DAP	Modelo de Falha
Cenário 1	BestDAP	——	Sem Falha
Cenário 2	UDSA	——	Sem Falha
Cenário 3	DDSA v1	——	Sem Falha
Cenário 4	DDSA v2	——	Sem Falha
Cenário 5	MDSA	——	Sem Falha
Cenário 6	BestDAP	Central	Falha Total
Cenário 7	UDSA	Central	Falha Total
Cenário 8	DDSA v1	Central	Falha Total
Cenário 9	DDSA v2	Central	Falha Total
Cenário 10	MDSA	Central	Falha Total
Cenário 11	BestDAP	Periférico	Falha Total
Cenário 12	UDSA	Periférico	Falha Total
Cenário 13	DDSA v1	Periférico	Falha Total
Cenário 14	DDSA v2	Periférico	Falha Total
Cenário 15	MDSA	Periférico	Falha Total
Cenário 16	BestDAP	Central	DAP Malicioso
Cenário 17	UDSA	Central	DAP Malicioso
Cenário 18	DDSA v1	Central	DAP Malicioso
Cenário 19	DDSA v2	Central	DAP Malicioso
Cenário 20	MDSA	Central	DAP Malicioso
Cenário 21	BestDAP	Periférico	DAP Malicioso
Cenário 22	UDSA	Periférico	DAP Malicioso
Cenário 23	DDSA v1	Periférico	DAP Malicioso
Cenário 24	DDSA v2	Periférico	DAP Malicioso
Cenário 26	MDSA	Periférico	DAP Malicioso

O DAP 4 representa o grupo de DAPs centrais, mais próximos a um número maior de medidores. Já o DAP periférico representa um grupo de DAPs periféricos.

Para cada cenário apresentado na Tabela 5.1, foi executado um total de dez rodadas de simulação, cada uma com duração de 500 segundos. Nos primeiros 100 segundos somente mensagens de controle do protocolo de roteamento são trocadas. Após esse período de inicialização, todos os medidores começam a enviar mensagens de medição periódica com frequência de uma a cada três segundos. Se o cenário de simulação foi configurado com um cenário de falha, então no tempo 150 segundos o DAP especificado começa a apresentar o comportamento esperado para o tipo de falha. Completadas as dez rodadas de simulação, são extraídas a média e o intervalo de confiança para cada uma das métricas definidas na Seção 5.4.

5.6 Análise do Impacto do Parâmetro Alpha na Proposta DDSA v1

A proposta DDSA v1 estabelece a utilização de um parâmetro *alpha* que controla sua Política de Elegibilidade de DAPs. Ao aumentar o valor de *alpha*, a tendência é que a quantidade de DAPs elegíveis para o medidor se torne menor, mas a qualidade desses DAPs se torna mais homogênea. Por outro lado, ao reduzir o valor de *alpha*, o tamanho da lista de DAPs elegíveis tende a aumentar, assim como a variabilidade na qualidade dos DAPs pertencentes à lista. Estabelecer uma boa relação entre redundância e qualidade é fundamental para que a proposta possa apresentar um bom desempenho. Sendo assim, nesta seção a proposta DDSA v1 é analisada considerando-se os valores de *alpha* 0,0, 0,2, 0,4, 0,6 e 0,8 nos cenários 13 e 23 da Tabela 5.1.

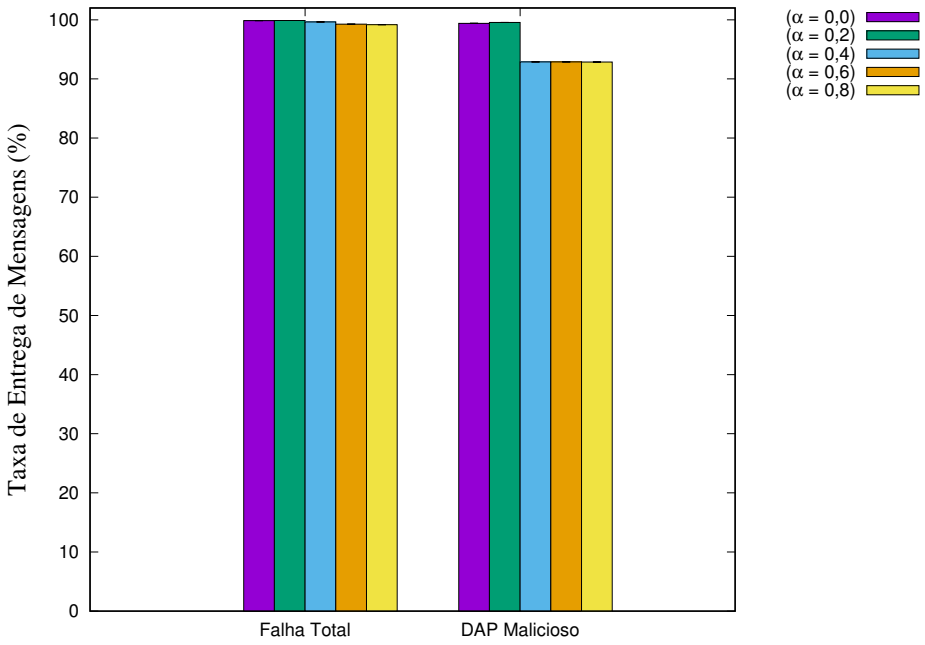
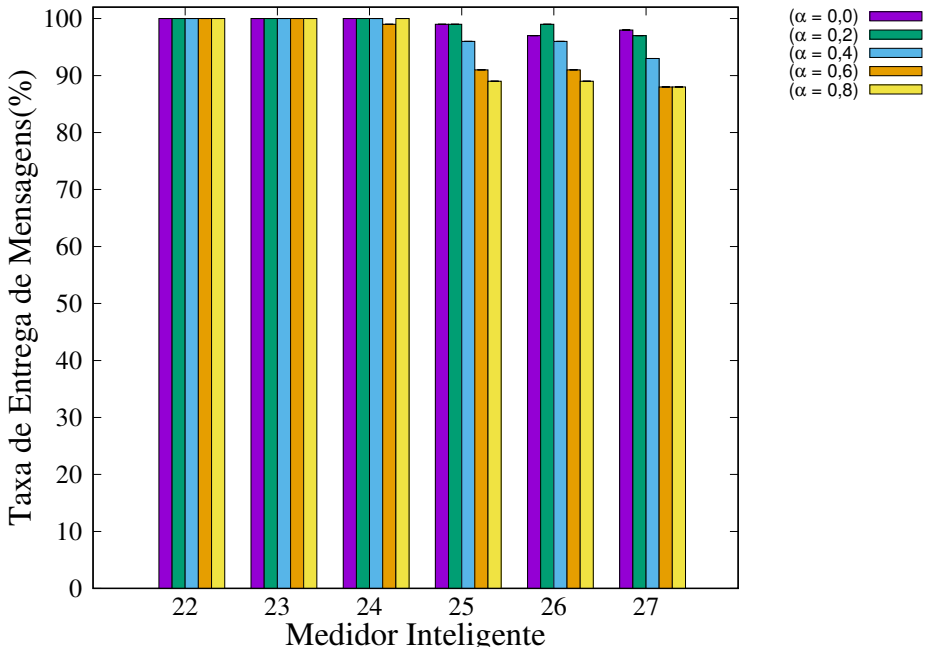
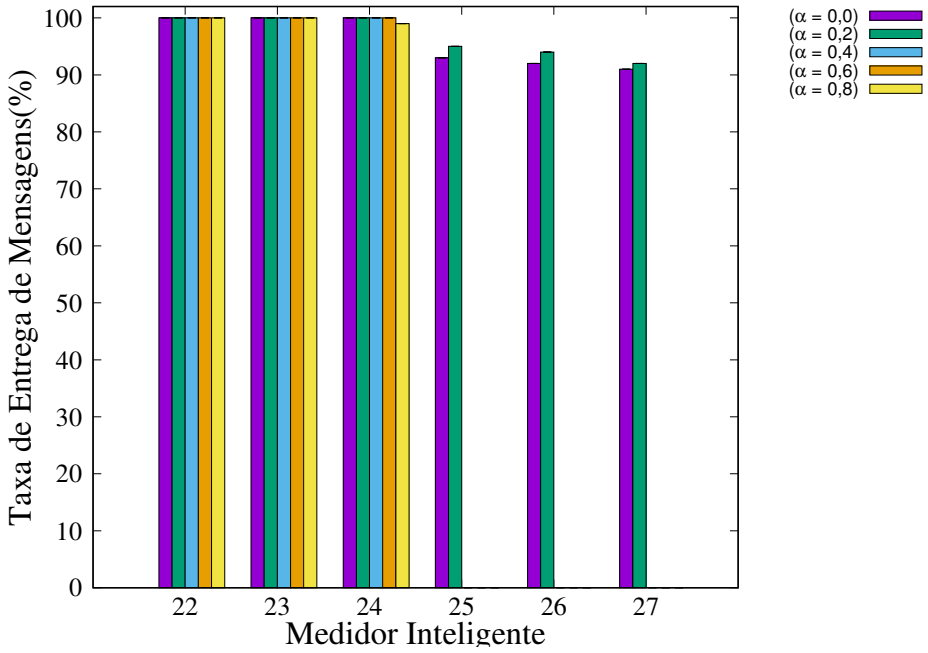


Figura 5.3: Taxa de Entrega de Mensagens considerando-se todos os medidores nos cenários 13 e 23 da Tabela 5.1 para os valores de *alpha* 0,0, 0,2, 0,4, 0,6 e 0,8.

A Figura 5.3 mostra como a Taxa de Entrega de Mensagens varia com os diferentes valores de *alpha* quando todos os medidores inteligentes presentes na IMA são considerados. No caso de uma Falha Total, o aumento do valor de *alpha* causa uma redução muito pequena na Taxa de Entrega de Mensagens. Na realidade, ao observar a Figura 5.4a, que representa a Taxa de Entrega de Mensagens para os medidores mais próximos ao DAP que falha, é possível notar que valores de *alpha* acima de $0,2$ causam uma redução progressiva no desempenho do DDSA v1. Com $alpha = 0,8$, os medidores mais próximos



(a) Falha Total



(b) DAP Malicioso

Figura 5.4: Taxa de entrega de mensagens considerando-se os medidores 22 a 27 nos cenários 13 e 23 da Tabela 5.1 para os valores de *alpha* 0,0, 0,2, 0,4, 0,6 e 0,8.

ao DAP que falha (25, 26 e 27) tem uma redução de aproximadamente 10% na Taxa de Entrega de Mensagens. Ocorre que com valores altos de *alpha* a redundância de DAPs é reduzida e quando um DAP falha os medidores mais próximos a ele ficam com poucas, senão nenhuma, alternativas para encaminhar suas mensagens. Como consequência, a

maioria das mensagens é enviada através do DAP com problemas, e, consequentemente, é perdida. Quando os medidores percebem que o DAP com problemas não é mais alcançável, ele deixa de ser escolhido para encaminhar as mensagens. Nesse ponto, dos DAPs que ainda são alcançáveis, aquele com menor custo passa a ter a maior probabilidade de seleção, permitindo que a rede se recupere.

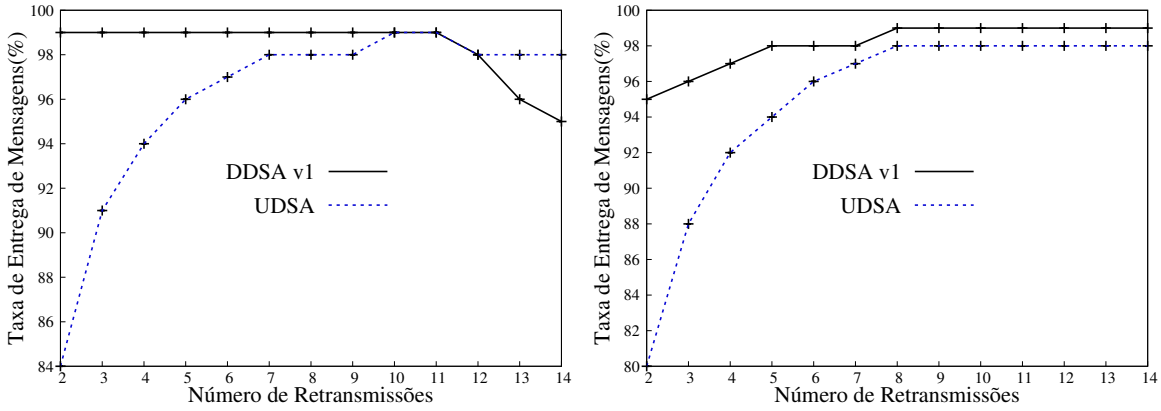
Por outro lado, quando uma falha causada por um DAP malicioso é considerada, é possível perceber na Figura 5.3 que valores altos de *alpha* causam uma redução significativa na Taxa de Entrega de Mensagens. Quando $alpha = 0,2$, a redundância de DAPs é preservada e não há perda de desempenho. Na verdade, a Figura 5.4b mostra que há um ligeiro aumento na Taxa de Entrega de Mensagens para os medidores mais próximos ao DAP que falha devido a não elegibilidade de DAPs com alto custo. Porém, para $alpha \geq 0,4$ a redundância de DAPs é eliminada, fazendo com que os medidores mais próximos enviem todas as suas mensagens através do DAP malicioso, gerando o seu descarte. Como o DAP malicioso continua alcançável por toda a simulação, nenhum outro DAP tem a chance de ser ecolhido pelo DDSA v1, fazendo com que nenhuma mensagem enviada pelos medidores 25 a 26 sejam recebidas, motivo pelo qual a Taxa de Entrega de Mensagem é zero.

Como resultado desta análise, é possível concluir que no cenário avaliado valores maiores que zero para o *alpha* não melhoram significativamente, ou até mesmo reduzem, o desempenho do DDSA v1. Uma vez que o DDSA v2 utiliza a mesma política de seleção e de elegibilidade do DDSA v1, é possível considerar que os resultados seriam análogos. Sendo assim, no restante dos experimentos realizados neste trabalho, tanto o DDSA v1 quanto o DDSA v2 terão o parâmetro *alpha* configurado como zero.

5.7 Análise do número de retransmissões nas propostas UDSA e DDSA v1

Uma característica muito importante para todas as propostas baseadas em seleção probabilística de DAPs é o número de retransmissões. A escolha de um valor baixo para esse parâmetro reduz o aproveitamento da disponibilidade de DAPs redundantes na rede. Por outro lado, a escolha de um valor muito alto para o número de retransmissões pode acarretar um aumento significativo no número de mensagens desnecessárias trafegando na rede, gerando mais colisões e, consequentemente, aumentando o atraso. No caso das propostas apresentadas neste trabalho, apenas a UDSA e a DDSA v1 definem um valor

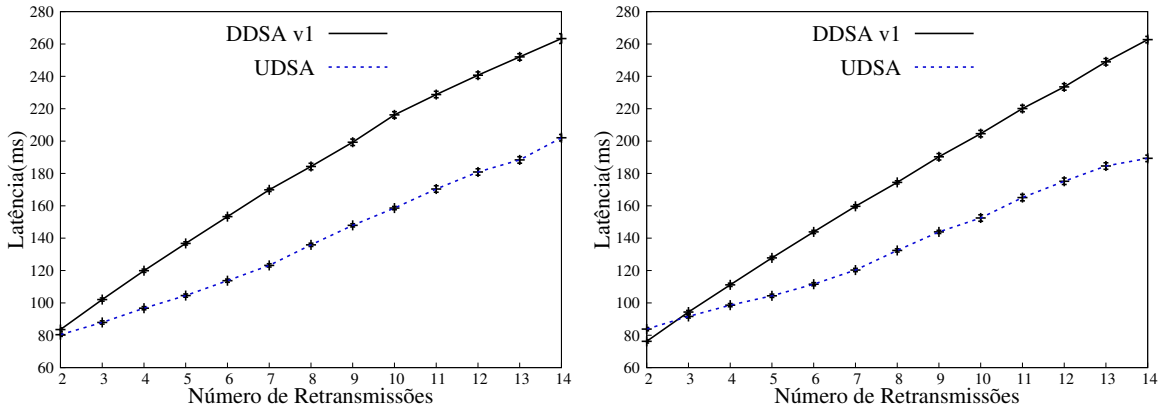
estático para o número de retransmissões. Sendo assim, nesta seção é realizada uma análise sobre como variam as métricas de Taxa de Entrega de Mensagens e de Latência conforme o número de retransmissões cresce para essas duas propostas.



(a) Falha Total (b) DAP Malicioso

Figura 5.5: Taxa de entrega de mensagens considerando-se todos os medidores quando o número de retransmissões varia de 2 a 14.

A Figura 5.5 mostra como a média da Taxa de Entrega de Mensagens, considerando todos os medidores, varia conforme o número de retransmissões do UDSA e do DDSA v1 aumenta de 2 até 14 em um cenário com Falha Total (cenários 12 e 13 da Tabela 5.1) - Figura 5.5a e em um cenário com DAP Malicioso (cenários 17 e 18 da Tabela 5.1) - Figura 5.5b.



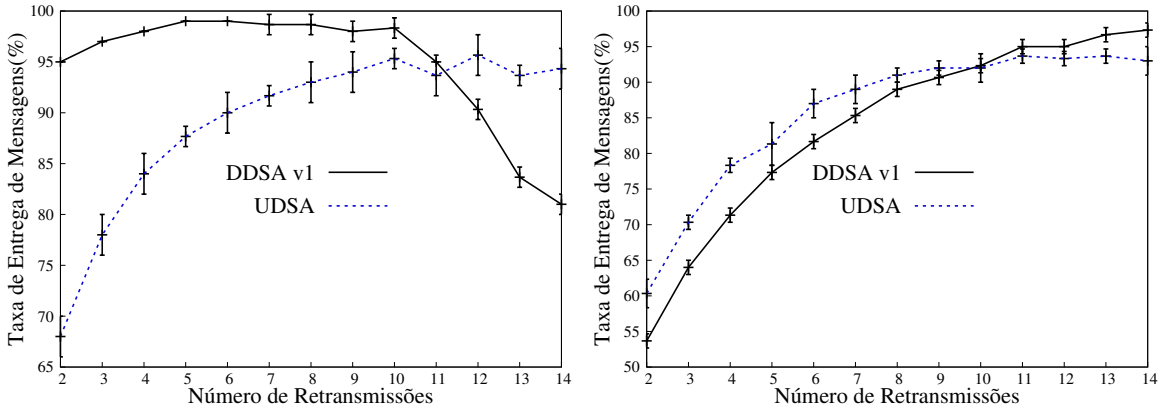
(a) Falha Total (b) DAP Malicioso

Figura 5.6: Média da latência considerando-se todas as mensagens (única cópia) enviadas e recebidas por todos os medidores para cada cenário de falha.

Observe que para se obter uma Taxa de Entrega de Mensagens acima de 98% foi preciso utilizar, em um cenário com Falha Total, duas e dez retransmissões para as propostas DDSA v1 e UDSA, respectivamente. No caso do cenário com DAP malicioso, a proposta

UDSA foi capaz de entregar um máximo de 98,73% das mensagens enviadas utilizando um total de onze retransmissões. Já a proposta DDSA v1 entregou acima de 99% das mensagens enviadas utilizando um número de retransmissões maior ou igual a oito.

Ao analisar a Figura 5.6, é possível perceber que a Latência média das mensagens cresce de forma aproximadamente linear com o número de retransmissões. Por essa razão, faz-se necessário escolher o número de retransmissões a ser utilizado com as propostas DDSA v1 e UDSA de forma a maximizar a Taxa de Entrega, mas sem causar penalidades desnecessárias à Latência. Também é importante que o mesmo número de retransmissões seja utilizado para uma proposta em ambos os cenários de falha, já que não é possível saber quando uma Falha Total ou um DAP malicioso ocorrerão. Nesse sentido, ao analisar a Figura 5.5, é possível concluir que o número de retransmissões apropriado para ambos os cenários de falha e ambas as propostas é igual a oito, pois a partir deste ponto, a Taxa de Entrega de Mensagens cresce pouco em comparação ao crescimento da latência e, no caso do DDSA v1 com Falha Total, essa taxa inclusive decresce a partir de onze retransmissões;



(a) Falha Total (b) DAP Malicioso

Figura 5.7: Média da taxa de entrega de mensagens dos medidores 25, 26 e 27 quando o número de retransmissões varia de 2 a 14.

Uma característica importante da AMI é que cada medidor é igualmente importante para o bom funcionamento da Rede Elétrica Inteligente. Isso significa que o *framework* THOR precisa garantir que todos os medidores da rede possuam uma boa Taxa de Entrega de Mensagens. Além disso, as falhas de DAP não são percebidas da mesma maneira por todos os medidores, estando, em geral, os mais próximos ao DAP que falha mais vulneráveis à falha em si. Nesse sentido, não é suficiente analisar apenas a média da Taxa de Entrega considerando todos os medidores, mas é necessário também investigar individualmente a Taxa de Entrega de Mensagens para esses DAPs mais próximos ao

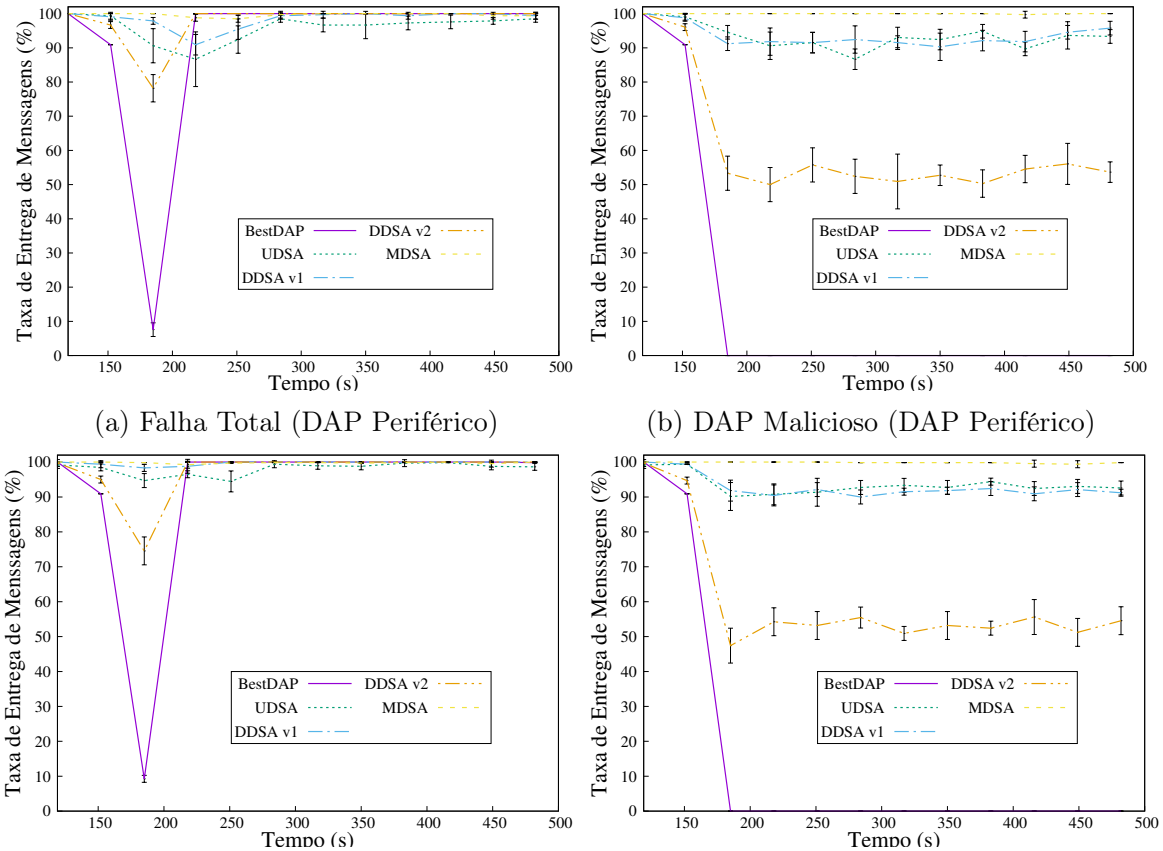
DAP que falha. A Figura 5.7 mostra como a média da Taxa de Entrega de Mensagens dos medidores 25, 26 e 27, os mais próximos ao DAP que falha (DAP periférico), varia com o número de retransmissões para as propostas DDSA v1 e UDSA.

Ao observar a Figura 5.7b, é possível notar que, no caso do DDSA v1, o número de retransmissões que apresenta a maior Taxa de Entrega de Mensagens é 14. Entretanto, a Figura 5.7a mostra que em uma Falha Total, um número de retransmissões acima de 10 reduz consideravelmente a Taxa de Entrega de Mensagens obtida com o DDSA v1. Para garantir um bom equilíbrio entre os dois cenários de falha, o número de retransmissões que será utilizado para o DDSA v1 nos próximos resultados analisados será igual a dez. Em relação à proposta UDSA, a Figura 5.7a mostra que a Taxa de Entrega de Mensagens para essa proposta é maximizada quando o número de retransmissões é definido como 10. No caso de um DAP malicioso, a Figura 5.7b mostra que a Taxa de Entrega de Mensagens cresce discretamente a partir de 10 retransmissões. Consequentemente, para manter um equilíbrio entre os dois cenários de falha, a proposta UDSA também será configurada com 10 retransmissões nos demais resultados apresentados neste trabalho.

5.8 Análise da Taxa de Entrega de Mensagens ao Longo do Tempo

Para compreender o impacto de uma falha de DAP na IMA, é útil analisar como a Taxa de Entrega de Mensagens varia ao longo de todo o tempo de simulação, como ilustrado na Figura 5.8. Para tanto, o período de simulação foi dividido em intervalos de 33 segundos, onde a Taxa de Entrega de Mensagens foi calculada considerando-se apenas as mensagens enviadas e recebidas dentro desse intervalo pelos medidores mais próximos ao DAP que falha (medidores 22 a 27, no caso do DAP periférico e medidores 16 a 18 e 28 a 30, no caso do DAP central, como ilustrado na Figura 5.10).

Primeiramente, observe que quando uma Falha Total ocorre ($t = 150$s), a Taxa de Entrega de Mensagens para o BestDAP cai rapidamente de 100% para aproximadamente 7%, no caso de falha no DAP Central (Figura 5.8a) e 9%, no caso de falha do DAP periférico (Figura 5.8c). Após o instante 200s, os medidores mais próximos ao DAP que falha passam a selecionar um novo melhor DAP, fazendo com que a rede se recupere e o BestDAP volta a entregar 100% das mensagens. Quando a falha é maliciosa (Figuras 5.8b e 5.8d) a Taxa de Entrega de Mensagens para o BestDAP também cai rapidamente, mas agora de 100% para 0%. Entretanto, como o DAP malicioso continua a enviar mensagens



(a) Falha Total (DAP Periférico)

(b) DAP Malicioso (DAP Periférico)

(c) Falha Total (DAP Central)

(d) DAP Malicioso (DAP Central)

Figura 5.8: Varição da Taxa de Entrega de Mensagens ao longo do tempo para os medidores 22 a 27 (DAP periférico), 16 a 18 e 28 a 30 (DAP Central), para todos os cenários de simulação com falha.

de controle do protocolo de roteamento, o BestDAP não consegue detectar o problema, fazendo com que a rede não se recupere mais. Uma vez que os medidores mais próximos ao DAP malicioso não são mais capazes de se comunicar com a Central de Controle e, portanto, se tornam indisponíveis, podemos considerar que houve um ataque de negação de serviço.

Por outro lado, é possível notar que quando uma implementação do *framework* THOR é utilizada, a perda de desempenho causada por uma Falha Total é bastante reduzida, já que o tempo de recuperação não existe ou é bem pequeno, pois cada medidor envia proativamente suas mensagens para mais de um DAP ao mesmo tempo. Da mesma forma, a utilização do *framework* THOR elimina a indisponibilidade dos medidores, já que estes continuam entregando uma fração das mensagens enviadas durante todo o tempo de simulação. Entre as propostas de implementação, fica claro que o DDSA v2 tem o pior desempenho, apresentando uma redução na Taxa de Entrega de Mensagens entre 22 e 26%, no caso de uma Falha Total (mas se recupera após o instante 200s e volta a entregar

100% das mensagens) e em aproximadamente 50% quando a falha é maliciosa, mas nesse caso a rede não se recupera e mantém a baixa performance até o fim da simulação.

As propostas UDSA e DDSA v1 apresentam comportamentos bem parecidos em todos os cenários avaliados. Considere inicialmente um cenário sem falhas. Nesse caso, o DDSA v1 no medidor 26 concentra o envio de cópias através dos DAPs 5 e 3 (os demais DAPs também são usados, mas em uma proporção bem menor), enquanto que o UDSA distribui as cópias de forma mais equilibrada através dos DAPs de 1 a 6 (apesar da escolha dos DAPs ser uniforme, nem todos são alcançáveis pelo medidor o tempo todo). Sendo assim, quando não há falhas, o UDSA apresenta uma desvantagem teórica em relação ao DDSA v1, já que ele reduz a probabilidade de entrega em caminhos de maior qualidade, sem aumentar significativamente a probabilidade de entrega em caminhos de menor qualidade (deixa de enviar algumas cópias por DAPs melhores para enviá-las por DAPs piores).

Quando a Falha Total ocorre no DAP periférico, porém, o UDSA possui uma vantagem teórica em relação ao DDSA v1, já que provê uma maior utilização da redundância de DAPs. Entretanto, o que ocorre é que no momento da falha, as cópias enviadas pelo medidor 31 para o DAP periférico serão perdidas, mas muitas cópias ainda são enviadas através do DAP 3. Consequentemente, apesar de perder muitas cópias, devido à falha, o DDSA v1 ainda é capaz de entregar a maioria das mensagens. Por outro lado, o UDSA perde menos cópias no momento da falha, mas como envia menos cópias para cada DAP restante, reduz a probabilidade de entrega para cada um deles, fazendo com que o UDSA entregue ligeiramente menos mensagens do que o DDSA v1. No caso do DAP periférico se comportar de forma maliciosa, o raciocínio é similar, onde a maioria das mensagens entregues à Central de Controle pelas duas propostas foram encaminhadas pelo DAP 3.

Por fim, note que a proposta MDSA praticamente não sofre qualquer impacto das falhas, tanto total quanto maliciosa, oferecendo assim maior resiliência à rede.

5.9 Análise da Média da Taxa de Entrega de Mensagens

Após analisar como a Taxa de Entrega de Mensagens varia com o tempo em todos os cenários de simulação, é interessante estudar também qual a fracção de mensagens, em média, é entregue à Central de Controle ao longo de todo o período da simulação. O primeiro gráfico, mostrado na Figura 5.9, apresenta a comparação da média da Taxa de Entrega de Mensagens, considerando todos os medidores, para cada um dos vinte e

seis cenários de simulação descritos na Tabela 5.1. Note que, nos cenários onde há um modelo de falha implementado, somente são consideradas as mensagens enviadas após o instante de falha. No gráfico, é possível observar que, quando não há falha de DAPs, aproximadamente 100% das mensagens enviadas são corretamente recebidas. Isso significa que, mesmo nos cenários que implementam um modelo de falha de DAP, antes do instante da falha, todas as propostas também entregam aproximadamente 100% das mensagens.

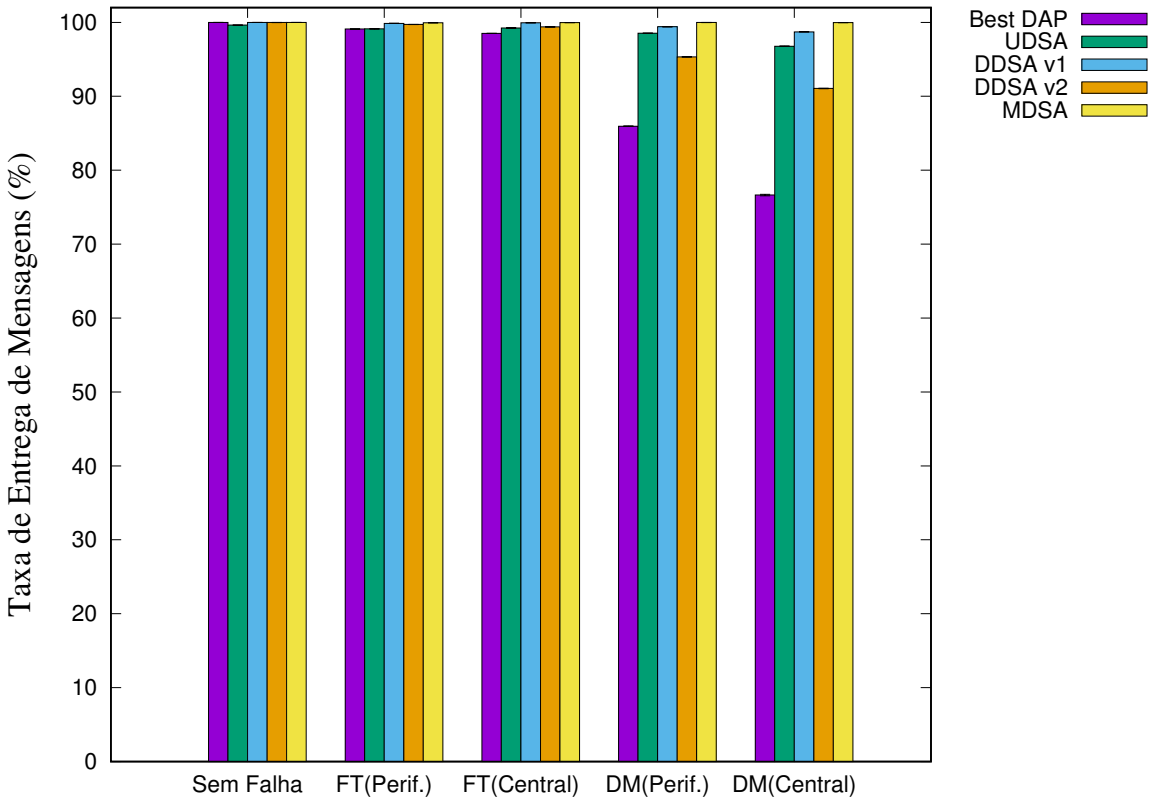
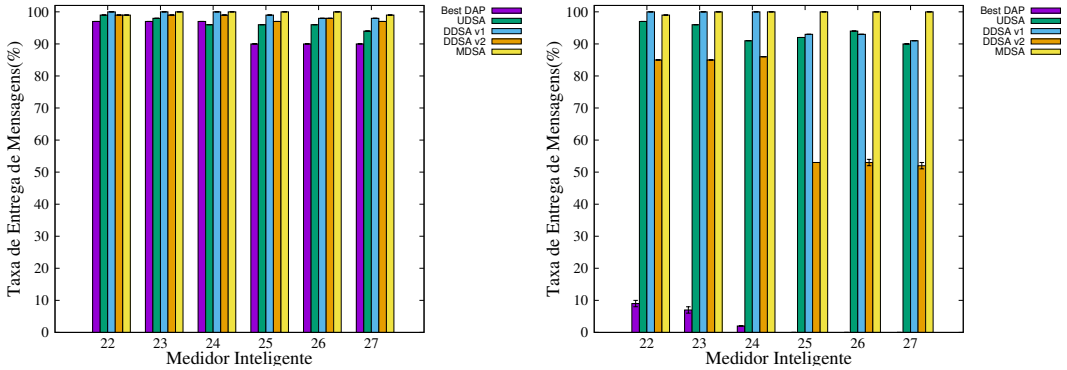


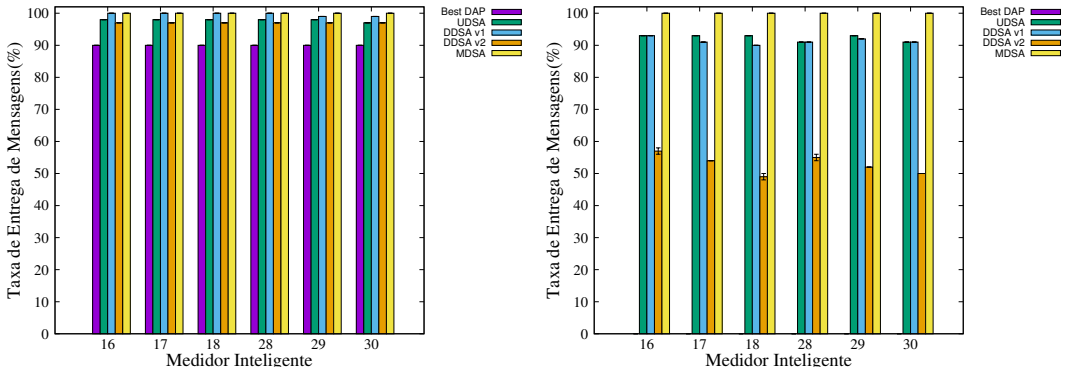
Figura 5.9: Taxa de entrega de mensagens considerando todos os medidores.

Em primeiro lugar, note que o impacto de uma Falha Total é consideravelmente menor do que o de uma falha causada por um DAP malicioso, independentemente da posição do DAP. Quando a IMA não implementa o *framework* THOR, o que é representado pelo BestDAP, a rede é capaz de entregar, em média, 23% menos mensagens no caso de uma falha causada por um DAP malicioso do que em um cenário sem falha. Na realidade, esses resultados são ainda piores se considerarmos para a média da Taxa de Entrega de Mensagens apenas os medidores mais próximos ao DAP que falha, sendo eles os medidores 22 a 27, no caso do DAP periférico e os medidores 16 a 18 e 28 a 30, no caso do DAP central, ilustrado na Figura 5.10. Como pode ser observado, se a IMA não implementa o *framework* THOR, no caso do DAP periférico se comportar de forma maliciosa, os medidores 22, 23 e 24 têm menos de 10% das suas mensagens entregues à Central de

Controle. Se o DAP malicioso for central, então todas as mensagens enviadas pelos medidores mais próximos a ele após a falha são perdidas. Quando a falha apresentada é total, uma IMA sem o *framework* THOR também sofre uma redução na taxa de entrega, mas mesmo assim todos os medidores continuam tendo no mínimo 90% das mensagens enviadas após a falha sendo entregues à Central de Controle. Esses resultados ilustram a necessidade de se implementar um mecanismo que garanta a resiliência da rede frente a falhas de DAPs.



(a) Falha Total (DAP Periférico) (b) DAP Malicioso (DAP Periférico)



(c) Falha Total (DAP Central) (d) DAP Malicioso (DAP Central)

Figura 5.10: Média da Taxa de Entrega de Mensagens considerando os medidores 22 a 27 (DAP Periférico), 16 a 18 e 28 a 30 (DAP Central), para os dois modelos de falha considerados.

Devido às suas similaridades, é interessante realizar a análise das propostas UDSA, DDSA v1 e DDSA v2 em conjunto. Observando a média de todos os medidores (Figura 5.9), é possível notar que, no caso de uma Falha Total, essas propostas possuem desempenho muito semelhante no que concerne a Taxa de Entrega de Mensagens. Há, porém, uma pequena desvantagem da proposta UDSA em relação às demais. Antes da falha, porém, a UDSA já apresentava uma Taxa de Entrega de Mensagens ligeiramente menor, devido às escolhas de DAPs com qualidade inferior (DAPs equiprováveis). Quando uma Falha Total ocorre, os medidores mais próximos ainda podem enviar algumas men-

sagens através de um DAP com custo maior, mas ainda assim aceitável. Entretanto, a probabilidade de entrega de uma mensagem continua baixa, já que, uma vez que o UDSA não implementa uma Política de Exclusão de DAPs, DAPs com custo muito alto (baixa probabilidade de entrega) podem ser selecionados.

Por outro lado, como o DDSA v1 escolhe DAPs de maior qualidade com maior probabilidade, antes da falha essa proposta garante a entrega de 100% das mensagens enviadas. Quando a Falha Total ocorre, os medidores mais próximos continuam enviando mensagens com maior probabilidade para o DAP com problemas. Entretanto, devido à utilização de retransmissões pró-ativas, outros DAPs com qualidade aceitável podem ser utilizados para encaminhar cópias das mensagens. Durante o tempo de recuperação da rede, algumas mensagens enviadas por medidores mais próximos ao DAP com problemas podem ser perdidas, mas após algum tempo a probabilidade de seleção do DAP com problemas chega a zero e ele é excluído da lista de DAPs alcançáveis.

Ao analisar os cenários com DAP malicioso, é possível notar que a proposta que apresenta os piores resultados é o DDSA v2 (figuras 5.9, 5.10b e 5.10d). Isso ocorre, pois essa proposta utiliza o custo de cada DAP para estimar o número de retransmissões mais adequado para atingir 99% de probabilidade de entrega. Entretanto, como o custo do DAP malicioso não reflete sua confiabilidade, o DDSA acaba subestimando o número de retransmissões. Pior ainda, como o DAP malicioso se anuncia com qualidade ótima, o DDSA v2 acaba calculando um valor ainda mais incorreto para o número de retransmissões. Como o DDSA v2 utiliza um Algoritmo de Seleção de DAPs similar ao do DDSA v1, ele envia mais cópias para o DAP de menor custo. Ou seja, o DDSA v2 gera menos cópias do que o necessário e a maioria delas é enviada para o DAP malicioso.

Após observar as figuras 5.9 e 5.10, fica claro que a proposta baseada em seleção probabilística de DAPs que mais se destaca é a DDSA v1. Sendo assim, é interessante compará-la agora com a proposta MDSA, que utiliza um algoritmo diferente pra seleção de DAPs. Pela Figura 5.9, é possível notar que o MDSA foi capaz de garantir a entrega de 100% das mensagens enviadas por todos os medidores em todos os cenários considerados. Por outro lado, o DDSA v1 apresentou um desempenho ligeiramente mais baixo nos cenários com DAP malicioso, obtendo entre 98 e 99% de Taxa de Entrega de Mensagens.

Observando a Figura 5.10 é possível notar que, de fato, o MDSA entrega 100% de todas as mensagens enviadas, inclusive pelos medidores mais próximos ao DAP malicioso. Por outro lado, nos cenários com DAP malicioso o DDSA v1 sofre uma pequena queda no seu desempenho, passando a entregar entre 90 e 93% das mensagens enviadas pelos

medidores mais próximos ao DAP malicioso. A queda no desempenho do DDSA v1 nos cenários com DAP malicioso se dá pelo fato de que a falha nunca é detectada pelo protocolo de roteamento, fazendo o DDSA v1 acreditar que o DAP malicioso é o melhor e, portanto, o mais provável de ser escolhido, durante todo o tempo da simulação. Por outro lado, mesmo na presença de um DAP malicioso, o MDSA continua enviando mensagens pelos demais DAPs, seguindo a política de enviar menos cópias por DAPs de melhor qualidade. Com isso, o DAP malicioso recebe menos cópias e DAPs com custo mais baixo recebem mais cópias.

5.10 Análise do *framework* THOR quanto à Latência

Como visto na seção anterior, as propostas DDSA e MDSA apresentam valores próximos para a Taxa de Entrega de Mensagens, tendo a diferença entre os dois sido de no máximo 10%, com vantagem para o MDSA. Entretanto, a Taxa de Entrega de Mensagens não é a única métrica importante a se considerar. Para algumas aplicações da IMA, a latência das mensagens é crítica, e uma mensagem muito atrasada pode ser considerada equivalente a uma mensagem perdida. Assim, é importante que a implementação do *framework* THOR não gere uma sobrecarga desnecessária na latência das mensagens.

Na Figura 5.11 é apresentado o gráfico da latência média, considerando-se as mensagens enviadas por todos os medidores. A Tabela 5.2 detalha esses resultados. Note que há uma pequena redução na latência do BestDAP entre os cenários sem falha e com DAP malicioso. Isso ocorre, pois todas as mensagens enviadas pelos medidores mais próximos ao DAP malicioso são perdidas e, portanto, não contabilizam na Latência. Também é interessante notar que a proposta DDSA v1 apresenta um aumento da latência entre os cenários sem falha e com Falha (Total e DAP Malicioso). Esse aumento ocorre devido aos medidores mais próximos ao DAP que falha. Logo após a falha, esses medidores continuam entregando suas mensagens através de DAPs alternativos. Entretanto, esses DAPs apresentam qualidade inferior ao que falhou, fazendo com que a camada de enlace tenha que efetuar mais retransmissões para entregar a mensagem, aumentando a latência desses pacotes.

Para analisar o comportamento das propostas de implementação do *framework* THOR, é interessante tomar como base o valor da latência obtido nos cenários de simulação que utilizam o BestDAP, já que nesses casos a latência obtida reflete puramente os atrasos gerados pela rede, sem nenhuma sobrecarga causada pelo THOR. É possível observar que

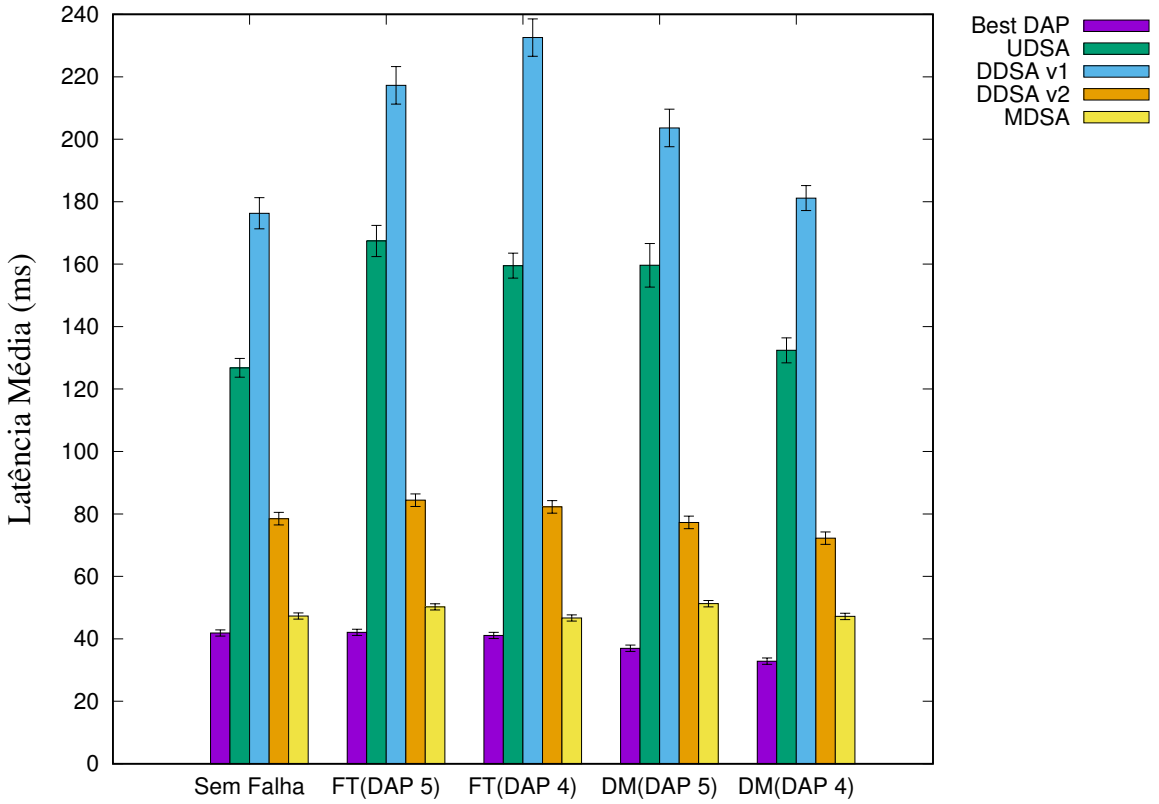


Figura 5.11: Média da Latência considerando todos os medidores.

Tabela 5.2: Média da Latência considerando todos os medidores.

		Best DAP		UDSA		DDSA v1		DDSA v2		MDSA	
Sem Falha	Média	41,89		126,79		176,3		78,49		47,32	
	Int. Conf.	1,0		3,0		5,0		2,0		1,0	
	Min.	2,93		2,93		2,93		2,93		2,93	
	Max.	83,59		1183,43		724,16		293,76		153,6	
		DAP P	DAP C	DAP P	DAP C	DAP P	DAP C	DAP P	DAP C	DAP P	DAP C
Falha Total	Média	42,07	41,07	167,42	159,52	217,25	232,56	84,41	82,27	50,24	46,69
	Int. Conf	1,0	1,0	5,0	4,0	6,0	6,0	2,0	2,0	1,0	1,0
	Min	2,93	2,0	2,93	2,0	2,93	2,0	2,93	2,0	2,93	2,0
	Max	85,16	83,0	1078,33	1559,0	837,57	830,0	496,83	293,0	221,44	295,0
DAP Malicioso	Média	36,98	32,85	159,63	132,4	203,62	181,15	77,28	72,24	51,26	47,18
	Int. Conf	1,0	1,0	7,0	4,0	6,0	4,0	2,0	2,0	1,0	1,0
	Min	2,93	2,0	2,93	2,0	2,93	2,0	2,93	2,0	2,93	2,0
	Max	82,57	82,0	10344,55	2773,0	751,75	724,0	293,76	321,0	144,71	177,0

a proposta que impõe a maior sobrecarga de latência é a DDSA v1, variando entre 134 e 191 milissegundos, de acordo com o cenário. Por outro lado, a proposta com a menor sobrecarga de latência é o MDSA, variando entre 5 e 14 milissegundos, dependendo do cenário. Essa diferença na latência entre as propostas DDSA v1 e MDSA pode ser explicada pelo número de retransmissões utilizado por elas. O DDSA v1 sempre realiza dez retransmissões para cada mensagem enviada por um medidor, enquanto que o MDSA calcula esse número automaticamente, de acordo com as condições da rede.

Pela Figura 5.12, que mostra o número de mensagens enviadas (incluindo as retrans-

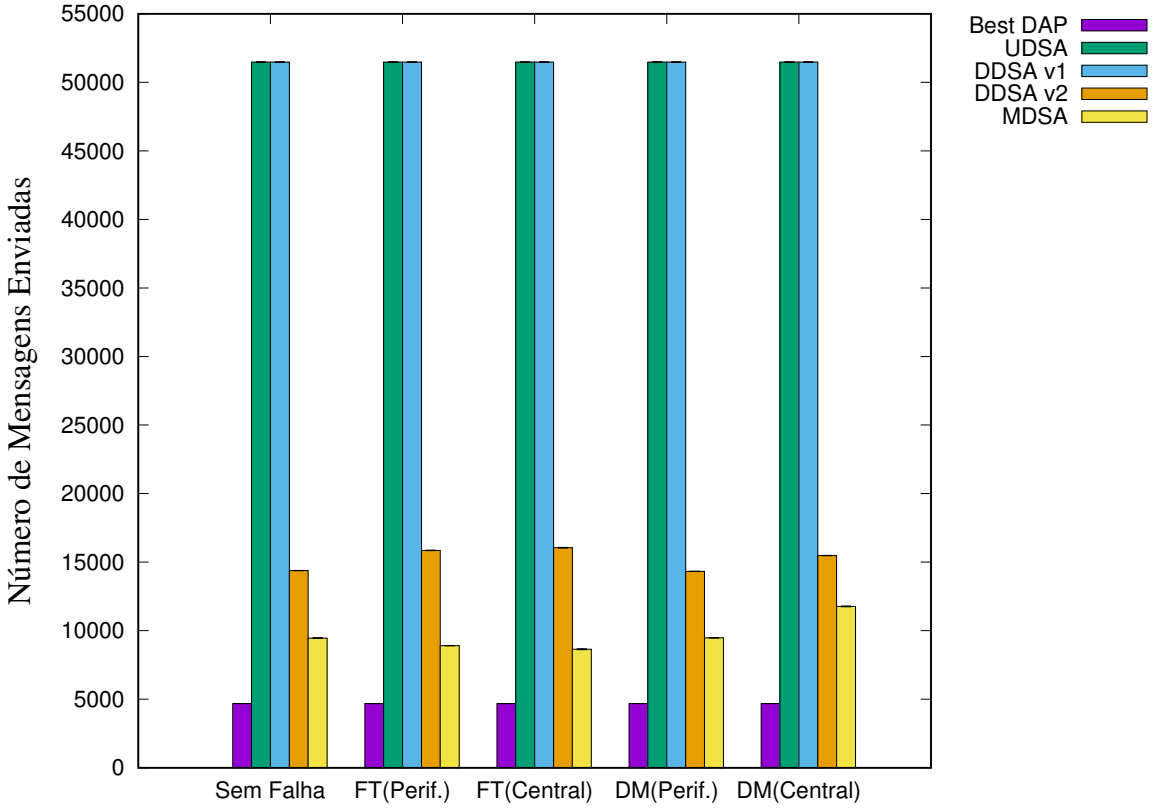


Figura 5.12: Número total de mensagens enviadas (incluindo todas as cópias) considerando-se todos os medidores.

missões), é possível verificar que o MDSA gera entre 39 e 43 mil mensagens a menos que o DDSA v1. Quanto mais mensagens são geradas, mais o meio é ocupado, aumentando o número de colisões e, consequentemente, o atraso. Essa maior contenção do meio também aumenta o número de colisões internas, já que uma mensagem passa mais tempo na fila de envio e as chances aumentam de uma nova mensagem ser gerada durante esse tempo, como ilustrado na Figura 5.13.

5.11 Conclusões do Capítulo

Após analisar a Taxa de Entrega de Mensagem e a Latência em diversos cenários, é possível concluir que o *framework* THOR tem fundamental importância para garantir a resiliência da IMA em cenários com falhas de DAP, maliciosas ou não. Dentre as propostas de implementação do *framework* THOR, aquelas que apresentaram os melhores resultados para a Taxa de Entrega de Mensagem foram o DDSA v1 e o MDSA, mas com vantagem para o MDSA, que foi capaz de entregar 100% das mensagens enviadas, até 10% mais que o DDSA v1. Do ponto de vista da Latência, o número alto de retrans-

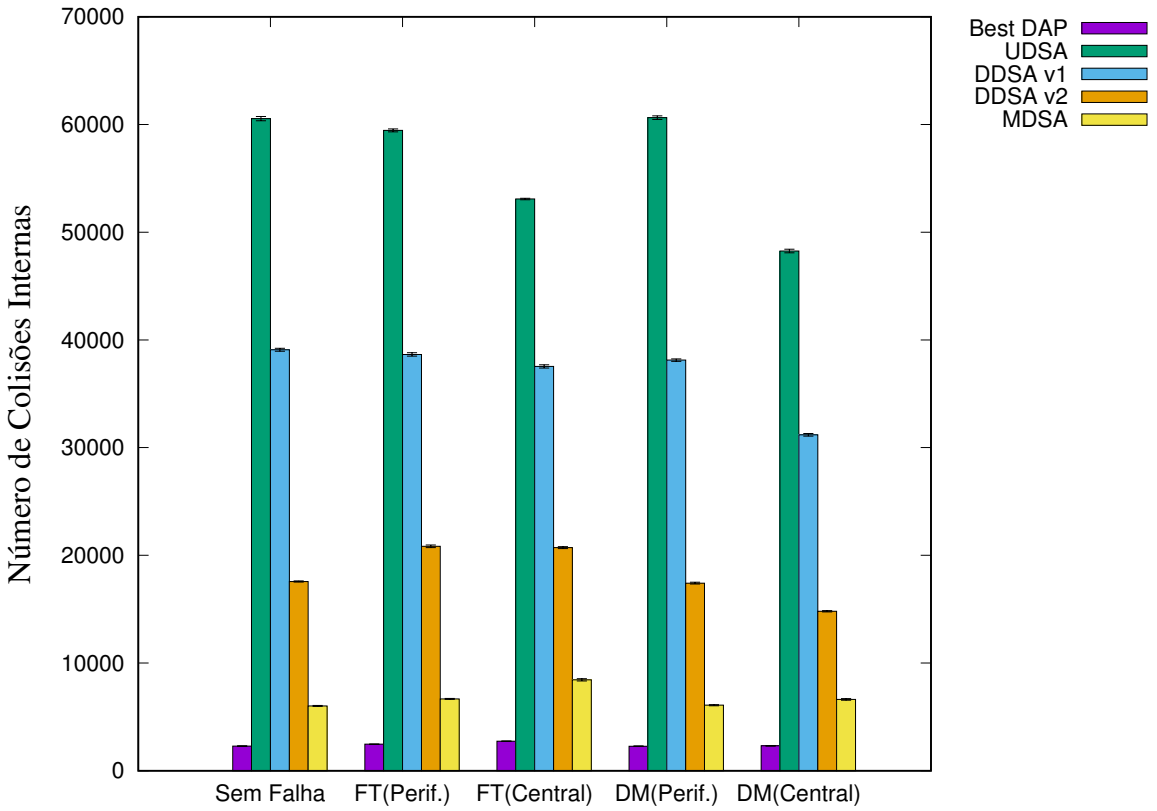


Figura 5.13: Total de colisões internas geradas nos medidores.

missões (necessário para atingir boa Taxa de Entrega de Mensagens) foi responsável por um aumento significativo na latência da rede quando o DDSA v1 foi utilizado. Por outro lado, o MDSA apresenta uma sobrecarga na latência muito menor do que a do DDSA v1, já que gera menos mensagens e, consequentemente, menos colisões internas. Com tudo isso, o MDSA se mostra como uma ótima proposta para garantir a resiliência da IMA em uma Rede Elétrica Inteligente.

Capítulo 6

Conclusão e Trabalhos Futuros

Neste trabalho, vimos que o modelo de rede elétrica que acompanha o homem moderno há aproximadamente um século está passando por profundas transformações. A evolução de tecnologias de comunicação e processamento hoje permitem que dispositivos outrora estritamente analógicos, como os medidores de energia, possam trocar informações e reagir a comandos gerados remotamente. Nessa nova realidade, operadores não precisam mais se deslocar até os consumidores para aferir o consumo de energia, consumidores passam a produzir e fornecer energia para a rede e novas soluções surgem para controlar a demanda e evitar o racionamento de energia. Para que todo esse sistema possa funcionar corretamente, é fundamental que os medidores, agora inteligentes, possam se comunicar sempre que necessário com a Central de Controle.

Uma vez que a comunicação dos medidores com o restante da rede se dá através dos agregadores (DAPs), é fundamental que, em caso de falha desses equipamentos, os medidores possam, ainda assim, manter a comunicação com a Central de Controle. Para que isso seja possível, é fundamental que a IMA seja projetada de forma que cada medidor seja coberto por mais de um DAP, garantindo redundância. Entretanto, a existência de DAPs redundantes por si só não garante a manutenção da comunicação em caso de falhas. Como visto neste trabalho, por padrão os protocolos de roteamento não tiram o melhor proveito dessa redundância, pois eles estabelecem uma única rota, aquela com o menor custo, por onde todos os pacotes serão encaminhados. Se o DAP que falha fizer parte dessa rota, então será necessário que todos os medidores detectem o problema e convirjam para uma nova rota. Enquanto isso, os pacotes enviados através do DAP com problemas são descartados, o que pode acarretar problemas sérios à estabilidade da rede elétrica, dependendo da criticidade do pacote perdido.

Para resolver esse problema, foi proposto nessa tese o *framework* THOR, que pode

ser utilizado para construir propostas que visam aproveitar a redundância de DAPs para garantir que a rede se recupere de falhas nesses equipamentos, garantindo alta taxa de entrega de pacotes e baixa latência. Além do *framework* em si, foram discutidas quatro propostas de implementação, sendo elas: UDSA, DDSA v1, DDSA v2 e MDSA. O UDSA realiza seleção probabilística de DAPs, onde cada DAP possui a mesma probabilidade de ser selecionado. Como visto, esta proposta é a que apresenta os piores resultados para a taxa de entrega de mensagens. Mesmo em um cenário sem falhas, uma vez que o UDSA seleciona DAPs com custo alto com a mesma probabilidade de DAPs com custo baixo, algumas mensagens são perdidas, reduzindo seu desempenho para esta métrica.

A segunda proposta analisada, o DDSA v1, permitiu que todos os medidores fossem capazes de entregar acima de 95% das mensagens enviadas em todos os cenários de falha. Entretanto, a eficiência do DDSA v1 em termos de taxa de entrega de mensagens tem, como contrapartida, valores altos de latência se comparados aos das propostas DDSA v2 e MDSA. O principal motivo desse baixo desempenho é que o DDSA v1 concentra a maior parte de suas retransmissões no DAP com menor custo, mas este DAP tem, em geral, alta probabilidade de entrega. Dessa forma, a maior parte das retransmissões executadas pelo DDSA v1 são desnecessárias, gerando um *overhead* na rede, o que provoca um aumento no número de colisões e, consequentemente, um aumento na latência.

O DDSA v2 foi proposto com o objetivo de sanar os problemas enfrentados pelo DDSA v1 através da utilização de uma política de retransmissão de mensagens que se adapta às condições da rede. O DDSA v2 é capaz de calcular o número de retransmissões necessário para que a mensagem enviada possa ser recebida na Central de Controle com probabilidade próxima a 100%. Entretanto, como pode ser observado nos resultados experimentais, a taxa de entrega de pacotes alcançada pelo DDSA v2 ficou abaixo daquela obtida pelo DDSA v1 quando há falha de um DAP.

Na realidade, o DDSA v2 ficou acima apenas do UDSA no cenário onde a falha do DAP foi total e ficou abaixo de todas as demais propostas no cenário onde o DAP se comportou como um buraco negro com repasse seletivo. A razão desse baixo desempenho foi o cálculo do número de retransmissões, que considera a probabilidade de entrega de todos os DAPs elegíveis, incluindo aquele que falha. Quando uma falha total ocorre, o DDSA v2 passa a calcular um número de retransmissões menor que o necessário até que a falha seja detectada e o DAP com problemas seja excluído da lista de DAPs alcançáveis. No caso de uma falha de buraco negro com repasse seletivo os resultados são ainda piores, pois a rede não é capaz de detectar a falha do DAP e o DDSA v2 calcula um número

de retransmissões ainda menor, já que o DAP malicioso informa à rede um valor para a métrica de roteamento melhor do que o real.

Por fim, o MDSA foi a proposta que apresentou os melhores resultados tanto para a taxa de entrega de mensagens quanto para a latência. Uma vez que essa proposta envia a mensagem para todos os DAPs elegíveis, ela realiza um bom aproveitamento da redundância de DAPs. Ao mesmo tempo, como o número de retransmissões para cada DAP é calculado de forma dinâmica e adaptativa, o MDSA evita o *overhead* gerado pelo DDSA v1, reduzindo o número de cópias enviadas, de colisões geradas e, como consequência, a latência na rede.

6.1 Trabalhos Futuros

Neste trabalho foram consideradas unicamente falhas em DAPs. Entretanto, uma vez que os medidores utilizam múltiplos saltos para chegar até os DAPs, a falha em um desses medidores também pode interromper a comunicação com a Central de Controle. Sendo assim, uma continuação natural do presente trabalho consiste na adição de um mecanismo que permita à rede se recuperar também de falha de medidores. Idealmente, esse mecanismo deveria ser capaz de evitar a formação de rotas para DAPs onde um mesmo medidor fizesse parte de mais de uma rota. Caso contrário, a falha em um único medidor poderia inviabilizar a redundância de DAPs existente.

Outro problema que também precisa ser tratado em trabalhos futuros é a introdução de mecanismos que garantam a privacidade, a autenticidade e a integridade das mensagens trocadas entre os medidores e a central de controle. O *framework* THOR demanda a utilização de um protocolo para descoberta de DAPs e as informações de controle trocadas nesse protocolo também precisam ser asseguradas, provavelmente utilizando algum sistema baseado em criptografia.

Por fim, além dos experimentos de simulação apresentados neste trabalho, também seria interessante avaliar as implementações do *framework* THOR em uma IMA real. Nesse sentido, no futuro nós pretendemos desenvolver uma IMA real como *testbed* para as propostas deste trabalho e de outros relacionados ao nosso grupo de pesquisa.

Referências

[1] Abid, M. R.; Khallaayoun, A.; Harroud, H.; Lghoul, R.; Boulmalf, M.; Benhaddou, D. A Wireless Mesh Architecture for the Advanced Metering Infrastructure in Residential Smart Grids. Em *2013 IEEE Green Technologies Conference (GreenTech)* (Abril 2013), páginas 338–344.

[2] Alsharif, A.; Nabil, M.; Mahmoud, M.; Abdallah, M. Privacy-Preserving Collection of Power Consumption Data for Enhanced AMI Networks. Em *2018 25th International Conference on Telecommunications (ICT)* (Junho 2018), páginas 196–201.

[3] Amin, S. M. Smart grid security, privacy, and resilient architectures: Opportunities and challenges. Em *2012 IEEE Power and Energy Society General Meeting* (Julho 2012), páginas 1–2.

[4] Araujo, J.; Lazaro, J.; Astarloa, A.; Zuloaga, A.; Garcia, A. High availability automation networks: PRP and HSR ring implementations. Em *Industrial Electronics (ISIE), 2012 IEEE International Symposium on* (2012), IEEE, páginas 1197–1202.

[5] Araujo, J. A.; Lazaro, J.; Astarloa, A.; Zuloaga, A.; Gárate, J. I. PRP and HSR for High Availability Networks in Power Utility Automation: A Method for Redundant Frames Discarding. *IEEE Transactions on Smart Grid 6*, 5 (Setembro 2015), 2325–2332.

[6] Brak, M. E.; Essaaidi, M. Wireless sensor network in smart grid technology: Challenges and opportunities. Em *2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)* (Março 2012), páginas 578–583.

[7] Bressan, N.; Bazzaco, L.; Bui, N.; Casari, P.; Vangelista, L.; Zorzi, M. The Deployment of a Smart Monitoring System Using Wireless Sensor and Actuator Networks. Em *2010 First IEEE International Conference on Smart Grid Communications* (Outubro 2010), páginas 49–54.

[8] Chang, C.; Liao, W. On Multipath Routing in Wireless Mesh Networks with Multiple Gateways. Em *2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (Dezembro 2010), páginas 1–5.

[9] Clausen, T.; Jacquet, P. Optimized Link State Routing Protocol (OLSR). `https://tools.ietf.org/html/rfc3626`. Acessado em: 19-07-2018.

[10] Dally, L.; Edwards, R. Evaluating the Communications Component of Your Smart Grid Solution. `http://www.landisgyr.com/webfoo/wp-content/uploads/2013/12/LAN-1306_WhitePaper_131210.pdf`. Acessado em: 19-03-2016.

[11] De Couto, D. S. J.; Aguayo, D.; Bicket, J.; Morris, R. A High-throughput Path Metric for Multi-hop Wireless Routing. Em *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking* (2003), páginas 134–146.

[12] do Valle, R. D. T.; Muchaluat-Saade, D. C. MeshAdmin: An integrated platform for wireless mesh network management. Em *2012 IEEE Network Operations and Management Symposium* (Abril 2012), páginas 293–301.

[13] Elma, O.; Selamoğullari, U. S. An overview of demand response applications under smart grid concept. Em *2017 4th International Conference on Electrical and Electronic Engineering (ICEEE)* (Abril 2017), páginas 104–107.

[14] Empresa de Pesquisa Energética (EPE). Balanço Energético Nacional - Relatório Final. Tech. rep., EPE, 2017.

[15] Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials 14*, 4 (Abril 2012), 944–980.

[16] Galli, S.; Scaglione, A.; Wang, Z. Power Line Communications and the Smart Grid. Em *2010 First IEEE International Conference on Smart Grid Communications* (Outubro 2010), páginas 303–308.

[17] Gao, J.; Xiao, Y.; Liu, J.; Liang, W.; Chen, C. P. A survey of communication/networking in Smart Grids. *Future Generation Computer Systems 28*, 2 (2012), 391 – 404.

[18] Garcia-Hernandez, J. Recent Progress in the Implementation of AMI Projects: Standards and Communications Technologies. Em *International Conference on Mechatronics, Electronics and Automotive Engineering - ICMEAE* (Novembro 2015), páginas 251–256.

[19] Gerk, L. F.; Muchaluat-Saade, D. C. Tuning IEEE 802.11e for wireless mesh networks. Em *2012 International Conference on Communications and Information Technology (ICCIT)* (Junho 2012), páginas 216–220.

[20] Gope, P.; Sikdar, B. An Efficient Privacy-Preserving Dynamic Pricing-based Billing Scheme for Smart Grids. Em *2018 IEEE Conference on Communications and Network Security (CNS)* (Maio 2018), páginas 1–2.

[21] Gujar, M.; Datta, A.; Mohanty, P. Smart Mini Grid: An innovative distributed generation based energy system. Em *2013 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)* (Novembro 2013), páginas 1–5.

[22] Hledik, R. How Green Is the Smart Grid? *The Electricity Journal 22*, 3 (2009), 29 – 41.

[23] Hu, X.; Lee, M. J. An efficient multipath structure for concurrent data transport in wireless mesh networks. *Computer Communications 30*, 17 (2007), 3358 – 3367.

[24] Hui, W.; Zhitao, G.; Tingting, Y.; Yue, X. Top-k query framework in wireless sensor networks for smart grid. *China Communications* (Junho 2014), 89–98.

[25] International, S. E. Smart meters Japan: TEPCO to deploy 27m by 2020 Olympic Games. `https://www.smart-energy.com/top-stories/smart-meters-japan-tepco-to-deploy-27m-by-2020-olympic-games/`, 2013. Acessado em: 29-11-2018.

[26] Jacquet, P.; Muhlethaler, P.; Clausen, T.; Laouiti, A.; Qayyum, A.; Viennot, L. Optimized link state routing protocol for ad hoc networks. Em *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International* (2001), páginas 62–68.

[27] Jhaveri, R. H.; Patel, S. J.; Jinwala, D. C. DoS Attacks in Mobile Ad Hoc Networks: A Survey. Em *2012 Second International Conference on Advanced Computing Communication Technologies* (Janeiro 2012), páginas 535–541.

[28] Karimi, B.; Namboodiri, V.; Jadliwala, M. Scalable Meter Data Collection in Smart Grids Through Message Concatenation. *IEEE Transactions on Smart Grid 6*, 4 (Julho 2015), 1697–1706.

[29] Khajavi, P.; Monsef, H.; Abniki, H. Load profile reformation through demand response programs using Smart Grid. Em *2010 Modern Electric Power Systems* (Setembro 2010), páginas 1–6.

[30] Kumar, S.; Das, N.; Islam, S. High performance communication redundancy in a digital substation based on IEC 62439-3 with a station bus configuration. Em *Power Engineering Conference (AUPEC), 2015 Australasian Universities* (2015), IEEE, páginas 1–5.

[31] Liang, X.; Li, X.; Lu, R.; Lin, X.; Shen, X. UDP: Usage-Based Dynamic Pricing With Privacy Preservation for Smart Grid. *IEEE Transactions on Smart Grid* (Março 2013), 141–150.

[32] Lopes, Y.; Saade, D. C. M.; de Albuquerque, C. V. N.; Fernandes, N. C.; Fortes, M. Z. Quality of Service for Wireless Network Implementation in Advanced Metering Infrastructure. *IEEE Latin America Transactions* (Outubro 2017), 1875–1880.

[33] Luo, Y.; He, J.; Liu, H.; Wu, L. Application of the distributed generation, micro and smart power grid in the urban planning. Em *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent* (Junho 2014), páginas 634–637.

[34] Mahmud, A. S. M. A.; Sant, P. Real-time price savings through price suggestions for the smart grid demand response model. Em *2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG)* (Abril 2017), páginas 65–69.

[35] Mohammed, H.; Tonyali, S.; Rabieh, K.; Mahmoud, M.; Akkaya, K. Efficient Privacy-Preserving Data Collection Scheme for Smart Grid AMI Networks. Em *2016 IEEE Global Communications Conference (GLOBECOM)* (Dezembro 2016), páginas 1–6.

[36] Nandiraju, D. S.; Nandiraju, N. S.; Agrawal, D. P. Adaptive state-based multi-radio multi-channel multi-path routing in Wireless Mesh Networks. *Pervasive and Mobile Computing 5*, 1 (2009), 93 – 109.

[37] Nandiraju, N. S.; Nandiraju, D. S.; Agrawal, D. P. Multipath Routing in Wireless Mesh Networks. Em *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems* (Outubro 2006), páginas 741–746.

[38] Natural Resources Canada, U.S. Department of Energy. Final Report on the Implementation of the Task Force Recommendations. Tech. rep., Natural Resources Canada and U.S. Department of Energy, Setembro 2006.

[39] Nguyen-Dinh, N.; Kim, G.-S.; Lee, H.-H. A study on GOOSE communication based on IEC 61850 using MMS ease lite. Em *2007 International Conference on Control, Automation and Systems* (Outubro 2007), páginas 1873–1877.

[40] NIST. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. `http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf`. Acessado em: 03-07-2016.

[41] Okabayashi, V. H.; Ribeiro, I. C. G.; Passos, D.; Albuquerque, C. V. N. A Resilient Dynamic Gateway Selection Algorithm Based on Quality Aware Metrics for Smart Grids. Em *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems* (2015), páginas 91–98.

[42] Passos, D.; Albuquerque, C. V. N. A Joint Approach to Routing Metrics and Rate Adaptation in Wireless Mesh Networks. Em *IEEE INFOCOM Workshops 2009* (Abril 2009), páginas 1–2.

[43] Ravichandran, A.; Malysz, P.; Sirouspour, S.; Emadi, A. The critical role of microgrids in transition to a smarter grid: A technical review. Em *IEEE Transportation Electrification Conference and Expo (ITEC)* (Junho 2013), páginas 1–7.

[44] Ravichandran, A.; Malysz, P.; Sirouspour, S.; Emadi, A. The critical role of microgrids in transition to a smarter grid: A technical review. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)* (Novembro 2015), páginas 205–2010.

[45] Rogge, H.; FKIE, F.; Baccelli, E.; Kaplan, A. Packet Sequence Number based ETX Metric for Mobile Ad Hoc Networks. `https://tools.ietf.org/html/draft-funkfeuer-manet-olsrv2-etx-01`. Acessado em: 20-02-2018.

[46] Rolim, G.; Passos, D.; Albuquerque, C.; Moraes, I. Moskou: A heuristic for data aggregator positioning in smart grids. *IEEE Transactions on Smart Grid 9*, 6 (2018), 6206–6213.

[47] Rolim G., Passos D., Albuquerque C. Modelling the Data Aggregator Positioning Problem in Smart Grids. páginas 632–639.

[48] Roser, M.; Ortiz-Ospina, E. World Population Growth. `https://ourworldindata.org/world-population-growth`. Acessado em: 12-11-2018.

[49] Saebi, J.; Javidi, M. H. Implementation of demand response in different control strategies of smart grids. Em *Iranian Conference on Smart Grids* (Maio 2012), páginas 1–4.

[50] Salami, A.; Farsi, M. M. A cooperative demand response program for smart grids. Em *2015 Smart Grid Conference (SGC)* (Dezembro 2015), páginas 99–104.

[51] Saleh, M. S.; Althaibani, A.; Esa, Y.; Mhandi, Y.; Mohamed, A. A. Impact of clustering microgrids on their stability and resilience during blackouts. Em *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)* (Outubro 2015), páginas 195–200.

[52] Shiobara, T.; Palensky, P.; Nishi, H. Effective metering data aggregation for smart grid communication infrastructure. Em *IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society* (Novembro 2015), páginas 2136–2141.

[53] Silva, B.; Passos, D.; Albuquerque, C. Reducing the Variability in Routing Decisions in Wireless Mesh Networks. Em *2018 IEEE Symposium on Computers and Communications (ISCC)* (Junho 2018), páginas 504–507.

[54] Sinha, A. K.; Kumar, N. Demand response managemengt of smart grids using dynamic pricing. Em *2016 International Conference on Inventive Computation Technologies (ICICT)* (Agosto 2016), páginas 1–4.

[55] Sofla, M. A.; King, R. Control method for multi-microgrid systems in smart grid environment—Stability, optimization and smart demand participation. Em *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)* (Janeiro 2012), páginas 1–5.

[56] Subhash, B.; Rajagopal, V. Overview of smart metering system in Smart Grid scenario. Em *2014 POWER AND ENERGY SYSTEMS: TOWARDS SUSTAINABLE ENERGY* (Março 2014), páginas 1–6.

[57] Tashtarian, F.; Montazerolghaem, A.; Abbasi, M. Distributed Lifetime Optimization of Wireless Sensor Networks in Smart Grid. Em *2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE)* (Agosto 2018), páginas 240–243.

[58] TCU. Impacto do apagão para consumidores/contribuintes. Tech. rep., TCU, Julho 2009.

[59] Ur-Rehman, O.; Zivic, N.; Ruland, C. Security issues in smart metering systems. Em *2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE)* (Agosto 2015), páginas 1–7.

[60] U.S. Department of Energy. Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investiment Grant Program. Tech. rep., U.S. Department of Energy, Setembro 2016.

[61] Xu, S.; Qian, Y.; Hu, R. Q. Reliable and resilient access network design for advanced metering infrastructures in smart grid. *IET Smart Grid 1*, 1 (2018), 24–30.

[62] Yaghmaee, M. H.; Kouhi, M. S.; Garcia, A. L. Personalized pricing: A new approach for dynamic pricing in the smart grid. Em *2016 IEEE Smart Energy Grid Engineering (SEGE)* (Agosto 2016), páginas 46–51.

[63] Yang, H.; Zhang, J.; Qiu, J.; Zhang, S.; Lai, M.; Dong, Z. Y. A Practical Pricing Approach to Smart Grid Demand Response Based on Load Classification. *IEEE Transactions on Smart Grid* (Janeiro 2018), 179–190.

[64] Ye, Z.; Krishnamurthy, S. V.; Tripathi, S. K. A framework for reliable routing in mobile ad hoc networks. Em *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies* (Março 2003), vol. 1, páginas 270–280.

[65] Yi, J.; Adnane, A.; David, S.; Parrein, B. Multipath optimized link state routing for mobile ad hoc networks. *Ad Hoc Networks 9*, 1 (2011), 28 – 47.

[66] Yussof, S.; Rusli, M. E.; Yusoff, Y.; Ismail, R.; Ghapar, A. A. Financial impacts of smart meter security and privacy breach. Em *Proceedings of the 6th International Conference on Information Technology and Multimedia* (Novembro 2014), páginas 11–14.