André Zimmermann

Arquitetura para Ganho de Eficiência Energética em Redes de Sensores Sem Fios de Próxima Geração

Florianópolis - SC

2008

UNIVERSIDADE FEDERAL DE SANTA CATARINA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

André Zimmermann

Arquitetura para Ganho de Eficiência Energética em Redes de Sensores Sem Fios de Próxima Geração

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

Orientador:

Prof. Dr. João Bosco Mangueira Sobral

Florianópolis, Junho de 2008

Arquitetura para Ganho de Eficiência Energética em Redes de Sensores Sem Fios de Próxima Geração

André Zimmermann

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Dr. Mario Antonio Ribeiro Dantas

Coordenador do Curso

Banca Examinadora

Prof. Dr. João Bosco Mangueira Sobral (Orientador)

Prof. Dr. Jorge Sá Silva

Prof. Dr. Carlos Barros Montez

Prof. Dr. Roberto Willrich

Agradecimentos

Aos meus progenitores e primeiros educadores, Lilian e Adonis, pela formação do meu caráter, pelo amor e apoio em meus projetos.

À Rode Anélia Martins, pelo inspirador exemplo de vida, pelo companheirismo, carinho e suporte incondicional.

À Verinha e seu *staff* que, por todos estes anos, com paciência e bom humor, responderam a tantas questões e resolveram tantos problemas.

Ao meu orientador, João Bosco Mangueira Sobral e aos amigos do grupo de investigação *Distributed Mobile Computing & Network Security*, em especial à Mestre Kathia Jucá, pelo incentivo à seguir a carreira acadêmica.

Ao Professor Jorge Sá Silva e aos amigos do Laboratório de Comunicação e Telemática do Centro de Informática e Sistemas da Universidade de Coimbra, pelas inspiradoras conversas e excelente ambiente de aprendizado. Agradeço em especial aos amigos Eduardo Cerqueira e Ricardo Silva pela frutífera parceria nas publicações.

Ao pessoal adepto à edição de textos LaTeX, meus amigos Adriano Fiorese, Fernando Matos, Rogério da Silva, Vinícius da Cunha e Lucas Gualdarben pela ajuda na resolução de problemas de compilação e dicas de formatação.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

6GLAD - Global to Link-layer Address Translation for 6LoWPAN Overhead Reduction

6LoWPAN - IPv6 Over Low Power Personal Area Networks

BAN - Body Area Networks

BSN - Data Sequence Number

CAP - Contention Access Period

CFP - Contention Free Period

CSMA-CA - Carrier Sense Multiple Access with Collision Avoidance

DNS-ALG - Domain Name Server – Application Level Gateway

DSN - Beacon Sequence Number

FFD - Fully-function Device

GTS - Guaranteed Time Slots

IETF - Internet Engineering Task Force

IETF-WG - Internet Engineering Task Force Working Group

IPv6 - Internet Protocol versão 6

LoWPAN HC1 - Low Power Wireless Personal Area Network Header Codification Type 1

MTU - Maximum Transfer Unit

NAT - Network Address Translation

RFC - Request for Comments

RFD - Reduced-function Device

RSSF - Rede de Sensores Sem Fios

UWB - Ultra Wide Band

WPAN - Wireless Personal Area Network

Resumo

A Nova Geração de Redes de Sensores Sem Fios irá integrar sistemas de comunicação além terceira geração. Como resultado desta integração, estes novos sistemas de comunicação serão alimentados pelas Redes de Sensores com informação colhida do ambiente, tornando-se cientes do contexto. Para alcançar a necessária conectividade entre redes IP e Redes de Sensores, o grupo de trabalho 6LoWPAN da *Internet Engineering Task Force* projetou uma camada de adaptação IPv6 para dispositivos de capacidades restritas. Esta pilha protocolar provê aos nós sensores interoperabilidade IPv6, evitando sobrecarga protocolar tanto quanto possível. Nesta dissertação, foram analisados e avaliados os possíveis cenários de comunicação IPv6 em Redes de Sensores sem Fios. Estas analises levaram a conclusão que, mesmo o 6LoWPAN sendo uma solução IPv6 leve o suficiente para ser executado em nós sensores, em cenários de comunicação global, isto é, quando há necessidade de utilização de endereçamento IPv6 globais e únicos, a sobrecarga protocolar é significativa e novas abordagens devem ser propostas. A fim de evitar sobrecarga de comunicação em Redes de Sensores Sem Fios quando há necessidade de comunicação com diferentes redes, foi proposta uma arquitetura que explora as técnicas do 6LoWPAN para supressão de cabeçalhos através de mecanismos de tradução transparente de endereços, alcançando maior eficiência energética.

Palavras-chave: Redes de Sensores Sem Fios, 6LoWPAN, Eficiência Energética.

Abstract

The next generation of wireless sensor networks will integrate communication systems beyond third generation paradigm. As a result of this integration, the new communication systems will be feed by the sensor networks with information gathered from the environment, achieving context awareness. To reach the necessary end-to-end connectivity between all-IP networks and sensor networks, the IETF 6LoWPAN working group designed an IPv6 adaptation layer for low power, low cost, low bit rate and short range devices. This protocol stack provides to the sensor networks IPv6 interoperability, avoiding overhead as much as possible. This document analyses and evaluates the associated IP overhead in different 6LoWPAN scenarios, from intra to inter network communication. We conclude that, even the 6LoWPAN being a light weight IP solution for link local sensor network communication, when data flows between different networks the overhead is too high and new approaches must be proposed. In order to avoid communication overhead when global IPv6 addressing is necessary in resource constrained networks, we propose an architecture to exploit 6LoWPAN crosslayering techniques to relief constrained networks from IP unnecessary headers through transparent address translation mechanisms.

Keywords: Wireless Sensor Networks, 6LoWPAN, Energy Awareness.

1 Introdução

Uma típica Rede de Sensores Sem Fios (RSSF) é formada por um conjunto de dispositivos, conhecidos como nós sensores. Estes equipamentos possuem capacidade de processamento, armazenamento e memória equivalentes à computadores pessoais do início dos anos noventa [HILL, 2000] e tipicamente são alimentados por baterias. Este nós são dotados de dispositivos sensores para mensurar os mais variados fenômenos, tais como: luminosidade, temperatura, pressão, ruído, aceleração, posição geográfica, radioatividade, componentes químicos, entre outros [KARL, 2005].

A comunicação é estabelecida por meio de interfaces de rede sem fio, para economizar energia, um dos maiores desafios quando se trabalha com RSSF, o rádio opera em baixa potência e em baixas taxas de transmissão. Tipicamente, o alcance do rádio de um nó sensor é de poucas dezenas de metros e a taxa de transmissão umas poucas dezenas de kilobits por segundo. O padrão IEEE 802.15.4, que vem tornando-se um padrão de indústria, provê taxas de transmissão nominais de até 250 kbps, operando na faixa dos 2.4 GHz [IEEE, 2006].

As RSSF podem ser utilizadas em uma série de aplicações, tais como: monitoramento ambiental, sensoreamento urbano, monitoramento de estruturas, automação predial e industrial, aplicações militares, tele-medicina, agricultura de precisão, logística, entre outros. Com a diminuição do custo dos nós sensores e a simplificação na operação e programação das plataformas a tendência é que as RSSF comecem a ser cada vez mais comuns. Estas proliferação e simplificação habilitarão utilizadores finais a tornar os dados coletados por suas RSSF disponíveis na Internet e qualquer pessoa autorizada poderá consultar via algum mecanismo de busca tipo Google [ESTRIN, 1999, p. 263–270]. Deste modo, as diversas RSSF colaboram para expandir

as fronteiras da Internet até o mundo físico.

Esta conectividade pode ser atingida por *proxies* que façam a tradução dos protocolos proprietários para IP ou por soluções baseadas em servidores web, como já foi proposto por [ESTRIN, 1999, p. 263–270] e [ZUNIGA, 2003], entre outros. A abordagem de se utilizar protocolos proprietários interfaceados por um servidor web pode representar para a RSSF uma economia em termos energéticos. Mas, tipicamente acarreta maior esforço de desenvolvimento. Por outro lado, a utilização de nós sensores que utilizem tecnologia IP traz como vantagem a utilização de uma infra-estrutura existente, bem conhecida e largamente utilizada. Além disso, protocolos Internet possuem padrões abertos e já contamos com uma diversidade de ferramentas para gerência e diagnóstico [KUSHALNAGAR, 2007].

O Protocolo Internet versão 6 (IPv6), padronizado pela norma RFC 2460 [DEERING, 1998], foi projetado para ser o sucessor da atual tecnologia de *internetworking*, o IP versão 4. As principais inovações trazidas foram o espaço de endereçamento alargado dos 32, na versão 4, para 128 bits na versão 6, representando 10 quatrilhões mais endereços. Isto afasta a possibilidade de exaustão de endereços sem necessidade de recorrer a técnicas de tradução de endereços que retirem a unicidade de endereços ou de *Classless Inter-Domain Routing* (CIDR), que torna as tabelas de encaminhamento mais complexas. Mais que a notória diferença no espaço de endereçamento, a versão 6 do protocolo IP incorpora de forma nativa mecanismos de segurança, comunicação multicast, mobilidade, maior simplicidade no encaminhamento e, vez que a parte do endereço correspondente ao dispositivo de rede é independente da parte que identifica a rede, é possível também que os dispositivos de rede se autoconfigurem [NARTEN, 2007].

Os protocolos desenvolvidos para RSSF devem possuir o melhor desempenho em termos de consumo energético, utilização de memória e processador. As tecnologias IP provêem conectividade global de forma transparente e demandam menor esforço de implementação. No entanto, não se apresentam como uma alternativa competitiva, face aos protocolos específicos para dispositivos de baixas capacidades. Neste sentido, o grupo de trabalho do Internet Engineering Task Force (IETF) para desenvolvimento do IPv6 para redes pessoais de baixo poder

de processamento, do original *IPv6 Over Low Power Personal Area Networks* (6LoWPAN) tem trabalhado em questões como diminuição do cabeçalho IPv6, fragmentação e remontagem de pacotes, auto-configuração e mobilidade, de forma a disponibilizar uma pilha protocolar que possa ser suportada pelas RSSF [MONTENEGRO, 2007].

O 6LoWPAN promove uma significativa redução nos gastos energéticos com sinalização IPv6 por meio de uma camada de adaptação com uma abordagem de carregar somente os cabeçalhos necessários para o cenário em questão. Esta filosofia promove, no melhor caso, uma redução no cabeçalho IPv6 de 40 bytes para 3 bytes. No entanto, nos cenários de conectividade global, isto é, quando os nós sensores utilizem endereços IPv6 globais, a eficiência do 6LoWPAN é significativamente reduzida.

1.1 Objetivos

O objetivo deste trabalho é a proposição de uma arquitetura para melhorar a eficiência energética, na camada de rede, em Redes de Sensores Sem Fios conectadas à Internet. A arquitetura deve manter a conectividade IPv6 - 6LoWPAN com transparência, sem acarretar custos extras nos nós sensores.

Objetivos Específicos

Como objetivos específicos, podemos citar:

- O estudo dos fatores que contribuem para o aumento de sinalização no 6LoWPAN assim como seus mecanismos de supressão de cabeçalhos;
- O estudo e utilização dos padrões e normas que contribuam para alcançar a redução na sobrecarga protocolar do 6LoWPAN;
- A escolha e o domínio das ferramentas de simulação, dos equipamentos e dos softwares para validação da arquitetura proposta;
- A proposta de mecanismos que proporcionem economia na utilização da largura de banda

e que tenham menor impacto na bateria dos nós sensores.

Justificativa e Resultados Esperados

As técnicas de compressão de cabeçalhos IPv6, RFC 4944 [MONTENEGRO, 2007], reduzem significativamente a sobrecarga de comunicação do IPv6 e a abordagem de pagar só pelo necessário na camada de adaptação proposta pela mesma RFC apontam o 6LoWPAN como uma tecnologia promissora para o surgimento de uma nova geração de RSSF [CULLER, 2007]. No entanto, o cenário onde o 6LoWPAN é energeticamente mais eficiente não oferece conectividade global, isto é, utiliza endereçamento IPv6 tipo *link-local*. Desta maneira, os mecanismos 6LoWPAN de supressão de cabeçalho Ipv6 podem reduzir 32 bytes dos 40 bytes originais, uma vez que os endereços Ipv6 de origem e destino podem ser reconstituídos a partir da camada 2.

Esta característica levou-nos a propor uma arquitetura, a qual denominamos *Global to Link-layer Address Translation for 6LoWPAN Overhead Reduction* (6GLAD), para explorar os mecanismos de compressão de cabeçalhos do 6LoWPAN enquanto transparentemente mantemos a conectividade IPv6 em escala global [ZIMMERMANN, 2008a]. O resultado esperado da utilização desta arquitetura é a redução no consumo energético e na utilização da largura de banda em redes de sensores sem fios.

1.2 Metodologia

Iniciamos este trabalho com o estudo da proposta do IETF para habilitar IPv6 em dispositivos de baixo poder de processamento e memória, isto é, o 6LoWPAN. Procedemos a uma análise teórica do *overhead* associado aos possíveis cenários 6LoWPAN para Redes de Sensores Sem Fios, isto levou-nos a constatação de que ainda há cenários com alto *overhead* associado. O conhecimento dos mecanismos adotados pelo 6LoWPAN e do custo de comunicação associado a cada cenário, guiou-nos na proposição da arquitetura.

A avaliação da arquitetura proposta deu-se em duas fases: O impacto em termos de consumo de largura de banda foi medido por meio do simulador Network Simulator-2 e o impacto em termos

energéticos foi avaliado utilizando-se uma plataforma de testes com nós sensores Crossbow MicaZ.

1.3 Limitações

Neste trabalho foi considerado apenas um ponto de conexão com a Internet, portanto o *gateway* é um ponto único sujeito à falhas. Consideramos também que o *gateway* tem memória e poder computacional suficiente para fazer as traduções e manter as tabelas de associação de endereços. Assumimos ainda, que o nó que executa o agente 6GLAD está energizado, portanto não nos preocupamos com o consumo energético deste. Além disso, questões relacionadas a segurança e qualidade de serviço em redes IPv6 não são tratadas neste trabalho.

1.4 Estrutura da Dissertação

O restante desta dissertação está organizado da forma que segue: No Capítulo 2 são apresentadas com detalhes as características e funcionalidades de cada camada da pilha protocolar 6LoWPAN e da tecnologia de comunicação sem fios IEEE 802.15.4. No Capítulo 3 é mostrado o estudo da sobrecarga protocolar relacionado a cada cenário 6LoWPAN possível. No Capítulo 4 é apresentada a estrutura da arquitetura proposta e os padrões IETF envolvidos. O Capítulo 5 trata da avaliação e resultados obtidos e o Capítulo 6 tece conclusões e propõe trabalhos futuros.

1.5 Publicações

Os estudos empreendidos no decorrer deste mestrado levaram à publicação de 2 artigos. O primeiro, intitulado *6GLAD: IPv6 Global to Link-layer ADdress Translation for 6LoWPAN Overhead Reducing* aborda estudos acerca da sobrecarga protocolar do 6LoWPAN e a proposição de uma arquitetura para explorar os mecanismos de supressão de endereços do 6LoWPAN, apresentada no Capítulo 4 desta dissertação. Este paper foi publicado no *4th EURO-NGI Conference on Next Generation Networks*, na Cracóvia, Polônia [ZIMMERMANN, 2008a].

O segundo trabalho foi publicado no 10º Workshop Brasileiro de Tempo Real e Sistemas Embarcados, no Rio de Janeiro, sob o título *An Efficient Communication Control Approach for Next Generation Wireless Sensor Networks* [ZIMMERMANN, 2008b]. Este artigo apresenta os resultados de simulação e prototipagem da arquitetura 6GLAD com os respectivos impactos em termos de consumo de largura de banda e consumo de bateria.

2 *Redes de Sensores Sem Fios Globalmente Interconectadas*

Tipicamente, as aplicações que fazem acesso aos dados de uma RSSF precisam utilizar um servidor *web* ou um *proxy* para traduzir as consultas feitas pela Internet para os protocolos proprietários utilizados nos nós sensores. Com o custo por nó sendo reduzido e as plataformas tornando-se mais simples de serem operadas, estas aplicações se tornarão mais e mais comuns. Com a proliferação e simplificação das RSSF, utilizadores sem experiência prévia estarão habilitados a tornarem os dados coletados por suas RSSF disponíveis na Internet e qualquer pessoa autorizada poderá encontrá-los via algum mecanismo de busca ao estilo do *Google* [ESTRIN, 1999, p. 263–270].

Soluções para disponibilizar os dados das RSSF via *proxies* proprietários ou servidores *web* foram propostas, entre outros, por [ESTRIN, 1999, p. 263–270] e [ZUNIGA, 2003]. Isto pode resolver problemas específicos de uma aplicação e normalmente requer um esforço de desenvolvimento maior. Por outro lado, a utilização de IPv6 em RSSF traz algumas vantagens face ao paradigma proprietário. Primeiramente, a natureza pervasiva das redes IP permite a integração das RSSF a uma infra-estrutura largamente utilizada, de funcionamento comprovado e bem conhecida. Segundo, a pilha protocolar é de especificação aberta, assim como as ferramentas para diagnose e gerência, evitando assim demasiado esforço de desenvolvimento. Por último, dispositivos que suportem IP podem ser conectados prontamente e de forma transparente a um mundo de outros equipamentos [KUSHALNAGAR, 2007].

Nas próximas seções serão apresentadas as camadas da pilha protocolar 6LoWPAN e IEEE 802.15.4.

2.1 IEEE 802.15.4

O IEEE 802.15.4 é um conjunto de especificações para dispositivos de capacidades restritas. Foi desenhado para ser utilizado em WPAN (Wireless Personal Area Network) com taxas de transmissão de até 250 Kbps a 2.4 GHz, 40 Kbps a 916 MHz e 20 Kbps a 868 MHz [IEEE, 2003]. Há também outra especificação, liberada sob o padrão IEEE 802.15.4a, para rádios que operem em UWB (Ultra Wide Band) e a IEEE 802.15.4-2006, também conhecida como IEEE 802.15.4b que cobre funcionalidades extras, simplificações e melhorias, enquanto mantém compatibilidade com o padrão IEEE 802.15.4.

As melhorias trazidas pelo padrão de 2006 foram a adição de mecanismos de *time stamping*, a extensão das modulações da freqüência dos 2.4GHz também para freqüências mais baixas, aumentando as taxas de transmissão, o suporte de escalonamento de *beacons*, melhora o uso das técnicas de criptografia e permite o envio de mensagens *broadcast* de forma sincronizada, entre outras [IEEE, 2006].

2.1.1 A camada física do IEEE 802.15.4

Na freqüência dos 2450MHz, uma faixa quase mundial de uso sem necessidade de licença, há 16 canais de comunicação. Na faixa dos 915MHz, que não requer licença na América do Norte, há 10 canais e, por fim, na faixa dos 868MHz, que não requer licença na Europa, há um canal.

A norma IEEE 802.15.4b, de 2006, introduziu o esquema de modulação O-QPSK e ASK nas freqüências de 868MHz e 915MHz. Contudo, uma vez que a compatibilidade precisa ser mantida com a versão de 2003, qualquer dispositivo IEEE 802.15.4b que esteja operando com estes tipos de modulação deve voltar a operar em BPSK se houver comunicação com outro que esteja a operar com esta modulação. As características de cada uma das faixas de freqüência do IEEE 802.15.4 podem ser consultadas na Tabela 2.1.

A camada física do padrão IEEE 802.15.4 é composta por um preambulo de 4 bytes para sin-

PHY (MHz)	Banda de freqüência (MHz)	Parâmetros de dispersão		Parâmetros de dados		
		(Kchip/s)	Modulação	Taxa de bits (kbps)	Taxa de símbolos (ksymbol/s)	Símbolos
868/915	868 – 868.6	300	BPSK	20	20	Binário
	902 – 928	600	BPSK	40	40	Binário
868/915 (opcional)	868 – 868.6	400	ASK	250	12.5	20-bit PSSS
	902 - 928	1600	ASK	250	50	5-bit PSSS
868/915 (opcional)	868 – 868.6	400	O-QPSK	100	25	16-ary Ortogonal
	902 - 928	1000	O-QPSK	250	62.5	16-ary Ortogonal
2450	2400 – 2483.5	2000	O-QPSK	250	62.5	16-ary Ortogonal

Tabela 2.1: *Características do padrão IEEE 802.15.4b*

cronização dos símbolos. Um byte para marcar o inicio de um quadro. Um byte de cabeçalho, sendo 7 bits para especificar o *Service Data Unit Length*, isto é o tamanho do quadro e 1 bit de uso reservado. A Figura 2.1 apresenta a organização de um frame IEEE 802.15.4.

4 Bytes	1 Byte	1 Byte	Até 127 Bytes
Preâmbulo	Início do delimitador	Cabeçalho PHY	Unidade de serviço de dados PHY

Figura 2.1: *Camada Física do Padrão IEEE 802.15.4*

2.1.2 A Camada de Acesso ao Meio do IEEE 802.15.4

A sub-camada de controle de acesso ao meio é responsável pelos serviços de dados e gerência da camada física. Por meio do envio de quadros (*frames*) com confirmação de recepção (*acknowledged frames*) e criptografia, a sub camada de acesso ao meio do padrão IEEE 802.15.4 provê mecanismos para tornar seguro e confiável a ligação entre pares. Esta camada ainda é responsável pela gerência dos pacotes de *beacon*, das entradas e saídas de nós da rede e dos mecanismos de GTS (*Guaranteed Time Slots*) A Figura 2.2 mostra o formato de um quadro IEEE 802.15.4. Nas subseções que seguem serão apresentados cada um dos campos e suas funções.

Controle do Frame	Seqüencial	Endereçamento	Área de Dados	Verificação do quadro
2 bytes	1 byte	variável	variável	2 bytes
Cabeçalho MAC			MAC Payload	Rodapé MAC

Figura 2.2: *Camada de Acesso ao Meio do Padrão IEEE 802.15.4*

Campo de Controle do Quadro

O campo de controle do quadro *frame control* é composto por 2 bytes, contém sinalizadores (*flags*), campos de endereçamento e o tipo do quadro. A organização deste campo pode ser vista na Tabela 2.2.

bit	Campo	Observações
0	**Frame Type**	O tipo do quadro especifica um dos quatro possíveis tipos de quadros MAC: Beacon = 000, Dados = 001, Aviso = 010, Comando = 011. Os outros quatro valores possíveis, a partir de 100 a 111, são reservados.
1		
2		
3	**Security Enabled**	Se estiver definido para 1 a proteção criptográfica está ligada.
4	**Frame Pending**	Se estiver definido para 1 significa que há mais dados para enviar.
5	**Ack Req.**	Se estiver definido para 1 o nó de destino deve confirmar o recebimento.
6	**Intra PAN**	1 para a comunicação intra PAN. Não carrega endereçamento da PAN.
7	**Reserved**	
8		
9		
10	**Destination Address mode**	00 = Sem endereço, o destino do quadro será o coordenador. 10 = endereço de 16 bits, 11 = endereço de 64 bits.
11		
12	**Reservado**	
13		
14	**Source Address mode**	00 = Sem endereço, a origem do quadro é o coordenador. 10 = endereço de 16 bits, 11 = endereço de 64 bits.
15		

Tabela 2.2: *Campos para o Controle do Quadro*

Campo do Número Seqüencial

Com 1 byte, este campo é usado para identificar o quadro. Se for um quadro tipo *Beacon*, este campo será o *Beacon Sequence Number* (BSN). Analogamente, caso seja um quadro de dados, comandos ou confirmação (*acknowledgement*) este será o *Data Sequence Number* (DSN). Cada

dispositivo da rede inicializa este campo com um número aleatório, mantém-no em uma variável e incrementa-o para cada quadro gerado. Quando um quadro tem seu campo de requisição de confirmação (*acknowledgment request field*) com o valor 1, o destinatário do quadro deverá enviar um quadro de confirmação com o valor do BSN ou DSN do quadro recebido.

Campos de Endereçamento

Os campos de endereçamento de um quadro IEEE 802.15.4 podem ser vistos na Figura 2.3 e abrangem os seguintes campos:

- **Identificador da PAN de Destino**

  O identificador da rede de destino, quando presente, possui 16 bits e especifica a PAN do destinatário de um quadro. Um quadro com origem e destino dentro da própria PAN, não possui este identificador. O valor 0xFFFF é o endereço de *broadcast*, se este campo contiver este endereço, o quadro deve ser aceito por qualquer dispositivo que esteja ouvindo o canal.

- **Endereço de Destino**

  O endereço de destino de um quadro, se presente, o tamanho deste campo é especificado pelo campo *Destination Address Mode* e pode ser de 16 ou 64 bits. O valor 0xFFFE significa que o dispositivo não possui um endereço de 16 bits associado e o valor 0xFFFF é reservado para comunicação em *broadcast*. Se o campo não existir, significa que o quadro deve ser entregue ao coordenador da rede.

- **Identificador da PAN de Origem**

  O identificador da rede de origem, quando presente, possui 16 bits especifica a PAN de origem de um quadro. Um quadro com origem e destino dentro da própria PAN, não possui este identificador. Este identificador é determinado pelo dispositivo coordenador no momento de configuração da rede e é comunicado a cada dispositivo no momento em que este associa-se à rede.

- **Endereço de Origem**

  O endereço de origem, se presente, tem o tamanho especificado pelo campo *Destination Address Mode* e pode ser de 16 ou 64 bits. Quando este campo não existe, significa que o quadro teve origem no coordenador.

ID da PAN de Destino	Endereço de Destino	ID da PAN de Origem	Endereço de Origem
0/2 bytes	0/2/8 bytes	0/2 bytes	0/2/8 bytes

Figura 2.3: *Campos de endereçamento da camada 2*

Campo de Dados (*Frame payload field*)

Este campo é o responsável pelo porte da informação propriamente dita. O tamanho é variável, uma vez que o tamanho dos outros campos é variável, assim como a quantidade de informação transmitida. Um quadro IEEE 802.15.4, incluindo cabeçalhos, tem no máximo 127 bytes. Este campo pode estar cifrado, neste caso, o campo *Security enabled* deve estar com valor igual a 1.

Campo de Checagem do Quadro (*Frame Check Sequence Field*)

É o rodapé do quadro, contém os 16 bits do resultado da aplicação de uma função *hash* calculada sobre todo o quadro. Este campo é útil para detectar erros de transmissão causados por interferências no canal de transmissão sem fios.

2.1.3 O Esquema de Endereçamento IEEE 802.15.4

Dispositivos IEEE 802.15.4 possuem endereços físicos de 64 bits. Após a realização da associação na rede, o coordenador pode lhes atribuir um endereço curto, de 16 bits. Neste caso, a unicidade de endereçamento fica restrita àquela RSSF e somente durante a duração da associação. Para o uso de IPv6, os endereços curtos devem estar sob um modos a seguir:

Endereços *Unicast* (Intervalo 1)

O primeiro bit possui valor zero e os outros 15 podem assumir qualquer valor. Esta classe de endereçamento possui um total de 32.768 endereços que variam de 0x0000 a 0x7FFF.

Endereços *Multicast* (Intervalo 2)

Os primeiros 3 bits levam o valor 100, os demais 13 bits podem assumir qualquer valor. Esta classe tem um total de 8192 endereços *multicast*, de 0x8000 a 0x9FFF.

Um endereço IPv6 do tipo *multicast* de 128 bits pode ser mapeado para um endereço de 16 bits concatenando-se os últimos 5 bits do 15^{o}octeto e o 16^{o}octeto inteiro dos 128 bits do endereço IPv6 *multicast* com os 3 primeiros bits dos 16 bits do endereço *multicast* IEEE 802.15.4. conforme ilustrado na Figura 2.4.

Value	1	0	0	X	X	X	X	X	X	X	X	X	X	X	X	X
bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0-2 bits short add.				3-7 bits of 15th octet					16th octet of the 128bit-address							

Figura 2.4: *Mapeamento de Endereços Multicast*

No entanto, as redes IEEE 802.15.4 não suportam *multicast* nativamente. Por isso os pacotes IPv6 *multicast* devem ser transmitidos sobre quadros IEEE 802.15.4 em modo *broadcast*.

Endereços Reservados (Intervalos 3, 4 e 5)

Quando os 3 primeiros bits do campo de endereçamento estão configurados como 101, 110 ou 111, o endereço nele contido faz parte, respectivamente, das classes 3, 4 e 5 de endereços reservados. Cada classe possui 8192 endereços que variam de 0xA000 à 0xBFFF, de 0xC000 à 0xDFFF e de 0xE000 à 0xFFFD, respectivamente para a classe 3, 4 e 5. O endereço 0xFFFF é reservado para *broadcast* e o endereço 0xFFFE reservado para indicar que um dispositivo não tem um endereço de 16 bits associado.

2.1.4 Tipos de Quadros IEEE 802.15.4

Existem 4 tipos de quadros IEEE 802.15.4: *Beacon*, *Data*, *Acknowledgement* e *Command*. As características de cada um destes quadros serão apresentadas nas próximas subseções.

Formato do quadro de Beacon

Os quadros do tipo *Beacon* são usados nos eventos de associação e desassociação em todas as redes. Nas redes com *Beacon* habilitado, este ainda é utilizado para sincronizar os dispositivos com o coordenador e estabelecer períodos livres de contenção. A Figura 2.5 mostra os campos de um quadro de *Beacon*. A seguir, é feita a explicação de cada campo deste tipo de quadro.

Figura 2.5: *Formato do Quadro tipo Beacon*

- **O campo de especificação do super quadro**

  No original, em inglês, *Superframe Specification*, este campo é usado pelo coordenador da rede para definir os limites de atividade e inatividade na utilização do canal. Os períodos ativos e inativos são configurados pelos campos *beacon order* e *superframe order*. Os períodos ativos são iniciados com um quadro *Beacon* e são seguidos de um *Contention Access Period* (CAP). Se presente, um *Contention Free Period* (CFP) segue-o. Qualquer *Guaranteed Time Slot* (GTS) deve ser alocado dentro do período CFP. A Tabela 2.3 mostra a organização do campo *superframe*, bit a bit.

- **O campo de especificação do GTS**

  No original, em inglês, chama-se *GTS Specification*. Este campo é composto por 1 byte, sendo que os 3 primeiros bits representam o *GTS descriptor count* que especifica o número de descritores no *GTS list*. Caso seu valor seja zero, então não há GTS em uso.

bit	Campo	Explicação
0	*Beacon order*	Este campo especifica o tamanho do *superframe*, isto é, o intervalo entre quadros tipo *beacon*. Os valores de *Beacon Order* (BO) variam de 0 à 14, o valor 15 é reservado, significando que quadros de *beacon* só são enviados quando requisitados.
...		
3		
4	*Superframe order*	Este campo especifica o tamanho da parte ativa do *superframe*, isto é, quando os dispositivos podem comunicar-se. Os valores podem variar de 0 à 14, sendo que 14 significa que os nós podem comunicar-se sempre. O valor 15 é reservado, significando que não existe *superframe*.
...		
7		
8	*Final CAP slot*	Este campo especifica em qual *slot* da porção ativa do *superframe* termina o *Contention Access Period* (CAP). O CAP pode crescer ou diminuir, de forma a dinamicamente acomodar o tamanho do CFP e manter os GTS.
...		
11		
12	*Battery life extent.*	Quando este bit é 0, o radio do coordenador fica ligado durante todo o CAP.
13	reservado	
14	*PAN coordinator*	Se este bit for 1, o quadro foi enviado pelo coordenador da rede.
15	*Association permit*	Se este bit for 1, o coordenador esta aceitando pedidos de associação a rede.

Tabela 2.3: *Especificação do super quadro*

Os próximos 4 bits são reservados e o último bit representa o *GTS permit*, que quando configurado em 1 quer dizer que o coordenador está aceitando *GTS requests*.

- **O campo de direções do GTS**

  No original, em inglês, chama-se *GTS Directions*. Este campo contém uma máscara de bits com o sentido de cada GTS no *superframe*. Um bit configurado em 1 significa que o GTS está relacionado com dados sendo recebidos pelo dispositivo, um bit configurado para 0 significa que os dados estão sendo enviados.

- **O campo lista de GTS**

  No original, em inglês, chama-se *GTS List*. Este campo tem tamanho máximo limitado a 21 bytes e sempre será múltiplo de 3 bytes. É definido pelo *GTS descriptor count* no campo *GTS specification*. Ele contém uma lista de elementos (descritores) com informação acerca de cada um dos *slots* que estão sendo mantidos. Cada um destes descritores é composto por um campo com o endereço do dispositivo e o *slot* no qual o respectivo GTS inicia-se.

- **O campo endereços pendentes**

No original, em inglês, chama-se *Pending Addresses*. Este campo tem 1 byte, sendo que os 3 primeiros bits correspondem ao número de endereços curtos no campo *Address List*. Após um bit de uso reservado, analogamente temos o número de endereços extensos que seguem os endereços curtos no campo *Address List*. A tabela 2.4 apresenta a organização deste campo.

bit	Campo	Explicação
0	Nmber of addresses pending	Este campo indica o número de endereços de 16 bits no campo *Address list field* do quadro.
1		
2		
3	Reserved	
4	Number of extended addresses pending	Este campo indica o número de endereços de 64 bits no campo *Address list* do quadro.
5		
6		
7	Reserved	

Tabela 2.4: *O campo endereços pendentes*

- **O campo *Address List***

  O tamanho deste campo é variável e é determinado pelos valores especificados no campo *Pending Address Specification*. Este campo contém uma lista de endereços de dispositivos que possuem mensagens pendentes com o coordenador. O número máximo de endereços na lista deve ser limitado a 7, pode conter endereços curtos de 16 bits ou extensos de 64 bits. Os endereços curtos devem ser listados antes e não podem ser do tipo *broadcast*.

- **O Campo de dados do *Beacon*** Neste campo são transportados dados do *Beacon*. Tem tamanho variável, pode ser transmitido de forma plana ou cifrado. Seu conteúdo, se presente, deve ser enviado às camadas superiores para ser processado.

Examplo de um superframe

O valor do *Beacon Interval* (BI) é calculado por $BI = 2^{BO}$. Por exemplo, dado um valor de *Beacon Order* igual a 5, teremos um *Beacon Interval* igual a 32. Para compartilhar este tempo

entre períodos ativos e inativos, é necessário configurar o tempo *Superframe duration* (SD), que é dado por $SD = 2^{SO}$. Na Figura 2.6 é dado um exemplo. O valor de SO é igual a 4, então SD receberá o valor 16. Os quadros tipo *Beacon* são representados em vermelho.

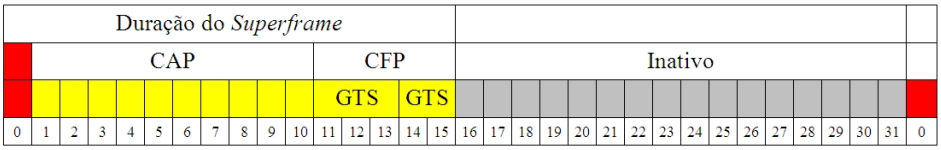

Figura 2.6: *Examplo de um superframe*

Formato do Quadro de Dados

O quadro para transporte de dados não adiciona nenhum campo novo. Os campos existentes também não sofrem modificações. O campo de dados (*payload*) contém a informação que será processada pelas camadas superiores. Este quadro, como outros, pode transportar informação em forma plana ou cifrada. Os pacotes 6LoWPAN são transportados neste campo.

Formato do Quadro de Comandos

No caso de redes com *Beacon* habilitado, o Quadro de Comandos (*Command Frame*) deve ser sempre transportado durante o período do CAP. O quadro de comandos não apresenta nada novo em relação ao quadro genérico. O campo de dados *(Payload)* de um Quadro de Comandos pode transportar um comando na forma plana ou cifrada. Seu campo de identificador deve ser um dentre os comandos aceitos pelo padrão IEEE 802.15.4. Os dispositivos do tipo FFD devem suportar todos os comandos enquanto os dispositivos do tipo RFD devem suportar apenas um subconjunto deles. A Tabela 2.5 apresenta a lista dos comandos definidos e aqueles que devem ser suportados pelos dispositivos RFD.

ID do comando	Nome do Comando	RFD	
		Tx	Rx
0x01	Requisição de Associação	x	
0x02	Resposta da Associação		x
0x03	Notificação de Desassociação	x	x
0x04	Requisição de Dados	x	
0x05	Notificação de conflito de PAN ID	x	
0x06	Notificação de Orfão	x	
0x07	Requisição de Beacon		
0x08	Realignment de Coordenador		x
0x09	Requisição de GTS		
0x0a – 0xff	Reservados		

Tabela 2.5: *Comandos IEEE 802.15.4*

O Formato do Quadro de *Acknowledgment*

O quadro de *Acknowledgment* possui somente os campos *frame control* e *sequence number* no cabeçalho MAC, conforme representado na Figura 2.7. Se um dispositivo possuir mais informações para enviar, o campo *pending* deve ter valor 1. Pacotes de *Acknowledgment* para pacotes IPv6 são transportados neste tipo de quadro.

Controle do Quadro	Número Seqüencial	Seqüência de checagem
2 bytes	1 byte	2 bytes
Cabeçalho MAC		Rodapé MAC

Figura 2.7: *O Formato do quadro de acknowledgment*

2.1.5 A topologia de uma rede IEEE 802.15.4

Os dispositivos de uma rede IEEE 802.15.4 podem ser de dois tipos: de funções restritas (do inglês, RFD *Reduced-function device*) e de funções completas (do inglês, FFD *Fully-function device*). O primeiro necessita estar em conformidade apenas com as camadas Física e de Acesso ao Meio e são supostos serem tão simples quanto um sensor passivo ou um interruptor de

uma lâmpada. Estes dispositivos de funções reduzidas comunicam-se com um, e apenas um, dispositivo de funções completas.

O coordenador da rede é um FFD executando serviços de sincronização. Há um coordenador principal e zero ou mais coordenadores alternativos, que são capazes de tomar o lugar do coordenador principal em caso de falha neste dispositivo. Estes coordenadores podem ser sensores, atuadores ou encaminhadores (*routers*), desempenhando outros papeis na rede. Topologias possíveis em redes IEEE 802.15.4 são:

Topologia em Estrela

É a topologia mais simples, a comunicação entre cada um dos nós e o coordenador dá-se em apenas um salto (*hop*). Todos os nós comunicam-se somente com o coordenador da rede. A Figura 2.8 ilustra esta topologia.

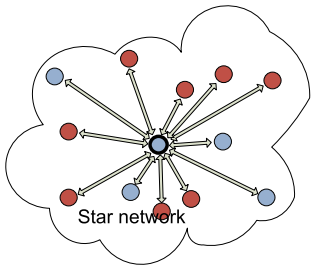

Figura 2.8: *Topologia em Estrela*

Topologias em estrela são bastante apropriadas para RSSF aplicadas ao corpo, ou *Body Area Networks* (BAN), já que a distancia entre os dispositivos é bastante reduzida. Ainda assim, a rede precisa ter um identificador único na sua esfera de influência. Este é ditado pelo dispositivo coordenador e comunicado aos demais dispositivos no momento da associação à rede.

Comunicação em *multi hop* é uma maneira eficiente de transpor obstáculos e aumentar a área de cobertura de uma rede. Além disso, a energia gasta na transmissão sem fios aumenta, no mínimo, com o quadrado da distância. Portanto, se a distância entre o nó origem e destino for dividida em trechos menores, o custo final, isto é, a soma dos trechos, será menor. No entanto, há um custo base que deve ser levado em conta, uma vez que os nós envolvidos precisam estar

ligados e manter informação acerca das tabelas de encaminhamento *routing tables* para que sejam úteis aos pares que estão comunicando-se. Portanto, ao configurar a topologia da rede, devemos ter em conta que também há um custo energético que cresce proporcionalmente ao número de nós envolvidos em uma comunicação *multi hop* [KARL, 2005].

Redes Ad-hoc

As Redes Ad-hoc são assim conhecidas pela capacidade de auto-organização e comunicação de forma dinâmica e independente de infra-estrutura pré-existente. Neste tipo de topologia, nas redes IEEE 802.15.4 as mensagens são encaminhadas de nó em nó através de dispositivos tipo FFD. Algumas topologias possíveis são as *mesh* e as *cluster-tree*. As Figuras 2.9 e 2.10 ilustram cada um dos casos.

As redes IEEE 802.15.4 com topologia *ad-hoc* possuem um, e somente um, dispositivo coordenador, podendo ter, de acordo com a topologia adotada, zero ou mais coordenadores alternativos. Comumente a topologia está relacionada com o tipo de aplicação que será executada na RSSF.

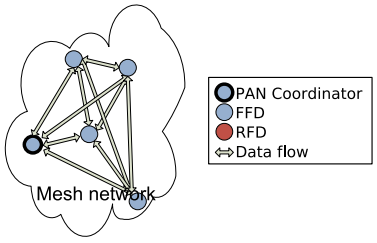

Figura 2.9: *Topologia de Rede Mesh*

Cluster tree network

Em uma rede tipo *Cluster tree* os nós são organizados em aglomerados (*clusters*) e gerenciados por um *cluster head*. A espinha dorsal (*backbone*) desta rede é composta por dispositivos tipo FFD, vez que os RFD não fazem encaminhamento de pacotes. A sincronização dos dispositivos é feita pelo dispositivo coordenador ou por outro FFD, caso este esteja configurado para assumir tal função.

O dispositivo coordenador estabelece o aglomerado (*cluster*) número zero e age como *cluster head*, enviando quadros tipo *beacon*. Um nó que receba um destes quadros pode requisitar ao *cluster head* permissão para entrar na rede como um nó filho. Se autorizado, o nó constará na lista de vizinhos do *cluster head* e o *cluster head* constará para o novo nó como seu nó pai. Após a entrada na rede, o novo dispositivo pode começar a transmitir *beacons* e pode vir a ter outros dispositivos anexados a si. O dispositivo coordenador pode definir quais FFD tornar-se-ão *cluster heads*.

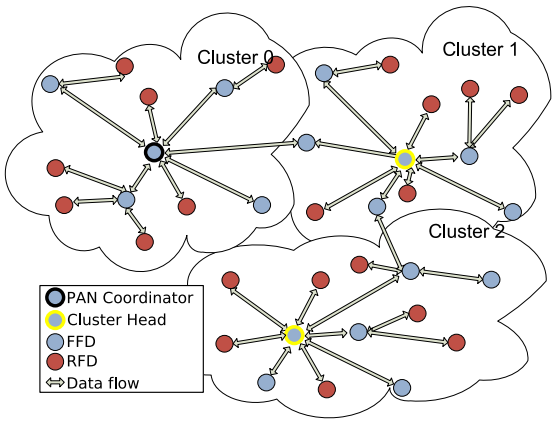

Figura 2.10: *Topologia tipo Cluster Tree*

2.2 IPv6 Over Low Power Personal Area Networks

Um grupo de trabalho da *Internet Engineering Task Force* (IETF) une esforços no sentido de fazer com que seja possível a comunicação IPv6 em redes IEEE 802.15.4. O grupo leva o mesmo nome da pilha protocolar, 6LoWPAN. Questões em discussão passam por: fragmentação e remontagem de pacotes [THUBERT, 2008], compressão dos cabeçalhos do Internet Protocol [KUSHALNAGAR, 2007], encaminhamento *mesh* e *multicast* [KASPAR, 2008], endereçamento IPv6 automático [CHAKRABARTI, 2007], mobilidade [SHIN, 2007], dentre outras.

O 6LoWPAN permite o transporte de pacotes IPv6 em redes IEEE 802.15.4 com topologia em

estrela ou ad-hoc, operando com endereços curtos de 16 bits ou longos de 64 bits. Podem operar com *guaranteed time slots* (GTS) ou sobre um canal *carrier sense multiple access with collision avoidance* (CSMA-CA) [IEEE, 2006].

A especificação do IPv6, requer que o link possa suportar pacotes de até 1280 octetos. No entanto, o campo de dados de um quadro IEEE 802.15.4 pode ter no máximo 102 octetos disponíveis após os cabeçalhos MAC. Este espaço útil a informação pode ficar ainda menor se alguma criptografia for aplicada: o espaço livre pode chegar à 93, 89 or 81 octetos se criptografia com chaves de 32, 64 ou 128 bits for aplicada, respectivamente. Portanto, a compressão de cabeçalhos IPv6 é condição importante para o sucesso do uso de IPv6 em RSSF. Além disso, questões como encaminhamento *mesh*, comunicação *multicast* e fragmentação precisam ser tratadas abaixo da camada IPv6. Portanto, o 6LoWPAN cria uma camada entre o IEEE 802.15.4 e o IPv6 com cabeçalhos específicos para cada uma destas funções. Estes cabeçalhos são adicionados ou removidos, conforme a necessidade do cenário. Com esta abordagem, apenas o que é realmente útil é carregado e a sobrecarga protocolar mantém-se o mais baixa possível. Nas Secções que seguem, cada um destes cabeçalhos será aprensentado. A Tabela 2.6 mostra a camada de adaptação proposta pelo 6LoWPAN.

Seq.	**Dispatch**	**Tipo de cabeçalho**
00	Não pretence a nenhum encapsulamento 6LoWPAN	
01	000001	Um pacote IPv6 normal.
	000010	Um pacote IPv6 com compressão LowPan_HC1
	...	Reservados
	010000	Cabeçalho de Broadcast (LoWPAN_BC0)
	...	Reservados
	111111	Os bits que seguem formam um campo adicional para outro valor de *Dispatch*.
10	Cabeçalho para encaminhamento *Mesh*.	
11	Cabeçalho para tartar fragmentação.	

Tabela 2.6: *Cabeçalhos da Camada de Adaptação do 6LoWPAN*

Cabeçalho 6LoWPAN para Encaminhamento Mesh

O encaminhamento *mesh* abaixo da camada 3 é independente do protocolo de rede e proporciona significativa redução nas tabelas de encaminhamento IPv6, uma vez que os endereços IEEE 802.15.4 são muito menores que os endereços IPv6. A Tabela 2.7 mostra os campos de um cabeçalho de encaminhamento *mesh* e a Figura 2.11 mostra o cabeçalho. O tamanho do cabeçalho varia em função do modo de endereçamento adotado, isto é, 16 ou 64 bits. Quando presente, o cabeçalho para encaminhamento *mesh* vem antes de qualquer outro cabeçalho 6LoWPAN e permite que protocolos de encaminhamento ad-hoc executem a entrega de pacotes mesmo quando os pares de uma comunicação não tenham alcançabilidade direta. O modo de funcionamento

bit	valor	Explicação
0	**1**	Os dois primeiros bits são 1 e 0, respectivamente e servem para identificar que este é um cabeçalho para encaminhamento *mesh*.
1	**0**	
2	Originador	Estes bits designam o tipo de endereçamento adotado para o originador do pacote e para o destinatário final do pacote. O código é 0 para endereços de 64 bits e 1 para endereços de 16-bits.
3	Destino Final	
4	Hops left	Este campo de 4 bits refere-se ao número máximo de nós pelos quais o pacote pode passer antes de ser descartado. É decrementado ao passar por cada nó. O valor 1111 é reservado e significa que há um campo de 1 byte para designar a quantidades de saltos permitidos.
...		
7		

Tabela 2.7: *Campos do Cabeçalho de Encaminhamento Mesh*

Value	**1**	**0**	Orig	Final	Hops left				Hops left	Originador	Destinatário Final
bit	0	1	2	3	4	5	6	7	Optional 8 bits	16 bits or 64 bits	16 bits or 64 bits

Figura 2.11: *Cabeçalho de Encaminhamento Mesh*

do cabeçalho é o seguinte: O remetente de um pacote, coloca seu próprio endereço físico no campo *source address* do quadro IEEE 802.15.4 e o endereço do nó que será o próximo salto no campo *destination address*. Quando este nó recebe o pacote, trata de alterar o campo *source address* do quadro IEEE 802.15.4 para seu próprio endereço e o campo *destination address* para o endereço do próximo salto.

O cabeçalho de suporte ao encaminhamento *mesh* serve para guardar os endereços do remetente original e do destinatário final do pacote. Portanto, a cada salto, o nó que recebe o pacote deve

verificar estes endereços, consultar sua tabela de encaminhamento e enviar o pacote ao nó mais apropriado, de acordo com o algoritmo de encaminhamento adotado.

Cabeçalhos para *Broadcast*

Quando um pacote IPv6 precisa ser transmitido em *multicast*, há um cabeçalho especial provido pela camada de adaptação do 6LoWPAN que trata de evitar que as mensagens entrem em *loop*. A estrutura deste cabeçalho é mostrada na Figura 2.12. Sendo o valor do Lowpan BC0 seguindo do campo *sequence number*.

Campo	**0**	**1**	Lowpan_BC0 *dispatch*						Número Seqüencial							
bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Figura 2.12: *Cabeçalho 6LoWPAN para Broadcast*

O Cabeçalho 6LoWPAN para Fragmentação

Quando um pacote 6LoWPAN, isto é, os cabeçalhos da camada de adaptação 6LoWPAN somados ao campo de dados, não é suficientemente pequeno para ser levado no campo de dados de um quadro IEEE 802.15.4, ele necessita ser partido em fragmentos e levado em 2 ou mais quadros. A Tabela 2.8 ilustra a estrutura do cabeçalho para fragmentação e remontagem. Na

bit	valor	Explicação
0	**1**	Os primeiros 5 bits identificam este cabeçalho como sendo o de fragmentação. O valor 11000 designa o primeiro fragmento de um pacote. Todos os demais fragmentos começam com o valor 11100.
1	**1**	
2	**0/1**	
3	**0**	
4	**0**	
5 ... 15	**Tamanho do Datagrama**	Este campo de 11 bits guarda o tamanho do pacote antes da fragmentação. Não há necessidade de ser carregado em todos os fragmentos, pois pode ser calculado na fase de remontagem.
16 ... 31	**Tag do Datagrama**	Este campo de 16 bits identifica os fragmentos de um mesmo datagrama. Pacotes sucessivos de um mesmo remetente devem ter valores sucessivos.
0 ... 7	**Datagram offset**	Este campo de 8 bits especifica, em incrementos de 8 octetos, quanto do pacote já foi transmitido até o fragmento atual. Não está presente no primeiro fragmento, já que seu valor é zero.

Tabela 2.8: *Campos do Cabeçalho de Fragmentação*

fase de remontagem, o destinatário pode usar os campos Tag, Endereço de Origem, Endereço de Destino e Tamanho do Datagrama para reconstruir o pacote. Quando um nó sofre um evento de desassociação da rede, ele deve descartar todos os fragmentos que estejam em sua posse.

Cada um dos cabeçalhos apresentados, quando presente, aparece na seguinte ordem: cabeçalho para encaminhamento *mesh*, cabeçalho para comunicação em *broadcast*, cabeçalho para fragmentação e finalmente o cabeçalho Lowpan HC1 e seus campos extras ou um pacote IPv6 na íntegra.

2.2.1 A camada de rede do 6LoWPAN

As técnicas de compressão e codificação de cabeçalhos IPv6 aplicadas no LoWPAN HC1 são independentes da informação do fluxo e apenas usam informações vindas da camada 2. O cabeçalho de um pacote IPv6 pode ser comprimido em 2 bytes, precedido por 1 byte do dispatch HC1. As codificações executadas pelo cabeçalho LoWPAN HC1 podem ser vistas na Tabela 2.9 e a correspondência entre os campos do cabeçalho IPv6 e do cabeçalho LoWPAN HC1 pode ser vista na Tabela 2.10.

IPv6 Origem	IPv6 destino	Traffic class e flow label	Next header	Codificação HC2
2 bits	2 bits	1 bit	2 bits	1 bit

Tabela 2.9: *A codificação do cabeçalho LoWPAN HC1*

Campo	**Tamanho IPv6**	**Tamanho HC1**	**Explicação**
Version	4 bits	-------	Assumido como IPv6.
Traffic class	8 bits	1bit	0=Não comprimido. Os campos seguem na íntegra. 1=Comprimidos. Os valores para os campos *traffic class* e *flow label* são ambos zero.
Flow label	20 bits		
Payload length	16 bits	-------	Pode ser inferido do tamanho do quadro ou do tamanho do datagrama da camada de adaptação.
Next header	8 bits	2 bits	Pode ser: UDP, ICMP, TCP ou "Não comprimido".
Hop limit	8 bits	8 bits	Único campo que não é comprimido.
Source address	128 bits	2 bits	Quando ambos os campos de endereçamento IPv6 são do tipo *link-local*, podem ser totalmente inferidos da camanda MAC.
Dest. address	128 bits	2 bits	
HC2 encoding	-------	1 bit	Se 1, o próximo cabeçalho é o definido em *Next header*
Total	40 Bytes	2 Bytes	

Tabela 2.10: *Camada de Adaptação 6LoWPAN*

Quando os campos não são codificados nem suprimidos eles são carregados na íntegra. A Tabela 2.11 mostra a codificação 6LoWPAN para endereços IPv6. O esquema de compressão de cabeçalhos da camada de transporte pode ser visto na Tabela 2.12.

bits	Opção
00	PI,II
01	PI,IC
10	PC,II
11	PC,IC

Opção	Explicação
PI	Prefixo carregado na íntegra.
PC	Prefixo comprimido. Endereço assumido como *Link-local*.
II	Identificador da Interface carregado na íntegra.
IC	Identificador da Interface comprimido. Derivável do *link-layer*.

Tabela 2.11: *Compressão de Endereços IPv6*

bits	Opção
00	Cabeçalho não comprimido
01	UDP
10	ICMP
11	TCP

Tabela 2.12: *Códigos para o Próximo Cabeçalho*

2.2.2 Camada de Transporte do 6LoWPAN

O esquema de codificação HC UDP permite comprimir os campos *source port, destination port e length*, enquanto o UDP *header checksum* é carregado na íntegra. Dos originais 8 bytes, a versão comprimida apresenta 4. A codificação do UDP é ativada pelos bits 5 e 6 do cabeçalho HC1. A Tabela 2.13 apresenta o esquema de codificação do cabeçalho HC UDP.

Bit	Campo	Explicação
0	Porta UDP de origem	As portas de origem e destino podem ser carregadas na íntegra, ocupando 16 bits cada (quando o valor deste campo é zero) ou podem ser comprimidas para um valor de 4 bits. As portas passam a ter o valor 0xF0B0 somado ao valor carregado no campo de 4 bits.
1	Porta UDP de destino	
2	Tamanho	0: O campo tamanho do segmento segue na íntegra. 1: O campo é omitido e calculado apartir das camadas inferiores.
...	Reservados	
7		

Tabela 2.13: *Campos de codificação HC UDP*

3 *Estudo da Sobrecarga Protocolar do 6LoWPAN*

Em dispositivos de capacidades restringidas, como os nós de uma RSSF, é imperativo que todo *overhead* seja evitado tanto quanto possível. Em algumas arquiteturas, o custo por bit transmitido pode chegar a centenas de vezes o custo de processá-lo. Portanto, a eficiência da arquitetura comunicação faz a diferença entre uma RSSF de vida curta ou longa.

Em [KUSHALNAGAR, 2007] é feita uma caracterização das redes pessoais de baixo poder de processamento (LoWPAN) e são abordados os problemas relacionados ao uso do IPv6 sobre estas redes. Além disso, é fornecida uma visão geral da pilha protocolar do 6LoWPAN e são descritos os objetivos do grupo de trabalho da IETF no que tange a comunicação IPv6 sobre este tipo de dispositivos. Esta pesquisa levou à publicação do padrão IETF para comunicação IPv6 sobre redes IEEE 802.15.4, publicado na RFC4944 [MONTENEGRO, 2007], na qual são definidos os formato de cabeçalhos, as técnicas de codificação e os mecanismos de compressão do 6LoWPAN.

Já o trabalho publicado em [MULLIGAN, 2007] apresenta uma comparação, em termos de tamanho do código fonte, tamanho total dos cabeçalhos, máximo número de nós suportados na rede, tipos de protocolos de encaminhamento *mesh* suportados e o tipo de conectividade com a Internet entre as arquiteturas 6LoWPAN, Zigbee e Zensys. O referido estudo demonstra que o 6LoWPAN, além de permitir a conectividade de forma transparente com a Internet é uma alternativa competitiva face às arquiteturas proprietárias.

Os benefícios da adoção do 6LoWPAN como infra-estrutura de rede para PAN e sobretudo para RSSF é também demonstrado em [CULLER, 2007] e [MULLIGAN, 2007]. Os autores apre-

sentam uma visão geral do padrão IEEE 802.15.4 e um gráfico com o *overhead* adicionado pelo uso do padrão 6LoWPAN e a energia gasta pra transmissão de dados utilizando 6LoWPAN em comparação com IEEE 802.15.4 sem os cabeçalhos 6LoWPAN adicionados. Esta comparação não traz, no entanto, resultados em termos absolutos, apenas um gráfico comparativo.

Buscando estender o estado-da-arte dos trabalhos anteriores, em [ZIMMERMANN, 2008a] apresentamos uma descrição detalhada da sobrecarga protocolar gerada nas comunicações 6LoWPAN. Exaustivos cenários foram apresentados com a respectiva avaliação da quantidade total de *overhead* gerado em cada um destes cenários. Este estudo, levou a proposição de uma arquitetura, apresentada no Capítulo 4, que mantém o cenário de conectividade global porém evita os custos associados a ela.

A camada de adaptação 6LoWPAN executa um importante papel no que tange a redução de sobrecarga protocolar de comunicação. Suprimindo campos da camada IPv6 e recuperando-os a partir de informação da camada 2. Com a compressão de cabeçalhos do 6LoWPAN, o tamanho dos cabeçalhos da camada de rede pode ser reduzido para apenas 3 bytes (um byte do *dispatch* + um byte de sinalizadores + um byte para carregar o campo *hop limit* do IPv6. A arquitetura da pilha protocolar 6LoWPAN emprega uma abordagem de pagar só pelo que se usa. Deste modo, apenas os cabeçalhos úteis são carregados [CULLER, 2007].

3.1 Tamanhos dos cabeçalhos 6LoWPAN

Os cabeçalhos 6LoWPAN são concatenados conforme o cenário da RSSF. A seqüência de cabeçalhos, quando presentes, é a seguinte: *mesh*, *broadcast*, fragmentação e Lowpan_HC1 seguido dos campos do IPv6 carregados na íntegra. O tamanho da camada de adaptação mais a de rede varia de acordo com fatores como arquitetura da rede, tamanho dos pacotes, escopo da comunicação e se a comunicação é *unicast* ou *broadcast*, em termos de bytes pode variar desde os 3 bytes até os 51 bytes. A seguir apresentamos cada cabeçalho com o *overhead* associado.

3.1.1 Cabeçalho de Encaminhamento Mesh

O cabeçalho de encaminhamento *mesh* é representado na Figura 3.1. Este tem 1 byte para sinalizadores de controle (*flags*) e número de saltos restantes (*hop limit*), seguidos pelos endereços do remetente original e destinatário final. O tamanho total deste cabeçalho depende do tipo de endereçamento utilizado na PAN. Os campos de endereçamento podem ter 2 bytes, em caso de endereços curtos ou 8 bytes cada, em caso de endereçamento estendido. Este cabeçalho pode conter um campo extra, para armazenar um número maior para o *hop limit*, neste caso 1 byte extra é carregado. A Figura 3.1 apresenta o tamanho do cabeçalho de encaminhamento *mesh*, o byte extra de extensão opcional do *hop limit* não é representado na figura.

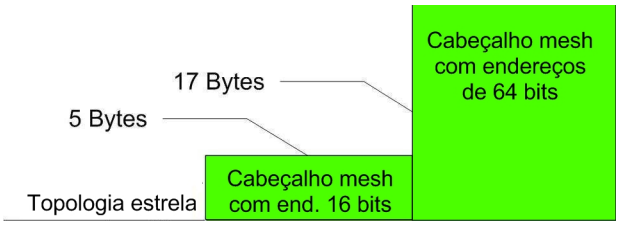

Figura 3.1: *Sobrecarga protocolar adicionada pelo cabeçalho de encaminhamento mesh*

3.1.2 Cabeçalhos em Unicast e Broadcast

Quando um pacote é transmitido em *unicast*, não há necessidade de cabeçalho extra. No entanto, quando ocorre comunicação IPv6 em *multicast*, a camada de adaptação trata da entrega do pacote aos múltiplos destinatários utilizando *broadcast* em camada 2. Para evitar que um nó receba um pacote por mais de uma vez, existe um campo com um número seqüencial que pode ser verificado e, em caso de ser um pacote em duplicado, descartar o pacote. Para este cabeçalho são acrescidos 2 bytes, conforme Figura 3.2.

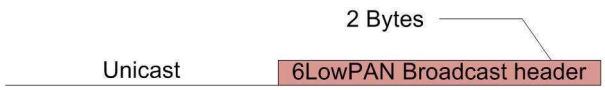

Figura 3.2: *Sobrecarga adicionada pelo cabeçalho de broadcast*

3.1.3 Cabeçalho para Fragmentação

A sobrecarga protocolar adicionada pelo cabeçalho de fragmentação é de 5 bytes. A Figura 3.3 os representa.

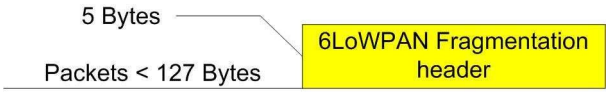

Figura 3.3: *Sobrecarga protocolar adicionada pelo cabeçalho de fragmentação*

3.1.4 Sobrecarga relacionada ao escopo da comunicação – Intra-RSSF vs Extra-RSSF

Quando a comunicação se dá entre dispositivos que estão na mesma RSSF, endereços IPv6 do tipo link-local podem ser utilizados. Um endereço link-local é formado pelo prefixo FE:80::/64 seguido pelo endereço físico do dispositivo. O prefixo FE:80::/64 pode ser omitido, pois é conhecido e padronizado e o endereço físico já é carregado na camada 2. Portanto, podemos suprimir totalmente os 16 bytes de endereçamento de cada um dos endereços IPv6 de origem e destino. Este mecanismo é o maior responsável pela redução de overhead de comunicação. No entanto, não pode ser utilizado quando o pacote cruza as fronteiras da RSSF, onde para manter a alcançabilidade há a necessidade de se carregar os endereços IPv6 únicos e globais de origem e destino. A Figura 3.4 denota a significativa diferença entre o overhead gerado em comunicações intra e inter RSSF.

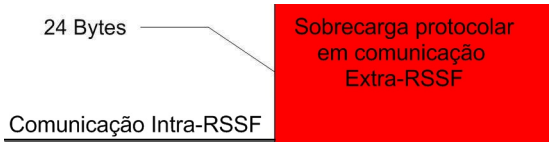

Figura 3.4: *Sobrecarga protocolar adicionada pelo endereçamento IPv6*

3.1.5 Outras Possíveis Fontes de Sobrecarga

Os campos *traffic flow e traffic class* do cabeçalho IPv6 original são simplesmente suprimidos e os valores considerados zero. Se, por qualquer razão, houver a necessidade de carregá-los com um valor diferente, eles serão adicionados ao fim do cabeçalho 6LoWPAN.

3.2 Cenários 6LoWPAN

De acordo com o requerido pela aplicação, uma RSSF pode apresentar diferentes características em termos de tamanho de pacote, topologia de rede, encaminhamento e escopo de comunicação. Estas características se refletem nos diferentes cabeçalhos que serão adicionados à camada de adaptação e de rede 6LoWPAN conforme a necessidade do cenário. As combinações de cabeçalhos da camada de adaptação geram 12 possíveis casos, que são aqui apresentados com atenção à sobrecarga protocolar gerada por cada um deles nos cenários Intra-RSSF e Extra-RSSF.

- **A: Topologia em Estrela, Unicast, Pequenos Pacotes**

  Este é o cenário de mais baixo custo. Não há necessidade de nenhum cabeçalho extra. A quantidade final de cabeçalhos é de apenas 3 bytes (o mínimo que uma rede 6LoWPAN pode ter:1 byte do dispatch 6LoWPAN, 1 byte do hop limit e 1 byte das flags) com em comunicação local e 27 bytes se endereçamento global for necessário.

- **B: Topologia em Estrela + Cabeçalho Broadcast**

  Algumas aplicações, tal como distribuição de código ou algumas operações de gerência da RSSF podem fazer uso IPv6 multicast, requerendo cabeçalho extra. Isto aumenta o cabeçalho em 2 bytes.

- **C: Topologia em Estrela + Cabeçalho de Fragmentação**

  O IPv6 requer um *Maximum Transfer Unit* (MTU) de, pelo menos, 1280 octetos. Qualquer meio que não possa prover isso, deve gerenciar a fragmentação e a remontagem dos pacotes abaixo da camada 3. Portanto, pacotes que não caibam nos 127 bytes do MTU do IEEE802.15.4 necessitarão ser fragmentados. Esta operação adiciona 5 bytes devido ao cabeçalho 6LoWPAN de fragmentação.

- **D: Topologia em Estrela + Cabeçalho Broadcast + Cabeçalho de Fragmentação**

  Este cenário pode acontecer, por exemplo durante a atualização do sistema operacional de um grupo de nós. Os pacotes grandes requerem fragmentação e, ao serem enviados em modo *broadcast*, demandam cabeçalho especial. O *overhead* acumulado gera 10 bytes por pacote se a comunicação for interna e até 34 bytes se o fluxo da comunicação for estabelecido com um dispositivo externo à RSSF.

- **E: Topologia Mesh com endereços curtos**

  Aumentar a área de cobertura da RSSF via comunicação em multi-hop tem o custo de ter de carregar um cabeçalho de encaminhamento *mesh*. Este cabeçalho adiciona 5 bytes quando os endereços são de 16 bits. A quantidade total de cabeçalhos deste cenário é de 8 bytes para comunicação local e 32 para comunicação global.

- **F: Topologia Mesh com endereços curtos + Cabeçalho Broadcast**

  Este cenário acarreta os mesmo 5 bytes do cabeçalho *mesh* somados aos 2 bytes do cabeçalho de *broadcast*. Total 10 bytes para comunicação local e 34 bytes para comunicação global.

- **G: Topologia Mesh com endereços curtos + Cabeçalho de Fragmentação**

  Somam-se 5 bytes do cabeçalho de fragmentação aos 5 bytes do cabeçalho *mesh*. Total 13 bytes em comunicação local e 33 bytes em comunicação global.

- **H: Topologia Mesh com endereços curtos + Cabeçalho Broadcast + Cabeçalho de Fragmentação**

Cenário com todos os cabeçalhos incluídos, total de 15 bytes para comunicação local e 33 bytes para comunicação global.

- **I: Topologia Mesh com endereços longos**

  Quando endereços longos (64 bits) são utilizados em redes IEEE 802.15.4, a camada 6LoWPAN necessita de cabeçalhos maiores para armazenar os endereços de origem e destino do pacote. O overhead total deste cenário é de 20 bytes para comunicação local e 44 para global.

- **J: Topologia Mesh com endereços longos + Cabeçalho Broadcast**

  Somam-se 2 bytes aos 3 bytes basicos e aos 17 bytes de cabeçalho mesh. Total 22 bytes para comunicação local. Em comunicação global somam-se ainda os 16 bytes do endereço do elemento externo à RSSF e o prefixo de rede do elemento da RSSF, totalizando 46 bytes.

- **K: Topologia Mesh com endereços longos + Cabeçalho de Fragmentação**

  Este cenário acarreta 25 bytes de cabeçalhos para comunicação local e 49 para comunicação global. Os cabeçalhos de fragmentação não se modificam em função do endereçamento.

- **L: Topologia Mesh com endereços longos + Cabeçalho Broadcast + Cabeçalho de Fragmentação**

  Este é o cenário com maior quantidade de cabeçalhos. São 17 bytes de cabeçalho mesh, 2 bytes de cabeçalho broadcast, 5 bytes de cabeçalho de fragmentação somados aos 3 bytes base do 6LoWPAN. Total de 27 bytes para comunicação local e 51 bytes em cenários de comunicação global.

A Figura 3.5 resume os 12 cenários apresentados neste capítulo. Em azul podemos ver a quantidade, em bytes, da sobrecarga protocolar gerada para cada um dos cenários para comunicação

intra-RSSF. Nota-se que a quantidade de sobrecarga protocolar introduzida pelo endereçamento IPv6 nos cenários de comunicação global, em vermelho, é significativa.

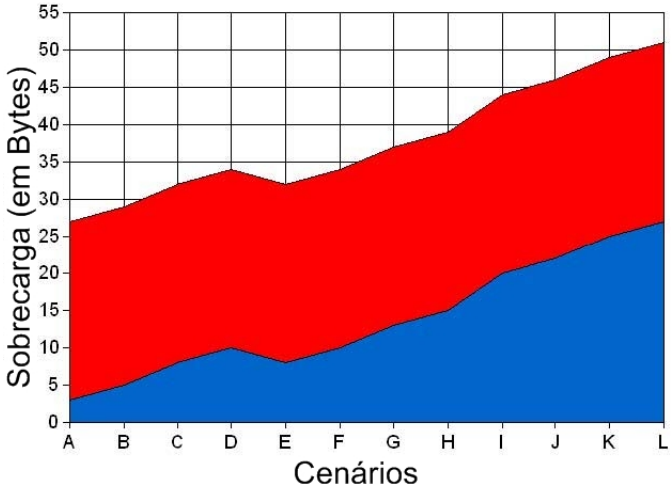

Figura 3.5: *Cenários 6LoWPAN com respectivos valores de sobrecarga protocolar*

4 A Arquitetura Proposta

A arquitetura para ganho de eficiência energética que é proposta nesta dissertação é baseada na tradução de endereços IPv6 do tipo *global-unique* para endereços do tipo *link-local*. Batizamos a arquitetura com o acrônimo 6GLAD, que designa *Global to Link-layer ADdress Translation for 6LoWPAN Overhead Reduction*[ZIMMERMANN, 2008a]. Esta tradução de endereços explora os mecanismos de redução de cabeçalhos do 6LoWPAN, em específico, a codificação dos endereços IPv6 de origem e destino, baseado nos endereços de camada 2. De fato, 80% do cabeçalho IPv6 (32 bytes dos 40 bytes) são gastos com endereçamento e é justamente nestes campos que a camada de adaptação do 6LoWPAN promove o maior ganho.

Quando um pacote IPv6 é transmitido em uma RSSF 6LoWPAN, ao invés dos campos da camada 3 serem diretamente encapsulados na camada 2, este são analisados e, sempre que possível suprimidos ou codificados. Deste modo, apenas a informação para remontagem do pacote é enviada. Quando a comunicação é feita em escopo local, inclusive os endereços IPv6 podem ser reconstruídos a partir da informação disponível na camada 2. No entanto, em cenários de comunicação de escopo global, o poder de supressão de cabeçalhos do 6LoWPAN é severamente afetado, pois a composição do endereçamento de camada 3 (IPv6) dos *hosts* fora da RSSF já não guardam relação com os de camada 2 (MAC).

A fim de estender os ganhos do 6LoWPAN também para os cenários de comunicação global, a arquitetura proposta opera um conjunto de traduções de endereços de rede (NAT) aos moldes do que é feito para redes IPv4 [SRISURESH, 2001]. Há que se ter em mente que a bidirecionalidade das conexões deve ser mantida. Isto é, deve ser possivel iniciar uma conexão tanto apartir da RSSF para a Internet quanto apartir de um host Internet para um nó da RSSF. Além disso

a unicidade de endereçamento deve ser mantida, cada nó da RSSF deve ser inequívocamente identificado, tal como se operasse com endereços únicos globais. Para tanto, faz-se necessária a aplicação, em simultâneo, de tradução de endereço um-para-um e tradução reversa de endereços. A técnica de aplicar estas traduções em simultanêo, nas redes IPv4, é conhecida como *Twice-NAT*, pois tanto o endereço de origem como o de destino de um pacote são alterados.

Estas operações garantem que o 6LoWPAN mantenha o *overhead* dentro da RSSF ao mínimo, enquanto são mantidas a conectividade global e a bidirecionalidade das conexões. Todas as traduções de endereço são transparentes para os demais agentes de rede, nós, serviços e utilizadores finais. O *gateway* 6GLAD pode ser colocado juntamente com o router 6LoWPAN, tal como no cenário da Figura 4.2. O objetivo é que, dentro da RSSF, os pacotes sejam transportados apenas utilizando endereços IPv6 tipo *link-local* e, ao passarem a fronteira da RSSF, sejam mapeados e traduzidos para endereços IPv6 do tipo *global-unique* pelo *gateway* 6GLAD. A conectividade global e a unicidade de endereços é mantida por um duplo mapeamento, onde os endereços locais de cada elemento da RSSF têm correspondência única a endereços IPv6 globais. De maneira análoga, qualquer elemento de fora da rede que esteja em comunicação com um nó da RSSF terá seu endereço IPv6 global associado a um endereço IPv6 local de um conjunto de endereços locais reservados. Por exemplo, do intervalo 3, apresentado na Secção 2.1.3 desta dissertação.

4.1 Tradução um-para-um de Endereços de Rede ou *Full-cone NAT*

Neste tipo de tradução, cada endereço interno do tipo *link-local* é mapeado para seu respectivo endereço externo do tipo *global-unique*. A bidirecionalidade é mantida, pois além dos nós internos poderem iniciar uma conexão com qualquer nó da Internet, um elemento externo pode alcançar um elemento com endereço traduzido via seu endereço externo do tipo *global-unique*. Diferentemente do *Restricted-cone NAT* nesta modalidade de tradução, não é necessário que um nó interno já tenha enviado algum pacote para que o nó externo possa alcança-lo. Não

há necessidade de manter uma tabela com os pares de endereços traduzidos, uma regra de tradução é suficiente. Na Figura 4.1, a regra é mapear o prefixo FE80 dos endereços tipo *link-local* para um prefixo globalmente alcançavel, no caso 301:B0FF. Esta técnica permite que os mecanismos de compressão 6LoWPAN codifiquem os endereços dos nós da RSSF baseado em seus endereços de camada 2, evitando assim o transporte dos 16 Bytes de endereçamento IPv6.

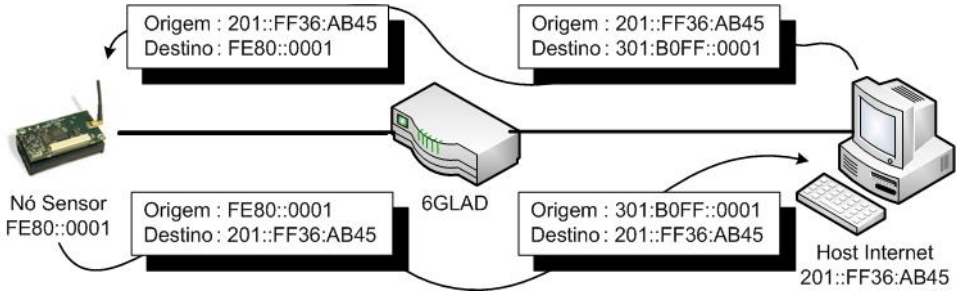

Figura 4.1: *Full-cone NAT*

4.2 Tradução Reversa de Endereços de Rede (Reverse-NAT)

Na tradução reversa de endereços de rede, é o endereço do elemento externo que é mapeado e traduzido para um endereço tipo *link-local* da rede interna. Neste caso, quando uma sessão é iniciada entre um nó da RSSF e um *host* da Internet, os pacotes, ao passarem pelo 6GLAD, sofrerão a tradução do endereço tipo *global-unique* do *host* externo, estes serão associados a endereços tipo *link-local* de uma classe reservada. A tabela de mapeamento para tradução reversa de endereços é atualizada em tempo de execução.

4.3 Dupla Tradução de Endereços de Rede (Twice-NAT)

A arquitetura 6GLAD executa a tradução tanto dos endereços dos nós da RSSF quanto dos endereços de *hosts* Internet que estejam em comunicação com algum nó. Esta técnica pode ser utilizada em comunicação IPv4 e é conhecida como *Twice-NAT* [SRISURESH, 1999a]. A

bidirecionalidade na origem das conexões continua a valer, de forma que as conexões possam ser iniciadas tanto por nós da RSSF assim como por hosts da Internet.

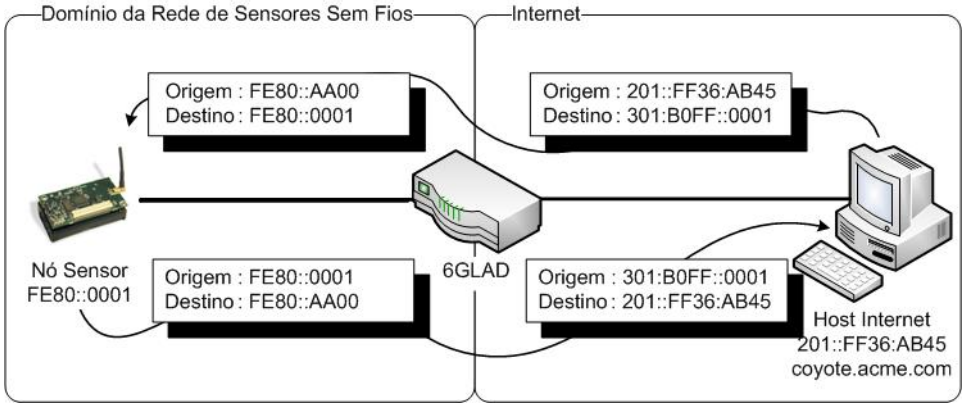

Figura 4.2: *A arquitetura do 6GLAD*

A Figura 4.2 mostra a arquitetura 6GLAD com alguns nós sensores com endereços IPv6 locais derivados de seus endereços físicos de 16 bits. Estes endereços sofrem a tradução do prefixo de rede ao passarem pelo 6GLAD. Um *host* da Internet em comunicação com um nó da RSSF também tem seu endereço mapeado para um endereços IPv6 tipo *link-local* do conjunto pré-definido. Nas conexões iniciadas por nós sensores da RSSF, o mapeamento do endereço do *host* Internet pode se dar via um *Domain Name Server – Application Level Gateway* (DNS-ALG) [SRISURESH, 1999b]. Este serviço recebe os pedidos de resolução de nomes, no exemplo o endereço IPv6 associado ao nome *coyote.acme.com* é 201::FF36:AB45, associa um endereço local ao endereço resolvido, no exemplo foi associado o endereço IPv6 FE80::AA00 e devolve ao nó sensor solicitante o endereço IPv6 do tipo *link-local* mapeado (FE80::AA00) para o endereço IPv6 *global-unique* do host desejado (201::FF36:AB45).

Desta forma, utilizando mecanismos transparentes, o uso de endereçamento IPv6 *link-local* é mantido dentro da RSSF. Isso habilita o 6LoWPAN a fazer a máxima supressão de campos de endereçamento IPv6. Simultaneamente, ao manter o mapeamento um-para-um de endereços *link-local* para endereços *global-unique*, os nós sensores continuam com unicidade de endereçamento, podendo ser alcançados globalmente.

5 *Avaliação e Resultados*

O estudo teórico acerca da sobrecarga de comunicação provocada pelos diversos fatores envolvidos nos possíveis cenários 6LoWPAN, apresentado no capítulo 3, mostra que a sobrecarga provocada pela perda de poder de compressão do 6LoWPAN em cenários que utilizam endereçamento global é significativa. No entanto, faz-se necessário a avaliação da arquitetura em um cenário de comunicação.

Neste capítulo são apresentados os resultados e a metodologia de avaliação da arquitetura proposta. A avaliação do impacto na utilização de largura de banda deu-se por meio de simulações recorrendo-se ao uso do Network Simulator-2. O impacto energético foi avaliado por meio da construção de uma plataforma de testes, utilizando-se nós sensores Crossbow MicaZ [CROSSBOW, 2008].

Este capítulo está subdividido em duas sub-seções, a primeira trata da construção da plataforma de testes, das ferramentas e equipamentos utilizados e dos resultados obtidos. A segunda trata dos aspectos relacionados a simulação e os resultados colhidos desta. Em ambos os ambientes a arquitetura 6GLAD foi comparada uma comunicação utilizando 6LoWPAN e com comunicação utilizando IPv6.

5.1 Experimentos na Plataforma de Testes

A avaliação foi executada em uma plataforma como a da Figura 5.1. Uma aplicação do tipo PING-PONG transportada sobre UDP foi analisada em 3 cenários: O primeiro utilizando a pilha protocolar do 6LoWPAN com endereços IPv6 do tipo *link-local* (designada 6GLAD);

O segundo com a pilha protocolar do 6LoWPAN com endereços IPv6 do tipo *global-unique* (designada 6LoWPAN) e o terceiro cenário utilizando a pilha protocolar do IPv6 com todos os campos carregados na íntegra (designada IPv6).

Figura 5.1: *Esquema da plataforma de testes*

Para cada cenário, um nó sensor com uma aplicação escrita em nesC programada para responder cada PONG com uma mensagem de PING, reportando o valor lido da bateria do nó sensor. O *sink node* está conectado a um PC portátil executando uma aplicação Java configurada para enviar uma mensagem PONG a cada segundo, esperar pela resposta PING e armazenar o valor colhido da bateria do nó sensor.

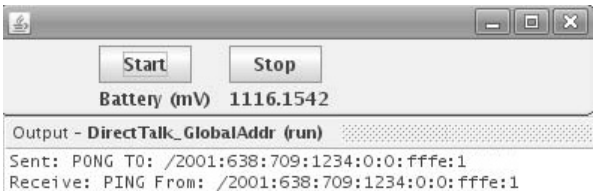

Figura 5.2: *Interface da Ferramenta de Medição da Bateria*

A Figura 5.2 apresenta a interface da ferramenta de medição do impacto energético. O objetivo foi analisar o impacto no consumo energético causado por um fluxo de pacotes com as diferentes abordagens (IPv6, 6LoWPAN e 6GLAD). Na figura pode ser visualizado um valor de bateria recebido, um PING enviado e um PONG recebido.

Para auxiliar a avaliação, lançamos mão de 2 agentes *sniffers*. O primeiro agente foi usado na camada 3, é conhecido como Wireshark [COMBS, 2008] e é baseado no código do tcpdump [TCPDUMP-TEAM, 2007]. O segundo agente foi utilizado para analisar a camada 2, é conhecido como *serial tun* e está incluído na distribuição de 6LoWPAN do TinyOS.

O Wireshark foi particularmente útil na avaliação e análise da reconstituição dos pacotes pelo 6LoWPAN na camada 3. A Figura 5.3 apresenta a interface do wireshark ao capturar um pacote de uma mensagem PONG com seus respectivos campos. A area 1 mostra a informação geral

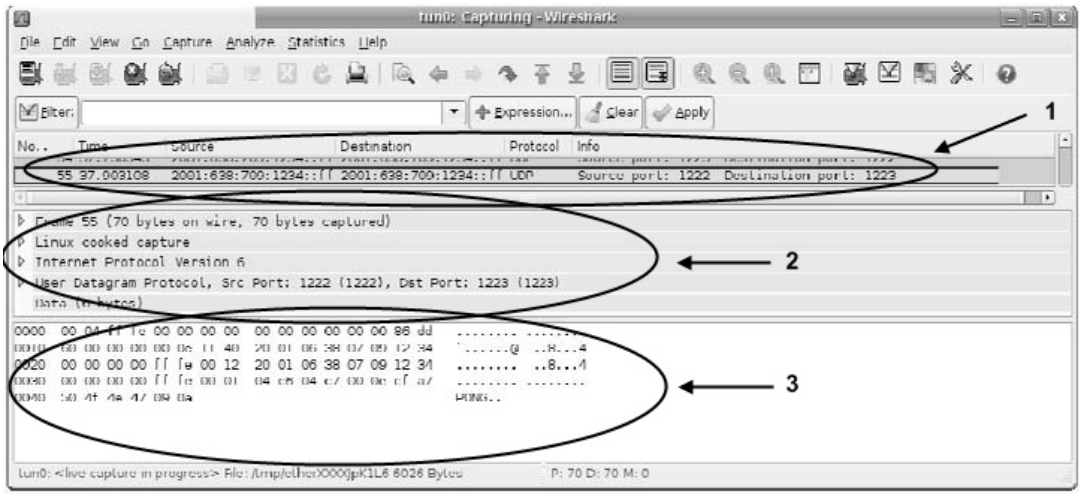

Figura 5.3: *A Interface do Wireshark*

acerca do pacote (*Source Address, Destination Address, Transport Protocol = UDP, Source Port and Destination Port*), a area 2 mostra a informação detalhada acerca do pacote (*Size, Operating System, Version, etc*) e a area 3 mostra o conteúdo do *payload*.

A aplicação *serial tun* permite a comunicação TCP/IP através da porta serial, fazendo-a trabalhar como se fosse uma porta ethernet. Também faz o papel de sniffer, capturando os quadros e mostrando-os. A Figura 5.4 mostra a interface do serial tun capturando um quadro durante a avaliação de desempenho que executamos. A area 1 mostra a compressão sofrida pelo pacote IPv6, a area 2 mostra que o tamanho do pacote após a compressão é de 57 bytes, a area 3 mostra o endereço IPv6 de origem e a area 4 mostra o endereço IPv6 de destino. Após a reconstituição do pacote, como apresentado na Figure 5.3, o tamanho do mesmo será de 70 bytes.

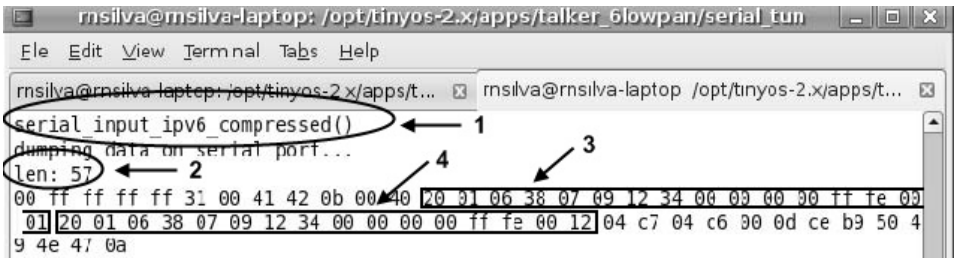

Figura 5.4: *A Interface do Serial tun*

Os *sniffers* foram também úteis para observar o comportamento da aplicação e replica-lo no ambiente simulado. A aplicação de monitoramento da bateria reportou valores que estão resumidos na Tabela 5.1. O valor *Base* é a quantidade, em milivolts, que a carga bateria decresceu

em 30 minutos, neste cenário o nó sensor enviava uma mensagem com o valor da bateria a cada 5 segundos. As medidas revelam que, comparado com o cenário do 6LoWPAN puro, a abordagem proposta pelo 6GLAD proporcionou uma diminuição de 38% no impacto nas baterias do nó sensor. Cabe salientar que não foi levado em consideração o fato de que o comportamento de descarga da bateria é não-linear. No entanto, os valores de descarga medidos a cada 5 segundos comportaram-se de forma homogênea para todos os cenários.

Tabela 5.1: *Redução na carga da bateria após 30 minutos*

Scenario	Base	6GLAD	6LoWPAN	IPv6
mV reduced	1,99	7,23	11,72	17,97

5.2 Simulação e Resultados

A fim de avaliar o impacto do *overhead* de comunicação em RSSF mais numerosas, o 6GLAD foi simulado utilizando o Network Simulator-2 (NS2). Foram gerados 8 cenários, utilizando-se o gerador de topologias GenSeN [CAMILO, 2007], A variável foi o número de nós, as demais características (estratégia de *deployment* = 'aleatório', orientação de antena = 'uma', nível de energia = 'igual para todos'). O GenSeN gera topologias para RSSF baseado em estudos de *deployments* reais. Uma vez que o *overhead* de comunicação é o foco do estudo desta simulação, não nos preocupamos aqui em ajustar os níveis energéticos dos sensores no simulador. Desta forma, todos os sensores transmitem com o mesmo alcance e possuem a mesma quantidade de energia. A primeira topologia foi gerada com apenas um agente 6GLAD e 2 nós sensores, tal como foi avaliado na plataforma de testes. O número de nós sensores presentes no cenário simulado foi sendo aumentado em escala exponencial, os cenários foram simulados com 4, 8, 16, 32, 64, 128 e 256 nós.

Na simulação, uma aplicação com as mesmas características de tamanho de pacote e tráfego foram simuladas. Para verificar o comportamento da rede com a implantação do 6GLAD, um agente para o NS-2 foi implementado para enviar e receber informação dos nós sensores. A Figura 5.5 ilustra a sobrecarga protolocar relacionada a cada uma das 3 abordagens: 6LoWPAN com 6GLAD, 6LoWPAN puro e IPv6 puro durante 30 minutos de simulação.

Os resultados revelam a eficiência do 6GLAD na redução de sinalização para todos os cenários. Comparado com a versão pura do 6LoWPAN, o 6GLAD minimiza o *overhead* em aproximadamente 27% sobre todos os cenários. Quando o 6GLAD é comparado com um cenário IPv6 puro, ele reduz a quantidade de *overhead* em 27% quando o cenário é composto por 2 nós sensores e em até 40% quando o cenário possui 256 nós sensores. Os resultados relatados nesta seção foram publicados no *Brazilian Workshop on Realtime and Embedded Systems* 2008 [ZIMMERMANN, 2008b].

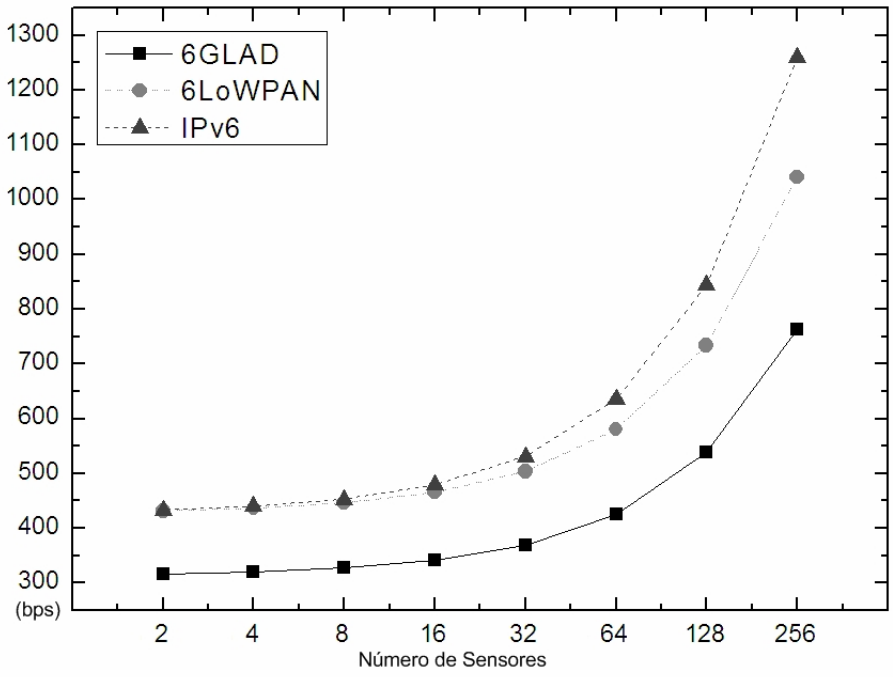

Figura 5.5: *Consumo de largura de banda por cenário*

6 Conclusão e Trabalhos Futuros

O protocolo proposto pelo grupo de trabalho 6LoWPAN da IETF foi estudado e as análises que fizemos aponta-o como uma tecnologia com potencial para fazer emergir uma nova geração de RSSF, transparentemente integradas a outras redes de nova geração. No entanto, nossos estudos demonstram que, em cenários de conectividade global, o 6LoWPAN perde significativamente sua capacidade de compressão de cabeçalhos. A fim de estender as vantagens do 6LoWPAN também para cenários de comunicação global, propusemos uma arquitetura denominada 6GLAD - *Global to Link-layer Address Translation for 6LoWPAN Overhead Reducing*. A abordagem utilizada foi a de explorar os mecanismos 6LoWPAN de supressão de cabeçalhos IPv6 via uma arquitetura que atua de forma transparente, tanto para as camadas superiores quanto para os demais agentes da RSSF.

Após análise teórica, avaliamos a arquitetura proposta via simulação e implementação em plataforma de testes, comparando-a com cenários sem a utilização da mesma. A análise teórica mostra que o 6GLAD ajuda o 6LoWPAN a reduzir 88,89% do volume do cabeçalho da camada de rede em cenários de comunicação global. Os experimentos em protótipos revelaram que, para a aplicação testada, a arquitetura proposta gastou 46% menos bateria que o esquema 6LoWPAN puro e as simulações no NS-2 mostraram que, em termos de economia de largura de banda, o uso da arquitetura 6GLAD proporcionou ganhos de 27% comparados ao 6LoWPAN puro.

Como trabalhos futuros, pretendemos estender as funcionalidades do agente 6GLAD desenvolvido para o NS-2, visando dar maior flexibilidade e facilidade de uso. A arquitetura pode ainda ser estendida para permitir múltiplos agentes 6GLAD, eliminando o ponto único sujeito

à falhas. Pode ainda ser estendida para atuar na camada de transporte, alterando as portas de comunicação UDP e explorando os mecanismos 6LoWPAN para compressão de portas. No que concerne a padronização, proporemos no 6LoWPAN IETF-WG o 6GLAD como uma funcionalidade extra no gateway 6LoWPAN. Estamos estudando ainda, como dotar a arquitetura de mecanismos de segurança e qualidade de serviço.

Referências Bibliográficas

[CAMILO, 2007] CAMILO, T. et al. Gensen: A topology generator for real wireless sensor networks deployment. **5th IFIP Workshop on Software Technologies for Future Embedded & Ubiquitous Systems**, 2007.

[CHAKRABARTI, 2007] CHAKRABARTI, S.; NORDMARK, E. **LowPan Neighbor Discovery Extensions - draft-chakrabarti-6lowpan-ipv6-nd-03**. [S.l.], March 2007.

[COMBS, 2008] COMBS, G. **Wireshark Network Protocol Analyser**. [S.l.], 2008. Disponível em: <http://www.wireshark.org>.

[CROSSBOW, 2008] CROSSBOW. Classroom kit for wireless sensor networks: Hardware datasheet. 2008.

[CULLER, 2007] CULLER, D. E.; HUI, J. 6lowpan tutorial: Ip on ieee 802.15.4 lowpower wireless networks. 2007.

[DEERING, 1998] DEERING, S.; HINDEN, R. Internet protocol, version 6 (ipv6) specification. December 1998.

[ESTRIN, 1999, p. 263–270] ESTRIN, D. et al. Next century challenges: Scalable coordination in sensor networks. In: **Mobile Computing and Networking**. [S.l.: s.n.], 1999. p. 263–270.

[HILL, 2000] HILL, J. et al. System architecture directions for networked sensors. **ACM SIGPLAN Notices**, p. 93–104, 2000.

[IEEE, 2003] IEEE. **Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)**. [S.l.], October 2003.

[IEEE, 2006] IEEE. **Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)**. [S.l.], September 2006.

[KARL, 2005] KARL, H.; WILLIG, A. **Protocols and Architectures for Wireless Sensor Networks**. [S.l.]: John Wiley and Sons Ltd, 2005.

[KASPAR, 2008] KASPAR, D. et al. Problem statement and requirements for 6lowpan mesh routing draft-dokaspar-6lowpan-routreq-05. DRAFT. April 2008.

[KUSHALNAGAR, 2007] KUSHALNAGAR, N.; MONTENEGRO, G.; SCHUMACHER, C. P. P. **IPv6 over low-power wireless personal area networks (6lowpans): Overview, assumptions, problem statement, and goals**. [S.l.], August 2007.

[MONTENEGRO, 2007] MONTENEGRO, G. et al. **Transmission of IPv6 Packets over IEEE 802.15.4 Networks**. [S.l.], 2007.

[MULLIGAN, 2007] MULLIGAN, G. The 6lowpan architecture. **EmNETS 2007: Fourth Workshop on Embedded Networked Sensors**, 2007.

[NARTEN, 2007] NARTEN, T. et al. Neighbor discovery for ip version 6 (ipv6). September 2007.

[SHIN, 2007] SHIN, M.-K. et al. Mobility support in 6lowpan draft-shin-6lowpan-mobility-01. November 2007.

[SRISURESH, 2001] SRISURESH, P.; EGEVANG, K. Traditional ip network address translator (traditional nat). IETF. January 2001.

[SRISURESH, 1999a] SRISURESH, P.; HOLDREGE, M. Ip network address translator (nat) terminology and considerations. IETF. August 1999a.

[SRISURESH, 1999b] SRISURESH, P. et al. Dns extensions to network address translators (dns_alg). September 1999b.

[TCPDUMP-TEAM, 2007] TCPDUMP-TEAM. Tcpdump: Computer network debugging tool. 2007.

[THUBERT, 2008] THUBERT, P. Lowpan simple fragment recovery draft-thubert-6lowpan-simple-fragment-recovery-00. March 2008.

[ZIMMERMANN, 2008a] ZIMMERMANN, A. et al. 6glad: Ipv6 global to link-layer address translation for 6lowpan overhead reducing. **4th EURO-NGI Conference on Next Generation Internet Networks**, 2008a.

[ZIMMERMANN, 2008b] ZIMMERMANN, A. et al. An efficient communication control approach for next generation wireless sensor networks. **10th Brazilian Workshop on Realtime and Embedded Systems**, 2008b.

[ZUNIGA, 2003] ZUNIGA, M.; KRISHNAMACHARI, B. Integrating future large-scale wireless sensor networks with the internet. **USC Computer Science Technical Report CS 03-792**, 2003.