UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA DE UM MODELO DE CONFIANÇA PARA O PROTOCOLO OLSR

JANAÍNA LAGUARDIA AREAL

ORIENTADOR: RICARDO STACIARINI PUTTINI

DISSERTAÇÃO DE MESTRADO
EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: 367/09 DEZEMBRO/2008

BRASÍLIA / DF: DEZEMBRO/2008

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA DE UM MODELO DE CONFIANÇA PARA O PROTOCOLO OLSR

JANAÍNA LAGUARDIA AREAL

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO REQUISITO PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

RICARDO STACIARINI PUTTINI, Doutor, UnB
(ORIENTADOR)

GEORGES DANIEL AMVAME NZÉ, Doutor, UnB
(EXAMINADOR INTERNO)

FLÁVIO ELIAS GOMES DE DEUS, Doutor
(EXAMINADOR EXTERNO)

DATA: BRASÍLIA/DF, 11 DE Dezembro 2008.

FICHA CATALOGRÁFICA

LAGUARDIA AREAL, JANAÍNA
Proposta de um modelo de confiança para o protocolo OLSR [Distrito Federal] 2008.
xix, 72pp., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2008).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica.

1. MANET 2. OLSR
3. CONFIANÇA COMPUTACIONAL

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

AREAL, J. L. (2008). PROPOSTA DE UM MODELO DE CONFIANÇA PARA O PROTOCOLO OLSR. Dissertação de Mestrado, Publicação 367/09 DEZEMBRO/2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, xix, 70 pp.

CESSÃO DE DIREITOS

NOME DO AUTOR: JANAÍNA LAGUARDIA AREAL
TÍTULO DA DISSERTAÇÃO: PROPOSTA DE UM MODELO DE CONFIANÇA PARA O PROTOCOLO OLSR
GRAU/ANO: Mestre /2008.

JANAÍNA LAGUARDIA AREAL
SQN 208 Bloco H apartamento 201
CEP 70.853-080 – Brasília – DF - Brasil

À Júlia.

AGRADECIMENTOS

Agradeço a Deus, por ter me permitido chegar até aqui.

Aos meus pais pela compreensão, apoio e carinho.

Aos amigos e colegas que, seja pelo apoio efetivo nas horas difíceis, seja pela simples companhia, de alguma forma, foram indispensáveis no meu equilíbrio emocional, durante o curso.

Ao Professor, Orientador e amigo Ricardo Staciarini Puttini, por ter me proporcionado esta oportunidade, pela paciência diante das dúvidas e dificuldades, pela dedicação, profissionalismo e tranqüilidade com que me guiou até a conclusão deste trabalho e pelo exemplo de vida e dedicação aos seus alunos.

Ao Professor e amigo, Rafael Timóteo de Sousa Júnior, pelas palavras, pelo apoio e orientação durante toda a jornada.

Ao professor Anderson Clayton Alves do Nascimento, pelo apoio e amizade durante o processo de aprendizado.

À equipe da RCIS (Research Center for Information Security), ao Professor Hideki Imai, ao Doutor Akira Otsuka, à Professora Frederique Oggier e à Doutora Hanane Fathi pela oportunidade de estagiar em uma das maiores equipes de pesquisa do mundo na área de segurança da informação, pelo apoio e por acreditar no meu trabalho.

À equipe do Labredes, em especial à Adriana pela amizade, pela ajuda nas horas difíceis e muito pela paciência durante todo o meu período de estudos. Ao Wesley e ao Wandemberg pela ajuda em todas as horas, pela amizade e por serem profissionais tão fantásticos.

À minha filha Júlia, que mais do que qualquer outra pessoa, tornou este, um sonho possível.

“Quando coisinhas pequenininhas tirarem você do sério, pare um segundo para contemplar o tamanho do sol ou a distância até as estrelas – isso sempre põe as coisas em perspectivas.”

Bradley Trevor Greive

RESUMO

Este trabalho apresenta um novo modelo de confiança computacional, desenvolvido para aprimorar o encaminhamento de pacotes em MANET que utilizam o protocolo OLSR.

Redes Móveis Ad hoc (MANET) são formadas de dispositivos móveis que se comunicam diretamente sem a necessidade de uma infra-estrutura prévia. Os nodos nestas redes atuam como roteadores. O protocolo *Optimized Link State Routing* (OLSR) é um dos protocolos em padronização para uso neste tipo de rede.

Os protocolos de roteamento para MANET não possuem mecanismos específicos de segurança. Assim, uma MANET está vulnerável a uma série de ataques relacionados ao protocolo de roteamento. Neste trabalho, abordamos os ataques de não colaboração relacionados ao encaminhamento de pacotes, isto é, quando um nodo assume a responsabilidade de encaminhar pacotes através da execução do protocolo de roteamento, mas não realiza essa operação conforme esperado.

O modelo de confiança proposto neste trabalho pretende avaliar qualitativa e quantitativamente a confiança computacional entre os nodos que participam do roteamento de uma MANET. Nossa proposta é baseada no modelo de J. Patel denominado *Trust and Reputation Model for Agent-based Virtual Organizations* (TRAVOS).

O modelo apresentado foi validado em um experimento do tipo prova de conceito. Para este experimento, o modelo proposto foi implementado como uma extensão do *daemon* UniK OLSRD (www.olsr.org). O modelo e a sua respectiva implementação foram testados em uma MANET real, com condições de operação hipotéticas.

Os resultados obtidos com a realização deste trabalho permitem evidenciar as seguintes contribuições:

- Apresentação e validação de um novo modelo de confiança computacional para melhorar a robustez do encaminhamento de pacotes em MANET.
- Implementação do modelo como extensão do *daemon* OLSR UniK.

ABSTRACT

This work presents a new computational trust model, developed to improve the packets forwarding in MANET using OLSR protocol.

Mobile Ad hoc Networks (MANET) are composed of mobile devices that communicate directly without the need of any prior infrastructure. The nodes in these networks operate as routers. The Optimized Link State Routing Protocol (OLSR) is a standard routing protocol in use on this type of network.

Routing protocols for MANET have no specific security mechanisms. Thus, a MANET is vulnerable to a variety of attacks related to the routing protocol. In this work, we tackle non-cooperation attacks related to the packet forwarding. This attack consist of a node that takes responsibility for packet forwarding through the binds of the routing protocol execution, but does not perform this operation as expected.

The trust model proposed in this work aims to evaluate qualitatively and quantitatively the computational trust between the nodes that participate in MANET routing. Our proposal is based on J. Patel's Trust and Reputation Model for Agent-based Virtual Organizations (TRAVOS).

The model presented was validated in a proof of concept experiment. For this experiment, the proposed model was implemented as an extension to the daemon Unik OLSRD (www.olsr.org). The model and its implementation have been tested in a real MANET with hypothetical operational conditions.

As results of this work we shall highlight the following contributions:

- Presentation and evaluation of a new computational trust model to improve the robustness of the packets forwarding in MANET.
- The actual implementation of the proposed model as an extension to the Unik OLSR daemon.

SUMÁRIO

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DE ACRÔNIMOS

ACK - Acknowledgement
AODV - Ad hoc On-Demand Distance Vector Routing
AP - *Access Point*
ANSN - Advertised Neighbor Sequence Number (OLSR)
BSS - Basic Service Set
CCA - Clear Channel Assessment
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
CTS - Clear to Send
DCF - Distributed Coordination Function
DFWMAC - Distributed Foundation Wireless MAC
DIFS - DCF Inter-Frame Spacing
DHSS - Direct Sequence Spread Spectrum
DSDV - Destination-Sequenced Distance Vector
DSR - Dynamic Source Routing Protocol
ESS - Extended Service Set
ETT - Estimated Transmission Time
ETX - Expected Transmission Count
FHSS – Frequency Hopping Spread Spectrum
GFSK - Gaussian Frequency Shift Keying
HNA - Host and Network Association (OLSR)
IANA - Internet Assigned Numbers Authority
IEEE - Institute of Electrical and Electronic Engineers
IETF - Internet Engineering Task Force
IP - Internet Protocol
LAN – Local Area Network
LQ – Link Quality
LQSR – Link Quality Source Routing
MAC - Medium Access Control
MANET - Mobile Ad hoc Network
MID - Multiple Interface Declaration (OLSR)
MPR - Multipoint Relay
NAV - Net Allocation Vector
NLQ - Neighbor Link Quality
OLSR - Optimized Link State Routing Protocol
PCF - Punctual Coordination Function
PSK - Phase Shift Keying
QoS - Quality of Service
RERR - Route Error
RFC - Request for Comments
RREP - Route Replay
RREQ - Route Request
RTS - Request to Send
SIFS - Short Inter-Frame Spacing
TC - Transmission Control (OLSR)
TBRPF - Topology Broadcast based on Reverse-Path Forwarding
TND - T Neighbor Discovery (TBRPF)

TRAVOS - Trust and Reputation Model for Agent-based Virtual Organizations
TTL - Time to Live
UDP - User Datagram Protocol
Wi-Fi - *Wireless-Fidelity*
WLAN - Wireless Local Area Network
WPAN - Wireless Personal Area Network

1. INTRODUÇÃO

A conectividade sem fio possibilitou uma revolução mundial no mercado de telefonia adicionando mobilidade na transmissão de voz, permitindo que as pessoas se mantenham conectadas umas as outras independentemente de suas localizações. Novas tecnologias pretendem realizar o mesmo com as redes de computadores, dentre as quais tem ganhando destaque às redes WLAN (*Wireless Local Area Network*) baseadas no padrão IEEE 802.11 [1].

As WLAN podem ser classificadas em redes com infra-estrutura e redes sem infra-estrutura. Neste trabalho serão consideradas as redes sem infra-estrutura, também conhecidas como redes móveis *ad hoc* ou MANET (*Mobile Ad hoc Network*) [2]. MANET é uma rede formada de dispositivos móveis, que se comunicam sem a necessidade de uma infra-estrutura, como por exemplo, um AP (*Access Point*). Neste tipo de rede, os nós dependem uns dos outros para estabelecer os caminhos de comunicação. Assim, a conectividade completa em uma rede *ad hoc* é estabelecida em nível IP e não em nível de enlace, sendo que os nós atuam também como roteadores [2].

Os protocolos de roteamento para redes *ad hoc* devem ser projetados levando em consideração aspectos de mobilidade, que acarretam mudanças constantes na topologia da rede [2]. O MANET *working group* do IETF executa os trabalhos relacionados à padronização dos protocolos de roteamento para este tipo de rede [3]. Até a finalização deste trabalho, foram publicadas *Request for Comments* (RFC) para os protocolos de roteamento *Ad hoc On Demand Distance Vector* (AODV) [4], *Optimized Link State Routing* [5], *Topology Dissemination Based on Reverse-Path Forwarding* (TBRPF) [6] e *Dynamic Source Routing* (DSR) [7]. Neste trabalho focamos nosso objeto de estudo no protocolo OLSR.

O OLSR é um protocolo pró-ativo, baseado em estado de enlaces. Tais algoritmos mantêm localmente informações sobre a configuração da rede e distribuem regularmente este conhecimento para outros nós. Utilizando-se destes dados, cada elemento calcula individualmente o melhor caminho para os destinos disponíveis. Cada roteador disporá a qualquer momento, de rotas pré-estabelecidas e nenhum tempo de descoberta será despendido quando uma comunicação for imediatamente requisitada.

Os protocolos de roteamento para MANET não possuem, em suas versões atuais, mecanismos específicos de segurança [8]. Assim, uma MANET que utilize um desses protocolos está vulnerável a uma série de ataques relacionados ao protocolo de roteamento [9]. Nós maliciosos que participam de uma MANET podem degradar o desempenho ou até impedir o funcionamento da rede executando vários tipos de ataques, tais como: obtenção de informações acerca da topologia da rede [10], fabricação e/ou modificação de mensagens do protocolo de roteamento [11][12] e não colaboração [10]. Neste trabalho, abordamos os ataques de não colaboração relacionados ao encaminhamento de pacotes, isto é, quando um nodo assume a responsabilidade de encaminhar pacotes através da execução do protocolo de roteamento, mas não realiza essa operação conforme esperado.

A confiança computacional vem sendo desenvolvida e aplicada em diversos trabalhos relevantes [13][14]. Esse conceito tem sido estendido e utilizado para aplicação em MANET [16][17][18][19][20][21][22]. Em especial, estamos interessados no estudo e adaptação de modelos de confiança para ambientes de computação distribuída, visando obter melhorias nos processos de roteamento em redes móveis *ad hoc*. Nesse sentido, pretende-se avaliar qualitativa e quantitativamente a confiança computacional existente entre os nodos que participam do roteamento de uma MANET, partindo-se da premissa que são considerados confiáveis os nodos que executam o protocolo de roteamento e o conseqüente encaminhamento de pacotes em nível IP conforme a especificação. Neste trabalho, tal avaliação é baseada principalmente no modelo de confiança proposto por J. Patel e denominado *Trust and Reputation Model for Agent-based Virtual Organizations* (TRAVOS) [15].

A exemplo do que ocorre com os principais modelos de confiança computacional estudados, tal avaliação deverá ser realizada a partir de evidências coletadas da observação de interações passadas entre os nodos e da troca de informações entre os nodos acerca das evidências coletadas.

O objetivo deste trabalho consiste na apresentação de um modelo de confiança computacional para aprimorar o encaminhamento de pacotes em MANET que utilizam o protocolo OLSR.

Nossa proposta possui as seguintes características:

- Modelo de confiança que classifica os nós vizinhos em confiáveis e não-confiáveis, possibilitando a exclusão de nodos não confiáveis do processo de

escolha de rotas do protocolo OLSR a partir da avaliação objetiva da confiança, eliminando os nós considerados não-confiáveis do roteamento multisalto (encaminhamento de pacotes).

- O modelo de confiança opera de modo colaborativo, mas preservando a autonomia de cada nó da rede, a fim de aproveitar os seguintes aspectos característicos das redes MANET: colaboração, distribuição, natureza wireless do enlace de dados.
- Utiliza-se uma métrica que permite avaliar a confiança que um nó tem em relação a cada um de seus vizinhos levando em consideração tanto a confiança direta, que é baseada nas evidências coletadas pelo próprio nodo acerca do nodo avaliado, quanto à reputação, que consiste na utilização da opinião de outros nós acerca do nó avaliado, construída a partir da troca de informações entre nodos acerca da confiança observada.
- O modelo emprega um mecanismo de troca colaborativa de informação entre os nodos vizinhos acerca da confiança direta observada.
- O *overhead* de processamento e comunicação em relação ao processo OLSR padrão deve ser mantido em níveis reduzidos, com objetivo de não comprometer a viabilidade da solução em função das limitações de recursos em dispositivos computacionais móveis – típicos de redes MANET. Para tanto, aproveita-se da natureza proativa do OLSR. Isto é, o protocolo realiza sinalização periódica.
- O modelo deve ser robusto na presença de nós que divulgam informações de confiança imprecisas ou falsas. Para tanto, utiliza-se uma métrica de confidência que permita avaliar a acuidade da medida de confiança calculada.
- O modelo deve adaptar-se ainda às características dinâmicas das redes MANET, em especial no que se refere à obsolescência das evidências coletadas para avaliação da confiança, através da introdução de um parâmetro de *aging*.

A metodologia de realização deste trabalho pode ser descrita nas seguintes etapas e atividades:

- Revisão bibliográfica: Este trabalho foi iniciado com um amplo levantamento bibliográfico das publicações que abordam a tecnologia de MANET. Foram estudadas, em cada publicação, as características e vulnerabilidades de uma

MANET, seus protocolos de roteamento e modelos de confiança já propostas em publicações anteriores.

- Definição dos requisitos para o modelo de confiança: Foram definidos os requisitos que deveriam ser satisfeitos pelo modelo de confiança a ser projetado.
- Escolha do(s) modelo(s) de confiança computacional de referência: O modelo de confiança TRAVOS [15] foi escolhido como base para o projeto do modelo proposto neste trabalho. O modelo original foi modificado e adaptado para tratar confiança em MANET.
- Implementação da proposta: O modelo de confiança proposto foi implementado em software, como extensão (plug-in) do sistema OLSR UniK [23][24].
- Experimentos e Validação: A proposta foi validada por um ensaio do tipo prova de conceito, onde o modelo e a sua respectiva implementação foram testados em uma MANET real, com condições de operação hipotéticas.
- Ajustes finais e redação da dissertação.

As melhorias e a compatibilidade da confiança do OLSR adaptado à confiança com o OLSR padrão também foi verificada com êxito.

Os resultados obtidos com a realização deste trabalho permitem evidenciar as seguintes contribuições:

- Apresentação e validação de um novo modelo de confiança computacional aplicado à melhoria da robustez do encaminhamento de pacotes em MANET.
- Implementação do modelo como extensão do *daemon* OLSR UniK.

O restante deste trabalho está organizado da seguinte forma: O Capítulo 2 discute os conceitos necessários à formulação e entendimento da nossa proposta e descreve os trabalhos relacionados. O Capítulo 3 apresenta o modelo de confiança proposto. O Capítulo 4 apresenta os resultados experimentais obtidos no processo de validação do modelo proposto. Finalmente, o Capítulo 5 traz as conclusões e considerações finais do trabalho.

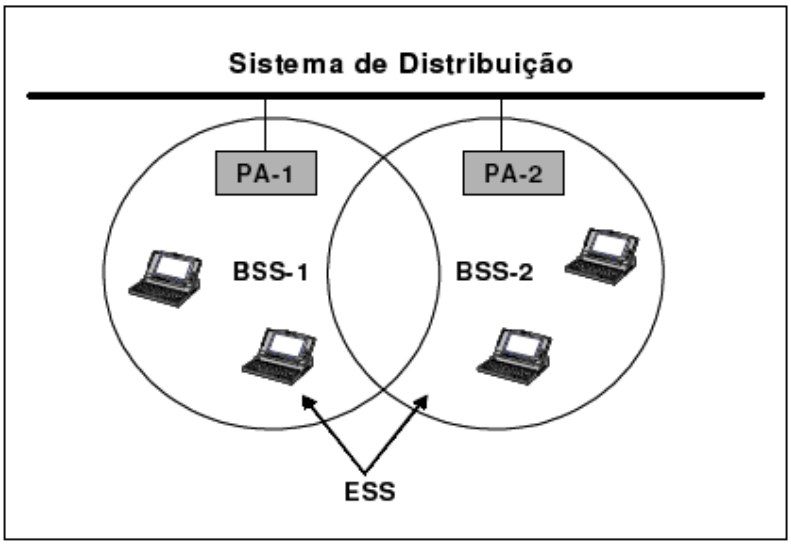
2. CONCEITOS E TRABALHOS RELACIONADOS

2.1. PADRÃO IEEE 802.11

O IEEE desenvolveu um padrão para redes locais sem fio (WLAN) que é identificado como IEEE 802.11 [1]. As redes wireless que fazem uso deste padrão são também conhecidas como Wi-Fi (*Wireless-Fidelity*). O projeto deste padrão foi iniciado em 1990 e seu escopo é desenvolver especificações detalhadas de controle de acesso ao meio (*Medium Access Control - MAC*) e da camada física para conexões wireless dentro de uma rede local (*Local Area Network* - LAN).

O IEEE 802.11 desenvolve uma série de especificações para um conjunto de equipamentos utilizados no estabelecimento de uma WLAN. Os padrões atualmente homologados são o 802.11b, que tem velocidade de 11 Mbps e opera na freqüência de 2,4 GHz; 802.11a, que opera na freqüência de 5 GHz e atinge velocidade de 54 Mbps; e 802.11g, que também opera em 2,4 GHz, mas tem velocidade de 54 Mbps. A definição do novo padrão 802.11n deverá impulsionar ainda mais a utilização das WLAN, pois com este novo padrão as redes poderão atingir até 540 Mpbs de taxa de transferência - o que o faz 50 vezes mais rápido que o 802.11b e 10 vezes mais rápido que o 802.11a e o 802.11g.

O padrão 802.11 implementa dois modelos de arquitetura para as redes móveis: infra-estruturado e *ad hoc*. O modelo infra-estruturado permite a comunicação dos dispositivos móveis com uma rede fixa. A área de cobertura é dividida em regiões menores denominadas células. Um grupo de dispositivos que se comunicam em uma célula constitui um BSS (*Basic Service Set*). O tamanho das células depende da potência de transmissão e recepção dos dispositivos, sendo que para a construção de redes maiores, múltiplos BSS são interligados através de um sistema de distribuição. Um elemento importante que permite a comunicação entre os dispositivos dentro de uma célula, ou mesmo entre BSS diferentes é o ponto de acesso. A interligação de vários BSS forma um ESS (*Extended Service Set*). A Figura 2-1 apresenta o modelo de arquitetura infra-estruturado para redes 802.11.

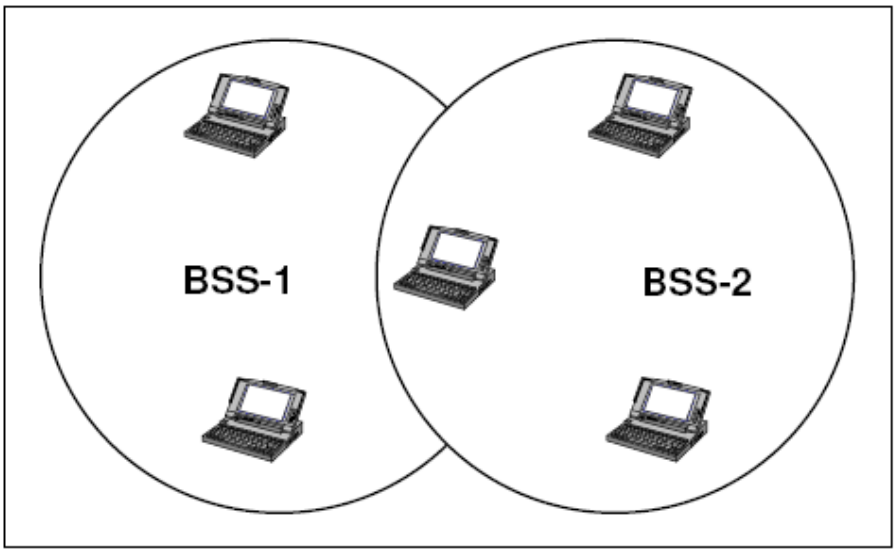


Fonte: *GAST, M. 2005 [1]*, com adaptações

Figura 2-1 - Modelo de Arquitetura Infra-Estruturado para Redes 802.11

O modelo de arquitetura *ad hoc*, adotado nas simulações realizadas para este trabalho, consiste em dispositivos móveis dentro de um mesmo BSS que se comunicam diretamente. A

A Figura 2-2 apresenta o modelo de arquitetura *ad hoc*.



Fonte: *GAST, M. 2005 [1]*, com adaptações

Figura 2-2 - Modelo de Arquitetura *Ad hoc* para Redes 802.11

A camada física do 802.11 é definida em três técnicas de acesso diferentes, são elas: espalhamento de espectro por salto de freqüência (FHSS – *Frequency Hopping Spread Spectrum*), espalhamento de espectro por seqüência direta (DHSS – *Direct Sequence Spread*

Spectrum) e infravermelho, sendo que todas elas utilizam o sinal CCA (*Clear Channel Assessment*) para identificar se o meio está livre ou não.

O DSSS é uma técnica de espalhamento de espectro, onde cada bit de dado é representado por múltiplos bits no sinal transmitido. Os dados são diretamente multiplicados por uma seqüência pseudo-randômica (também denominada chips) de alta taxa, resultando no sinal a ser transmitido. Este sinal é enviado somente após a aplicação da modulação PSK (*Phase Shift Keying*), sendo que a técnica de modulação por chaveamento de fase não necessariamente é a mesma para todas as taxas de transmissão. O 802.11 define um *chipping* de 11 bits, chamado de *Barker Sequence*, para codificar toda a informação a ser transmitida, ou seja, cada seqüência de 11 bits representa um simples bit do dado (0 ou 1).

Diferentemente do DSSS, o FHSS é uma técnica de espalhamento que divide a banda passante disponível em sub-canais de pequena largura e faz com que o transmissor e o receptor saltem para um outro sub-canal após ter estado, durante um determinado tempo, em um deles. Cada um destes sub-canais em uso são alterados de acordo com um código (seqüência) pseudo-randômico, sendo que o transmissor e o receptor devem estar sincronizados com relação ao padrão de saltos. O acesso básico desta banda utiliza uma modulação gaussiana por chaveamento de freqüência (GFSK – *Gaussian Frequency Shift Keying*).

Já a especificação do infravermelho usa comprimentos de onda de 850nm a 950nm. O infravermelho foi projetado para áreas internas. Os dispositivos recebem os dados por transmissões refletidas ou em linhas de visada. Opera com transmissões cujo alcance máximo é de 10 metros aproximadamente (ou 20 metros na ausência de interferências).

A camada MAC do 802.11 define um novo protocolo de controle de acesso ao meio, o DFWMAC (*Distributed Foundation Wireless MAC*), que suporta dois métodos de acesso, um obrigatório e baseado no controle distribuído e o outro centralizado, baseado em consultas realizadas por pontos de acesso aos dispositivos móveis, dando-lhes a permissão de transmissão e recepção dos quadros. Estes dois métodos podem coexistir, sendo o distribuído a base para o método centralizado.

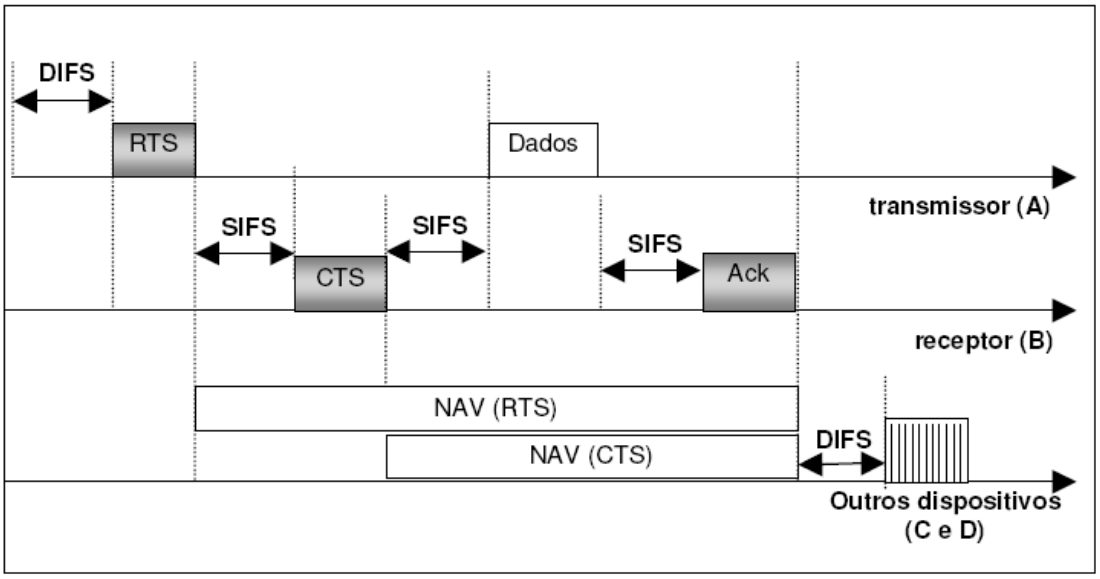
O método de acesso básico do DFWMAC, também conhecida como CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) com reconhecimento. Este mecanismo requer que cada dispositivo fique escutando a transmissão dos outros usuários. Se o canal está livre, o dispositivo deve aguardar um período de tempo em silêncio, para então

transmitir. Caso contrário, o dispositivo deve esperar que a transmissão do outro dispositivo finalize, mais o tempo que o receptor envie o reconhecimento, além de um novo período de silêncio. O DFWMAC adiciona ao método CSMA/CA com reconhecimento, um mecanismo opcional que envolve a troca de quadros de controle RTS (*Request to Send*) / CTS (*Clear to Send*) antes mesmo da transmissão dos quadros de dados.

O tempo de acesso para um dispositivo acessar o meio depende dos níveis de prioridade definidos pelo DFWMAC. Para o controle distribuído são utilizados dois níveis de prioridade: o *Short Inter-Frame Spacing* (SIFS), que representa o espaço entre quadros menores, sendo, portanto, o menor tempo de espera para acesso ao meio (maior prioridade) e o DCF *Inter-Frame Spacing* (DIFS), que representa o espaço entre os quadros da DCF, sendo este parâmetro o que denota o maior tempo de espera e, portanto, a menor prioridade de acesso ao meio.

O mecanismo de controle de acesso distribuído (*Distributed Coordination Function* - DCF) está ilustrado na Figura 2-3. Nesta figura, podemos observar que um dispositivo (A) com quadros para transmitir, deve primeiro escutar o meio livre por um período de silêncio mínimo (DIFS), antes mesmo de utilizá-lo. Quando este dispositivo ganha a posse do meio, ao invés de enviar imediatamente o quadro de dados, transmite um quadro de controle RTS, que carrega uma estimativa de duração no tempo da futura transmissão de quadros. O dispositivo receptor (B), em resposta ao quadro RTS, envia um quadro de controle CTS (que também armazena o tempo da futura transmissão) avisando que está pronto para receber os dados. Só então o transmissor envia os dados, que é respondido com um reconhecimento (ACK) enviado pelo receptor.

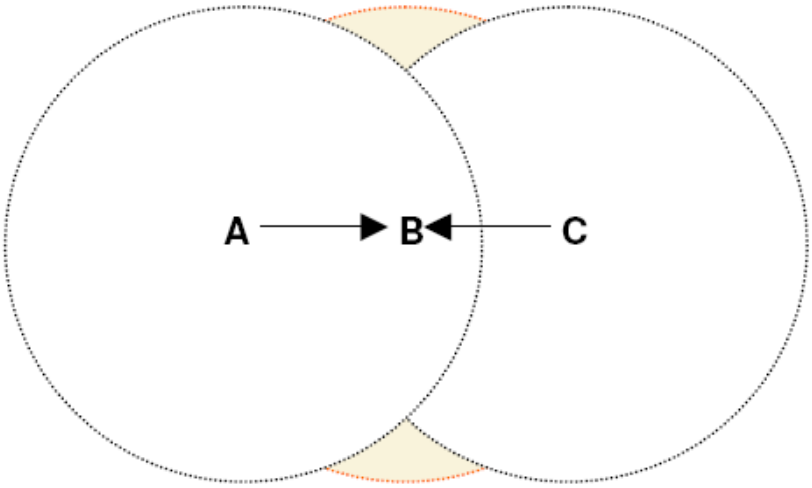
O SIFS é o tempo utilizado para a transmissão de quadros carregando respostas imediatas (CTS e ACK) como mostra a Figura 2-3. Se RTS e CTS não sofrem nenhuma colisão, todos os outros dispositivos que estão dentro da região de transmissão armazenam informações sobre a duração da transmissão subseqüente.



Fonte: *GAST, M. 2005 [1]*, com adaptações

Figura 2-3 - Método de Acesso do DFWMAC Distribuído

Nos sistemas de rádio baseados em detecção do meio, pode ocorrer um fenômeno conhecido como problema do "terminal escondido". Este problema aparece quando uma estação pode receber quadros de duas ou mais estações, mas estes terminais não estão dentro do mesmo raio de alcance de transmissão. Neste caso, um transmissor pode "ouvir" o meio e concluir erroneamente que não há nenhuma transmissão. No entanto, outra estação está transmitindo e isto pode gerar colisões no terminal receptor. A Figura 2-4 mostra uma situação onde existe a possibilidade de colisões no receptor provocadas pelo problema do "terminal escondido". As estações A e C estão dentro da mesma área de alcance do destino B, porém não recebem sinais uma da outra. O problema surge quando A e C enviam quadros simultaneamente para B, provocando colisões de quadros neste destino.



Fonte: *GAST, M. 2005 [1]*, com adaptações

Figura 2-4 - Problema do Terminal Escondido

Para solucionar este problema, pode ser utilizado o esquema de troca de dados de controle RTS e CTS da camada MAC. Quando um dispositivo de origem envia um quadro RTS e recebe a confirmação de reserva do canal para transmissão através de um quadro CTS do destino, todos os dispositivos dentro do raio de alcance tanto do transmissor quanto do receptor "escutam" estes quadros de controle. Considerando que tais quadros armazenam informações sobre a duração da transmissão subseqüente, a camada MAC de cada um dos dispositivos que recebe estes quadros sabe quando uma transmissão termina. Assim, as tentativas de transmissão ficam para depois do intervalo de tempo alocado. Estes valores que correspondem ao tempo de transmissão de outros terminais são armazenados em cada dispositivo através de tabelas denominadas NAV (*Net Allocation Vector*). Este mecanismo é conhecido como *Virtual Carrier Sense*. A Figura 2-3 apresenta este comportamento para os dispositivos C e D.

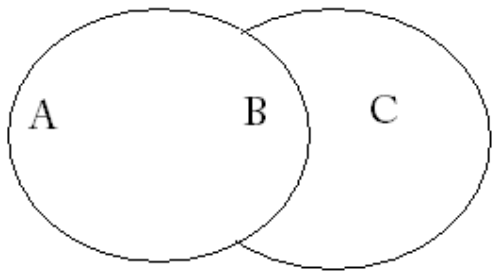
O método de acesso distribuído do DFWMAC não garante que um dispositivo consiga acessar o meio. Para oferecer um serviço determinístico, o padrão suporta opcionalmente um método centralizado, baseado na função de coordenação pontual (PCF – *Punctual Coordination Function*) centralizada. Utilizando o PCF, um ponto de acesso controla o acesso ao meio determinando, a cada momento, qual dispositivo deve transmitir. As redes *ad hoc* não utilizam esta função, devido à ausência de um ponto de acesso. Por este motivo, o método centralizado não será descrito neste trabalho.

2.2. MANET

Redes móveis *ad hoc* ou MANET consistem em uma coleção de dispositivos independentes de qualquer infra-estrutura, formando uma rede temporária e de forma arbitrária [2]. O grande interesse por esta tecnologia deve-se ao baixo custo, a facilidade de implantação e a grande variedade de aplicações que estas redes podem fornecer.

Cada um dos dispositivos que fazem parte da MANET possui uma interface sem fio e comunica-se com os outros dispositivos através de tecnologias de transmissão como ondas de rádio ou infravermelho. Estes dispositivos freqüentemente são móveis, mas também podem comportar-se como um ponto de acesso à Internet, por exemplo. A comunicação entre eles somente é possível quando um está dentro do raio de alcance do outro, sendo, portanto vizinhos imediatos. Conseqüentemente, um pacote que deve alcançar um destino, fora da área de transmissão da origem, deverá utilizar outros dispositivos intermediários como roteadores. Assim, cada dispositivo deve prover mecanismos de roteamento para outros dispositivos na rede, permitindo o estabelecimento de rotas entre pares de dispositivos com múltiplos saltos (*multi-hop*), ao contrário do que acontece nas redes infra-estruturadas, onde existem pontos de acesso fixos e centrais que permitam a comunicação com um simples salto (*single-hop*).

A Figura 2-5 apresenta uma MANET simples com apenas três dispositivos. Os dispositivos com identificações A e C não estão dentro do raio de alcance um do outro. Contudo, o dispositivo B pode ser utilizado como roteador para encaminhar mensagens de A até C. No entanto, o roteamento em redes *ad hoc* [2] não é tão simples como mostra a Figura 2-5. Em uma situação onde vários dispositivos estão se comunicando ao mesmo tempo em que se movimentam, mecanismos de roteamento que considerem a mobilidade dos dispositivos devem ser adotados.



Fonte: *GAST, M. 2005 [1]*, com adaptações

Figura 2-5 - MANET com três dispositivos

Quando comparadas com outras redes, as MANET apresentam vantagens e desvantagens, que devem ser consideradas antes mesmo de se adotar este padrão de redes móveis. Como vantagens, podemos citar [2]:

- Rápida instalação: formação de redes temporárias e arbitrárias sem a necessidade de uma infra-estrutura prévia para encaminhar e gerenciar mensagens pela rede.
- Tolerância a falhas: problemas em alguns dos dispositivos podem ser resolvidos com a reconfiguração dinâmica da rede, o que pode provocar retardos mais altos, mas a rede continua em um estado operacional.
- Conectividade: se dois dispositivos estão dentro do mesmo raio de alcance de transmissão, eles têm um canal de comunicação direto, diferentemente do que acontece nas redes infra-estruturadas ou mesmo nas redes fixas.
- Mobilidade: em contraposição à restrição de mobilidade em computadores fixos, ou a falta de comunicação enquanto um dispositivo move-se em uma região ausente de infra-estrutura prévia.

MANET apresentam, basicamente, os mesmos problemas relacionados a qualquer rede móvel devido à utilização de enlaces sem fio para a comunicação e a mobilidade dos dispositivos. Como principais desvantagens, podemos citar [2]:

- Banda passante: os enlaces de comunicação sem fio apresentam bandas passantes bem menores e limitadas devido a utilização do ar como meio de transmissão.
- Erros nos enlaces sem fio: a taxa de erros em um enlace sem fio é considerada muito alta, um bit errado para cada 105 a 106 bits transmitidos.
- Localização: para as redes fixas, os dispositivos podem ser localizados através do endereço IP, que indica implicitamente a localização de cada um deles. Nas redes *ad hoc*, localizar um terminal móvel é algo meio complicado, uma vez que não são disponíveis informações geográficas e o endereço do dispositivo não tem nenhuma relação com a sua posição.
- Roteamento: como nas redes fixas a topologia dificilmente se altera, não há necessidade de novas rotas serem estabelecidas freqüentemente. Nas redes *ad hoc*, os dispositivos movem-se livremente e de forma não-determinística, havendo a

necessidade de um mecanismo de roteamento específico que considere as características de mobilidade destas redes.

É importante ressaltar que os problemas de largura de banda variável, altas taxas de erros e localização dos dispositivos móveis são típicos de qualquer ambiente sem fio. Porém, o problema de roteamento é específico para as redes móveis *ad hoc*. A comunicação entre os dispositivos móveis em redes infra-estruturadas é responsabilidade das Estações de Rádio Base que se comunicam através de redes fixas [25].

Existem diversas razões que tornam o roteamento e a localização de um dispositivo móvel muito mais difícil em redes móveis do que em redes fixas. Podemos citar como principais motivos [26]:

- Mobilidade e topologia dinâmica da rede: os enlaces mudam freqüentemente de acordo com a mobilidade dos dispositivos móveis, o que provoca mudanças na topologia da rede;
- Vazão: uma das principais preocupações em MANET, já que o espectro é um recurso escasso, principalmente, em se tratando de aplicações multimídia;
- Retardo: requisito importante para praticamente todos os tipos de aplicações, especialmente aquelas que apresentam uma relação com o tempo, tais como áudio e vídeo;
- Inexistência de uma entidade central: a operação de roteamento em MANET é mais complexa pela ausência de uma entidade central que coordene a rede de forma completa;
- Comunicação através de enlaces sem fio: pode provocar problemas relacionados à conectividade, propagação de sinais e baixa velocidade do canal.

Existem várias tecnologias que podem ser utilizadas em MANET, entre elas o IEEE 802.11 [1], utilizado neste trabalho, e a tecnologia Bluetooth [27], que é um padrão para redes pessoais sem fio (WPAN).

2.3. PROTOCOLOS DE ROTEAMENTO PARA MANET

A combinação da comunicação sem fio e da mobilidade introduziu restrições inexistentes nos ambientes de redes tradicionais. Um dos principais desafios para as MANET

é determinar, de forma rápida, rotas válidas e eficientes entre pares de dispositivos, uma vez que a mobilidade provoca mudanças freqüentes na topologia da rede.

Se existe a necessidade de adoção de um protocolo de roteamento em redes *ad hoc*, por que não utilizar os protocolos de roteamento convencionais, já testados e adotados para vários ambientes de redes fixas. O principal motivo é que estes protocolos foram projetados para topologias estáticas e podem não convergir rapidamente quando houver a necessidade de se estabelecer rotas entre pares de dispositivos que se movimentam continuamente. Os protocolos de roteamento convencionais são baseados nos algoritmos de vetor de distância e de estado de enlace, que podem até ser utilizados em MANET com baixo nível de mobilidade dos dispositivos, ou seja, onde a topologia não muda freqüentemente. Estes protocolos utilizam tabelas para armazenar informações de roteamento entre os vários pares de dispositivos da rede.

Para manter estas informações atualizadas, mensagens de roteamento são propagadas, periodicamente e em broadcast, entre os dispositivos e os seus vizinhos (aqueles que estão em sua área de alcance). Porém, estas abordagens apresentam problemas quando adotadas em redes *ad hoc* [28]:

- As mensagens de atualização periódicas provocam um aumento na utilização da largura de banda da rede e no consumo de energia dos dispositivos, que são recursos escassos em ambientes de redes móveis;
- A transmissão entre dois dispositivos em uma rede de comunicação sem fio não trabalha necessariamente bem em ambas direções, pois antenas com alcances de transmissão diferentes podem ser utilizadas;
- A propagação de informações de roteamento, que depende do número de dispositivos existentes, pode provocar uma sobrecarga na rede à medida que aumenta o número de dispositivos, diminuindo, assim, a escalabilidade.

Uma vez que os protocolos de roteamento convencionais não atendem às exigências das MANET, é imprescindível a adoção de protocolos de roteamento específicos para estas redes. Corson e Macker [2] descrevem as características desejáveis para tais protocolos, entre elas:

- Operar de forma distribuída, ou seja, não ser dependente de nenhum ponto de acesso fixo e central;

- Garantir que as rotas estabelecidas sejam livres de loops;
- Adoção de múltiplas rotas, para evitar que os pacotes não sejam entregues por ausência de rotas;
- Suportar conexões unidirecionais e modos de operação dos dispositivos (*standby*) que consumam pouca energia das baterias.

Para julgar o mérito e o desempenho de um protocolo de roteamento, o grupo de trabalho MANET enumera algumas métricas que os protocolos devem seguir [2]. Essas métricas foram divididas em qualitativas e quantitativas e devem ser avaliadas independentes de qualquer protocolo de roteamento. A Tabela 2-1 descreve as métricas qualitativas de um protocolo de roteamento para MANET. A Tabela 2-2 mostra os pontos quantitativos que devem ser observados para analisar o desempenho de um protocolo de roteamento MANET.

Tabela 2-1 - Métricas qualitativas para um protocolo de roteamento para MANET

Métrica	Descrição
Operação distribuída	Propriedade essencial para o roteamento nas redes *ad hoc*, uma vez que a centralização de informações é inviável neste contexto.
Livre de loops	Para que os pacotes não fiquem trafegando durante um período de tempo relativamente grande na rede, pode ser usada como solução uma variável do tipo TTL (*time to live*), entretanto uma abordagem mais estruturada é indicada.
Operação sob demanda	O algoritmo de roteamento deve ser adaptável às condições de tráfego; se isto for feito de forma inteligente, os recursos de energia e largura de banda são utilizados de forma mais eficiente.
Operação pró-ativa	Em alguns momentos, a latência adicionada pela operação sob demanda poderá ser inaceitável; se os recursos de energia e largura de banda permitirem, operações pró-ativas são desejáveis.
Segurança	Se as camadas de rede e de enlace não garantirem segurança, os protocolos de roteamento estarão vulneráveis a muitas formas de ataque; é necessário que haja mecanismos adicionais para inibir modificações nas operações dos protocolos.
Operação no período de inatividade (*sleeping mode*)	Como resultado da necessidade de conservação de energia, os nós devem parar de transmitir e/ou receber pacotes durante períodos de inatividade, sem que isto resulte problemas significativos para o roteamento.

Tabela 2-2 - Métricas quantitativas para um protocolo de roteamento para MANET	
Métrica	Descrição
Atraso e desempenho de dados fim a fim	Dados estatísticos como variância, média e distribuição são muito importantes na avaliação da eficácia de um protocolo de roteamento.
Tempo de descobrimento da rota	Uma forma particular de medir o atraso do pacote fim a fim no que diz respeito aos algoritmos de roteamento sob demanda é o tempo requerido para estabelecer rotas quando requisitadas.
Porcentagem dos pacotes entregue fora da ordem	Medida externa para avaliar o desempenho do roteamento de protocolos da camada de transporte como TCP, que entregam os pacotes na ordem correta.
Eficiência	Se a eficácia do roteamento é uma medida externa na avaliação do desempenho, a eficiência é uma medida interna de sua efetividade. Se o tráfego de pacotes de dados e de controle deve compartilhar o mesmo meio, e a capacidade dos meios é limitada, então o tráfego excessivo dos pacotes de controle causará impacto no desempenho do roteamento.

Nenhum protocolo projetado possui características ótimas para todos os cenários. Assim, os trabalhos coordenados pelo grupo de trabalho MANET identificaram recentemente um conjunto protocolos de roteamento para MANET que deverão constituir um núcleo de protocolos que provejam, com abrangência e flexibilidade, o serviço de roteamento nos diversos cenários de aplicação das MANET. Até a finalização deste trabalho, foram publicadas RFC para os protocolos de roteamento *Ad hoc On Demand Distance Vector* (AODV) [4], *Optimized Link State Routing* [5], *Topology Dissemination Based on Reverse-Path Forwarding* (TBRPF) [6] e *Dynamic Source Routing* (DSR) [7].

2.3.1. Classificação

Os protocolos de roteamento para MANET são classificados em Reativos e Pró-Ativos.

Os protocolos pró-ativos tentam manter informações de roteamento consistentes para todos os dispositivos, já os protocolos reativos atuam sob demanda, criando e mantendo rotas somente quando requisitado por um determinado dispositivo.

2.3.1.1. Protocolos Reativos

Nos protocolos reativos a descoberta de rota é feita sob demanda, ou seja, somente quando um nodo deseja se comunicar com o seu destino. Após a rota ser estabelecida, ela é

mantida por um mecanismo de manutenção de rotas até que ela seja inacessível ou não ser mais apropriada.

Nesta abordagem o overhead de comunicação para determinação de rotas é diminuído, economizando banda e energia. Porém, apresenta um maior atraso no encaminhamento dos pacotes.

Devido a sua natureza de *flooding*, estes protocolos são escaláveis com relação à freqüente mudança na topologia da rede. Mas, não são quanto ao número total de nodos a menos que se utilize uma arquitetura hierárquica.

2.3.1.2. Protocolos Pró-Ativos

Os protocolos pró-ativos tentam avaliar continuamente a disposição dos nodos na rede com o intuito de ao ser solicitado um encaminhamento de dados, já se tenha o conhecimento da rota para o destino. Para tanto, cada host mantêm uma ou mais tabelas com informações referentes à rede e respondem a mudanças na topologia rede propagando atualizações a fim de manter a sua consistência. Estas atualizações são iniciadas por mecanismos de temporização.

A vantagem deste tipo de abordagem é o atraso mínimo para o envio dos dados, pois a rota pode ser obtida diretamente na tabela de roteamento. Entretanto, a atualização constante destas tabelas, causa uma contínua utilização da rede para troca de pacotes e informações de roteamento.

Estes protocolos são escaláveis em relação à freqüência da conexão fim-a-fim. Protocolos pró-ativos não são escaláveis com relação ao número de nodos, mas podem adquirir essa propriedade se for utilizada uma arquitetura hierárquica [29].

2.3.2. DSR

O DSR (*Dynamic Source Routing*) [7] é um protocolo de MANET sob-demanda que utiliza roteamento pela fonte, ou seja, o nó fonte adiciona a cada pacote de dados toda a rota até o destino. Quando todas as rotas já foram descobertas, não há *overhead* com mensagens de controle e caso haja uma mudança de topologia, desde que esta não influencie o roteamento, é ignorada pelo DSR.

Outra característica importante é a capacidade de armazenar múltiplas rotas para o mesmo destino, o que o diferencia de outros protocolos sob demanda e pode ser utilizado para

prover melhor qualidade de serviço, seja através da redundância ou do balanceamento de carga.

Como todos os pacotes de dados contêm o endereço de todos os nós até o destino, cada nó intermediário pode atualizar suas tabelas de roteamento com base nessa informação. Por outro lado, a grande desvantagem do DSR também está no fato de ele carregar toda a rota nos pacotes de dados, o que acarreta um overhead à medida que aumenta o número de saltos, ou seja, o cabeçalho de dados se torna maior.

2.3.2.1. Descoberta de Rotas no DSR

Quando um nó precisa de uma rota para um destino não presente na sua tabela de roteamento, ou que tenha expirado, ele efetua o procedimento de descoberta de rotas. Uma vez completado, ele encontra uma ou mais rotas para o destino, ou conclui que o destino não está alcançável. Nesse procedimento são utilizados dois tipos de mensagens: Requisição de Rota (RREQ - *Route REQuest*) e Resposta de Rota (RREP - *Route REPly*).

Os dois tipos de mensagem são identificados pelo endereço do nó de origem, definido como endereço iniciador (*initiator address*) e pelo identificador de broadcast (*broadcast id*). À medida que os pacotes são encaminhados, a estação verifica a existência desse par em seu *cache*, assim como se a mensagem excedeu o tempo de expiração. Caso o tempo tenha expirado, a estação descarta o pacote, caso contrário, ela o processa. Esse procedimento evita a formação de loops na rede, ou seja, rotas onde uma rota passa duas vezes por um mesmo nó não alcançando o destino.

Conforme mostra a Figura 2-6**,** o nó A inicia a inundação de uma RREQ para D e fica aguardando por uma ou mais respostas. Uma RREP é gerada se uma estação ou mais souberem de uma rota até o destino ou se a própria estação for o destino. No caso, o nó D vai emitir uma resposta de rota para C e este para B e finalmente para A. Se nenhuma rota for encontrada, o nó A deve tentar novamente a RREQ mais tarde. Cada nó que retransmite a RREQ armazena o seu identificador na mensagem retransmitida.

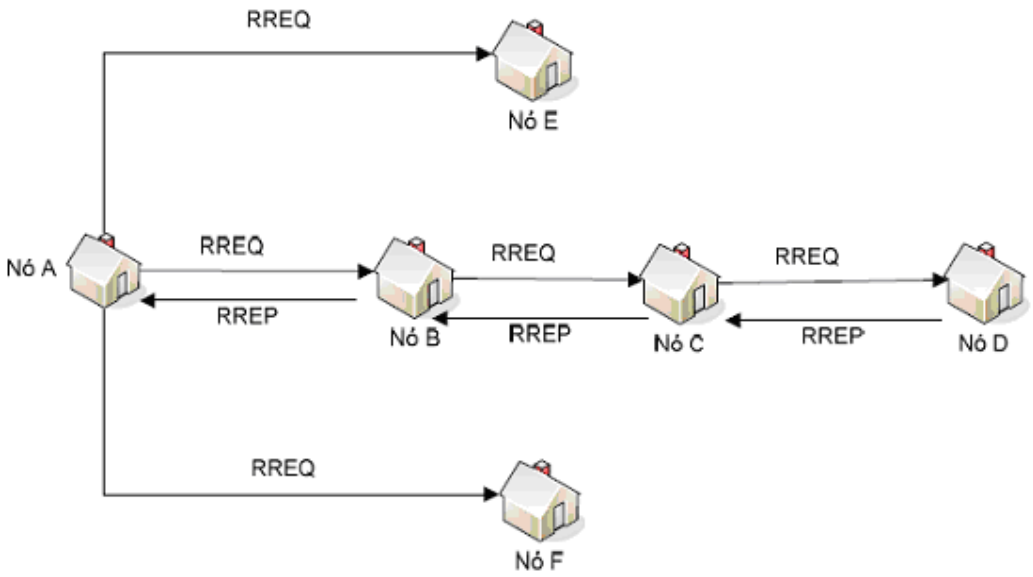


Figura 2-6 - Descoberta de Rotas DSR

Assim, quando a RREQ chegar ao nó D, ele terá a informação de toda a rota desse percurso, bem como cada nó intermediário terá do percurso até si, devendo então atualizar suas tabelas de roteamento. Nesse momento D envia em *unicast* à estação A uma RREP, que segue exatamente a rota reversa da utilizada pela RREQ.

2.3.2.2. Manutenção de Rotas no DSR

O mecanismo de manutenção de rotas é executado periodicamente e entra em ação quando um nó recebe um pacote de dados para um destino não mais conhecido, ou seja, quando durante o envio de dados o enlace para o salto seguinte deixa de estar operacional.

O nó que detectou o problema constrói uma mensagem de erro de rota (RERR – *Route ERRor*) e a envia ao iniciador. Ao receber essa mensagem, o iniciador apaga essa rota e procura por outra rota no *cache* de rotas de sua tabela de roteamento. Caso não exista uma rota, ele reinicia um novo processo de descoberta de rotas.

Quando um nó intermediário recebe um pacote de erro de rota, ele também deve apagar de sua tabela a rota correspondente, inclusive para todos os nós intermediários presentes no caminho antes do ponto de falha. No DSR, os nós ainda podem não só se utilizar das informações de rota dos pacotes sendo roteados por si, como também escutar outros pacotes da rede em modo promíscuo de maneira a manter atualizadas suas tabelas de roteamento. Nesse modo os nós processam também os pacotes de outros destinatários.

2.3.3. AODV

O protocolo AODV [2], assim como o DSR, também é um protocolo sob demanda, realizando a descoberta de rotas de forma semelhante ao DSR. A principal diferença é que o AODV confia no estabelecimento dinâmico das entradas nas tabelas de roteamento dos nós intermediários, ou seja, não utiliza roteamento pela fonte para os pacotes de dados e nem *cache* de rotas. A vantagem desse processo é o menor overhead dos pacotes com mensagens de controle, reduzindo a sobrecarga da rede.

Entretanto, o AODV envia muito mais pacotes de controle na rede para a descoberta e manutenção de rotas do que o DSR. Este, porém, utiliza pacotes maiores. Isso acontece porque o DSR possui acesso a muito mais informações de rota do que o AODV, como no processo de descoberta de rotas, onde cada nó intermediário pode aprender rotas para qualquer nó ao longo da rota. Ouvir a rede promiscuamente também pode dar acesso ao DSR a muitas informações de rota. Portanto, por possuir uma quantidade de informações mais limitada, o AODV depende de mais processos de descoberta de rotas, o que acarreta uma quantidade maior de pacotes de controle na rede [30].

2.3.3.1. Descoberta de Rotas no AODV

Da mesma maneira que o DSR, o AODV utiliza mensagens de Requisição de Rota (RREQ - *Route REQuest*) e Resposta de Rota (RREP - *Route REPly*), sendo identificados pelo endereço iniciador e pelo identificador de broadcast para evitar loops na rede.

Quando um roteador quer obter uma rota, envia o pacote de RREQ, que inunda a rede até que algum nó que conheça uma rota até o destino, ou o próprio destino, responda com um RREP. A mensagem de RREP contém apenas os endereços de fonte e destino, contador de saltos e número de seqüência do destino. Essas informações são usadas pelos nós intermediários que têm guardada a informação de rota do RREQ, ou seja, de quem veio essa mensagem. Com as informações do RREQ é formada a rota reversa para transmissão do RREP, além de que cada nó intermediário pode usá-la para atualizar sua tabela de roteamento.

Potencialmente, podem-se economizar mensagens de controle na rede, se depois outros nós vierem a pedir uma rota para o iniciador.

Uma diferença entre o AODV e o DSR é que no primeiro, cada rota possui um tempo de expiração, uma vez que cada nó não recebe atualizações sobre a validade de suas rotas, o

que ocorre no segundo caso. Assim, se a rota não for utilizada para transporte de dados após o tempo de expiração, ela é apagada. O AODV não possui a capacidade de suportar múltiplas rotas, diferente do DSR, onde toda a rota até um destino é armazenada.

2.3.3.2. Manutenção de Rotas

Quando um nó intermediário descobre uma falha de enlace, ou seja, não consegue encaminhar uma mensagem, ele envia ao nó de origem uma mensagem de RERR, da mesma maneira que o DSR.

Ao receber esse pacote, o nó de origem atualiza sua tabela de roteamento excluindo essa rota e inicia um novo processo de descoberta de rota. Conforme explicado no item anterior, se uma rota não for utilizada após um tempo de expiração, ela também é excluída.

2.3.4. TBRPF

O protocolo TBRPF [6] é também um protocolo que provê roteamento salto-a-salto ao longo de caminhos de número mínimo de saltos para cada destino.

Cada nó calcula uma árvore de origem que provê caminhos para todos os nós alcançáveis da rede, baseado em informação de topologia parcial armazenada em sua tabela de topologia, usando uma modificação do algoritmo de Dijkstra. Para minimizar a sobrecarga de controle, cada nó informa somente parte de sua árvore de origem aos vizinhos, ao contrário de outros protocolos, como o OSPF usado nas redes tradicionais interconectadas à Internet, que transmite a árvore de origem completa para seus vizinhos de um salto.

O TBRPF usa uma combinação de atualizações periódicas e diferenciais para deixar todos os vizinhos informados das atualizações. Se um enlace é usado por um vizinho para formar sua árvore de menor caminho, esse enlace será escolhido para as atualizações periódicas. Cada nó pode também reportar informações adicionais de topologia e até mesmo a topologia completa para garantir redes móveis mais robustas. O TBRPF faz a descoberta dos vizinhos usando mensagens *HELLO* "diferenciais" que informam somente as alterações ocorridas no estado dos enlaces para os vizinhos (ativo ou perdido). Isso resulta em mensagens *HELLO* menores que aquelas utilizadas em outros protocolos de roteamento do tipo LS como o OSPF e o OLSR.

Consiste de dois módulos separados: o primeiro é o Módulo de Descoberta de Vizinhos, denominado TND (T *Neighbor Discovery*), e o segundo é o Módulo de

Roteamento. O TND é que opera através do envio de mensagens *HELLO* "diferenciais" periódicas com seus vizinhos, informando somente as mudanças de estado dos enlaces (ativo ou perdido). O Módulo de Roteamento opera baseado em informação parcial de topologia, obtida através de atualizações periódicas e diferenciais de topologia.

Observe que em redes sem fio, é possível que uma única interface simples **I** receba pacotes de múltiplas interfaces **J** associadas com o mesmo nó vizinho. Isto pode ocorrer, por exemplo, se o vizinho usar uma antena direcional com diferentes interfaces representando diferentes feixes de transmissão. Por esta razão, o TBRPF inclui endereços de interface de vizinho nas mensagens *HELLO*, ao contrário do OSPF, por exemplo, que inclui somente os IDs do roteadores nos pacotes *HELLO*.

Cada nó TBRPF mantém uma tabela de vizinhos para cada interface local **I**, para conter informações de estado relativas a cada interface **J** de vizinho, percebida por I, como mostra a Figura 2-7. Isto é, para cada enlace (**I, J**) entre a interface I e uma interface de vizinho **J** é criada uma entrada na tabela de vizinhos de **I**. O estado de cada enlace pode ser unidirecional (1-*Way*), bidirecional (2-*Way*) ou perdido (*Lost*). A tabela de vizinhos da interface **I** determina o conteúdo das mensagens HELLO enviadas pela interface **I**, e é atualizada com base nas mensagens *HELLO* recebidas pela interface **I** (e possivelmente através de notificações da camada de Enlace).

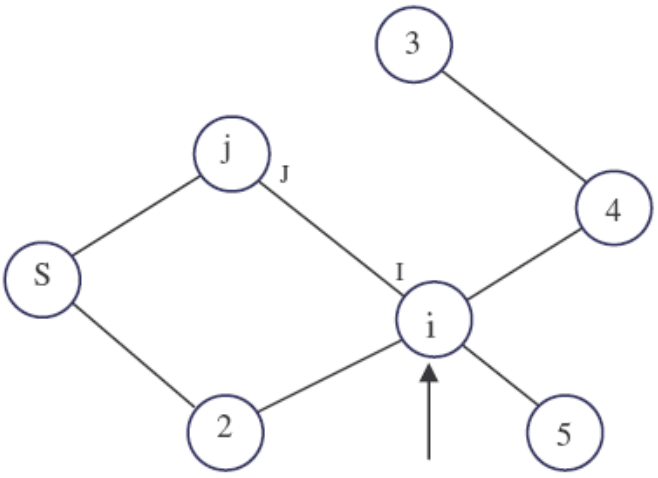


Figura 2-7 - Interface do nó i escuta pacotes de múltiplas interfaces do nó j

Cada nó TBRPF envia (em cada interface) pelo menos uma mensagem *HELLO* por *HELLO_INTERVAL*. Cada mensagem *HELLO* contém três (possivelmente vazias) listas de endereços de interfaces de vizinhos, que são formadas por três subtipos de

mensagens:*Neighbor Request, Neighbor Reply e Neighbor Lost*. Cada mensagem *HELLO* contém ainda o número de seqüência corrente de *HELLO* (HSEQ), que é incrementado em cada transmissão de *HELLO*.

Assuma que a interface **I** pertence ao nó **i**, e a interface **J** pertence ao nó **j**. Quando o nó **i** muda o estado de um enlace (**I, J**), ele inclui o endereço da interface de vizinho **J** na lista apropriada (*Request/Reply/Lost*) em, no máximo, *NBR_HOLD_COUNT* (tipicamente 3) *HELLO*s consecutivos enviados pela interface **I**. Isto garante que o nó **j** receberá, ainda, um desses *HELLO*s pela interface **J**, ou perderá todos os *NBR_HOLD_COUNT HELLO*s e assim declarará que o enlace (**J,I**) foi perdido (*Lost*).

Para entender como o TBRPF opera, imagine que o nó **S,** conforme mostrado na Figura 2-8, seja a origem das mensagens de atualização. Todo nó **i** na rede escolhe seu próximo salto (digamos, nó **p**) em seu caminho de menor número de saltos em direção a **S** como sendo seu nó pai com respeito a **S**. Em vez de inundar toda a rede, o nó **i** somente propaga as atualizações de **LS** (mensagens *HELLO*), originadas no nó **S**, se encaminhadas por seu nó pai (**p**) e retransmite-as, então, para seus filhos relativos a **S**. Mais ainda, somente as informações relativas aos enlaces que resultarem em mudanças na árvore de origem de **i** é que serão incluídas por **i** em suas mensagens de atualização.

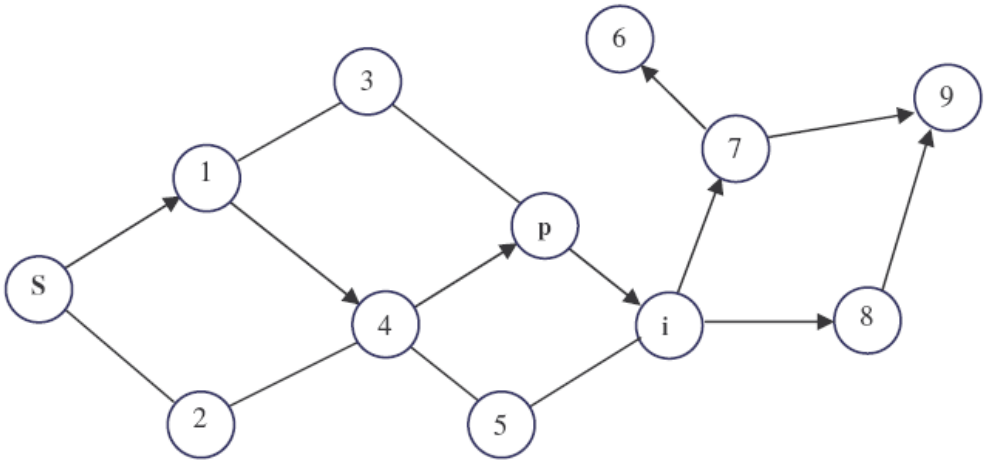


Figura 2-8 - Nó p é o pai do nó i no caminho de propagação a partir do nó S

O algoritmo utilizado reduz o tráfego de controle ao estabelecer que um nó só propaga as mensagens de controle relativas a uma rota informada anteriormente por um certo nó S, se a informação de atualização tiver sido encaminhada pelo seu nó pai em relação a S.

Como ele consiste de dois módulos separados de Descoberta de Vizinhos e de Roteamento, é possível experimentar outros algoritmos de descoberta de vizinhos que façam uso de recursos de localização, por exemplo, compondo-o com o módulo de roteamento, para ajustar seu desempenho de forma a melhor atender a um cenário específico.

2.3.5. OLSR

O OLSR (*Optimized Link-State Routing*) [5] é um protocolo pró-ativo, baseado em estados de enlace. Desta forma, periodicamente os nós inundam a rede com o estado de seus enlaces. Assim, todos os nós podem construir um mapa completo da topologia.

A RFC 3626 que especifica o protocolo OLSR, detalha todos os componentes para o funcionamento do protocolo. A seguir serão descritos somente os componentes essenciais para o entendimento deste projeto, a saber: o formato do pacote, a mensagem de *HELLO*, o cálculo do MPR, a descoberta de topologia e o cálculo da tabela de roteamento. São ainda definidos componentes para suporte a múltiplas interfaces (*Multiple Interface Declaration - MID*) e divulgação de gateways para a Internet (*Host and Network Association - HNA*). Entretanto, por não apresentarem relevância para a proposta deste trabalho, eles não serão detalhados.

Como todo protocolo pró-ativo, o OLSR disponibiliza rotas imediatamente. O que diferencia o OLSR de outros protocolos pró-ativos é que ele utiliza os chamados *Multipoint Relays* (MPR), que servem para diminuir o número de mensagens de controle na rede.

Normalmente, quando um nó recebe pacotes de controle sobre atualizações dos estados de enlace, ele retransmite essas informações para todos os seus vizinhos, esse mecanismo é denominado inundação. Dessa maneira cada nó pode receber o mesmo pacote dos seus vizinhos diversas vezes, gerando uma grande sobrecarga de controle na rede. Esse problema ainda é agravado pelo fato de o OLSR ser um protocolo pró-ativo, ou seja, estar sempre trocando informações. O objetivo dos MPR é minimizar esse problema através da seleção de nós que irão fazer a inundação.

Cada nó da rede escolhe os seus MPR, ou seja, nós designados para retransmitir os pacotes de controle. A escolha de um nó como MPR é baseada na premissa de que o nó consiga alcançar todos os seus vizinhos de dois saltos através do menor número de MPR possível. Ou seja, através dos MPR o nó de origem deve alcançar qualquer nó a dois enlaces de distância, de maneira que todos esses recebam as mensagens de controle da origem.

A Figura 2-9 ilustra o funcionamento desse tipo de rede e seu alcance. No exemplo da Figura 2-9a, é feita a inundação normal sem o uso de MPR. Já na Figura 2-9b somente os nós designados, que são os MPR do nó "A" (destaque) irão retransmitir os pacotes de inundação.

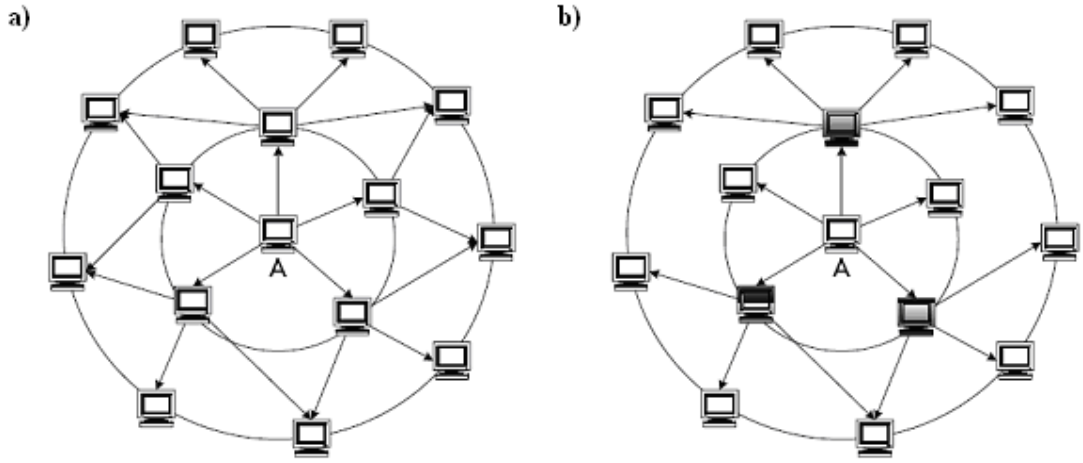


Figura 2-9 - Mecanismos MPR a) Inundação Normal; b) Inundação com MPR

Assim, como cada nó possui seus MPR designados, a comunicação entre quaisquer nós da rede é feita pelos MPR dos nós intermediários. Essa otimização faz com que esse protocolo produza menor sobrecarga de controle, principalmente para redes grandes e de alta densidade, sendo por outro lado melhor aplicável àquelas redes com pouca mobilidade, onde a topologia permaneça constante uma vez que não é gerado nenhum controle adicional de tráfego.

2.3.5.1. MPR

Os nós MPR possuem uma responsabilidade especial, pois informam o estado dos links da rede. Então, o único requerimento do OLSR para prover a rota de menor caminho para todos os destinatários é que os nós MPR informem o estado do link para seus seletores de MPR, isto é, os nós que escolheram como MPR.

Informações adicionais do estado de link podem ser utilizadas como, por exemplo, para redundância. Os nós que foram selecionados como MPR por algum nó vizinho anunciam essa informação periodicamente em suas mensagens de controle. No cálculo da rota, os MPR são usados para formar a rota de um nó dado para qualquer outro da rede. Mais ainda, o protocolo utiliza os MPR para facilitar a inundação das mensagens de controle de rede. O

OLSR foi desenvolvido para trabalhar independentemente de qualquer outro protocolo e não possui referência com a camada de enlace.

Para calcular o MPR, cada nodo seleciona, de maneira independente, seu próprio conjunto de MPR, entre seus vizinhos com os quais ele possui um enlace simétrico. O conjunto de MPR deve ser computado de modo que, através dos nós contidos neste conjunto, seja possível se atingir todos os vizinhos a dois saltos.

Para prover rotas para nós distantes a mais de 2 saltos, cada nodo mantêm informações sobre a topologia da rede. Essa informação é adquirida através de mensagens de controle de topologia (*Topology Control - TC*).

Os nós que foram selecionados como MPR por outros nós periodicamente geram mensagens TC, anunciando a lista de todos os nós seletores (MPR). Mensagens TC são disseminadas por *flooding* em toda a rede pelos MPR. Um campo de número de seqüência de mensagem (SN) é usado para evitar o processamento duplicado de mensagens. Este campo é gerado como uma seqüência de números inteiros, incrementada a cada mensagem gerada.

A escolha dos MPR por um nó se dá de maneira independente dos outros nós da rede. São utilizados apenas enlaces simétricos, que são anunciados aos demais nós através do campo tipo de vizinho presente na mensagem *HELLO*.

O algoritmo para a escolha dos MPR é executado para cada interface de rede física, sendo os MPR de um nó a união dos MPR de todas as interfaces. Toda vez que for detectada a entrada ou saída de um nó a até dois saltos de distância, o algoritmo de escolha dos MPR deve ser executado novamente.

O algoritmo para o cálculo do MPR é heurístico. Para realizá-lo, define-se:

- N = Conjunto dos vizinhos por um salto.
- N2 = Conjunto dos vizinhos por dois saltos, excluindo-se os membros de N e o próprio nó de origem.
- MPR = Conjunto de vizinhos selecionados como MPR.
- D(x) = Número de vizinhos com enlace simétricos de x excluindo-se todos os membros de N e o nó de origem, sendo x um membro de N.
- A(x) = Número de vizinhos de x em N2, sendo x um membro de N.

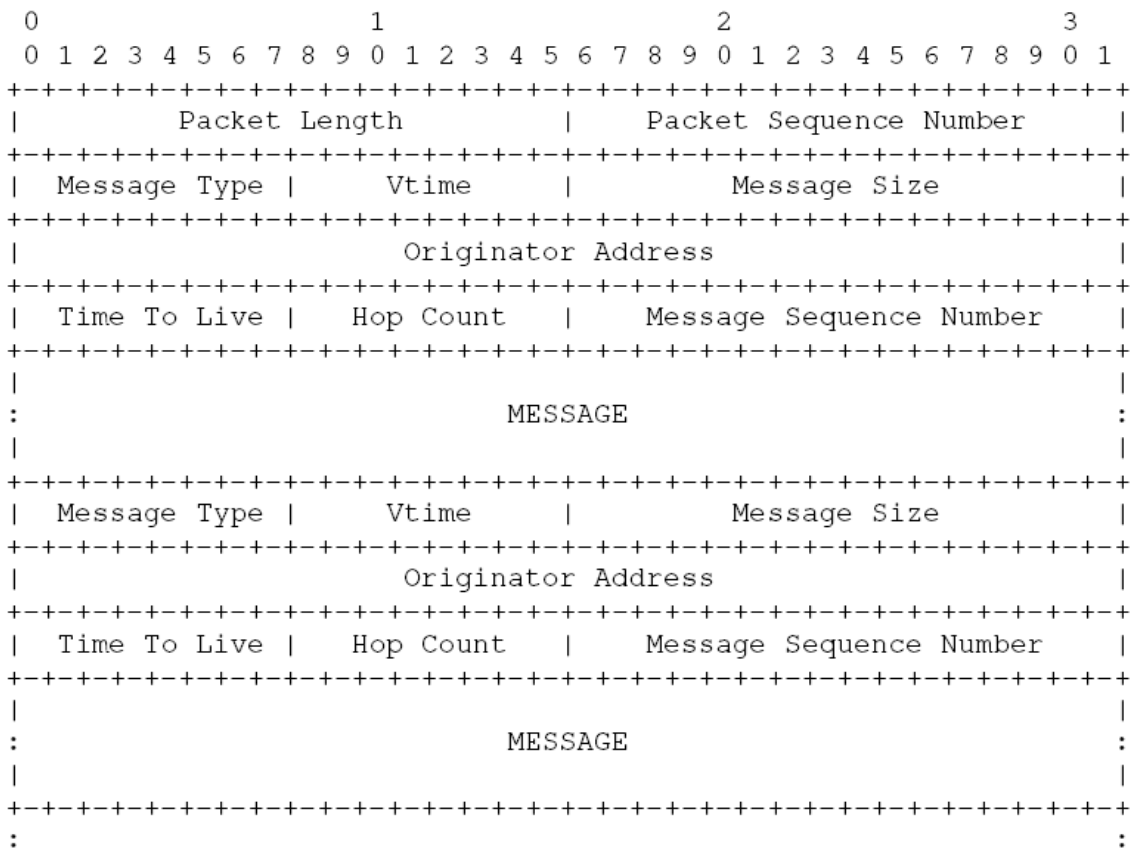
Resumindo, seu funcionamento é dado pelos seguintes passos:

1. Preencher os conjuntos N e N2 e deixar vazio o conjunto MPR.
2. Calcular D(x) para todo x que pertença a N.
3. Selecionar em N todos os nós que sejam os únicos a atingir algum membro em N2 e transferi-los para o conjunto MPR.
4. Excluir de N2 todos os nós vizinhos dos nós em MPR.
5. Calcular a alcançabilidade, que representa o número de nós em N2 que cada nó de N alcança.
6. Escolher o nó em N que possui a maior alcançabilidade entre os vizinhos em N2. Em caso de empate, escolher o que possui o maior D(x). Transferir o membro de N escolhido para MPR.
7. Excluir de N2 todos os nós vizinhos do novo membro em MPR.
8. Se N2 não estiver vazio, voltar ao passo 5.
9. Se N2 estiver vazio, fim do algoritmo.

Assim, no caso de redes com mudanças de topologia constantes, como por exemplo, causadas por maior mobilidade, é recomendado que se tenha um conjunto maior de MPR redundantes para evitar o recálculo desse algoritmo.

2.3.5.2. Formato do Pacote

O OLSR tem todos os seus pacotes de controle enviados sobre UDP (*User Datagram Protocol*), utilizando a porta de número 698, concedida pela IANA. O formato básico dos pacotes do OLSR omitindo cabeçalhos IP e UDP é descrito na Figura 2-10.



Fonte: RFC 3626 [5]

Figura 2-10 - Pacote do OLSR

O campo *Packet Lenght* representa o tamanho do pacote todo enquanto o campo *Packet Sequence Number* é um número que deve ser incrementado toda vez que um pacote é transmitido, sendo utilizado apenas para a detecção de perda de pacotes.

O campo *Message Type* representa o tipo de mensagem que é transmitida, como por exemplo, mensagens *HELLO* e mensagens TC, que correspondem aos tipos 1 e 2, respectivamente.

O campo *Vtime* representa o tempo de validade dos dados contidos na mensagem, caso o nó não venha a receber nenhuma nova mensagem com atualizações.

Os campos seguintes *Message Type, Originator Address* e *Time To Live* são, respectivamente, o tamanho da mensagem desde o campo tipo da mensagem até o fim do pacote ou o início da mensagem seguinte, o endereço IP de quem gerou a mensagem e o tempo de vida.

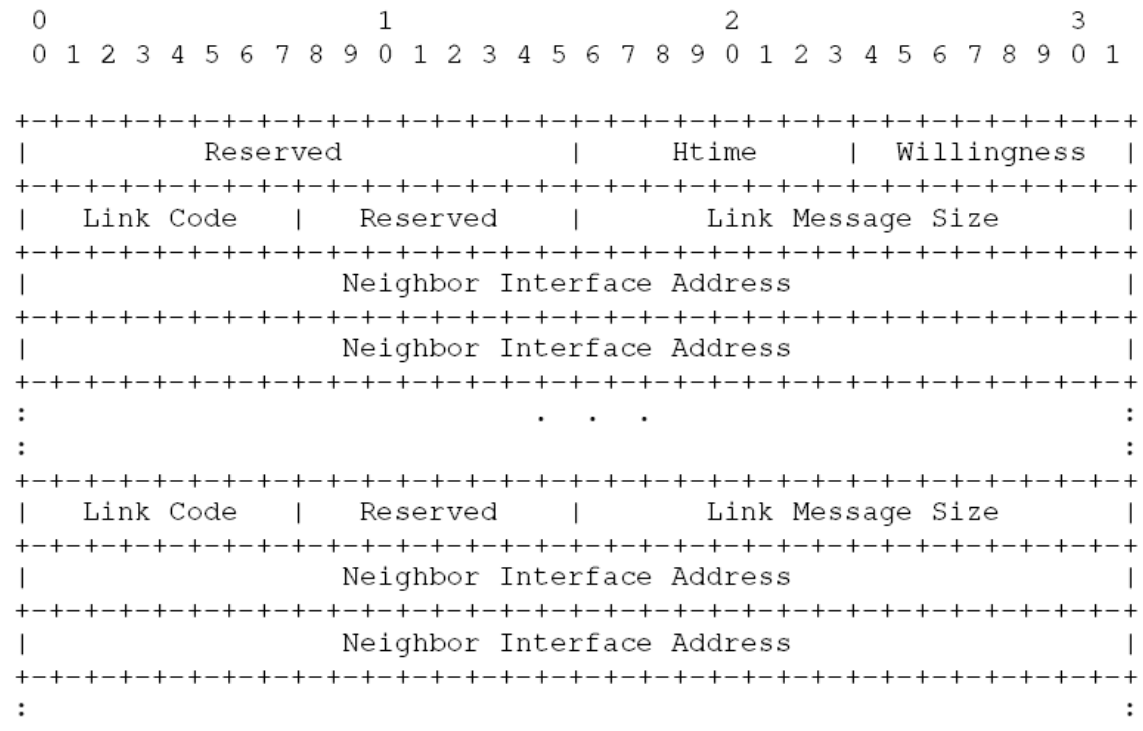
O campo *Hop Count* deve ser incrementado por todo nó antes de ser encaminhado e representa a distância em saltos percorrida pelo pacote.

O campo de *Message Sequence Number* contém um número de seqüência da mensagem tem por objetivo evitar que uma mensagem seja processada duas vezes pelo mesmo nó.

O campo MESSAGE contém as mensagens que são transmitidas pelo pacote do OLSR, onde cada pacote pode ter concatenado várias mensagens de maneira a diminuir a sobrecarga com pacotes de controle na rede.

2.3.5.3. Mensagem *HELLO*

A mensagem *HELLO* tem por objetivo tanto a descoberta de vizinhos e a sinalização da seleção de MPR, bem como a verificação da conectividade do enlace aos vizinhos. Essa mensagem não deve ser encaminhada pelos nós, por isso seu TTL (*Time to Live*) é colocado em 1. O formato da mensagem de *HELLO*, que corresponde ao campo MESSAGE do pacote na Figura 2-10 é mostrado na Figura 2-11**.**



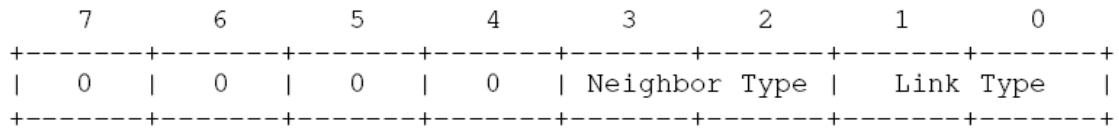
Fonte: RFC 3626 [5]

Figura 2-11 - Mensagem *HELLO*

O campo *Htime* especifica o intervalo de emissão desse tipo de mensagem. O campo *Willigness* especifica se o nó pode (WILL_DEFAULT), não pode (WILL_NEVER) ou sempre (WILL_ALWAYS) será selecionado como MPR.

O campo *Link Code* é divido conforme mostrado na Figura 2-12, onde *Link Type* indica para cada enlace do emissor do *HELLO* com um vizinho:

- *Symmetric*: o enlace foi verificado como simétrico.
- *Asymmetric*: a comunicação só foi verificada em uma direção.
- *Unspec*: indica que nenhuma informação especifica sobre o enlace foi dada.
- *Lost*: Indica que o enlace foi perdido.



Fonte: RFC 3626 [5]

Figura 2-12 - *Link Code*

O campo *Neighbor Type* indica, para cada enlace com um vizinho do nó que enviou o *HELLO*, que pelo menos uma interface desse vizinho tem conexão simétrica com o emissor (SYM_NEIGH), ou ainda que o enlace é simétrico e selecionado como seu MPR (MPR_NEIGH), ou é assimétrico ou indisponível (NOT_NEIGH).

Ao receber uma mensagem *HELLO*, o nó deve atualizar sua tabela de enlaces, ou seja, uma tabela que contém os vizinhos distantes um salto, incluindo as informações sobre o tipo de enlace e validade daquela informação (campo *Vtime*).

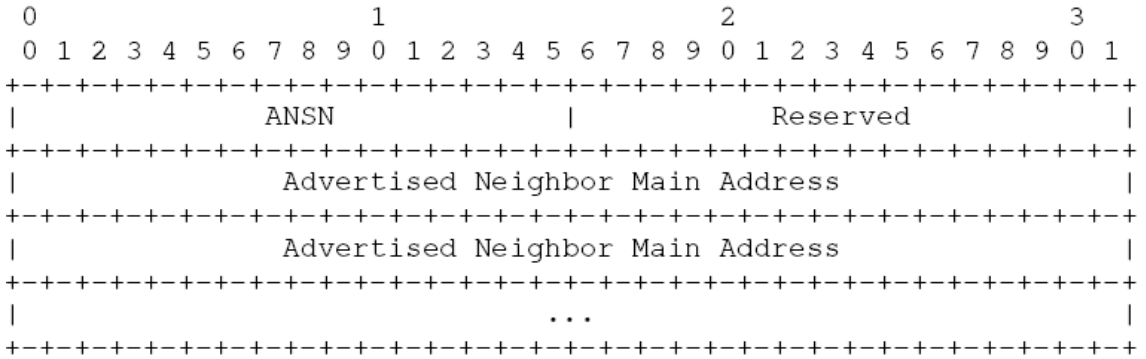
Da mesma maneira, o nó também deve atualizar a tabela de vizinhos distantes um salto incluindo a informação relativa à sua voluntariedade (ser MPR ou não). Note que essa tabela é parecida com a anterior, já que ambas funcionam em par. Entretanto, a primeira guarda informações relativas ao estado do enlace, enquanto que a segunda sobre o vizinho. No caso desse vizinho ter selecionado este nó como MPR, o que é indicado pelo campo tipo de vizinho igual a MPR_NEIGH, ele deve ser adicionado à lista de selecionador MPR. Essa lista identifica que nós selecionamos este nó como MPR.

O nó deve processar também as informações relativas aos nós distantes dois saltos dele, ou seja, aqueles com os quais seus vizinhos possuem alcance direto, mas com os quais ele não possui. Assim, para cada endereço listado no campo endereço da interface do vizinho, o nó deve checar se este não é o próprio e adicioná-lo à tabela de vizinhos distantes de dois saltos, incluindo o endereço do vizinho emissor do pacote e o tempo de validade da informação.

Em todas as tabelas, de enlaces, de vizinhos distantes de um salto e de vizinhos distantes de dois saltos, a informação é excluída da tabela caso o seu tempo de validade expire ou o campo estado do link da mensagem *HELLO* indique que o enlace deixou de existir ou, ainda no último caso, que se tornou assimétrico. A construção da mensagem *HELLO* é feita de maneira análoga à recepção, onde cada nó deve enviar as informações referentes à sua tabela de enlaces, de vizinhos e de seus MPR.

2.3.5.4. Descoberta da Topologia

Os mapas de topologia são construídos através da propagação das informações relativas aos vizinhos obtidas das mensagens *HELLO* e pelas mensagens de controle de topologia (Topology Control Messages – TC messages). Essas mensagens, cujo formato pode ser visualizado na Figura 2-13, são disseminadas pelos nós MPR, contendo informações suficientes para que cada nó construa suas tabelas de roteamento.



Fonte: RFC 3626 [5]

Figura 2-13 - Mensagem TC

O campo ANSN (*Advertised Neighbor Sequence Number*) representa o número de seqüência do anúncio. Toda vez que alguma mudança de topologia for detectada, esse número

deve ser incrementado. Esse mecanismo permite que os demais nós saibam qual é a mensagem mais recente sobre a topologia da rede.

Cada campo *Advertised Neighbor Main Address* contém o endereço de um nó vizinho ao emissor do pacote. Esse nó deve ser distante um salto e devem ser enviados na mensagem pelo menos os endereços dos nós selecionados como MPR do nó originador do pacote.

A mensagem de controle de topologia deve ser enviada com TTL de valor máximo e deve ser propagada de maneira a atingir todos os nós da rede. Através da lista de vizinhos contidos no pacote, cada nó obtém todas as informações necessárias para construir sua tabela de roteamento. Mesmo quando a tabela de vizinhos estiver vazia, o nó deve ainda assim enviar a mensagem TC de forma a que os demais nós possam atualizar suas tabelas de roteamento.

Ao receber uma mensagem TC, caso o enlace não exista na tabela de topologia, o nó deve adicionar para cada vizinho anunciado uma entrada contendo o endereço do emissor do pacote, o número de seqüência (ANSN) e o tempo de validade da informação.

A mensagem TC pode conter como redundância outros nós que não os MPR, o que ajudaria a criar outras rotas para o tráfego de dados. Existem três parâmetros de configuração definido: o primeiro, no qual só os endereços dos MPR são incluídos nos vizinhos anunciados, o segundo, onde além dos MPR, os nós selecionados para serem MPR de outros nós são enviados e, finalmente, o terceiro modo de operação onde todos os vizinhos são incluídos.

2.3.5.5. Cálculo da Tabela de Roteamento

A tabela de roteamento é construída com base nas informações contidas na tabela de enlaces e na tabela de topologia, sendo reconstruída quando uma dessas tabelas sofre uma mudança, ou ainda quando umas das tabelas de vizinhos distantes de um salto e de vizinhos distantes de dois saltos sofrem mudança.

Cada campo da tabela de roteamento, conforme a Figura 2-14 tem o seguinte significado:

- R_dest_addr: Endereço do destino da rota;
- R_next_addr: Endereço do próximo salto;

- R_dist: Distância em saltos até o destino;
- R_iface_addr: Interface de saída da rota.

```
1.  R_dest_addr    R_next_addr    R_dist   R_iface_addr
2.  R_dest_addr    R_next_addr    R_dist   R_iface_addr
3.      ,,             ,,           ,,         ,,
```

Fonte: RFC 3626 [5]

Figura 2-14 - Tabela de Roteamento

Para a construção da tabela de roteamento, os nós distantes de um e de dois saltos são adicionados com base nas informações das mensagens *HELLO*. Já para os outros nós, essas informações são baseadas na tabela de topologia construída a partir das mensagens TC com base nas informações de distância, endereço do nó de origem da mensagem e do vizinho anunciado.

Muitos nós podem ser utilizados como endereço do próximo salto (R_next_addr) para alcançar um destino (R_dest_addr), entretanto aqueles selecionados para serem MPR de outro nó são preferíveis como próximo salto. Pela forma como a sua rota é calculada, não é possível ter múltiplas rotas para um mesmo destino, uma vez que a cada vez que for calculada a tabela de roteamento, apenas uma rota para cada destino será obtida.

As entradas são gravadas na tabela de roteamento para cada destino na rede em que o caminho é conhecido. Todos os destinos, para os quais os caminhos estão interrompidos ou que seja conhecido "parcialmente", não são gravados na tabela de roteamento.

A tabela de roteamento é renovada quando ocorre uma mudança em:

- No conjunto de links,
- No conjunto de vizinhos,
- No conjunto de vizinhos a até dois saltos de distancia,
- Nas interfaces múltiplas associadas à base de informação.

Precisamente, a tabela de roteamento é recalculada no caso de um novo vizinho ou um vizinho perdido, quando um conjunto de nós a 2 saltos é criado ou removido, quando uma tupla de topologia é criada ou removida ou quando há mudança nas interfaces múltiplas associadas à base de informação. A renovação desta informação de roteamento não gera nenhuma mensagem a ser transmitida, nem na rede, nem na vizinhança a 1 salto de distância.

Muitos nós podem ser utilizados como endereço do próximo salto (R_next_addr) para alcançar um destino (R_dest_addr), entretanto aqueles selecionados para serem MPR de outro nó são preferíveis como próximo salto. Pela forma como a sua rota é calculada, não é possível ter múltiplas rotas para um mesmo destino, uma vez que a cada vez que for calculada a tabela de roteamento, apenas uma rota para cada destino será obtida.

2.3.5.6. Métricas de Roteamento para OLSR

ETX

A métrica ETX (*Expected Transmission Count*) visa minimizar o número esperado de tentativas de transmissão para uma transmissão com sucesso, incorporando os efeitos de taxa de perda, assimetria nas taxas de perda nas duas direções de um enlace e interferência ao longo dos sucessivos enlaces de um caminho. Nos protocolos de roteamento para MANET, mencionados anteriormente, o melhor caminho é aquele que minimiza a métrica número de saltos, a despeito da vazão em todos os caminhos possíveis.

Utilizando simplesmente a métrica número de saltos, os protocolos assumem que cada enlace ou está funcionando ou está inoperante e neste caso simplesmente não há nenhuma comunicação. Embora essa suposição seja muito próxima da realidade para redes cabeadas, não é o caso das redes sem fio. Enlaces com uma elevada taxa de perda de pacotes dados, entregando menos de 50% dos pacotes, mas ainda sim transportando mensagens de controle, seriam considerados da mesma maneira que enlaces com boa vazão.

A proposta da métrica ETX é encontrar caminhos que produzam o menor número necessário de retransmissões. Para isso a métrica prevê o número de retransmissões esperadas fazendo medições da taxa de perda de pacotes para cada enlace da rede. O objetivo é, assim, encontrar rotas com a melhor vazão.

Para tanto, se o ETX de um enlace é o número de transmissões necessárias para enviar um pacote sobre ele, o ETX de uma rota será a soma dos ETX de cada enlace. Em um teste descrito em [30], usando ETX com os protocolos DSR e *Destination-Sequenced Distance Vector* (DSDV), foram obtidas vazões melhores por uma razão de dois com o uso do ETX. Os resultados apresentados são melhores à medida que o número de saltos aumenta, mostrando a eficácia da métrica conforme a rede cresce.

No caso do protocolo OLSR a solução adotada foi diferente da vista em [1], uma vez que para medir a taxa de erro foi usado a própria mensagem *HELLO*, que já é transmitida periodicamente na rede, ao invés de se criar outro tipo de mensagem, evitando assim o aumento da sobrecarga de controle da rede. Uma desvantagem de seu emprego, é que sempre será enviado um pacote de tamanho pequeno, uma vez que a mensagem *HELLO* possui essa característica.

Como cada nó sabe que as mensagens *HELLO* são transmitidas periodicamente, ele pode medir a taxa de erro relacionando a quantidade de pacotes recebidos com a quantidade de pacotes esperados em uma determinada janela de tempo.

Por exemplo, se 3 em cada 10 mensagens *HELLO* não forem recebidas pelo vizinho, tem-se uma taxa perda de 3/10 = 30%. Assim, como 7 mensagens chegaram tem-se uma qualidade de enlace (*Link Quality* – LQ) de 70%.

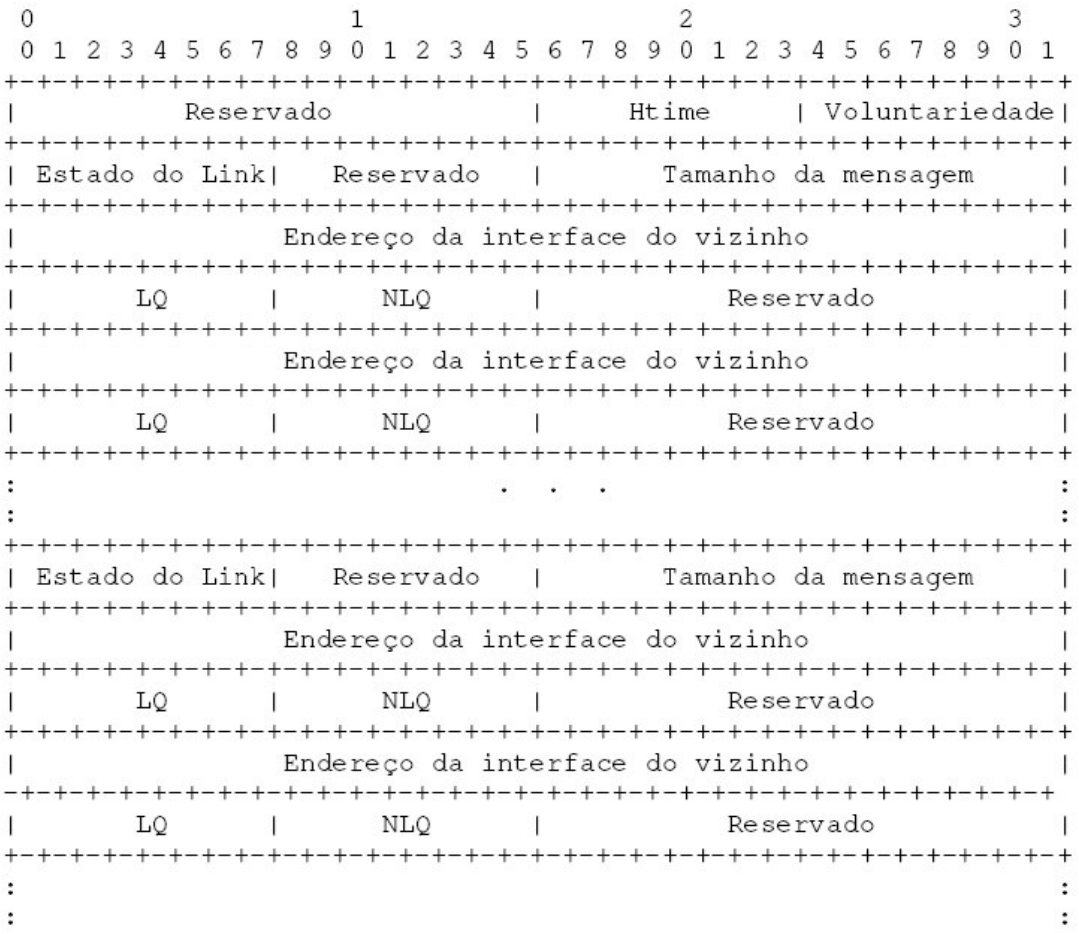
Entretanto, como os enlaces são bidirecionais, cada nó também obtém informações sobre a qualidade do enlace relativa aos pacotes que ele está enviando, ou seja, a visão que os vizinhos têm de seu enlace (*Neighbor Link Quality* – NLQ). Como ambos esses valores são enviados em percentagem, eles representam a probabilidade de um pacote atravessar um enlace com sucesso em cada direção. Assim, a probabilidade de sucesso de uma transmissão será o produto dessas: LQ x NLQ.

Pode-se concluir então que o número de tentativas esperado para que um pacote possa ser transmitido com sucesso pode ser visualizada na equação 2.1.

$$ETX = \frac{1}{LQ \times NLQ} \qquad (2.1)$$

É importante notar que esse valor é válido nos dois sentidos do trajeto, uma vez que haverá retransmissão tanto se o pacote de dados quanto se o respectivo ACK forem perdidos.

Finalmente, conforme mencionado anteriormente, o ETX de uma rota será a soma da métrica de cada enlace dos nós intermediários. Para incluir a informação de qualidade do enlace nas mensagens *HELLO* do OLSR, elas foram modificadas como proposto na RFC 3626 e mostrado anteriormente. Conforme a Figura 2-15, a nova mensagem chamada de LQ *HELLO* contém agora dados sobre a qualidade do enlace.

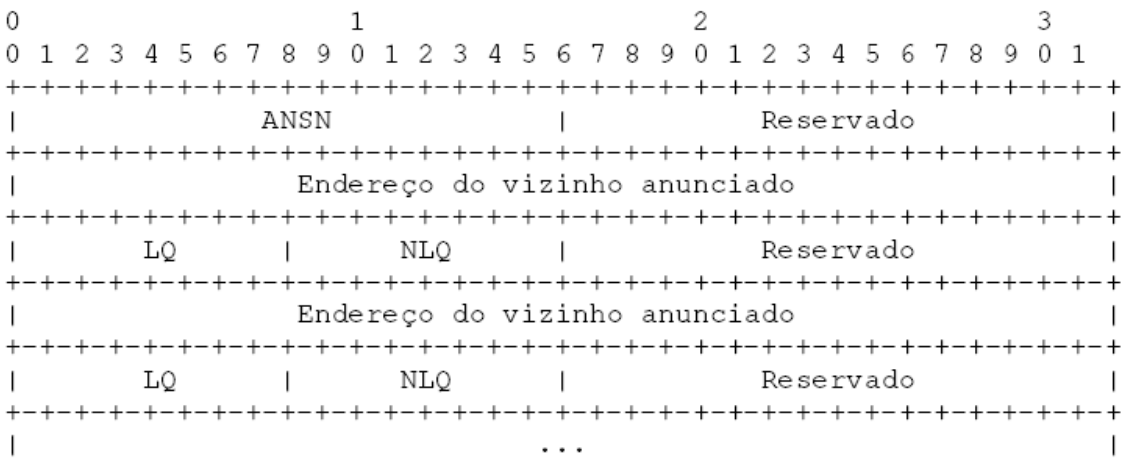


Fonte: RFC 3626 [5]

Figura 2-15 - Mensagem LQ *HELLO*

Após o endereço do vizinho foi incluída a informação relativa à qualidade do enlace nos dois sentidos.

Para transmitir essa informação para todos os vizinhos para que eles a considerem no cálculo da rota, também foi necessário alterar a mensagem de controle de topologia, que foi denominada LQ TC, e cujo formato é apresentado na Figura 2-16**.**



Fonte: RFC 3626 [5]

Figura 2-16 - Mensagem LQ TC

Da mesma maneira que na LQ *HELLO*, informações relativas à qualidade do enlace do nó que está enviando a mensagem com o respectivo vizinho são incluídas logo após seu endereço.

Para a construção da tabela de roteamento utilizando a qualidade da métrica é empregado o algoritmo de Dijkstra, onde é procurado em toda a topologia o caminho de menor custo entre dois nós.

ETT

Uma grande desvantagem da métrica ETX é levar em conta apenas a taxa de perdas em um dado enlace, para um tamanho pequeno de pacote. Uma métrica proposta para descrever de forma mais precisa a qualidade do enlace é a ETT (*Expected Transmission Time*) [31], que leva em consideração também o tempo de transmissão do pacote em cada enlace.

Em [31], foi desenvolvida uma solução baseada no protocolo *Link Quality Source Routing* (LQSR), onde essa métrica foi testada e aplicada. Neste trabalho, foi também proposta uma combinação dessa métrica onde são utilizados múltiplos rádios, entretanto como no nosso trabalho só foi testado e implementado o ETT, só nos ateremos a esse ponto.

Uma forma de calcular a métrica ETT é utilizar o valor do ETX, obtido como explicado anteriormente, e multiplicá-lo pelo tamanho do pacote dividido pela banda passante do enlace, de maneira a obter o tempo esperado de transmissão do pacote. Assim, se S for o

tamanho do pacote e B a banda do enlace teremos roteamento e apenas uma rota para cada destino será obtida como mostra a equação 2.2.

$$ETT = ETX \times \frac{S}{B} \qquad (2.2)$$

Para obter uma estimativa da banda passante do enlace, foi usado o método de pares de pacote, onde a cada minuto um nó envia um par de pacotes para os seus vizinhos. Nesse método, implementado em [21], esses pacotes são enviados em *unicast*. O primeiro pacote é pequeno, contém 137 bytes e o segundo é grande, de 1137 bytes. Quando um nó recebe esse par de pacotes, ele calcula a diferença de tempo e comunica esse valor de volta ao emissor. A banda é calculada após coletadas 10 amostras consecutivas e dividindo o tamanho do segundo pacote pela menor dessas amostras.

Essa medida pode não ter muita precisão, mas é suficiente para distinguir a qualidade de enlaces bons e ruins. Conforme resultados obtidos em [21], para taxas mais baixas, a precisão é maior, mas para mais altas o resultado subestima a taxa real de transmissão. Esse problema é causado devido ao fato de que o *overhead* envolvido na transmissão do pacote, como tempo para enviar um ACK, se tornam mais significativos à taxas mais altas.

De acordo com os resultados obtidos em [21], em ambientes com taxa de transmissão variável o ETT apresenta um desempenho 16% superior à métrica ETX e 38,6% superior à métrica número de saltos.

2.3.6. Segurança

Uma MANET apresenta alguns diferenciais em relação às redes sem fio estruturadas, tais como mobilidade, rápida instalação, alta conectividade entre os nós e tolerância a falhas devido à existência de diversas rotas entre os dispositivos móveis. Entretanto, a maioria dos protocolos de roteamento utilizados em MANET não utiliza mecanismos de segurança, pois assumem que o ambiente é composto apenas por nós com comportamento de acordo com a especificação do protocolo [3]. Esta suposição torna uma MANET vulnerável à presença de nós maliciosos, já que o roteamento depende dos nós intermediários que formam a rota entre a fonte e o destino de um pacote. Esses nós podem degradar o desempenho ou até impedir o funcionamento da rede através de vários ataques, dentro os quais: ataques de interrupção de roteamento e de consumo de recursos [9][12].

Enquanto estes ataques são possíveis em redes cabeadas, a natureza das redes sem fio aumenta seus efeitos, dificultando a detecção ou prevenção de ataques [12]. Simulações realizadas em [32] utilizando o protocolo DSR demonstraram que com a presença de 10% a 40% de nós maliciosos na rede, a vazão média da rede diminuiu entre 16% e 32%.

Várias pesquisas têm sido realizadas com o objetivo de evitar os problemas causados pela falta de segurança no roteamento através de protocolos de encaminhamento seguro para redes MANET. Algumas abordagens, baseadas em mecanismos de criptografia, propõem melhorar a segurança de alguns protocolos de roteamento existentes, como o OLSR [12][33], AODV [34][35] e DSR [36][37].

A segurança da transmissão de dados foi o principal objetivo de tais esforços, desconsiderando a topologia das informações. No entanto, estas abordagens permitem que todos os dados roteados sejam protegidos contra falsificação, mas não verificam a consistência da informação do protocolo de controle, *HELLO* e TC, não impedindo, portanto, que algum roteador malicioso divulgue uma informação incorreta sobre a topologia da rede.

Outro tema de investigação utilizada é o sistema de detecção de intrusão, para garantir a operação de encaminhamento (*forwarding*) em uma MANET. A maior parte desta pesquisa de baseia em uma arquitetura genérica distribuída, cada nó possui seu próprio sistema de detecção de intrusão local (LIDS) e uma detecção global realizada através de um modulo que permite a cooperação entre as LIDS [38][39]. Outros estudos tratam o problema de cooperação (um dos conceitos relacionados com a confiança) em MANET, fazendo com que nós inicialmente egoístas (*selfish nodes*) comecem a colaborar [21][40]. Estas técnicas estão interessadas na detecção de um comportamento egoísta dos nós, mas não permitem a verificação e detecção das informações sobre a topologia da rede.

Neste trabalho, estamos interessados em aplicar a confiança ao protocolo de roteamento OLSR para verificar e detectar as informações, disseminada pelos nós, sobre a topologia da rede.

Existem diversos trabalhos que tratam da questão da confiança em redes *ad hoc* [16][17][18][19][20][22]. No entanto a maioria deles está focada apenas nos problemas de identificação de nós maliciosos.

A seguir algumas definições e conceitos sobre confiança e confiança computacional e como nos baseamos nela para a adaptação do OLSR, que é o objetivo da nossa proposta.

2.4. CONFIANÇA COMPUTACIONAL

[41][42][43][44][45][46][47][48][49][50][51][52][53][54][55][13][56][57][58]

Está fora de questão a importância da confiança e da reputação nas sociedades humanas. No entanto, não é surpresa que várias disciplinas, cada uma de uma perspectiva diferente, tenham estudado e usado os dois conceitos. Psicologia [41], sociologia [42] filosofia [43] e economia [44][45] são disciplinas que tem dedicado esforços ao estudo de confiança e reputação.

O estudo da confiança e da reputação tem varias aplicações em tecnologias da informação e comunicação. Sistemas de confiança e reputação têm sido reconhecidos como fatores-chave para adoção de comércio eletrônico bem sucedido. Estes sistemas são usados por agentes de softwares inteligentes tanto como mecanismo de procura por confiança trocada entre parceiros quanto para incentivar os processos de tomada de decisão sobre quando honrar contratos. A reputação é usada em mercados eletrônicos como imposição de confiança, e mecanismo de incentivos para evitar trapaças e fraudes [46][47][48].

Não há muito trabalhos que dão uma visão geral de confiança e reputação do ponto de vista da ciência da computação. Dellarocas [48] apresenta uma visão geral sobre mecanismos de reputação online que são usadas atualmente em web sites comerciais. Na área da confiança, Grandison *et al.* [49] examinam as várias definições de confiança para aplicações de internet. Existem também algumas propostas para estabelecer uma tipologia para reputação [50] e confiança [51].

2.4.1. Classificação

Confiança e reputação podem ser analisadas de perspectivas diferentes e podem ser utilizadas em uma vasta gama de situações. Isso torna a classificação dos modelos de confiança e reputação uma tarefa difícil. Sabater e Sierra [14] propuseram uma classificação baseada em modelos computacionais, considerando as características especiais destes modelos e o ambiente onde eles estão inseridos que é utilizada neste trabalho. Esta classificação apresenta os seguintes critérios:

Modelo Conceitual

De acordo com o modelo conceitual de referência, os modelos de confiança e reputação podem ser caracterizados como:

- Cognitivos: Em modelos baseados em abordagens cognitivas, confiança e reputação são compostas de crenças subjacentes e não são funções do grau destas crenças [52]. Na abordagem cognitiva, o estado mental que conduz a confianca em um outro agente ou assinala a reputação, assim como as conseqüências mentais da decisão e do ato de basear a decisão em outro agente, são partes essenciais do modelo.

- Teoria dos Jogos: Confiança e reputação são consideradas probabilidades subjetivas pela qual um individuo A espera que outro individuo, B, execute certa ação da qual depende o seu bem-estar [53]. Confiança e reputação não são resultados do estado mental do agente em sentido cognitivo, mas sim o resultado de um jogo mais pragmático com funções utilitárias e agregações numéricas de interações passadas.

Fontes de Informações

É possível classificar modelos de confiança e reputação considerando as fontes de informações que foram usadas para calcular os valores de confiança e reputação. Experiências diretas e informações provindas de testemunhas são as "tradicionais" fontes de informações usadas por modelos de confiança e reputação computacionais. Além destas, alguns modelos começaram, recentemente, a usar a informação associada a aspectos sociológicos do comportamento dos agentes.

O tipo de informação disponível para um agente depende da sua capacidade sensorial. O uso de várias fontes de informações, se usadas de forma inteligente em um modelo, pode aumentar capacidade dos valores calculados de confiança e reputação, mas ao mesmo tempo aumenta a complexidade do modelo. Mais ainda, cenários que permitem agentes a obter informações diversas demandam agentes mais inteligente, e por esta razão, mais complexos.

- Experiência direta: Esta é, sem dúvida, a fonte de informação mais confiável para um modelo de confiança e reputação. Existem dois tipos de experiências diretas em que um agente pode incluir como parte do seu conhecimento. O primeiro tipo, e usado por todos os modelos de confiança e reputação analisados neste trabalho, é

a experiência baseada em interações diretas com o parceiro. O segundo tipo não é tão comum e é restrito a cenários que são preparados para permiti-lo. Usualmente, naqueles modelos em que a observação sobre as atividades dos parceiros é considerada e um certo nível de ruído na informação obtida é assumido.

- Informação de Testemunha: Também chamada de *ord-of-mouth* ou *indirect information*, é a informação que vem de outro membro da comunidade. Esta informação pode ser baseada nas suas próprias experiências diretas ou pode ser informação provida por outros agentes da comunidade. Se a experiência direta é a mais confiável fonte de informações para um modelo de confiança e reputação, informação provinda de testemunhas é usualmente a mais abundante. No entanto, é uma forma mais complexa para modelos de confiança e reputação usarem a informação. A razão é a incerteza que gera este tipo de informação. Não é incomum que testemunhas manipulem ou escondam partes da informação em seu beneficio próprio.

- Informação Sociológica: A base deste conhecimento são as relações sociais entre agentes e todos os agentes que estão inseridos na sociedade. Na vida real, os indivíduos que pertencem a uma dada sociedade estabelecem diferentes tipos de relacionamentos entre eles. Exemplos destas relações podem ser a dependência, a troca, a competição e a colaboração. Também é verificado que cada indivíduo faz uso de uma ou de várias regras na sociedade. As duas, tanto as relações quanto as regras que o(s) individuo(s) usam na sociedade influenciam no seu comportamento e na interação com os demais. As relações sociais estabelecidas entre agentes em um sistema multi-agentes são reflexões simplificadas de relações mais complexas estabelecidas entre semelhantes em uma sociedade. Este tipo de informação só se torna disponível em cenários onde existe uma grande interação entre os agentes. Normalmente, somente alguns modelos de confiança e reputação usam esse conhecimento aplicado a comunidades de agentes para calcular ou melhorar o modo de calcular os valores de confiança e reputação. Estes modelos usam técnicas como *social network analysis*. Análise da rede social é o estudo de relações sociais entre indivíduos em uma sociedade que emergiu como um conjunto de métodos para analise de estruturas sociais, que permite especificamente uma investigação sobre os aspectos relacionais destas estruturas.

No entanto, o uso destes métodos depende da disponibilidade do dado relacional [54]. Embora atualmente o número de modelos que levam em conta este tipo de informação seja reduzido, é imaginável que o aumento da complexidade em sistemas multi-agente tornará este tipo de sistema muito importante em um futuro próximo.

- Preconceito: O uso do prejuízo/preconceito para calcular valores de confiança e a reputação é outro mecanismo não muito comum, mas presente em alguns modelos de confiança e reputação. Preconceito é o mecanismo de atribuir propriedades (como por exemplo, a reputação) a um individuo baseado em sinais que identificam o individuo como membro de um dado grupo. Estes sinais podem ser qualquer coisa, desde um uniforme, um comportamento diferente, etc. Um estudo sobre a análise do uso de sinais em confiança é feito por Bacharach e Gambetta em [55]. Como a maioria das pessoas usa a palavra "preconceito" se referindo a atitudes negativas ou hostis de um grupo para outro grupo social, usualmente definido racialmente. No entanto, as conotações negativas que a palavra "preconceito" tem em sociedades humanas deve ser revista quando aplicada a comunidades de agentes. Diferentemente de sinais usados em sociedades humanas que vão desde a cor da pele até a opção sexual, o conjunto de sinais usados em modelos de confiança e reputação computacional está normalmente fora da discussão ética.

Tipos de Visibilidade

A confiança e a reputação de um indivíduo pode tanto ser vista como uma propriedade global compartilhada por todos aqueles que estão a observar, quanto uma propriedade subjetiva de cada individuo com acesso restrito. No primeiro caso, o valor de confiança e reputação é calculado a partir de opiniões de indivíduos que no passado interagiram com o individuo que está sendo avaliado. Este valor é avaliado publicamente para todos os membros da comunidade e atualizado a cada vez que um membro emite uma nova avaliação do individuo em questão. No segundo caso, cada individuo atribui um valor de confiança/reputação a cada membro da comunidade de acordo com elementos mais pessoais como experiências diretas, informações recebidas por testemunhas e relações já conhecidas entre os membros da comunidade. Em último caso, não é possível falar sobre

confiança/reputação de um individuo X, já que temos que falar sobre a confiança e a reputação de um individuo X sob o ponto de vista de um individuo Y.

Em modelos que consideram a confiança e a reputação como uma propriedade global, o maior problema é a falta de personalização deste valor. Algo que é ruim para mim, pode ser aceitável para outras pessoas. No entanto, esta abordagem pode ser aceitável em cenários mais simples onde é possível atribuir uma simples "forma de pensar" para todos os membros das comunidades, mas isto não é útil no caso dos agentes terem que lidar com relacionamentos mais complexos e subjetivos.

A antítese desses modelos são modelos que consideram confiança e reputação como uma propriedade subjetiva. Cada agente usa sai experiência pessoal e o que outros agentes lhe disseram pessoalmente sobre qualquer coisa que seja assunto, para construir a confiança e reputação de cada membro da comunidade. Estes modelos são indicados para ambientes médios e pequenos onde os agentes se encontrem com certa freqüência tornando possível estabelecer fortes conexões entre eles.

2.4.2. Confiança Computacional e Modelos de Reputação

Vários modelos de confiança computacional e reputação têm aparecido nos últimos anos, cada um com a sua característica e usando diferentes soluções técnicas. Nesta seção iremos falar um pouco sobre alguns modelos já conhecidos e depois fazer uma comparação.

O modelo de confiança proposto por Marsh [13] somente leva em consideração as interações diretas. Neste trabalho ele diferencia três tipos de confiança:

- Confiança básica: Modela a disposição da confiança independente de qual agente está na frente. A confiança aqui é calculada sobre todas as experiências acumuladas pelo agente.
- Confiança Geral: Esta é a confiança em que um agente tem em outro sem levar em consideração uma situação especifica. Simplesmente representa a confiança geral que um agente tem no outro.
- Confiança Situacional: É o valor de confiança que um agente tem em outro dada uma situação especifica.

Sporas [56] propõe uma versão evoluída dos modelos de reputação online. Neste modelo, apenas as classificações mais recentes entre dois usuários é considerada. Outra

característica importante é que usuários com valores muito altos de reputação experimentam variações muito menores de classificação após a atualização, do que usuários de baixa reputação. Usando uma técnica muito próxima ao sistema de Glicko [57] – método computacional usado para validar a força do jogador em jogos de *pairwise*, Sporas incorporou a medida de confiabilidade da reputação do usuário baseada no desvio padrão dos valores de reputação. Este modelo tem a mesma característica geral do modelo comentado anteriormente, no entanto, este se apresenta mais robusto a mudanças no comportamento do usuário e a medida de confiabilidade melhora a usabilidade do valor da reputação. A desvantagem deste modelo é a utilização do valor de reputação atribuído a uma testemunha como medida de confiabilidade. Se o agente é um bom vendedor, isto não significa que ele também tem de ser uma testemunha confiável.

A proposta de Schillo *et al.* [58] é direcionada para cenários onde o resultado de uma interação entre dois agentes (do ponto de vista da confiança) é uma expressão booleana: boa ou ruim, não há graus de satisfação. Concretamente, para realizar os experimentos eles propuseram um conjunto de jogos chamado dilema do prisioneiro com uma fase de seleção de parceiro. Cada agente recebe os resultados do seu jogo mais a informação dos jogos que aconteceram no conjunto de vizinhos. O resultado da interação neste cenário é uma impressão da honestidade do parceiro (se ele fez o que disse que fez na fase de seleção de parceiro) e qual foi o seu comportamento de acordo com as ações normais do dilema do prisioneiro (cooperação ou defesa). O modelo é baseado em teoria da probabilidade.

Neste modelo, evidências testemunhais podem vir de entrevistas e talvez, como as testemunhas podem ter diferentes motivos para tentar enganar o agente sobre sua observação verdadeira. Com isto, cada agente é confrontado com o ruído na informação e também com a possibilidade de que a fonte de informação possa influenciar sobre os dados fornecidos.

A resposta de uma testemunha a uma pergunta é o conjunto de experiências observadas (e não um resumo delas). Dado isto, os autores assumem que não vale a pena para a testemunha dar uma informação falsa.

No entanto, o modelo assume que a testemunha, apesar de nunca mentir, pode esconder informação para que os outros agentes se mostrem, aparentemente, menos confiáveis. Assumindo que informação negativa será sempre relatada pela testemunha, o problema é reduzido para saber até que ponto essas testemunhas tem distorcido os dados comunicados (escondendo observações positivas). Para realizar este procedimento, trair

(esconder informação) é modelado como um processo estocástico onde um agente decide informar sobre um fato positivo de outro agente com a probabilidade p e esconde esta informação com probabilidade 1 – p. A aplicação deste processo pode ser visto como o experimento de Bernoulli e a repetição do experimento como cadeia de Bernoulli. A teoria da probabilidade então é utilizada para estimar o valor escondido de informações positivas. Este processo pode ser aplicado recursivamente do agente alvo através de todos os seus antecessores até o nó raiz da *TrustNet*.

Abdul Rahman e Hailes [59] usam quatro níveis de crença para tipificar o agente de confiança: VT (*very trustworthy*), T (*trustworthy*), U (*untrustworthy*) e VU (*very untrustworthy*). Para cada parceiro e contexto, o agente mantém uma tupla com o número de experiências passadas em cada categoria. Então, do ponto de vista da interação direta, a confiança no parceiro dado um certo contexto é igual ao grau de que corresponde ao valor máximo na tupla. Por exemplo, se a tupla associada de um parceiro dado um contexto é (0, 0, 4, 3), a confiança associada para este parceiro será T, que corresponde a terceira posição na tupla. Se há mais de uma posição na tupla com um valor máximo, o modelo da um grau de confiança incerto de acordo com a tabela de situações que cobre este tipo de caso. Existem três tipos de valores de incerteza que cobre situações onde a maioria das experiências são boas e alguns são ruins, a maioria é ruim e algumas são boas e um valor igual de experiências boas e ruins.

Em ordem de combinar informações, o modelo dá maior relevância à informação que vem de agentes com ponto de vista similar. Ou seja, ele da mais importância a informação que precisa de pouco ajuste, ou, melhor ainda, que não precisa de ajuste algum porque provém de agentes que tem perspectivas similares em um dado contexto.

Ao contrário de outros modelos de confiança onde a informação de testemunhas é fundida com a informação direta para se obter a confiança em um tema especifico, o propósito deste modelo é avaliar a confiança nas informações transmitidas por testemunhas. Experiências diretas são usadas para comparar o ponto de vista destas testemunhas com a percepção direta do agente e então ser capaz de ajustar as informações provenientes dos mesmos em conformidade.

No modelo de confiança proposto por Esfandiari e Chandrasekharan [52], dois mecanismos de um-a-um são propostos. O primeiro é baseado na observação. Eles propuseram o uso de redes Bayesianas e para realizar a aquisição de confiança por

aprendizado Bayesiano. No caso mais simples de uma estrutura já conhecida e amplamente observada, a tarefa de observar é reduzida a considerações estatísticas.

O segundo mecanismo de aquisição de confiança é baseado em interação. A abordagem é a mesma usada em [60]. Existem dois protocolos principais de interação, o protocolo explorador onde o agente pergunta aos outros sobre fatos conhecidos para avaliar o seu grau de confiança e o protocolo de consulta onde o agente pede conselho para agentes confiáveis.

Para lidar com informações de testemunhas, cada agente constrói um gráfico relacionado rotulado onde os nós representam agentes onde a conexão/ponte (a, b) representa o valor de confiança que a tem em b. As conexões/pontes são abstraídas se o valor da confiança é desconhecido. Neste tipo de gráfico, existe a possibilidade de ciclos que diminuem artificialmente o valor da confiança e de caminhos que tiverem valores contraditórios. Para resolver este problema. Ao invés de usar um valor único para a confiança. O modelo usa um intervalo de confiança determinado pelos valores mínimos e máximos de todos os caminhos sem os ciclos que conectam dois agentes.

Os autores afirmam que o cálculo deste intervalo de confiança é equivalente ao problema de roteamento em uma rede de comunicação e, portanto, algoritmos distribuídos já conhecidos podem resolver o problema aplicado a esta situação.

No modelo proposto por Yu e Singh [61][62][63], a informação armazenada por um agente sobre interações diretas é um conjunto de valores que refletem a qualidade destas interações, o que eles chamam de qualidade de serviço (QoS - *Quality of Service*). Somente as experiências mais recentes com parceiros concretos são consideradas para os cálculos. Cada agente escolhe um *threshold* alto e um baixo que define a fronteira do que é considerado QoS que é atribuída ao agentes confiáveis, QoS com uma classificação não clara e QoS atribuída a agentes não confiáveis. Então, usando uma informação já armazenada, juntamente com a teoria de evidência Dempster-Shafer, um agente pode calcular a probabilidade que o seu parceiro presta um serviço atribuído a cada um destes grupos. Se a diferença entre a probabilidade e o serviço que pertence ao primeiro e ao ultimo grupo for maior que o threshold de confiança, o agente a ser avaliado é considerado confiável.

Este modelo não combina informação direta com informação de testemunha (as duas fontes de informação que são levadas em consideração). Se a informação direta está disponível, esta vai ser a única fonte que vai ser considerada para determinar a confiança do

agente alvo. Somente quando a informação direta não está disponível o modelo apela para a informação da testemunha.

No modelo de reputação de Sen e Sajja [64], os dois tipos de experiências diretas são consideradas: interação direta e interação observada. No cenário onde este modelo é usado, as observações são "barulhentas", e podem diferir de algum modo da performance atual.

Somente interações diretas podem dar a percepção exata da realidade. Reforçar o aprendizado é o mecanismo escolhido para atualizar o valor de reputação. Devido ao ruído subjacente nas observações, a regra usada para atualizar o valor de reputação quando existe uma nova interação tem efeito maior do que a regra para atualizar o valor quando há uma nova observação.

O valor da reputação varia de 0 para 1. Valores maiores que 0,5 representam um bom desempenho, e valores menores que 0,5 representam um mau desempenho.

A principal característica do modelo de AFRAS [65] é o uso de conjuntos fuzzy para representar os valores de confiança. Assim que um novo conjunto fuzzy que mostra o grau de satisfação das ultimas interações com um dado parceiro é calculado, o antigo valor de reputação e o novo valor de reputação são agregados usando uma agregação ponderada. Os pesos desta agregação são calculados de um único valor que é chamado remembrance ou memory. Este fator permite que o agente dê mais importância para a última interação ou para o antigo valor de reputação.

A principal idéia por trás do modelo de reputação apresentada por Carter *et al*. [66] é que a reputação de um agente é baseada no grau de comprimento das funções atribuídas a ela pela sociedade. Se a sociedade julga que as funções estão sendo cumpridas, estes agentes são recompensados uma reputação positiva, em outro caso, são punidos com uma reputação negativa. Os autores formalizam o conjunto de funções com as informações compartilhadas pela sociedade e propõem métodos de calcular o grau de satisfação com cada uma destas funções.

O modelo de confiança proposto por Castelfranchi e Falcone [67] é um claro exemplo de modelo cognitivo de confiança. A base deste modelo é a forte relação entre confiança e delegação. Eles afirmam que 'confiança é o fundo mental da delegação'. Em outras palavras, a decisão que um agente X delega para um agente Y é baseada em um conjunto especifico de

crenças e objetivos os quais chamamos ‘confiança’. No entanto, ‘somente agente com objetivos e crenças pode confiar’.

Regret [68] apresenta um modelo de confiança e reputacao orientado para pequenos ambientes complexos de e-commerce, onde relações sociais entre indivíduos têm uma importante função no jogo. O sistema leva em consideração três fontes diferentes de informações: experiências diretas, informações vindas de agentes externos e estruturas sociais.

Neste trabalho, a confiança é tratada para encaminhamento seguro de pacotes em redes OLSR. As métricas e probabilidades usadas neste trabalho é baseada no TRAVOS [15], que é um modelo de confiança e reputação baseada em agentes e a confiança é medida através de probabilidade. Este trabalho é validado pela valor da confiança baseada em interações passadas e reputação obtida pelos outros nós.

Neste modelo de confiança, existem três métodos de calcular a confiança em outro agente. Patel modela o ambiente no qual o TRAVOS é aplicado como um sistema multi-agente formado por n agentes, e denota o conjunto de todos os agentes como $\mathrm{A} = \{a_1, a_2, ..., a_n\}$.

Vários pares de agentes $\{a_x, a_y\} \subseteq \mathrm{A}$ podem interagir uns com os outros, governados por contratos que especificam as obrigações de cada agente em relação a seu parceiro de interação. Uma interação entre a_1 e a_2 é considerada bem sucedida por a_1 se a_2 cumpre suas obrigações. Pela perspectiva de a_1, a avaliação de uma interação entre a_1 e a_2 é resumida em uma variável binária, O_{a_1,a_2}, onde $O_{a_1,a_2} = 1$ indica uma interação bem sucedida para a_1 com a_2 e $O_{a_1,a_2} = 0$, uma interação mal sucedida. Uma avaliação de uma interação observada no tempo t é denotada como $O^t_{a_1,a_2}$, e o conjunto de todas as avaliações observadas de um tempo t_0 a t, como $O^{t_0:t}_{a_1,a_2}$.

Em qualquer ponto no tempo t, o histórico de interações entre agentes a_1 e a_2 é guardado como valores ordenados, $\Re^t_{a_1,a_2} = \left(m^t_{a_1,a_2}, n^t_{a_1,a_2}\right)$, onde o valor de $m^t_{a_1,a_2}$ é o número de interações bem sucedidas de a_1 com a_2 no tempo t, enquanto $n^t_{a_1,a_2}$ é o número de interações mal sucedidas de a_1 com a_2 no tempo t.

A tendência de um agente a_2 cumprir ou não com as obrigações para com o agente a_1 é governada por seu comportamento. O comportamento de a_2 em relação à a_1, denotado por B_{a_1,a_2}, é modelado como o valor esperado de O_{a_1,a_2}.

Cada agente mantém um nível de confiança em cada agente presente no sistema. O nível de confiança de um agente a_1 em um agente a_2, é denotado por τ_{a_1,a_2}. Especificamente, o nível de confiança calculado utilizando somente as interações do próprio agente com outro é conhecido como confiança direta, denotado por $\tau^d_{a_1,a_2}$. Por outro lado, o nível de confiança calculado utilizando somente opiniões capturadas por outros é conhecido como reputação, denotado por $\tau^r_{a_1,a_2}$. A confiança calculada da combinação de experiência direta com opiniões de terceiros é conhecida como confiança combinada, denotada por $\tau^c_{a_1,a_2}$.

Outra métrica utilizada nesse modelo de confiança é a confidência, que consiste em uma métrica que representa a acuidade do valor de confiança calculado por um agente, dado o número de observações que são utilizadas para o cálculo dessa confiança. A confidência de a_1 na sua avaliação de a_2 é denotado por γ_{a_1,a_2}.

No cálculo da confiança direta, é realizada uma abordagem probabilística baseada nas experiências individuais de um agente no papel daquele que confia. Se o agente a_1 tem informações completas sobre o agente a_2, a probabilidade de a_2 cumprir com suas obrigações é expressa por B_{a_1,a_2}, de acordo com a_1. Entretanto, geralmente, não se assume que haja informação completa. Assim, a confiança direta $\tau^d_{a_1,a_2}$ em um tempo t é definida como o valor esperado de B_{a_1,a_2}, dado um conjunto de avaliações $O^{1:t}_{a_1,a_2}$ de interações observadas.

$$\tau^d_{a_1,a_2} = \mathrm{E}\left[\mathrm{B}_{a_1,a_2} \mid O^{1:t}_{a_1,a_2}\right] \qquad (2.3)$$

O valor esperado de uma variável aleatória contínua depende da função densidade de probabilidade (PDF) utilizada para modelar a probabilidade que a variável terá um determinado valor. Nas análises Bayesianas, a família beta de PDFs é comumente utilizada como uma distribuição prévia para variáveis aleatórias que possuem valores contínuos no intervalo [0,1].

A fórmula geral para distribuições beta é dada pela Equação 2.4. Essa fórmula possui dois parâmetros, α e β, os quais definem o formato da função densidade quando plotada.

$$f(b \mid \alpha, \beta) = \frac{b^{\alpha-1}(1-b)^{\beta-1}}{\int U^{\alpha-1}(1-U)^{\beta-1} dU} \qquad (2.4)$$

onde $\alpha, \beta > 0$

Utilizando-se dessa função, é possível calcular o valor da confiança direta. Primeiro, é preciso encontrar o valor de α e β. Assumindo previamente, antes de interagir, que todos os valores possíveis de B_{a_1,a_2} são iguais, os valores iniciais de α e β são $\alpha = \beta = 1$. Baseando-se em técnicas padronizadas, considerando as observações realizadas nas interações, esses parâmetros podem ser calculados adicionando o número de interações bem sucedidas ao valor inicial de α e o número de interações mal sucedidas a β.

$$\hat{\alpha} = m^{1:t}_{a_1,a_2} + 1 \ \textbf{e} \ \hat{\beta} = n^{1:t}_{a_1,a_2} + 1 \qquad (2.5)$$

Assim, o valor final de $\tau^{d}_{a_1,a_2}$ é calculado aplicando a equação padrão para o valor esperado de uma distribuição beta.

$$\tau^{d}_{a_1,a_2} = \frac{\hat{\alpha}}{\hat{\alpha} + \hat{\beta}} \qquad (2.6)$$

Pelas Equações 2.5 e 2.6 pode-se deduzir que o valor da confiança direta e a distribuição mudam conforme um agente ganha experiência interagindo com o outro agente, o que promove a modificação do formato da curva de distribuição, visto que o valor dos parâmetros é alterado com o tempo.

2.4.3. Confiança Computacional Aplicada a MANET

Pirzada e McDonald [17] propõem um modelo de confiança a fim de estimar a confiabilidade das rotas. Assim, esta pode ser uma métrica adicional no cálculo das rotas. Embora não garanta 100% de segurança, o modelo proposto permite aos nós optar pela rota mais confiável. Uma extensão ao protocolo DSR é proposta para avaliar a eficácia do

esquema de confiança proposto. No entanto, o modelo se restringe ao protocolo DSR,e depende integralmente do uso do modo promíscuo, ignorando as limitações de energia dos nós móveis. Outro problema é a grande quantidade de informação que deve ser armazenada, em cada nó da rede.

Buchegger e Le Boudec [19] investigaram o compromisso entre robustez e eficiência na utilização de sistemas de reputação em redes *ad hoc*. Também é proposto um mecanismo baseado em estatística Bayesiana para filtrar nós difamadores são considerados para computar a reputação de um determinado nó, tanto os dados obtidos através de observações como dados enviados por outros nós. Eles mostram que levar em consideração as recomendações de outros nós pode acelerar o processo de descoberta de nós maliciosos.

Theodorakopoulos e Baras [18] analisaram a questão da inferência de grau de confiança como uma generalização do problema de menor caminho em um grafo orientado, onde as arestas correspondem a opinião que um vértice possui sobre o outro. Eles consideram que os nós formam sua opinião baseada estritamente em observações locais. A opinião de cada nó inclui o grau de confiança mais um valor que representa a precisão do grau de confiança. O objetivo é capacitar os nós a construir indiretamente relações de confiança baseada apenas em interações locais.

Virendra *et al.* [21] apresentam uma arquitetura baseada na confiança que permite aos nós da rede tomarem decisões referentes ao estabelecimento de chaves e a formação de grupos com outros nós. O esquema de confiança proposto também se baseia numa avaliação feita pelo próprio nó e na recomendação de outros nós. Entretanto, o procedimento utilizado na avaliação do nó é baseado na monitoração dos nós e em um mecanismo de pergunta e resposta. Assim, o nó avaliador envia uma pergunta ao nó avaliado e depois compara a resposta com as informações obtidas durante a fase de monitoração.

A confiança tem sido utilizada ainda como um meio para fazer valer a colaboração entre os nós. Em [69], além de apresentar um panorama das aplicações de confiança em MANET, foi demonstrado a eficácia do raciocínio de confiança na detecção de mau comportamento em OLSR. Esta aplicação foi estendida em [16], que compara os resultados da simulação levando em conta o total de nós da rede e os nós alertas para casos de ataques. Este trabalho é considerado uma nova etapa a partir dessas referencias citadas neste parágrafo.

3. MODELO DE CONFIANÇA PARA OLSR

Este capítulo apresenta o modelo de confiança para o protocolo OLSR proposto, principal contribuição deste trabalho. A confiança estudada é relacionada com encaminhamento robusto de pacotes e com o roteamento em MANET que utiliza o protocolo OLSR. Assim, o principal objetivo do modelo consiste em classificar os nós vizinhos em confiáveis e não-confiáveis a partir da avaliação objetiva da confiança. Como conseqüência dessa avaliação, os nodos não confiáveis são excluídos do processo de escolha de rotas do protocolo OLSR, eliminando-os do encaminhamento de pacotes.

Resumidamente, a operação do modelo pode ser descrita nas seguintes etapas:

- Um nó envia pacotes que precisam ser encaminhados para um de seus vizinhos, conforme sua tabela de roteamento, e ouve promiscuamente o meio de comunicação (enlace de dados) para verificar se o vizinho irá encaminhar o pacote ou falhará ao encaminhá-lo. Cada pacote enviado para encaminhamento permitirá uma observação do comportamento do nodo vizinho. Isso permite que cada nó calcule uma medida direta de confiança para cada um dos seus vizinhos.
- A informação relacionada à confiança direta dos vizinhos é disseminada para os demais através de mensagens de *HELLO*, modificadas para permitir essa funcionalidade.
- Cada nó utiliza as informações anunciadas pelos vizinhos acerca de suas opiniões sobre o comportamento dos outros nós e calcula uma reputação para cada um de seus vizinhos.
- Os nós avaliam a confiança em cada um dos seus vizinhos, considerando tanto a medida de confiança direta quanto a medida da reputação. Essa medida consolidada é utilizada para determinar quais são os vizinhos não confiáveis.
- Os vizinhos considerados não confiáveis são excluídos do esquema de roteamento OLSR.

Seguindo a abordagem de J. Sabater e C. Serra [36], o modelo proposto tem as seguintes características:

- Modelo conceitual de jogo teórico: a confiança e a reputação são o resultado de funções utilitárias de um jogo pragmático e agregações numéricas de interações passadas.
- As fontes de informação incluem tanto experiências diretas (confiança direta) quanto opiniões coletadas de outros agentes (reputação).
- A visibilidade não é global no sentido em que a confiança e a reputação são atualizadas apenas localmente.
- Contexto único (i.e. roteamento OLSR).

A função utilitária usada para observar e avaliar o comportamento dos pares está relacionada ao encaminhamento dos pacotes. O modelo proposto tira proveito da natureza *broadcast* de uma rede sem fios, o que permite ao nó monitorar o comportamento do vizinho quando um pacote deve ser encaminhado por ele. Cada vez que um pacote IP é enviado a um vizinho para ainda ser encaminhado na rede, uma interação é observada. A interação é bem sucedida se o vizinho encaminhar o pacote como esperado e é considerada mal sucedida se este não o fizer.

Nesse sentido, a melhoria do processo OLSR proposta se traduz na em uma melhor escolha dos nós MPR. Essa seleção deverá considerar a informação de confiança e reputação acerca dos nós vizinhos. Nós considerados não-confiáveis (por exemplo, aqueles que não conseguem enviar os pacotes como esperado) não devem ser selecionados como MPR e são excluídos do conjunto de vizinhos a dois saltos de distância e dos algoritmos de escolha de MPR.

Embora as informações sobre confiança possam ser anunciadas para toda a rede, por exemplo, através de modificações nas mensagens TC, somente foi considerada a troca de informações entre os vizinhos através de mensagens *HELLO*. Há duas razões principais para justificar esta escolha. Primeiro, se um nó não-confiável é excluído tanto do conjunto de vizinhos a dois saltos e do processo de escolha de MPR, este não será, conseqüentemente, escolhido para encaminhar pacotes. Neste caso, espera-se que outros nodos confiáveis na vizinhança possam fornecer a conectividade possivelmente provida pelos nós não confiáveis. Todas essas questões são resolvidas completamente no mecanismo de controle de vizinhança do OLSR. Em segundo lugar, mensagens *HELLO* possuem um campo RESERVED (vide Figura 2-11) destinado para implementações futuras ou não especificadas no protocolo

padrão. Esse campo é usado para trocar informações sobre a confiança direta entre os vizinhos, sem maiores preocupações sobre compatibilidade com o OLSR padrão, permitindo a coexistência de instâncias OLSR compatíveis com a RFC 3626 e instâncias que tenham a extensão de confiança proposta.

A medida de confiança é gerada para cada vizinho combinando tanto a confiança direta quanto a reputação. Se esta medida de confiança no que diz respeito a um vizinho está abaixo do limiar pré-definido, o nó é considerado não confiável. A confidência é também calculada, a fim de fornecer uma medida de quão confiável é o valor de confiança / reputação utilizado no modelo.

Os valores iniciais de confiança direta (antes de qualquer interação passada) são sempre definidos como completamente confiáveis, uma medida que corresponde ao comportamento inicial do nó OLSR, dado que o nó espera para a colaboração imediatamente, mesmo sem identificar seus vizinhos.

As seções seguintes apresentam, com maiores detalhes, as características do modelo de confiança proposto.

3.1.1. Medidas de Confiança e Reputação

O modelo de confiança proposto, adotamos a mesma formulação proposta por Patel [15]. Nesse sentido, os nodos da MANET compõem o sistema multi-agente, denotado por $\mathrm{A} = \{a_1, a_2, ..., a_n\}$. Calculamos as medidas de confiança direta ($\tau^d_{a_i,a_j}$) a partir de informações acerca de interações passadas, sendo cada interação representada pela variável binária $O^t_{a_i,a_j}$, onde $O^t_{a_i,a_j}$ = 1 indica uma interação bem sucedida e $O^t_{a_i,a_j}$ = 0 uma interação mal sucedida. Do mesmo modo, calculamos a reputação, $\tau^r_{a_i,a_j}$, a partir de informações recebidas de outros nodos. Finalmente, calculamos a confidência γ_{a_i,a_j} e a confiança consolidada τ_{a_i,a_j}. Os cálculos realizados em nosso modelo, no entanto, usam premissas diferentes e são realizados de uma maneira nova, conforme mostrado a seguir.

O cálculo da confiança direta do modelo de Patel é derivado da análise Bayesiana clássica e assume que uma PDF beta para a variável aleatória O_{a_i,a_j} (vide seção 2.4.2, Eq.

2.3). Em sua formulação original, o cálculo da confiança direta possui memória infinita. Em nosso modelo usamos um estimador de média com memória finita [70] para o cálculo da confiança direta, conforme ilustra a Equação 3.1. O parâmetro α está relacionado com a memória do estimador e deve ser configurado para refletir o grau de tolerância a erros ou falhas eventuais, que são comuns em MANET.

$$\tau_{a_i,a_j}^{d,t} = \tau_{a_i,a_j}^{d,t-1} + \alpha(O_{a_i,a_j}^{t} - \tau_{a_i,a_j}^{d,t-1})$$

Onde: $\alpha \in]0,1[$ (3.1)

t e t-1 referem-se aos tempos atuais e anteriores das estimativas, respectivamente

A formulação proposta na equação 3.1 introduz, portanto, um parâmetro de *aging*, que se refere à obsolescência das evidências coletadas para avaliação da confiança.

Inicialmente, todos os nodos são considerados totalmente confiáveis, isto é, $\tau_{a_i,a_j}^{d,0} = 1$. Essa inicialização é outra importante diferença com relação ao modelo de Patel [15], que utiliza 0,5 como valor inicial para a confiança direta. Este valor não seria adequado para ser usado no caso do OLSR, pois ou teríamos um limiar de confiança muito baixo ou os nodos seriam já inicialmente considerados não confiáveis e eliminados do roteamento OLSR.

Cada nó também calcula uma estimativa de confidência (γ_{a_i,a_j}), que no nosso modelo é avaliada simplesmente em função da quantidade acumulada de interações passadas (n) na medida τ_{a_i,a_j}^{d} , como mostra a Equação 3.2:

$$\gamma_{a_i,a_j} \begin{cases} 0 \text{ se } n < \dfrac{1}{\alpha} \\ 1 \text{ c.c.} \end{cases} \qquad (3.2)$$

Cada nó dissemina na vizinhança sua medida de confiança direta τ_{a_i,a_j}^{d} e sua respectiva certeza γ_{a_i,a_j} através das mensagens *HELLO*. Com esta informação, os vizinhos calculam a reputação τ_{a_i,a_j}^{d} de outros nós, conforme a Equação 3.3:

$$\tau^{r}_{a_i,a_j} = \frac{\sum_{k=1,k\neq i}^{K} \gamma_{a_k,a_j} \tau^{d}_{a_k,a_j} \tau^{d}_{ai,a_k}}{\sum_{k=1,k\neq i}^{K} \tau^{d}_{ai,a_k}} \qquad (3.3)$$

Note que a reputação medida $\tau^{r}_{a_i,a_j}$ é na verdade a soma formada por todas as medidas diretas de confiança $\tau^{d}_{a_k,a_j}$ disponibilizada através das mensagens *HELLO* que tem uma certeza diferente de zero, ponderada pela medida direta de confiança que o nó tem para o nó que fornece a informação $\tau^{d}_{a_i,a_k}$. Desta forma, nós permitimos que a informação que chega proveniente de nós não-confiáveis possam ser minimizadas ou mesmo excluídas na avaliação da reputação.

Finalmente, a medida de confiança τ_{a_i,a_j} utilizada para a decisão final sobre a idoneidade de um nó é calculada combinando a confiança direta e a reputação de um nó como mostra a Equação 4.4:

$$\tau^{r}_{a_i,a_j} = \begin{cases} \tau^{d}_{a_i,a_j} \text{ se } \tau^{r}_{a_i,a_j} = 0 \\ \mathrm{w}_1.\tau^{d}_{a_i,a_j} + \mathrm{w}_2\tau^{r}_{a_i,a_j} \text{ c.c.} \end{cases} \qquad (3.4)$$

onde : w1 + w2 = 1

Os parâmetros w_1 e w_2 são fatores de ponderação que equilibram a medida direta da confiança e da reputação.

3.1.2. Adaptação da mensagem de HELLO

A fim de lidar com a troca de informações sobre confiança nos nós , foi usado o campo *"RESERVED"* para cada anúncio de link na mensagem *HELLO* para compartilhar o τ^{d} e γ com outros nós. A proposta de sintaxe para este campo não utilizado é mostrado na Figura 3-1.

O código de τ^d no campo Td é um *integer* sem sinal calculado pela multiplicação de τ^d por 127 (7 bits significantes). γ, por sua vez, só assume valores binários (0 ou 1). Portanto, apenas um bit é usado para codificá-lo, representado no campo c.

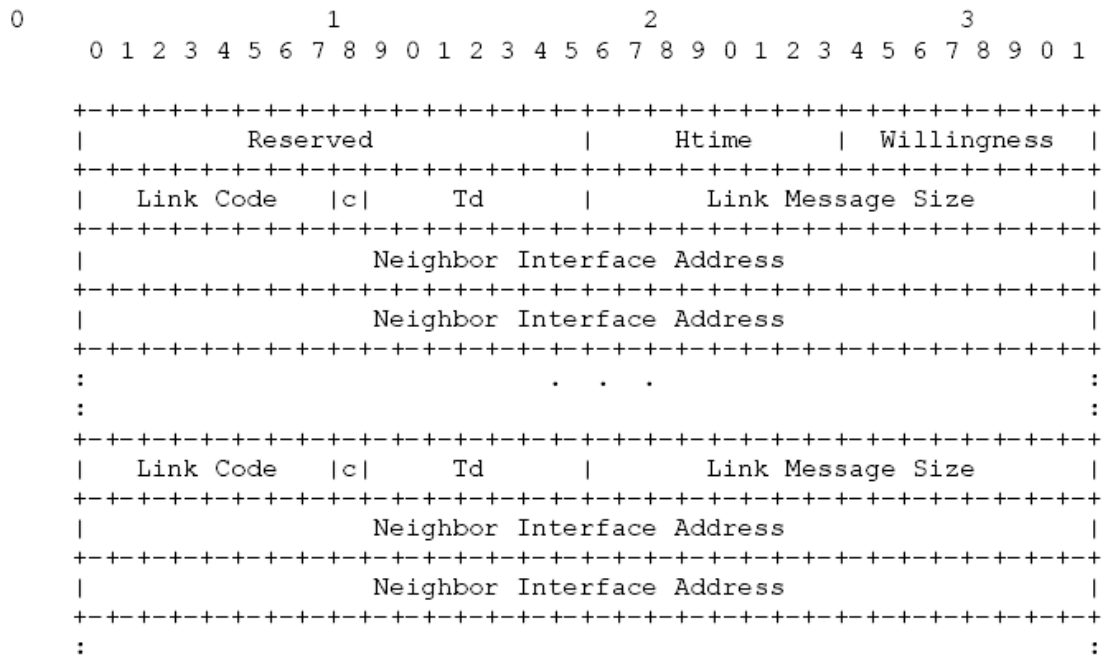


Figura 3-1 - Adaptação da mensagem *HELLO*

3.1.3. Impacto sobre o Escalonamento do Protocolo

Na proposta de protocolo o escalonamento é realizado como uma nova etapa, em comparação com o OLSR padrão. Portanto, as operações do OLSR com nossa extensão de confiança são as seguintes:

- Descoberta de vizinhança;
- Seleção de MPR;
- Controle de Topologia e Atualização;
- Atualização do link set com a informação sobre os nós não-confiáveis;
- Roteamento.

3.1.4. Experimentos e Resultados

Fizemos uma experiência simples, a fim de validar nosso esquema proposto. Usamos o *daemon olsrd* compatível com a RFC 3626 [23] e seu plug-in [24], para implementar o modelo proposto. Em seguida, construímos um ambiente de testes constituído por uma MANET real com topologia mostrada na Figura 3-2. Essa MANET foi implementada com computadores do tipo *laptop*, com sistema operacional *Debian GNU / Linux* e utilizando interfaces de rede IEEE 802.11g em modo *ad hoc*. Os nós A, B, C, D e E estavam executando o nosso *olsrd* habilitado para confiança e os nós G, H, X e Y estavam executando o *olsrd* padrão (compatível com a RFC 3626). Após 180 segundos de tempo inicial com o OLSR normal em operação na rede (incluindo os nós X e Y), observamos que o conjunto de MRP selecionados por B era MPR_B = { A, X }, enquanto que o conjunto de MRP selecionados por G era MPR_G = { F, Y }. Em seguida, foram iniciados fluxos contínuos de dados (10 pacotes ICMP por segundo) entre B e G e entre G e A, com as rotas representadas na Figura 3-3.

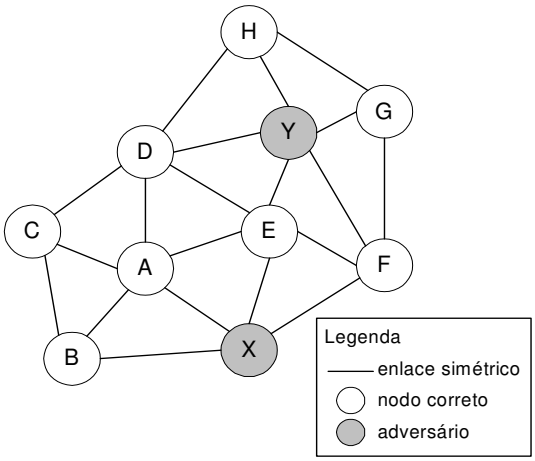
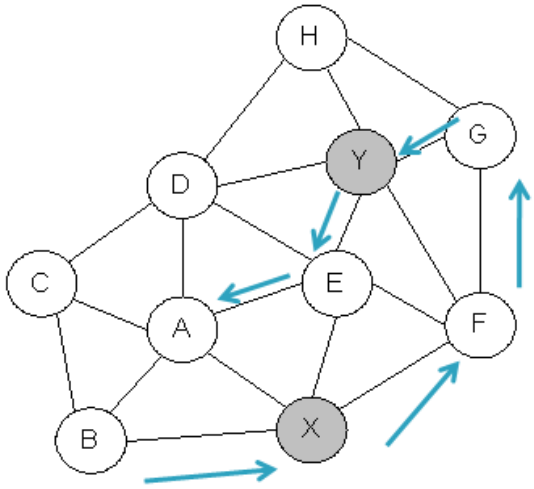


Figura 3-2 - Ambiente de Testes



B -> G: ROTA B->X->F->G

G -> A: ROTA G->Y->E->A

Figura 3-3 - Fluxo de dados contínuos

Após a rede e os fluxos de dados alcançarem a estabilidade, o mecanismo de encaminhamento de pacotes foi desabilitado nos nós X e Y, como mostra a Figura 3-4, mas sem que estes deixassem de transmitir corretamente as mensagens TC, i.e., o OLSR continuou a ser executado corretamente no X e Y. Desse modo, X e Y passaram a não colaborar com o roteamento, deixando de encaminhar pacotes que eles deveriam fazê-lo conforme o protocolo de roteamento.

Começamos a acompanhar, a partir de então, a medida de confiança nos nós OLSR com a confiança habilitada, (A, B, C, D, E e F).

Nos experimentos, usamos os seguintes parâmetros:

- $\alpha = 0{,}10$;
- $w_1 = w_2 = 0{,}5$;
- limiar de confiança = 0,7.

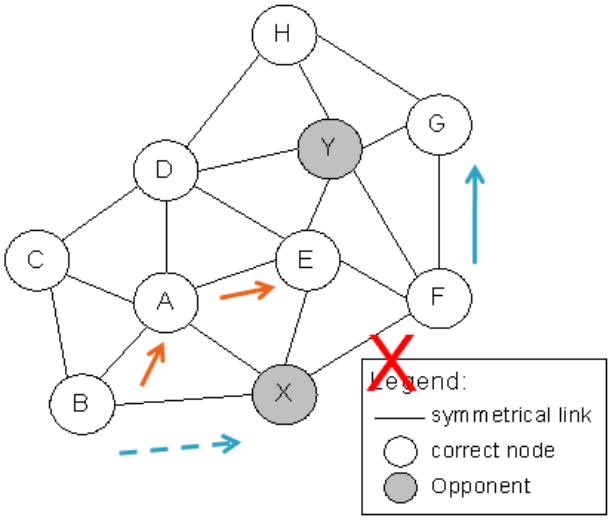


Figura 3-4 - Fluxo após o estado estacionário

Nestes experimentos, foram notadas as seguintes evidências:

- Depois de 1 segundo, o vizinho de X a um salto (i.e. A, B, E e F) e Y (A, D, E e F) tinham a medida Td abaixo de 0,5, para X e Y respectivamente. X foi eliminado pelo conjunto MPR de A, D, E e F.
- Dado a confiança habilitada na configuração do OLSR, o conjunto MPR do nó B mudou para MPR_B = { A, C } e o fluxo de dados de B para G foi restabelecido através da seguinte rota alternativa:

  B -> G: ROTA B->A->E->F->G

- O Fluxo de dados de G para A foi permanentemente interrompido (Figura 3-5), pois G não implementou a confiança do OLSR.
- Os Nós A e C também marcaram o nó Y como não-confiável, mas somente após dois ciclos de *HELLO* depois do Y ter começado a agir como nó malicioso. No mesmo caminho, os nós C e D marcaram o X como não confiável. Isto aconteceu porque um nós vizinho a um salto e com a confiança habilitada no OLSR anunciou uma baixa reputação dos dois nós. No entanto, o nó B nunca marcou o Y como não confiável porque ele não está a 2 saltos de distancia de Y e B não recebeu um anuncio de ma reputação sobre Y.

- O OLSR padrão em G e H não foram perturbados pela confiança habilitada no OLSR dos outros nós, mostrando a compatibilidade do nosso OLSRD reforçado com outras implementações do OLSR padrão.

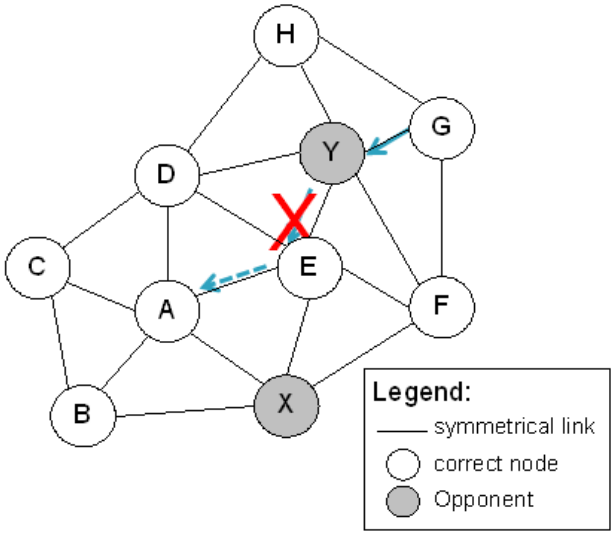


Figura 3-5 - Fluxo de dados de G para A interrompido

A análise dessas evidências demonstra a aplicabilidade do modelo proposto, pois:

- Os nodos que possuíam o OLSR com o mecanismo de confiança proposto habilitado puderam detectar corretamente os vizinhos que não estavam colaborando com o encaminhamento de pacotes e eliminá-los do roteamento OLSR.
- Essa operação permitiu que o encaminhamento OLSR fosse efetivamente melhorado, pois uma nova rota alternativa foi corretamente estabelecida evitando os nodos não confiáveis.
- Os nodos que executavam o OLSR padrão continuaram operando normalmente e não foram afetados pela modificação realizada.

Certamente, experimentos adicionais serão necessários para demonstrar a validade do modelo em situações mais gerais. Tais experimentos poderão ser realizados usando um ambiente de simulação de redes (e.g. ns-2). Por limitação de tempo, tais experimentos não foram conduzidos no contexto deste trabalho.

Não obstante, os resultados obtidos apontam para a validade do modelo, devendo-se ter especial preocupação em estabelecer os parâmetros mais adequados para utilização em cada caso (i.e. α, w_1, w_2 e o limiar de confiança).

4. CONCLUSÕES

Neste trabalho a confiança estudada é relacionada com encaminhamento robusto de pacotes e com o roteamento em MANET que utiliza o protocolo OLSR. Assim, o principal objetivo do modelo consiste em classificar os nós vizinhos em confiáveis e não-confiáveis a partir da avaliação objetiva da confiança. Como conseqüência dessa avaliação, os nodos não confiáveis são excluídos do processo de escolha de rotas do protocolo OLSR, eliminando-os do encaminhamento de pacotes.

O nosso modelo faz uso do protocolo de roteamento OLSR, que é um protocolo pró-ativo, baseado em estado de enlaces onde cada roteador disporá a qualquer momento, de rotas pré-estabelecidas e nenhum tempo de descoberta será despendido quando uma comunicação for imediatamente requisitada.

As métricas e probabilidades usadas neste trabalho são baseadas no TRAVOS [15], que é um modelo de confiança e reputação baseada em agentes e a confiança é medida através de probabilidade. Este trabalho é validado pela valor da confiança baseada em interações passadas e reputação obtida pelos outros nós onde existem três métodos de calcular a confiança em outro agente.

Neste trabalho a medida de confiança é gerada para cada vizinho combinando tanto a confiança direta quanto a reputação. Se esta medida de confiança no que diz respeito a um vizinho está abaixo do limiar pré-definido, o nó é considerado não confiável. A confidência é também calculada, a fim de fornecer uma medida de quão confiável é o valor de confiança / reputação utilizado no modelo.

O modelo proposto tira proveito da natureza *broadcast* de uma rede sem fios, o que permite ao nó monitorar o comportamento do vizinho quando um pacote deve ser encaminhado por ele. Cada vez que um pacote IP é enviado a um vizinho para ainda ser encaminhado na rede, uma interação é observada. A interação é bem sucedida se o vizinho encaminhar o pacote como esperado e é considerada mal sucedida se este não o fizer.

Os valores iniciais de confiança direta (antes de qualquer interação passada) são sempre definidos como completamente confiáveis, uma medida que corresponde ao comportamento inicial do nó OLSR, dado que o nó espera para a colaboração imediatamente, mesmo sem identificar seus vizinhos.

A fim de lidar com a troca de informações sobre confiança nos nós foi usado o campo *"RESERVED"*, destinado para implementações futuras ou não especificadas no protocolo padrão. Esse campo é usado para trocar informações sobre a confiança direta entre os vizinhos, sem maiores preocupações sobre compatibilidade com o OLSR padrão, permitindo a coexistência de instâncias OLSR compatíveis com a RFC 3626 e instâncias que tenham a extensão de confiança proposta.

A proposta apresentada foi validada com uma implementação real do modelo como uma extensão de plug-in do *daemon* OSLR UniK e seu uso em uma MANET com condições de operação hipotética.

A proposta necessita ainda de uma validação mais abrangente, o que poderá ser realizado na forma de simulações. Em tais experimentos, torna-se importante fazer um estudo do comportamento do modelo em função de seus parâmetros numéricos (α, w_1 e w_2).

Este trabalho foi apresentado no 7th *International Information and Telecommunication Technologies Symposium* [71], em dezembro de 2008.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] GAST, M. - 802.11 Wireless Networks: The Definitive Guide, O'Reilly, ISBN 0-596-10052-3, 656 pages, April 2005.

*[2] CORSON, S. e MACKER, J. - Mobile Ad hoc Networking (*MANET*): Routing Protocol Performance Issues and Evaluation Considerations, IETF RFC 2501, 1999.*

[3] Website do MANET Working Group – http://www.ietf.org/html.charters/manet-charter.html.

[4] PERKINS, C e BELDING-ROYER, E. - Ad hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.

[5] CLAUSEN, T. e JACQUET, P. - Optimized Link State Routing Protocol (OLSR), IETF RFC-3626, 2003.

[6] OGIER, R., TEMPLIN, F. e LEWIS, M. - Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), IETF RFC 3684, 2004.

[7] JOHNSON, D., HU, Y., e MALTZ, D. - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, IETF RFC 4728, 2007.

[8] ARGYROUDIS, P.G. e O'MAHONY, D. - Secure Routing for Mobile Ad hoc Networks, IEEE Communications Surveys & Tutorials, vol. 7, pp. 2-21, 2005.

[9] HU, Y-C. e PERRIG, A. - A Survey of Secure Wireless Ad hoc Routing, IEEE Security and Privacy, IEEE Educational Activities Department, Vol. 2, pp. 28-39, 2004.

[10] ZHOU, L. e HAAS, Z. J. - Securing Ad hoc Networks. IEEE Networks, 13(6):24-30, November/December 1999.

[11] HUBAUX, J., BUTTYAN, L. e CAPKUN, S. - The Quest for Security in Mobile Ad hoc Networks, Proceedings of ACM Symposium on Mobile Ad hoc Networking and Computing – MobiHOC 2001, 2001.

[12] PUTTINI, R. S., ME, L., DE SOUSA JR., R. T. - On the Vulnerabilities and Protection of Mobile Ad hoc Network Routing Protocols. In: Proceedings of the 3rd International Conference on Networking ICN2004. IEEE, pp. 676-684, New Jersey, USA. 2004.

[13] MARSH, S. - Formalizing Trust as a Computational Concept. PhD Thesis, University of Stirling, (1994).

[14] SABATER, J. e SIERRA, C. - Review on Computational Trust and Reputation Models. Artificial Intelligence Review (2005) 24:33-60.

[15] PATEL, J. - A Trust and Reputation Model for Agent-Based Virtual Organizations, Thesis of Doctor of Philosophy, Faculty of Engineering and Applied Science. School of Electronics and Computer Science, University of Southampton, January 2007.

[16] ADNANE, A., BIDAN, C. e DE SOUSA JR., R.T. - Effectiveness of Trust Reasoning for Attack Detection in OLSR, In Proceedings of 6th International Workshop on Security in Information Systems - WOSIS 2008, 2008.

[17] PIRZADA, A. A. e MCDONALD, C. - Establishing Trust in Pure Ad-hoc Networks, In Proceedings of 27th Australasian Computer Science Conference (ACSC'04), Dunedin, 2004.

[18] THEODORAKOPOULOS, G. e BARAS, J.S. - Trust Evaluation in Ad-hoc Networks, In Proceedings of the ACM Workshop on Wireless Security (WiSE'04), 2004.

[19] BUCHEGGER, A. e LE BOUDEC, J.Y. - Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks). In Proceedings of Third ACM International Symposium on Mobile Ad hoc Networking and Computing - : MobiHoc 2002, 2002.

[20] PISSINOU, N., GHOSH, T., MAKKI, K. - Collaborative Trust-Based Secure Routing in Multihop Ad hoc Networks. In Proceedings of Third International IFIP-TC6 Networking Conference (3042):1446–1451, 2004.

[21] VIRENDRA, M., JADLIWALA, M., CHANDRASEKARAN, M. e UPADHYAYA, S. - Quantifying Trust in Mobile Ad-hoc Networks, In Proceedings of IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems (KIMAS'05), 2005.

[22] YAN, Z., ZHANG, P. e VIRTANEN, T. - Trust Evaluation Based Security Solution in Ad hoc Networks, In Proceedings of the Seventh Nordic Workshop on Secure IT Systems,(NordSec'03), 2003.

[23] TØNNESEN, A. - OLSR UniK. Software disponível em http://www.olsr.org, 2004.

[24] TØNNESEN, A., HAFSLUND, A. e KURE, Ø. - The UniK - OLSR Plugin Library, OLSR Interop and Workshop, 2004.

[25] SMITH, C. e COLLINS, D. - 3G Wireless Networks, McGraw-Hill Telecom Professional, 2001.

[26] AMORIM, G. F. - Análise de Desempenho de Protocolos de Roteamento com Diferenciação de Serviços em Redes de Comunicação Móvel Ad hoc. Dissertação de Mestrado. Instituto Militar de Engenharia – Secretaria de Ciência e Tecnologia. Rio de Janeiro, 2002.

[27] MILLER, M. - *Descobrindo o Bluetooth*, Campus, 2001.

[28] JOHNSON, D. B. - *Routing in Ad hoc Networks of Mobile Hosts,* Workshop on Mobile Computing Systems and Applications, pp. 158-163, December 1994.

[29] CORRÊA, U. C. - Proposta de um *Framework* de Roteamento para Redes Móveis *Ad hoc*, Dissertação (Mestrado), Universidade Federal de Santa Catarina, 2005.

[30] DAS, S.R., PERKINS, C.E. e ROYER, E.M. - Performance Comparison of Two On-Demand Routing Protocols for Ad hoc Networks", IEEE Personal Communications, Fevereiro/2001.

[31] DRAVES, R., PADHYE, J. e ZILL, B. - Routing in Multi-Radio, Multi-hop Wireless Mesh Networks, In Proceedings of ACM MOBICOM 2004, 2004.

[32] MARTI, S., GIULI, T., LAI, K., and BAKER, M. - Mitigating routing misbehavior in mobile ad hoc networks, In Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, 2000.

[33] RAFFO, D. - Security Schemes for the OLSR Protocol for Ad hoc Networks, PhD Thesis, University of Paris 6, 2005.

[34] SANZGIRI, K., DAHILL, B., LEVINE, B., ROYER, E. e SHIELDS, C. - A Secure Routing Protocol for Ad hoc Networks. In International Conference on Network Protocols (ICNP). Paris, France, IEEE Computer Society. 78–87, 2002.

[35] GUERRERO, M. e ASOKAN, N. - Securing Ad Hoc Routing Protocols, In Proceedings of 2002 ACM Workshop on Wireless Security (WiSe'2002), in conjunction with the ACM MOBICOM2002, September, 2002.

[36] HU, Y.C., PERRIG, A. E JOHNSON, D. - Ariadne: A secure On-demand routing protocol for ad hoc networks, In Proceedings of ACM MobiCom 2002, Sep. 2002.

[37] PAPADIMITRATOS, P. e HAAS, Z.J. - Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[38] PUTTINI, R. S., PERCHER, J-M., MÉ, L., DE SOUSA JR., R.T. - A fully distributed IDS for MANET. *In: IEEE Computer Society, ISCC, 331–338, 2004.*

[39] PUTTINI, R.S. - Um modelo de segurança para redes móveis *ad hoc*. Brasília, 2004. 191 f. Tese (Doutorado) – Universidade de Brasília.

[40] MICHIARDI, P. - Mécanismes de sécurité et de coopération entre noeuds d'un réseau móbile ad hoc. Ecole nationale supérieur des télécommunications, Paris, 2004.

[41] BROMLEY, D. B. - Reputation, Image and Impression Management. John Wiley & Sons, 1993.

[42] BUSKENS, V. - The Social Structure of Trust'. Social Networks (20), 265—298, 1998.

[43] Plato - The Republic (370BC). Viking Press, 1955.

[44] MARIMON, R., J. P. NICOLINI, e P. TELES - Competition and Reputation, In Proceedings of the World Conference Econometric Society, Seattle, 2000.

[45] CELENTANI, M., D. FUDENBERG, D. K. LEVINE, e W. PSENDORFER - Maintaining a Reputation Against a Long-Lived Opponent, Econometrica 64(3), 691—704.5, 1966.

[46] eBay: 'eBay'. http://www.eBay.com. (Acessado em 20/11/2008)

[47] Amazon: 'Amazon Auctions'. http://auctions.amazon.com. (Acessado em 20/11/2008)

[48] DELLAROCAS, C. - The digitalization of Word-Of-Mouth: Promise and Challenges of Online Reputation Mechanisms, Management Science, 2003.

[49] GRANDISON, T. AND M. SLOMAN - A survey of trust in Internet application, IEEE, Communications Surveys, Fourth Quarter, 2000.

[50] MUI, L., A. HALBERSTADT, AND M. MOHTASHEMI - Notions of Reputation in Multi-Agent Systems: A Review, In Proceedings of the first international joint conference on autonomous agents and multiagent systems (AAMAS-02), Bologna, Italy. pp. 280—287, 2002.

[51] MCKNIGHT, D. H. AND N. L. CHERVANY - Notions of Reputation in Multi-Agent Systems: A Review, In Proceedings of the 34th Hawaii International Conference on System Sciences, 2002.

[52] ESFANDIARI, B. AND S. CHANDRASEKHARAN - On How Agents Make friends: Mechanisms for Trust Acquisition, In Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada. pp. 27—34, 2001.

[53] GAMBETTA, D. - Trust: Making and Breaking Cooperative Relations, Chapter: Can We Trust Trust?, pp. 213—237. Basil Blackwell, Oxford, 1990.

[54] SCOTT, J. - Social Network Analysis. SAGE Publications, 2000.

[55] BACHARACH, M. AND D. GAMBETTA - Trust in Society, Chapter: Trust in signs, Russell Sage Foundation, 2001.

[56] ZACHARIA, G. - Collaborative Reputation Mechanisms for Online Communities, Master's thesis, Massachusetts Institute of Technology, 1999.

[57] GLICKMAN, M. E. - Parameter estimation in large dynamic paired comparison experiments, Applied Statistics (48), 377—394.18, 1999.

[58] SCHILLO, M., P. FUNK, AND M. ROVATSOS - Using Trust for Detecting Deceitful Agents in Artificial Societites, Applied Artificial Intelligence (Special Issue on Trust, Deception and Fraud in Agent Societies), 2000.

[59] ABDUL-RAHMAN, A. AND S. HAILES - Supporting Trust in Virtual Communities, In Proceedings of the Hawaii's International Conference on Systems Sciences, Maui, Hawaii, 2000.

[60] LASHKARI, Y., M. METRAL, AND P. MAES - Collaborative Interface Agents, In Proceedings of the Twelfth National Conference on Artificial Intelligence, AAAI Pres, 1994.

[61] YU, B. AND M. P. SINGH - Towards a Probabilistic Model of Distributed Reputation Management, In Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada. pp. 125—137, 2001.

[62] YU, B. AND M. P. SINGH - Distributed Reputation Management for Electronic Commerce, Computational Intelligence 18(4), 535—549, 2002.

[63] YU, B. AND M. P. SINGH - An Evidential Model of Distributed Reputation Management, In Proceedings of the first international joint conference on autonomous agents and multiagent systems (AAMAS-02), Bologna, Italy. pp. 294—301, 2002.

[64] SEN, S. AND N. SAJJA - Robustness of Reputation-based Trust: Booblean Case, In Proceedings of the first international joint conference on autonomous agents and multiagent systems (AAMAS-02), Bologna, Italy. pp. 288—293, 2002.

[65] CARBO, J., J. MOLINA, AND J. DAVILA - Comparing predictions of SPORAS vs. a Fuzzy Reputation Agent System, In 3rd International Conference on Fuzzy Sets and Fuzzy Systems, Interlaken. pp. 147—153, 2002.

[66] CARTER, J., E. BITTING, AND A. GHORBANI - Reputation Formalization for an Information-Sharing Multi-Agent System, Computational Intelligence 18(2), 515—534, 2002.

[67] CASTELFRANCHI, C. AND R. FALCONE - Principles of Trust for MAS: Cognitive Anatomy, Social Importance, and Quantification, In Proceedings of the International Conference on Multi-Agent Systems (ICMAS'98), Paris, France. pp. 72—78, 1998.

[68] SABATER, J. AND C. SIERRA - Reputation and Social Network Analysis in Multi-Agent Systems, In Proceedings of the first international joint conference on autonomous agents and multiagent systems (AAMAS-02), Bologna, Italy. pp. 475—482, 2002.

[69] ADNANE, A., DE SOUSA JR, R.T, BIDAN, C. e MÉ, L - Autonomic trust reasoning enables misbehavior detection in OLSR, In 23rd Annual ACM Symposium on Applied Computing (ACMSAC 2008): Trust, Recommendations, Evidence and other Collaboration Know-how (TRECK) track, March 16-20, 2008.

[70] TITTERNINGTON, D. M. - Recursive Parameter Estimation using Incomplete Data, J. R. Statist. Soc. B, n.o 46, pp. 257-267.

[71] LAGUARDIA, J.A., PUTTINI, R.S., DE SOUSA JR. R.T. - A new trust-based extension to the HELLO message improves the choice of routes in OLSR networks, In Proceedings of 7th I2TS, Dec. 2008.