Endereçamento em redes *ad hoc* móveis: conceitos, protocolos e tendências

João Batista Pinto Neto [1,2]
Luís Henrique Maciel Kosmalski Costa [1]

Resumo: Uma rede móvel *ad hoc*, do inglês *mobile ad hoc network* (Manet) é um sistema autônomo de estações móveis conectadas por meio de enlaces sem fio. Manets são sistemas de comunicação sem infraestrutura e distribuídos, que exigem esquemas de endereçamento eficientes e rápidas rotinas de roteamento para garantir a mobilidade dos nós e os requisitos das aplicações heterogêneas. Os nós em uma Manet se deslocam aleatoriamente e, muitas vezes, atuam como roteadores. No entanto, essas funcionalidades da rede são dependentes do endereço IP dos nós, implicando na adoção de mecanismos de endereçamento para contemplar a atribuição única de endereço e baixa sobrecarga de rede. Manets podem ser facilmente configuradas e podem ser aplicadas a inúmeros cenários, mesmo em lugares desertos, e podem ser a única forma de comunicação em caso de catástrofes naturais e guerras. Este trabalho apresenta um estudo dos mecanismos de detecção de endereços duplicados e os principais protocolos de autoconfiguração propostos para redes *ad hoc* móveis.

***Palavras-chave*:** Redes *ad hoc* móveis. Redes sem fio. Endereçamento.

Abstract: *A mobile ad hoc network (Manet) is an autonomous system of mobile hosts connected by wireless links. Manets are unstructured distributed communication systems, which require efficient addressing schemes and fast routing capabilities to cope with node mobility and heterogeneous application requirements. Nodes in a Manet move randomly and often act as routers at the same time. Nevertheless, these functionalities are dependent of correct node IP Address assignment to ensure uniqueness and low network overhead provided by effective addressing mechanisms. Manets can be easily set up and have a large number of application scenarios, even in desert places and may be the only communication means in case of natural catastrophes and war. This work presents a survey of duplicate address detection mechanisms and major proposed auto-configuration protocols for mobile ad hoc networks.*

***Keywords*:** *Mobile ad hoc networks. Wireless networks. Addressing.*

1 Introdução

Redes *ad hoc* móveis, do inglês *mobile ad hoc networks* (Manets), integram uma categoria de redes sem fio que não necessitam de infraestrutura para o estabelecimento de comunicação entre os nós. São redes dinamicamente auto-organizáveis, nas quais os nós podem se comunicar diretamente entre si. Cada nó em uma Manet atua como roteador encaminhando pacotes para os nós diretamente conectados a ele. Essas características tornam as Manets ideais para aplicações em atividades militares, redes pessoais (Personal area network - PAN), operações de emergência e redes domésticas para transmissão de áudio e vídeo.

Devido à limitação da área de cobertura e da movimentação randômica dos nós, as rotas são muito dinâmicas, obrigando os protocolos de roteamento a manter e reconstruir as rotas de forma rápida e segura. Nas redes cabeadas, a atribuição de endereços IP aos nós é feita usando o protocolo DHCP (Dynamic host configuration protocol), porém, as Manets não têm infraestrutura ou administração centralizada para fornecer endereço dinâmico

[1]Universidade Federal do Rio de Janeiro - PEE/COPPE/GTA
[2]Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Rua Padre Augustinho, 2765 - 76803-826 Porto Velho-RO
{pinto@gta.ufrj.br;luish@gta.ufrj.br}

http://dx.doi.org/10.5335/rbca.2015.5143

por meio do protocolo DHCP, pois obrigaria o nó servidor DHCP a estar sempre conectado à rede, o que seria praticamente impossível devido à mobilidade dos nós [1]. A tarefa de atribuição de endereços é de responsabilidade dos próprios nós, que devem realiza-la de forma cooperativa. Além de contemplar possíveis uniões de partições de redes, os protocolos de roteamento enfrentam também problemas relacionados com o meio físico, tais como taxas atrasos de transmissão variáveis e alta taxa de perda de pacotes, características inerentes dos canais sem fio.

A evolução dos padrões de redes sem fio e dos dispositivos móveis tem contribuído para incentivar o desenvolvimento de aplicações usando Manets. Outro fator positivo é a utilização de rádios com várias interfaces que possibilitam o uso de vários canais simultaneamente pelo mesmo nó, aumentando a capacidade da rede e a vazão. Porém, a atribuição de canais não é trivial e deve ser feita com critério para evitar a surdez e o problema de terminal escondido [2].

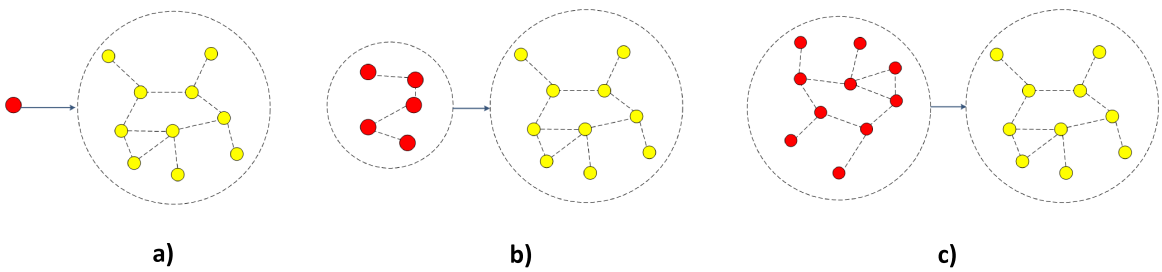
O presente trabalho apresenta conceitos, protocolos e tendências dos mecanismos de detecção de endereços duplicados e de autoconfiguração propostos para redes *ad hoc* móveis com o objetivo de fomentar a pesquisa e fornecer suporte a trabalhos acadêmicos em Manets.

Este trabalho está organizado da seguinte forma: na seção 2, serão abordados os mecanismos de detecção de endereço duplicado; na seção 3 serão apresentados os principais protocolos de autoconfiguração de endereço; na seção 4, as tendências das aplicações e tecnologias aplicadas às Manets, enquanto a seção 5 apresenta as considerações finais.

2 Mecanismos de detecção de endereço duplicado

A definição formal de detecção de endereço duplicado (DAD), proposta por Perkins et al. [3], "é o processo pelo qual um nó que solicita um endereço IP determina se um endereço candidato por ele selecionado está disponível. Um nó já contemplado com um endereço IP participa da DAD para proteger seu endereço IP de ser acidentalmente subtraído para uso por outro nó". A duplicação de endereços em uma Manet ocorre quando um novo nó é inicializado na rede ou quando um nó se desloca de uma rede para outra. Nos dois casos, é necessária a verificação, se o endereço atribuído ao novo nó ou o endereço do nó entrante já está em uso na rede. No caso do deslocamento de um nó de uma rede para outra, três situações podem ocorrer (Figura 1). Um único nó deixa uma rede e ingressa em outra (Figura 1a), um grupo de nós deixa uma rede e ingressa em outra (Figura 1b) ou, ainda, duas redes se unem, como na Figura 1c. Diferentes mecanismos de detecção de duplicação de endereço devem ser aplicados em cada caso, incluindo difusão, inundação e geração de novo identificador para a união de redes.

Figura 1 – Ocorrência de conflito de endereço em Manets



Fonte: Huq, (2010) [4].

2.1 Classificação dos mecanismos de DAD

Segundo Huq et al. [4], pode-se classificar os mecanismos de detecção de duplicação de endereços de diversas formas. As principais são:

a) Quanto ao agente responsável pela ação de detecção

Ação de um nó líder: comum em redes particionadas em grupos denominados aglomerados (*cluster*), um nó é eleito como cabeça do aglomerado (*cluster head*) e é responsável por manter a lista de endereços

livres e em uso na rede, gerenciando a atribuição, a recuperação e o conflito de endereços. Em virtude da mobilidade dos nós, o sistema de eleição deve ser eficiente para não causar sobrecarga na rede;

Ação de um nó individual: neste caso, é de responsabilidade do nó entrante promover meios de detectar o conflito e resolvê-lo quando for o caso, utilizando mensagens de inundação na rede;

b) Quanto à natureza da detecção

Detecção proativa: ao invés de detectar e resolver conflitos implementados por algoritmos específicos, a detecção proativa força o nó a monitorar a rede constantemente e detectar anomalias por meio da análise das tabelas de roteamento e das mensagens de controle enviadas pelos nós. A vantagem desse mecanismo é a detecção precoce de conflitos sem impor sobrecarga na rede. O monitoramento pode ser feito por qualquer um dos agentes descritos anteriormente;

Detecção reativa: neste caso, nenhuma ação é tomada até que seja relatada na rede uma inconsistência na tabela de roteamento. Os nós envolvidos iniciam então algoritmos para solucionar o conflito. Embora não apresente sobrecarga na rede, esse mecanismo pode prejudicar o tráfego devido à detecção tardia de conflito;

c) Quanto à precisão da detecção

Detecção de endereço duplicado forte (SDAD): estes mecanismos de detecção agem de forma proativa vasculhando a rede em busca de conflitos de endereços. Um mecanismo SDAD garante que não há endereços duplicados dentro de um intervalo de tempo limitado. A desvantagem é a alta sobrecarga na rede. Mecanismos SDAD podem ser implementados por um nó líder ou individual;

Detecção de endereço duplicado fraca (WDAD): os mecanismos WDAD apresentam menor precisão na detecção de endereços duplicados em relação ao SDAD, ou seja, não garantem a inexistência de duplicidade todo o tempo, e com isto geram menor sobrecarga. Podem detectar conflitos de endereço de forma reativa. Enquanto o mecanismo SDAD age de forma proativa, fazendo a verificação de duplicação em toda a rede antes de atribuir um endereço a um novo nó, os mecanismos WDAD toleram endereços duplicados na rede, por tempo limitado, desde que não haja ação na rede que gere conflitos, ou seja, uma duplicação que tenha como consequência o envio de pacotes à destinação incorreta.

Além das classificações dos mecanismos de detecção de endereço duplicado apresentadas, Huq et al. [4] propõem as seguintes métricas de desempenho:

a) Precisão: medida da eficiência na detecção de conflitos e da capacidade de evitar falsas ocorrências;

b) Taxa de detecção: definida como a razão entre o número de endereços duplicados detectados e o número total de endereços duplicados existentes na rede;

c) Sobrecarga: definida como a razão entre o número de pacotes de controle necessários para executar o mecanismo de detecção e o número de pacotes de dados transmitidos na rede.

Essas métricas auxiliam na identificação das características dos mecanismos de detecção de endereço duplicado, conforme demonstrado no Quadro 1.

Quadro 1 – Análise de desempenho dos mecanismos de DAD

Classificação	**Precisão**	**Taxa de detecção**	**Sobrecarga**
Detecção proativa	–	Alta	Alta
Detecção reativa	–	Baixa	Baixa
SDAD	Alta	–	Alta
WDAD	Baixa	–	Baixa

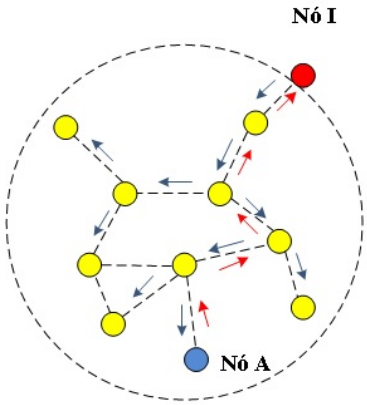
Fonte: Huq, (2010) [4].

Embora a classificação e as métricas propostas por Huq et al. [4] sejam relevantes para a escolha do mecanismo de DAD ideal para uma Manet, cuidados devem ser tomados na sua escolha, haja vista que essa é uma abordagem teórica e a implementação real carece de um conhecimento mais profundo desses mecanismos. Para prover ferramentas adicionais para avaliação, os principais mecanismos de DAD serão abordados nas próximas seções.

2.2 *Strong DAD*

O mecanismo proposto por Perkins et al. [3] no Internet *draft IP address autoconfiguration for ad hoc Networks*, e denominado posteriormente de *Strong duplicate address detection* (SDAD), executa inicialmente a geração randômica do endereço pelo nó ingressante na faixa 169.254.0.0/16. Após gerar o endereço candidato (FirstPermAddr), o nó ingressante configura sua interface com o endereço imediatamente anterior (LastTmpAddr), que será usado temporariamente durante o processo de atribuição de endereço. A Figura 2 ilustra passo a passo o processo de autoconfiguração.

Figura 2 – Processo de DAD - Exemplo de associação de nó



Fonte: Kim e Chung, (2008) [5].

O processo de autoconfiguração ocorre em cinco passos, quais sejam:

a) passo 1: o nó I gera os endereços FirstPermAddr e LastTmpAddr.

b) passo 2: o nó I envia uma mensagem em *broadcast* usando o protocolo ICMP (ping) informando o endereço FirstPermAddr pretendido.

c) passo 3: todos os nós roteiam o pacote ICMP.

d) passo 4: o nó A, que detecta o conflito de endereço com o endereço FirstPermAddr, responde o ping para o endereço LastTmpAddr do nó I, que reinicia o procedimento retornando ao passo 1.

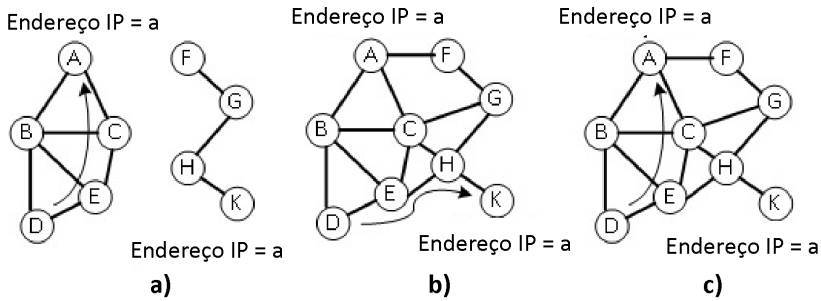
e) passo 5: caso não haja resposta após três tentativas sucessivas temporizadas, o nó ingressante atribui o endereço FirstPermAddr à sua interface de rede.

Deve-se observar que esse mecanismo envolve uma inundação na rede provocada pelo nó ingressante. Além disso, a temporização entre as tentativas deve ser proporcional ao diâmetro da rede, o que compromete a escalabilidade e, em consequência, prejudica o tráfego de dados [3]. O mecanismo também não garante unicidade do endereçamento na ocorrência de desconexões temporárias e apresenta elevada sobrecarga quando o espaço de endereços disponíveis fica reduzido. No caso de união de Manets todos os nós precisam ser verificados, porém, não há na descrição do protocolo informação de como detectar esse evento. Da mesma forma, na ocorrência de particionamento temporário da rede por um tempo não limitado, nada impede que as duas partes atribuam os mesmos endereços, o que compromete a unicidade de endereços [6].

2.3 *Weak DAD*

Diferentemente do mecanismo SDAD, o *Weak duplicate address detection* (WDAD), proposto por Vaidya [6], não requer a detecção de duplicação de endereços de todos os endereços e, além disso, ele tolera a duplicação por um período limitado de tempo. A preocupação dos pesquisadores foi de resolver as limitações impostas pelo SDAD, como a inundação para detecção de cada endereço gerado, e solucionar problemas de endereçamento na ocorrência de particionamento e união de redes. Para ilustrar o funcionamento do protocolo, considere-se a Figura 3, em que mostra duas redes distintas contendo nós com o mesmo endereço.

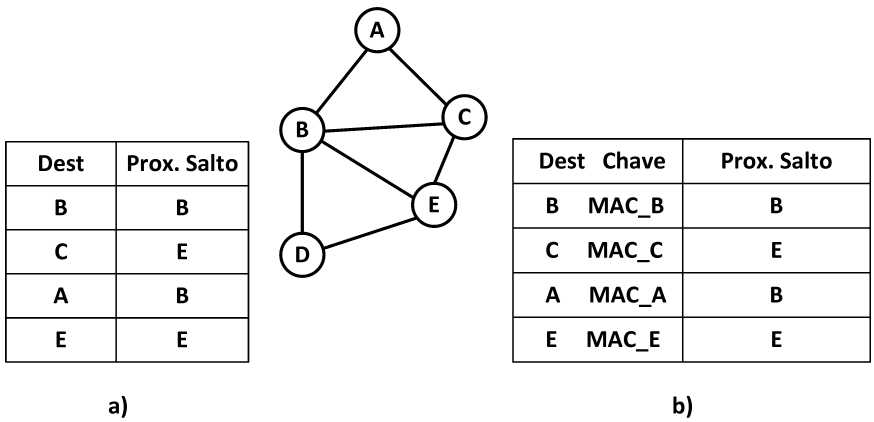
Figura 3 – Mecanismo de WDAD - União de Redes



Fonte: Vaidya, 2002 [6].

Antes da união, o nó D usa o endereço *a* para encaminhar pacotes via [E,C] para o nó A (Figura 3a). Após a união, duas situações podem ocorrer: os pacotes destinados ao nó A são encaminhados pelo nó D ao nó K (Figura 3b) ou continuam sendo encaminhados pelo nó D ao nó A (Figura 3c). A primeira situação não é aceitável, porém, a última pode ser tolerada temporariamente para que não haja perda de pacotes destinados ao nó A, a partir de D.

Figura 4 – Utilização do protocolo OLSR pelo WDAD



Dest	Prox. Salto
B	B
C	E
A	B
E	E

a)

Dest Chave	Prox. Salto
B MAC_B	B
C MAC_C	E
A MAC_A	B
E MAC_E	E

b)

Fonte: Vaidya, (2002) [6].

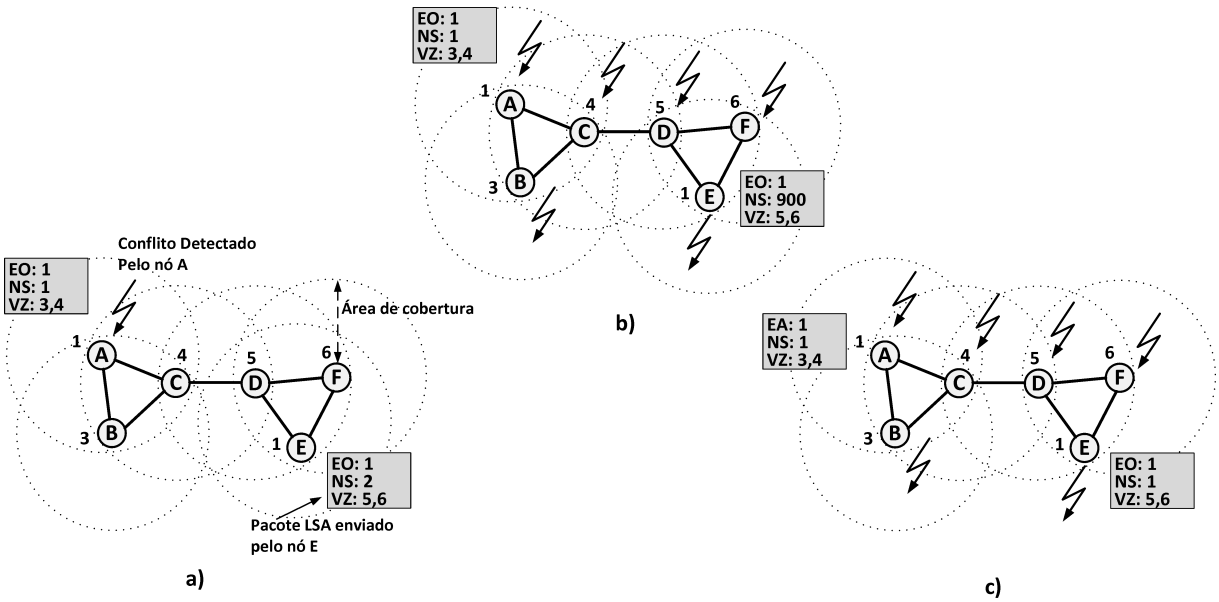
Para garantir a unicidade de endereçamento na rede, o WDAD usa uma chave única associada ao endereço IP no momento da sua geração. A chave padrão é o endereço físico, mas pode ser uma chave de geração randômica no caso de redes em que haja a possibilidade de duplicação do endereço MAC. Como a associação não pode ser feita no cabeçalho IP do pacote, a solução proposta é atrelar a dupla (IP, Chave) no protocolo de roteamento. A Figura 4a apresenta a tabela de roteamento original do nó D construída pelo protocolo OLSR (*Optimized link state routing*) [7]. A Figura 4b mostra a tabela de roteamento alterada, do mesmo nó, construída para trabalhar em conjunto com o mecanismo WDAD. As alterações no anúncio de estado de enlace (*Link state announcement* – LSA) consistem em bloquear a rota ao receber uma mensagem de atualização do estado do *link* que contenha o mesmo endereço IP com chave diferente e anunciar a detecção de duplicação de endereço na rede. Ao receber a

mensagem o nó usa o mecanismo SDAD para gerar um novo endereço e anuncia a todos os nós o novo endereço. Para não perder pacotes durante esse processo, os pacotes endereçados ao antigo endereço são tunelados com o endereço novo. O mecanismo apresenta sobrecarga, embora pequena, ao associar o endereço IP à chave e em maior escala no momento da detecção do conflito de endereço quando o mecanismo SDAD é chamado, provocando inundação na rede. O protocolo suporta união de redes por estar continuamente testando a unicidade dos endereços.

2.4 Detecção de endereço duplicado passiva (PDAD)

Proposto por Weniger (2003) [8], esse mecanismo pertence à categoria de detecção proativa e trabalha em conjunto com protocolos de roteamento, com a diferença, em relação ao *WDAD*, de não alterar as tabelas de roteamento. Todos os nós analisam as mensagens de anúncio de estado de enlace (LSA) e executam algoritmos para detectar inconsistências e inferir a existência de duplicidade de endereços na rede. A Figura 5 ilustra o mecanismo PDAD-SN, que usa os números de sequência dos LSAs.

Figura 5 – Mecanismo de PDAD-SN e variações



Fonte: Weniger, (2005) [9].

O mecanismo se baseia nas seguintes regras básicas, obrigatórias em Manets configuradas adequadamente:

a) um nó usa números de sequência em ordem crescente;

b) um nó usa um número de sequência uma única vez (com exceção de quando ocorre o *wrap-around* do número de sequência);

c) dois nós não podem ter os mesmos vizinhos, se eles estiverem a mais de dois saltos um do outro.

Nas três variações propostas do algoritmo PDAD-SN, os nós **A** e **E** têm o mesmo endereço. Na primeira variação (Figura 5a), se o nó **E** recebe um LSA com o endereço de origem (EO) igual ao seu, ele não pode determinar a procedência do pacote em razão da pequena diferença dos números de sequência (NS) e também porque o pacote recebido tem um número de sequência menor que o atual. Porém, na situação inversa, se o nó **A** recebe o pacote de **E** com um número de sequência maior que o atual, ele detecta a duplicidade de endereço. Na segunda variação, denominada PDAD-*Sequence number difference* (SND), ilustrada na Figura 5b, a detecção de endereço duplicado é feita por meio da diferença dos números de sequência e dos respectivos tempos em que os LSAs foram recebidos. Neste caso a detecção é feita pelos nós intermediários.

Finalmente, na última situação, denominada PDAD-*Sequence number equal* (SNE), os números de sequência são iguais. Os nós intermediários, neste caso, também podem detectar a duplicidade de endereço ao constatar que os vizinhos (VZ) são diferentes (Figura 5c). Além do algoritmo PDAD-SN e suas variações, o autor apresenta mais dois algoritmos (PDAD-LP e PDAD-NH) baseados na frequência de atualização de rotas e na informação de vizinhos que podem ser usados em conjunto para aumentar a eficiência do mecanismo. Devido à ausência de geração de mensagens, o mecanismo não apresenta sobrecarga na rede, porém, é dependente de protocolo de roteamento e apresenta eficiência na detecção proativa de conflito de endereço. A proposta tem abordagem distribuída e suporta a união de redes.

3 Protocolos de autoconfiguração de endereço

A natureza dinâmica das Manets proporciona um vasto campo de pesquisa direcionado a encontrar soluções para o problema do endereçamento dos nós de forma eficiente e segura. O desvanecimento inerente dos canais das redes sem fio e a mobilidade são alguns desafios a serem enfrentados. Com relação à distribuição de endereços IP, a conexão e a desconexão aleatória dos nós dificultam o gerenciamento, gerando conflitos de endereços. Esses fatores, acrescidos da união e do particionamento das redes, têm tirado o sono de muitos pesquisadores, haja vista o número de propostas publicadas sobre o tema [10].

O correto funcionamento de uma Manet exige que um protocolo de autoconfiguração de endereços atenda, além dos requisitos de dinamicidade e escalabilidade da rede, os objetivos de baixa perda de pacotes e atraso mínimo de entrega. Segundo Rohit et al. [11], os protocolos de autoconfiguração de endereço de uma Manet devem focar para os seguintes objetivos:

a) Atribuir endereços IP únicos: garantir que dois ou mais nós não obtenham o mesmo endereço IP;

b) Funcionalidade: um endereço IP deve ser associado ao nó somente enquanto o mesmo permanecer na rede. Quando o nó deixar a rede, o endereço deve ficar disponível para ser associado a outro nó;

c) Robustez à perda de mensagens: em caso de falha de algum nó ou perda de mensagens, o protocolo deve ser rápido o suficiente para prevenir que dois ou mais nós tenham o mesmo endereço IP;

d) Permitir roteamento multissaltos: se um nó tem um endereço IP livre, ele deve ser atribuído a um nó requisitante mesmo se ele estiver a dois ou mais saltos de distância;

e) Minimizar a sobrecarga na rede: os pacotes de controle do protocolo devem causar o mínimo de prejuízo ao tráfego dos pacotes de dados;

f) Tratamento de pedidos simultâneos: o protocolo deve implementar uma rotina que impeça a atribuição do mesmo endereço IP quando dois nós o requisitarem ao mesmo tempo;

g) Gerenciar o particionamento ou a união da rede: o protocolo deve ser capaz de realizar a união de duas Manets assim como o particionamento da rede em duas Manets diferentes;

h) Garantir sincronização: o protocolo deve se adaptar às rápidas mudanças da topologia da rede devido à mobilidade dos nós. A sincronização deve ser realizada periodicamente para garantir a atualização permanente da rede.

Além dos objetivos mencionados, o protocolo deve atender também a critérios de segurança no momento da atribuição do endereço. Redes *ad hoc* não dispõem de mecanismos centralizados de segurança como *firewall* e detecção de intrusos e *proxy*. Portanto, a segurança da rede é uma atribuição de responsabilidade de todos os nós participantes. Embora alguns protocolos de autoconfiguração de endereço implementem defesas contra ameaças, este é um desafio ainda em aberto [12].

O problema fundamental de atribuir endereço para os nós de uma Manet, seja para contemplar os objetivos destacados por Villalba et al. (2011) [10] ou para solucionar os desafios da mobilidade dos nós, do particionamento e da união de redes, têm gerado muitas propostas de protocolos de autoconfiguração de endereços. Porém, todas

têm um objetivo em comum: garantir a unicidade de endereço do nó na rede por meio de mecanismos de controle centralizado (tabelas de alocação de endereço) ou mecanismos de detecção de conflito de endereços.

Os protocolos de autoconfiguração em Manets são classificados como *stateless*, *stateful* e híbridos, que reunem características das duas categorias anteriores. Os mecanismos de DAD são usados em protocolos *stateless*, conforme será tratado nas próximas seções.

3.1 Abordagem *stateless*

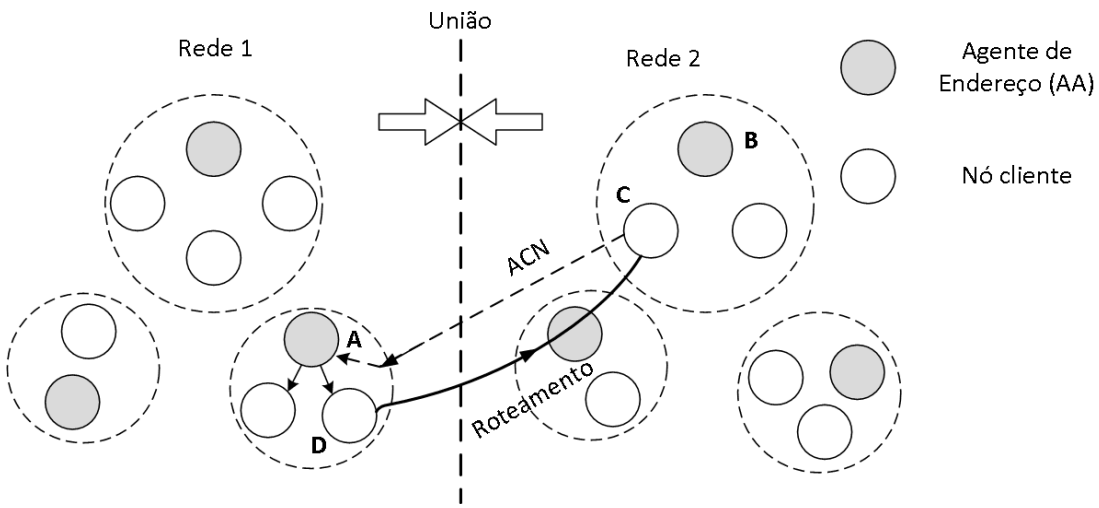
Os protocolos de autoconfiguração de endereço *stateless* caracterizam-se por não manter tabelas de alocação de endereços. Os nós que entram na rede geram seu próprio endereço ou atribuem endereços para outros nós, baseados no endereço físico da interface sem fio ou de forma randômica. Para evitar conflito de endereçamento, um procedimento de detecção de endereço duplicado (DAD), responsável por manter a integridade da distribuição dos endereços na rede, é disparado quando um novo nó requisita um endereço à rede ou quando há um processo de união de duas Manets.

3.1.1 *Apac*

O protocolo *Agent based passive auto-configuration* (APAC), proposto por Li et al. [13], cria a figura do agente de endereço (*Address agent* – AA), um nó responsável pela distribuição de endereços IP na rede. Os AAs têm uma limitação quanto ao número de clientes, o que divide a rede em grupos. Os endereços, à medida que são atribuídos, são armazenados nos AAs de cada grupo. Quando um nó deseja associação ele envia uma mensagem de busca de AA. Caso nenhum AA responda, ele gera seu próprio endereço e um identificador AA que o habilita a gerar endereços para os novos nós. Após gerar um endereço, o AA o atribui ao nó entrante e o processo de verificação de conflito é realizado pelo mecanismo PDAD. Todos os nós podem detectar conflitos, porém, somente um AA pode resolver. Quando um nó sai da rede por um tempo predeterminado, o AA recupera seu endereço, eliminando-o da tabela de endereços atribuídos na rede.

No caso de união de redes, há maior chance de haver conflitos de endereço. Nesse caso, qualquer nó que detectar um conflito de endereços deve informar ao AA. A Figura 6 ilustra um exemplo típico de união de redes em que ocorre um conflito. Os nós **A** e **B** têm o mesmo identificador AA, e o nó **C** detecta o conflito por intermédio dos LSAs (PDAD). O nó **C** envia uma notificação de conflito de endereço (*Address conflict notification* – ACN) para **D**, que a encaminha para **A**. O nó **A** gera novo identificador AA e informa aos nós membros, resolvendo o conflito.

Figura 6 – Apac - Detecção de conflitos de IP na união de redes



Fonte: Li, (2007) [13].

O protocolo garante a unicidade na atribuição de endereços IP na rede mantendo uma tabela de endereços

alocados residente nos agentes de cada grupo. O protocolo não usa um servidor central para distribuição de endereços. Essa função é responsabilidade dos nós agentes de endereço. O protocolo suporta união e particionamento de redes e é dependente de protoclo de roteamento proativo. O protocolo apresenta baixa sobrecarga, característica do mecanismo PDAD.

3.2 Abordagem *stateful*

Os protocolos desta categoria, também denominada categoria livre de conflito, utilizam uma tabela de alocação de endereços que pode ser centralizada ou distribuída, para atribuir endereços aos nós da rede.

3.2.1 MANETconf

O protocolo Manetconf, proposto por Nersagi e Prakash [14], utiliza duas tabelas de alocação de endereços. Uma contém todos os endereços em uso na rede e a outra contém todos os endereços pendentes a serem atribuídos aos novos nós. Todos os nós participantes da rede têm uma cópia de ambas as tabelas que são atualizadas a cada evento, como entrada e saída de nós, união e particionamento de redes.

Quando um novo nó se associa a rede, ele envia uma mensagem de busca de vizinhos. Caso não haja resposta, ele assume ser o primeiro nó da rede e inicializa as tabelas. Caso um ou mais vizinhos atendam à requisição, o nó entrante seleciona um dos vizinhos, denominado **iniciador**, e o processo de associação começa com os seguintes passos:

a) passo 1: o nó entrante envia uma mensagem de requisição de endereço ao Iniciador;

b) passo 2: o Iniciador então seleciona um endereço que não esteja nas suas tabelas, atualiza a tabela de pendência com o endereço selecionado e envia uma mensagem a todos os nós da rede informando a inserção;

c) passo 3: o nó que recebe a mensagem de inclusão na tabela de pendência verifica em suas tabelas se há ocorrência de conflitos. Caso não haja, ele envia uma mensagem de resposta positiva, concordando com a inserção. Caso contrário, envia uma mensagem de resposta negativa;

d) passo 4: se todas as mensagens recebidas pelo Iniciador forem positivas, ele retira o endereço da tabela de pendências, o adiciona na tabela de endereços alocados, atribui o endereço ao nó entrante e informa a todos os nós da rede a nova inserção;

e) passo 5: caso o Iniciador receba pelo menos uma resposta negativa, ele retorna ao passo 2, reiniciando o processo.

O protocolo usa uma identificação única para cada rede. Essa identificação é composta pelo menor endereço IP da rede e por um identificador universal único (*Universal unique identifier* – UUID), que permite gerenciar a união e o particionamento de Manets. Na união, os nós mais exteriores que detectarem identificadores de rede diferentes trocam suas tabelas de endereços alocados, criando uma tabela contendo todos os endereços alocados das duas tabelas. Os endereços duplicados são eliminados, fazendo com que um dos nós descarte o seu antigo endereço e inicie o processo de aquisição novamente. A tabela é então replicada para todos os nós da nova rede [15].

No caso do particionamento, a partição que ficar com o nó de menor endereço mantém o identificador da rede e exclui todos os endereços que migraram para a outra partição. Na partição restante, o nó de menor endereço cria um novo identificador da rede e o propaga para todos os nós da nova rede. As operações de união e particionamento dependem da existência de um protocolo de roteamento proativo na rede para que os nós detectem os eventos a partir da análise das tabelas de roteamento [14].

O protocolo garante a unicidade na atribuição de endereços IP na rede mantendo uma tabela de endereços alocados residente em cada nó da rede. O protocolo não usa um servidor central para distribuição de endereços. Essa função é responsabilidade de todos os nós da rede. O protocolo suporta união e particionamento de redes e é dependente de protocolo de roteamento proativo. O protocolo apresenta alta sobrecarga, em virtude das mensagens de inundação que podem comprometer o tráfego de dados.

3.2.2 *Prophet*

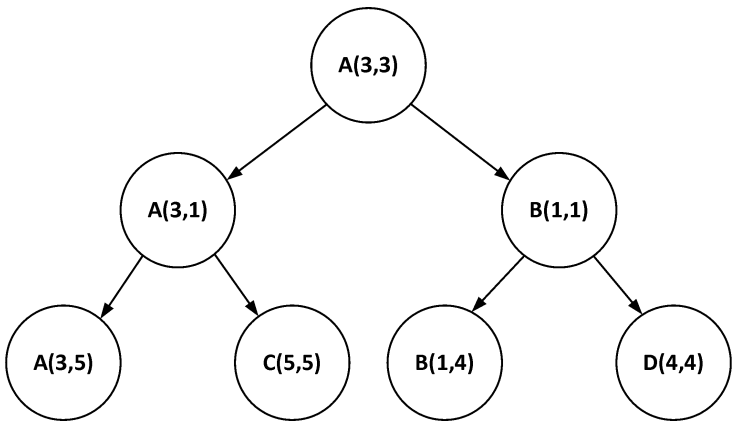
A proposta do protocolo Prophet, que não deve ser confundido com o seu homônimo das redes tolerantes a atrasos e desconexões (*Delay and disruption tolerant networks* – DTNs), não contempla detecção de conflito adotada pelos dois protocolos apresentados anteriormente. Esse protocolo é descentralizado e não mantém uma tabela estática dos endereços. A alocação de endereços é feita de forma randômica, sequencialmente, dentro de um espaço grande o suficiente para que não ocorra duplicidade. O algoritmo usa uma função *f(n)* que gera números inteiros a partir de uma semente dentro de um conjunto **R** que satisfaça duas propriedades:

a) o intervalo entre duas ocorrências do mesmo número é extremamente longo.

b) a probabilidade de mais de uma ocorrência do mesmo número em um limitado número de sequências diferentes iniciadas por sementes diferentes é baixa.

A Figura 7 ilustra o algoritmo de geração de endereços do *PROPHET*. No exemplo $R \in [1, 8]$ e *f(n)=(endereço X semente X 11) mod* 7. O processo é iniciado pelo nó A, primeiro da rede, que gera a semente 3 e o endereço 3 a partir de *f(n)*. Quando o nó B se aproxima, o nó A gera o endereço 1 e a nova semente 1 para o nó B e atualiza a sua semente. O processo se repete quando C se aproxima de A e D se aproxima de B.

Figura 7 – Protocolo Prophet - Alocação de endereços



Fonte: Zhu, Ni e Mutka, (2003) [16].

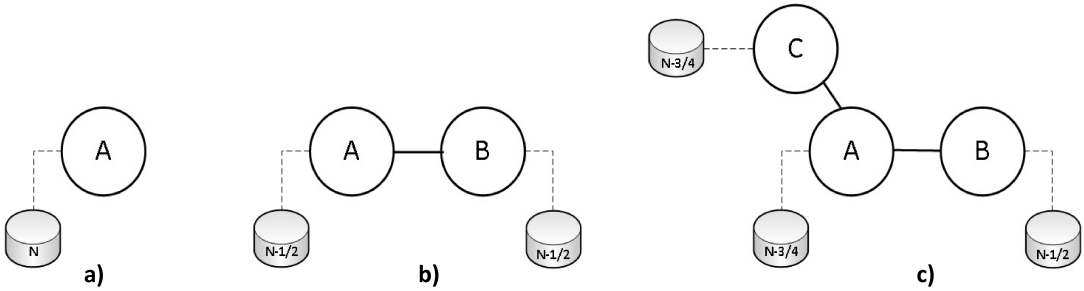
O protocolo suporta união e particionamento por meio da inclusão da semente raiz nas mensagens do protocolo de roteamento. A unicidade de endereços é garantida pelo processo de alocação, com baixa probabilidade de colisão. O nó A, gerador da semente raiz da rede, é chamado nó **profeta**, pois, a partir da semente raiz, o protocolo roda um algoritmo para prever a ocorrência de endereços duplicados. Caso seja detectado um alto número de endereços duplicados, uma outra semente raiz deve ser gerada [16].

3.2.3 *MAAA*

O protocolo *Mobility-aided address allocation* (MAAA), proposto por Chen, Fleury e Razafindralambo (2009) [17] é uma solução de atribuição de endereços usando uma distribuição de espaços disjuntos de endereços entre os nós, garantindo unicidade e escalabilidade. A manutenção das tabelas de alocação é de responsabilidade exclusiva dos nós, ou seja, cada nó ingressante torna-se um servidor, que vai gerenciar um escopo de endereços livres, distribuídos uniformemente, entre os nós vizinhos. A Figura 8 apresenta o processo de atribuição de endereços do MAAA.

O sistema é inicializado delegando a um nó o escopo completo (Figura 8a) ou, no caso de vários nós, dividindo-o igualmente entre eles. Quando o nó ingressa na rede ele faz uma requisição de endereço em *broadcast* para seus vizinhos, que respondem informando a faixa de endereços livres. No exemplo, somente o nó A responde que tem disponível N endereços. O nó B então retira e atribui a ele um endereço e divide o restante dos (N-1) endereços uniformemente com o nó A (Figura 8b). O nó C, que entra, realiza a mesma operação com A, seu

Figura 8 – Protocolo *MAAA* - Alocação de endereços



Fonte: Chen, Fleury e Razafindralambo, (2009) [17].

único nó vizinho (Figura 8c). À medida que o número de nós aumenta na rede, o número de servidores aumenta, porém com faixas de endereços livres cada vez menores. No caso geral, quando um nó entrante faz a requisição de endereço e um número S de vizinhos respondem, informando suas faixas de endereços, o nó entrante, após retirar um endereço, soma todas as faixas e as divide uniformemente formando S+1 blocos. Em seguida, ele retém um dos blocos para distribuição, e envia aos vizinhos os remanescentes.

O protocolo prevê o envio do conjunto de endereços a um vizinho escolhido randomicamente quando um nó deixa a rede abruptamente. Porém, não oferece solução explícita quando o nó desconectar-se abruptamente, problema que deve ser estendido no caso de particionamento da rede. O protocolo é imune a mudanças na topologia da rede e aproveita-se da mobilidade dos nós para aumentar a eficiência da distribuição de endereços, além de não depender do protocolo de roteamento.

3.3 Abordagem híbrida

Please wait...

Os protocolos dessa categoria exploram os mecanismos e abordagens das categorias *stateless* e *stateful* apresentadas anteriormente. Essa característica confere a eles maior demanda de recursos do nó, como processamento e espaço de memória.

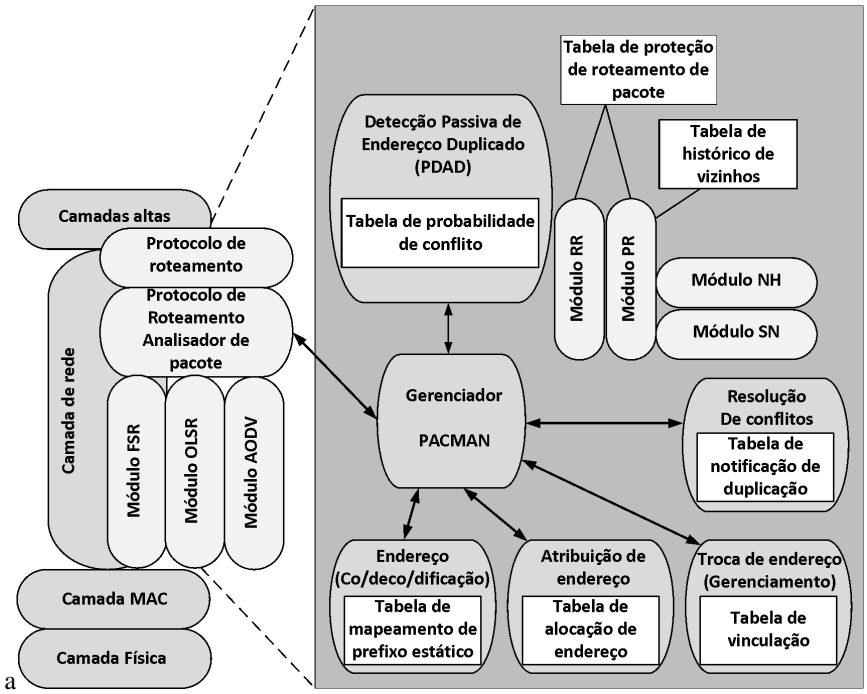
3.4 Pacman

O protocolo *Passive autoconfiguration for mobile ad hoc networks* (PACMAN) usa o mecanismo PDAD para detectar conflitos de endereço e mantém uma tabela de endereços alocados, o que lhe confere a participação na categoria de protocolos de autoconfiguração de endereços híbridos. Proposto por Weniger (2005) [9], esse protocolo, cuja arquitetura é mostrada na Figura 9, gera de forma randômica o endereço do nó entrante e aplica o mecanismo PDAD para detecção de conflito.

A Figura 9 revela a complexidade do protocolo em que o processo de associação de um nó na rede começa com o nó entrante atribuindo o próprio endereço IP. O protocolo usa um algoritmo probabilístico que seleciona randomicamente um endereço de um espaço disponível, dependente do número de nós e do tamanho da tabela de alocação. O gerenciador Pacman verifica se o endereço gerado não está em conflito com nenhum endereço da tabela de alocação e atribui imediatamente o endereço ao nó entrante. Embora esse processo seja muito rápido (alguns milissegundos), é possível, com baixíssima probabilidade, a atribuição duplicada de endereço, que será detectada pelo mecanismo PDAD. Ao detectar um conflito, o nó inicia o processo de eliminação de conflito executando o módulo Gerenciamento de troca de endereço, destacado na arquitetura do protocolo. O protocolo contempla a união e o particionamento de redes sem o uso de algoritmos ou procedimentos adicionais, além do mecanismo PDAD. A recuperação de endereços descartados é feita com a atualização das tabelas construídas pelos protocolos de roteamento. O protocolo também codifica/decodifica os endereços IP para minimizar a sobrecarga dos protocolos de roteamento.

O protocolo garante a unicidade de endereçamento executando a geração randômica do endereço IP e com-

Figura 9 – Protocolo Pacman - Arquitetura



a

Fonte: Weniger, (2005) [9].

parando o endereço gerado com uma tabela de endereços alocados. A manutenção da unicidade é garantida pelo mecanismo PDAD. O protocolo é dependente de protocolos de roteamento proativos. O protocolo apresenta baixa sobrecarga na rede, porém, conforme mostrado, exige nós com recursos consideráveis. O protocolo suporta união e particionamento de rede e tem abordagem distribuída.

4 Tendências em Manets

Uma abordagem nova é considerar a Manet como um conjunto de aglomerados (*clusters*) com o propósito de minimizar a carga administrativa, delegando a cada *cluster* a responsabildade de endereçamento e controle de acesso. Um mecanismo de configuração dinâmica e hierárquica de endereços IPv6, proposto por Wang e Qian (2015) [18], usa essa abordagem para configuração de endereços de forma distribuída e centralizada. Um nó central distribui blocos de endereços IPv6 para os nós centrais de cada *cluster*, denominados *cluster heads*, que fazem a distribuição para os membros do *cluster*. A proposta garante total ausência de conflito de endereços, mesmo no caso de união e particionamento da rede.

O protocolo IPv6 contempla um mecanismo de autoconfiguração para estações denominado IPv6 *Stateless address autoconfiguration*, especificado na RFC 4862 [19]. Esse mecanismo distribui e verifica conflitos de IP de forma semelhante ao mecanismo SDAD. É um mecanismo muito eficiente, porém, seu alcance é de um salto apenas, o que inviabiliza a sua aplicação em Manets em virtude da necessidade de verificação da duplicidade em toda a rede. Uma solução usando uma versão otimizada do protocolo *Neighbor discovery for IP version 6* (IPv6), especificado na RFC 4861, denominada ND++, foi proposta por Grajzer, Zernicki e Glabowski (2014) [20]. A proposta consiste em usar o protocolo de roteamento OLSR para estender a verificação de duplicidade para além de um salto. O processo é realizado em duas etapas. Na primeira etapa, o nó gera o endereço na forma padrão e checa a duplicidade com os vizinhos. Na segunda etapa, o protocolo entra em ação executando uma inundação controlada e, usando os nós *Multipoint relays* (MPRs) do OLSR, procede à verificação de conflito dentro de um diâmetro determinado por uma sobrecarga definida.

Essas duas propostas mostram que o campo de pesquisa em Manets está ainda pouco explorado. Com a

expansão dos dispositivos móveis, a adoção do conceito de internet das coisas e a chegada dos novos padrões de redes sem fio, um horizonte maior se abre para o desenvolvimento de novas aplicações comerciais baseadas nas Manets. Porém, para atingir esses objetivos é necessário reinventar a Manet para trabalhar com o protocolo IPv6. Segundo Jayanthi, Rabara e Akokiaraj (2010) [21], os benefícios proporcionados pelo IPv6 nas Manets começam com: o aumento do espaço de endereçamento, unicidade de endereços, esquema hierárquico de endereçamento e alcance global. Acrescenta-se, ainda, a melhora nos protocolos de mobilidade e roteamento, possibilitando comunicação fim a fim de qualidade. Novos serviços poderão ser suportados com a integração dos serviços de rede *multicast* e *anycast*, aumentando a escalabilidade da rede.

5 Considerações finais

O presente trabalho apresentou um estudo sobre o endereçamento IP em Manets. Os conceitos, mecanismos e protocolos aqui apresentados têm como objetivo fornecer uma visão geral da tecnologia de autoendereçamento necessária para as Manets. O estudo mostra que o problema de endereçamento em Manets é ainda um tópico em aberto, e que os novos padrões e tecnologias de redes sem fio não foram completamente explorados. Deve-se atentar que grande parte dos resultados dos trabalhos apresentados é fruto de simulações e pode não apresentar o mesmo desempenho quando implementada na prática. O motivo principal é a falta de modelos de propagação mais próximos às condições reais do ambiente em que as aplicações serão usadas. A grande maioria das simulações é realizada usando o modelo de propagação espaço livre. O desenvolvimento de modelos mais realistas certamente proporcionará o desenvolvimento de soluções robustas e confiáveis.

Agradecimentos

Este trabalho foi parcialmente financiado pelo projeto Infraestrutura Móvel Inteligente baseada em Redes Celulares e Veiculares, da Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (Faperj), pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes). Foi também apoiado pela Fundação de Amparo ao Desenvolvimento das Ações Científicas e Tecnológicas e à Pesquisa do Estado de Rondônia (Fapero).

Referências

[1] TAGHILOO, M. et al. New approach for address auto-configuration in manet based on virtual address space mapping (vasm). In: INFORMATION AND COMMUNICATION TECHNOLOGIES: FROM THEORY TO APPLICATIONS, 3, 2008. Damascus, Syria: Proceedings of 3rd Information and Communication Technology Agency, 2008. p. 1–6.

[2] CORMIO, C. et al. A multi-channel multi-interface mac for collision-free communication in wireless ad hoc networks. In: EUROPEAN WIRELESS CONFERENCE, 2010 . Lucca, Italy: Proceedings of IEEE European Wireless Conference, 2010. p. 306–313.

[3] PERKINS, C. E. et al. *IP Address Autoconfiguration for Ad Hoc Networks*. 2001. Disponível em: <https://tools.ietf.org/html/draft-perkins-manet-autoconf-01>. Acesso em: 25 set. 2015.

[4] HUQ, S. Z. U. et al. Study of detection of ip address conflicts in manets. GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, Global Journals Inc. (US), Delaware, USA, v. 10, n. 1, p. 23–26, 4 2010.

[5] SANG-CHUL, K.; JONG-MOON, C. Message complexity analysis of mobile ad hoc network address autoconfiguration protocols. IEEE TRANSACTIONS ON MOBILE COMPUTING, Institute of Electrical and Electronics Engineers, Davis, USA, v. 7, n. 3, p. 358–371, March 2008. ISSN 1536-1233.

[6] VAIDYA, N. H. Weak duplicate address detection in mobile ad hoc networks. In: ACM INTERNATIONAL SYMPOSIUM ON MOBILE AD HOC NETWORKING & COMPUTING, 3, 2002. Lausanne, Switzerland: Proceedings of the 3rd Mobile Ad hoc Networking and Computing, 2002. p. 206–216. ISBN 1-58113-501-7.

[7] JACQUET, P. et al. *Optimized Link State Routing Protocol for Ad Hoc Networks*. 2001. 62–68 p. Inria, Rocquencourt, France: Hypercom Project, 2001. p. 62-68.

[8] WENIGER, K. Passive duplicate address detection in mobile ad hoc networks. In: IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE, 2003. New Orleans, LA, USA: Proceedings of WCNC, 2003. v. 3, p. 1504–1509 vol.3. ISSN 1525-3511.

[9] WENIGER, K. Pacman: passive autoconfiguration for mobile ad hoc networks. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Institute of Electrical and Electronics Engineers, Davis, USA, v. 23, n. 3, p. 507–519, 2005. ISSN 0733-8716.

[10] VILLALBA, G. L. J. et al. Auto-configuration protocols in mobile ad hoc networks. SENSORS OPEN ACCESS JOURNAL, Basel, Switzerland, v. 11, n. 4, p. 3652–3666, 2011. ISSN 1424-8220.

[11] ROHIT, R.; SINGH, D. A study of various addres allocation schemes for mobile ad hoc networks. INTERNATIONAL JOURNAL OF EMERGING TRENDS AND TECHNOLOGY IN COMPUTER SCIENCE, India, v. 3, n. 1, p. 100, 2014.

[12] OROZCO, S. A. L. et al. Security issues in mobile ad hoc networks. INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS, v. 2012, n. 818054, p. 6, March 2012.

[13] LI, L. et al. Agent-based passive autoconfiguration for large scale manets. WIRELESS PERSONAL COMMUNICATIONS, Springer, New York, USA, v. 43, n. 4, p. 1741–1749, 2007. ISSN 0929-6212.

[14] NESARGI, S.; PRAKASH, R. Manetconf: configuration of hosts in a mobile ad hoc network. In: INFOCOM 2002 - ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES, 21, 2002. [S.l.]: Proceedings of IEEE International Conference on Computer Communications, 2002. v. 2, p. 1059–1068 vol.2. ISSN 0743-166X.

[15] CHU, X.; LIU, J.; SUN, Y. Address allocation mechanisms for mobile ad hoc networks. In: MISRA, S.; WOUNGANG, I.; MISRA, S. C. (Ed.). *Guide to Wireless Ad Hoc Networks*. London: Springer London, 2009, (Computer Communications and Networks). p. 333–354. ISBN 978-1-84800-327-9.

[16] ZHOU, H.; NI, L.; MUTKA, M. Prophet address allocation for large scale manets. In: INFOCOM - ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS, 22, 2003. [S.l.]: Proceedings of IEEE International Conference on Computer Communications, 2003. v. 2, p. 1304–1311 vol.2. ISSN 0743-166X.

[17] CHEN, Y.; FLEURY, E.; RAZAFINDRALAMBO, T. Scalable address allocation protocol for mobile ad hoc networks. In: INTERNATIONAL CONFERENCE ON MOBILE AD-HOC AND SENSOR NETWORKS, 5, 2009. Fujian, China: Proceedings of IEEE Mobile ad-hoc and Sensors Networks Conference, 2009. p. 41–48.

[18] WANG, X.; QIAN, H. Dynamic and hierarchical ipv6 address configuration for a mobile ad hoc network. *International Journal of Communication Systems*, John Wiley & Sons, New Jersey, USA, v. 28, n. 1, p. 127–146, 2015. ISSN 1099-1131.

[19] THOMSON, S.; NARTEN, T.; JINMEI, T. *IPv6 Stateless Address Autoconfiguration*. 2007. Disponível em: <https://tools.ietf.org/pdf/rfc4862.pdf>. Acesso em: 11 set. 2015. RFC 4862.

[20] GRAJZER, M.; ZERNICKI, T.; GLABOWSKI, M. Nd++ an extended ipv6 neighbor discovery protocol for enhanced stateless address autoconfiguration in manets. *International Journal of Communication Systems*, John Wiley & Sons, New Jersey, USA, v. 27, n. 10, p. 2269–2288, 2014. ISSN 1099-1131.

[21] JAYANTHI, J. G.; RABARA, S.; AROKIARAJ, A. M. Ipv6 manet: An essential technology for future pervasive computing. In: INTERNATIONAL CONFERENCE ON COMMUNICATION SOFTWARE AND NETWORKS, 2, 2010. Singapore: Proceedings of IEEEE Communications Software an Networks Conference, 2010. p. 466–470.