# Protocolo de Roteamento
# AODV (Ad-hoc On-demand Distance Vector)

**Gabriel L. S. Araujo, Victor H. G. Pinheiro, Diogo H. S. Sobrinho,**
**Carlos A. S. Andrade, Luiz H. S. Santos**

Instituto de Tecnologia – Universidade Federal do Pará (UFPA)
Caixa Postal 479 – 66.075-110 – Belém – PA – Brasil
gabriellucas71@gmail.com, victor.cavzod@hotmail.com, casdea@gmail.com,
dio henriques@hotmail.com, 1007luiz@hotmail.com

***Abstract.*** *The article describes the route algorithm Ad Hoc On-Demand distance Vector (AODV), a router algorithm dynamic for mobile networks, will be show your way to operate, messages formats that make part of AODV, the AODV and aggregated networks and the security for this type of network. And important characteristics about AODV, for the reader conclude the viability e the utility of the algorithm.*

***Resumo.*** *O artigo descreve o algoritmo de roteamento Ad Hoc On-Demand Distance Vector (AODV), um algoritmo de roteamento dinâmico para redes móveis, será apresentado seu modo operante, formato das mensagens que fazem parte do AODV, o AODV e redes agregadas e a segurança para este tipo de rede. E características importantes sobre o AODV, para o leitor concluir a viabilidade e a utilidade do algoritmo.*

## 1.Introdução

O Ad hoc On-Demand Distance Vector (AODV) possibilita um roteamento dinâmico, auto iniciativo e multihop entre dois nós que solicitam estabelecer uma rede adhoc. O AODV permite que os nós obtenham rotas rápidas para novos destinos, e não requer nós que serviriam de rota para destinos que não estão em comunicação. O AODV também permite os nós agirem em tempo hábil em situações onde ocorre a quebra de um link ou uma mudança na topologia da internet. Por exemplo, quando ocorre a queda de um link, os nós afetados são capazes de invalidar rotas de comunicação, graças as notificações do AODV.

Uma característica distintiva do AODV é o uso de um número da sequência de destinos para cada entrada de rota. O número de sequência dos destinatários é criado pelo destinatário para ser incluído junto de qualquer informação de rota enviada aos nós que as requisitam. A organização feita pelo número de sequência dos destinatários permite uma simplicidade maior na operação e uma liberdade de loop. Por exemplo, diante duas rotas para um destino, o nó solicitante terá de escolher a com o maior número da sequência.

## 2.Características Gerais

Requisições de rotas (RREQs), Requisições de respostas (RREPs) e Erros de rota (RERRs), são tipos de mensagens definidas pelo AODV. Tais mensagens são recebidas via UDP. Se espera que o nó solicitante utilize o seu endereço IP como remetente das mensagens. Para a transmissão de mensagens, será utilizado o IP limitado (255.255.255.255), isso significa que tais mensagens não são enviadas às cegas. Entretanto, as operações do AODV requerem certas mensagens (exemplo: RREQ), para serem disseminadas através da rede ad hoc. O alcance de tais RREQ é indicado pelo TTL (Tempo de...), localizados no cabeçalho do IP.

Enquanto os extremos da rota a ser comunicada possuírem rotas validas, o AODV não desempenha nenhuma tarefa. Quando é necessária uma rota para um destino novo, o nó transmite uma mensagem RREQ afim de encontrar tal rota. A rota é determinada quando o RREQ alcança seu destino ou um nó intermediário uma rota "suficientemente nova" para o destino. Uma rota "suficientemente nova" é uma entrada de rota valida paro destino, no qual o número de sequência associado é maior do que o contido no RREQ. A rota se torna disponível quando a origem recebe uma transmissão RREP de volta para a origem do RREQ.

Os nós monitoram o status do link dos próximos hops em rotas ativas. Quando uma quebra do link em uma rota ativa é detectada, uma mensagem RERR notifica outros nós que uma quebra ocorreu. A mensagem RERR indica os destinos (possivelmente sub redes) inalcançáveis devido à quebra do link.

Visando ativar esse feedback de erros, cada nó possui uma "precursor list", contendo o endereço IP de cada vizinho que provavelmente será usado como hop. O conteúdo de uma "precursor list" é adquirido durante o processo gerador de uma mensagem RREP, que por definição, deverá ser enviada à um nó definido na própria "precursor list". Se a RREP tem um prefixo de comprimento diferente de 0, o remetente da RREQ, que solicitou a RREP, está incluído entre os precursores da rota para a sub rede

O AODV é um protocolo de roteamento que lida com a administração de tabelas de rotas. As informações contidas nessas tabelas devem abranger até mesmo rotas de vida curta, tais como as criadas para armazenar temporariamente os caminhos em direção reversa aos nós que originaram RREQs. Comumente são utilizados os seguintes campos para cada entrada na tabela de rotas:

- Endereço de IP destino.
- Número da sequência de destinos
- Estado da rota (Válida, inválida, necessita reparos, em reparação)
- Interface de rede
- Hop counts (número de hops (saltos) necessários para alcançar cada destino)
- Lifetime (Tempo de expiração da rota)

Gerenciar o número de sequência é crucial para evitar loops de roteamento, mesmo quando ocorre uma quebra de link e o nó se torna inalcançável para fornecer a sua informação sobre o número de sequência. Quando ocorre alguma das situações de quebra ou desativação de um link e o destino se torna inalcançável, o número de sequência dessa rota se torna indisponível para o manuseio e a sua entrada na tabela é marcada como inválida.

## 3.Terminologia

O protocolo utiliza especificações para palavras maiúsculas com significados convencionais como, MUST, SHOULD, etc., para indicar níveis de solicitações em vários de seus recursos.

Active ou Valid route: Uma rota em direção ao destino que possui uma tabela de entradas de roteamentos marcada como válida. Apenas active routes podem ser usadas para encaminhar pacotes de dados.

Broadcast: Transmite para o IP de transmissão limitado, 255.255.255.255. Um pacote de broadcast pode não ser encaminhado "cegamente", mas é útil para disseminação de mensagens do AODV para a rede ad hoc.

Destination node (nó): Endereço IP no qual os pacotes de dados serão enviados. Os nós de destino e origem são capazes de se identificar em uma transição de dados quando o seu endereço foi gravado no cabeçalho do endereço IP. As rotas para os nós de destino são fornecidas graças ao protocolo AODV, que leva o endereço IP do nó de destino desejado em mensagens RREQ e RREP.

Forwarding node (encaminhamento): Nó que encaminha pacotes destinados a outro nó, retransmitindo-os para um próximo hop que está mais perto do destino unicast ao longo de um caminho que já foi especificado usando mensagens de controle.

Forward route: Uma rota configurada para o envio de pacotes de dados de um nó que origina uma operação de descobrimento de rota em direção ao destino desejado para os pacotes.

Invalid route: Rota expirada que foi definida em um status de invalidez em sua entrada na tabela de roteamento. É usada para armazenar informações de rotas validas por um período de tempo estendido. Este tipo de rota não pode ser usada para encaminhar pacotes, mas pode prover informações uteis para reparações de rotas e para futuras mensagens RREQ.

Originating node: Inicia uma mensagem de descobrimento de rota AODV (RREQ) para ser processada e possivelmente retransmitida por outros nós dentro da rede ad hoc.

Reverse route: Rota configurada para encaminhar um pacote reply (RREP) emitido do destino ou de um nó intermediário, para a origem.

Número de sequência: Um algarismo crescente mantido por nós de origem. Contido nas mensagens do protocolo de roteamento, é usado por outros nós para determinar quão nova é a informação enviada.

## 4.Aplicabilidade

O protocolo AODV é projetado para redes com milhares de nós móveis, podendo assim gerenciar taxas de mobilidades baixas, moderadas e altas assim como uma variedade de níveis de trafego de dados. AODV é utilizado para o uso em redes onde os nós podem "confiar" uns aos outros, seja por uso de chaves pré-configuradas ou porque sabe-se que não há nós maliciosos intrusos. AODV objetiva reduzir a disseminação do trafego de controle e eliminar sobrecargas em trafego de dados, otimizando a performance da rede.

## 5.Formato de mensagens

### 5.1 - Route request (RREQ):

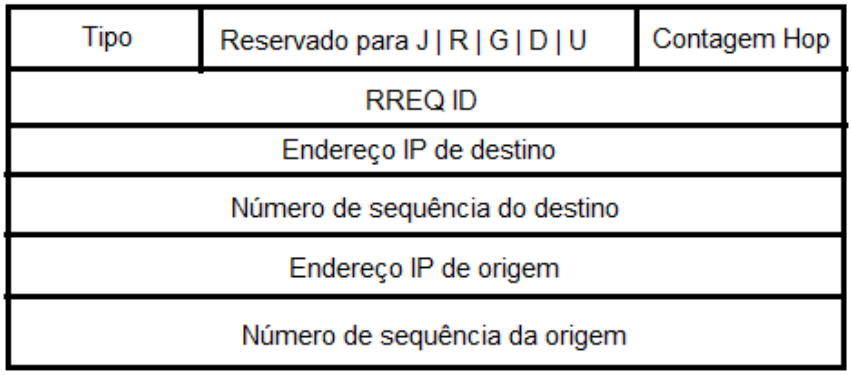


**Fig. 1 – Formato da mensagem RREQ.**

J: Join flag R: Repair flag

G: Gratuitous RREP flag; indica quando uma RREP deve ser transmitida para o nó especificado no campo "Endereço IP de destino".

D: Destination only flag; indica que apenas o destino deve responder a RREQ.

U: Unknown sequence number; indica que o número de sequência do destino é desconhecido.

Nulo: Se o campo conter um 0 ou estiver em branco, sua recepção deverá ser ignorada.

Hop count: Número de hops entre a origem e o nó solicitante.

RREQ ID: Número de sequência único capaz de identificar a RREQ quando enviada em conjunto do endereço IP.

Endereço IP de destino. Número de sequência do destino.

Endereço IP de origem. Número de sequência da origem.

### 5.2 - Route reply (RREP):

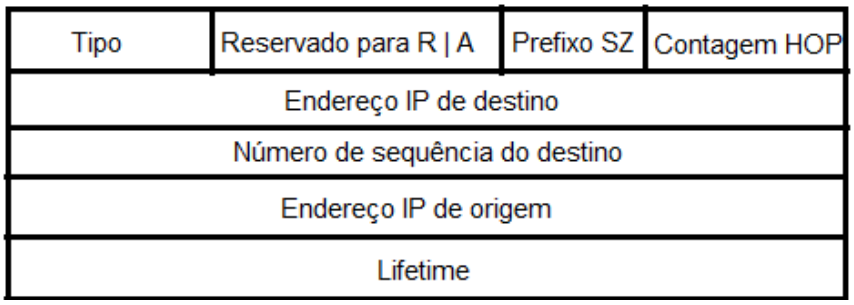


**Fig. 2 – Formato da mensagem RREP.**

R: Repair flag. A: Requer reconhecimento.

Nulo: Se o campo conter um 0 ou estiver em branco, sua recepção deverá ser ignorada.

Prefix SZ (Size, tamanho): Prefixo de 5 bits de tamanho, determina que o próximo hop indicado pode ser usado para qualquer nó com o mesmo prefixo de roteamento.

Hop count: Número de hops entre a origem e o nó solicitante.

Endereço IP de destino. Número de sequência do destino.

Endereço IP de origem.

Lifetime: Tempo em ms no qual cada nó receptor da RREP considera a rota, válida.

O Prefix size permite que um roteador de uma subrede forneça uma rota para cada host na subrede, tal rota definida pelo prefixo de roteamento e pelo Prefix size. Para ativar esta funcionalidade, o rotador da subrede deve garantir alcance para todos os hosts que a compartilham. Quando o prefixo é não nulo, qualquer informação de roteamento ou precursor data 'MUST', ser contido de acordo com a rota da subrede, e não ao endereço de IP do destino em si.

O Bit 'A' é usado qual o link no qual a mensagem RREP é enviada está instável ou unidirecional. Quando uma mensagem RREP contém o bit 'A' setado, o receptor de tal mensagem deve retornar uma mensagem RREP-ACK.

### 5.3 - Route error (RERR):

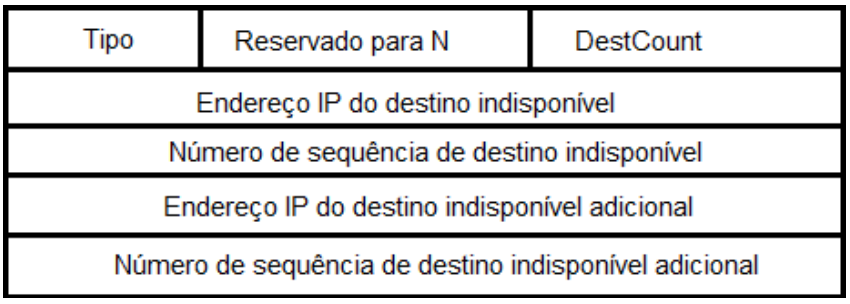


**Fig. 3 – Formato da mensagem RERR.**

N: No delete flag, presente quando um nó realizou um reparo local do link e nós posteriores não devem excluir tal link.

Nulo: Se o campo conter um 0 ou estiver em branco, sua recepção deverá ser ignorada.

DestCount: Número de destinos indisponíveis incluídos na mensagem

Endereço de IP indisponível: IP do destino que se tornou indisponível devido à quebra de link

Número de sequência do destino indisponível: Número de sequência do destino indisponível.

A mensagem RERR é enviada quando uma quebra de link torna indisponível um ou mais destinos para alguns vizinhos do nó.

### 5.4 - Route reply acknowledgment (RREP-ACK):

RREP-ACK é uma mensagem que DEVE, ser enviada em resposta a uma mensagem RREP setada com o bit 'A'. Isto é feito quando existem links unidirecionais que possam impedir a realização de um ciclo de descoberta de rota.


**Fig. 4 – Formato da mensagem RREP-ACK.**

Nulo: Se o campo conter um 0 ou estiver em branco, sua recepção deverá ser ignorada.

## 6. Operação

O AODV, quando comparado com algoritmos clássicos de roteamento como vetor de distâncias e *link state*, apresenta uma grande redução no número de mensagens de roteamento na rede. Isto é devido à sua abordagem reativa. A forma de funcionamento do AODV é semelhante a de algoritmos tradicionais, o que pode facilitar no caso de uma possível interconexão da rede ad hoc a uma rede fixa. Mesmo funcionando de forma semelhante aos algoritmos tradicionais, o AODV pode suportar tráfego *multicast* e *unicast*. Este protocolo procura uma solução intermediária entre o roteamento reativo e o pró-ativo.

No primeiro a latência é grande, já que é necessário esperar o tempo de resposta da requisição de rotas. No segundo, o volume de informações trocadas torna a abordagem proibitiva para redes ad hoc.

O AODV apresenta apenas uma rota para cada destino, o que pode não ser uma boa característica. Felizmente o protocolo pode ser facilmente alterado para garantir o suporte a várias rotas para um mesmo destino.

O desempenho do AODV é tão bom quanto o DSR para todas as taxas de movimentação e velocidades testadas, conseguindo também alcançar a sua meta de eliminar a sobrecarga causada pelos algoritmos *source routing*. No entanto, para isto ele causa uma sobrecarga na rede com pacotes de roteamento, e gerando um custo maior que o DSR para altas taxas de mobilidade.

## 6.1 – Variáveis

• Número de sequência da fonte (SrcSeqNum): número de sequência gerado pelo nó fonte.

• Número de sequência do destino (DestSeqNum): número de sequência crescente usado como forma de se verificar o quão recente é uma rota, pois o DestSeqNum com o maior valor é que representará a rota mais atual.

• Identificador fonte (SrcID): especifica o nó fonte que pretende enviar pacotes a um determinado nó da rede; • Identificador do destino (DestID): especifica o nó destino que deverá receber pacotes de um determinado nó fonte.

• Identificador de broadcast (BcastID): quando vários broadcasts são enviados à rede, cada um recebe um identificador que é relacionado a uma determinada mensagem RREQ, podendo assim identificá-la. É incrementado a cada nova requisição de rota enviada.

• Tempo de vida das mensagens (TTL): contador que representa o tempo que se considera até que uma mensagem possa ser descartada; • Número de hops: número de saltos necessários para se alcançar um determinado nó a partir de um nó origem**.**

## 6.2 - Mensagens

•HELLO: enviadas periodicamente para se confirmar a conectividade local entre vizinhos.

• RREQ: mensagens de requisição de rota enviadas a toda a rede para encontrar o nó destino, quando a rota já não é conhecida.

• Route Reply (RREP): resposta à requisição de rota especificando como chegar até o nó destino.

• Route Error (RERR): aviso de queda de enlace. Quando um enlace deixa de existir entre dois nós é enviado uma RERR.

## 6.3 – Princípios de Operação

Quando um nó quer enviar um pacote a outro nó e ainda não possui uma rota determinada, o nó fonte envia um RouteRequest (contendo SrcID, DestID, SrcSeqNum, DestSeqNum, BcastID e TTL a todos os seus vizinhos por difusão. Caso um vizinho não seja o destino ou não possua uma rota válida para o destino, ele repassa a RREQ aos seus vizinhos . Este processo se repete até a requisição atingir o destino ou um nó que conheça uma rota para este, inundando a rede.

Um nó de destino, ao responder a RREQ, envia pelo caminho reverso uma mensagem RREP, que contém o endereço da fonte e do destino, o número de sequência do destino, o contador de saltos (incrementado de uma unidade a cada salto) e seu TTL.

Antes de enviar a RREP, o nó de destino atualiza o seu número de sequência para o máximo entre o valor atual e o valor que constava na RREQ. Em cada nó atravessado no caminho reverso pela RREP é armazenado, em uma entrada referente ao destino, o próximo salto para alcançar o destino, ou seja, o endereço do vizinho de quem se recebeu a resposta e o número de sequência do destino.

A movimentação de um nó ativo pode provocar a queda de um dado enlace que estava sendo utilizado. Nesta situação uma mensagem de erro (RERR) é enviada a todos os nós afetados, avisando sobre a queda do enlace. Dessa forma, cada nó por onde passa a RERR deve decidir se continua ou não a repassar esta mensagem, além de ter que atualizar a sua tabela de roteamento, registrando que os destinos especificados na mensagem estão inalcançáveis e atualizando seus números de sequência.

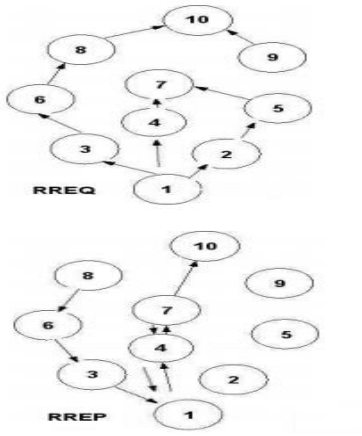


**Fig. 5 - Mensagens RREQ e RREP no AODV.**

A Figura 6.1 ilustra as mensagens RREQ e RREP do AODV na rede. O broadcast de RREQ se inicia com o nó 1 enviando RREQ aos nós 2, 3 e 4, que por sua vez verificam se possuem a rota até o nó destino 10. Caso não possuam, eles enviam RREQ aos seus vizinhos diretamente conectados. Os nós 5, 6 e 7 são os vizinhos de 2, 3 e 4 respectivamente. Como o nó 7 possui uma rota até o nó destino 10, então ele envia uma RREP até o nó fonte. Caso outro nó possuísse também uma rota até o nó 10, este nó responderia com uma RREP ao nó fonte. Como, por exemplo, o nó 8.

## 7. AODV e a Rede Agregada

### 7.1 - Utilização

O protocolo AODV foi projetado para ser utilizado em nós móveis com endereços IP que não estejam relacionados com os de outros nós, pois é baseado no uso em redes Ad Hoc. Porém, em alguns casos é necessário que haja uma relação entre alguns nós, situados em uma sub-rede, para que eles possam se mover em conjunto dentro de uma área limitada.

Um nó móvel é qualquer dispositivo que está conectado a internet, recebendo e transferindo dados por meio de ondas de rádio, portanto, conferindo-lhe o termo móvel, tendo a sua posição não-fixa, por exemplo, telefone celular, rede local Wi-Fi, comunicação por satélite. Por isso foi necessário a criação de protocolos que pudessem lidar com estes tipos de nós, que não possuem um local fixo.

### 7.2 - Aplicações em Redes Ad Hoc

A rede Ad Hoc, é uma rede que não necessita de uma infraestrutura de conexão física, ela utiliza **algoritmo de inundação** para a transmissão de dados, no qual do nó de origem é transmitido uma mensagem para nós vizinhos e os nós vizinhos transmitem também uma mensagem, exceto de volta para o nó de origem, repetindo o processo até certo limite de saltos, para que não ocorra loop infinito.

Ad hoc On-demand Distance Vector, é o protocolo de roteamento Reativo do tipo Vetor Distância utilizado em rede Ad Hoc. Este protocolo somente determina uma rota se caso for necessário a troca de dados entre nós, formando uma rota por meio de inundação da rede, depois de estabelecido uma rota que conecta os nós extremos para o fluxo de dados, esta é mantida até que seja necessário uma nova rota.

A necessidade de uma nova rota pode ser preciso, pois ocorreu erro de transmissão de dados, desconexão de algum nó intermediário ou o tempo do TTL (Time-To-Live, tempo em que a rota é mantida) expirou e foi requisitado outro envio ou recebimento de novos pacotes de antigos relacionamentos entre nós.

### 7.3 - Vantagens e Desvantagens do Algoritmo de Inundação (Broadcast) em AODV

A utilização de um algoritmo de inundação em AODV tem a vantagem de transmitir pacotes reduzindo o tráfego na rede, pois só determina uma rota quando é necessária a ligação entre nós e o roteamento do vetor distância não requer muita memória.

Porém a desvantagem seria na demora em toda a vez que for feita uma ligação entre nós, o tempo de estabelecimento dessa conexão seria a causa do atraso, pois somente depois desse tempo, a rota estaria formada e liberada para transmissão de pacotes. Para aumentar o desempenho na rede AODV, é preciso que seja calculado o tempo do TTL para que o maior número possível de mensagens seja transmitido através da rota formada, mas não gerando conflito com o tempo TTL desperdiçado, em que a rota não possui nenhuma transmissão de pacotes. Ou seja, o tempo TTL tem que ser aproximadamente igual ao tempo de uso para a transmissão completa de pacotes entre os nós conectados e o tamanho do pacote a ser enviado. Por isso, utiliza-se a reciclagem de algumas rotas mais requisitadas, para que esse tempo de descobrimento de rotas não atrase o tempo de transferência de pacotes.

### 7.4 - Exemplo de pesquisa de melhoria para AODV

Abaixo há alguns gráficos mostrando os resultados relacionados a uma pesquisa envolvendo o método VTOA (Variable Time Out Assignment), que significa esperar os valores das rotas, para identificar os tamanhos e atribuir um tempo adequado de permanência daquela rota. Ou seja, quanto maior a rota, provavelmente maior a ocorrência de erro, então maior terá de ser o seu tempo de mantimento de rota.

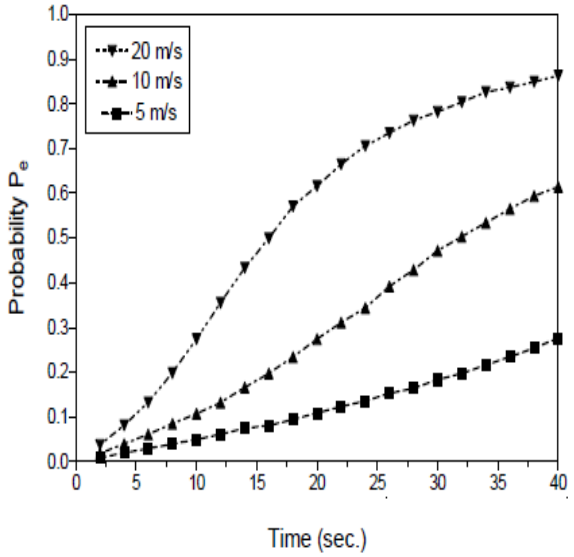


**Fig. 6 – Cálculo da probabilidade de erro para diferentes tipos de rotas contabilizando o tempo.**

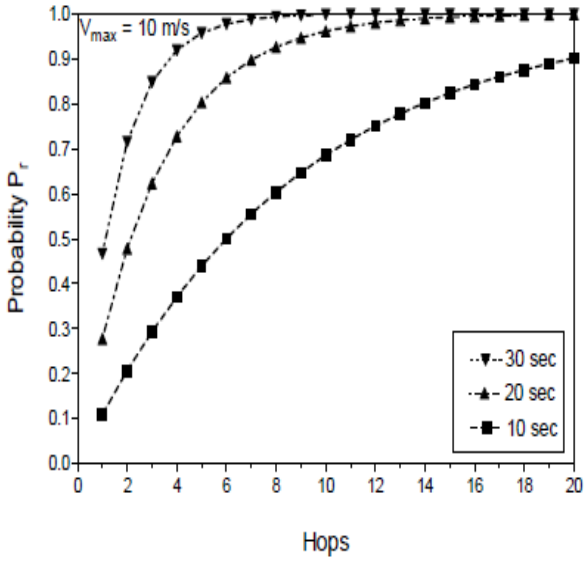


**Fig.7 – Cálculo da probabilidade de erro para diferentes tipos de rotas contabilizando o números de saltos.**

Percebe-se que quanto mais enlaces uma rota possuir, maior o tempo de transporte, maior o número de saltos e maior a probabilidade de ocorrer um erro no envio dos pacotes. Portanto, os tempos de conexão da rota deve ser apropriado a cada rota.

O gráfico abaixo revela a mudança entre o AODV normal e o AODV aplicada o método VTOA, no qual podemos reparar que o AODV com VTOA possui uma menor sobrecarga de roteamento que o AODV padrão.

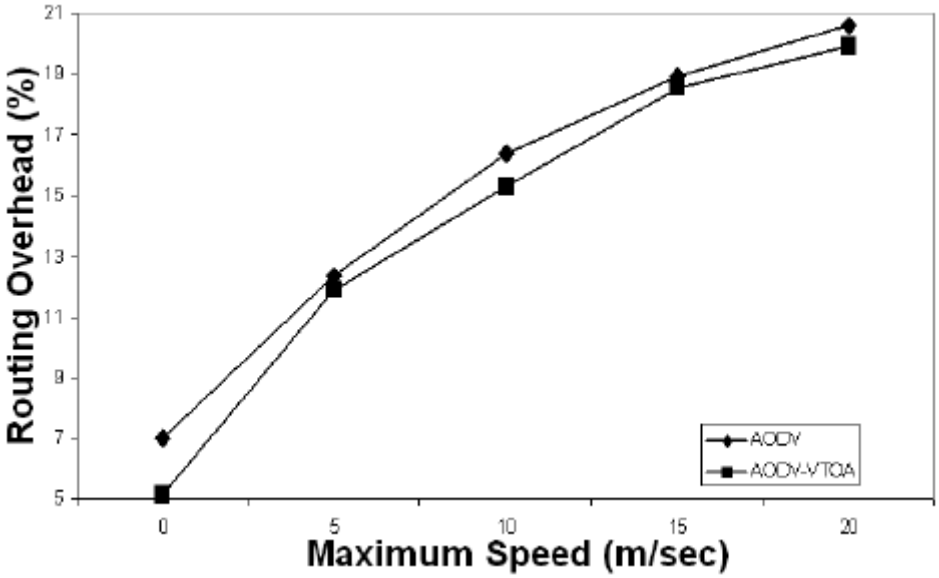


**Fig.8 – Diferença entre o AODV padrão e o AODV com VTOA.**

## 8.Segurança

O AODV é um dos mais populares algoritmos de roteamento para Redes MANETs (Mobile Ad Hoc Network) e redes de malha[6]. As MANETs, estão sendo desenvolvidas sem levar em conta a segurança[9]. Entretanto resguardar a segurança da transmissão não é o bastante se não for implementada uma segurança no roteamento[9]. Portanto em redes MANETs com necessidade de segurança, devem ser considerados dois sistemas de proteção: um para proteger a transmissão dos dados e outro para fazer um roteamento seguro[4]. Existem bons estudos de sobre sistemas de proteção sobre redes ponto a ponto. Mas não existem tantos trabalhos de como fazer descoberta de rotas com protocolos de roteamento de uma maneira segura.

As MANETs são vulneráveis a vários tipos de ataques, que são classificados como ataques ativos e passivos. Ataques ativos interferem no funcionamento da rede. Exemplos de ataques desse tipo são, BlackHole attack - um nó malicioso está presente na rede para atrair o tráfego para ele, provendo informações falsas sobre o caminho requisitado. O GrayHole é um ataque parecido, a diferença é que ele pode atacar qualquer nó, dentro do raio, por um período pequeno e não o tempo todo, assim sendo mais difícil de detectar[7].

Alguns métodos de segurança que podem ser utilizados serão mostrados abaixo, além deles, uma extensão do AODV que tem a intenção de prover mais segurança em relação ao AODV, esta extensão é chamada SAODV (Secure AODV).

### 8.1 - Chaves Simétricas

É de se esperar que todos se conheçam na rede para utilizar este método, por causa do modo com que ele é implementado. Nesse sistema todos que quiserem fazer parte da rede devem conhecer a chave. Se conhecendo não há problema de compartilharem a chave e transmitir dados pela rede, desse modo é de se esperar que ninguém faça nada que possa prejudicar os outros usuários da rede. Para utilizações militares este método pode ser útil[4].

### 8.2 - Chaves Assimétricas[9]

Agora, considere que nem todos se conheçam na rede, que é uma situação provável já que a rede é de nós móveis. Nesse método existem as chaves públicas e privadas. Todos os usuários tem as chaves públicas dos outros e cada um tem a sua chave privada. Desse modo, quando um arquivo for enviado, o usuário usa a chave pública do destinatário para criptografar o pacote, assim só que pode descriptografar o pacote é o detentor da chave privada. Esse método além de prover mais segurança permite a detecção de mensagens forjadas.

### 8.3 - Detecção de Mal Comportamento[9]

Este é um método com eficiência muito específica, já que ele funciona detectando grandes variações no tráfego da rede. Ataques como os citados anteriormente, são alvos deste método. É difícil garantir a integridade e autenticação das mensagens de roteamento. Por isso há controvérsias quanto ao seu uso.

### 8.4 - Secure AODV

O SAODV é uma extensão do AODV, que pode ser usada para proteger o mecanismo de descoberta de rota provendo ferramentas de segurança, como a manutenção da integridade do pacote, autenticação e confiabilidade. O SAODV assume que a rede tenha um sistema de chaves assimétricas adequado. Assim cada nó Ad Hoc é capaz de seguramente verificar a relação entre o endereço dado e a suas chaves. A função de gerenciar as chaves é do Administrador de Chaves.

Além disso, outros dois mecanismos são utilizados no SAODV são assinaturas digitais para proteger os campos não mutáveis e cadeias de Hash (#), para proteger a contagem dos campos que o único campo mutável e extremamente importante nas mensagens do AODV. A autenticação de informações imutáveis podem ser realizadas em uma transferência ponto-a-ponto, o que não pode ser feito com informações mutáveis. RERR, são protegidas de forma diferente, por causa da quantidade de informações mutáveis que há nela. portanto cada nó, gerando ou repassando informações, usa um mecanismo digital de autenticação para assinar toda a mensagem e qualquer nó vizinho que receba, é capaz de verificar a assinatura.

## 9.Conclusão

Todos os assuntos abordados neste trabalho tiveram o objetivo de mostrar o funcionamento padrão do protocolo AODV, como os seus objetivos nas redes Ad Hoc, o seu principio para o funcionamento como protocolo, o seu método de comunicação através de mensagens, as operações feitas com cada característica do protocolo, as formas como o protocolo descobre novas rotas e as mantém até serem atualizadas, e uma abordagem sobre a segurança neste protocolo. Este protocolo procura uma solução intermediária entre o roteamento reativo e o proativo. No primeiro a latência é grande, já que é necessário esperar o tempo de resposta da requisição de rotas. No segundo, o volume de informações trocadas torna a abordagem proibitiva para redes ad hoc. Portanto, percebe-se que o protocolo AODV é uma solução para muitos problemas que possuem falta de mobilidade e flexibilidade de conexão em uma estrutura de rede.

## 10.Referências


[1] C. Perkins (2003), "Ad hoc On-Demand Distance Vector (AODV) Routing – RFC3561", https://www.ietf.org/rfc/rfc3561.txt.

[2] LIU Jian, Changqiao Xu (2009), "An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks", Fifth International Conference on Information Assurance and Security.

[3] M. Rios, Senior Member, IEEE (2015), "Variable Route Expiration Time Based on a Fixed Probability of Failure for Ad-Hoc Networks Routing Applications", IEEE LATIN AMERICA TRANSACTIONS, VOL. 13, NO. 1, JAN. 2015.

[4] Guo-ping XU, Jian-hui LIU (2010), "Improvement of AODV Routing Protocol based on Wireless mesh networks", International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE).

[5] Emmanouil A. Panaousis, Christos Politis (2009), "A Game Theoretic Approach for Securing AODV in Emergency Mobile Ad Hoc Networks", The 9th IEEE International Workshop on Wireless Local Networks (WLN 2009), Zürich, Switzerland; 20-23 October 2009.

[6] Li, Qing. Zhao, Meiyuan. Walker, Jesse. Hu, Yih-Chun. Perrig, Adrian. Trappe, Wade. "SEAR: A Secure Efficient Ad Hoc On Demand Routing Protocol for Wireless Networks"

[7] Singh, Kuldeep. Rani, Sudesh (2014). "A Performance Study of Various Security Attacks on AODV Routing Protocol in MANET".

[8] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong. Song, Joo-Han. "Experimental Comparisons between SAODV and AODV Routing Protocols"

[9] Zapata, Manel Guerrero. "Secure Ad hoc On-Demand Distance Vector Routing"