Novas Tecnologias de Redes de Computadores

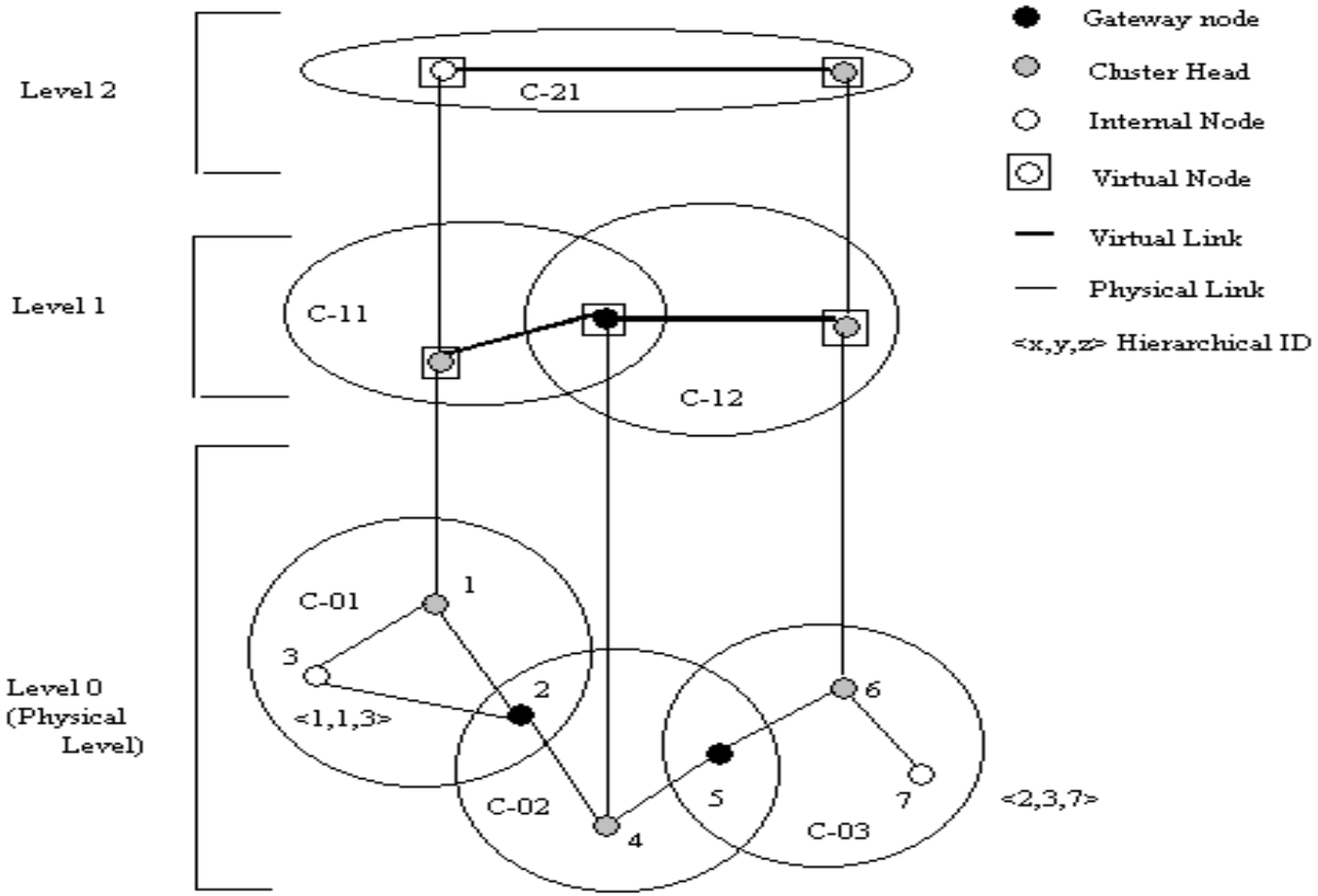
Ricardo José Cabeça de Souza
www.ricardojcsouza.com.br
rjcsouza@superig.com.br
2013

MANET (Mobile Ad Hoc Network)

Hierarchical State Routing (HSR)

- São atribuídas, geralmente, regras de roteamento diferenciadas para os nós da rede
- Princípio utilizado nesse tipo de protocolo pressupõe a organização dos nós em grupos, de acordo com suas características e demandas
- Estabelecimento de funcionalidades diferenciadas para os nós de dentro e de fora de cada grupo
- Tamanho dos pacotes de atualização de rotas tornam-se menores porque contêm informações somente sobre parte da rede, e não sobre toda a rede

Hierarchical State Routing (HSR)

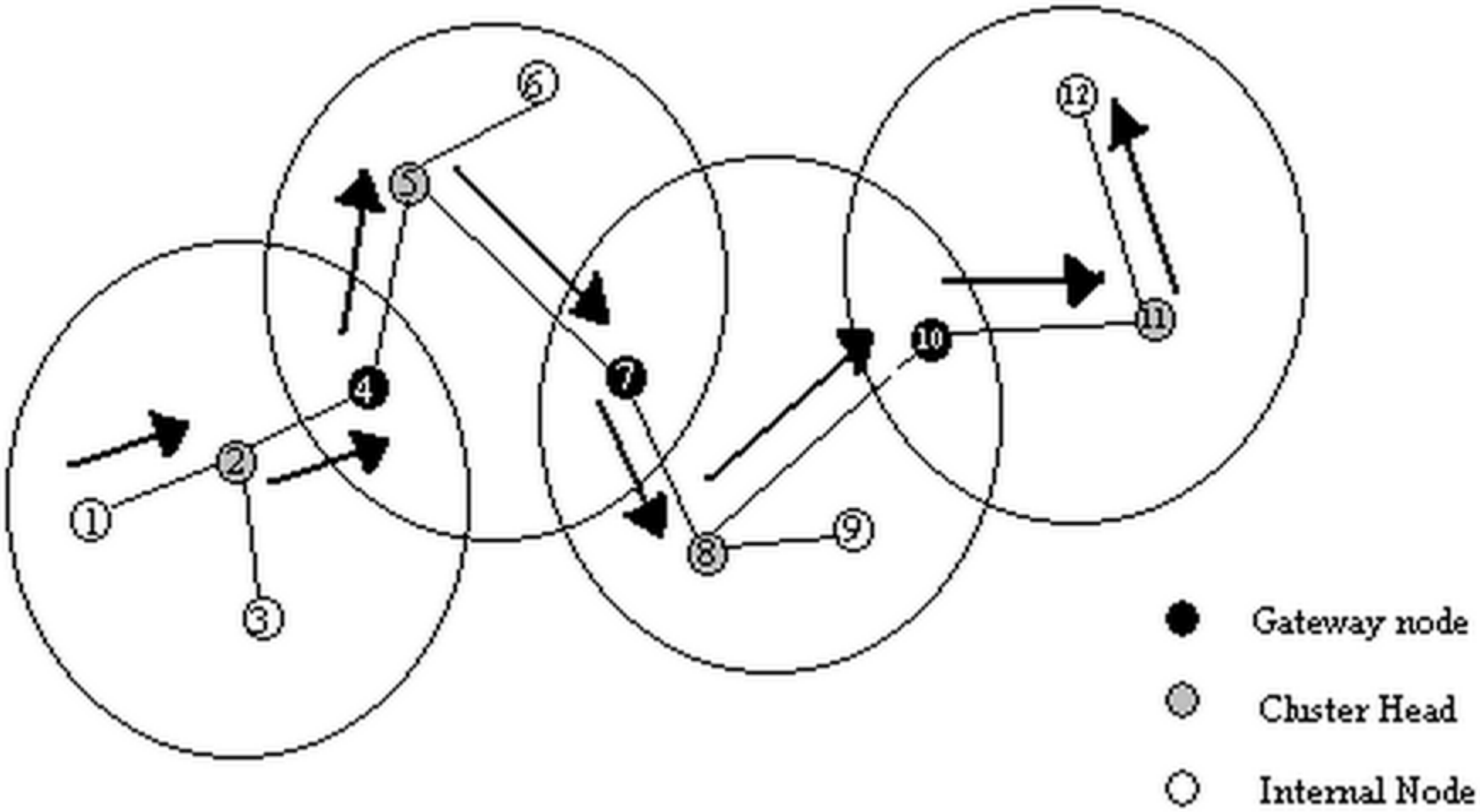


Fonte da Imagem: http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/fig2.gif

Clusterhead Gateway Switch Routing (CGSR)

- Os nós móveis são agregados em cluster
- É eleito um para representar a cabeça do cluster
- Todos os nós se comunicam com os demais através do nó cabeça do cluster
- Um cluster pode ter mais de uma cabeça

Clusterhead Gateway Switch Routing (CGSR)

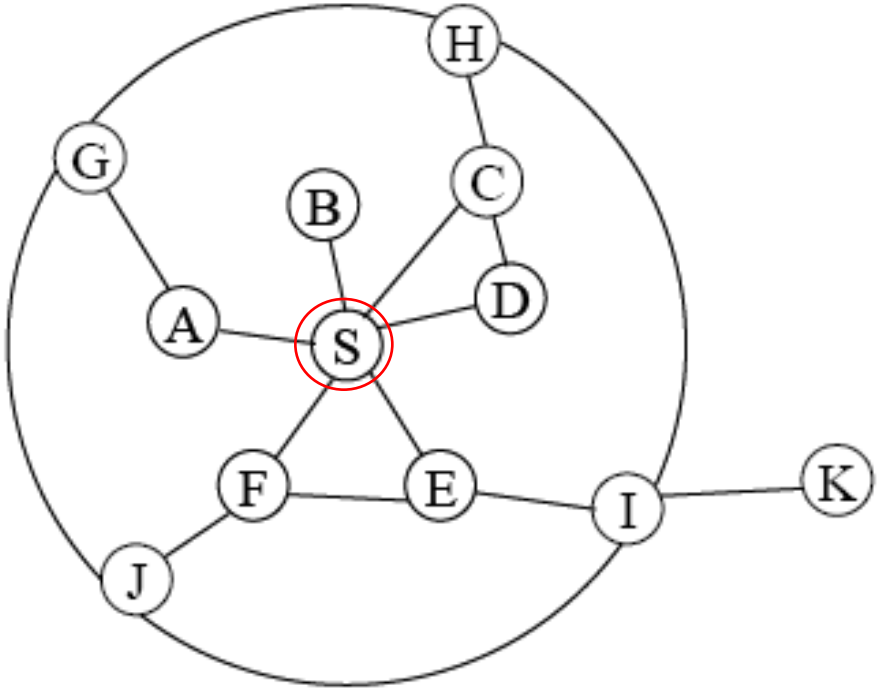


ZONE ROUTING PROTOCOL (ZRP)

- Protocolo híbrido → reativo/pró-ativo
- Cada nó define sua própria zona de roteamento conforme a distância dos nós
- Para o roteamento dentro desta zona, qualquer protocolo pode ser utilizado, inclusive LS ou DBF
- O nó mantém a informação completa de como encontrar os hosts dentro desta zona
- No roteamento entre zonas é utilizado on-demand routing

ZONE ROUTING PROTOCOL (ZRP)

- ROTEAMENTO
  - Zona é definida pelo número de hops (ρ)

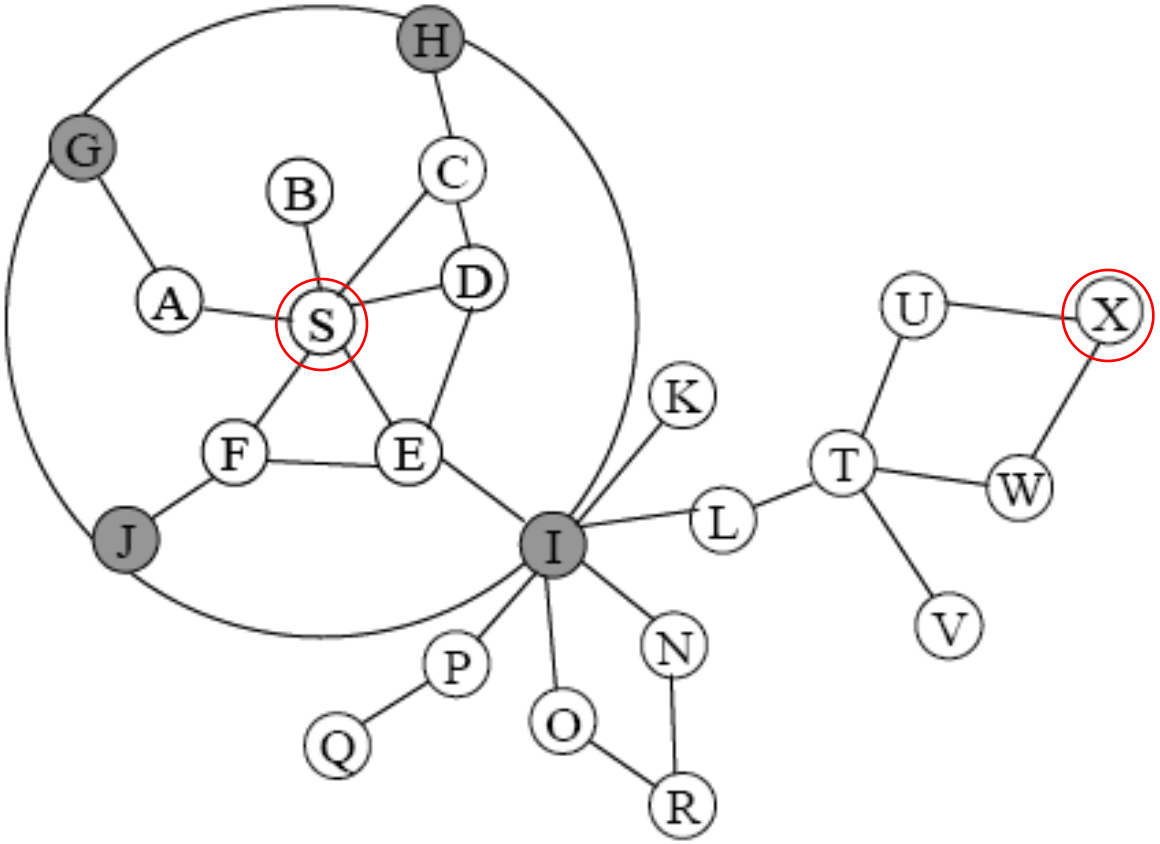


Ex: ρ = 2

ZONE ROUTING PROTOCOL (ZRP)

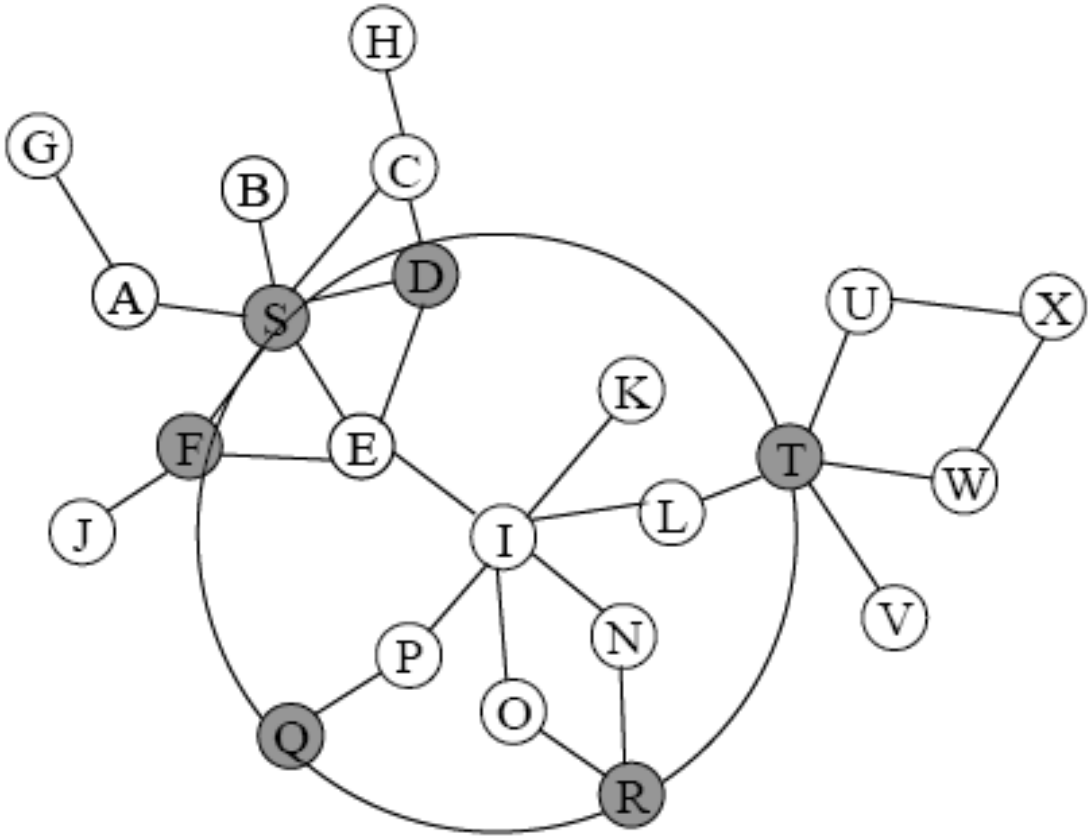
- ROTEAMENTO
  - Verifica onde se encontra o destino
    - Se dentro da zona envia diretamente
      - Usa **IntrA-zone Routing Protocol** (IARP) – Pró-ativo
      - Mantém informações de roteamento da zona
    - Se está fora, procura o caminho através de multicast para os nós da borda (utilizando o caminho mais curto dentro da zona)
      - Usa **IntEr-zone Routing Protocol** (IERP) – Reativo
      - Procura nova rota
    - Se o caminho é conhecido por algum host da borda, este responde com o caminho
    - Se não, faz o mesmo em sua própria borda

ZONE ROUTING PROTOCOL (ZRP)



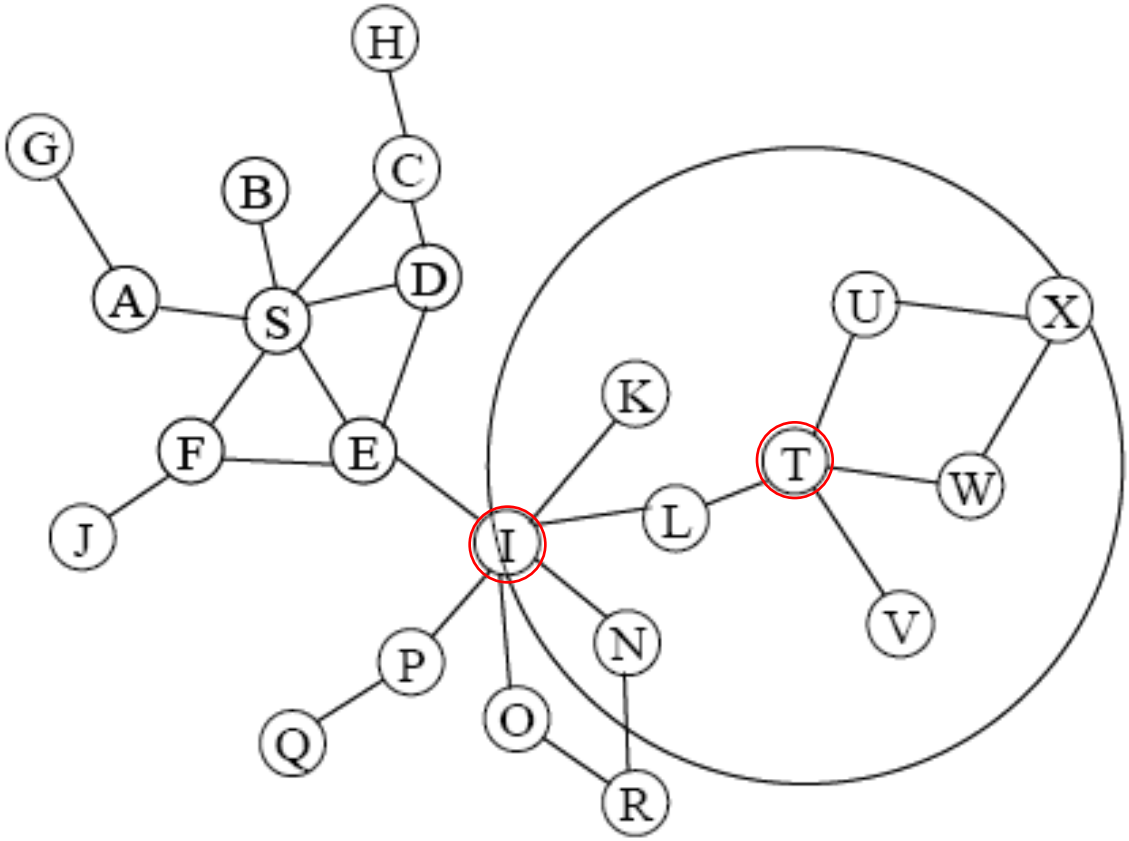
- S deseja enviar mensagem para X
-Verifica sua zona ρ = 2 (usa tabela IARP)
-Se não encontra, procura na borda (usa o IERP)
- I verifica sua zona
- Se não encontra, procura em sua borda

ZONE ROUTING PROTOCOL (ZRP)



- S deseja enviar mensagem para X
-Verifica sua zona ρ = 2 (usa tabela IARP)
-Se não encontra, procura na borda (usa o IERP)
- **I verifica sua zona**
- **Se não encontra, procura em sua borda**
- Se não encontra, procura em sua borda
- Finalmente, em **T** encontra o destino
-

ZONE ROUTING PROTOCOL (ZRP)

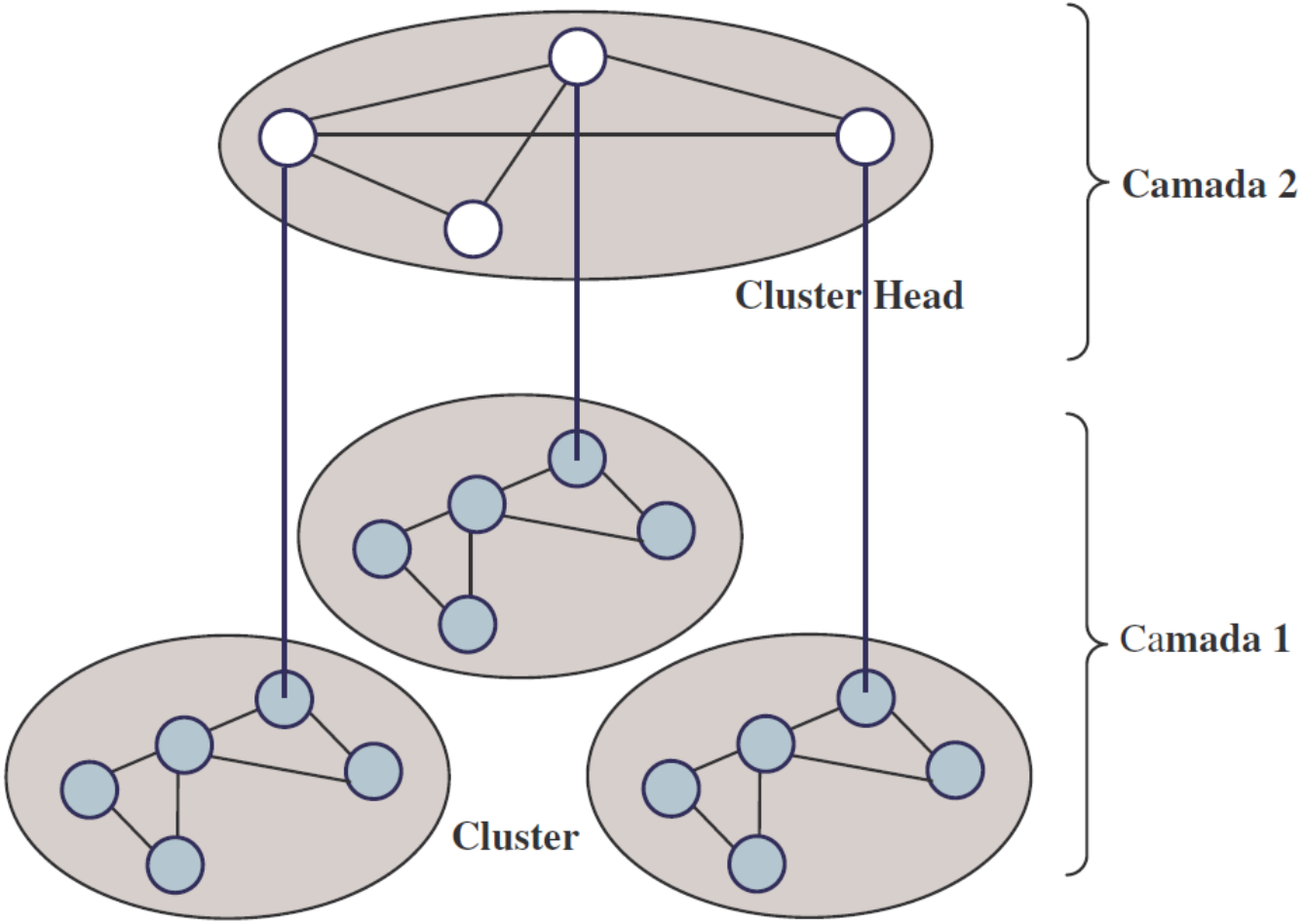


- S deseja enviar mensagem para X
-Verifica sua zona ρ = 2 (usa tabela IARP)
-Se não encontra, procura na borda (usa o IERP)
- I verifica sua zona
- Se não encontra, procura em sua borda
- **Se não encontra, procura em sua borda**
- Finalmente, em **T** encontra o destino
- **T atualiza sua tabela e encaminha o caminho para a origem (caminho reverso)**

Landmark Ad hoc Routing (LANMAR)

- Adota esquema para roteamento em redes Ad hoc, dividindo a rede em zonas (sub-redes lógicas) pré-definidas
- Cada zona contém um nó Baliza (Lanmark) pré-selecionado
- É assumido que todos os nós numa zona se movem em grupo e permanecem conectados entre si através do protocolo FSR

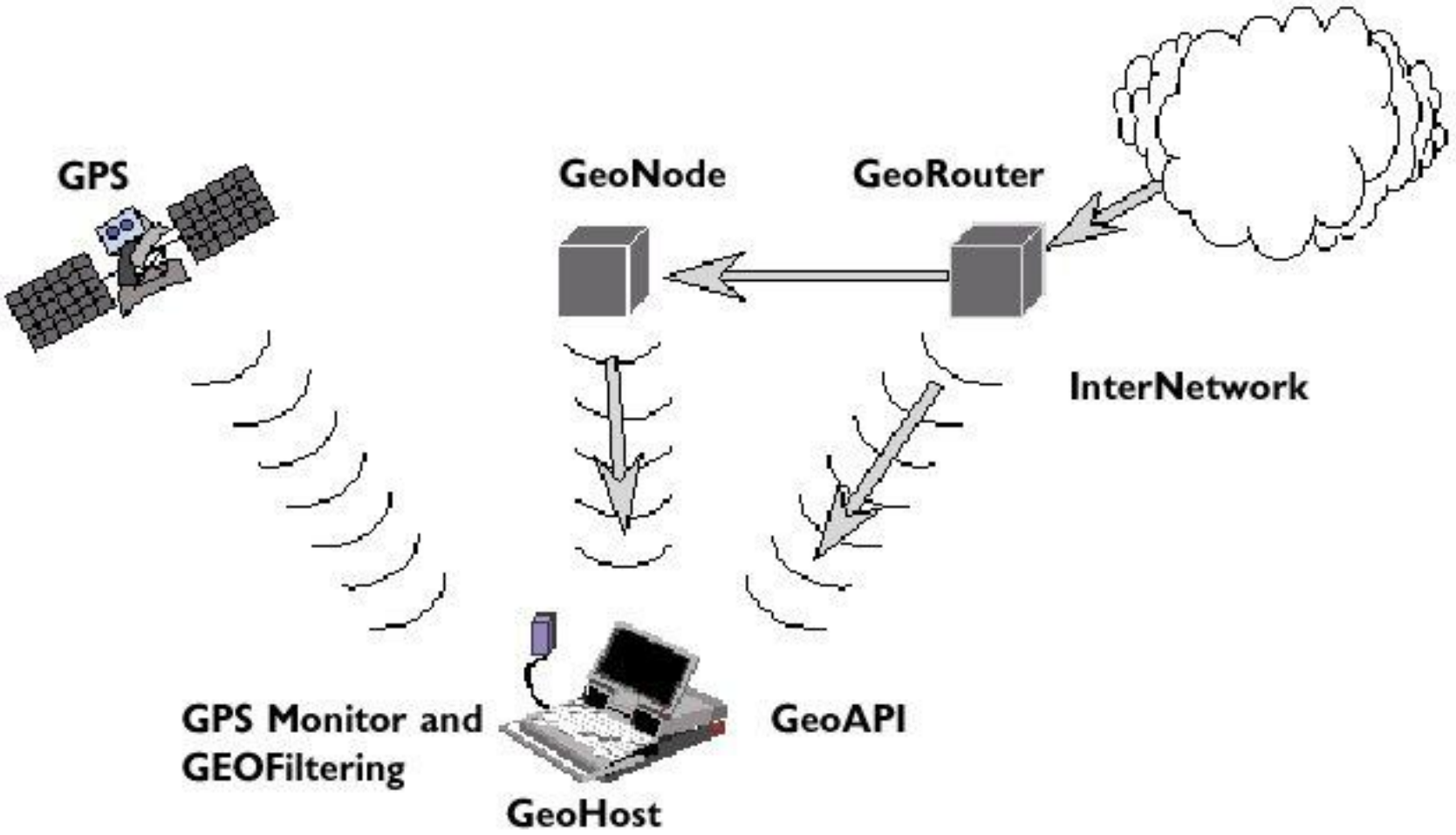
Landmark Ad hoc Routing (LANMAR)



Geographic Addressing and Routing (GeoCast)

- Roteamento baseado em GPS
- Permite o envio de mensagens para todos os nós de uma área geográfica específica
- Usa informações geográficas em vez dos endereços lógicos dos nós

Geographic Addressing and Routing (GeoCast)

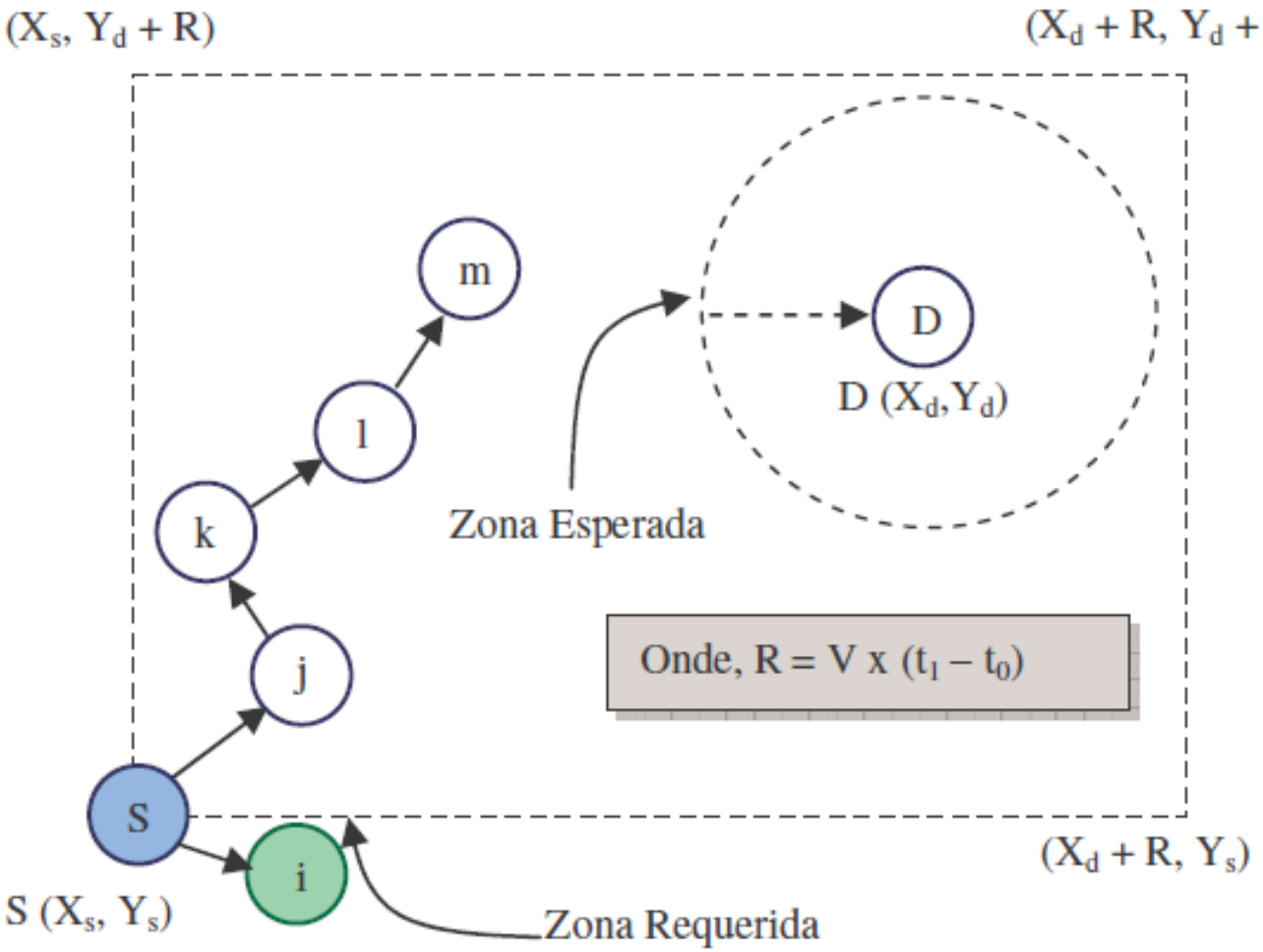


Fonte da Imagem: http://deliveryimages.acm.org/10.1145/300000/299176/figs/f2.jpg

Location-Aided Routing (LAR)

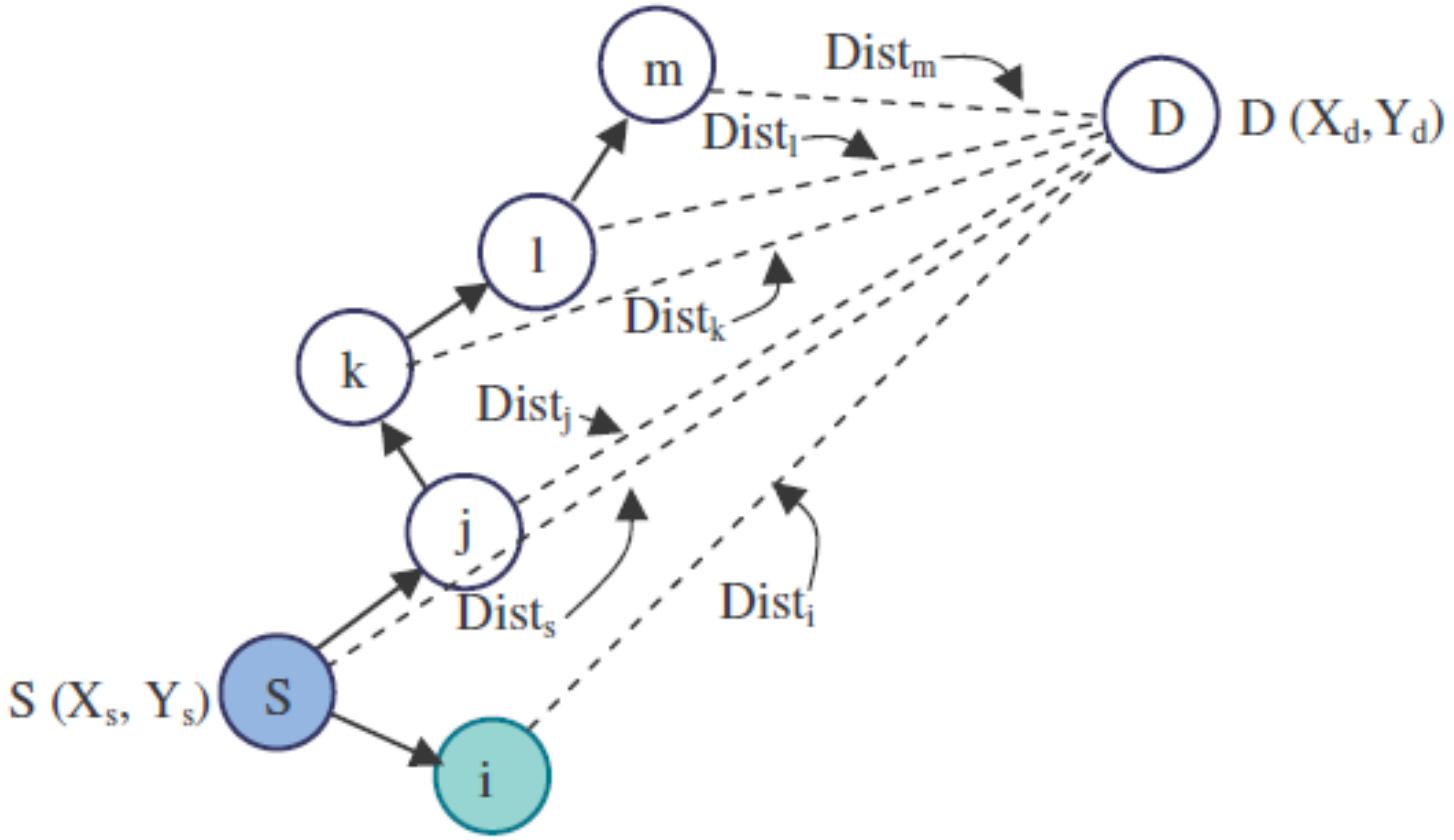
- Protocolo **Sob-Demanda (On-Demand) com Localização (GPS – Global Positioning**
- Utiliza um algoritmo semelhante ao usado no protocolo **DSR,** complementado pelo uso de GPS para restringir a área de inundação dos pacotes **RREQ**

Location-Aided Routing (LAR)



Propagação apenas para os nós dentro da Zona de Requisição

Location-Aided Routing (LAR)



Cada nó recalcula sua distância até o destino p/decidir se propaga o RREQ ou não.

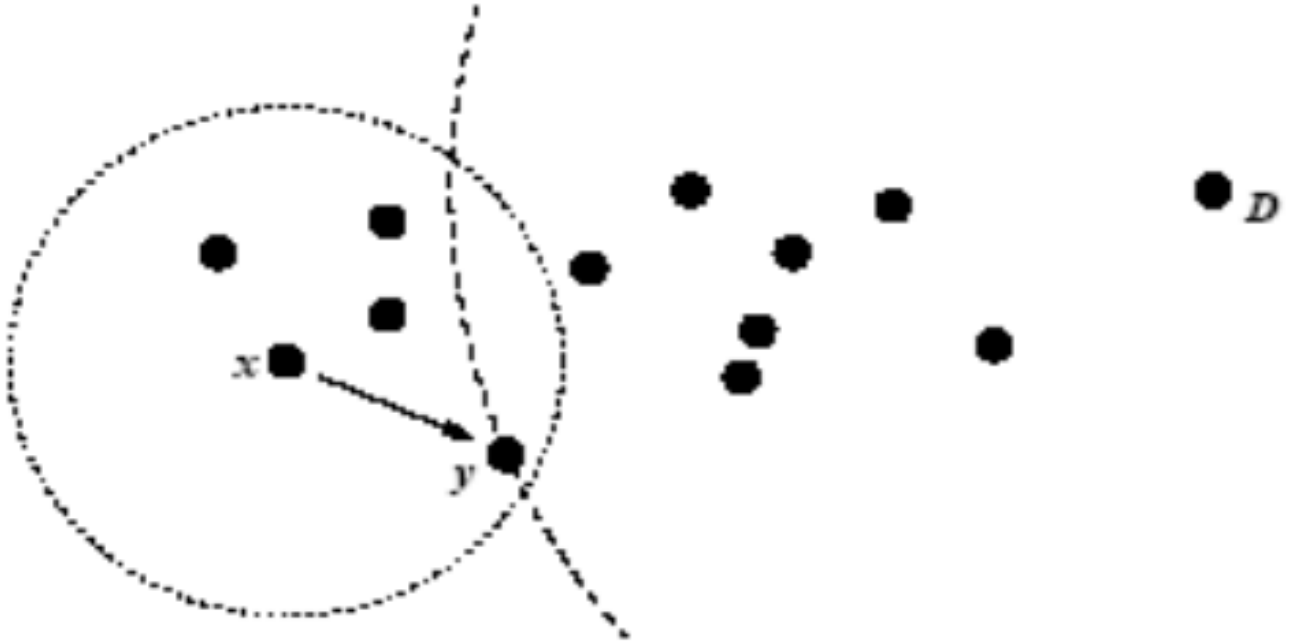
Distance Routing Effect Algorithm for Mobility (DREAM)

- Protocolo do tipo Pró-ativo que utiliza informações de Localização (Global Positioning System)
- Guarda as coordenadas de cada nó em uma Tabela de Localização para os outros nós, em vez dos vetores de rota, como é feito na maioria dos demais protocolos

Greedy Perimeter Stateless Routing (GPSR)

- Protocolo de encaminhamento ágil e eficiente para redes móveis sem fio
- Explora a correspondência entre a *posição geográfica* e conectividade em uma rede sem fio
- Usa as posições dos nós para tomar decisões de encaminhamento de pacotes

Greedy Perimeter Stateless Routing (GPSR)



Greedy forwarding example. y is x's closest neighbor to D

COMPARAÇÃO

Característica	PROTOCOLO					
	TBRPF	**OLSR**	**DSR**	**AODV**	**GSR**	**ZRP**
Características de Bellman-Ford (Caminho mais curto)				X		X
Características de Link State					X	X
Abordagem Pró-ativa	X	X	X		X	X
Abordagem Reativa				X		X
Suporta múltiplos caminhos	X	X		X	X	X
Suporte a QoS					X	X
Livre de loops	X	X	X	X	X	X
Flood na transmissão ou pedido de rota	X	X	X	X		X
É escalável					X	X
Necessita de mensagens periódicas	X	X		X	X	X
Possui mecanismos para encurtar o tamanho das tabelas ou o número de atualizações	X	X		X	X	X
Nodos intermediários necessitam inteligência para tentar encontrar o caminho	X	X		X	X	X

Mobile Ad Hoc Network

Segurança

Fundamentos Segurança

- **REQUISITOS DE SEGURANÇA**
  - **Autenticação**
    - Garantir que dada entidade é quem diz ser
  - **Confidencialidade**
    - Garante sigilo da informação
  - **Integridade**
    - Permite garantir que a informação não foi modificada
  - **Não-repúdio**
    - Impede emissor negue a sua autoria
  - **Disponibilidade**
    - Garantir os recursos da rede disponíveis

Segurança em MANETs

- Técnicas de segurança pré-existentes para redes fixas não são eficazes com a introdução de dispositivos móveis
  - Firewalls
  - Criptografia
  - Sistemas de Detecção de Intrusão (IDS) tradicionais
  - Servidor de Autenticação

Segurança em Manets

- Manets são suscetíveis a ataques
- Uso do meio de transmissão – ar
- Grau de comprometimento dos nós é alto
- Mobilidade – vantagens e desvantagens
- Principal alvo – falhas e fraquezas dos protocolos de roteamento

Vulnerabilidades das MANETs

- Baseada em comunicação sem fio
- Não há a necessidade do intruso ter acesso físico à rede ou passar por várias linhas de defesa como firewalls ou gateways
- Qualquer nó pode ser atacado
- MANETs não têm uma linha de defesa clara e qualquer nó constituinte deve estar preparado para encontros com um adversário direta ou indiretamente

Vulnerabilidades das MANETs

- As MANETs são vulneráveis porque
  - Sua comunicação é feita em um meio aberto
  - Sua topologia é dinâmica
  - Utiliza algoritmos cooperativos
  - Não tem um ponto central de controle e monitoramento
  - Não tem uma linha de defesa clara

Ataques em Manets

- ATIVOS
  - Os recursos são usados para degradar ou anular o fluxo de mensagens na rede
  - Atacante interfere no funcionamento da rede enviando mensagens
- PASSIVOS
  - Objetivam obter informações sobre rotas
  - Atacante não interfere no funcionamento da rede

Problemas com Ataques

- Rotas com loops
- Timeout – tempo de vida de uma rota demorado
- Métricas falsas ou exageradas
- Repetição de mensagens de atualização

Problemas com Ataques

- Cada membro da rede deve estar preparada para enfrentar adversário
- Nós inimigos podem participar do processo de descoberta de rotas (RREQ e RREP)

Ataques

- **Espionagem**
  - Escuta passiva da rede
  - Atacante tenta pegar informações importantes
  - Revelação de Informações Críticas
  - Se pontos vulneráveis são encontrados, essas informações são passadas para outros nós maliciosos que poderão realizar ataques ativos

Ataques

- Gerados a partir de uma estação
  - Ex: Buraco Negro (Black hole)
- Gerados por duas ou mais estações
  - Buraco da minhoca (Wormhole)
- Ataques de Camada Física
  - Exaurir a energia da rede → negação de serviço
  - Interferência contínua/esporádica
  - Introdução de ruído na rede(mesma freqüência)
    - Gerar interferência no sinal transmitido, negando o serviço no canal de comunicação
    - Técnicas de espalhamento espectral e salto de freqüência melhoram esse problema
    - Aumento da potência → consumo energia

Ataques

- Ataques de Camada de Enlace (MAC)
  - Indução de colisões
    - Colisões propositais causadas por nó malicioso com o objetivo de negar uso do canal
  - Exaustão
    - Danificação de pacotes de dados e/ou controle → detectados pelo checksum → gera retransmissão
    - Tentativa de retransmissão sucessivas com o objetivo de sobrecarregar o destino
- Ataques a Camada de Rede
  - Objetivo de prejudicar o roteamento e transferência dos dados

Ataques

- Ataques de Camada de Rede
  - Negação de Serviço
    - Sobrecarrega a rede com pedidos de rota (RREQ)
  - Modificação de Métricas
    - Alterações de valores das métricas de uma rota ou alterações de campos de mensagem de controle
      - Redirecionamento (Altera número de sequência da rota)
      - Redirecionamento (Altera contador de saltos)
      - Negação de serviço (Altera informações de rota)

Ataques

- Ataques de Camada de Rede
  - **WORMHOLE**
    - Dois atacantes criam um túnel de comunicação por um enlace de baixa latência, através do qual irão trocar informações da rede, replicando-as do outro lado do túnel, de forma a tornar excepcionalmente atrativo o enlace formado
    - Permite gerar, no momento que desejarem, diversos tipos de prejuízos à rede
  - **BLACKHOLE**
    - Todos os pacotes são atraídos até o nó malicioso
    - Nós maliciosos negam a recepção de pacotes de roteamento, reduzindo a quantidade de informação de roteamento disponível para os demais nós

Ataques

- Ataques de Camada de Rede
  - **SINKHOLE**
    - Atacantes forçam pacotes a passar por um determinado nó, facilitando a ação de outros ataques
  - **INUNDAÇÃO**
    - Nós maliciosos tentam derrubar os recursos limitados das vítimas como processador, memória, bateria ou largura de banda
  - **ENCAMINHAMENTO SELETIVO (BURACO CINZA)**
    - Nós maliciosos descartam pacotes seletivamente, dificultando a detecção

Ataques

- Ataques de Camada de Rede
  - **Estouro (*Overflow*) da Tabela de Roteamento**
    - Protocolos de roteamento ad hoc pró-ativos armazenarem todas as rotas anunciadas pelos seus vizinhos
    - A estratégia deste ataque é anunciar diversas rotas para nós inexistentes, de modo a aumentar progressivamente o tamanho da tabela de roteamento, até que ela estoure e o nó não possa mais armazenar as rotas reais

Ataques

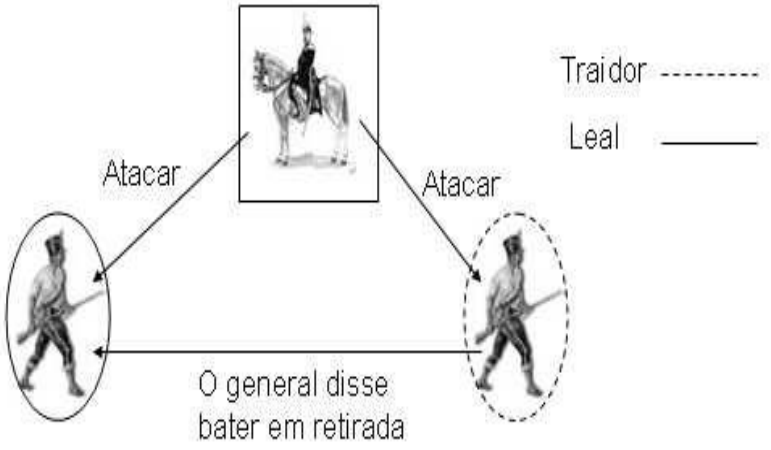
- Ataques de Camada de Rede
  - **SYBIL**
    - É praticamente impossível, em sistemas computacionais distribuídos, que nós que não se conhecem apresentem identidades distintas convincentes
    - Sem a existência de um ponto central para controlar a associação de uma identidade a uma entidade, é sempre possível para uma entidade desconhecida apresentar múltiplas identidades
  - **ACELERAÇÃO**
    - Nós maliciosos encaminham rapidamente as mensagens de pedido de rota quando é iniciada uma descoberta de rota, com objetivo de participar de qualquer descoberta de rota

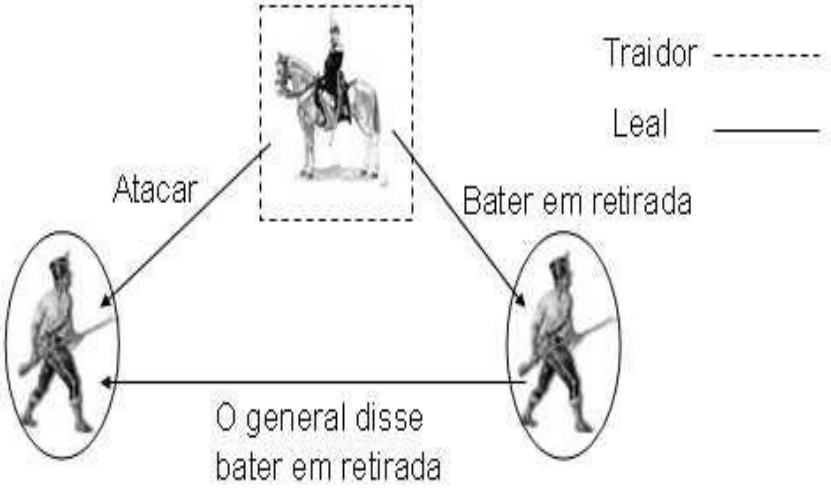
Ataques

- Ataques de Camada de Rede
  - **Personificação (spoofing)**
    - Estação esconde seu IP ou endereço MAC e finge ser outra máquina
    - Pode causar loops, atrair ou repelir tráfego, gerar mensagens de erro de rotas falsas, dividir a rede, etc.
    - Alvo principal → pacotes de controle responsáveis pelas informações roteamento

Ataques

- Ataques de Camada de Rede
  - **Ataque bizantino**
    - Ligado a problemas de tolerância a falhas
    - Um ou mais nós maliciosos trabalham em conluio para gerar problemas como *loops* de roteamento, pacotes de roteamento falsos, escolha de caminhos não-ótimos, entre outros, utilizando mensagens de controle dos protocolos que estão sendo utilizados





Ataques

- Ataques de Camada de Rede
  - **Fabricação**
    - **Intruso fabrica dados FALSOS e os envia para outra estação**
      - Envenenamento da tabela de roteamento
        - Gerar RREQ, RREP, RERR
      - Sobrecarregar Tabela Roteamento
        - Informar muitas rotas inexistentes
    - **Inundação de Hello**
      - Hello identifica se o vizinho está ativo
      - Estação vizinha aceita a rota anunciada por ela
      - Induz tráfego das informações pela rota anunciada

Ataques

- Ataques de Camada Transporte
  - **Inundação de SYN**
    - Para realizar a comunicação utilizando o TCP, é necessário um período de tempo para o estabelecimento da conexão.
    - Cada processo de conexão ocupa um espaço de memória no nó até que seja concluído.
    - Este ataque visa explorar essa característica, gerando vários pedidos de conexão para a vítima.
    - Cada um desses pedidos, que nunca é completado, provoca a alocação de mais recursos, até o momento que acontece um estouro de memória

Referências

- KUROSE, James F. Redes de Computadores e a Internet: uma abordagem top-down. 3. Ed. São Paulo: Pearson Addison Wesley, 2006.
- http://pt.wikipedia.org/wiki/Ad_hoc acesso em 28/08/2008
- CÂMARA, Daniel http://homepages.dcc.ufmg.br/~danielc/redes/roteamento.html acesso em 28/08/2008
- GOLDMAN, Alfredo. Redes Móveis Ad Hoc. Minicurso SBRC, 2002.
- http://www.ietf.org/rfc/rfc3626.txt acesso em 28/08/2008
- http://www.ietf.org/rfc/rfc4728.txt acesso em 28/08/2008
- http://www.ietf.org/rfc/rfc3561.txt acesso em 28/08/2008
- BEIJAR, Nicklas. Zone Routing Protocol. http://www.netlab.tkk.fi/opetus/s38030/k02/Papers/08-Nicklas.pdf acesso em 28/08/2008.
- http://www.gta.ufrj.br/ensino/CPE825/2006/resumos/OLSR.ppt

Referências

- LIMA, Claudinei Quaresma. Rotas Hierárquicas e Segurança em Redes Ad Hoc. Tese de Mestrado. ITA: São José dos Campos, 2006.
- ALBINI, Luiz C. P. etc. al. Segurança em Redes Ad Hoc. Proposta de Minicurso para SBrT2008. http://www.sbrt.org.br/sbrt08/docs/LuizAlbini_Seguranca.pdf
- FRANCESQUINI, Emilio de Camargo. Detecçao de Intrusos em MANETs. http://grenoble.ime.usp.br/movel/detecao.ppt
- http://www.cs.virginia.edu/~cl7v/cs851-papers/dsdv-sigcomm94.pdf
- http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/aodv/indice.html
- PUTTINI, Ricardo Staciarini. Redes Móveis Ad Hoc. UNB.
- REZENDE, Nelson Soares de. **Redes Nóveis sem Fio Ad Hoc**. UFRJ: Rio de Janeiro, 2004.