UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Disciplina:
Redes de Sensores

Prof. Guilherme L. Moritz
Prof. Ohara K. Rayel

PPGSE - UTFPR

Tarefa de Aula

Ataques ao Protocolo RPL em Redes de Sensores Sem Fio

Hermano Pereira

Curitiba, 13 de junho de 2016

Introdução

Artigos:

A Taxonomy of Attacks in RPL-based Internet of Things

Mayzaud, A.; Bodonnel, R.; Chrisment, I.; Int. Journal of Network Security – May 2016.

A Survey: Attacks on RPL and 6LoWPAN in IoT

Pongle, P.; Chavan, G.; Int. Conference on Pervasive Computing – IEEE- 2015.

Introdução

A Taxonomy of Attacks in RPL-based Internet of Things

Contribuição: taxonomia para classificação de ataques ao RPL construída com diversos trabalhos relacionados, detalhes dos ataques e contra-medidas.

A Survey: Attacks on RPL and 6LoWPAN in IoT

Contribuição: levantamento dos principais ataques sobre RPL e 6LoWPAN.

RPL

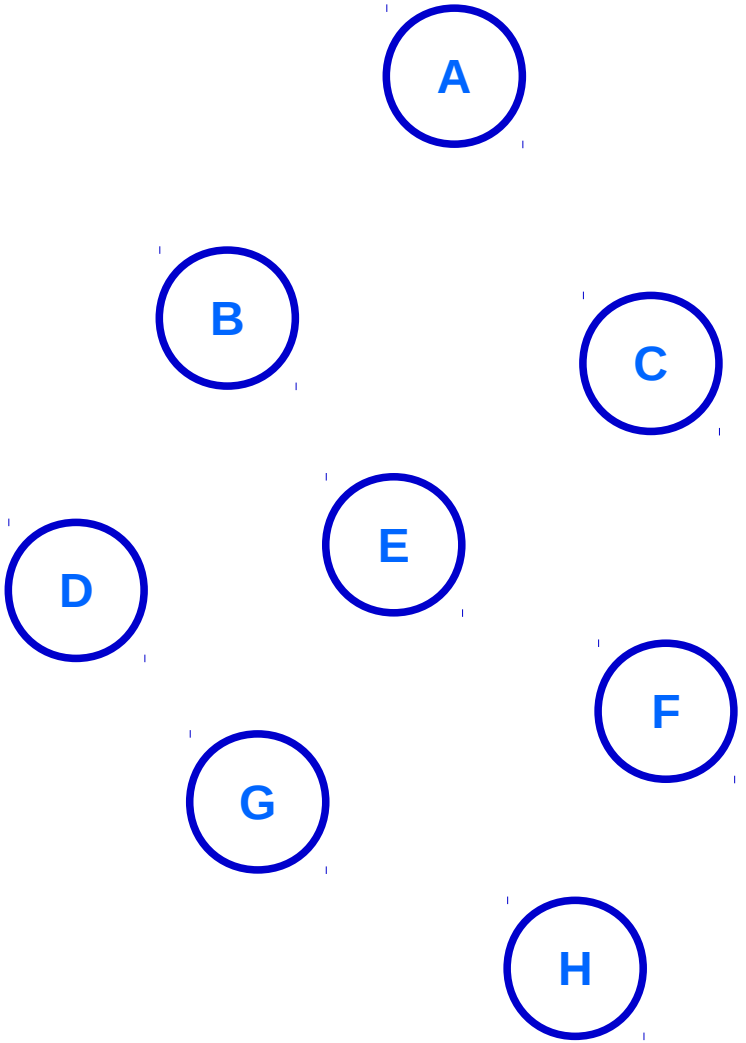
Routing Protocol for Low Power and Lossy Networks

- Principal alvo de ataques
- Roteamento na Internet das Coisas
- RFC 6550
- 802.15.4 (6LowPAN) 802.15.4e (6tsch)

Convergência do Protocolo RPL:

- Formar um DAG (grafo)

Directed
Acyclic
Graph

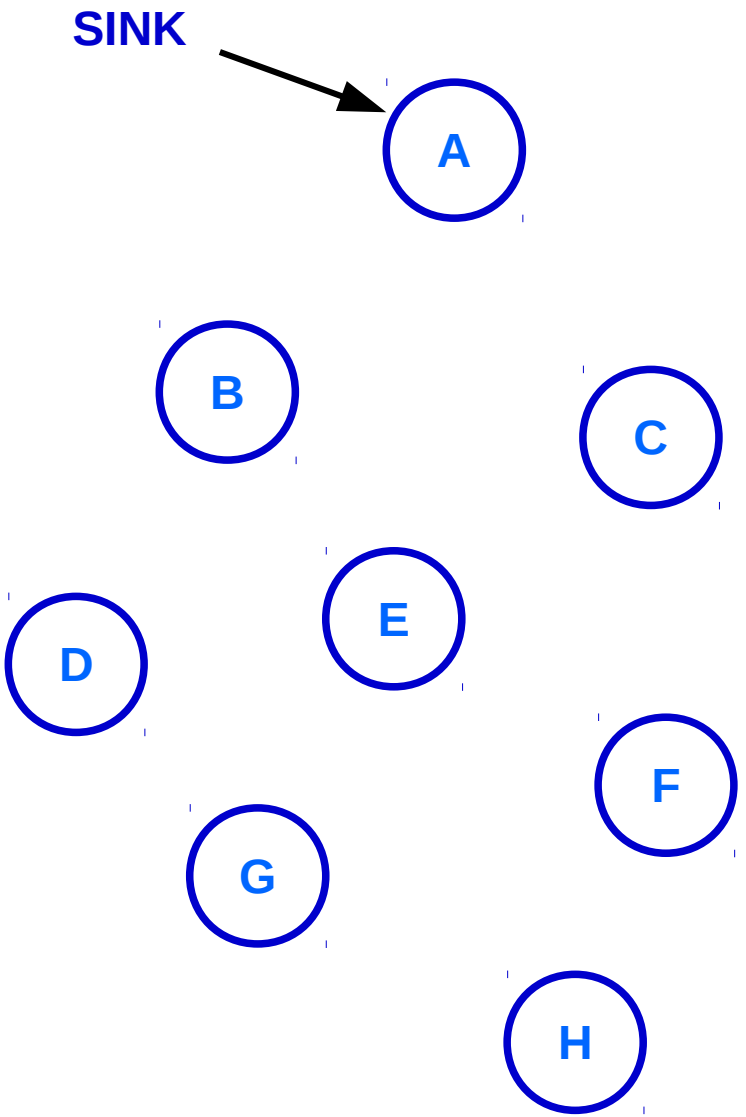


Convergência do Protocolo RPL:

- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

Destination
Oriented
DAG



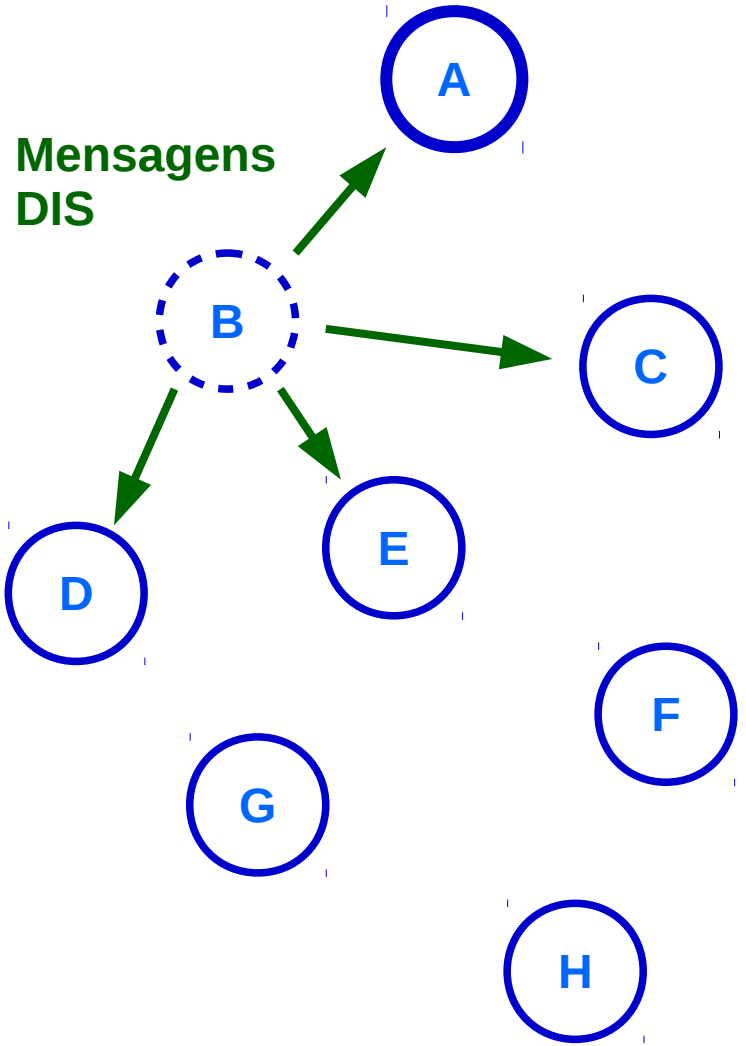
Convergência do Protocolo RPL:

- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

- Nó busca por topologia (DIS)

DODAG
Information
Solicitation



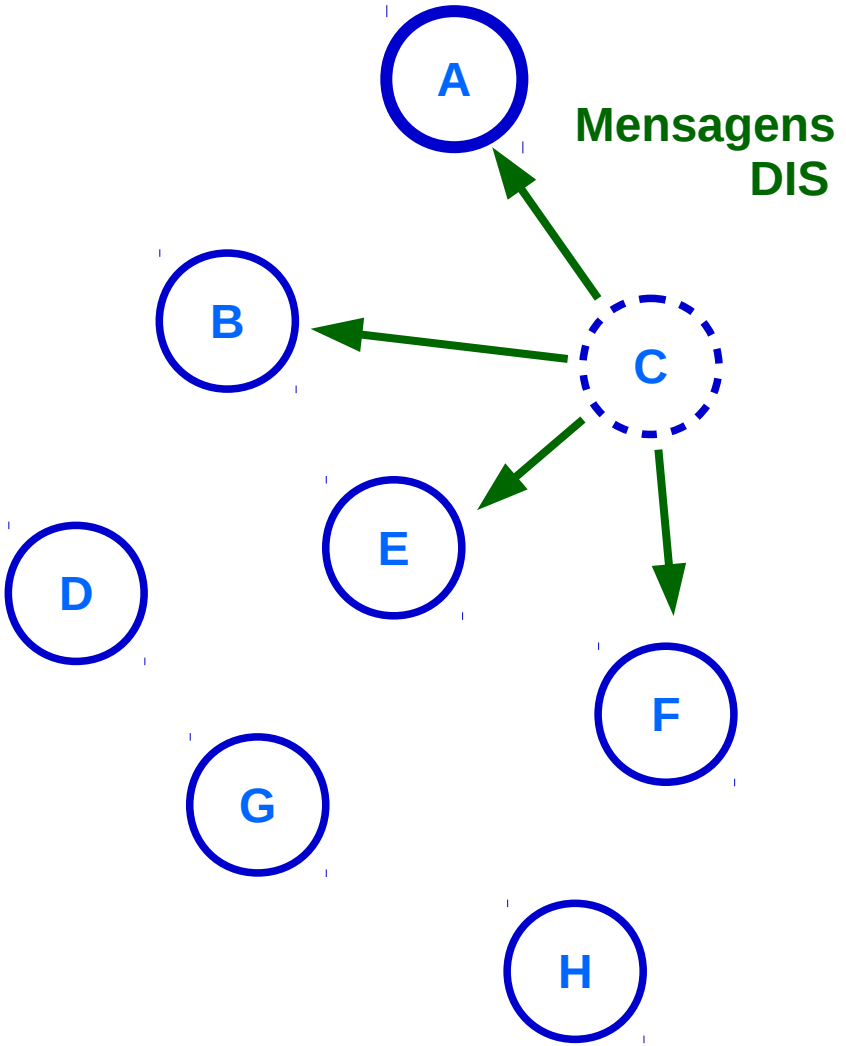
Convergência do Protocolo RPL:

- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

- Nó busca por topologia (DIS)

DODAG
Information
Solicitation



Convergência do Protocolo RPL:

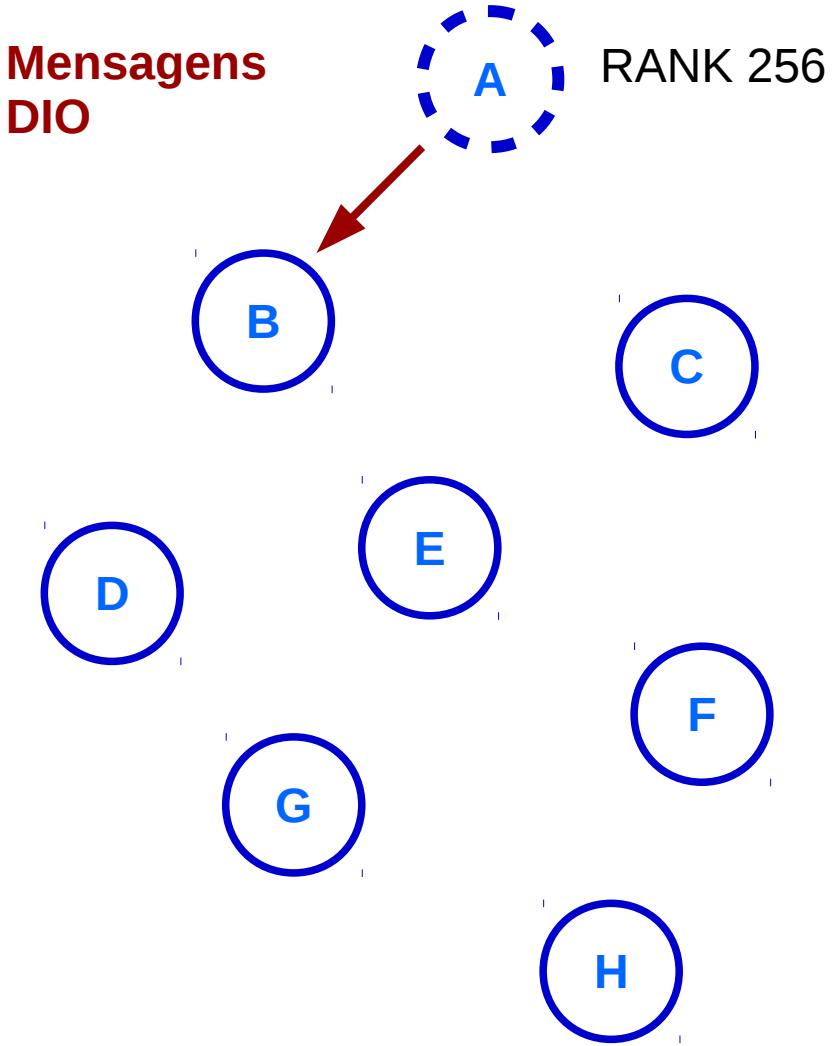
- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

- Nó busca por topologia (DIS)

- Nó pai fornece informação (DIO)

DODAG
Information
Object



Convergência do Protocolo RPL:

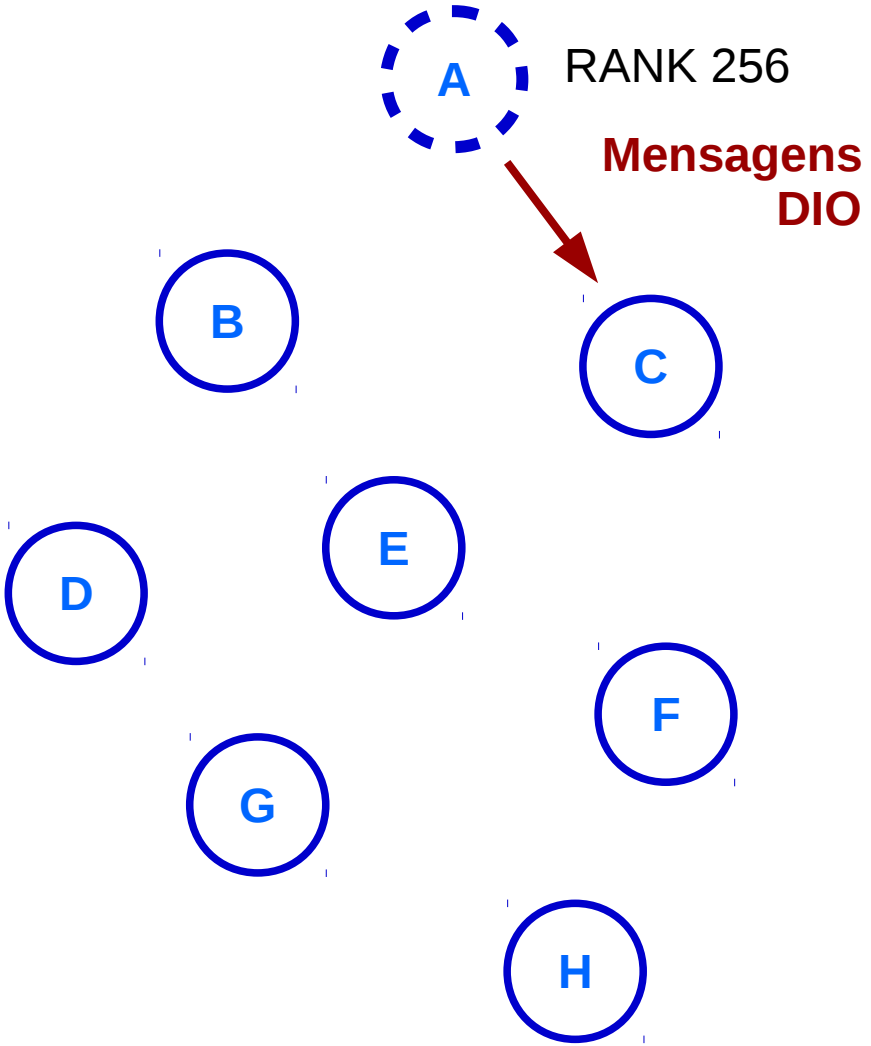
- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

- Nó busca por topologia (DIS)

- Nó pai fornece informação (DIO)

DODAG
Information
Object



Convergência do Protocolo RPL:

- Formar um DAG (grafo)

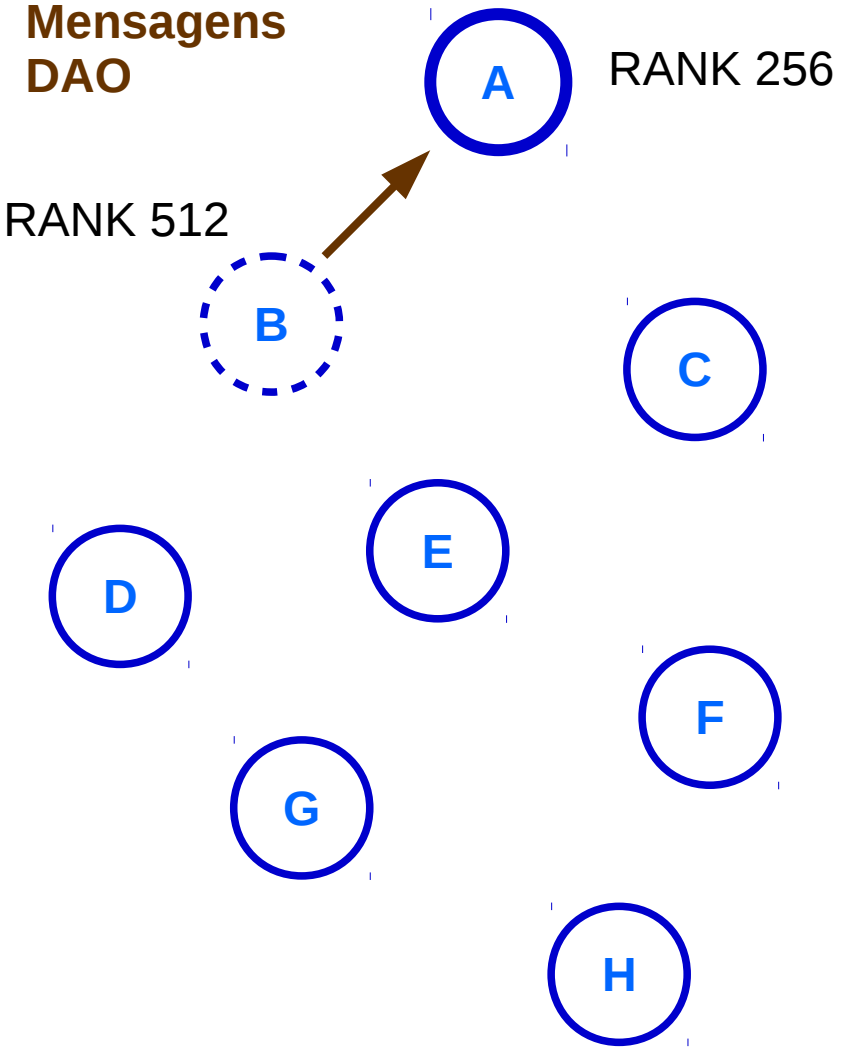
- Formar DODAG (um nó sink)

- Nó busca por topologia (DIS)

- Nó pai fornece informação (DIO)

- Nó confirma *upward* (DAO)

Destination
Advertisement
Object



Convergência do Protocolo RPL:

- Formar um DAG (grafo)

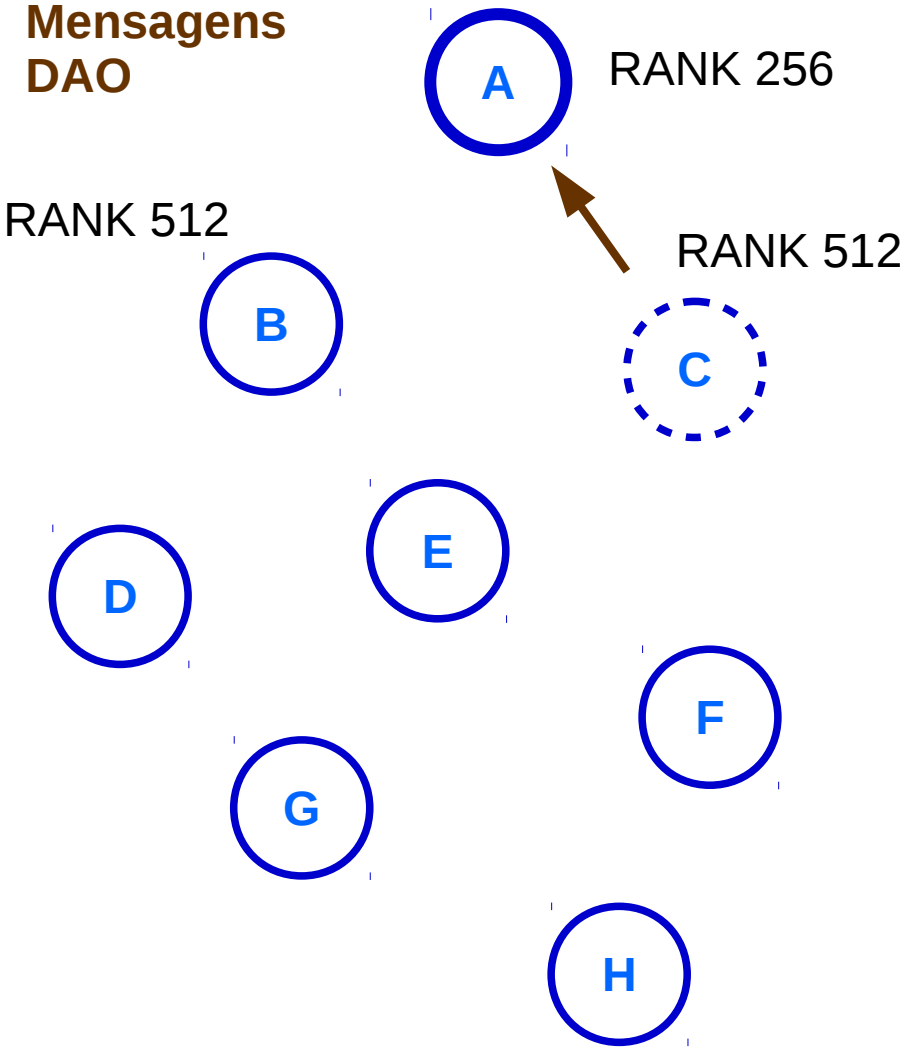
- Formar DODAG (um nó sink)

- Nó busca por topologia (DIS)

- Nó pai fornece informação (DIO)

- Nó confirma *upward* (DAO)

Destination
Advertisement
Object



Convergência do Protocolo RPL:

- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

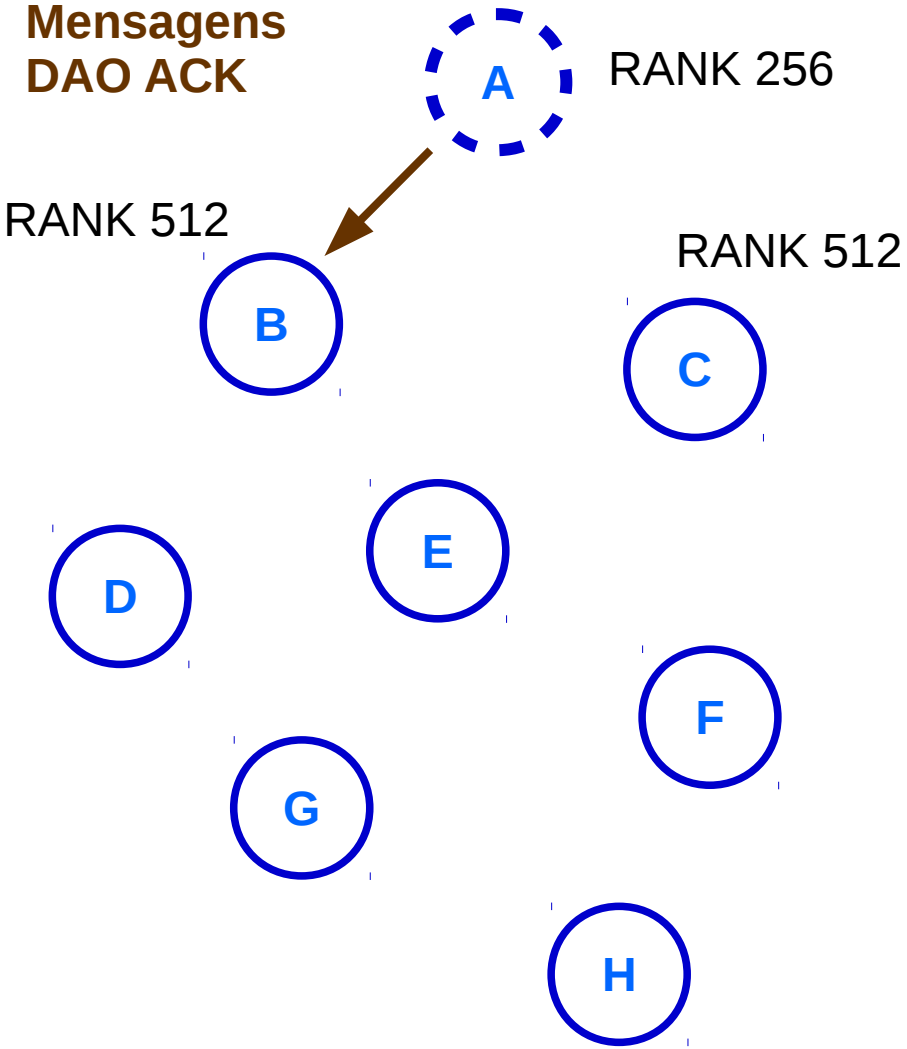
- Nó busca por topologia (DIS)

- Nó pai fornece informação (DIO)

- Nó confirma *upward* (DAO)

- Sink confirma *downward* (DAO-Ack)

DAO-**Ack**



Convergência do Protocolo RPL:

- Formar um DAG (grafo)

- Formar DODAG (um nó sink)

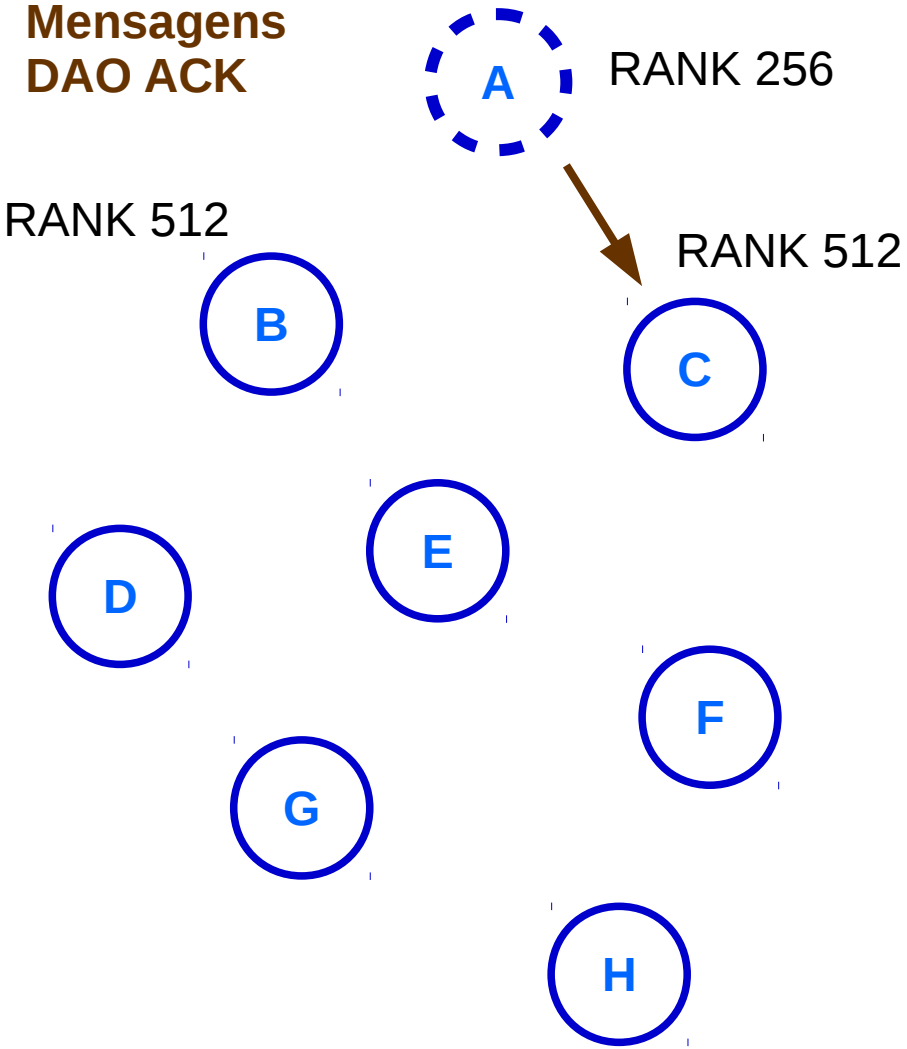
- Nó busca por topologia (DIS)

- Nó pai fornece informação (DIO)

- Nó confirma *upward* (DAO)

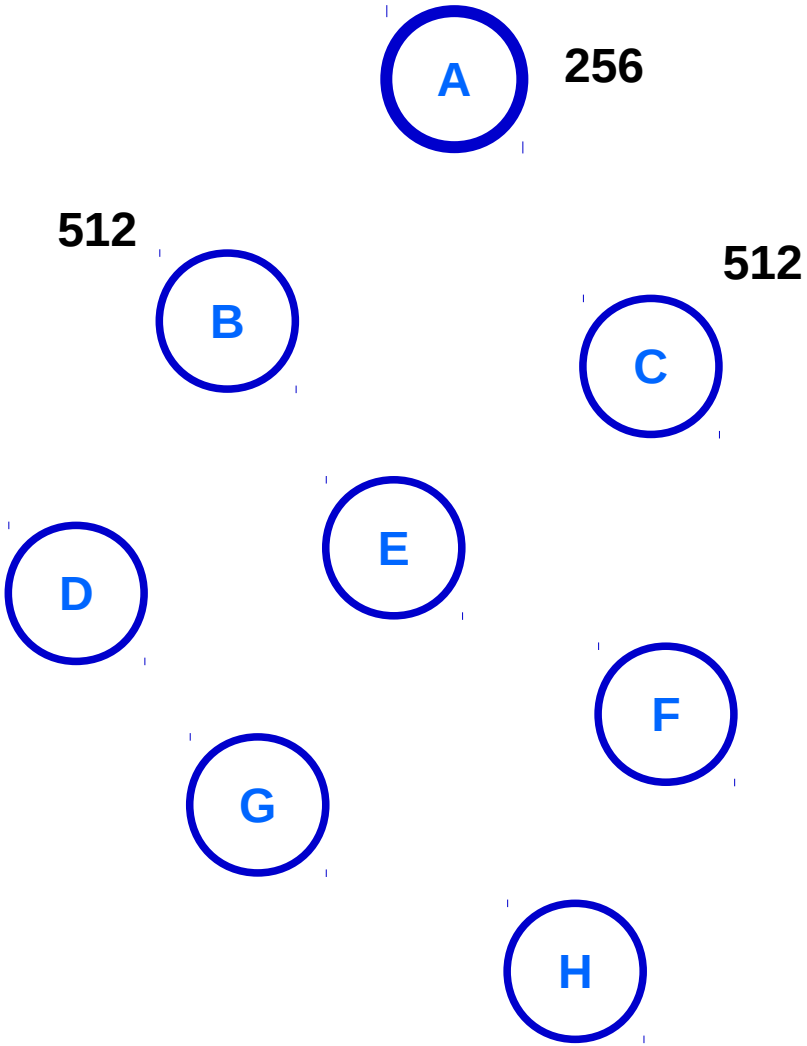
- Sink confirma *downward* (DAO-Ack)

DAO-**Ack**



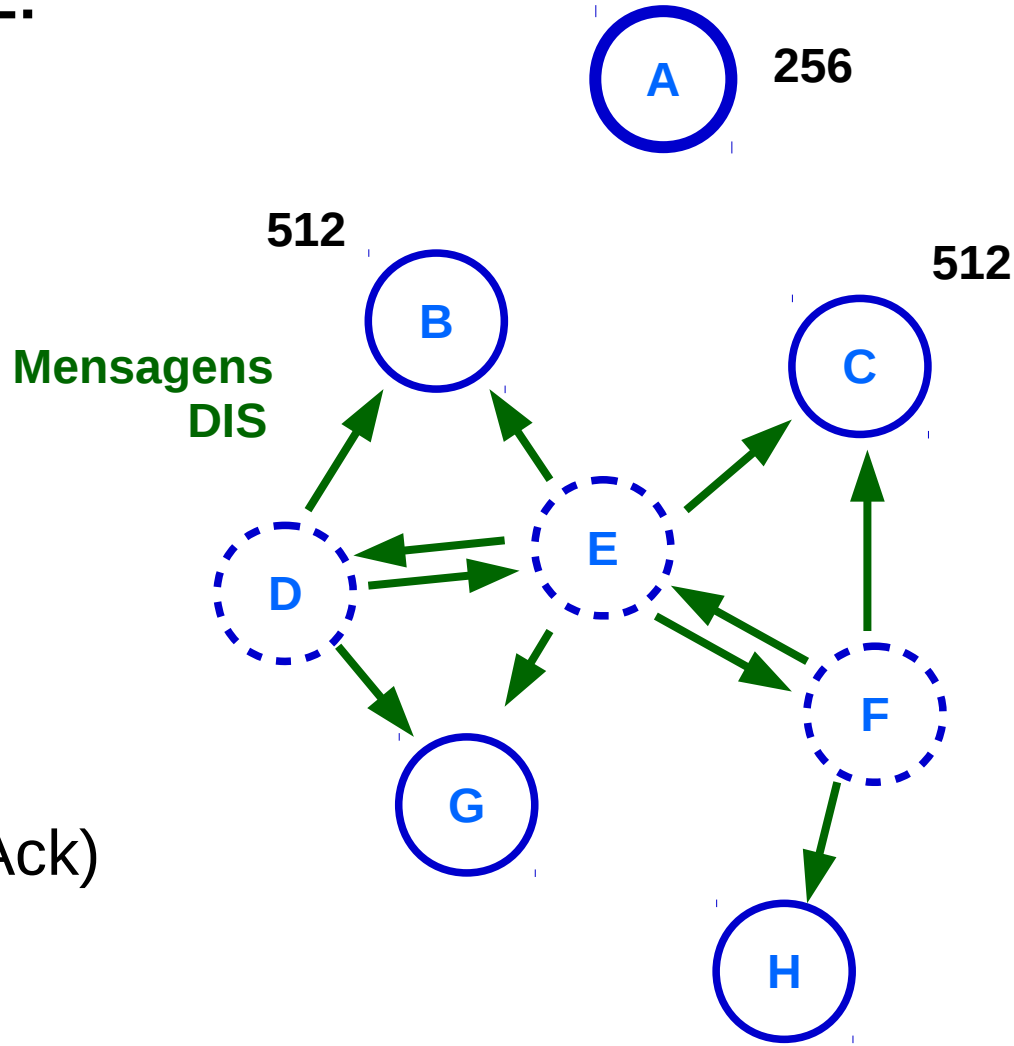
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



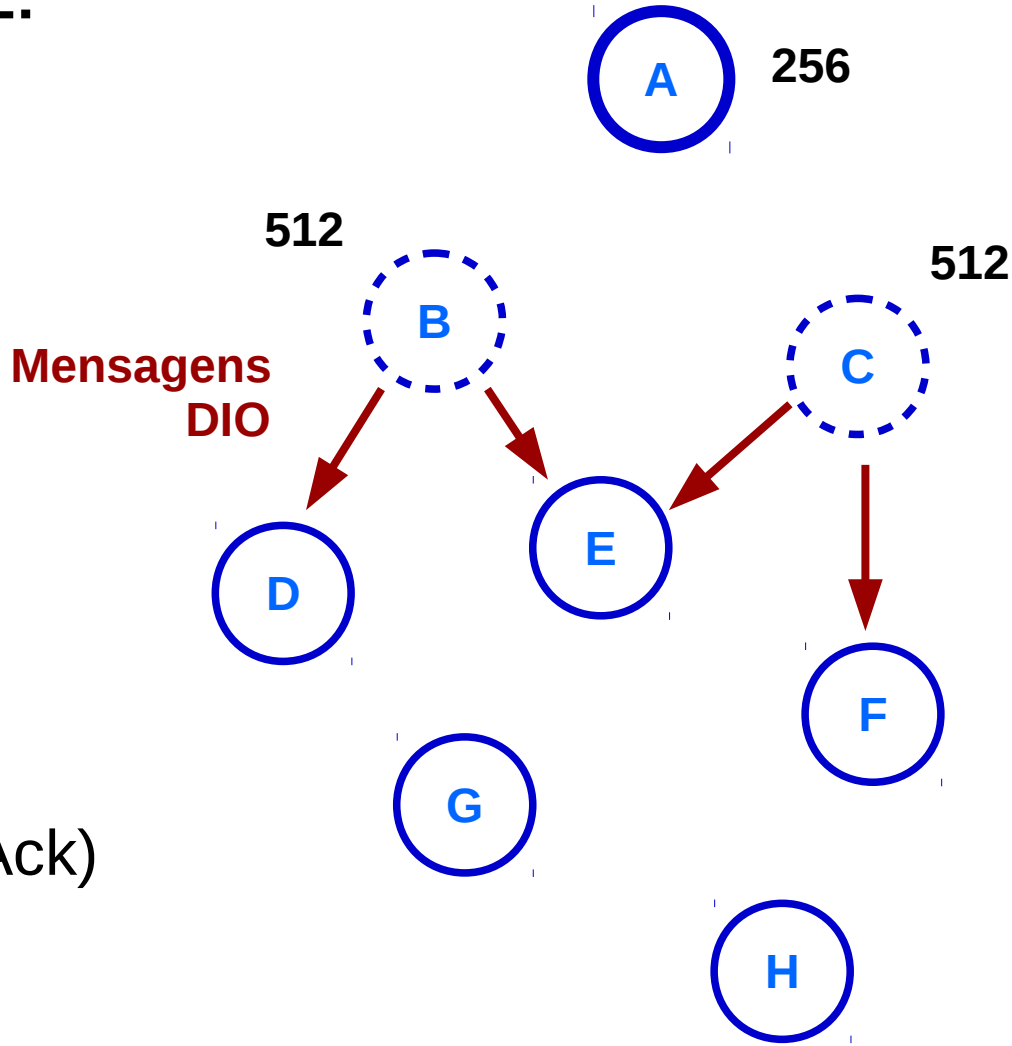
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



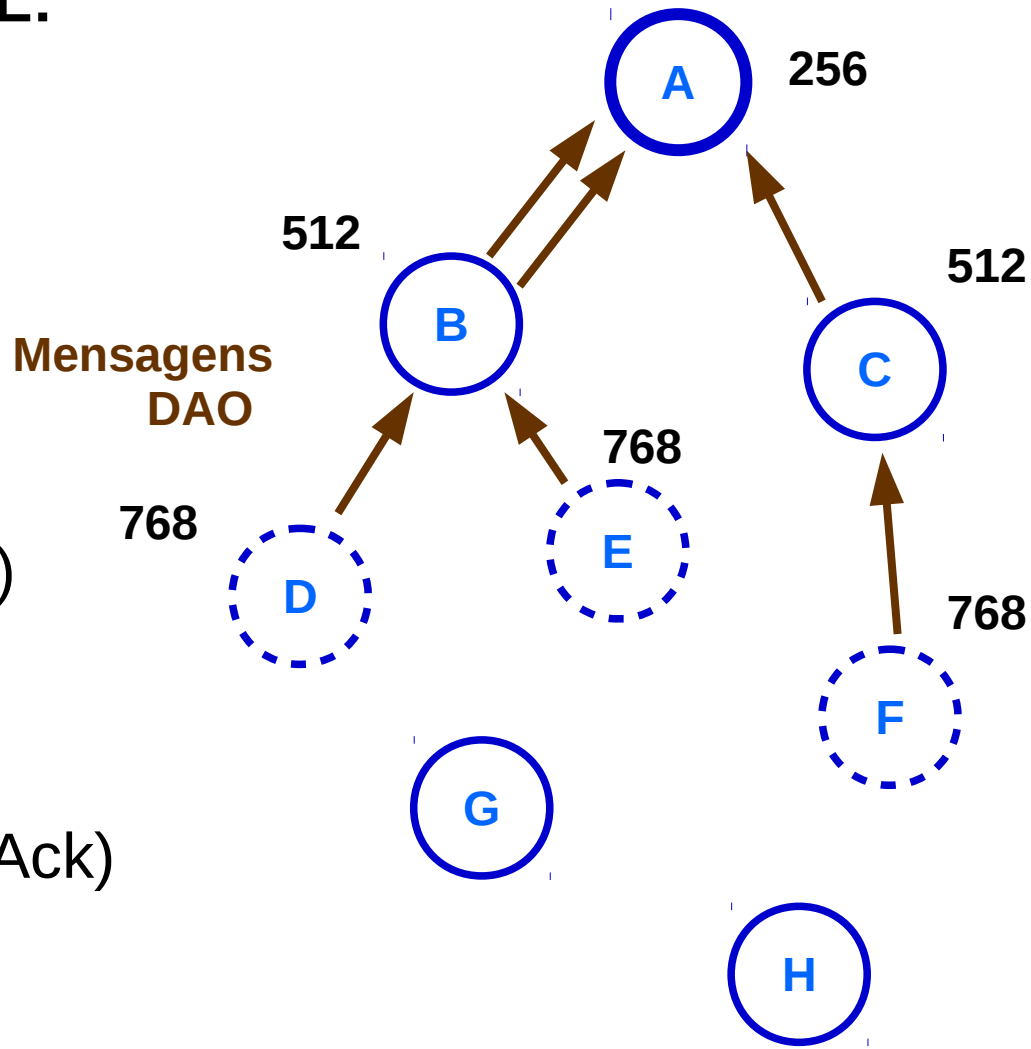
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



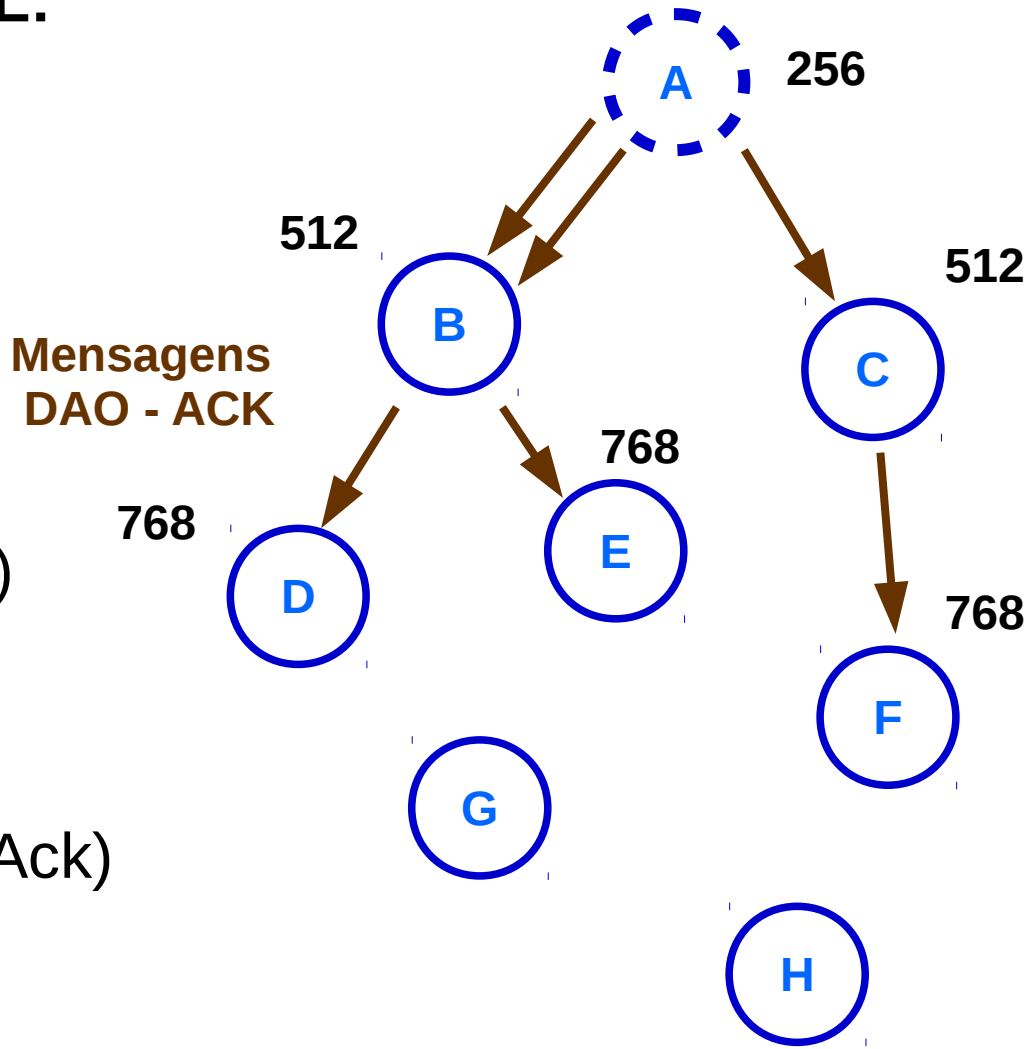
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



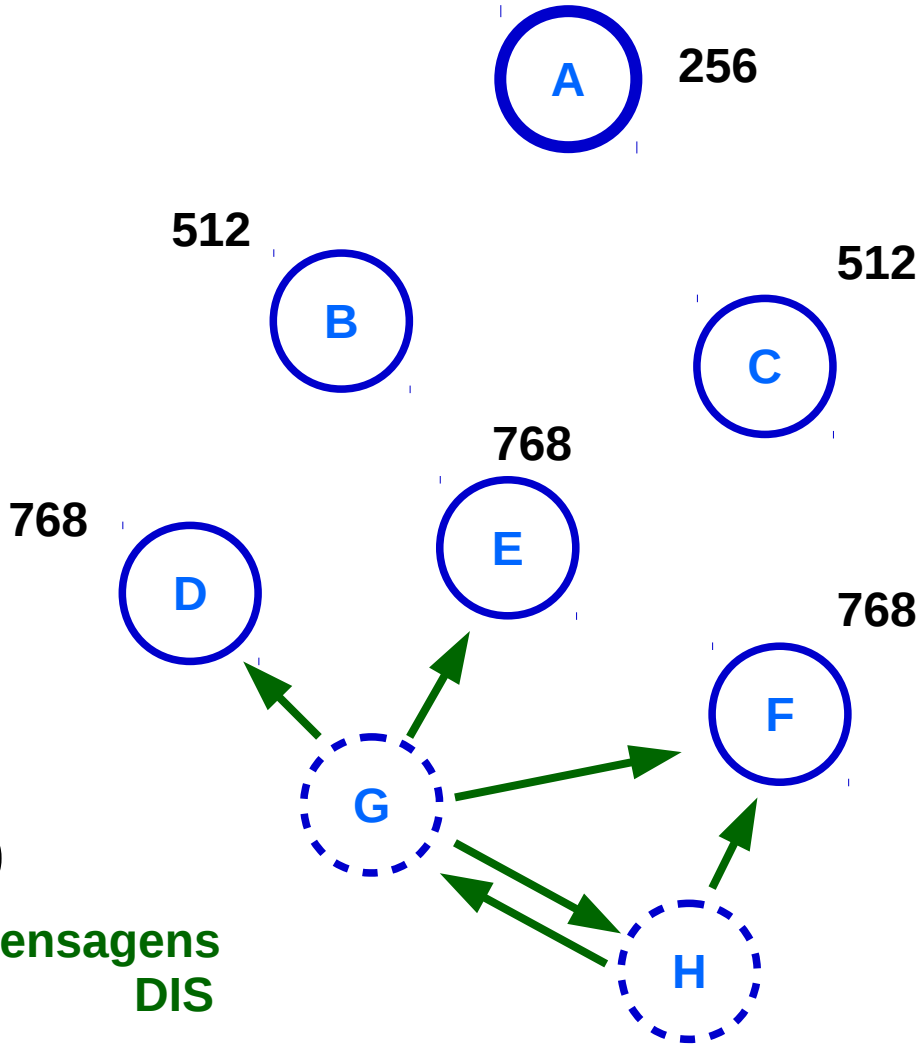
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



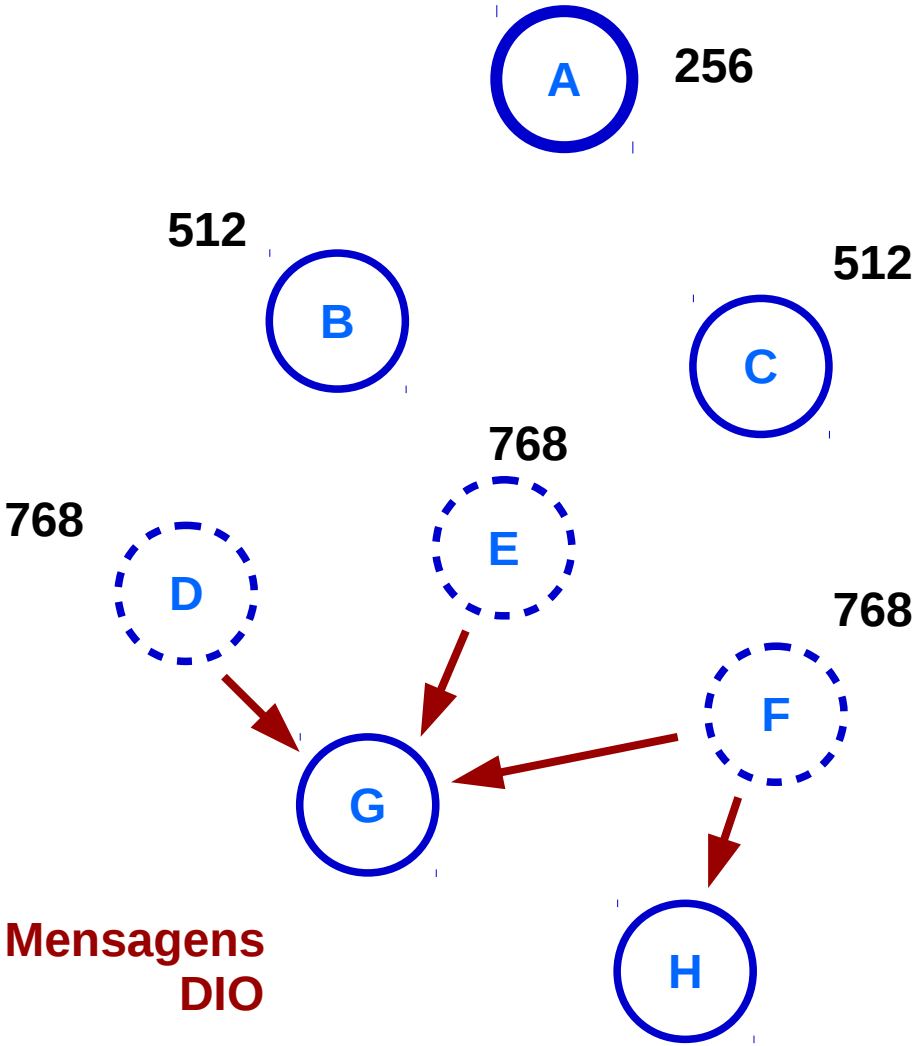
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



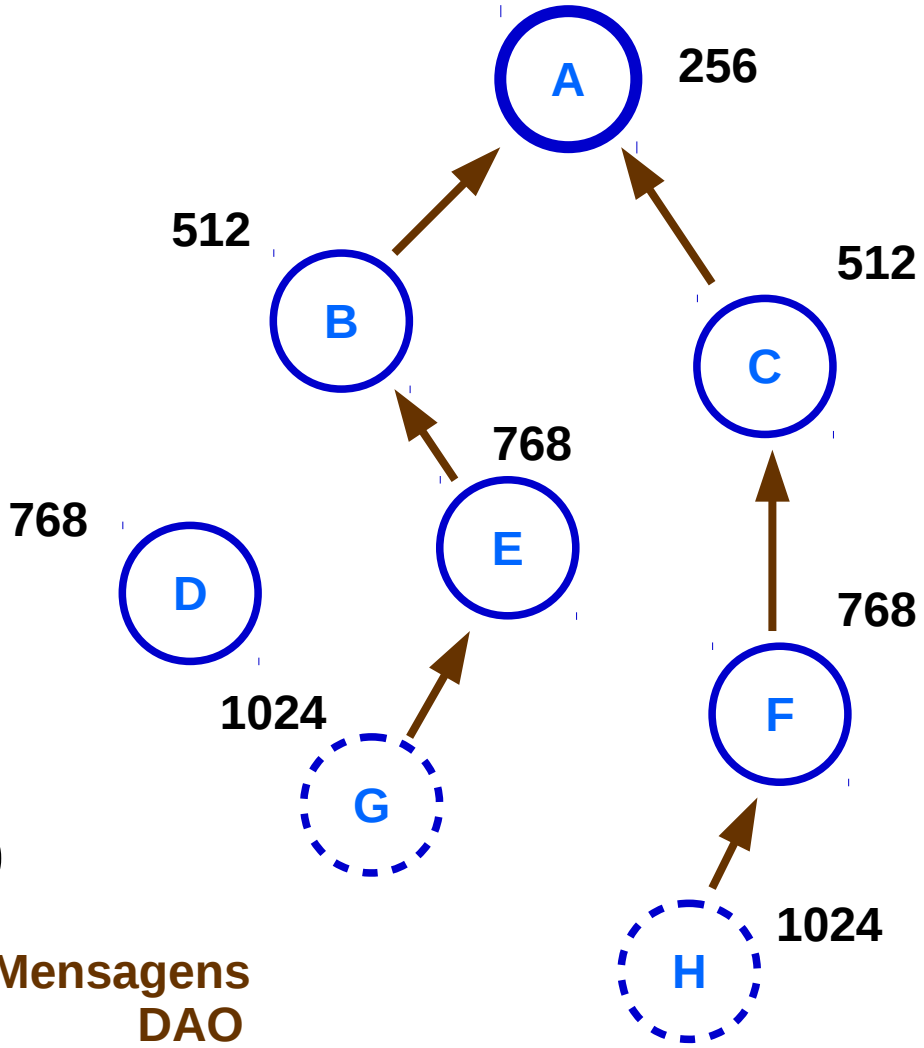
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



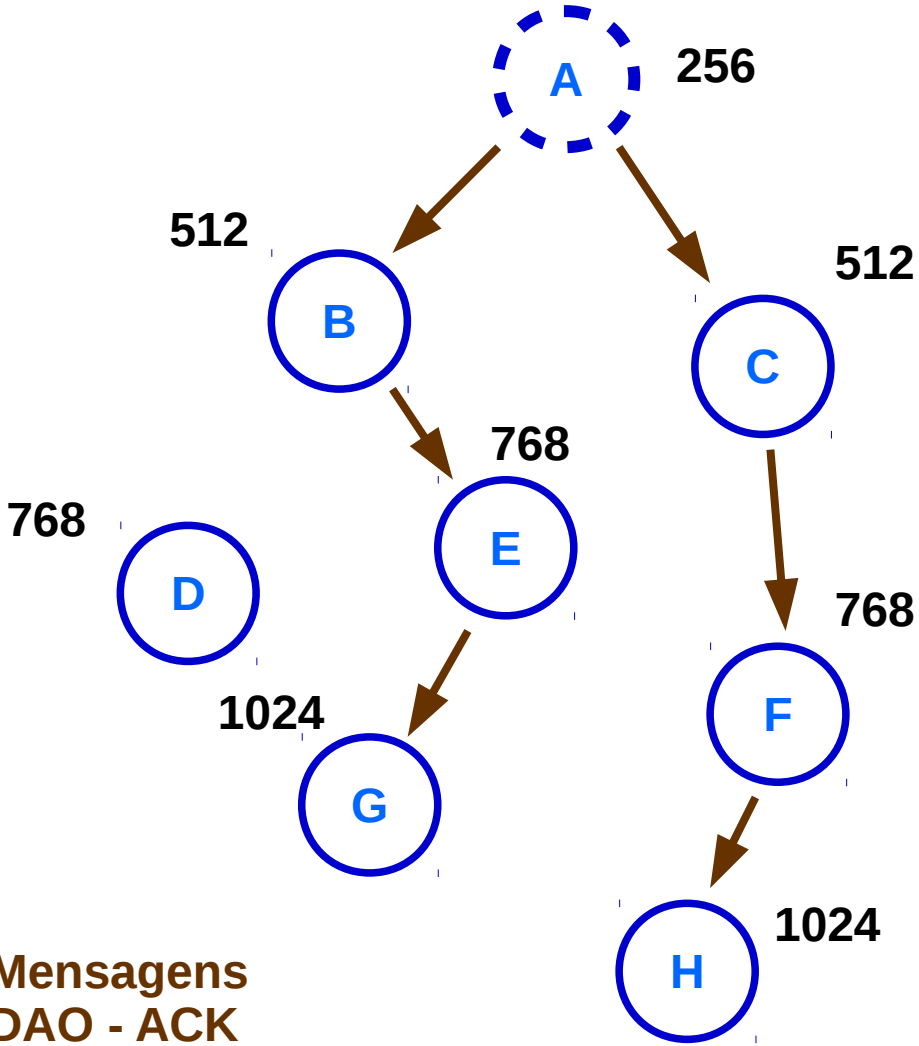
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



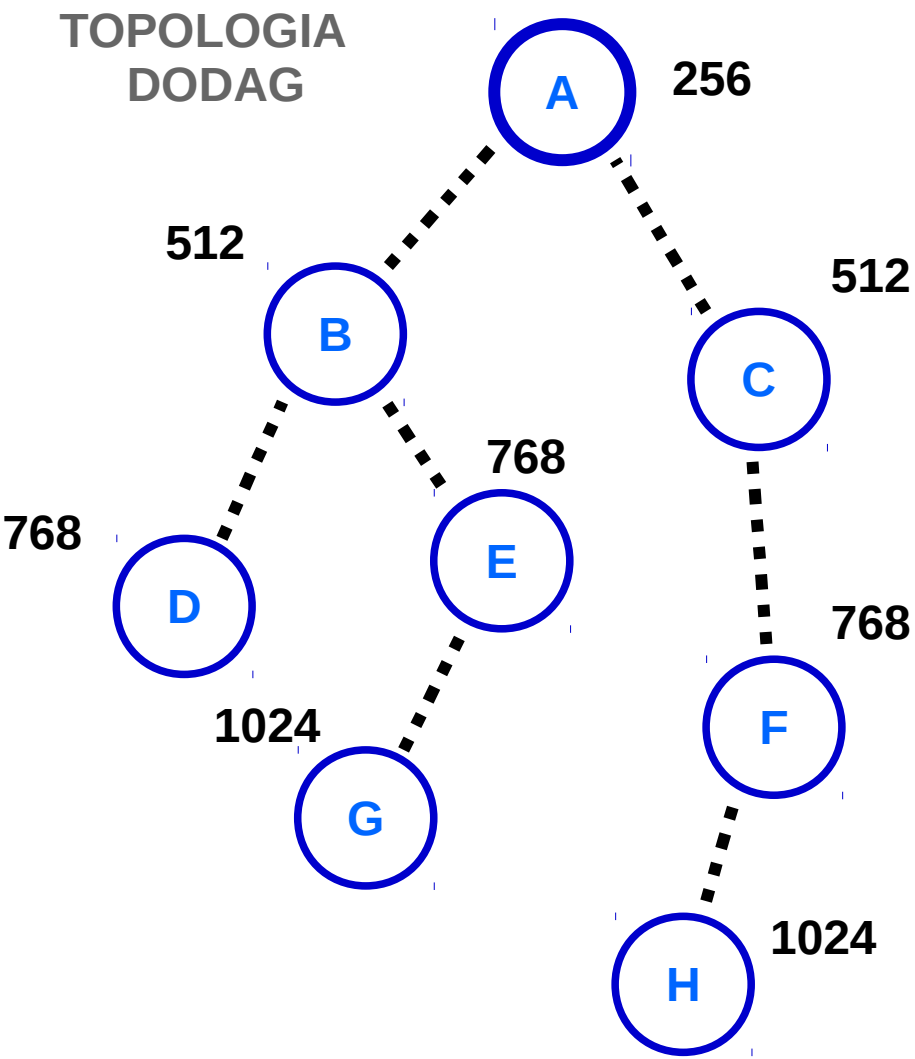
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



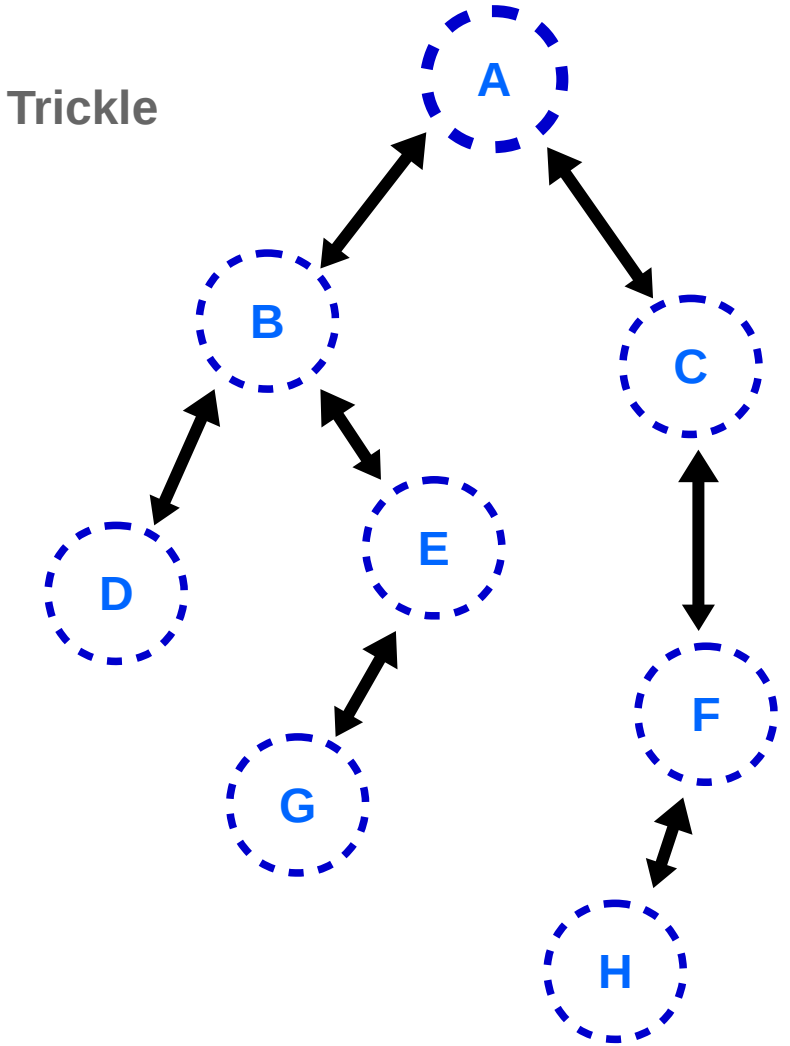
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)



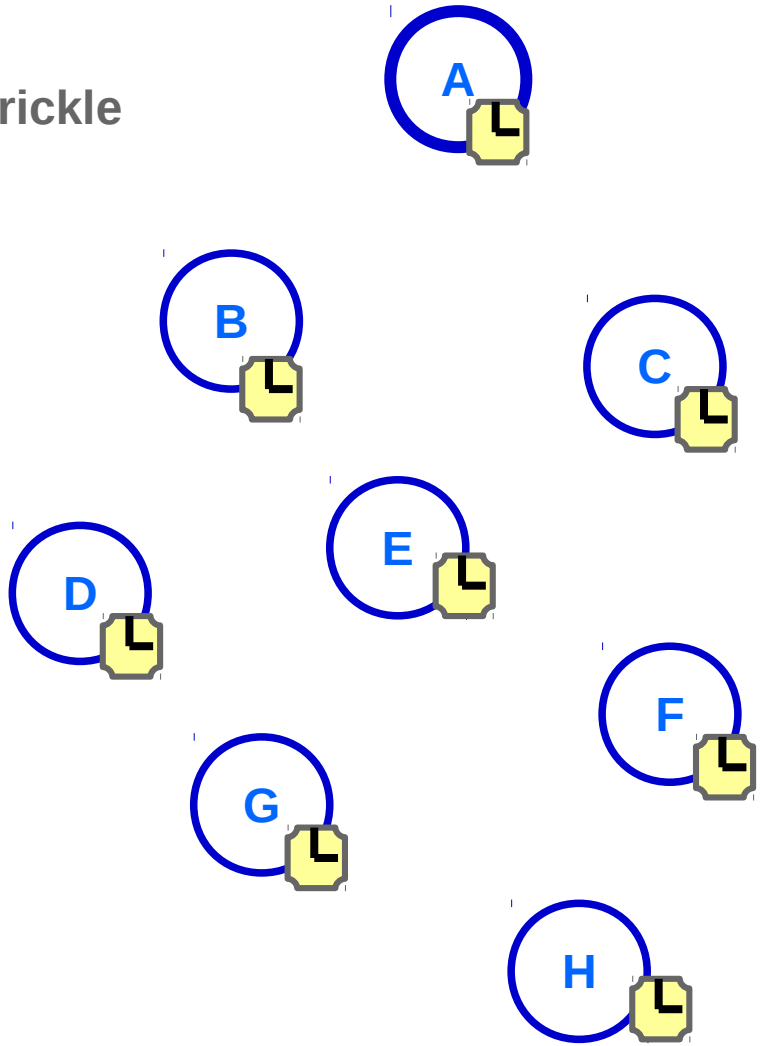
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)
- Mensagens de Controle (Trickle timer)



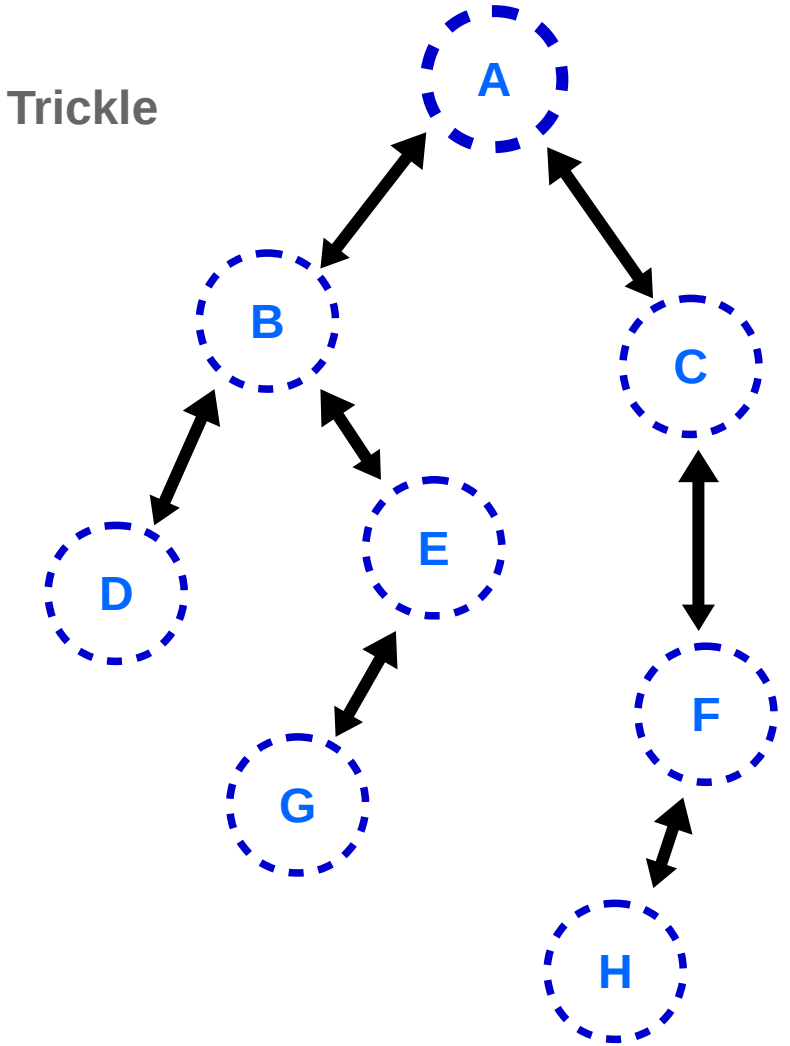
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)
- Mensagens de Controle (Trickle timer)



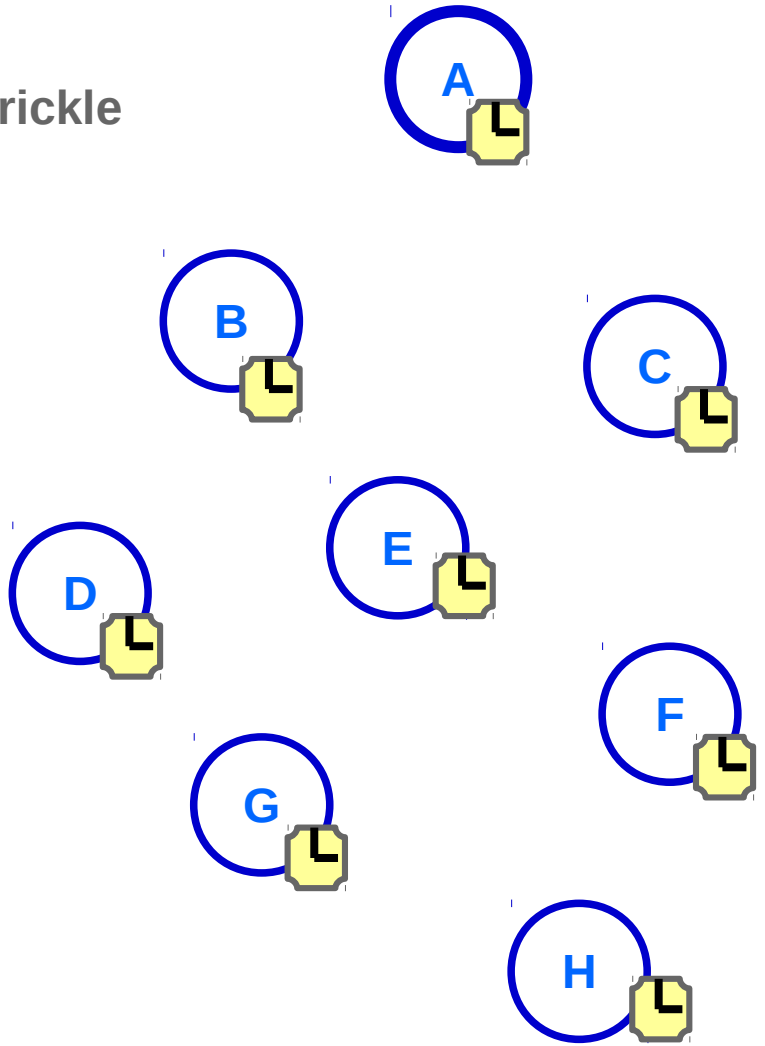
Convergência do Protocolo RPL:

- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)
- Mensagens de Controle (Trickle timer)

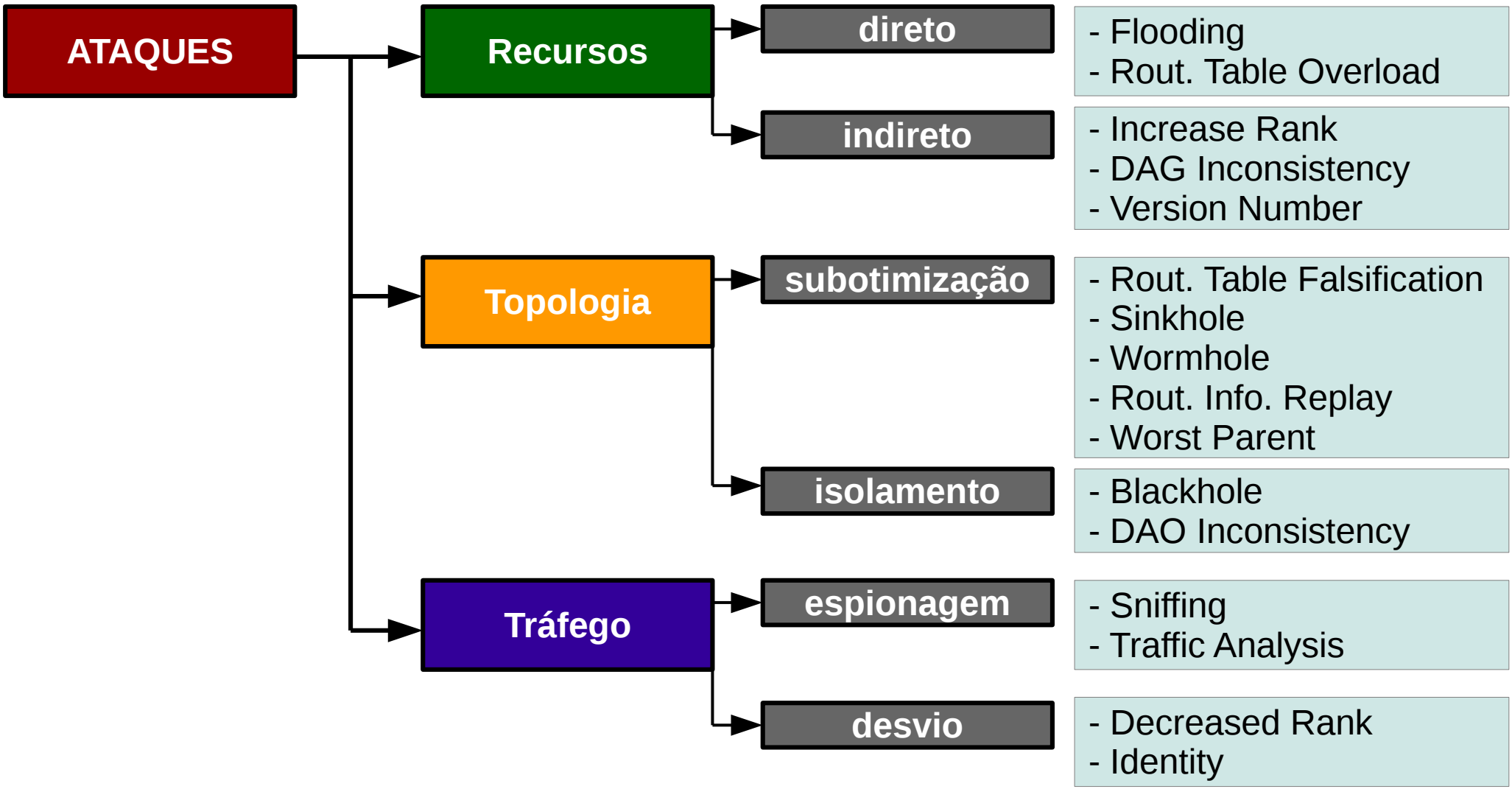


Convergência do Protocolo RPL:

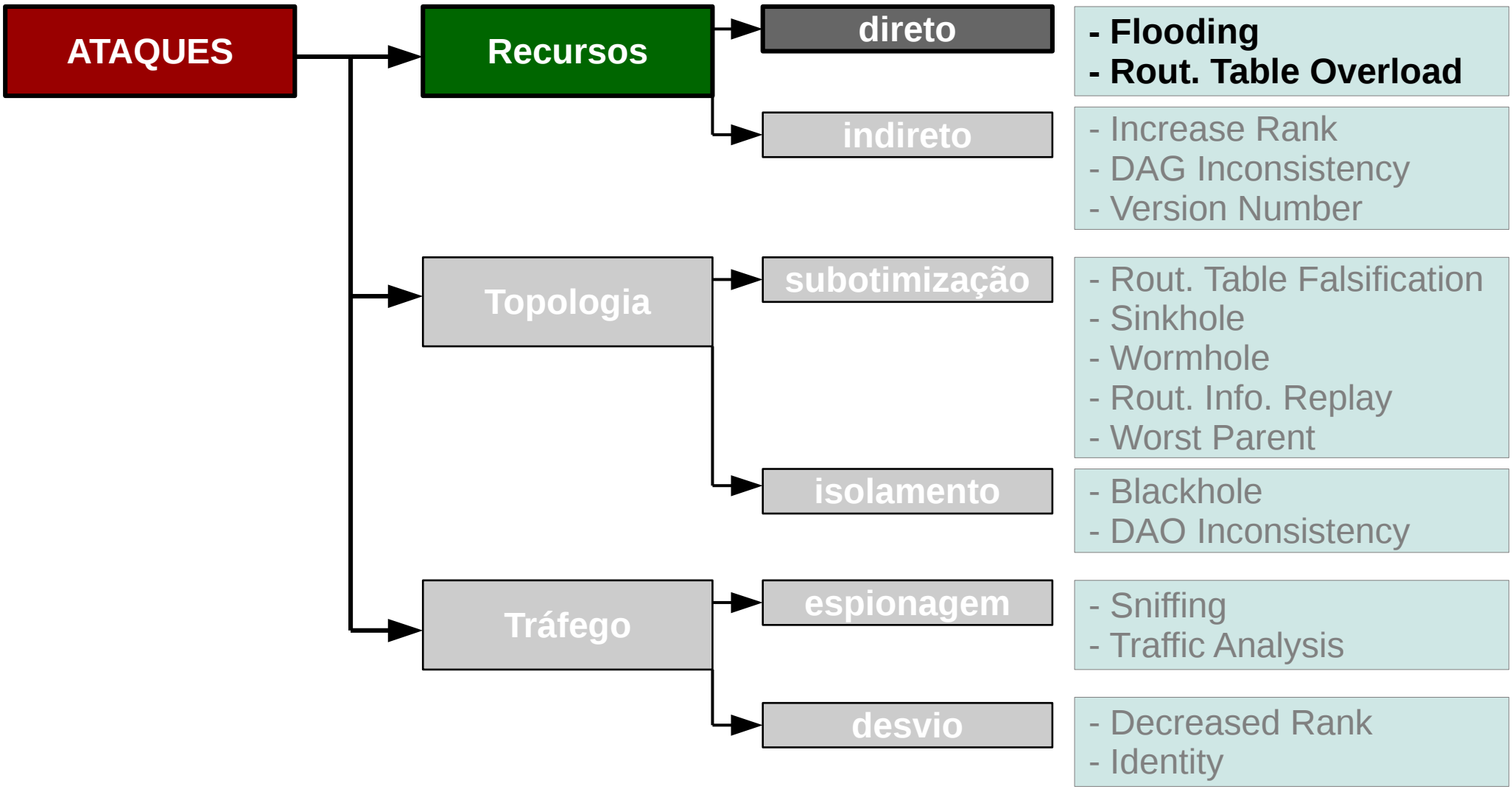
- Formar um DAG (grafo)
- Formar DODAG (um nó sink)
- Nó busca por topologia (DIS)
- Nó pai fornece informação (DIO)
- Nó confirma *upward* (DAO)
- Sink confirma *downward* (DAO-Ack)
- Mensagens de Controle (Trickle timer)



Ataques sobre RPL



Ataques sobre RPL



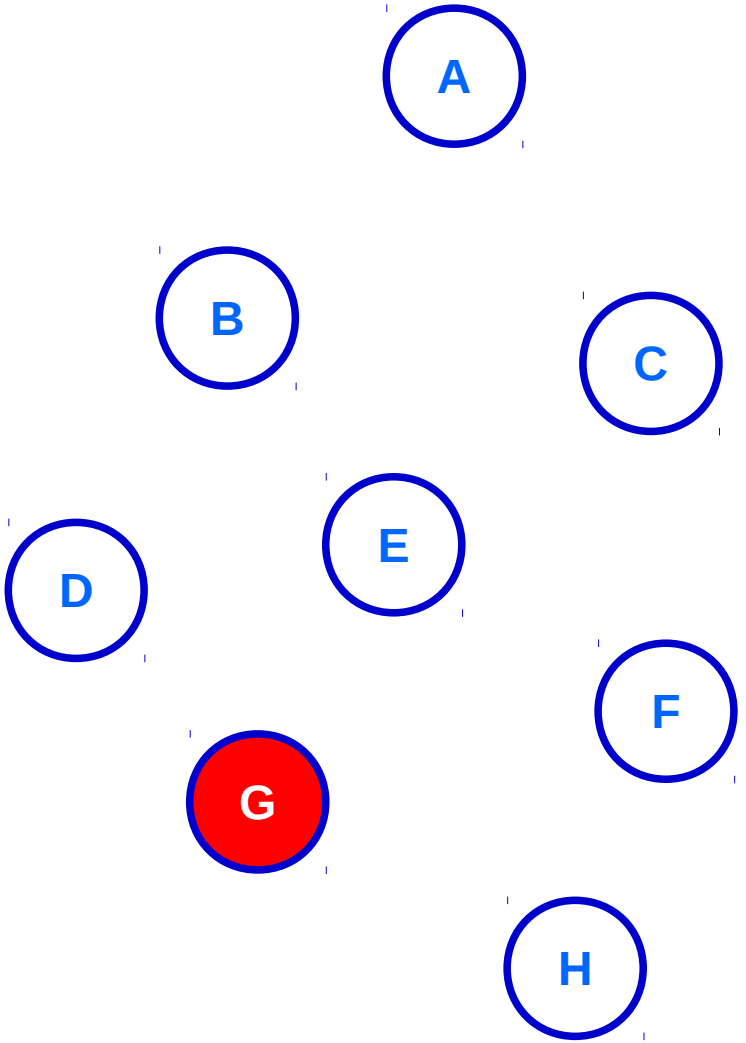
Ataque de Inundação
(Flooding Attack)

- Inundar com mensagens

Ataque de Inundação (Flooding Attack)

- Inundar com mensagens

- Mensagens DIS



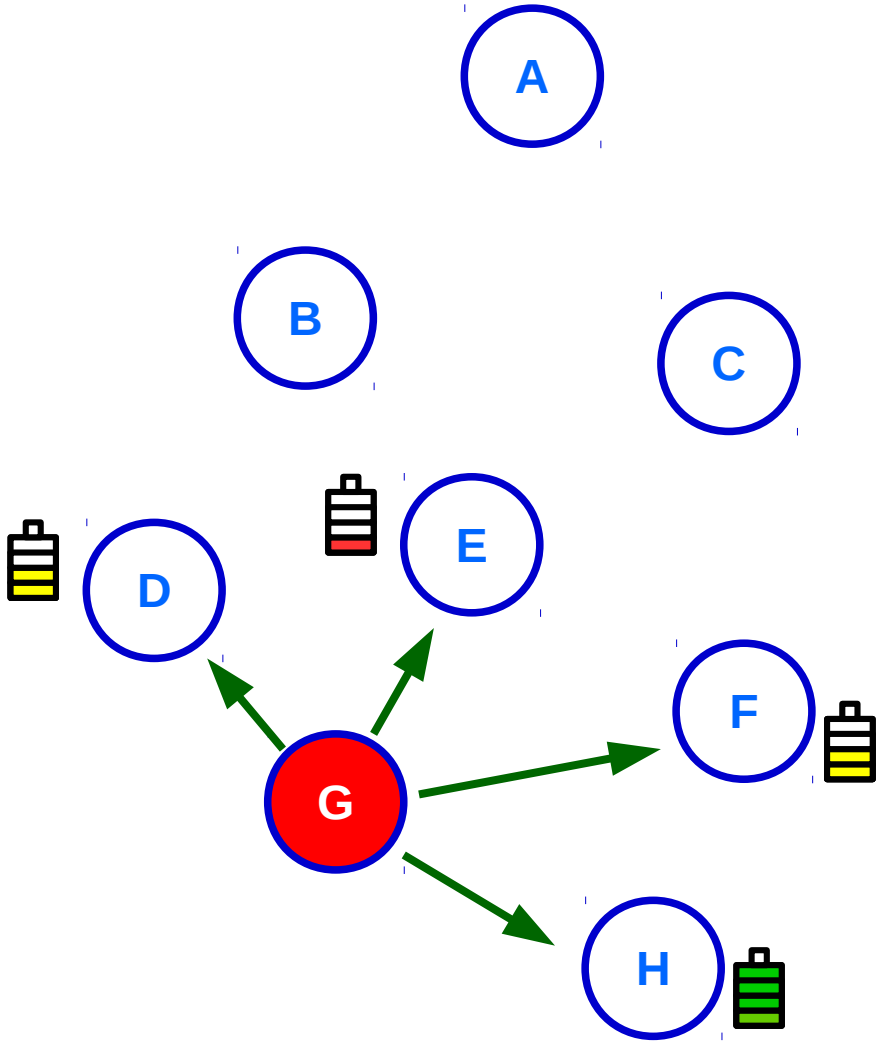
Ataque → Recursos - Direto

Ataque de Inundação (Flooding Attack)

- Inundar com mensagens

- Mensagens DIS

- Ignorar DIO



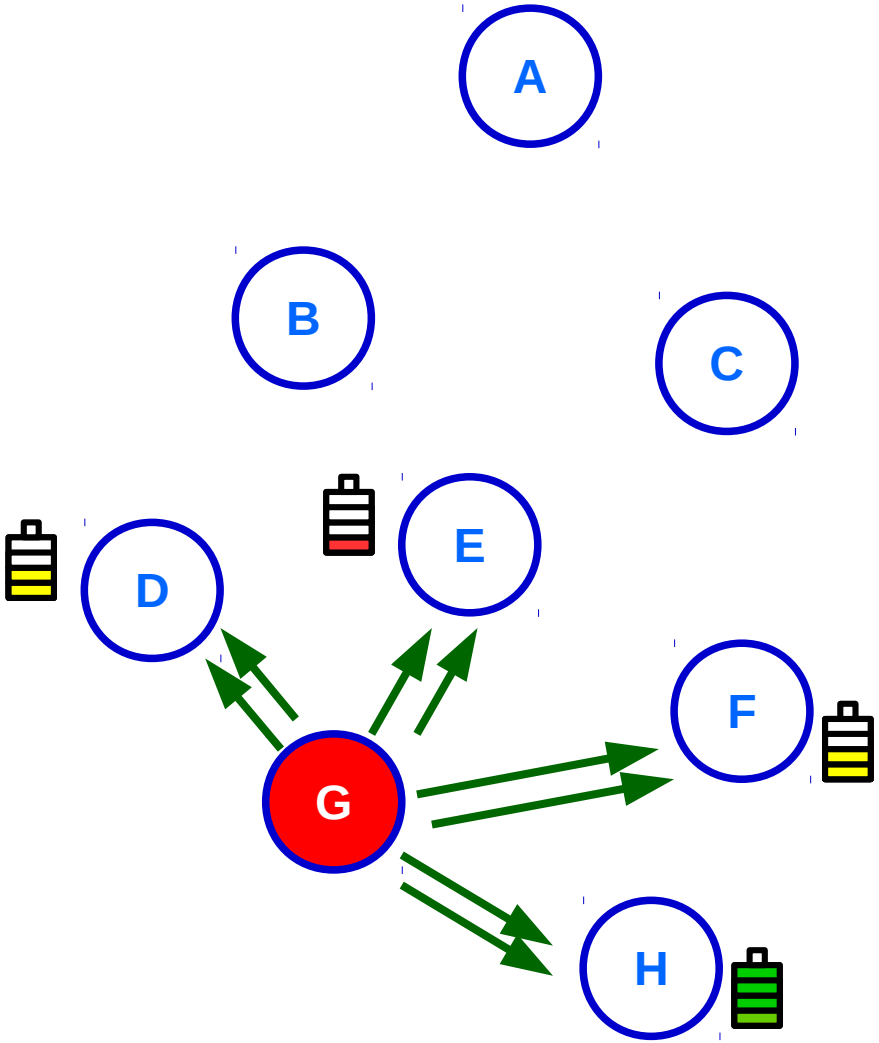
Ataque → Recursos - Direto

Ataque de Inundação (Flooding Attack)

- Inundar com mensagens

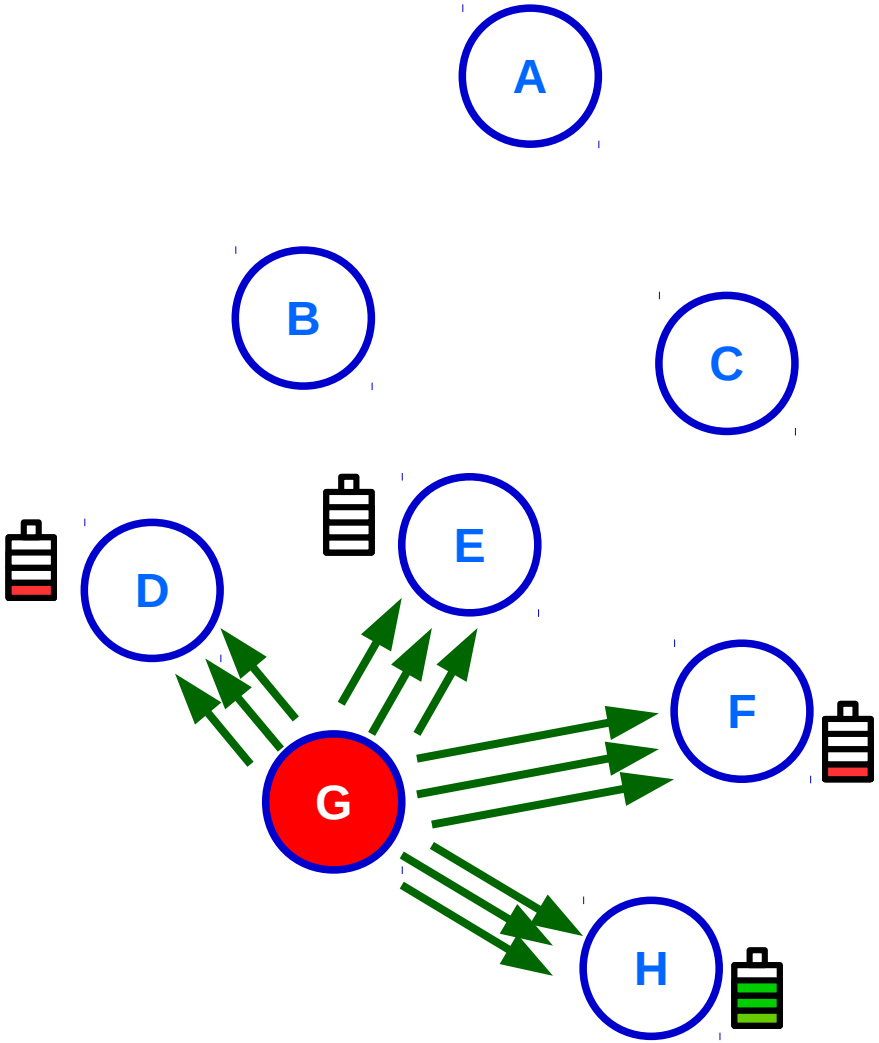
- Mensagens DIS

- Ignorar DIO



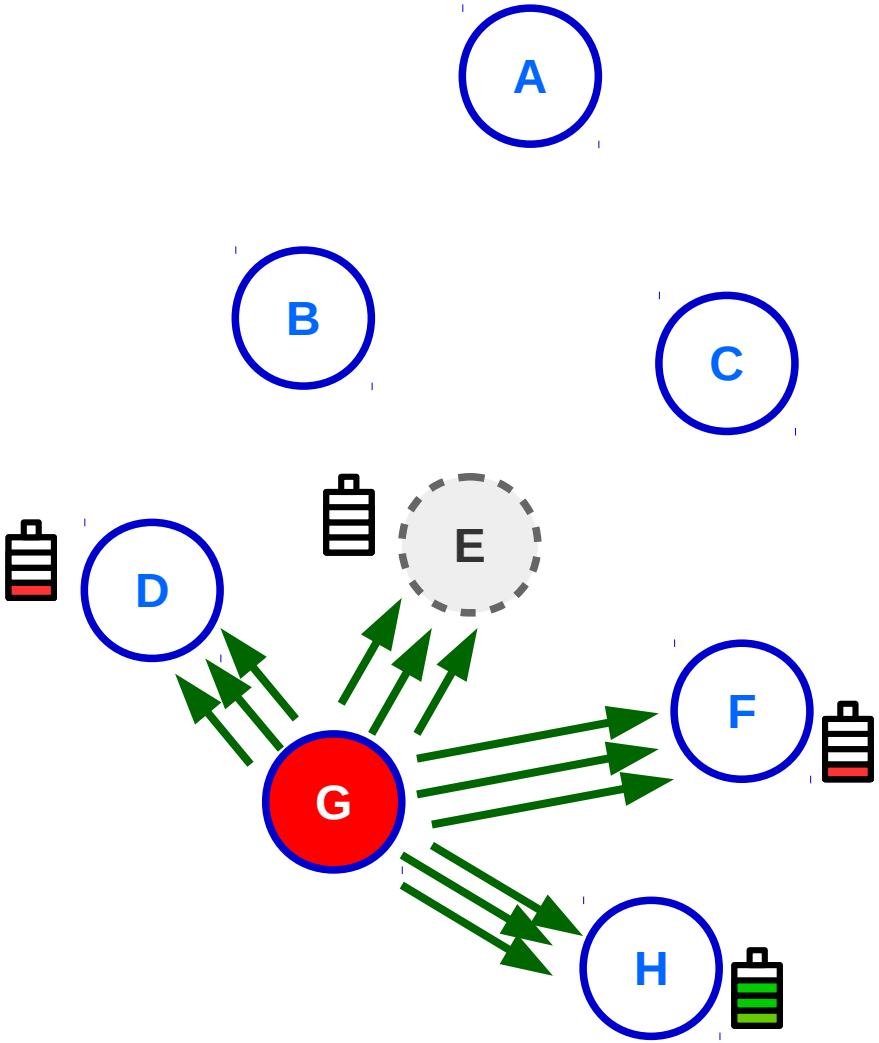
Ataque de Inundação (Flooding Attack)

- Inundar com mensagens
- Mensagens DIS
- Ignorar DIO
- Reiniciar contadores de Trickle



Ataque de Inundação (Flooding Attack)

- Inundar com mensagens
- Mensagens DIS
- Ignorar DIO
- Reiniciar contadores de Trickle
- Esgotar os recursos

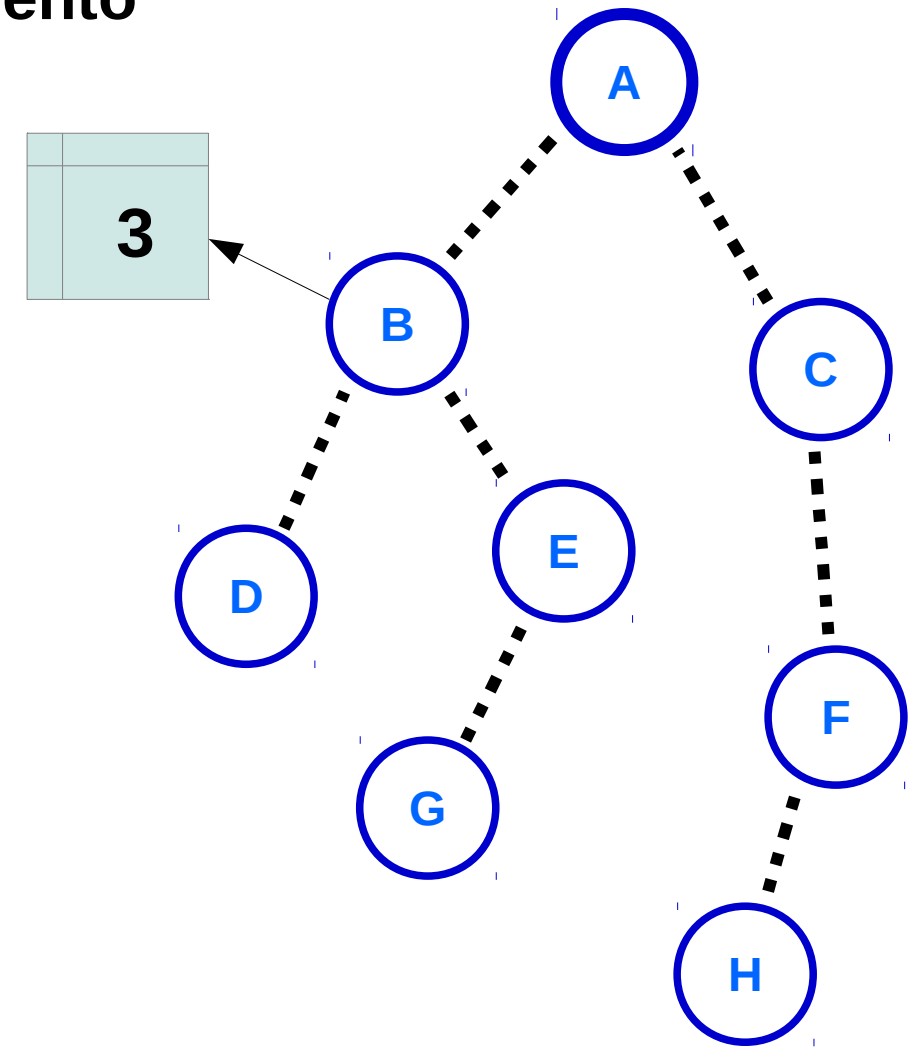


Sobrecarga da Tabela de Roteamento (Routing Table Overload)

- Modo armazenamento (storing)

Sobrecarga da Tabela de Roteamento (Routing Table Overload)

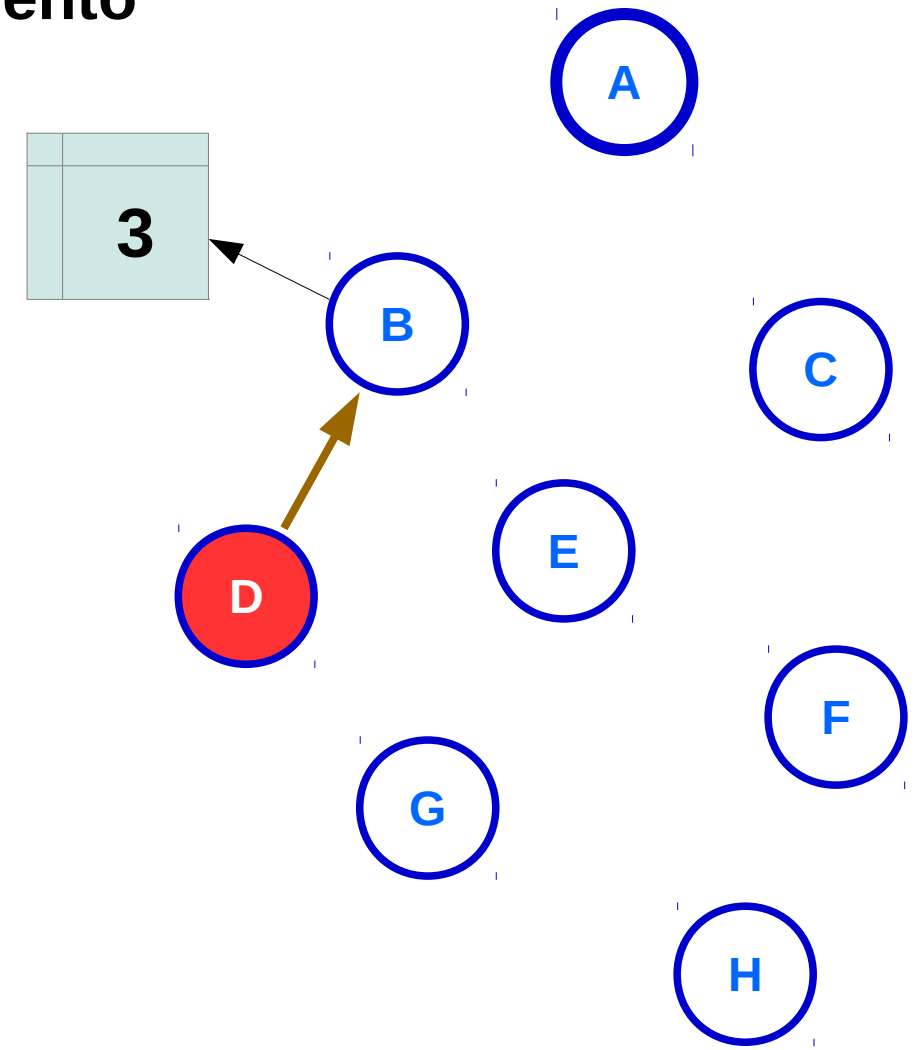
- Modo armazenamento (storing)



Sobrecarga da Tabela de Roteamento (Routing Table Overload)

- Modo armazenamento (storing)

- Mensagens DAO



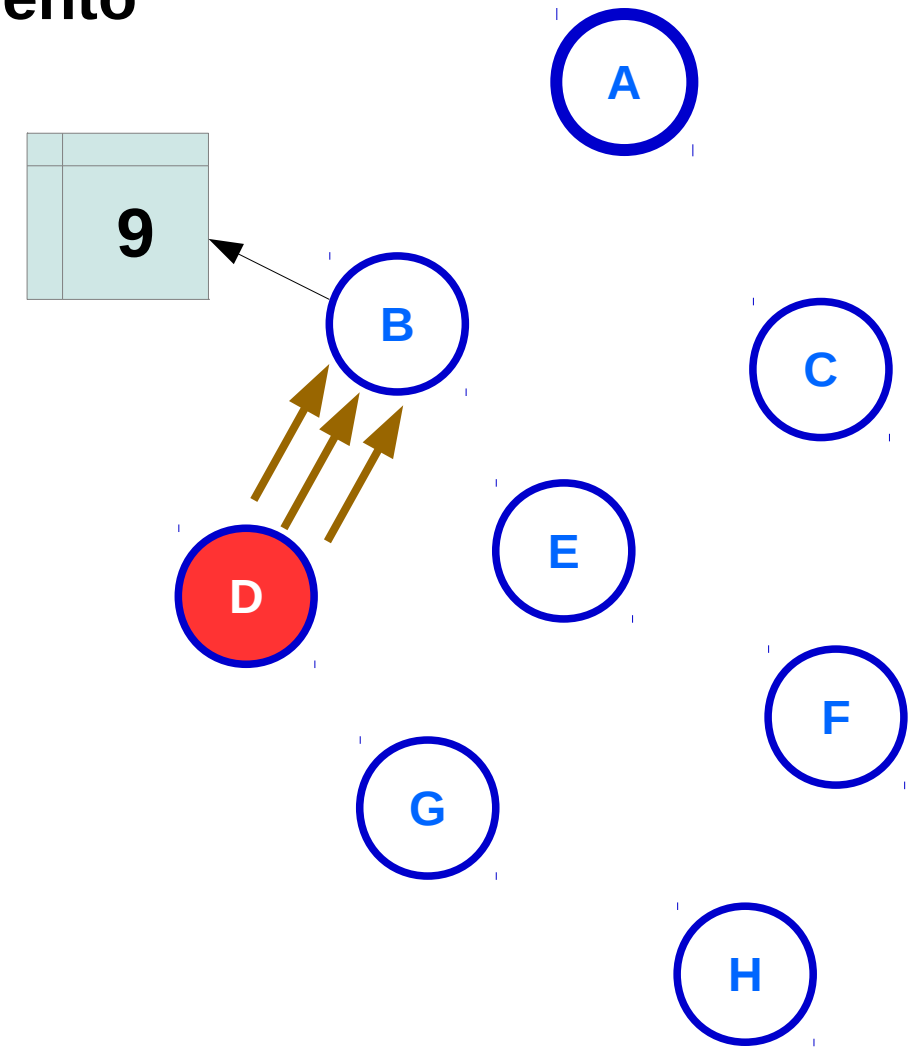
Ataque → Recursos - Direto

Sobrecarga da Tabela de Roteamento (Routing Table Overload)

- Modo armazenamento (storing)

- Mensagens DAO

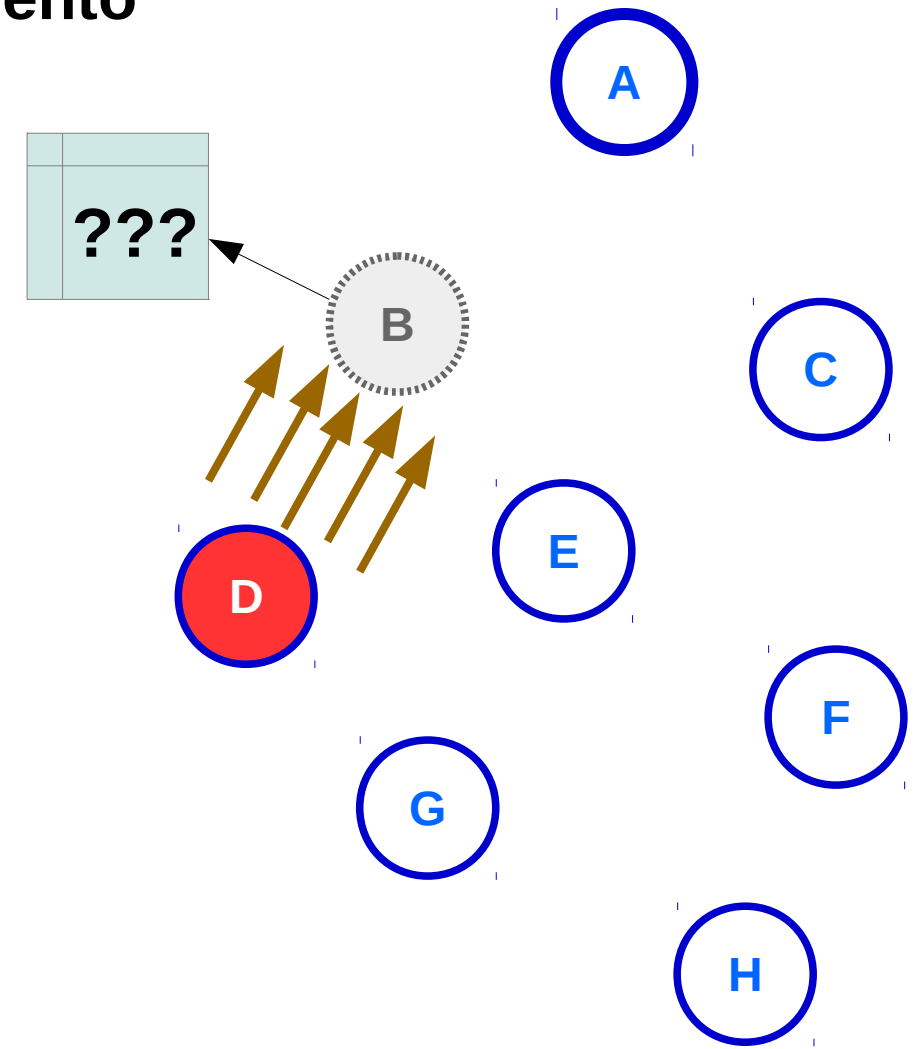
- Novas rotas (falsas)



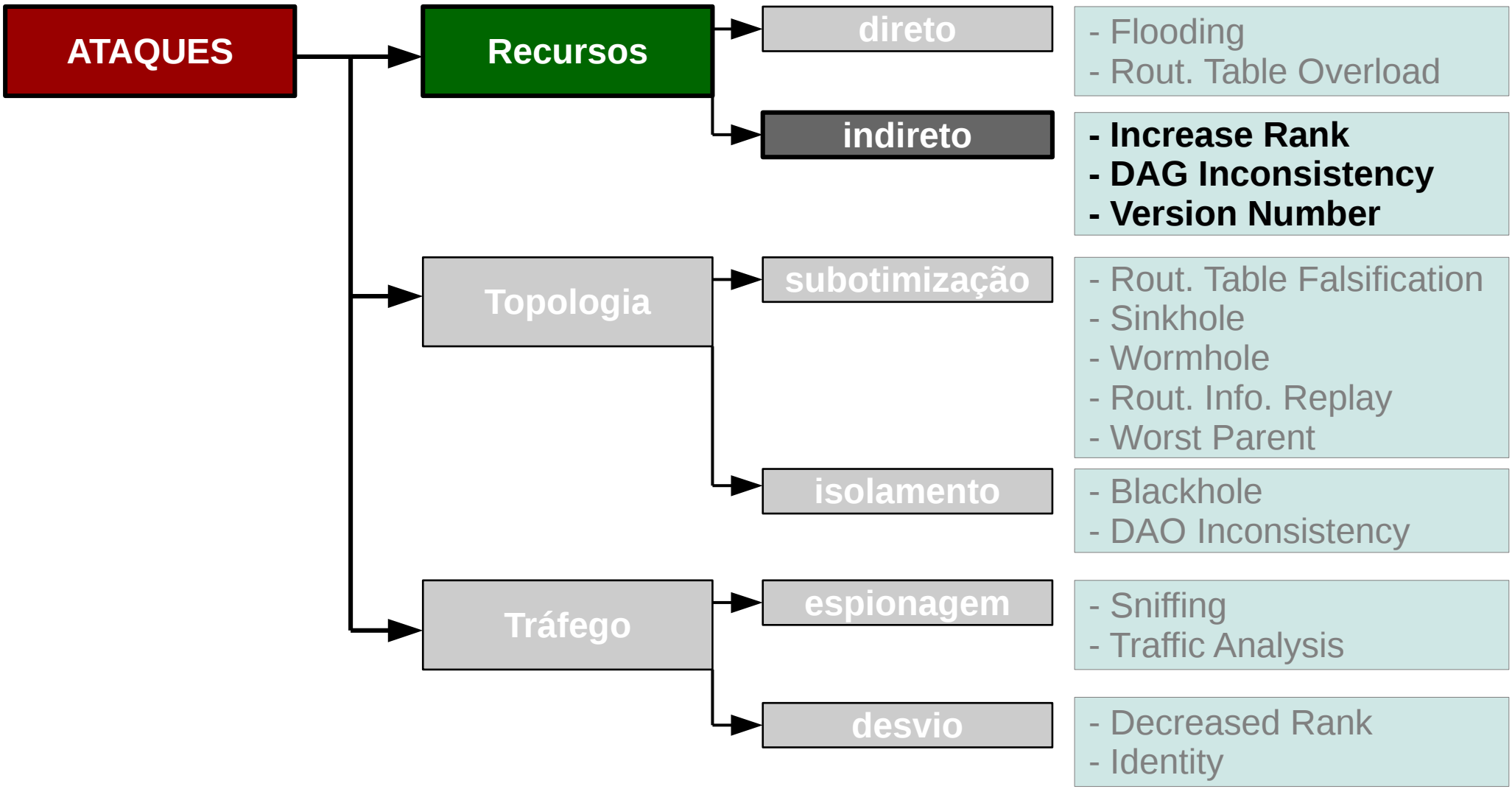
Ataque → Recursos - Direto

Sobrecarga da Tabela de Roteamento (Routing Table Overload)

- Modo armazenamento (storing)
- Mensagens DAO
- Novas rotas (falsas)
- Sobrecarga (Overload)



Ataques sobre RPL

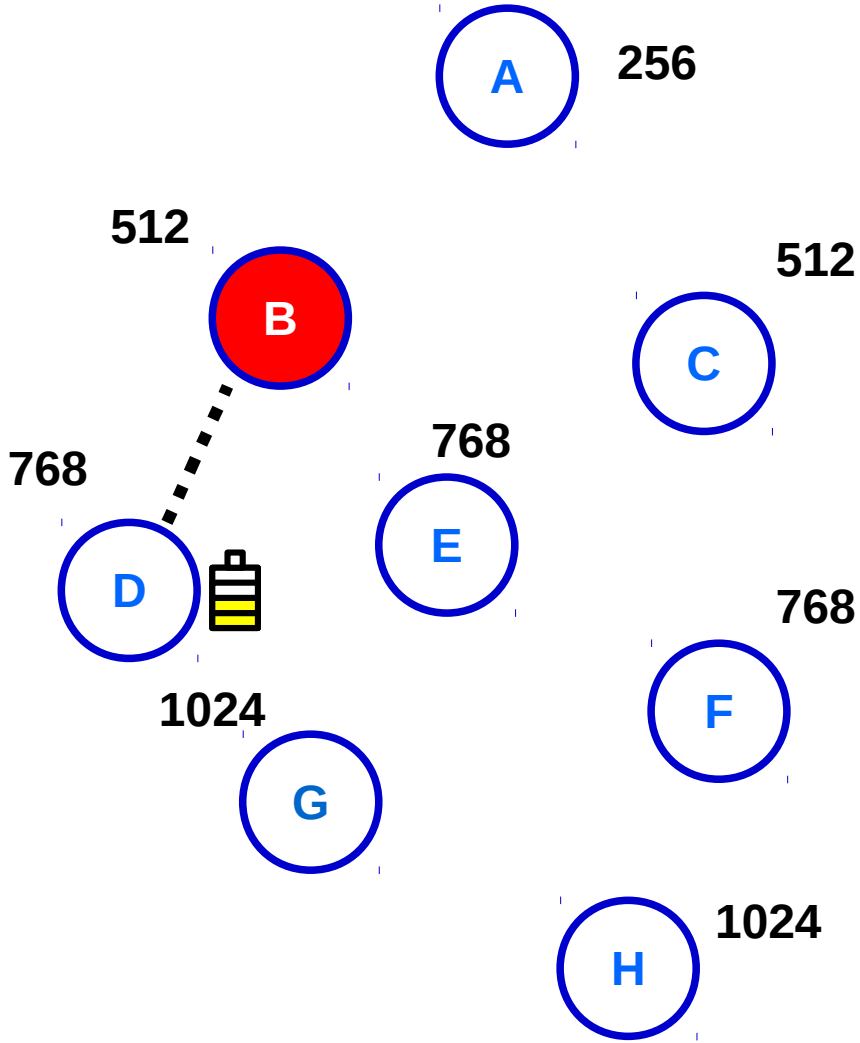


Ataque de Incremento de Rank (Increase Rank Attack)

- O nó é pai da sua vítima

Ataque de Incremento de Rank (Increase Rank Attack)

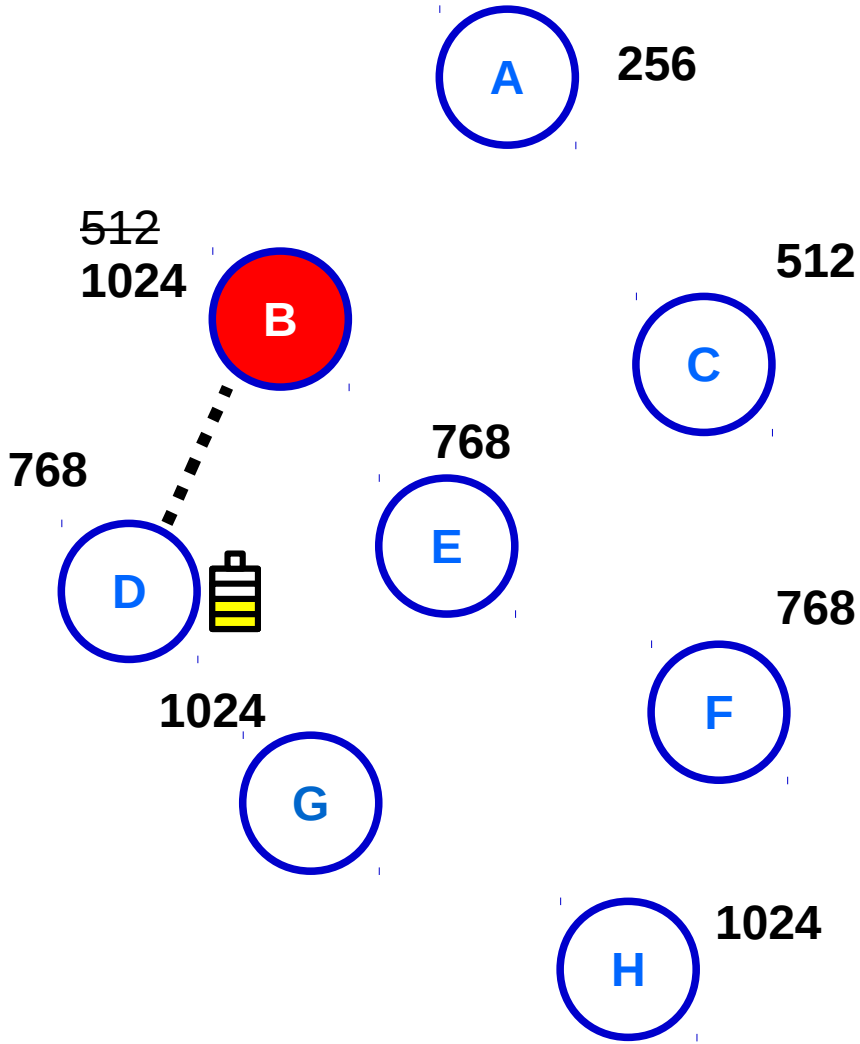
- O nó é pai da sua vítima



Ataque de Incremento de Rank (Increase Rank Attack)

- O nó é pai da sua vítima (vice-versa)

- O atacante aumenta o Rank

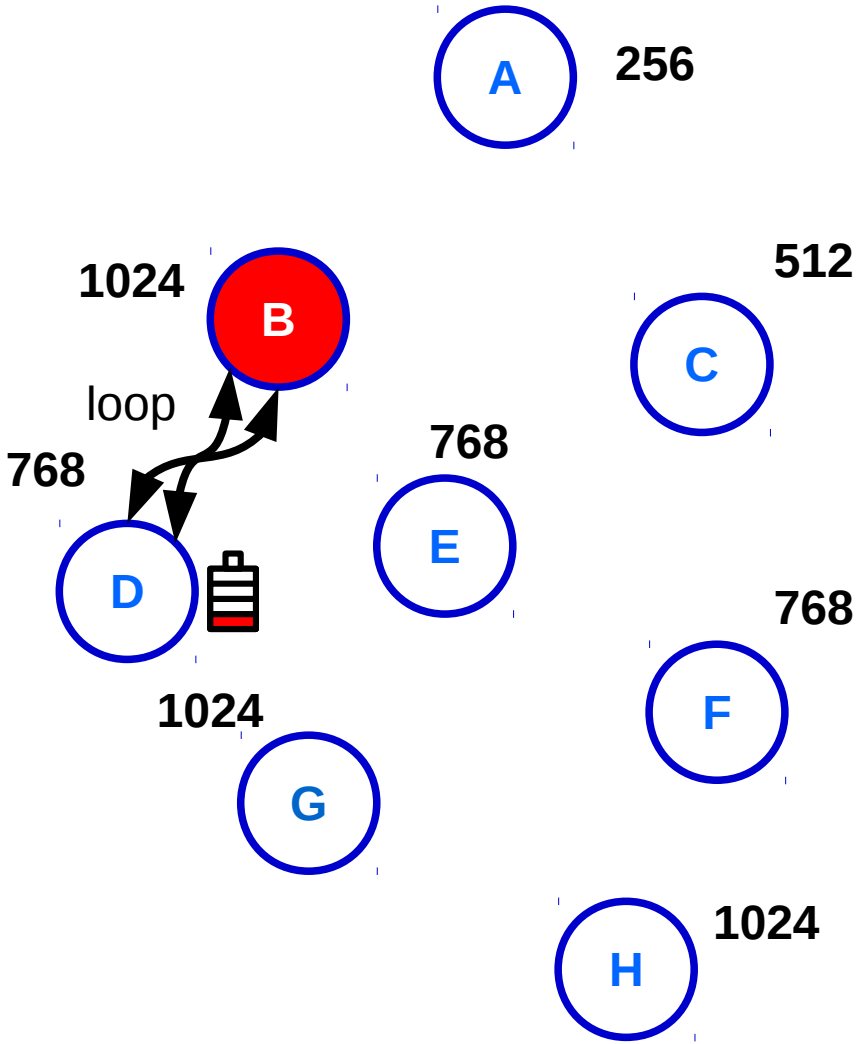


Ataque de Incremento de Rank (Increase Rank Attack)

- O nó é pai da sua vítima (vice-versa)

- O atacante aumenta o Rank

- Looping de roteamento

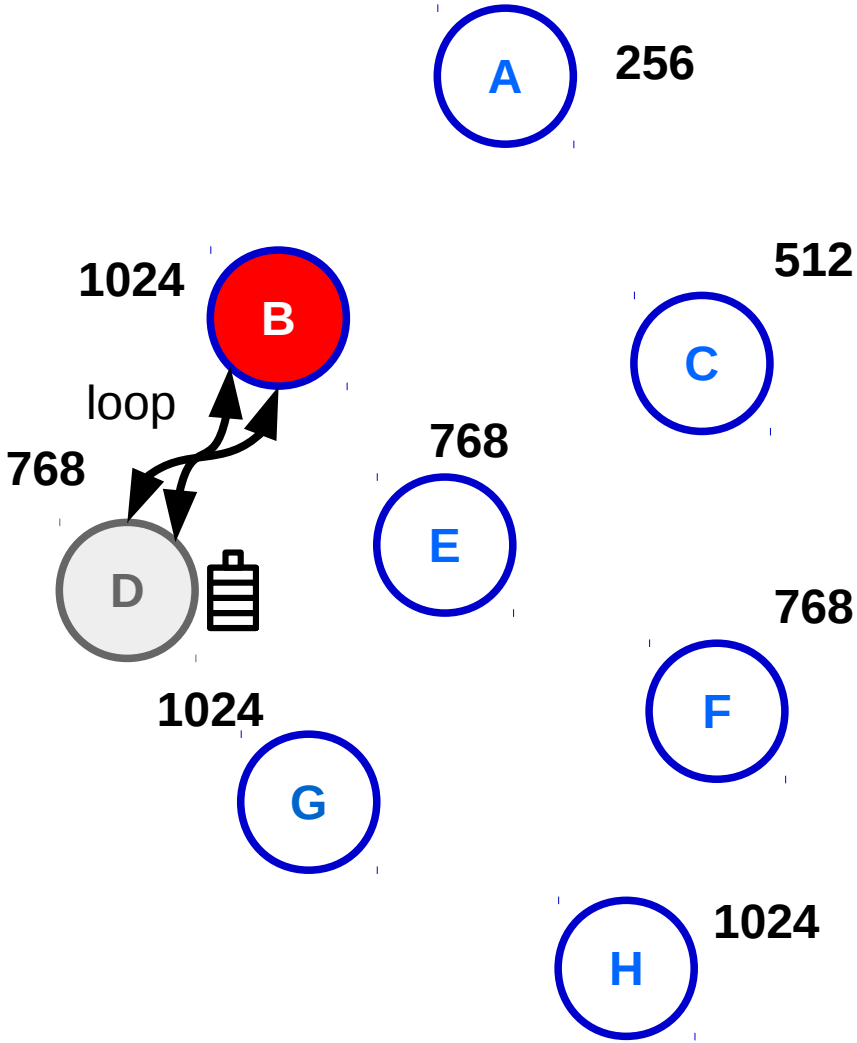


Ataque de Incremento de Rank (Increase Rank Attack)

- O nó é pai da sua vítima (vice-versa)

- O atacante aumenta o Rank

- Esgotamento de Recursos



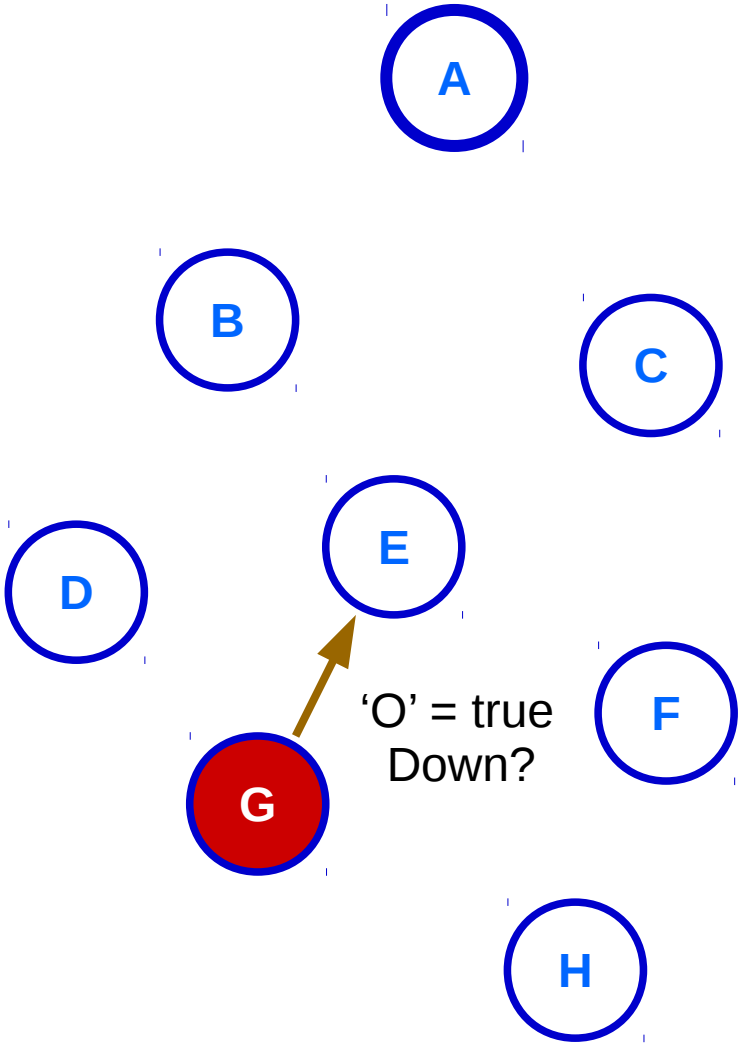
Ataque de Inconsistência DAG (DAG Inconsistency Attack)

- Flag ‘O’ identifica inconsistência

Ataque de Inconsistência DAG (DAG Inconsistency Attack)

- Flag ‘O’ identifica inconsistência

- Atacante forja flag ‘O’

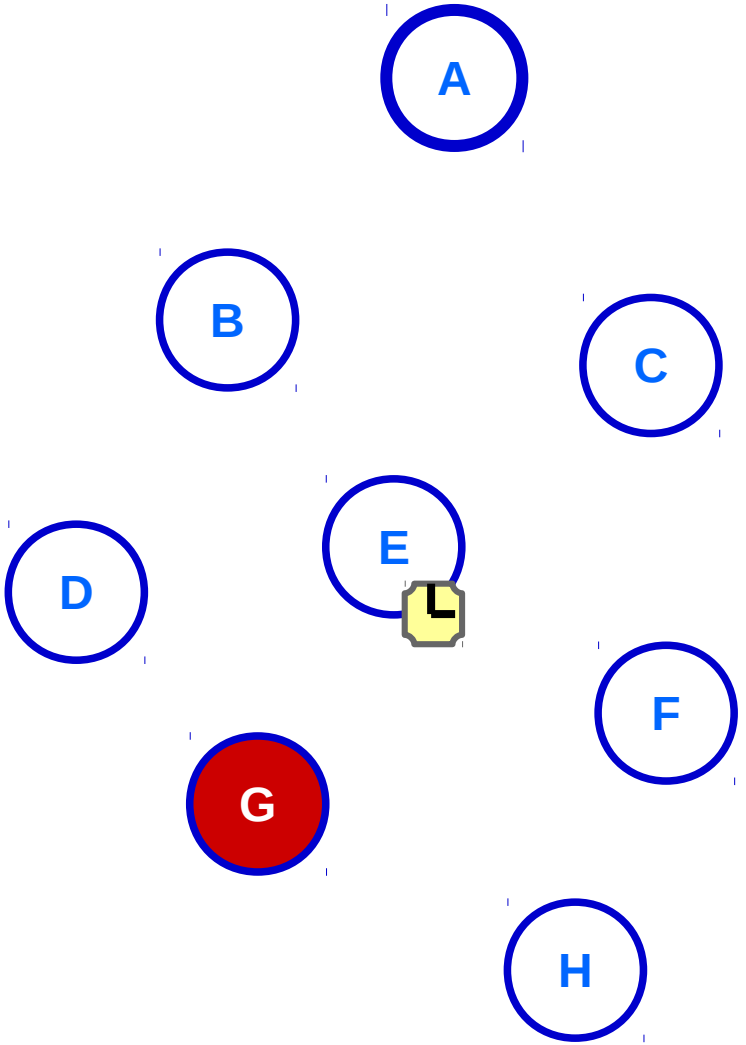


Ataque de Inconsistência DAG (DAG Inconsistency Attack)

- Flag ‘O’ identifica inconsistência

- Atacante forja flag ‘O’

- Inconsistência! Resetar timers (trickle)



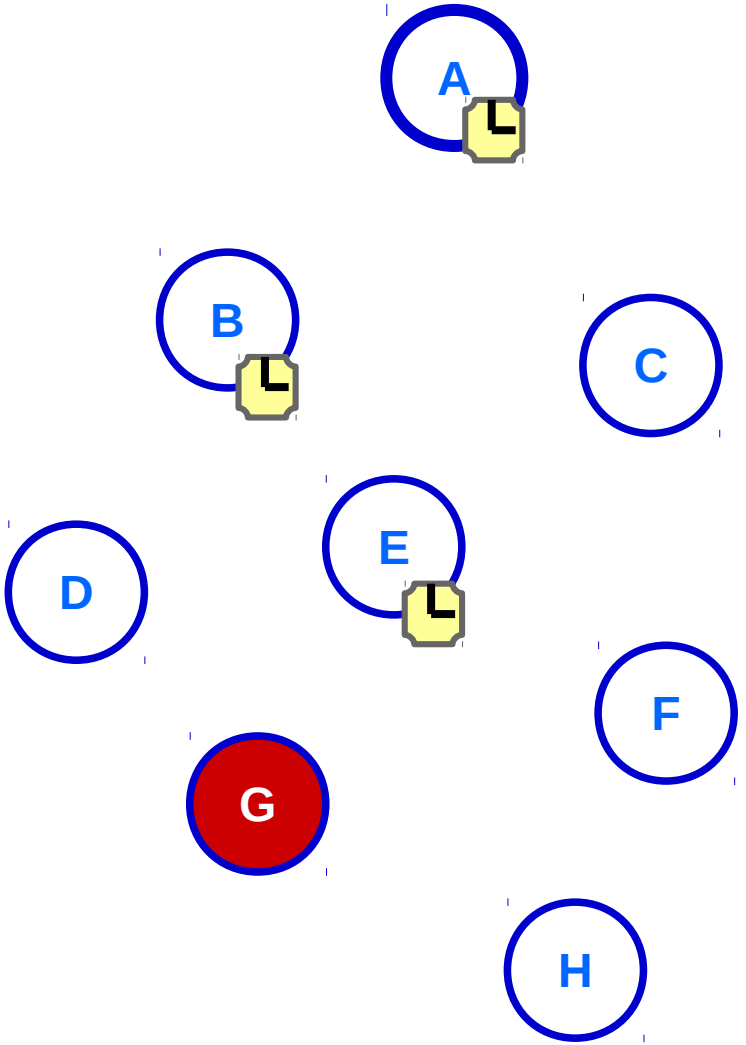
Ataque de Inconsistência DAG (DAG Inconsistency Attack)

- Flag ‘O’ identifica inconsistência

- Atacante forja flag ‘O’

- Inconsistência! Resetar timers (trickle)

- Recursos são desperdiçados



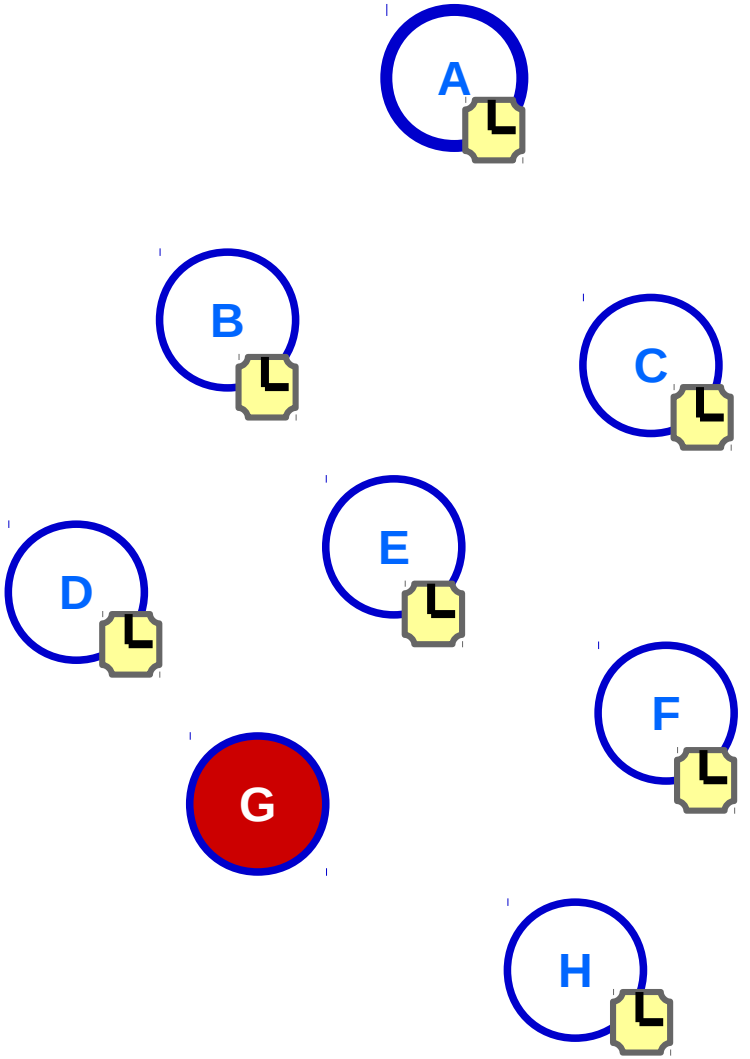
Ataque de Inconsistência DAG (DAG Inconsistency Attack)

- Flag ‘O’ identifica inconsistência

- Atacante forja flag ‘O’

- Inconsistência! Resetar timers (trickle)

- Recursos são desperdiçados

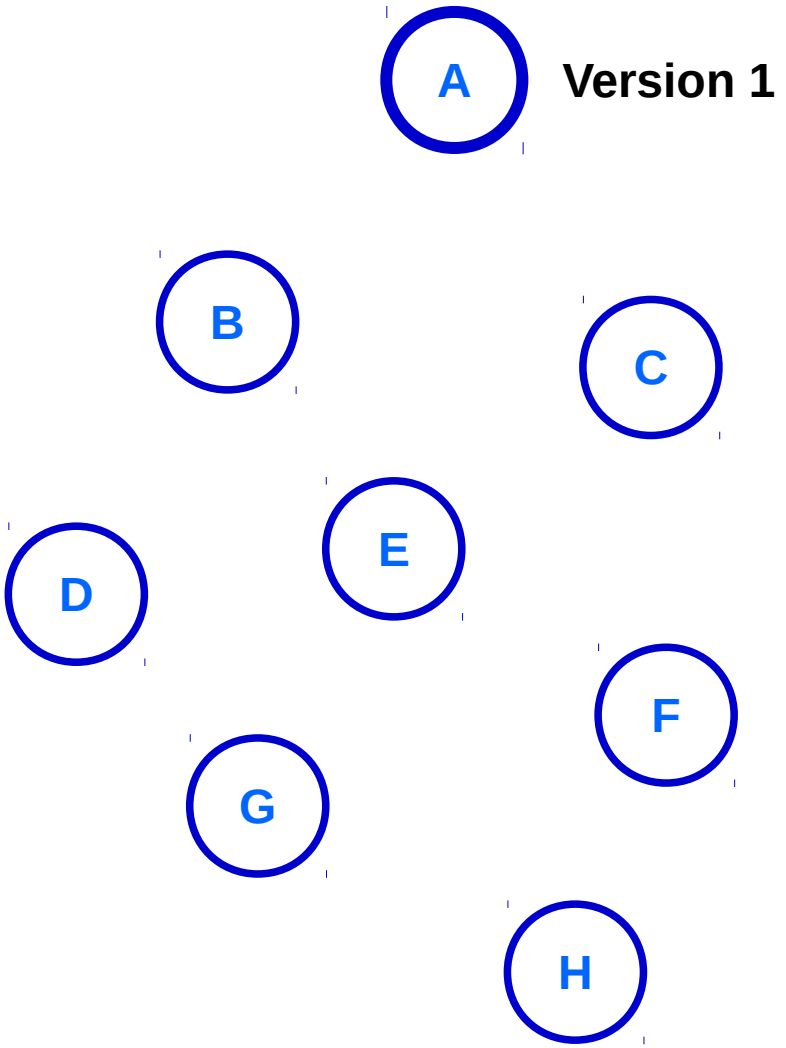


Ataque ao Número de Versão
(Version Number Attack)

- Versão da DODAG (controle do sink)

Ataque ao Número de Versão (Version Number Attack)

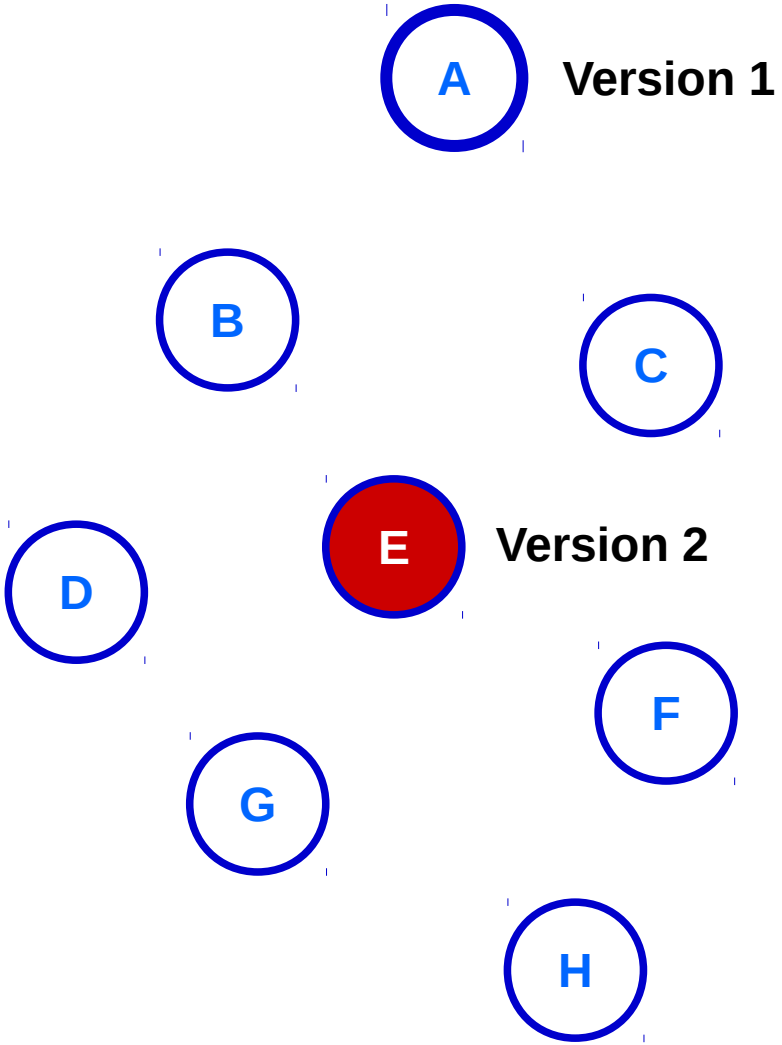
- Versão da DODAG (controle do sink)



Ataque ao Número de Versão (Version Number Attack)

- Versão da DODAG (somente sink)

- Atacante fornece nova versão

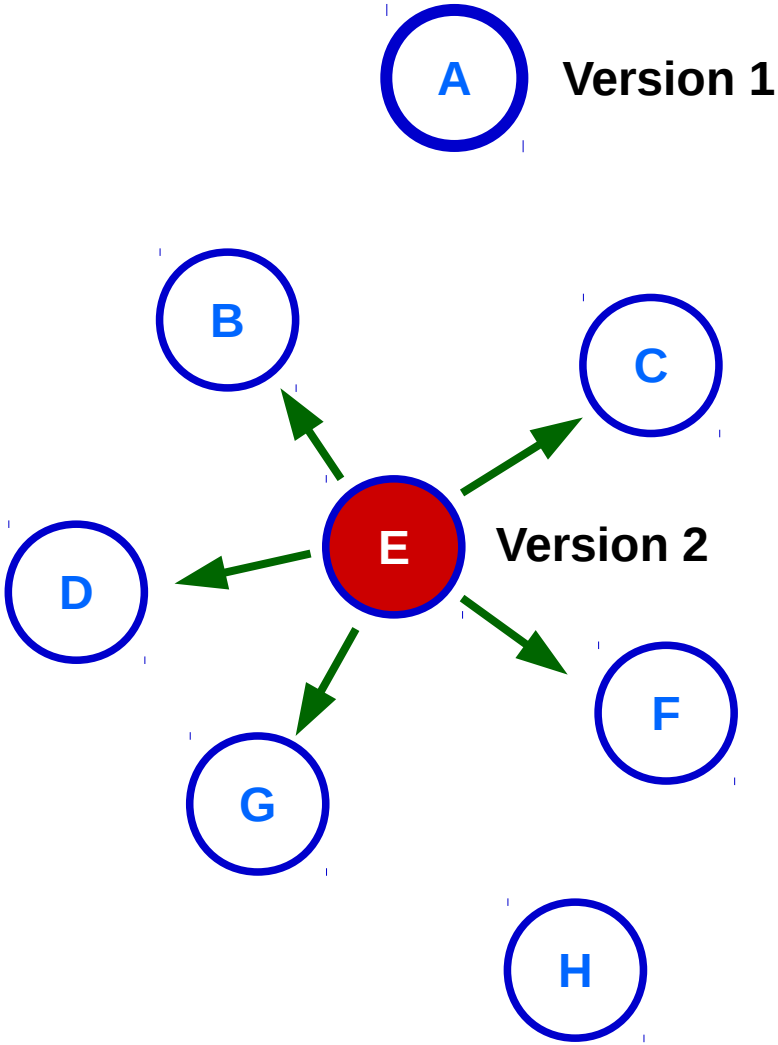


Ataque ao Número de Versão (Version Number Attack)

- Versão da DODAG (somente sink)

- Atacante fornece nova versão

- Força reconstrução da DODAG



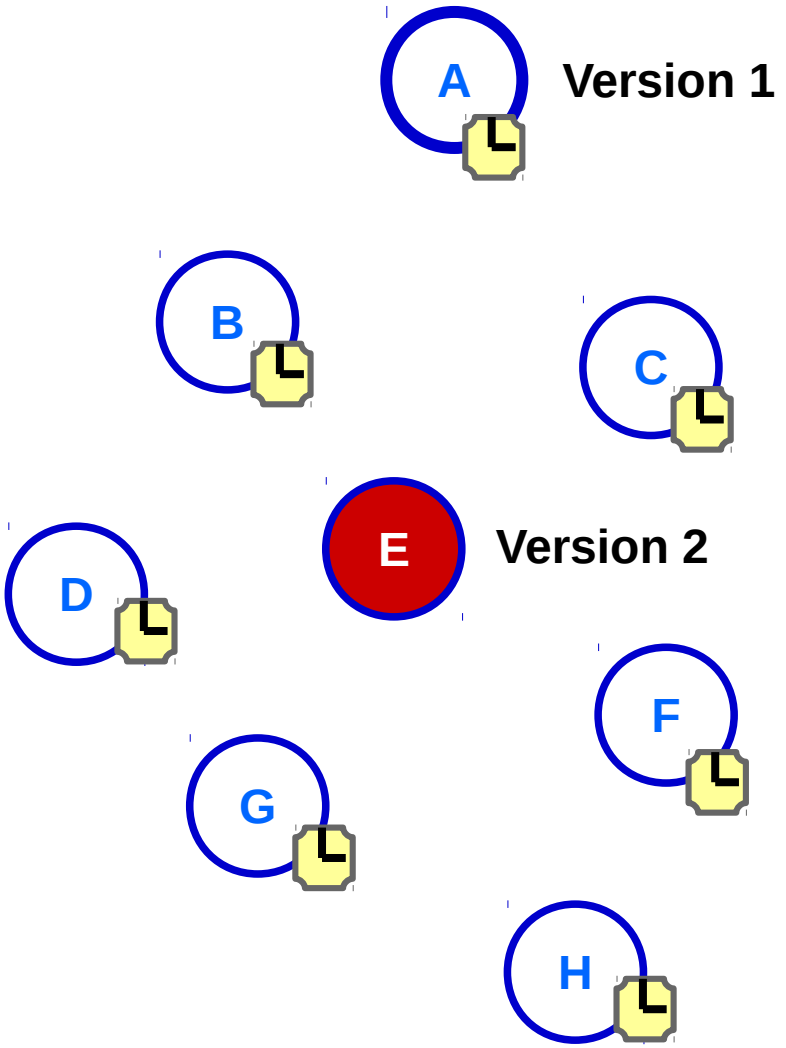
Ataque ao Número de Versão (Version Number Attack)

- Versão da DODAG (somente sink)

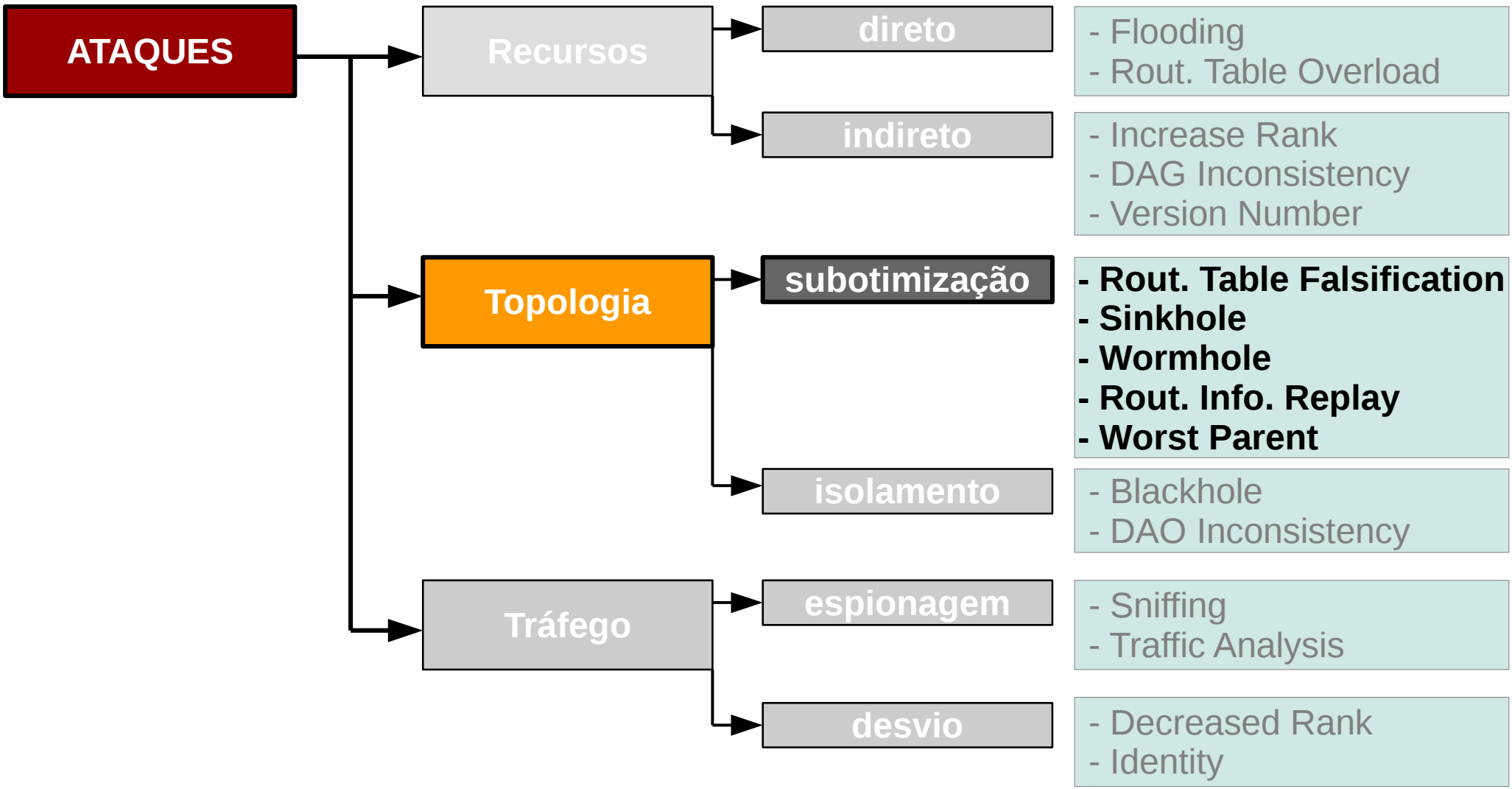
- Atacante fornece nova versão

- Força reconstrução da DODAG

- Desperdício de recursos



Ataques sobre RPL



UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

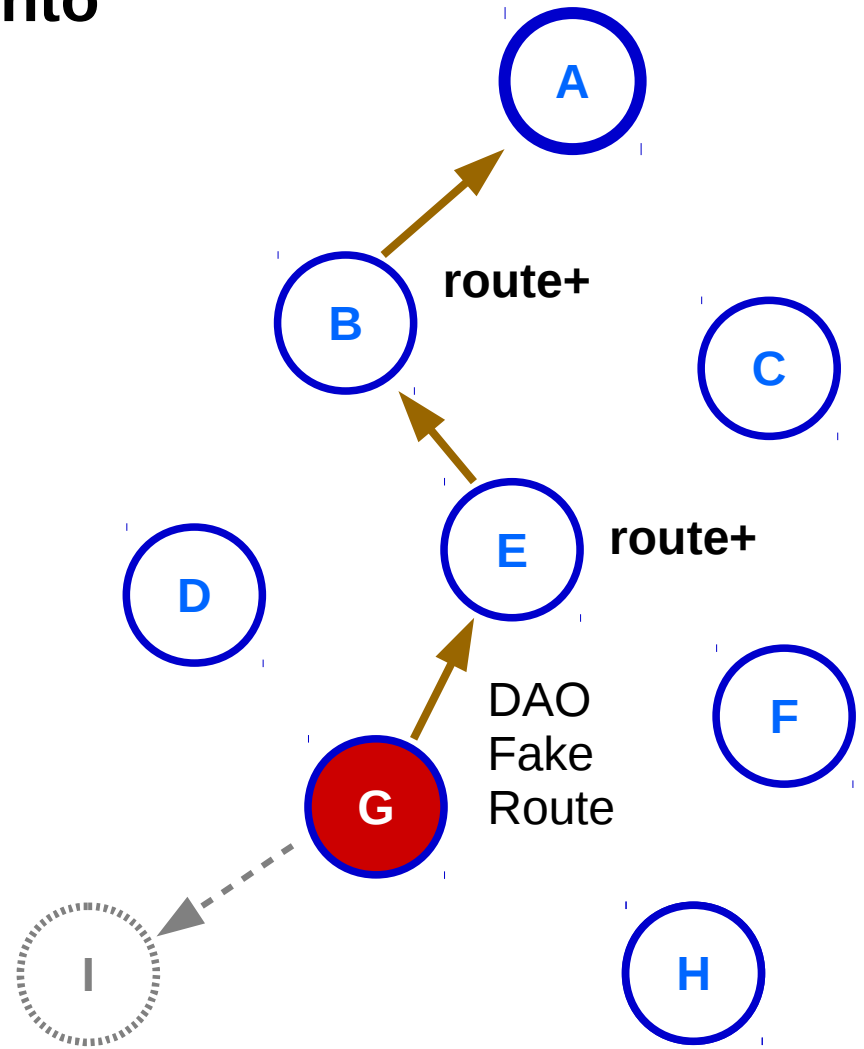
Falsificação de Tabela de Roteamento (Routing Table Falsification)

- Nó pai permite rotas (store mode)

Falsificação de Tabela de Roteamento (Routing Table Falsification)

- Nó pai permite rotas (store mode)

- Rotas falsas são armazenadas

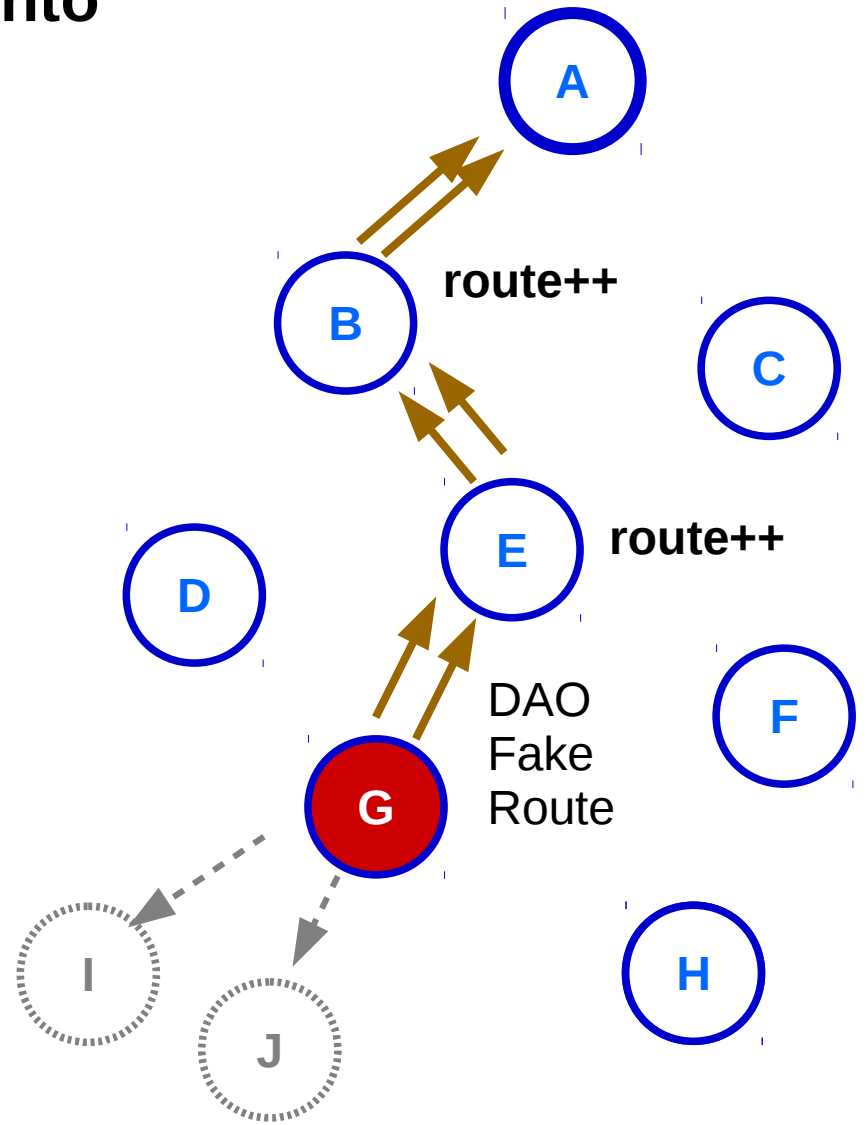


Falsificação de Tabela de Roteamento (Routing Table Falsification)

- Nó pai permite rotas (store mode)

- Rotas falsas são armazenadas

- Degradação da rede

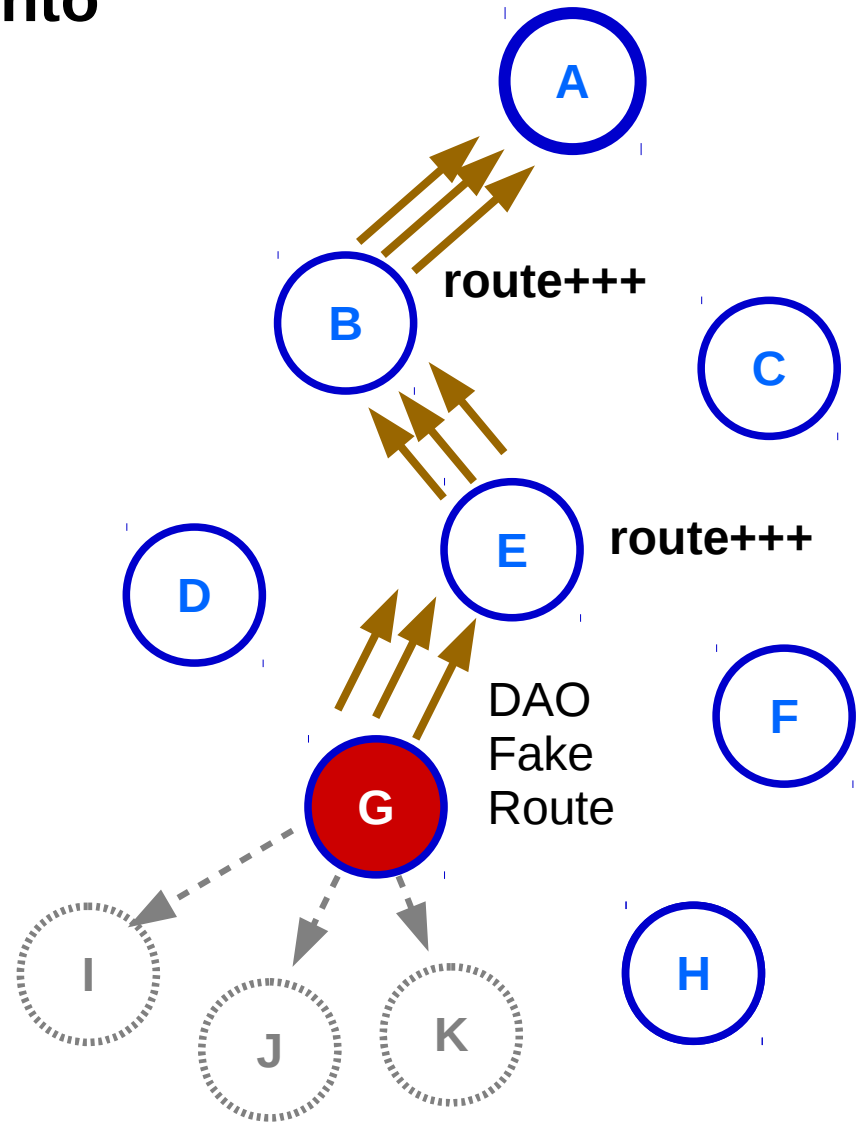


Falsificação de Tabela de Roteamento (Routing Table Falsification)

- Nó pai permite rotas (store mode)

- Rotas falsas são armazenadas

- Degradação da rede



UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

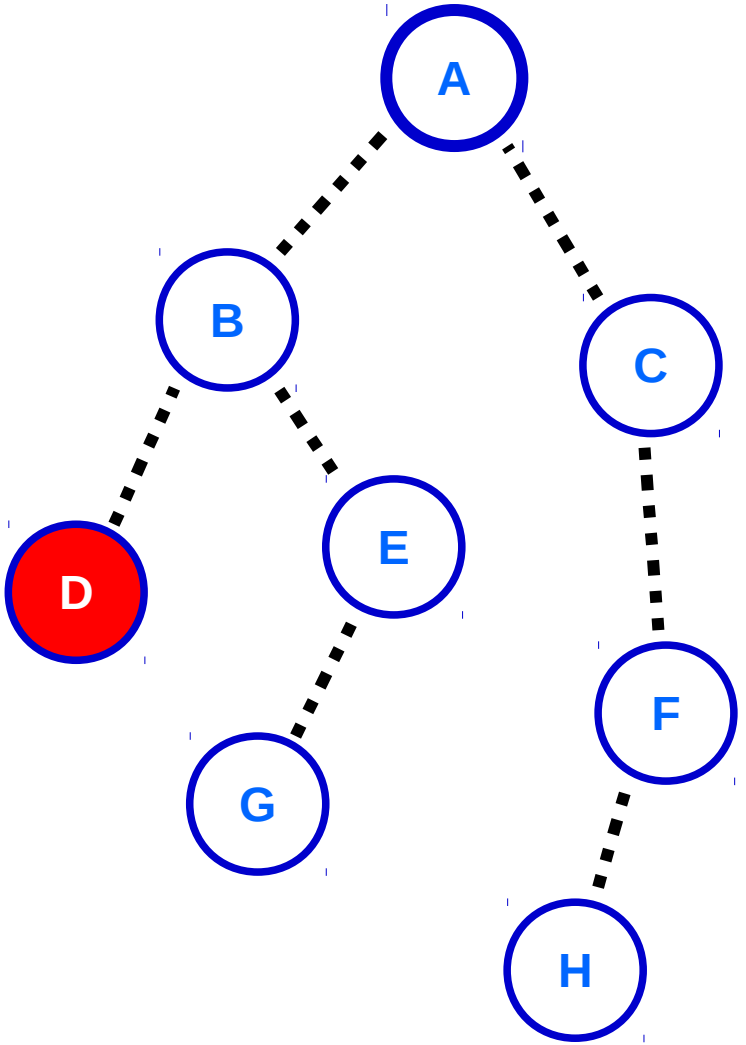
Ataque do Buraco de Escoamento (Sinkhole Attack)

- Explora mecanismos de roteamento

Ataque do Buraco de Escoamento (Sinkhole Attack)

- Explora mecanismos de roteamento

- Nó atacante atrai o roteamento

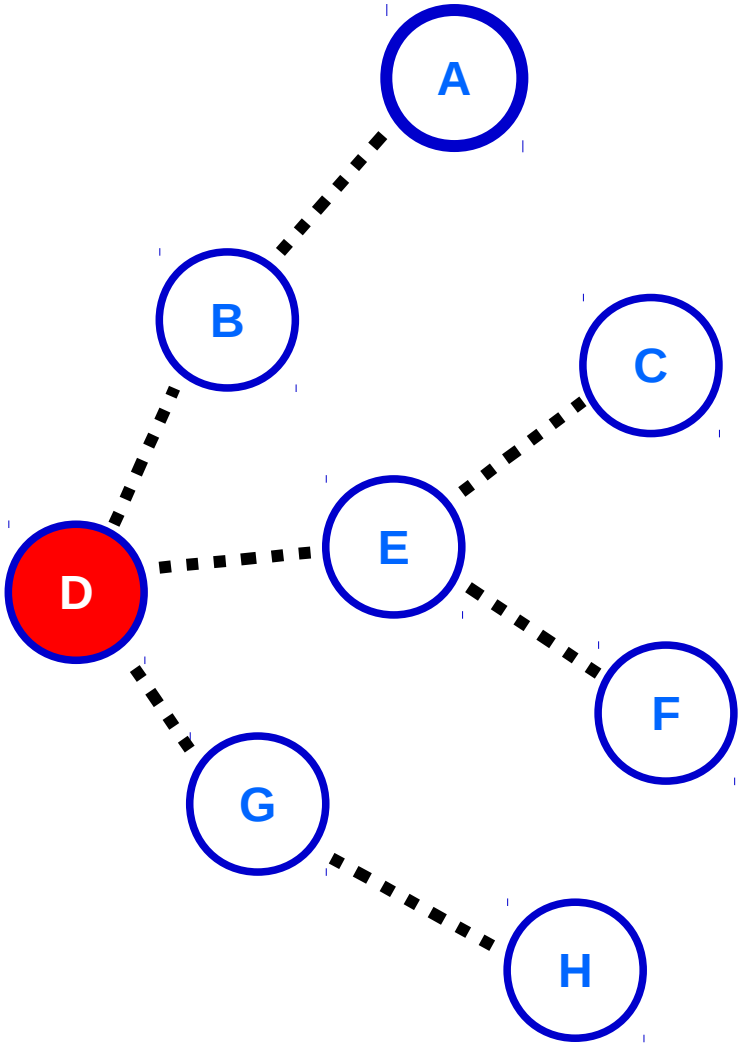


Ataque do Buraco de Escoamento (Sinkhole Attack)

- Explora mecanismos de roteamento

- Nó atacante atrai o roteamento

- Altera topologia, degrada a rede



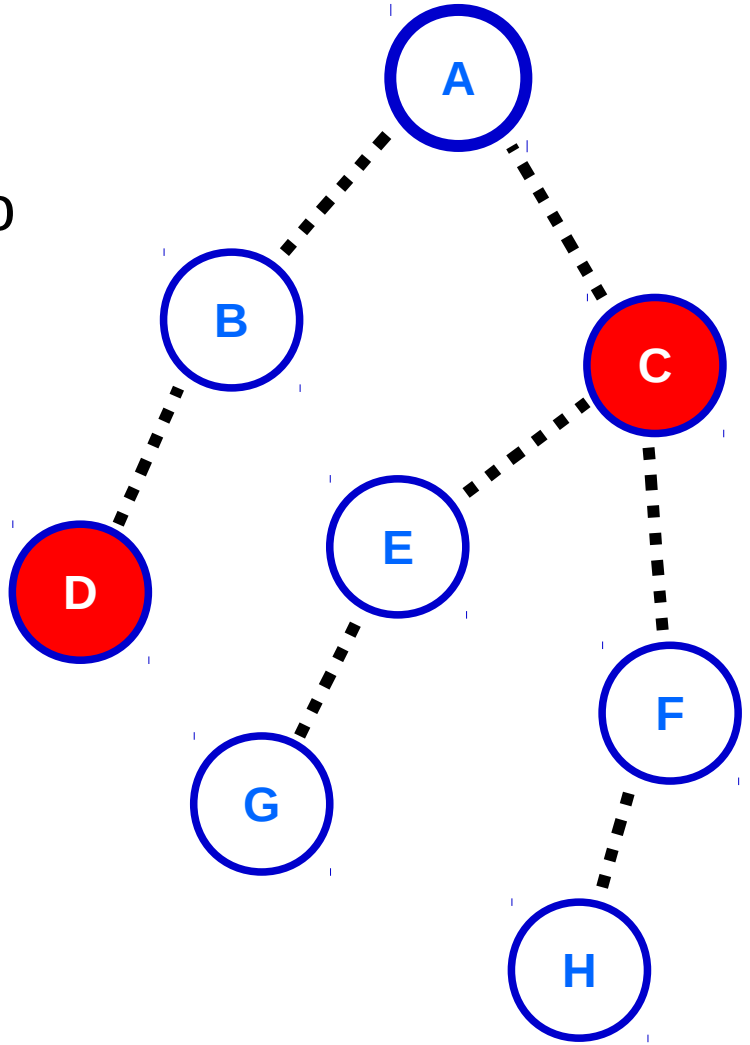
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Ataque do Buraco de Minhoca
(Wormhole Attack)

- Explora mecanismos de rot/tunelamento

Ataque do Buraco de Minhoca (Wormhole Attack)

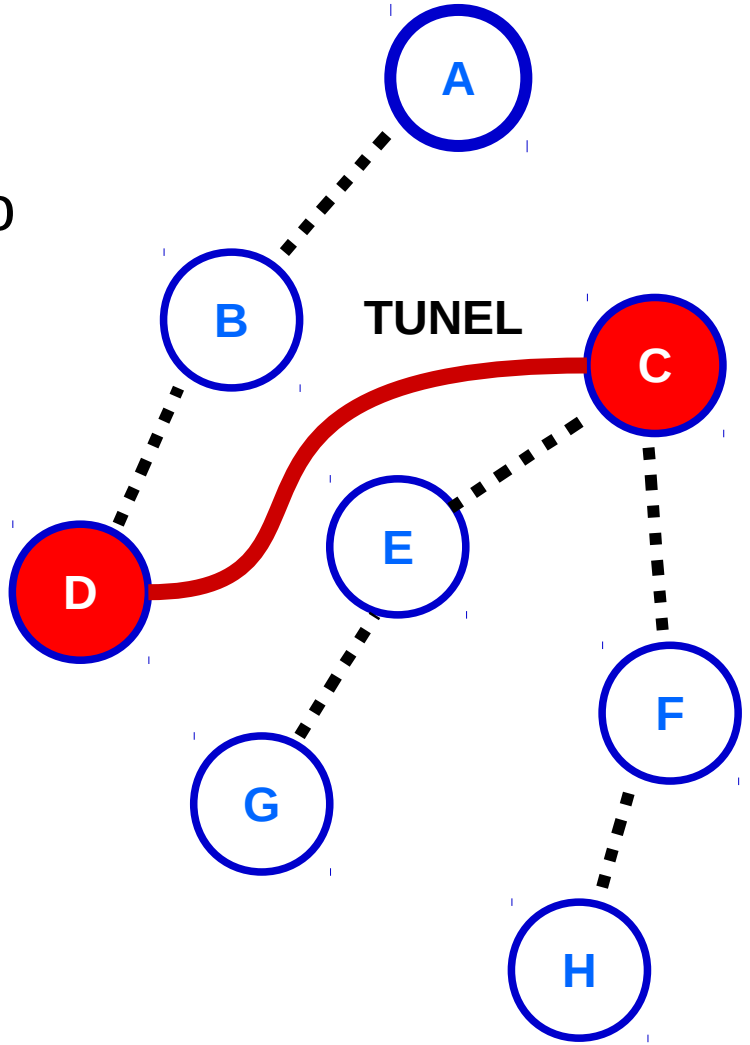
- Explora mecanismos de rot/tunelamento



Ataque do Buraco de Minhoca (Wormhole Attack)

- Explora mecanismos de rot/tunelamento

- Modifica a topologia, degrada a rede

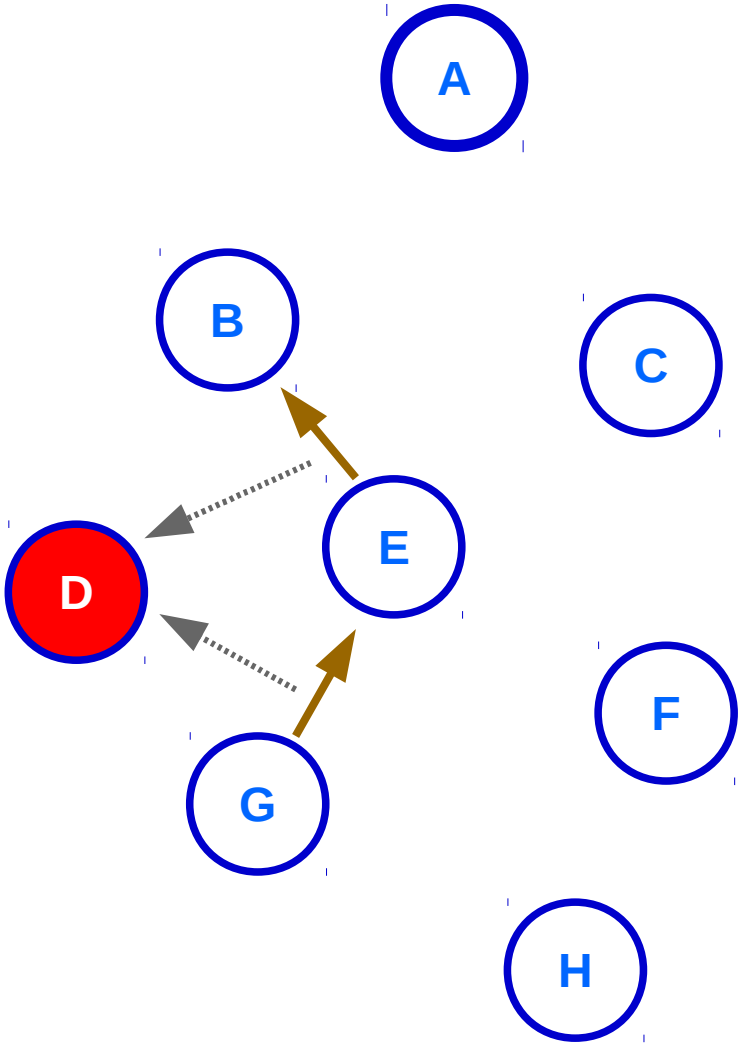


Repetir Informação de Roteamento (Routing Information Reply)

- Captura informações de outros nós

Repetir Informação de Roteamento (Routing Information Reply)

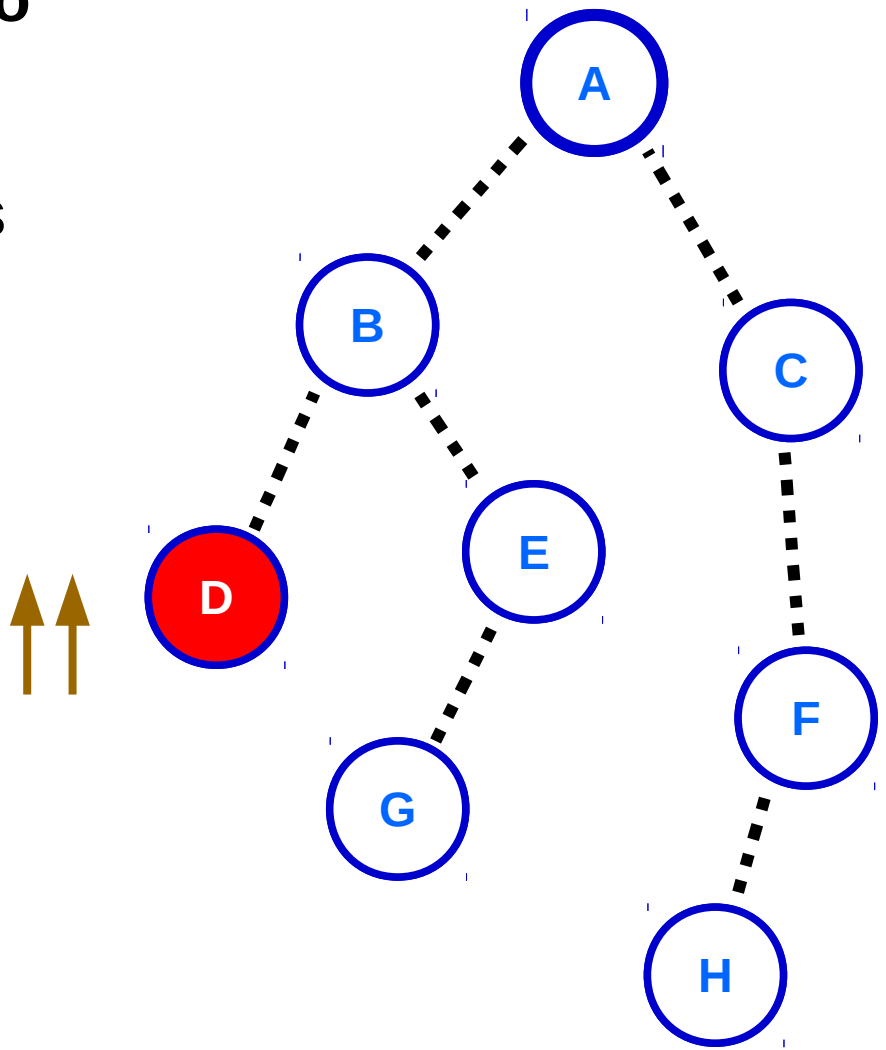
- Captura informações de outros nós



Repetir Informação de Roteamento (Routing Information Reply)

- Captura informações de outros nós

- Guarda e aguarda

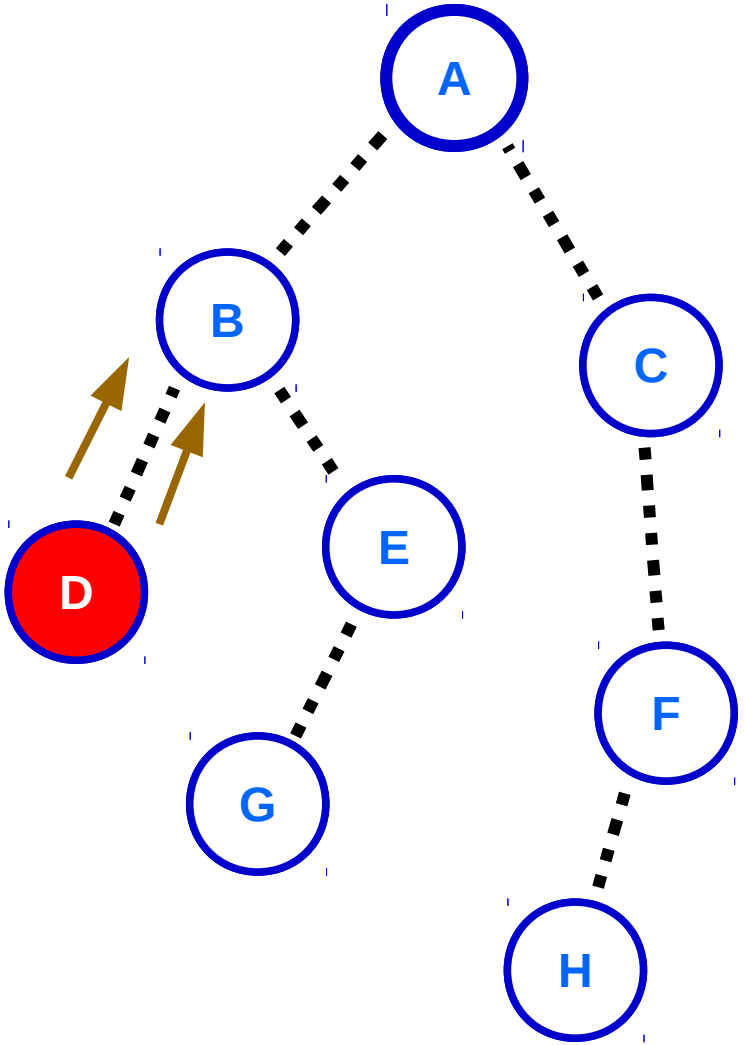


Repetir Informação de Roteamento (Routing Information Reply)

- Captura informações de outros nós

- Guarda e aguarda

- Repete as informações na rede



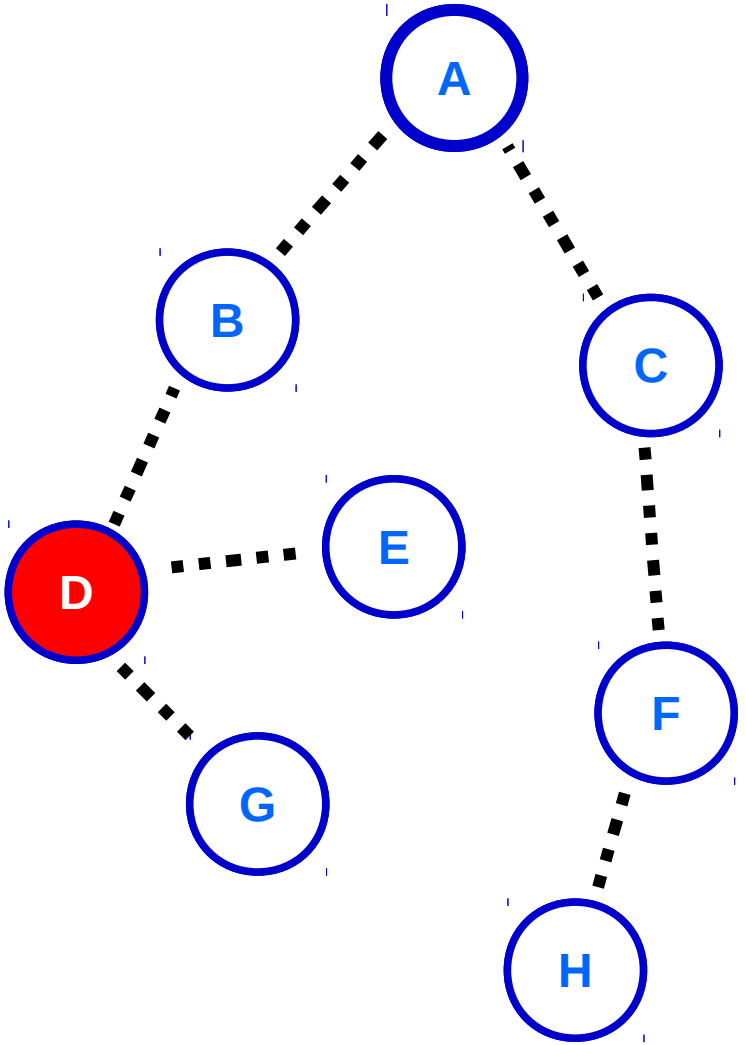
Repetir Informação de Roteamento (Routing Information Reply)

- Captura informações de outros nós

- Guarda e aguarda

- Repete as informações na rede

- Causa mudanças na topologia e
  Degradação na rede



UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

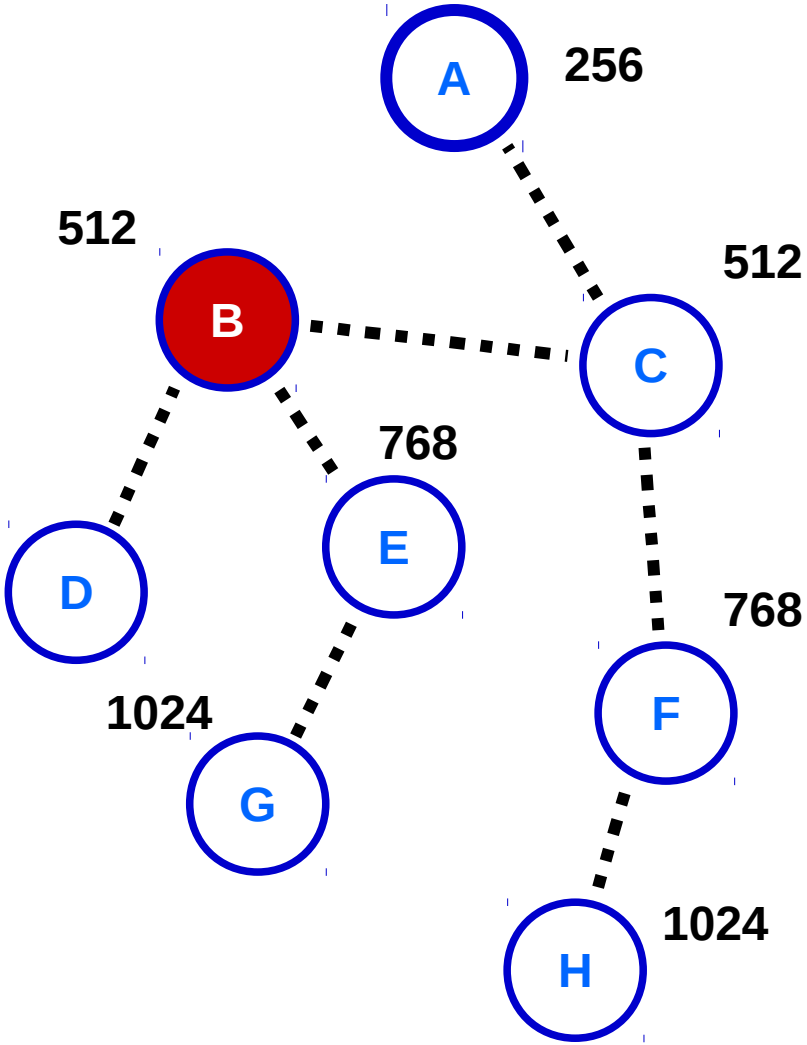
Ataque de Seleção do Pior Pai (Worst Parent Attack)

- Seleciona pior nó como pai

Ataque de Seleção do Pior Pai (Worst Parent Attack)

- Seleciona pior nó como pai

- Mudança na topologia

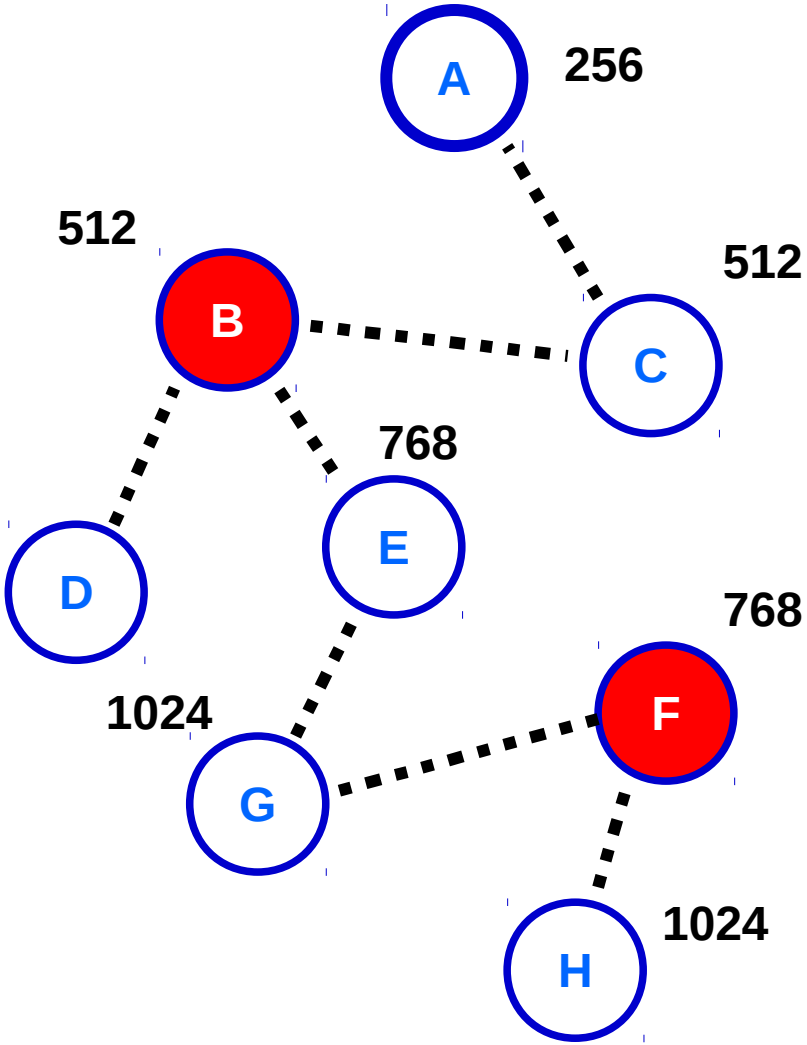


Ataque de Seleção do Pior Pai (Worst Parent Attack)

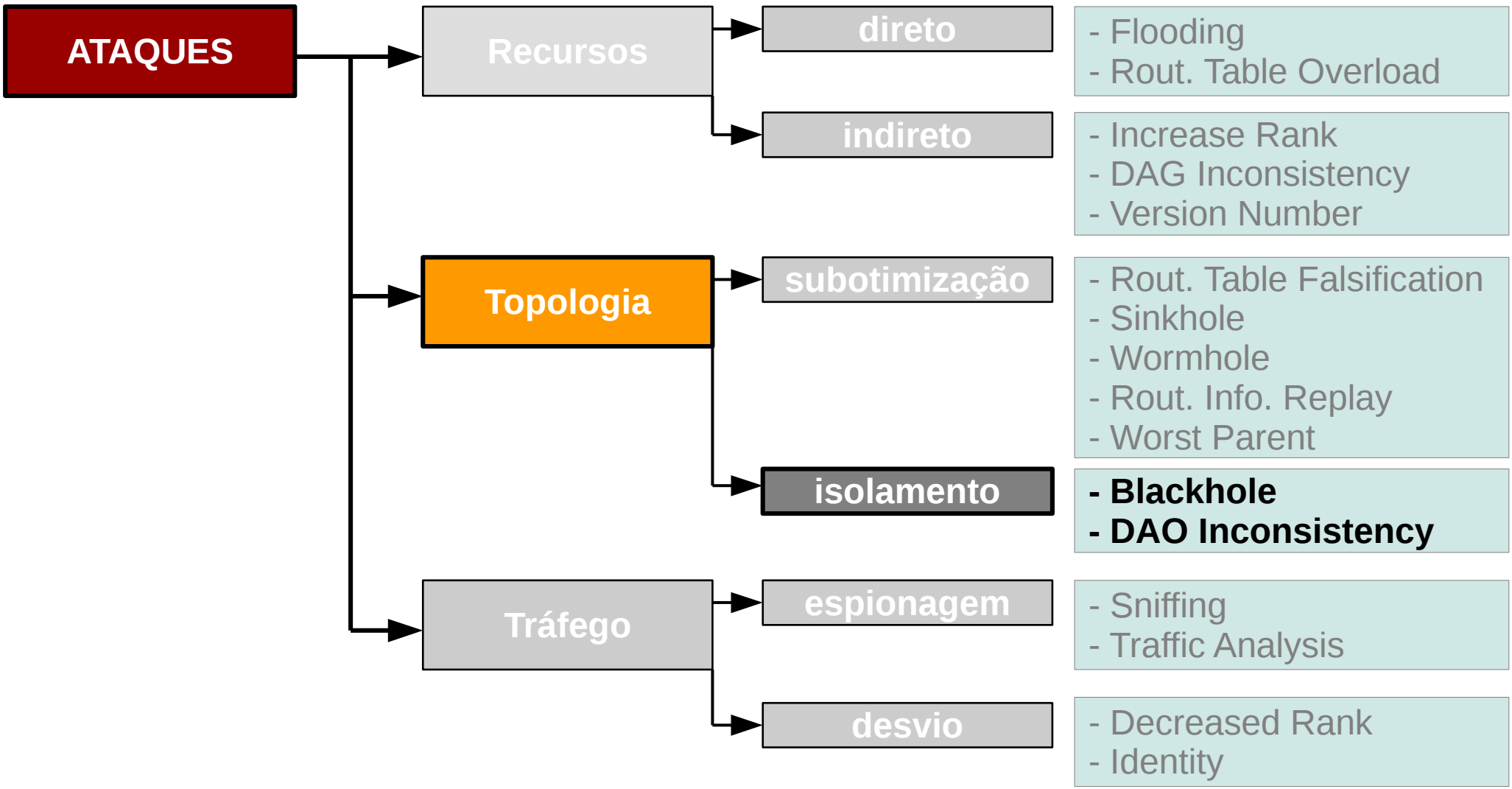
- Seleciona pior nó como pai

- Mudança na topologia

- Degrada a rede



Ataques sobre RPL



UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

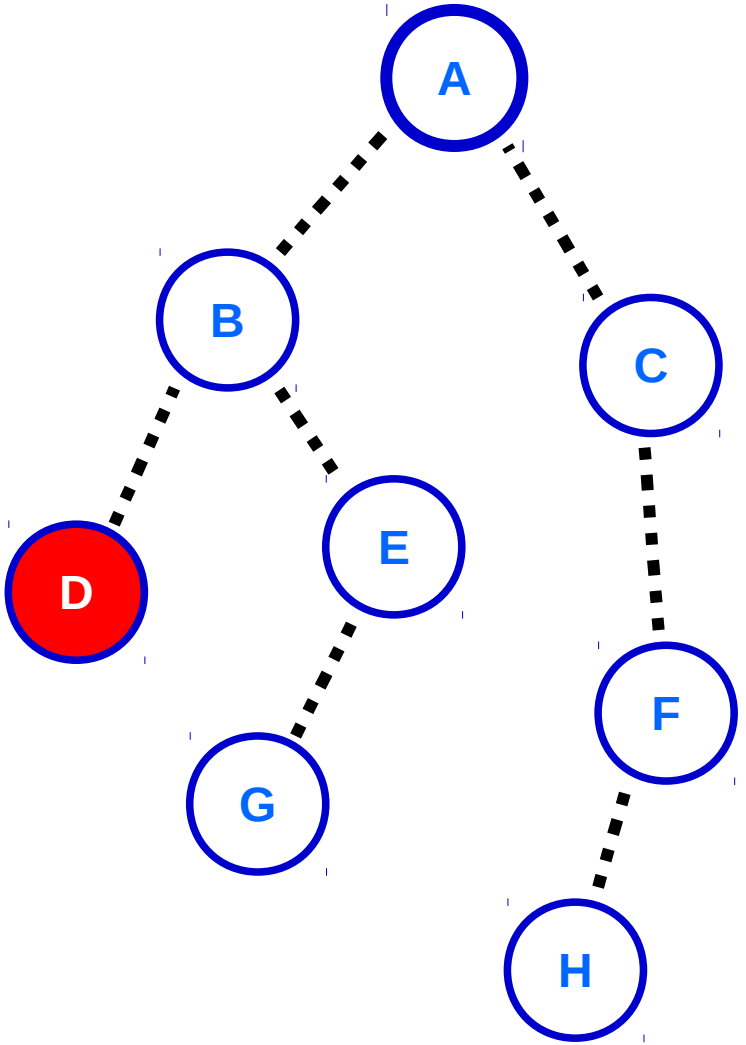
Ataque do Buraco Negro
(Blackhole Attack)

- Explora mecanismos de roteamento

Ataque do Buraco Negro (Blackhole Attack)

- Explora mecanismos de roteamento

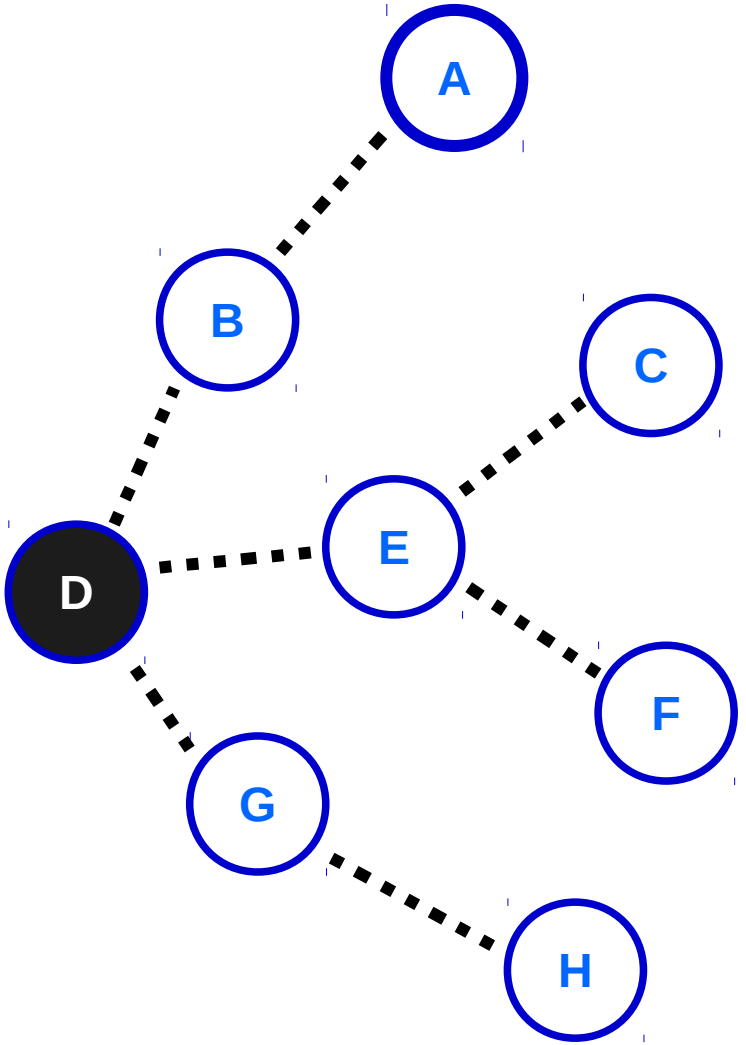
- Nó atacante atrai o roteamento



Ataque do Buraco Negro (Blackhole Attack)

- Explora mecanismos de roteamento

- Nó atacante atrai o roteamento

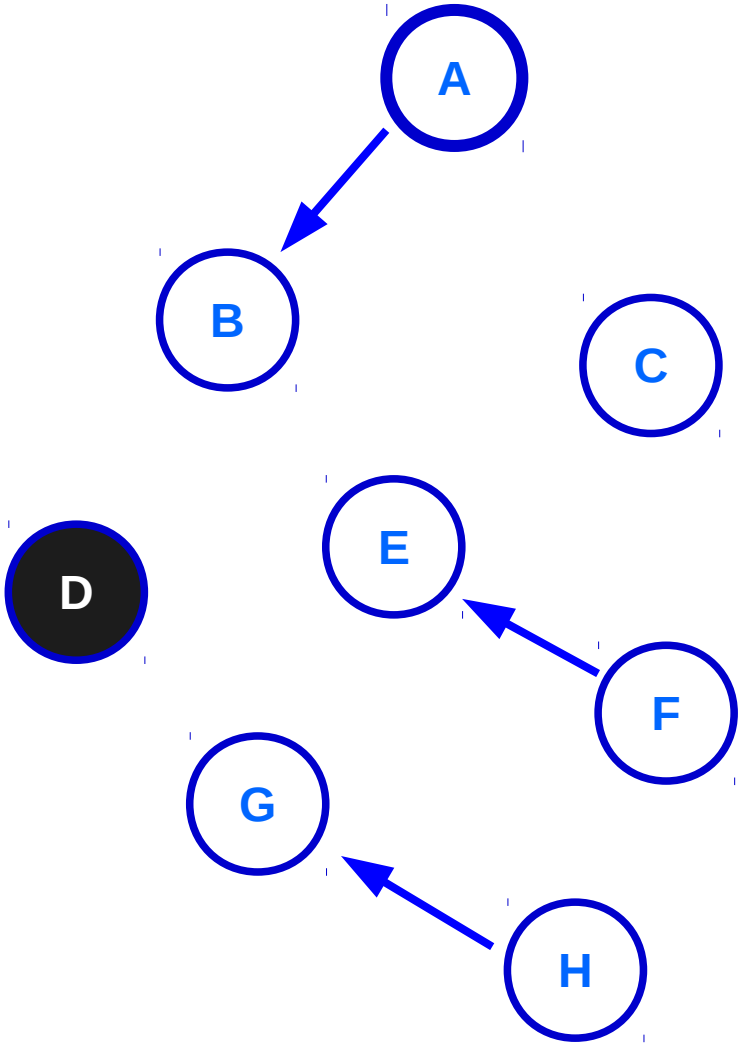


Ataque do Buraco Negro (Blackhole Attack)

- Explora mecanismos de roteamento

- Nó atacante atrai o roteamento

- Nó descarta pacotes da rede

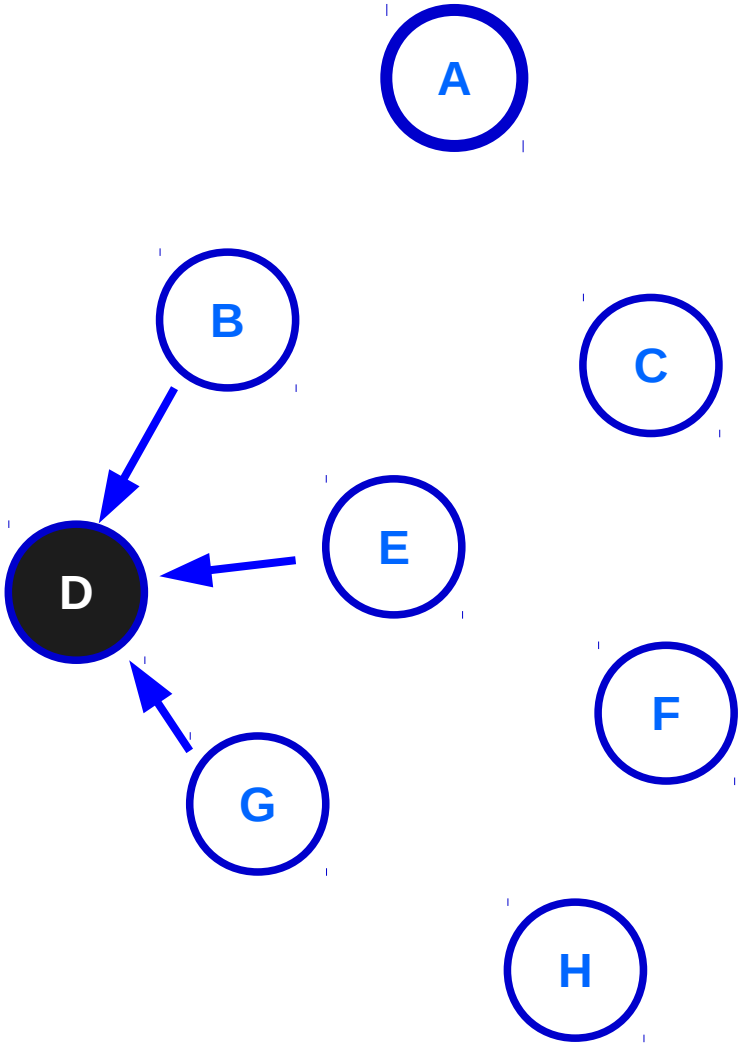


Ataque do Buraco Negro (Blackhole Attack)

- Explora mecanismos de roteamento

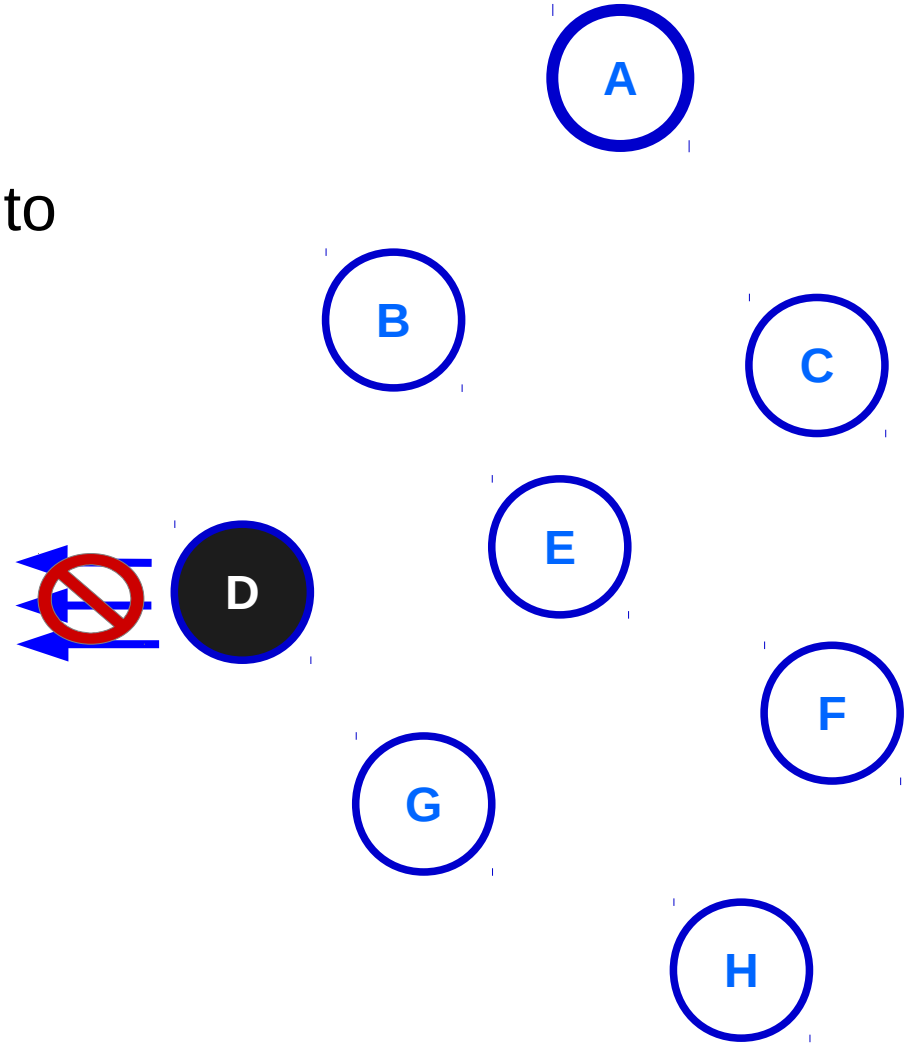
- Nó atacante atrai o roteamento

- Nó descarta pacotes da rede



Ataque do Buraco Negro (Blackhole Attack)

- Explora mecanismos de roteamento
- Nó atacante atrai o roteamento
- Nó descarta pacotes da rede
- Rede inoperável

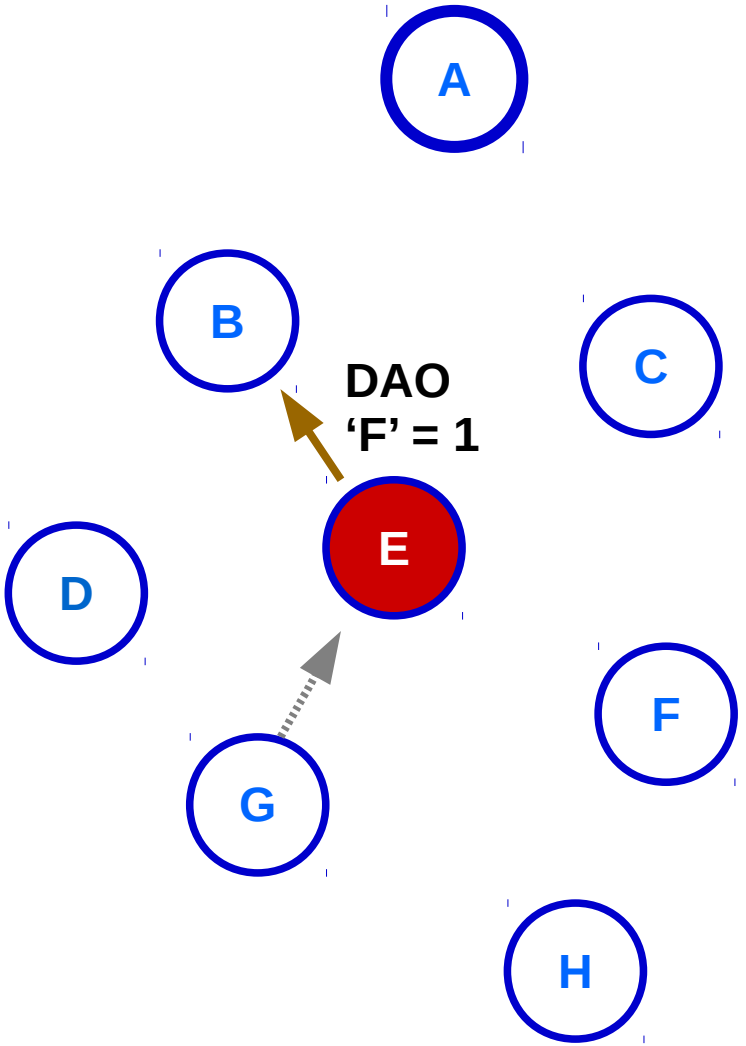


Ataque de Inconsistência DAO
(DAO Inconsistency Attack)

- Flag ‘F’ identifica forwarding error

Ataque de Inconsistência DAO (DAO Inconsistency Attack)

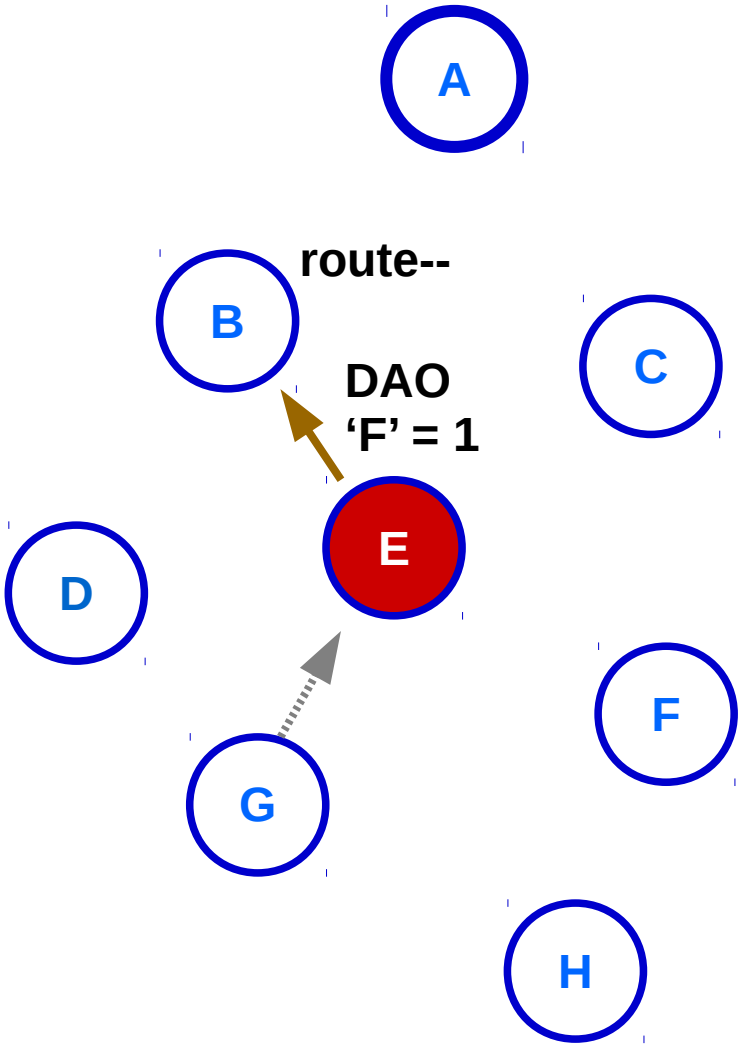
- Flag ‘F’ identifica forwarding error



Ataque de Inconsistência DAO (DAO Inconsistency Attack)

- Flag ‘F’ identifica forwarding error

- Nó pai descarta roteamento

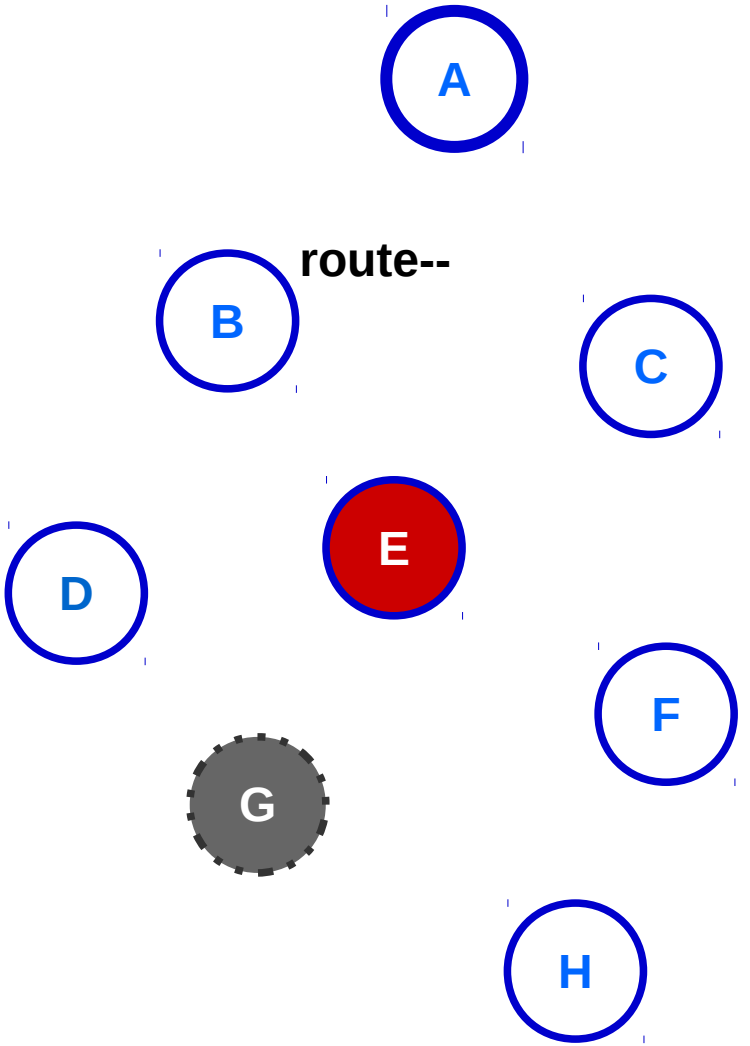


Ataque de Inconsistência DAO (DAO Inconsistency Attack)

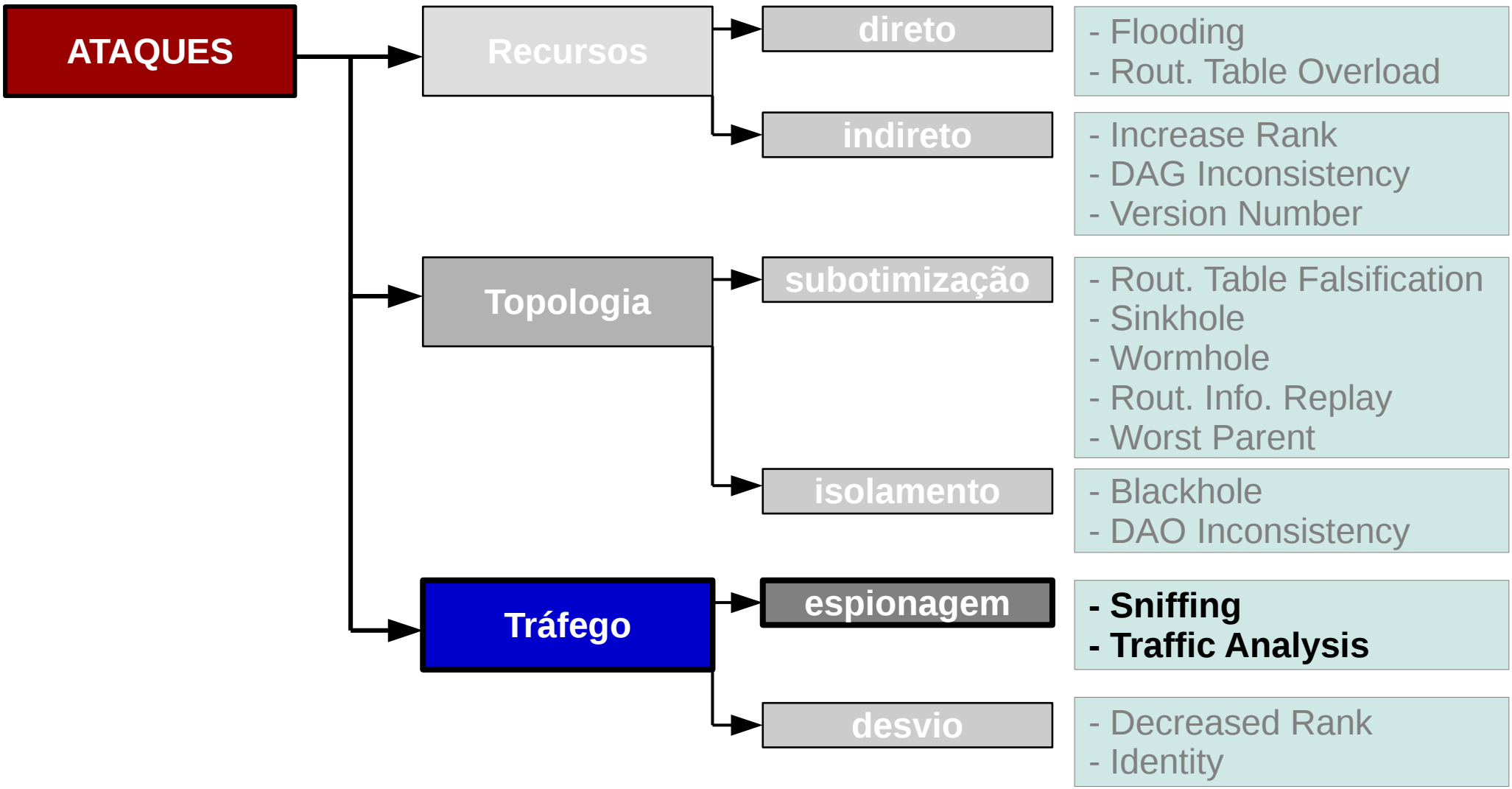
- Flag ‘F’ identifica forwarding error

- Nó pai descarta roteamento

- Vítima fica isolada



Ataques sobre RPL



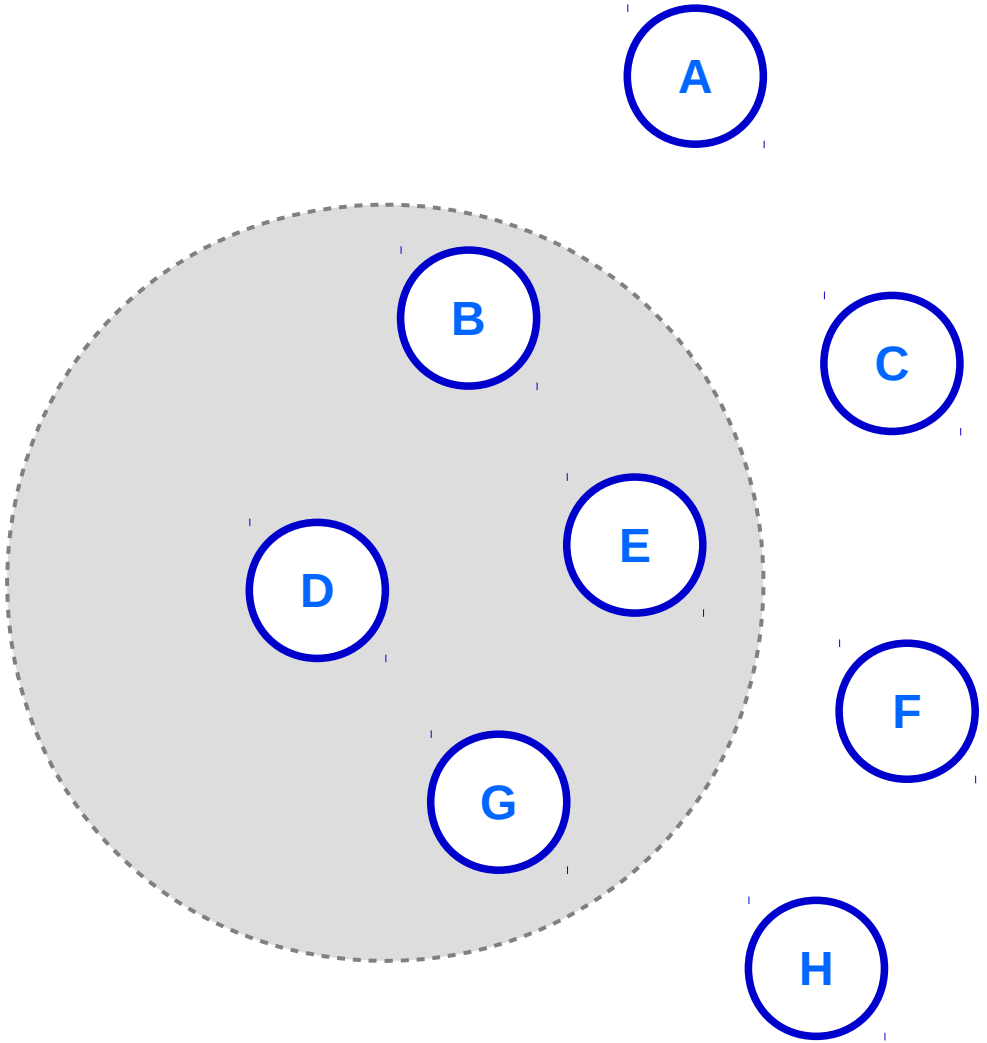
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Captura de Pacotes (Sniffing)

- Captura de Mensagens de Controle

Captura de Pacotes (Sniffing)

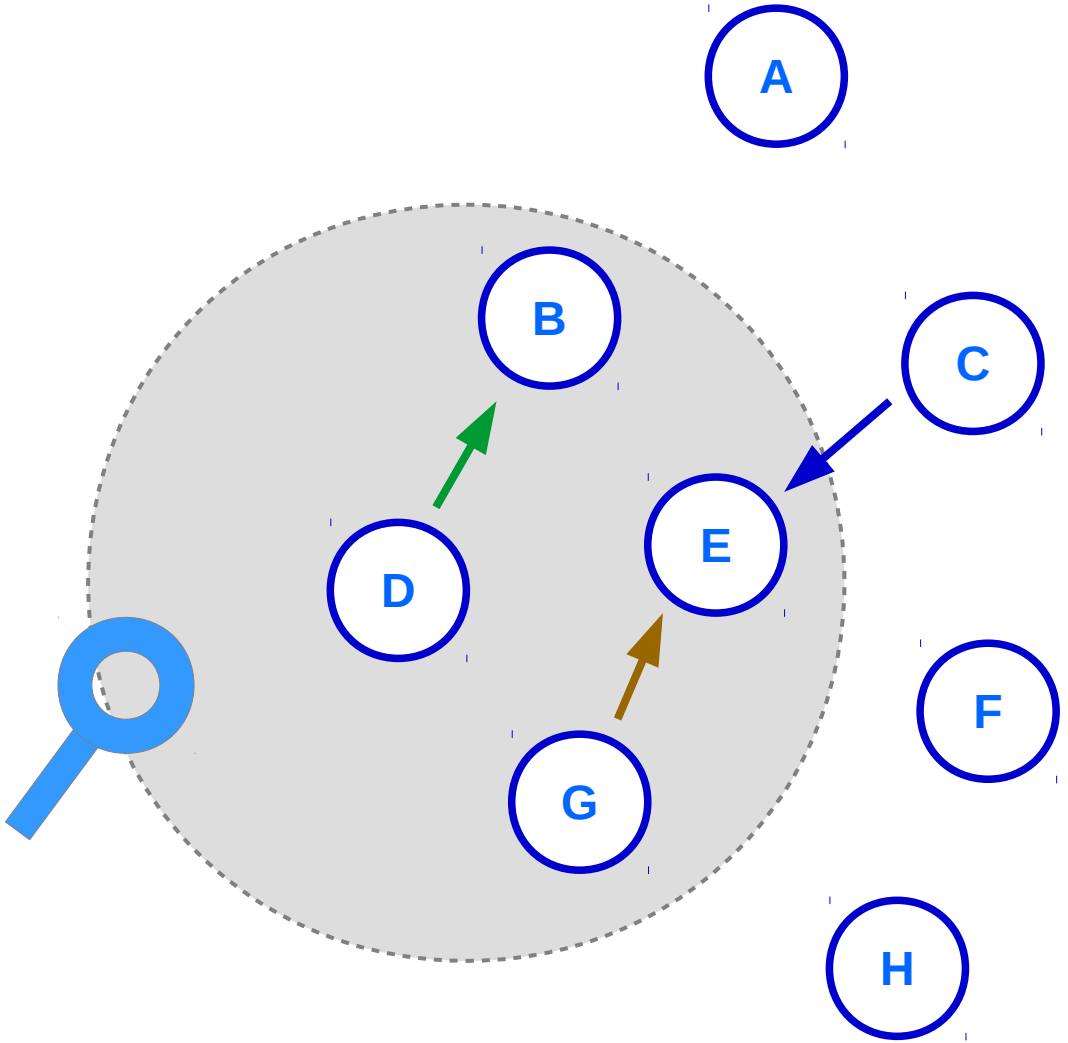
- Captura de Mensagens



Captura de Pacotes (Sniffing)

- Captura de Mensagens

- Difícil detecção

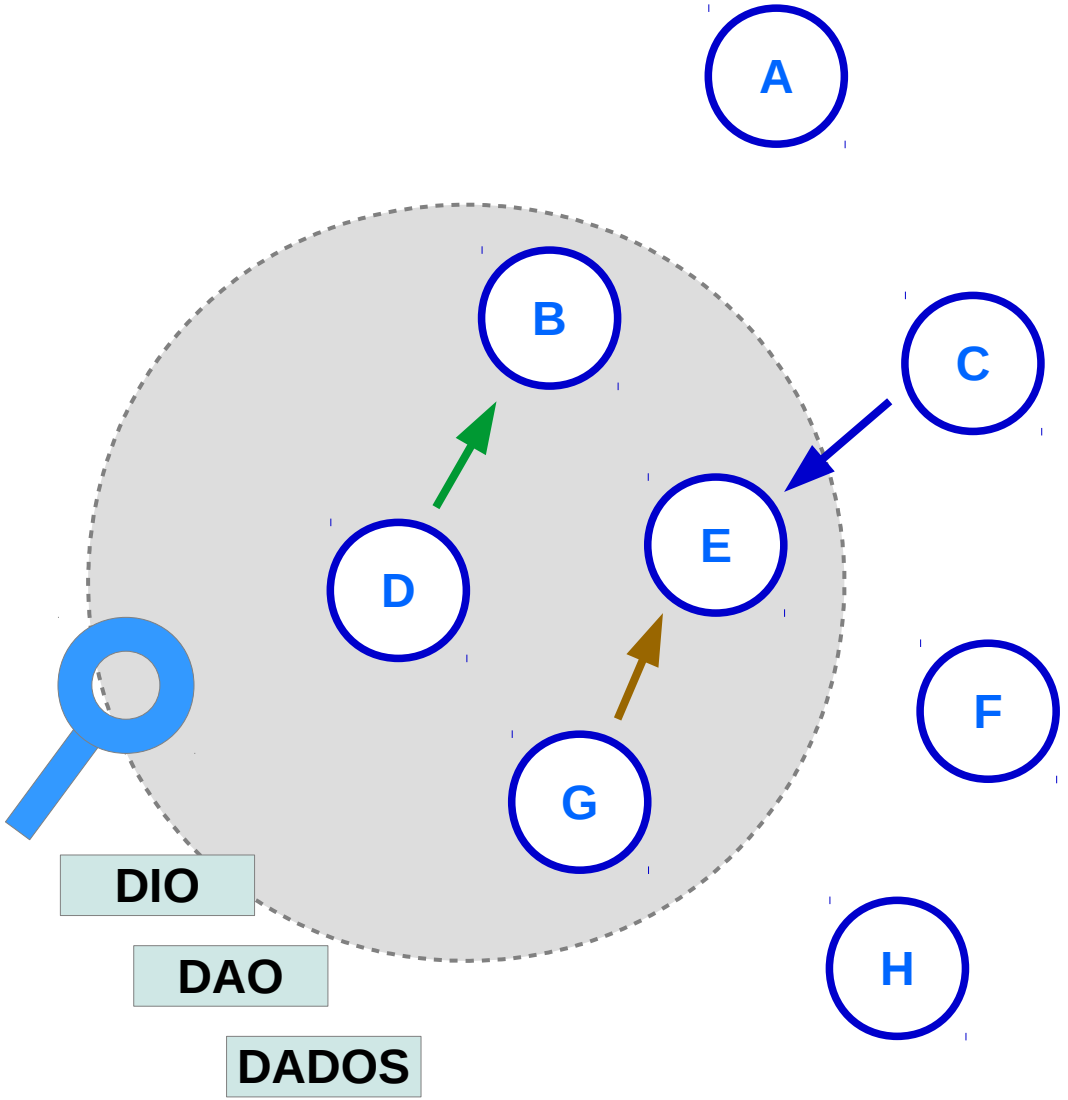


Captura de Pacotes (Sniffing)

- Captura de Mensagens

- Difícil detecção

- Espionar informações



UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

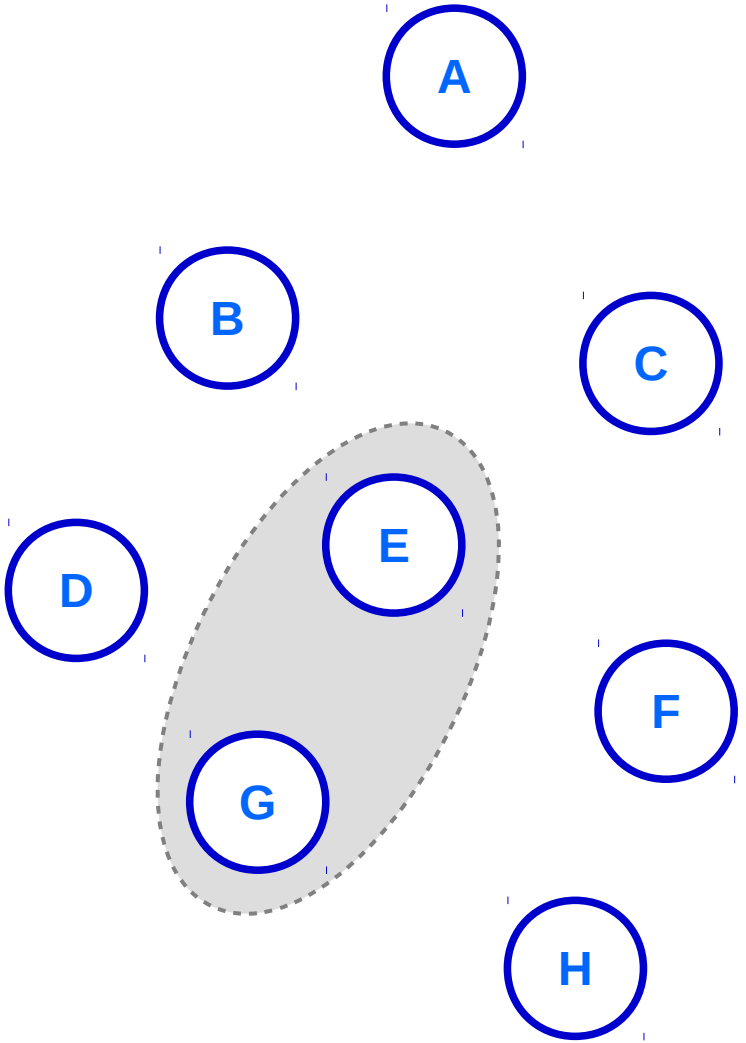
Ataque de Análise de Tráfego
(Traffic Analysis Attack)

- Captura de Mensagens de Controle

Ataque de Análise de Tráfego (Traffic Analysis Attack)

- Captura de Mensagens de Controle

- Avaliar comportamento Pai e Filho

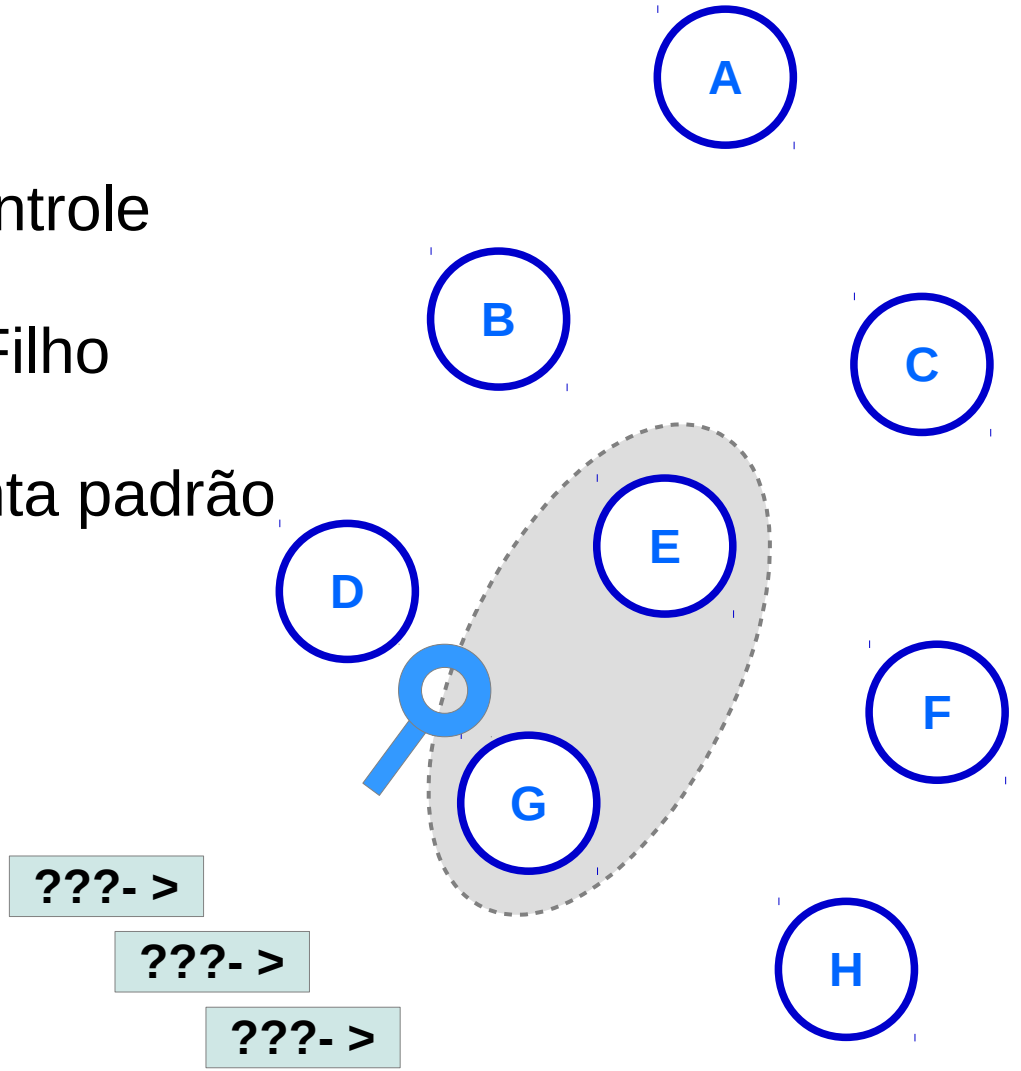


Ataque de Análise de Tráfego (Traffic Analysis Attack)

- Captura de Mensagens de Controle

- Avaliar comportamento Pai e Filho

- Mesmo criptografado, apresenta padrão



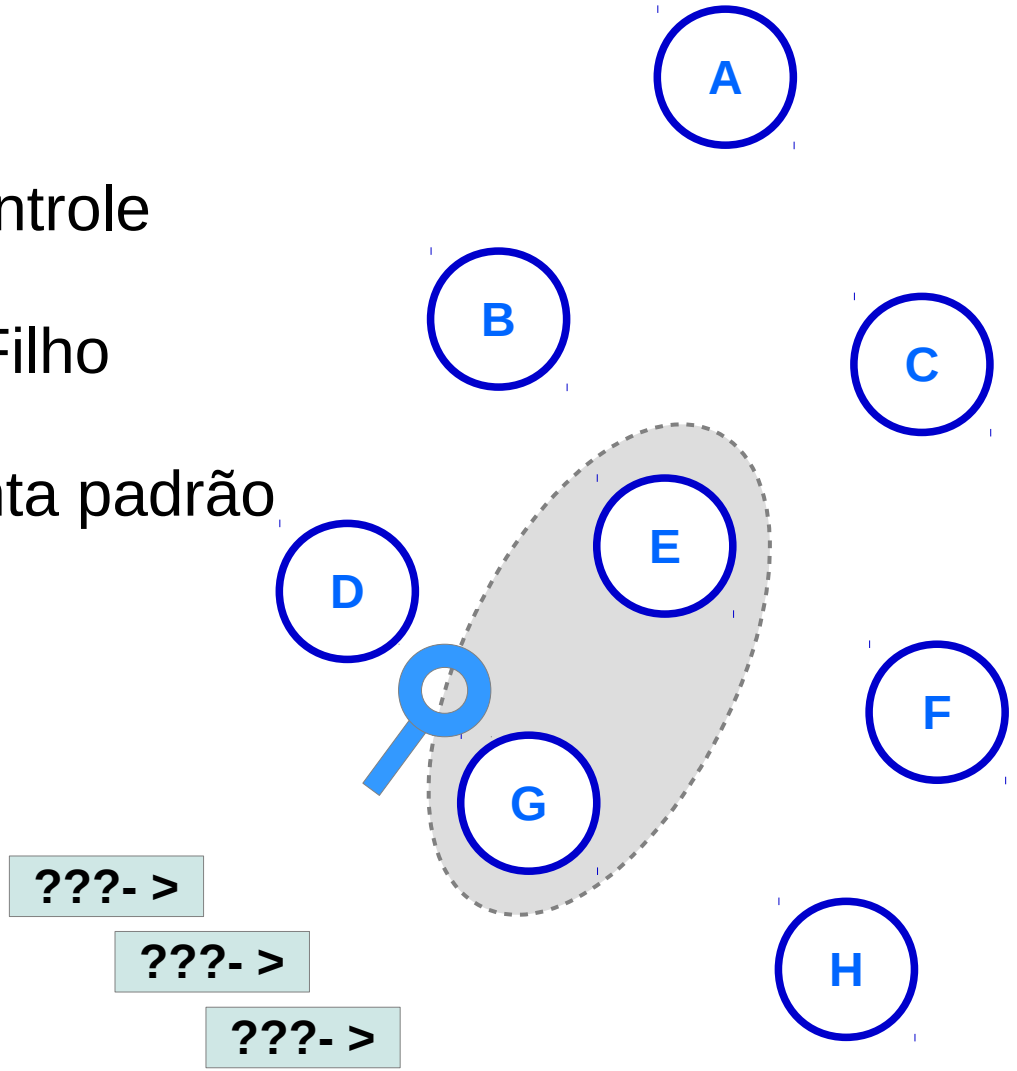
Ataque de Análise de Tráfego (Traffic Analysis Attack)

- Captura de Mensagens de Controle

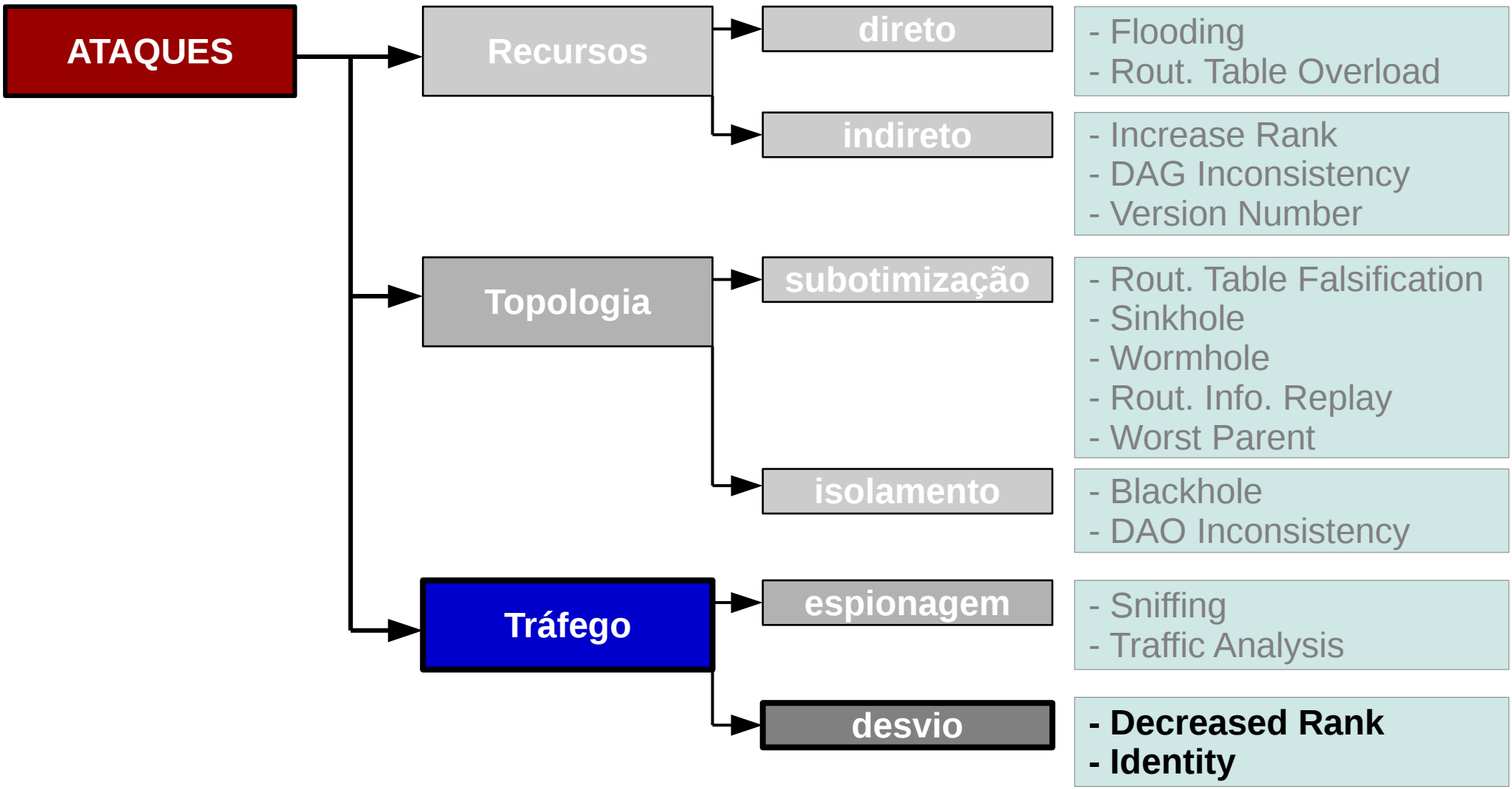
- Avaliar comportamento Pai e Filho

- Mesmo criptografado, apresenta padrão

- Preparar outros ataques



Ataques sobre RPL

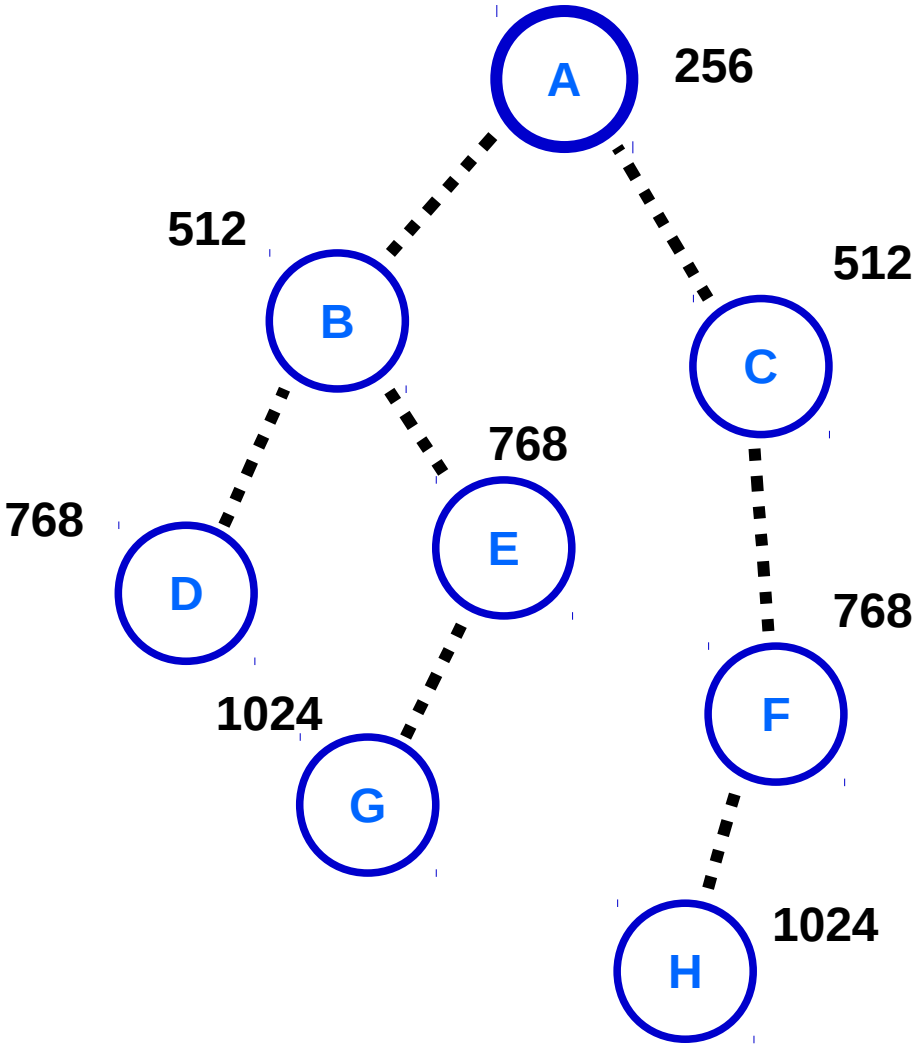


Ataque que Diminui o Rank (Decrease Rank Attack)

- Reduzir o valor de Rank

Ataque que Diminui o Rank (Decrease Rank Attack)

- Reduzir o valor de Rank

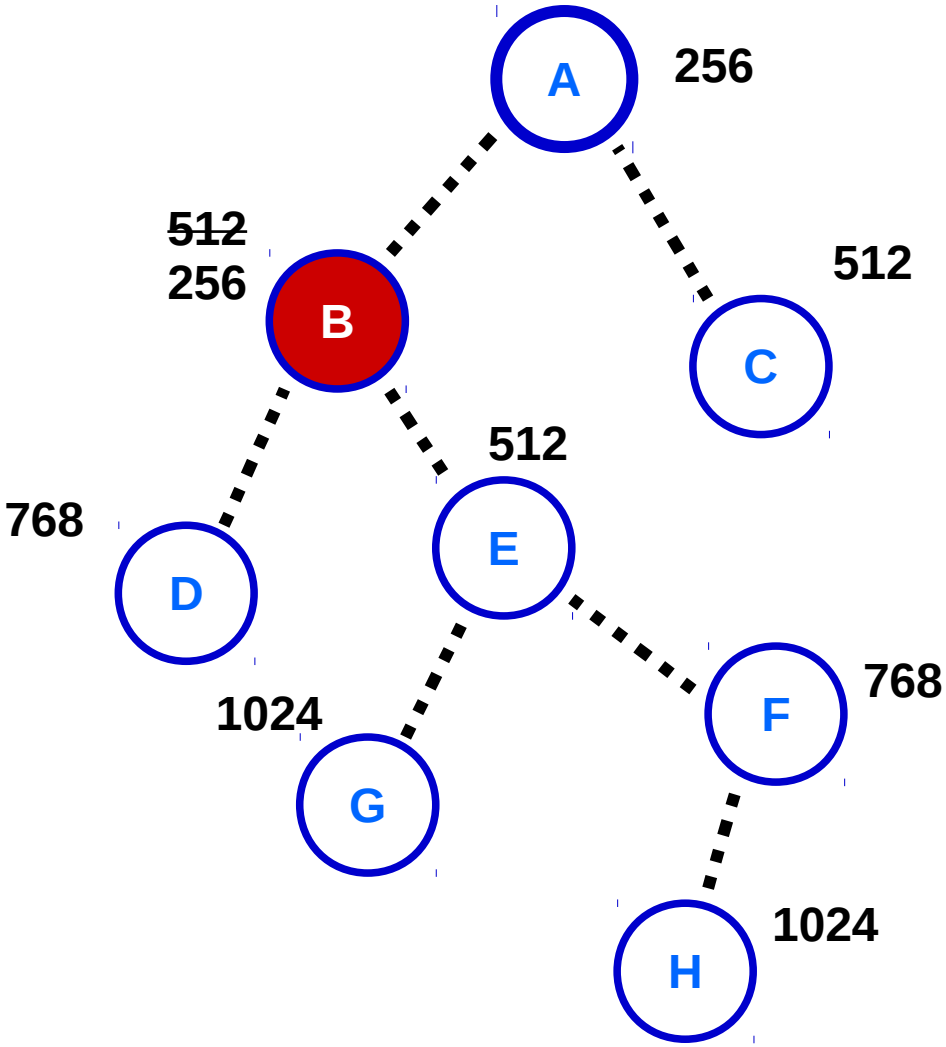


Ataque que Diminui o Rank (Decrease Rank Attack)

- Reduzir o valor de Rank

- Obter o controle da rede

- Modificar conteúdo



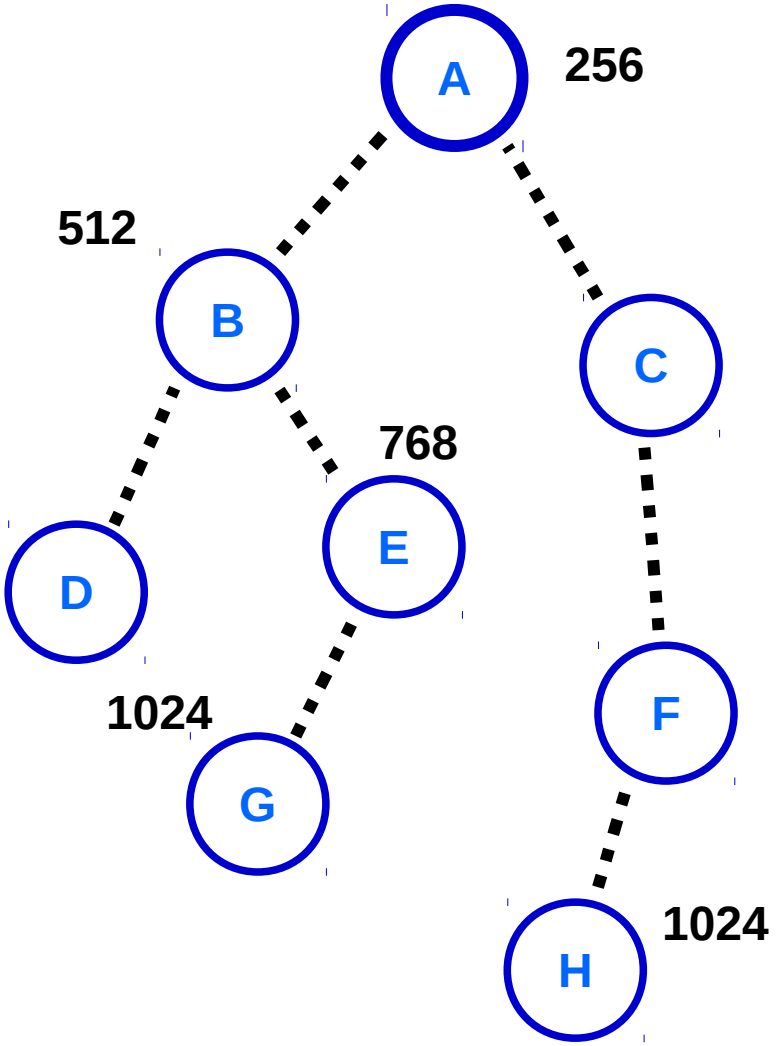
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Ataque de Identidade (Identity Attack)

- Clonar nós

Ataque de Identidade (Identity Attack)

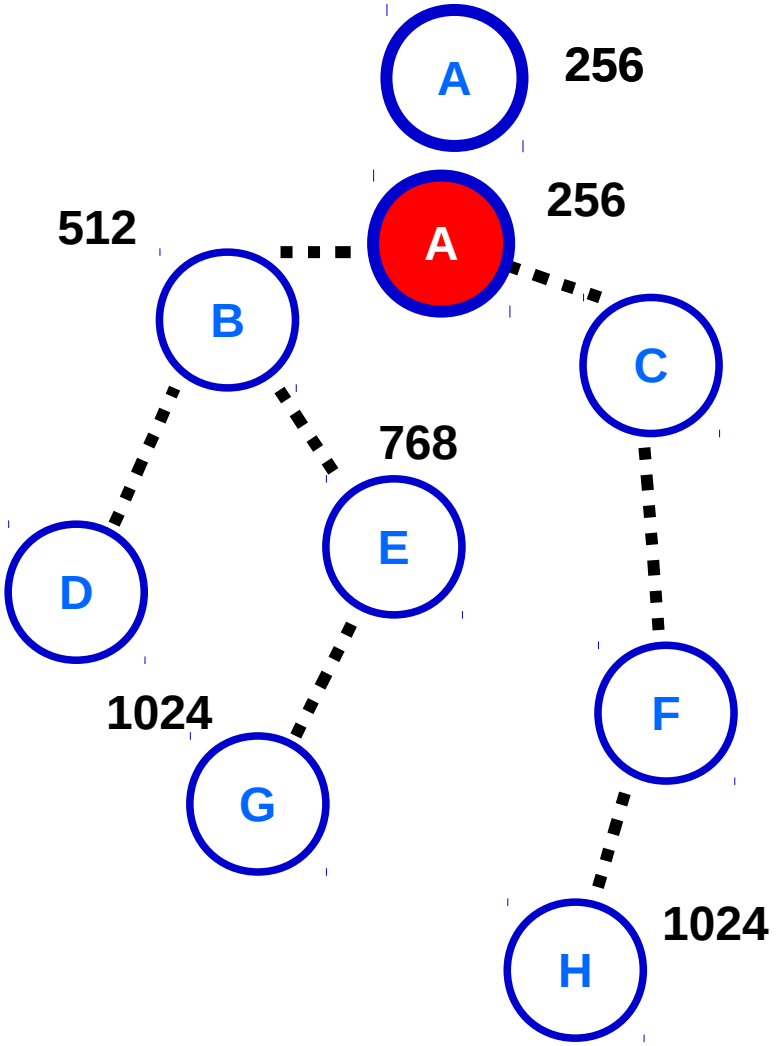
- Clonar nós



Ataque de Identidade (Identity Attack)

- Clonar nós

- Spoofing, Sybil

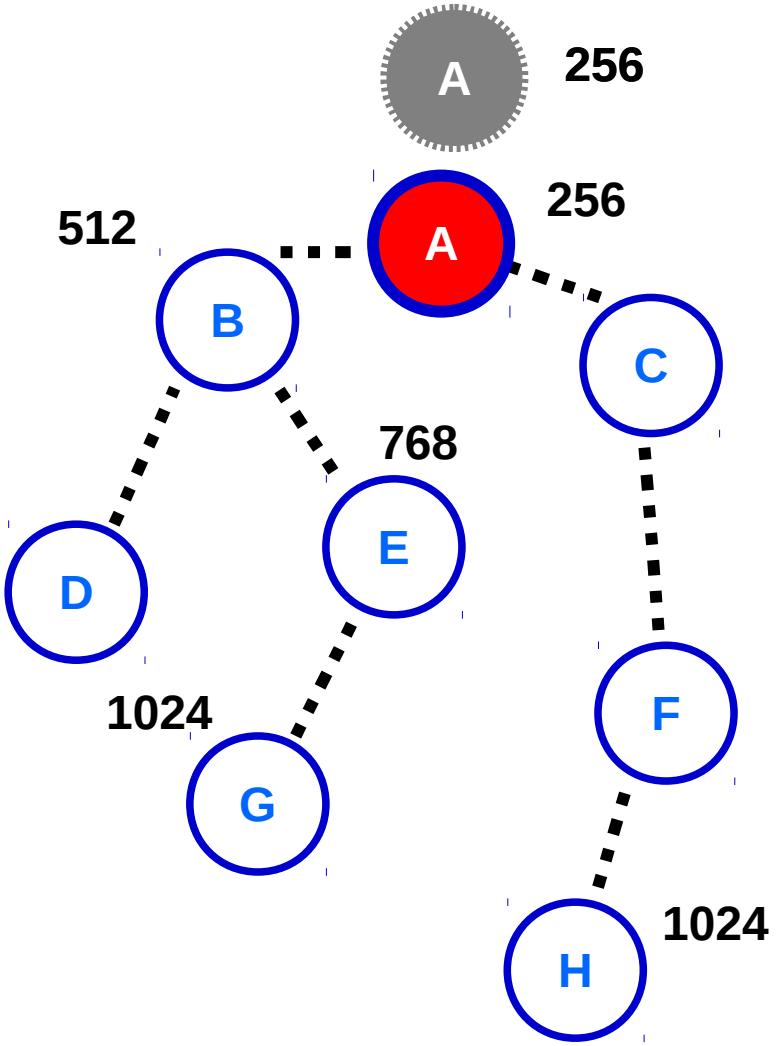


Ataque de Identidade (Identity Attacks)

- Clonar nós

- Spoofing, Sybil

- Controle da rede



Contra-Medidas

Métodos Criptográficos

- Confidencialidade, Autenticidade, Integridade, Disponibilidade
Problema: sabotar o sensor

Detecção e Alertas de Intrusão

- Monitoramento constante
- Nó wifi difícil detecção

Triagem

- Pós ataques

Considerançõe Finais

Referências

A Taxonomy of Attacks in RPL-based Internet of Things

Mayzaud, A.; Bodonnel, R.; Chrisment, I.; Int. Journal of Network Security – May 2016.

A Survey: Attacks on RPL and 6LoWPAN in IoT

Pongle, P.; Chavan, G.; Int. Conference on Pervasive Computing – IEEE- 2015.