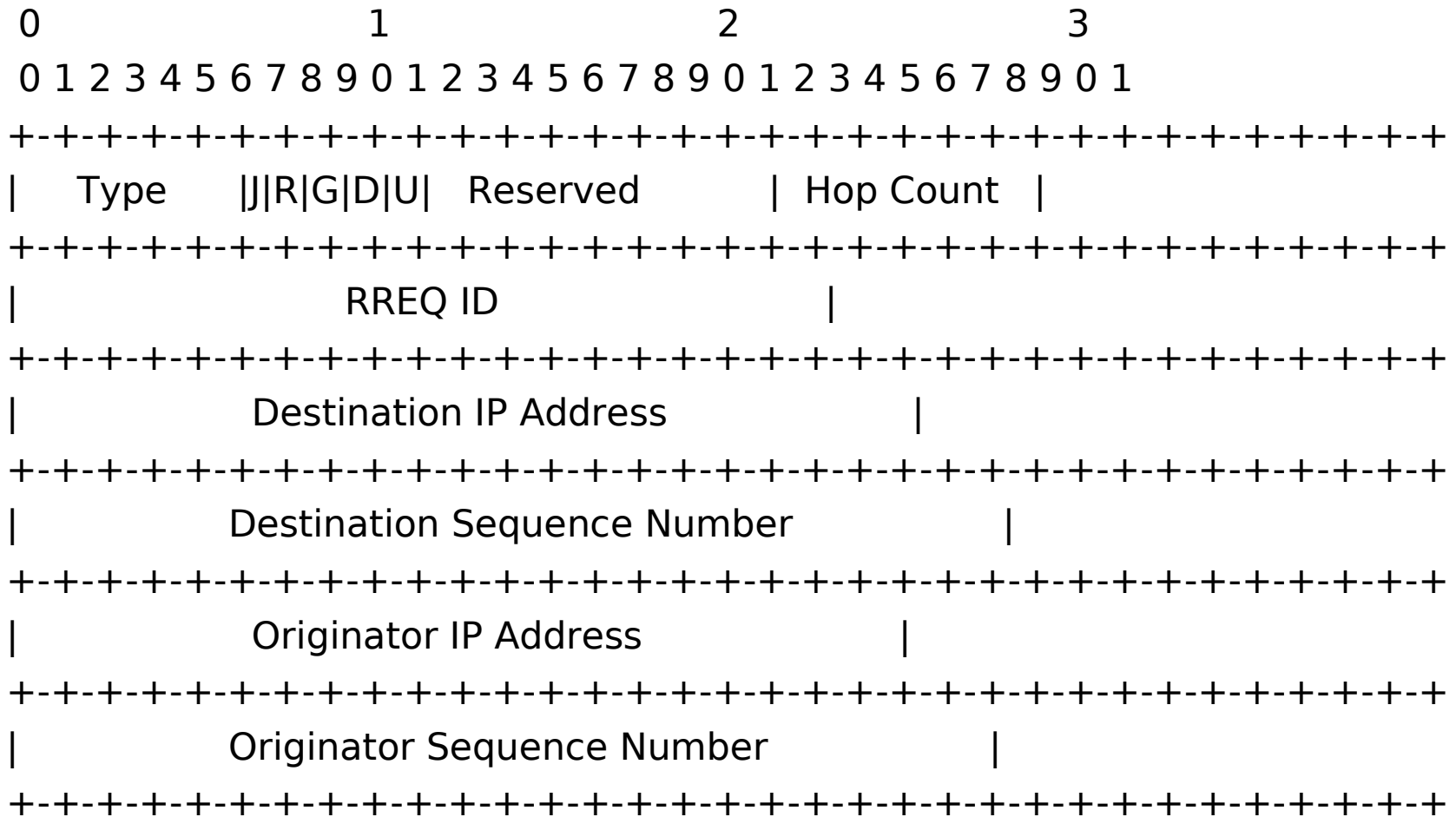


# Počítačové siete 2

## Smerovacie protokoly 2

Martin Drozda

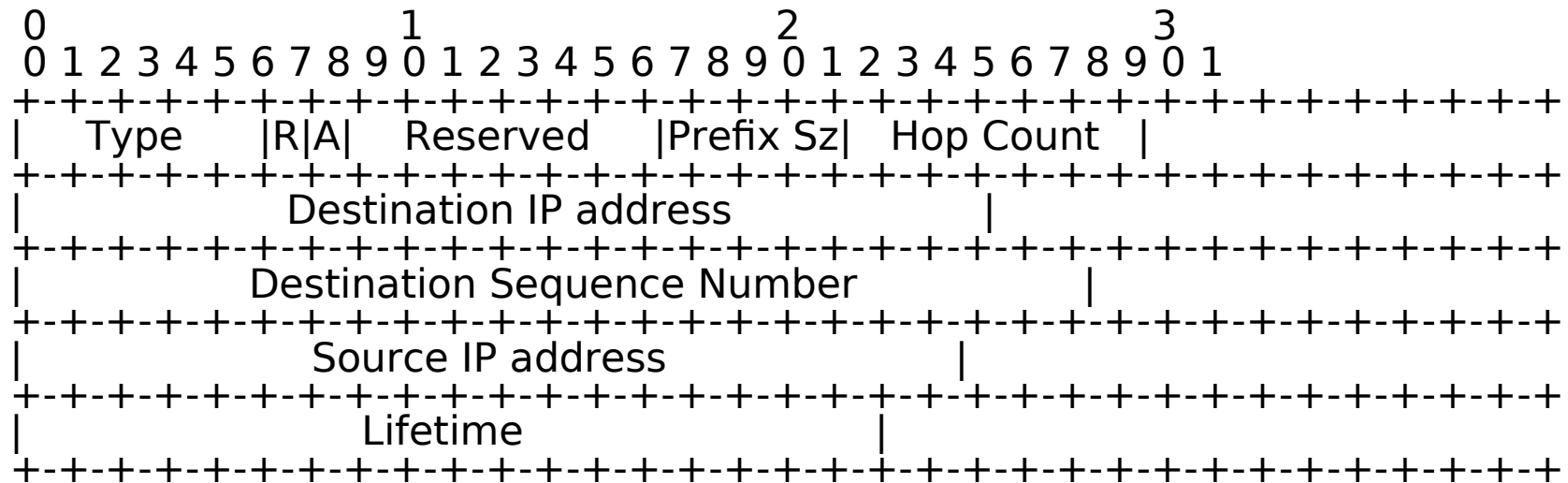
# AODV: RREQ Format



- J      Join flag; reserved for multicast.
- R      Repair flag; reserved for multicast.
- G      Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field.
- D      Destination only flag; indicates only the destination may respond to this RREQ.
- U      Unknown sequence number; indicates the destination sequence number is unknown.

After a node receives a RREQ and responds with a RREP, it discards the RREQ. If the RREQ has the 'G' flag set, and the intermediate node returns a RREP to the originating node, it **MUST** also unicast a gratuitous RREP to the destination node.

# AODV: RREP Format



**Prefix Size (Prefix Sz)** The Prefix Size Field indicates the nodes within a destination's subnet that are reachable via the same route. For example, a prefix size of eight (8) is equivalent to a subnet mask of 255.255.255.0. For a host route the prefix size is zero (0), This is equivalent to a subnet mask of 255.255.255.255.

The Route Reply Acknowledgment (RREP-ACK) message **MUST** be sent in response to a RREP message with the 'A' bit set. This is typically done when there is danger of unidirectional links preventing the completion of a Route Discovery cycle.

# AODV: RREP Format

R Repair flag; used for multicast.

A Acknowledgment required.

Lifetime The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

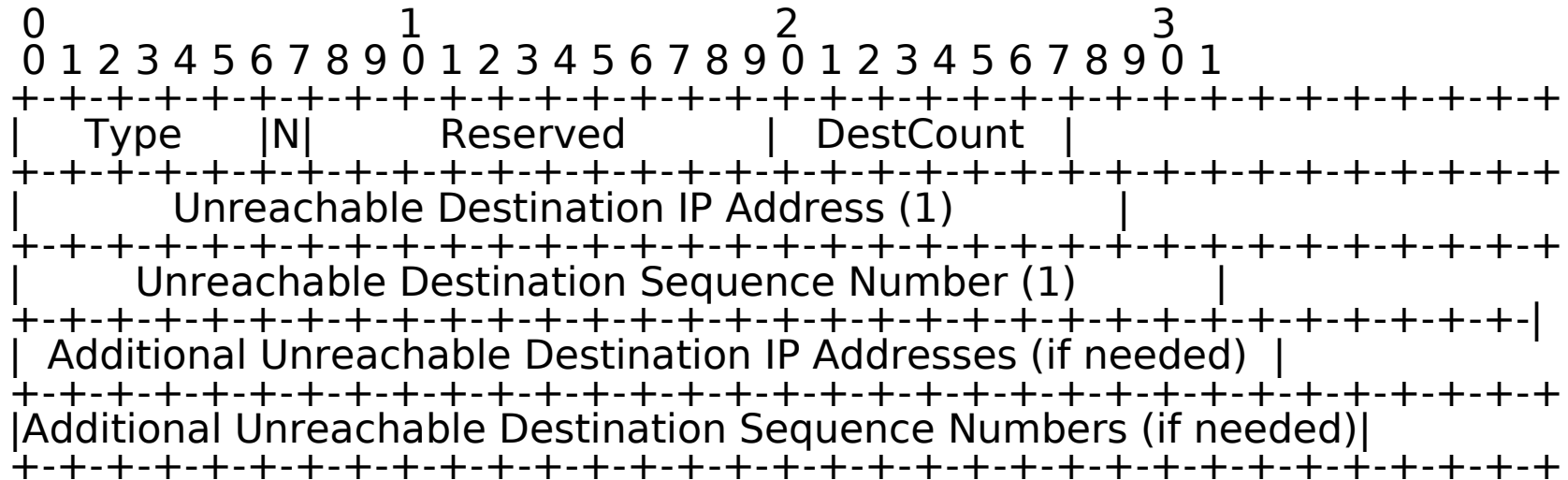
Hop Count The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.

Destination IP Address  
The IP address of the destination for which a route is supplied.

Destination Sequence Number  
The destination sequence number associated to the route.

Originator IP Address  
The IP address of the node which originated the RREQ for which the route is supplied.

# AODV: RERR Format



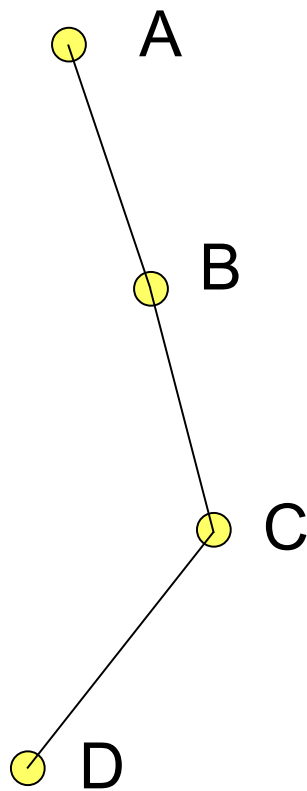
N No delete flag; set when a node has performed a local repair of a link, and upstream nodes should not delete the route.

DestCount The number of unreachable destinations included in the message; MUST be at least 1.

Unreachable Destination IP Address  
The IP address of the destination that has become unreachable due to a link break.

Unreachable Destination Sequence Number  
The sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.

# Problém počítania donekonečna



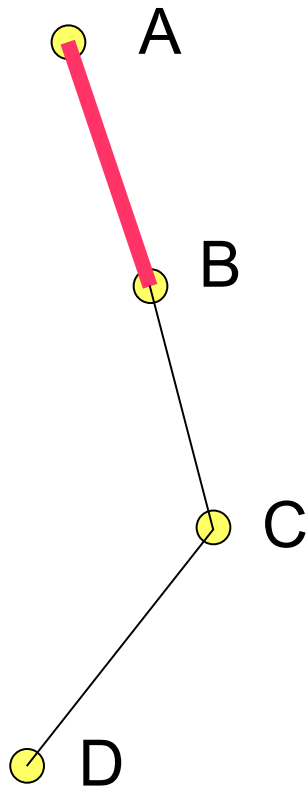
Smerovacia tabuľka A:  
B: 1 C: 2 D: 3

Smerovacia tabuľka B:  
A: 1 C: 1 D: 2

A: 2 B: 1 D: 1

A: 3 B: 2 C: 1

# Problém počítania donekonečna



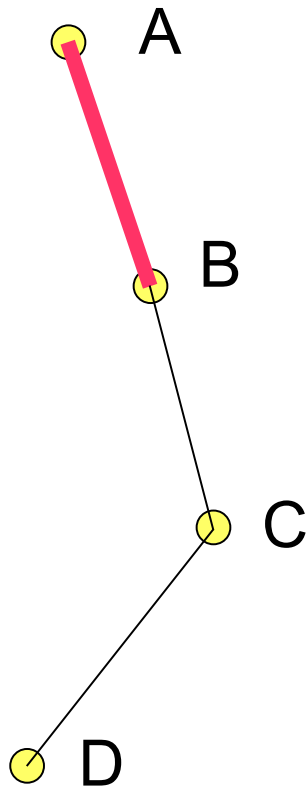
Linka A-B prestane existovať

B inkrementuje vzdialenosť k A, pretože vidí, že C má platnú cestu k A

Potom C inkrementuje svoju vzdialenosť k A, pretože B inkrementovalo svoju vzdialenosť k A



# Problém počítania donekonečna



Riešenie:

- Ohraničené počítanie
- Horizon splitting: uzol C nepošle smerovaciú informáciu uzlu B
- Sekvenčné čísla?

Formálny dôkaz, že smerovanie v AODV nevytvára slučky je uvedený v pôvodnom článku (Perkins, Royer 1999).

perkins 1999\_adhoc.pdf — aodv3

11 of 11 200%

Thumbnails

5

6

7

8

9

10

11

### A. Proof of the Loop-free Property

Verifying that AODV establishes only loop-free routes is easy because of the effect of the destination sequence number on the maintenance of routes. Suppose that there is a loop in a route to a destination  $Z$ , and that nodes  $X_i$  are the nodes in the loop for  $i=1,2,\dots,n$ . As a matter of terminology, we say that  $X_i$  “points to”  $X_j$  (symbolically,  $X_i \rightarrow X_j$ ) if the routing table entry of  $X_i$  for destination  $Z$  shows node  $X_j$  as the next hop to  $Z$ . Then, for each  $X_i$ ,  $X_i \rightarrow X_{i+1}$  for  $i=1,2,\dots,n$ , and furthermore  $X_n \rightarrow X_1$ .

Let  $T_i$  be the destination sequence number for the route entry at  $X_i$  for destination  $Z$ . Then,  $T_i \leq T_{i+1}$  whenever  $X_i \rightarrow X_{i+1}$ , because of the processing of the RREP specified in Section 2.1.2. Since  $T_1 \leq T_2 \leq \dots \leq T_n \leq T_1$ , evidently the destination sequence numbers are the same for every node  $X_i$  in the routing loop. Moreover, if it were possible to create a routing loop, this

equality would have to be created. Furthermore, sequence numbers are all the same for all nodes in the loop. This information must have been disseminated to all nodes in the loop by the same RREP transmitted from the source to the destination.

Consider now the metric used to select the next hop. Since  $X_i \rightarrow X_{i+1}$  only if  $T_{i+1} > m_n + (n - 1)$ . But because  $T_i \leq T_{i+1}$  and  $n = 0$ ; this is a contradiction.

An inductive argument can be used to show that there can be the minimum length of a routing loop. We can always construct another routing loop of length  $k$  just by modifying the route to point to  $X_2$  instead of  $X_1$ . For  $k \geq 3$ , showing that it is impossible to have a routing loop of length  $k$  using destination sequence numbers. This argument shows that routing loops cannot exist. Therefore, routing loops cannot exist. This means that there can be no routing loops.

Formálny dôkaz, že smerovanie v AODV vytvára slučky je uvedený v článku (van Glabbeek et al. 2013).

2013GlabbeekEtAlMswim.pdf

1 of 10

136.50%

Index

- Introduction 7
- AODV 2
- The AODV RFC 3
- AODV Yields Loops 5
- AODV Implement... 7
- Methodology 8
- Related Work 9
- Discussion & Con... 9
- References 10

## Sequence Numbers Do Not Guarantee Loop Freedom —AODV Can Yield Routing Loops—

Rob van Glabbeek  
NICTA, Australia  
University of New South Wales,  
Australia  
rvrg@cs.stanford.edu

Peter Höfner  
NICTA, Australia  
University of New South Wales,  
Australia  
Peter.Hoefner@nicta.com.au

Wee Lum Tan  
NICTA, Australia  
University of Queensland,  
Australia  
WeeLum.Tan@nicta.com.au

Marius Portmann  
NICTA, Australia  
University of Queensland,  
Australia  
marius@itee.uq.edu.au

### ABSTRACT

In the area of mobile ad-hoc networks and wireless mesh networks, sequence numbers are often used in routing protocols to avoid routing loops. It is commonly stated in protocol specifications that sequence numbers are sufficient to *guarantee* loop freedom if they are monotonically increased over time. A classical example for the use of sequence numbers is the popular Ad hoc On-Demand Distance Vector (AODV) routing protocol. The loop freedom of AODV is not only a common belief, it has been claimed in the abstract of its RFC and at least two proofs have been proposed. AODV-based protocols such as AODVv2 (DYMO) and HWMP also claim loop freedom due to the same use of sequence numbers.

In this paper we show that AODV is not a priori loop free; by this we counter the proposed proofs in the literature. In fact, loop freedom hinges on non-evident assumptions to be made when resolving ambiguities occurring in the RFC. Thus, monotonically increasing sequence numbers, by themselves, do *not* guarantee loop freedom.

### Categories and Subject Descriptors

C.2.2 [Network Protocols]: Routing protocols; Protocol verification; F.3.1 [Specifying and Verifying and Reasoning about Programs]: Invariants

### Keywords

AODV; loop freedom; process algebra; routing protocols; wireless mesh networks

### 1. INTRODUCTION

Wireless Mesh Networks (WMNs), which can be considered to include Mobile Ad-hoc Networks (MANETs), have gained considerable popularity and are increasingly deployed in a wide range of application scenarios, including emergency response communication, intelligent transportation systems, mining and video surveillance. They are self-organising wireless multi-hop networks that can provide broadband communication without relying on a wired backhaul infrastructure, a benefit for rapid and low-cost network deployment.

Highly dynamic topologies are a key feature of WMNs and MANETs, due to mobility of nodes and/or the variability of wireless links. This makes the design and implementation of robust and efficient routing protocols for these networks a challenging task, and a lot of research effort has gone into it.

Loop freedom is a critical property for any routing protocol, but it is particularly relevant and challenging for WMNs and MANETs. Descriptions as in [9] capture the common understanding of loop freedom: “A routing-table loop is a path specified in the nodes’ routing tables at a particular point in time that visits the same node more than once before reaching the intended destination.” Packets caught in a routing loop, until they are discarded by the IP Time-To-Live (TTL) mechanism, can quickly saturate the links and have a detrimental impact on network performance. It is therefore critical to ensure that protocols prevent routing loops.

Sequence numbers, indicating the freshness of routing information, have been widely used to guarantee loop freedom, in particular for distance vector protocols such as DSDV [20], AODV [19], AODVv2 (formerly known as DYMO) [21] and

# AODV: bez smerovacích slučiek?

Formálny dôkaz, že smerovanie v AODV vytvára slučky je uvedený v článku (van Glabbeek et al. 2013).

Dôvody:

- Nepresná špecifikácia protokolu
- Protokol je špecifikovaný ako IETF RFC
- Nedodržiavanie špecifikácie pri implementácii

# RFC: must, should, may

1. **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

# RFC: must, should, may

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

AODV RFC:

„Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field (see sections 6.3, 6.6.3).

# TORA (Temporally-Ordered Routing Algorithm)

Reaktívny protokol.

Link reversal: algoritmus založený na zmene orientácie hrán.

*Podpora:*

- Hľadania ciest
- Údržby ciest
- Odstraňovanie nepoužívaných ciest

# TORA: hľadanie ciest

TORA počíta orientovaný acyklický graf s koreňom v cieľovom uzle

QRY: query packet: obsahuje id cieľového uzlu (broadcast)

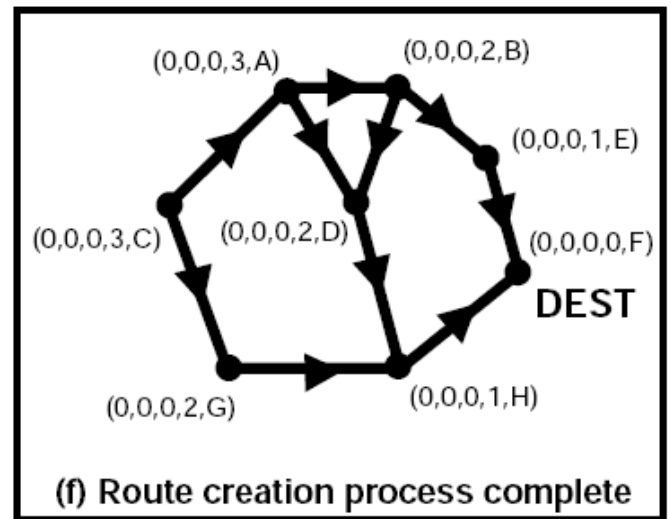
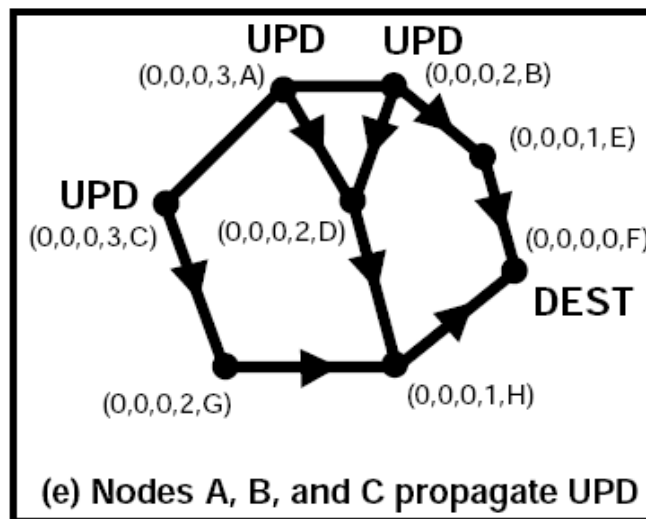
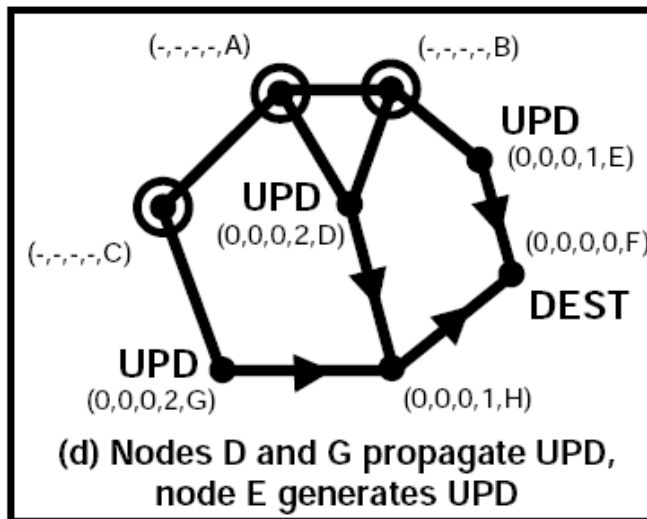
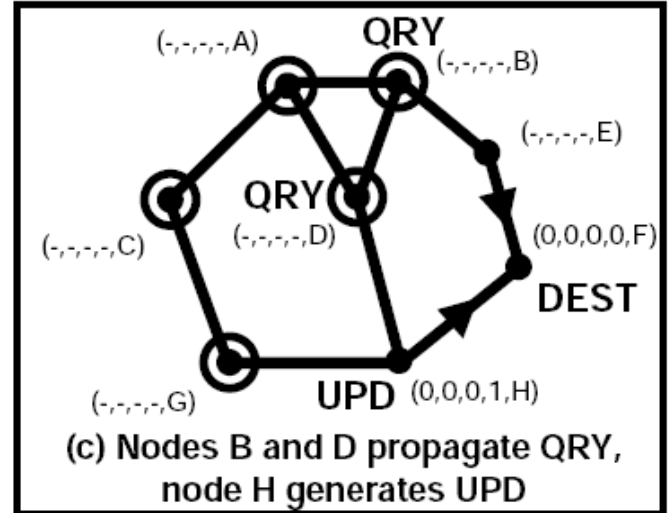
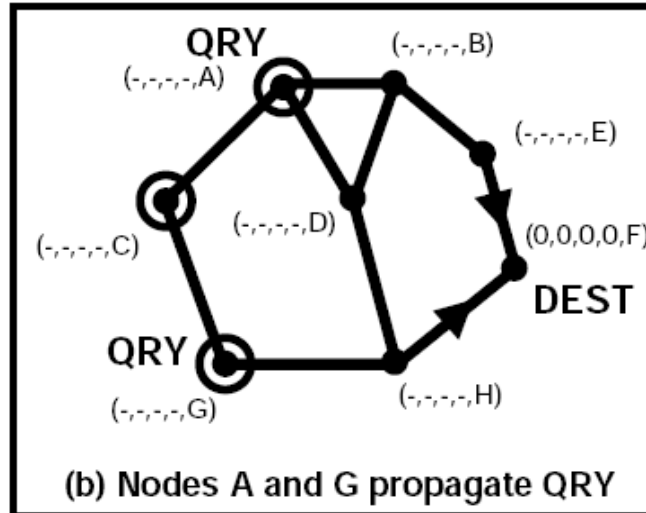
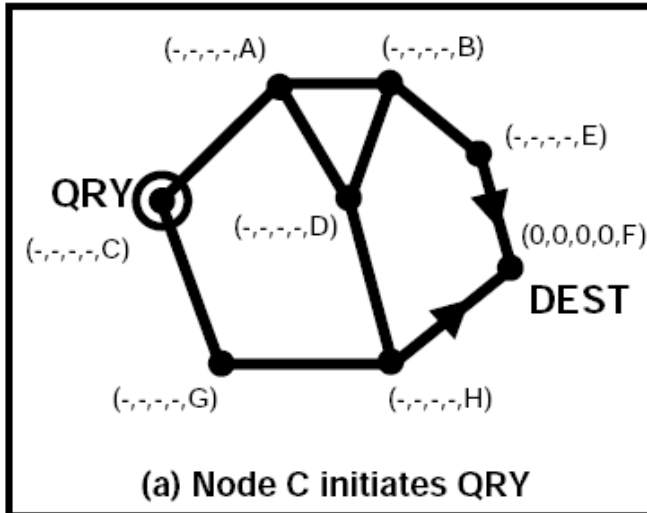
UPD: update packet: obsahuje výšku uzlu (broadcast)

Každý uzol  $i$  má uloženú:

- Výšku uzla  $H_i = (\text{reference level; delta to reference level}) = (\text{reference level, originator id; } r_i, \text{ delta to ref. level, id})$
- Výšku svojich susedov (pole)  $NH_i$
- Stav liniek k susedom (pole)  $LN_i$



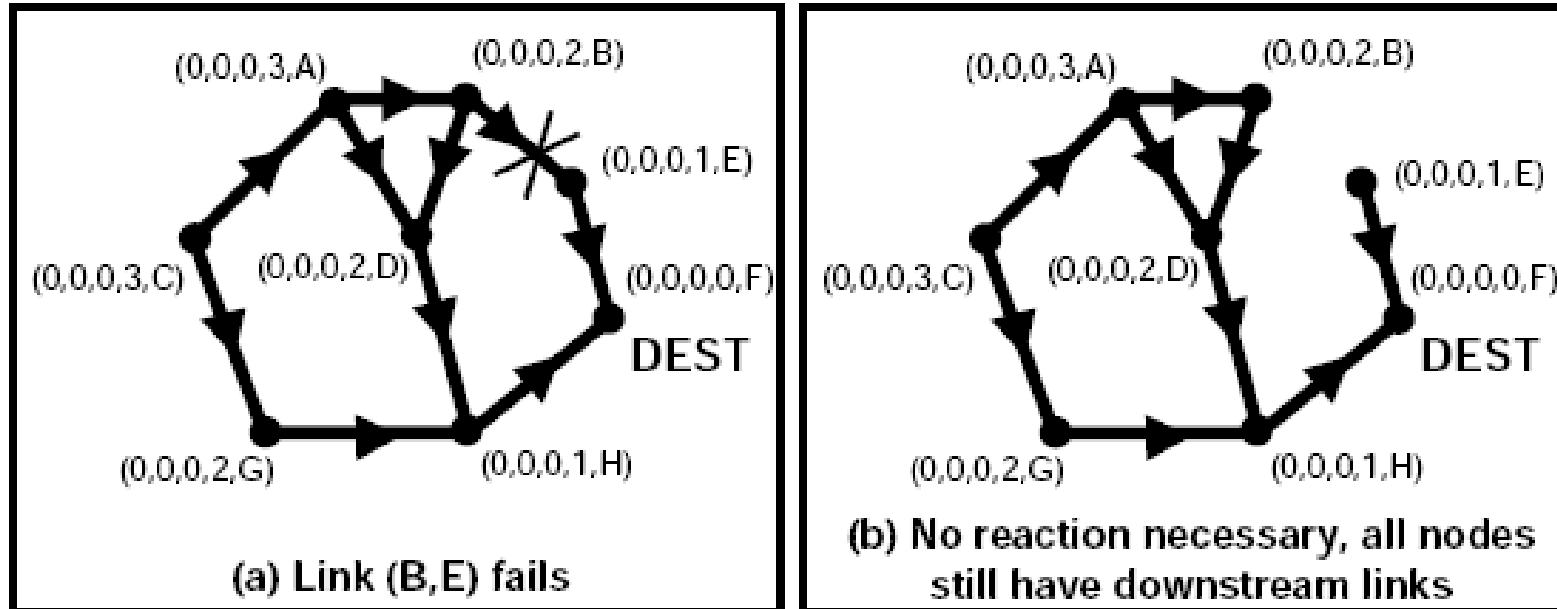
# TORA: príklad



- Linka (hrana) má orientáciu horeprúdom, doleprúdom alebo nedefinovanú
- Výška cieľového uzla je rovná ZERO, výška ďalších uzlov je NULL (ndefinovaná)
- Ak je cieľový uzol susedným uzlom, nastav jeho výšku na ZERO
- Aktualizuj stav liniek k susedom. Ak výška suseda je NULL, potom linka nemá orientáciu.

Ak uzol  $j$  potrebuje cestu k cieľovému uzlu, potom pošle (cez broadcast) QRY a nastaví  $RR=true$  (Route requested)

- Prípád A: sused, ktorý nemá žiadnu doleprúdovú linku prepošle QRY a nastaví  $RR=true$ . Ak  $RR=true$  potom nie je QRY poslaný ďalej.
- Prípád B: uzol  $i$  s doleprúdovou linkou a výškou NULL aktualizuje svoju výšku ( $height_i = height_j + 1$ ) a výšky susedov v  $NH_i$ . Potom pošle UPD (cez broadcast).
- Prípád C: uzol  $i$  s doleprúdovou linkou a výškou inou ako NULL, ak už poslal UPD potom prestane preposielať QRY, v opačnom prípade pošle UPD.

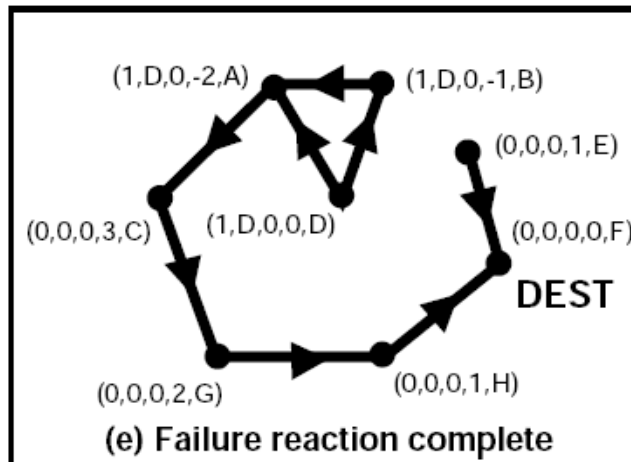
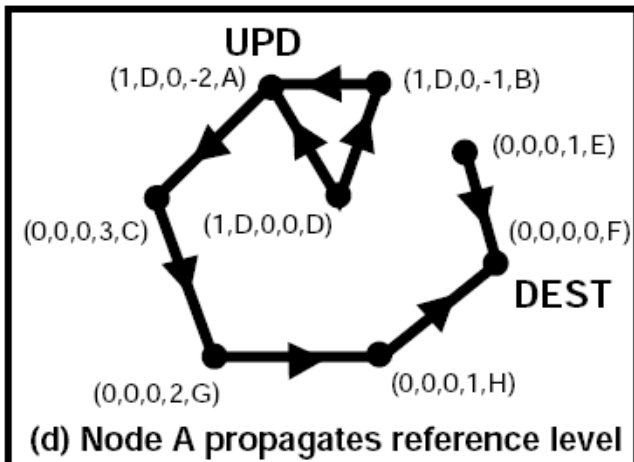
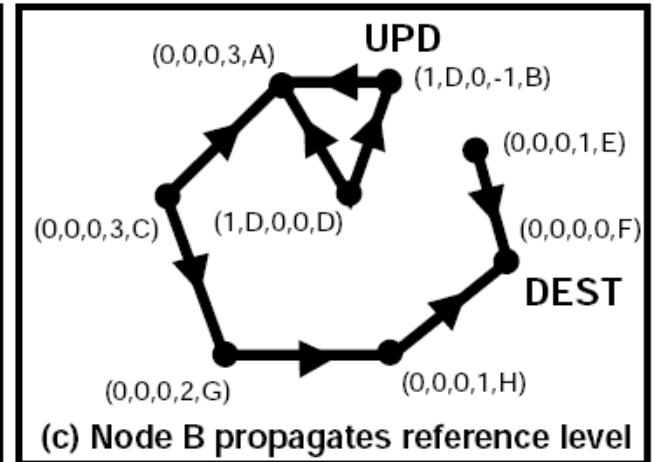
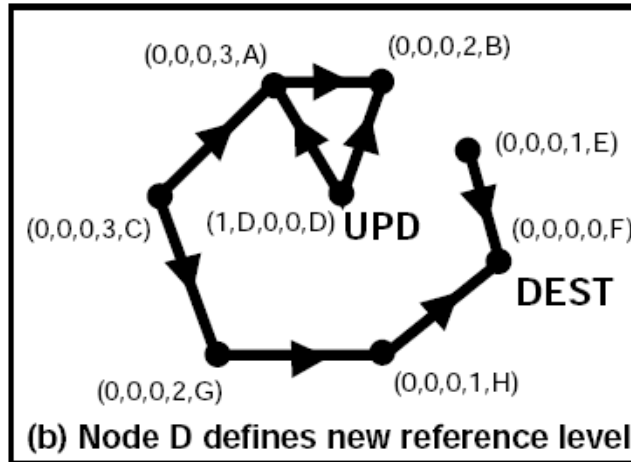
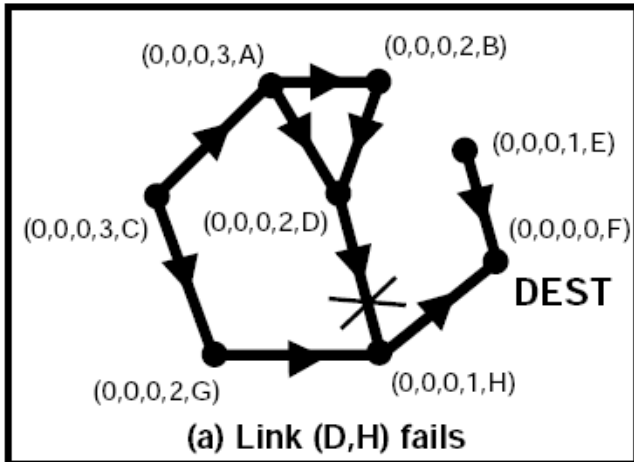


Ak existuje doleprúdová linka, žiadna reakcia nie je potrebná

Ak uzol nemá žiadnu doleprúdovú hranu, zmení orientáciu všetkých hrán.

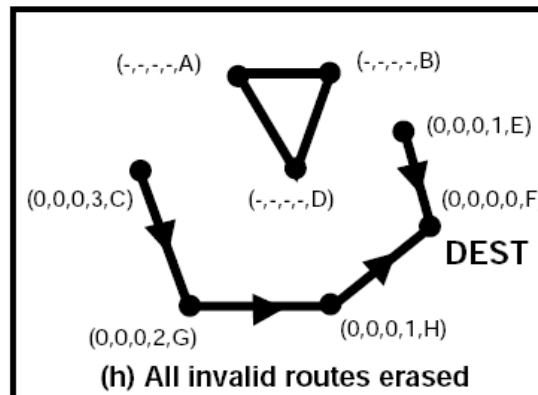
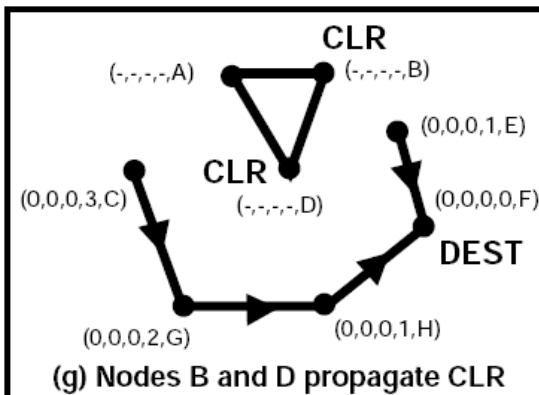
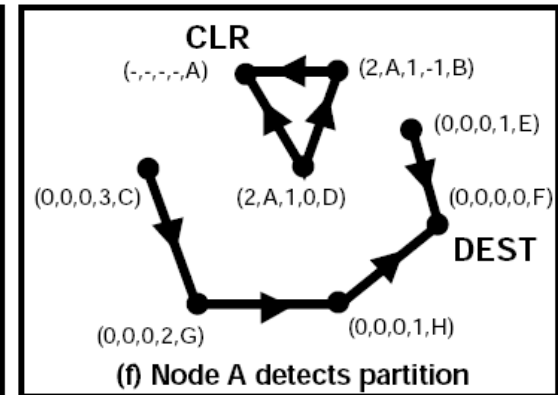
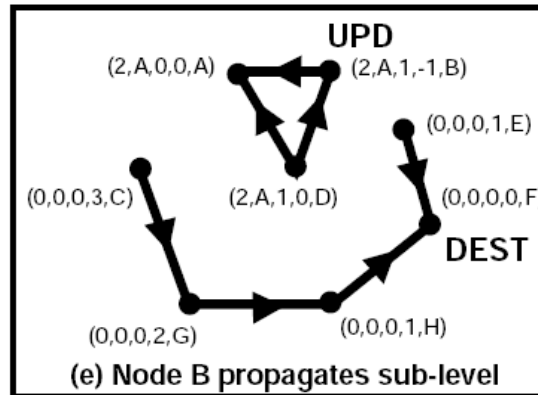
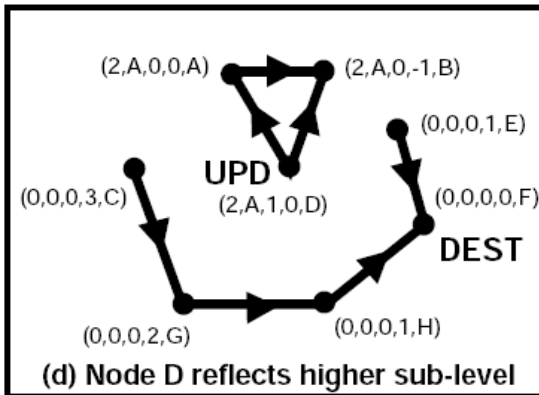
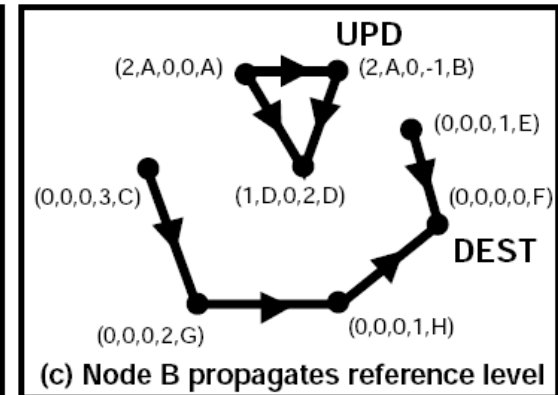
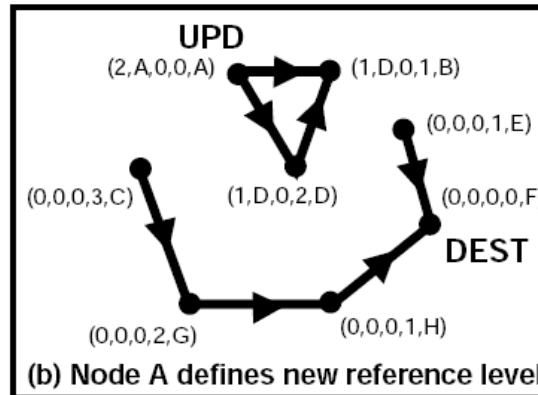
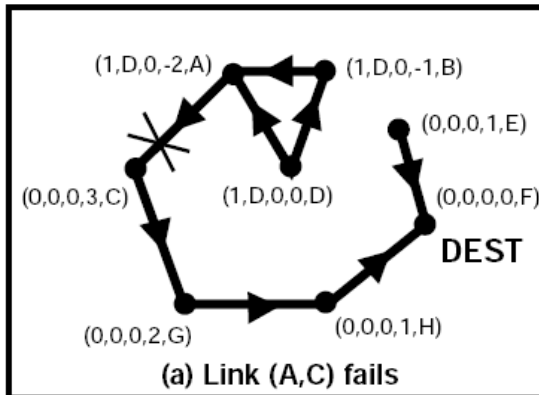
Uzol zmení orientáciu len tých hrán, ktorých orientácia ešte nebola zmenená.

Ak uzol nemôže zmeniť orientáciu hrany, pretože bola zmenená susedným uzlom, potom bol nájdený izolovaný komponent. Takýto uzol nastaví príznak „odzrkadlenia“ a zmení orientáciu všetkých hrán. Zmena orientácie s týmto príznakom sa šíri až k pôvodnému uzlu, ktorý stratil doleprúdovú linku. Tento uzol následne cez broadcast pošle CLR, ktorý vynuluje používané dátové štruktúry.



Ak doleprúdová linka neexistuje, potom je potrebné nastaviť novú referenčnú úroveň (reference level), prípadne inkrementovať sublevel.

# TORA: zrušenie ciest (CLR)



# TORA: propagating, reflecting reference level

Hlavné mechanizmy:

- Propagating: uzol i prepošle referenčnú hladinu svojho najvyššieho suseda a zvolí si výšku nižšiu ako výška jeho susedov.
- Reflecting: hladina, ktorá ešte nebola „odzrkadlená“ bola prijatá od všetkých susedov. Uzol i odzrkadlí vyšší sub-level tak, že nastaví bit r.



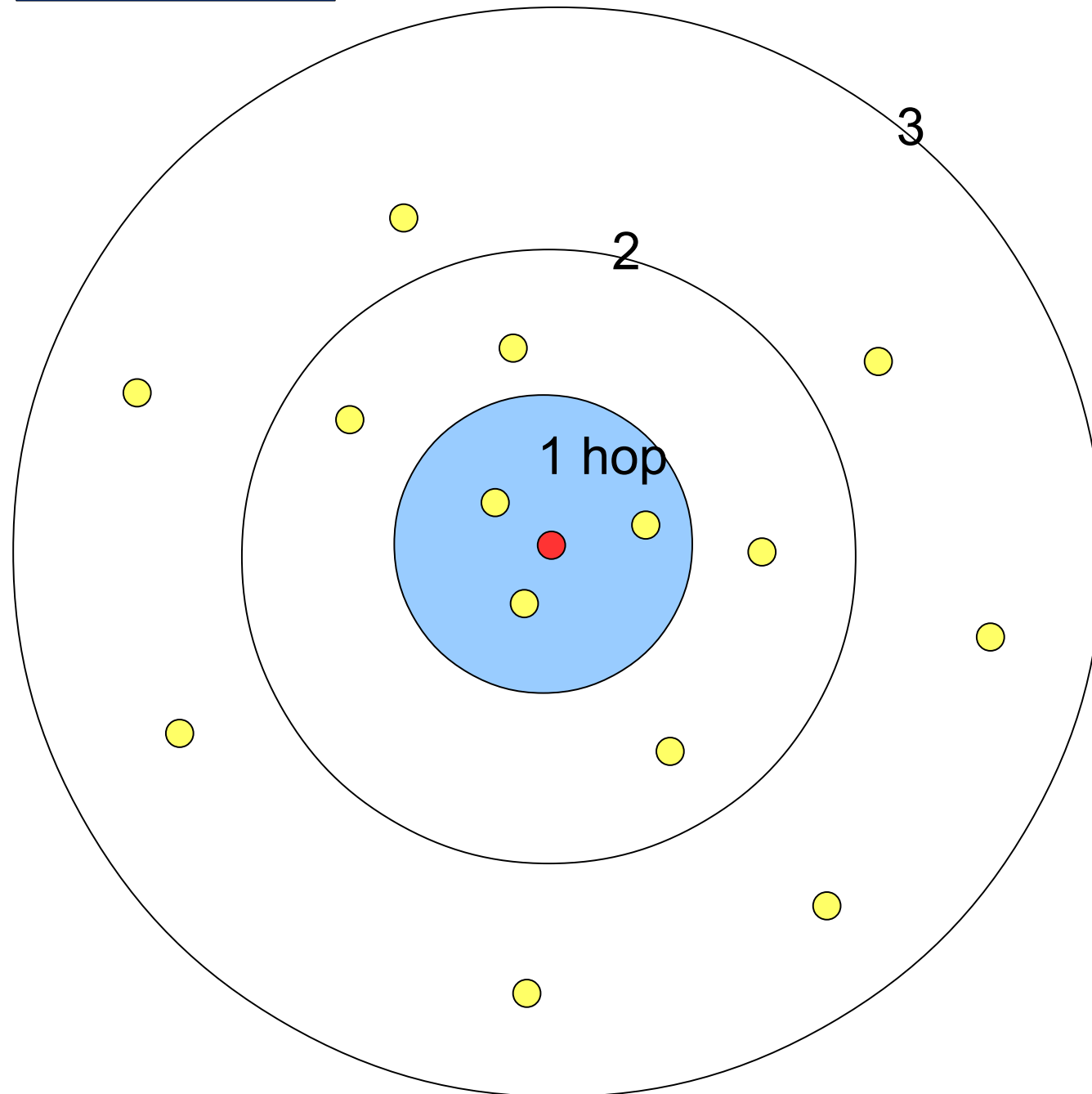
- Distribuovaná údržba ciest
- Cesty bez slučiek
- Ak je to možné, vypočíta viacero ciest k cieľovému uzlu
- Lokálna reakcia (RERR nie je lokálna reakcia)
- Minimalizácia komunikácie medzi uzlami

# Fisheye routing (FSR)

*Stratégia:* Kvalita informácie o smerovaní sa znižuje so vzdialenosťou k cieľovému uzlu. Cesty sú presnejšie blízko cieľového uzla.

Proaktívne, link state smerovanie.

# Fisheye routing: príklad



Rôzna frekvencia  
výmeny  
smerovacej  
informácie pre  
rôzne  
vzdialenosti od  
cieľového uzla.

*Proaktívne, link state smerovanie.*

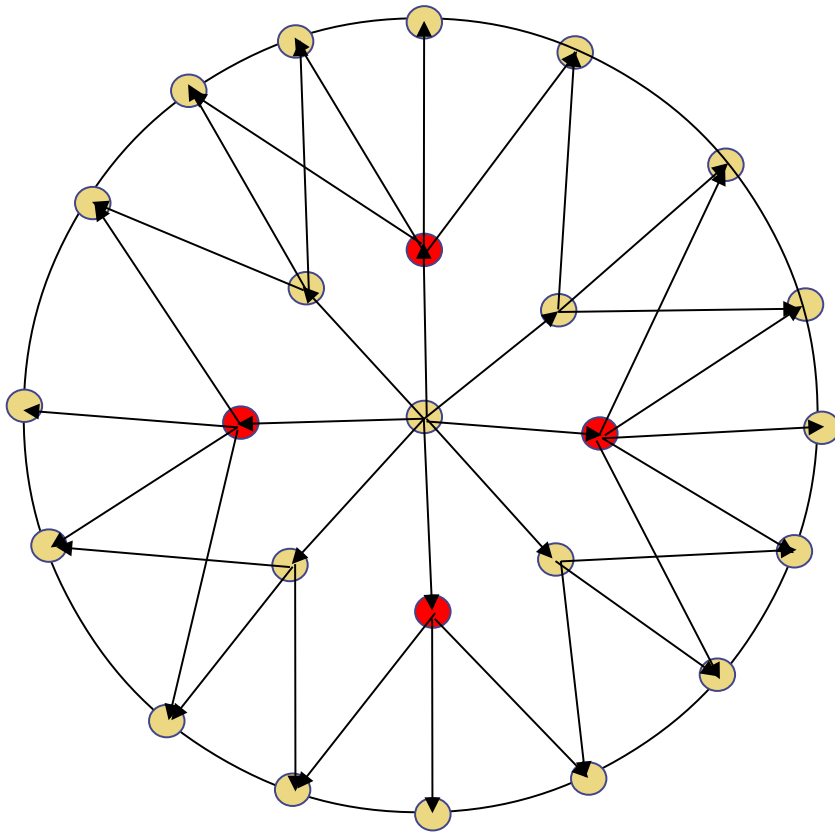
*Optimalizácia:* multipoint (uzly, ktoré pokrývajú všetky uzly do vzdialenosti 2 od zdrojového uzla).

Len multipoint uzly môžu preposlať topologickú informáciu. Ostatné uzly môžu túto informáciu prijať, ale nie preposlať.

HELLO pakety môžu byť použité na identifikáciu uzlov a na preposlanie topologickej informácie.

*Multipoint:*

- Informácie z HELLO paketov
- Vybraný tak, aby všetci susedia do vzdialenosti 2 boli pokrytí



4 multipoint uzly (červené)

Stratégia: použitie uzlov, ktoré majú vysoký stupeň (veľa susedov) na preposlanie smerovacej informácie.

# OLSR: zložitosť

Overhead (počet paketov s topologickou informáciou):  $O(n^2)$   
Pamäť potrebná pre uloženie smerovacej informácie:  $O(n^2)$

*Výhoda:* redukované zahltenie média

*Nevýhoda:* informácia o susedoch do vzdialenosti 2 je potrebná

Simulačné nástroje podporujú aj statické smerovanie, teda smerovanie vložené priamo používateľom a nie vypočítané smerovacím protokolom.

Statické smerovanie je užitočné pre off-line výpočet optimálneho smerovania a následné porovnanie s cestou vypočítanou smerovacím protokolom.

# Distance routing effect algorithm for mobility (DREAM)

*Stratégia:* čím je vzdialenosť dvoch uzlov väčšia, tým sa javí menšia ich vzájomná rýchlosť. Frekvencia výmeny smerovacej informácie je závislá od pohybu dvoch uzlov.

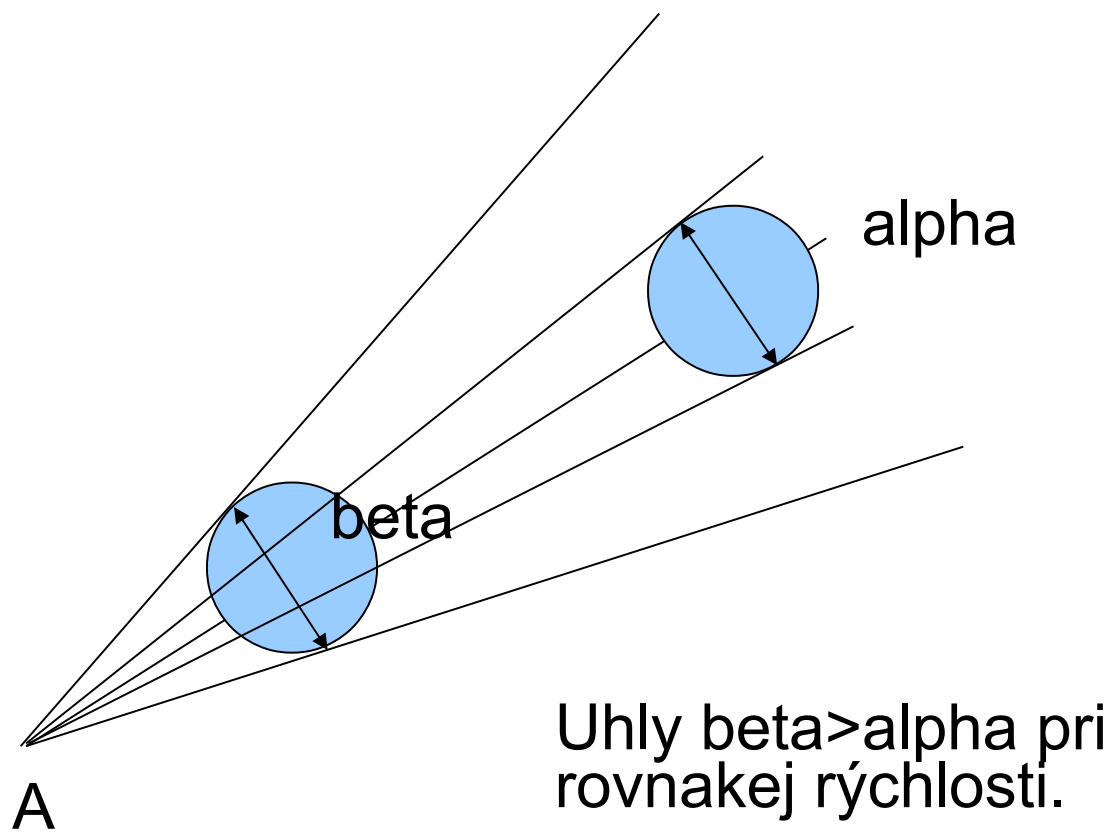
Predpoklad: každý uzol má prístup k GPS informácii.

Proaktívny protokol s výmenou GPS informácie.



Ak uzol A potrebuje poslať správu m uzlu B, potom použije lokačnú informáciu o uzle B aby získal smer k uzlu B. Správa je preposlaná susedom v danom smere a tí postupujú rovnako až pokým správa nie je doručená uzlu B.

GPS informácia je preposielaná cez broadcast. Čím je vzdialenosť dvoch uzlov väčšia, tým menej často je preposielaná.



Proaktívne, link state smerovanie.

Stratégia: organizovanie uzlov do zhlukov (clusterov).

*Výhoda:* podpora pre skupinový pohyb.

*Nevýhoda:* ak sa líder zhluku pohne je potrebné zvolit' nového lídra, čo môže mať za následok zvýšenú spotrebu energie.

Typy uzlov:

- Líder: koordinátor zhluku.
- Gateway uzol: uzol ležiaci medzi dvoma zhlukmi, sprostredkúva komunikáciu medzi zhlukmi.
- Vnútorne uzly: všetky ostatné uzly.

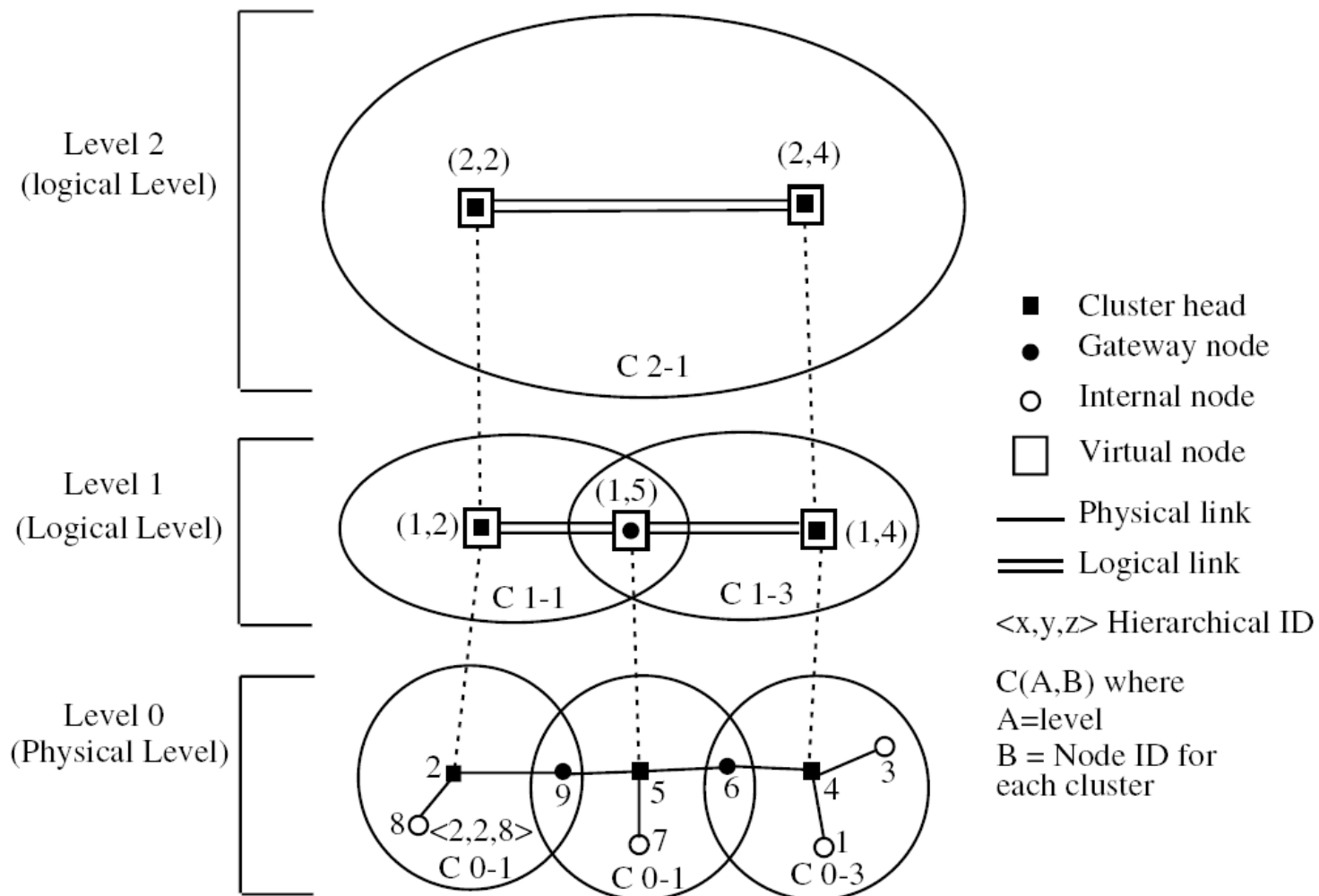
HID: Hierarchické ID

Uzol 8: HID (2,2,8)

Uzol 3: HID (4,4,3)

Spojenie 8-3

Fyzické spojenie: (2,9,5,6,4)

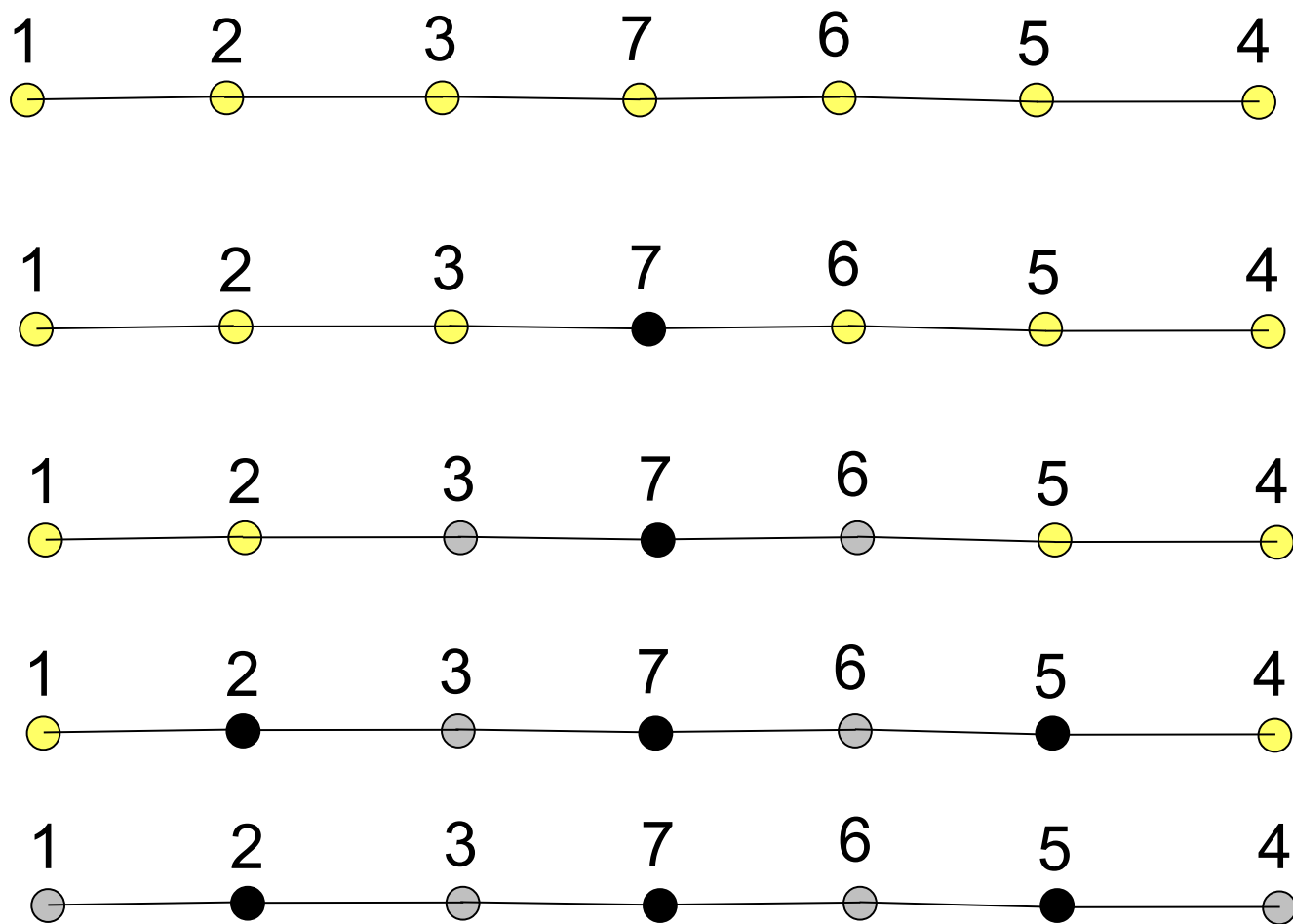


## *Maximálna nezávislá množina*

Výpočet:

1. Uzol sa stane lídrom, ak žiaden jeho sused nie je líder, v prípade konfliktu sa stane líder, ak má nižšie (vyššie) id (IP adresu).
2. Všetky susediace uzly sa stanú členmi zhuku.
3. Ukončenie: keď je každý uzol buď líder alebo člen zhuku.

# Formovanie zhlukov

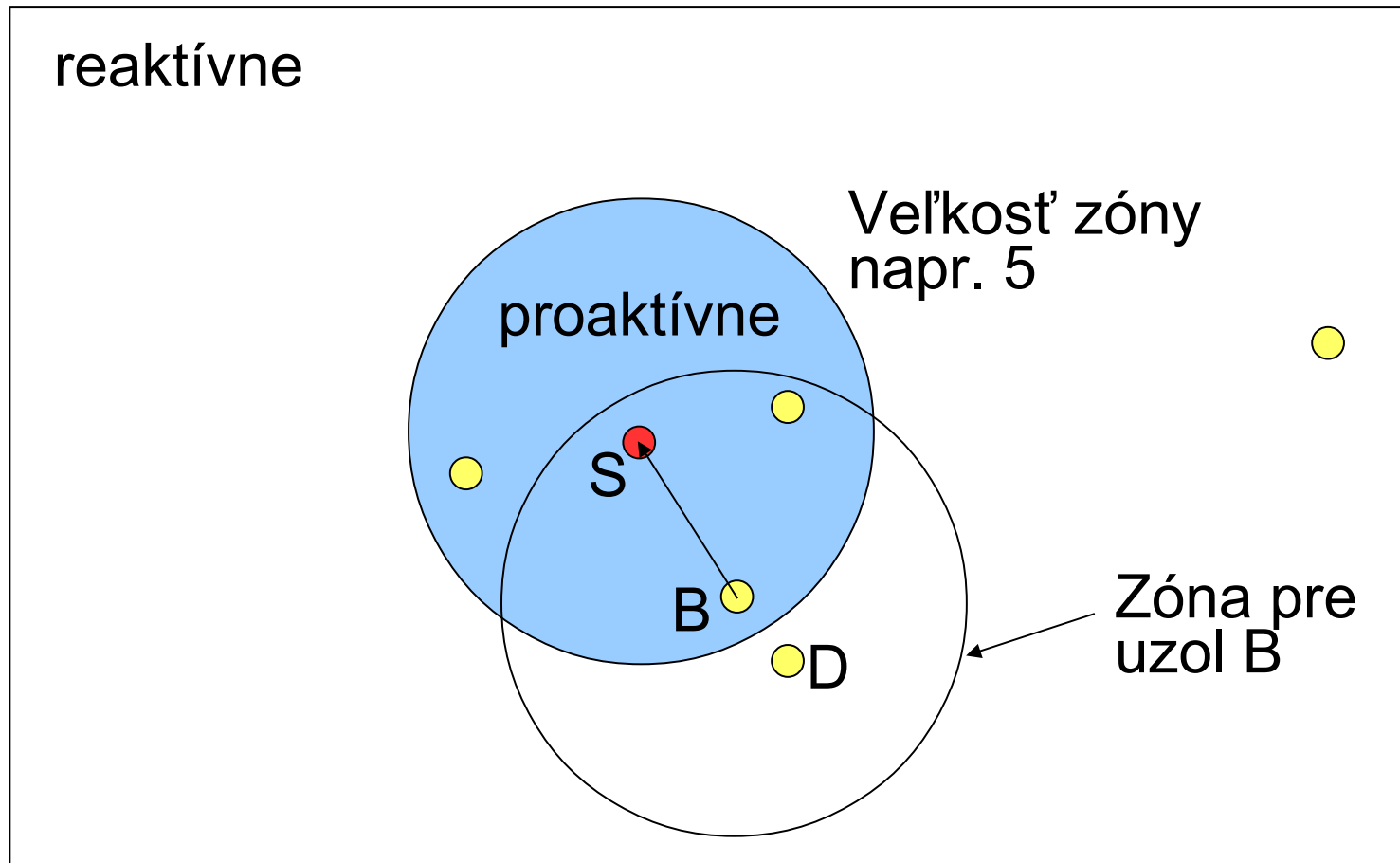


# Zone routing protocol (ZRP)

Hybridné smerovanie: proaktívne a reaktívne smerovanie.

Zóna: podmnožina uzlov do vzdialenosti  $n$  od zdrojového uzla využíva proaktívne smerovanie. Pre ostatné uzly je využívané reaktívne smerovanie.

Výhoda: uzly za hranicou zóny odpovedajú s RREP.



Veľkosť smerovacej tabuľky je ohraničené veľkosťou zóny a počtom cieľových uzlov.



# Smerovanie založené na probabilistickom preposielaní RREQ

Gossip based ad hoc routing

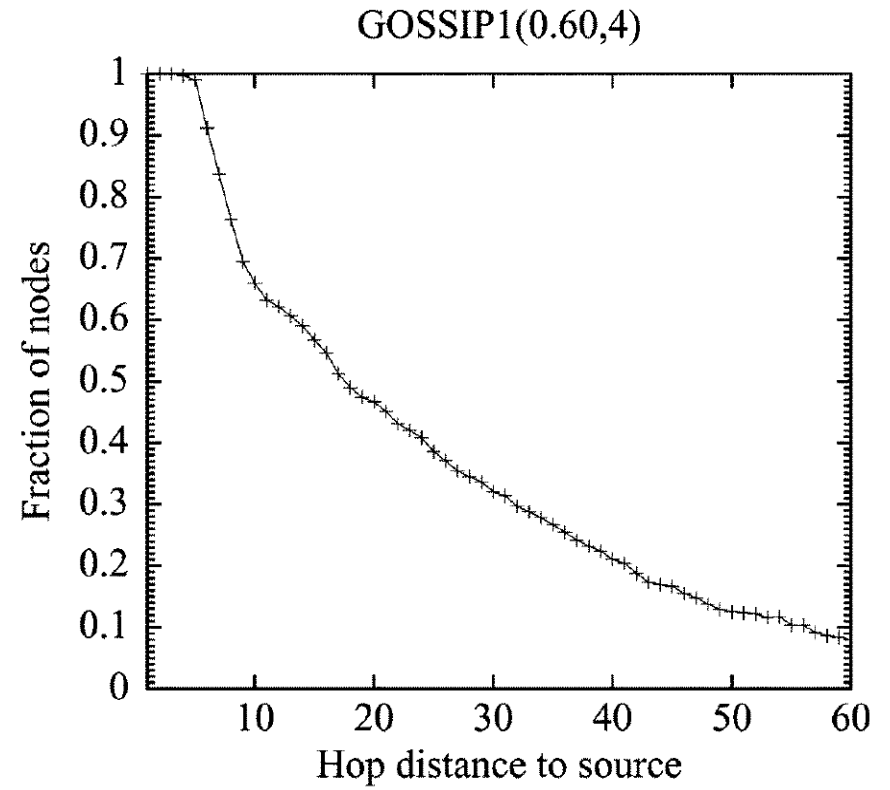
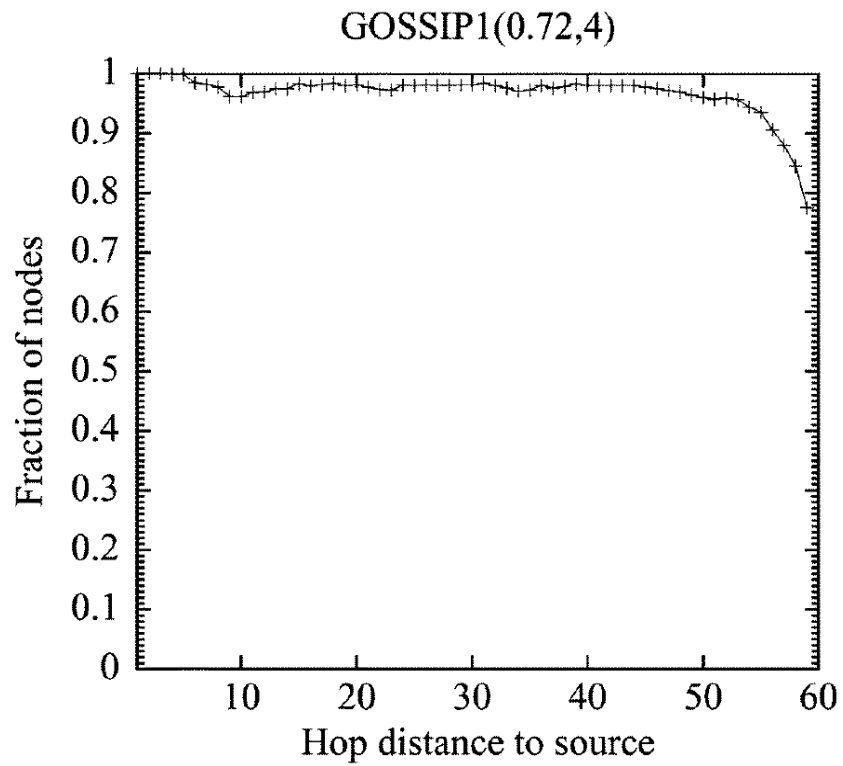
Pakety sú preposielané s pravdepodobnosťou  $p$ .

GOSSIP1( $p$ ): RREQ sú preposielané s pravdepodobnosťou  $p$ .

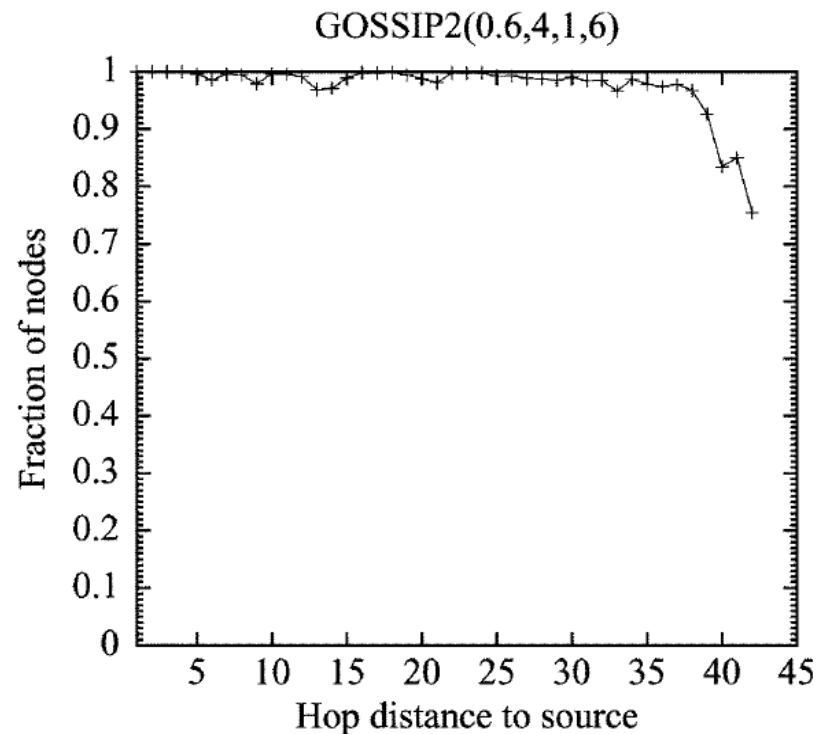
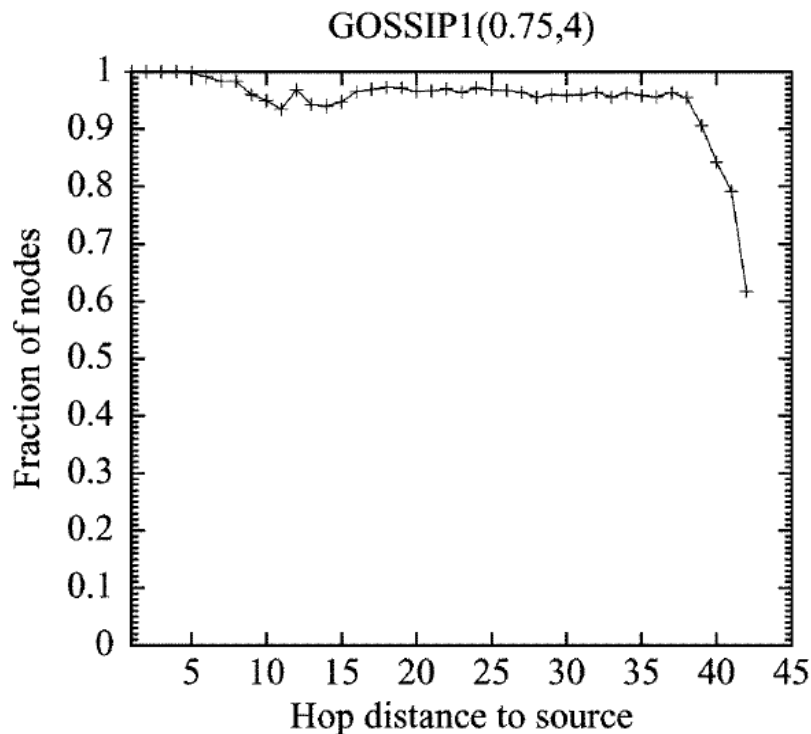
GOSSIP1( $p,k$ ): RREQ sú do vzdialenosti  $k$  preposielané s pravdepodobnosťou 1.0 a potom s pravdepodobnosťou  $p$ .

GOSSIP1( $p,0$ ) = GOSSIP1( $p$ )

# GOSSIP1(p,k)



GOSSIP2(p1, k, p2, n): RREQ su preposielané s pravdepodobnosťou 1.0 do vzdialenosti k, potom s pravdepodobnosťou p1. Ak má uzol menej ako n susedov sú preposielané s pravdepodobnosťou p2, kde  $p2 > p1$ .



# GOSSIP3(p, k, m)

GOSSIP3(p, k, m): uzol čaká pokým nedostane do určitého času RREQ aspoň od m uzlov, ak nie potom je RREQ preposlané, v opačnom prípade nie je RREQ preposlané.

Všetky druhy GOSSIP smerovania sú výrazne závislé od topológie siete.

Obrázky z Haas et al., *Gossip based ad hoc routing*, IEEE/ACM Transaction on Networking, 2006.

# Live Q&A

Live otázky a odpovede sú plánované cez Discord.