STU FEI

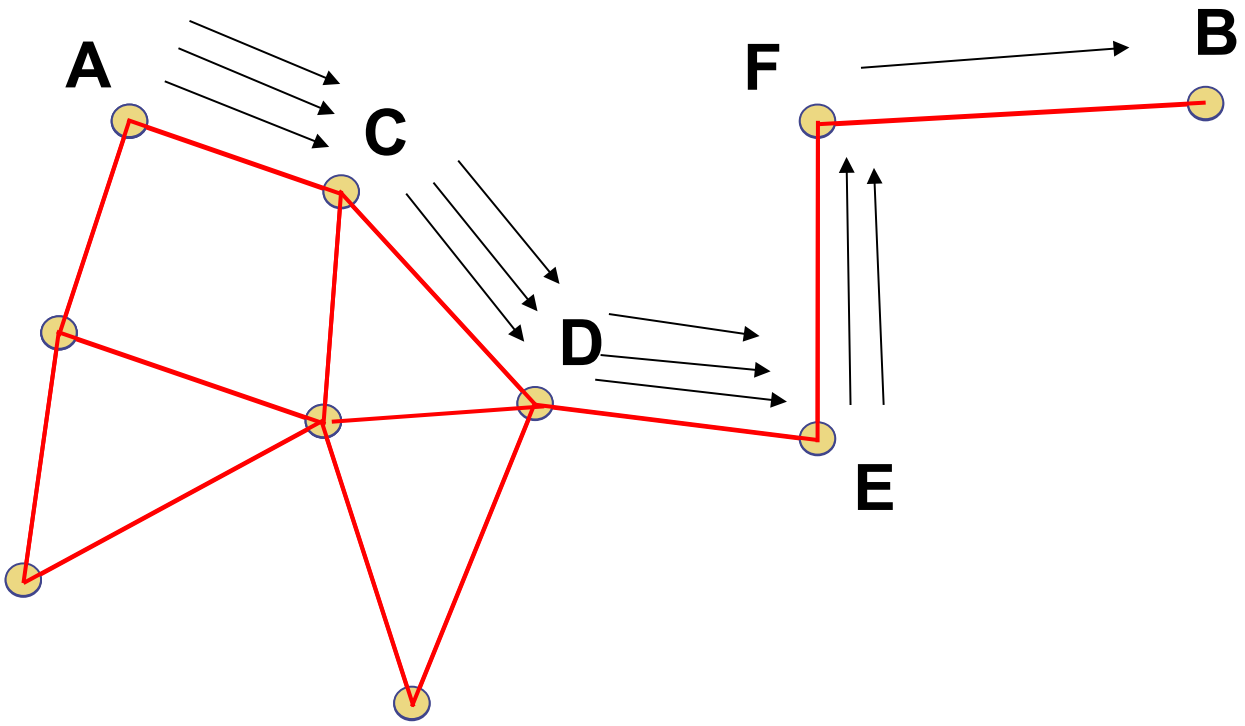
Počítačové siete 2

Multicast smerovanie, útoky v ad hoc sieťach

Martin Drozda

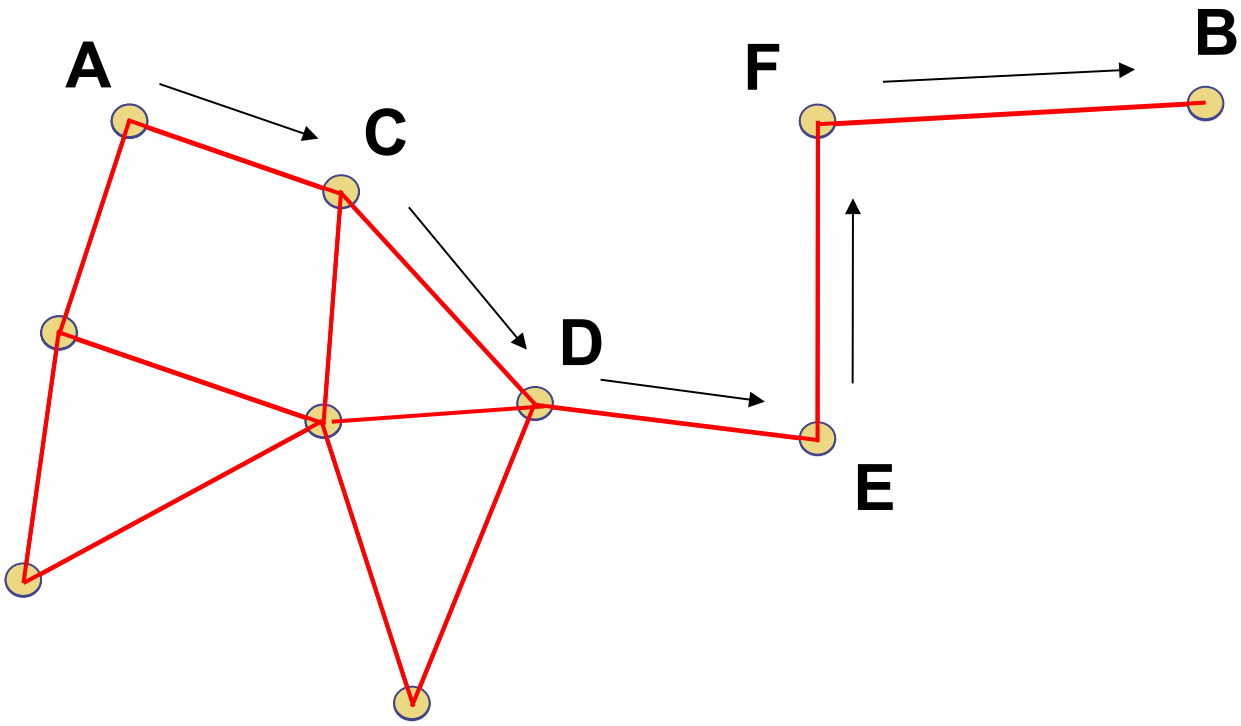
Unicast

Je potrebné poslať identickú informáciu uzlom E, F a B



Multicast

Multicast = jeden používateľ posiela identickú informáciu podmnožine používateľov



Multicast

Multicast = jeden používateľ posiela podmnožine používateľov

(Unicast = jeden používateľ posiela jednému používateľovi)

Potrebné vlastnosti:
- Pridanie sa k skupine
- Opustenie skupiny
- Údržba multicastového stromu
- Oprava prerušených liniek

Požiadavky:
- Distribuovaný algoritmus
- Bez slučiek (strom nemá slučky, preto je vhodný kandidát pre multicast)

Multicast: ciele

- Robustnosť vs efektívnosť
- Adaptívnosť
- Mobilita bez limitov
- Interoperabilita

Multicast AODV

RREQ-RREP-RERR spolu s MACT

MACT – multicast activation control message

Každý uzol udržuje 3 smerovacie tabuľky:

- Smerovaciu tabuľku identickú s AODV
- Multicast smerovaciu tabuľku: obsahuje IP lídra a IP celej skupiny
- Smerovaciu tabuľku s lídrami multicast skupín.

Multicast AODV

Smerovacia tabuľka:

- IP cieľového uzla
- Sekvenčné číslo cieľového uzla
- Vzdialenosť k cieľovému uzlu
- Nasledujúci uzol

Multicast AODV

Multicast smerovacia tabuľka:

- IP multicast skupiny (IPv6 poskytuje dosť adries)
- IP lídra multicast skupiny
- Sekvenčné číslo multicast skupiny
- Nasledujúci uzol k lídrovi skupiny

MAODV

RREQ formát:

- J_flag (join flag)
- R_flag (repair flag)

- source_addr
- source_seq
- dest_addr
- dest_seq
- hop_count

MAODV

RREP formát:

- R_flag (repair)
- U_flag (update)

- dest_addr
- dest_seq
- hop_count

MAODV je rozšírenie AODV.

Multicast AODV

MACT formát:

- J, P, G, U flags
- source_addr
- source_seq
- dest_addr

J	Join flag; príznak je nastavený, keď sa uzol chce stať členom multicast skupiny
P	Prune flag; príznak je nastavený, keď sa uzol chce odpojiť od multicast skupiny
G	Group Leader flag; príznak je nastavený, keď člen multicast stromu nevie opraviť prerušenú linku a signalizuje členovi skupiny, že sa má stať novým lídrom
U	Update flag; príznak je nastavený, keď uzol opraví prerušenú linku a vzdialenosť lídra je dôsledkom toho iná

MAODV: pristúpenie ku skupine

Pristúpenie a odchod musí byť vždy možné!

RREQ :
- J_flag=true
- dest_addr=multicast_group_IP
- seq_number=last_known_seq_number

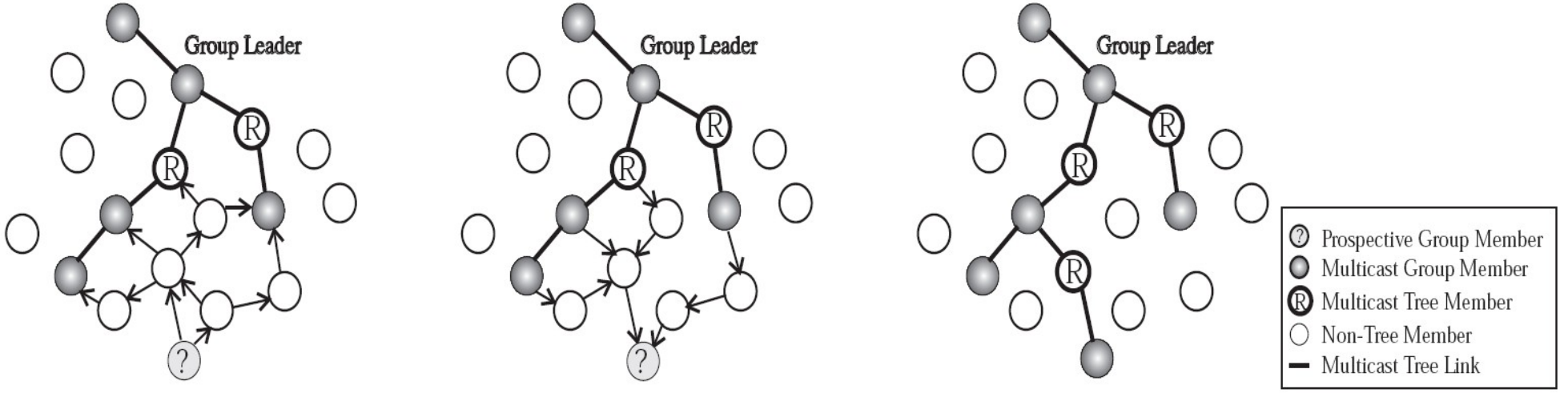
RREQ je poslané cez broadcast alebo unicast:

- unicast je využitý, keď cesta k lídrovi je známa
- broadcast v opačnom prípade

Len člen multicast stromu odpovie na RREQ.

Ak nepríde odpoveď RREP, potom sa tento uzol stane lídrom skupiny.

MAODV: pristúpenie



(a) RREQ Message Propagation (b) RREPs sent back to source (c) Multicast Tree Branch Addition

Multicast strom obsahuje aj uzly, ktoré nie sú členom multicast skupiny.

Obrázok zdroj:Elizabeth M. Royer and Charles E. Perkins. Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol. Proceedings of MobiCom '99, Seattle, WA, August 1999, pp. 207-218.

MAODV: pristúpenie

RREP:
- Pole Mgroup_hops inkrementované pri každom preposlaní uzlom
- Pole group_leader_addr nastavené na IP adresu lídra

Zdrojový uzol po prijatí RREP aktualizuje svoju multicast smerovaciu tabuľku

MAODV: pristúpenie

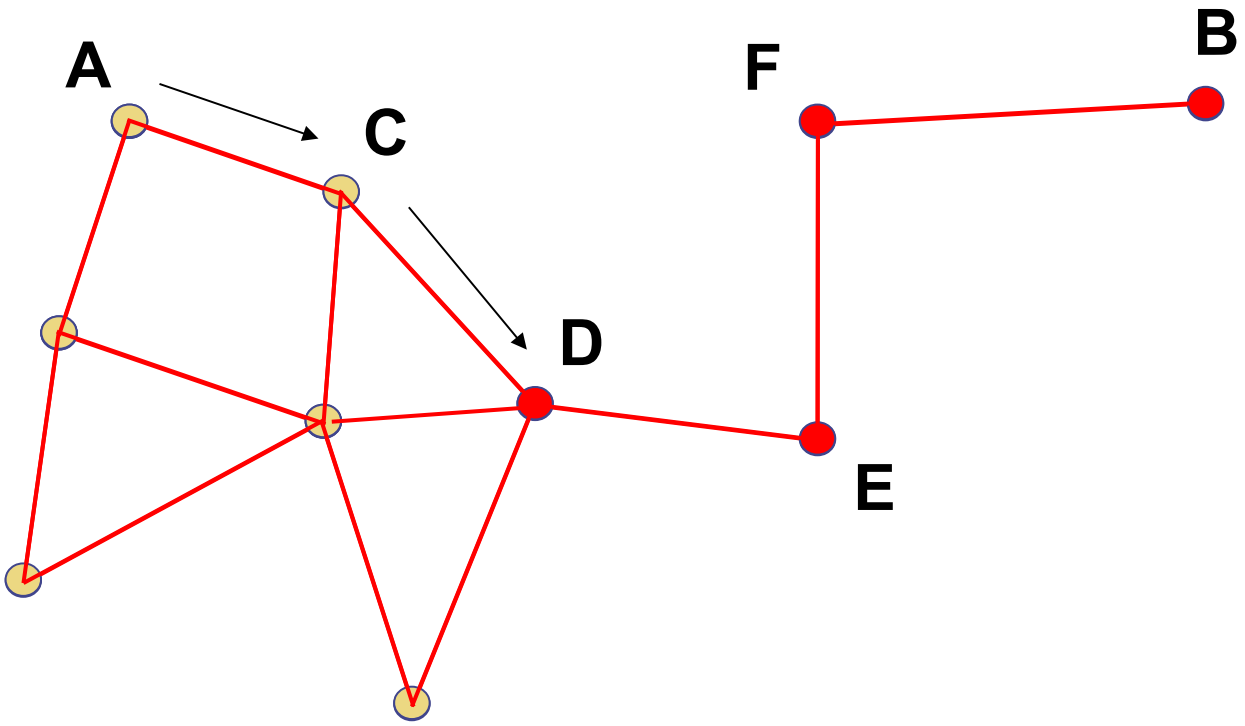
Aktivácia cesty s MACT:

- Zdrojový uzol čaká route_discovery_timeout
- Zdrojový uzol sa rozhodne pre najkratšiu cestu
- Zdrojový uzol pošle MACT s dest_addr=multicast_group_ID
- Nasledujúci uzol prepošle MACT, až po uzol, ktorý je členom multicast skupiny
- Uzol, ktorý poslal RREP, ale nedostal MACT zruší túto cestu v multicast smerovacej tabuľke po mtree_build millisekundách.

Použitie MACT zaručuje, že graf využitý na smerovanie je strom (a ten z definície nemá slučky)

MAODV: MACT

Zdrojový uzol môže prijať niekoľko RREP.



Smerovanie z uzla A, ak členmi multicast skupiny sú D, E, F, B.

MAODV: údržba

Líder skupiny je zodpovedný za udržovanie skupiny.

Líder skupiny pošle každých group_hello_interval seconds Hello správu.

Hello správa je implementovaná ako nevyžiadaný RREP s TTL vyšším ako priemer siete (parameter).

Hello správa obsahuje IP adresu lídra.

Líder inkrementuje multicast sekvenčné číslo, keď je to potrebné

Ak uzol prijme Hello, potom aktualizuje svoju tabuľku s lídrami skupín.

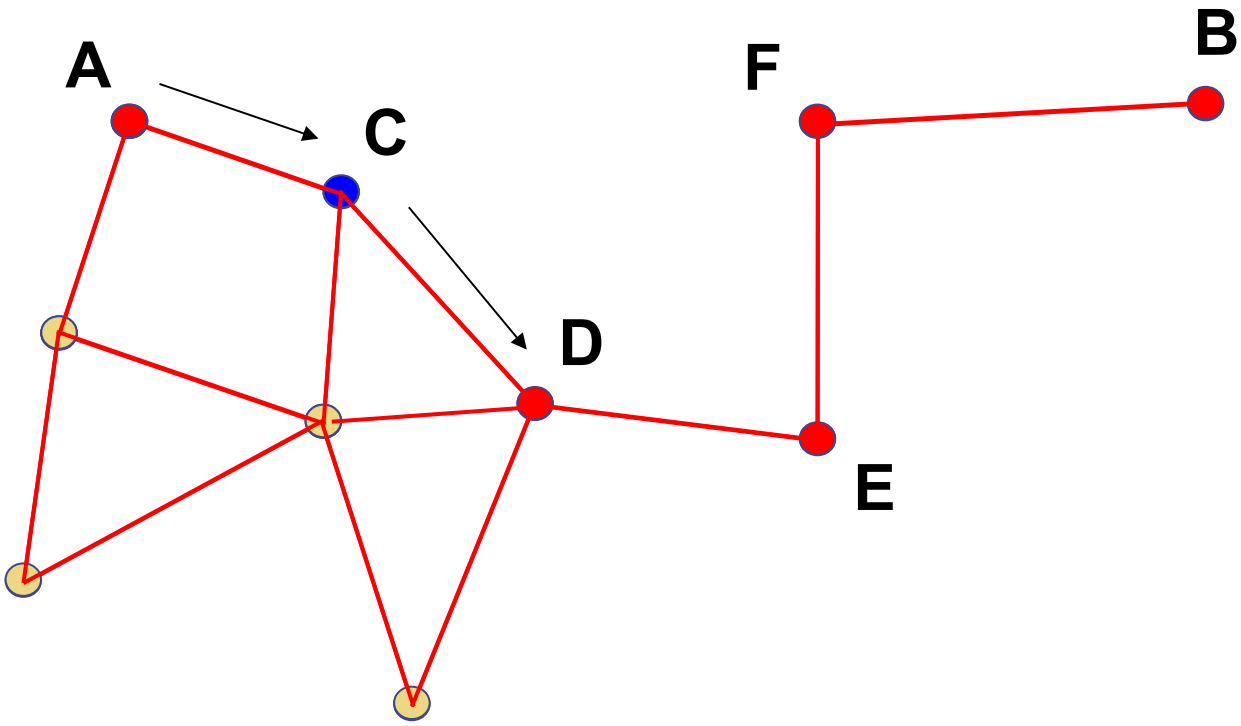
MAODV: odchod zo skupiny

Ak sa člen multicast skupiny rozhodne odísť je potrebné aktualizovať multicast strom a nepotrebné časti odstrániť (vykoná sa tzv. pruning).

- Uzol, ktorý je listom multicast stromu pošle MACT s P_flag príznakom nastaveným a dest_addr=multicast_group_ID.
- V opačnom prípade, keď uzol dostane MACT s P_flag príznakom nastaveným, ak uzol nie je člen multicast skupiny, potom prepošle MACT

MAODV: odchod zo skupiny

Ak sa uzol A rozhodne odísť, potom uzly C a D, ktoré nie sú členom multicast skupiny, sú odpojené z multicast stromu.



MAODV: oprava

Oprava je potrebná, ak je linka prerušená.

Detekcia po: hello_interval*(1+allowed_hello_loss)
hello_interval = 5s
allowed_hello_loss = 2

Uzol pošle RREQ s dest_addr=group_leader_ID, s nastaveným J_flag príznakom a Mgroup_Hop nastaveným na vzdialenosť od lídra.

Len uzly, ktoré sú bližšie ako Mgroup_Hop smú odpovedať s RREP.

Ak nie je prijatý žiadny RREP, potom sa po rreq_attempts stane lídrom skupiny (ak je člen skupiny). Ak uzol nie je členom multicast skupiny, potom pošle MACT s P_flag príznakom nastaveným a oddelí sa od multicast stromu.

Nový líder skupiny oznámi tento fakt pomocou Group hello s nastaveným príznakom U_flag_set.

MAODV: spájanie stromov

V prípade, uzol prijme Group hello od pôvodného lídra, potom je zrejmé, že stromy je možné spojiť.

Uzol sa pokúsi spojiť dva stromy, ak je členom multicast skupiny a ak jeho líder má menšie ID.

- Uzol pošle svojmu lídrovi RREQ s R_flag príznakom nastaveným.
- Líder skupiny povolí spojenie skupín pomocou RREP.
- Uzol pošle cez unicast RREQ s R_flag príznakom nastaveným lídrovi druhej skupiny.
- Líder druhej skupiny nastaví sekvenčné číslo na vyššie sekvenčné číslo týchto dvoch skupín.
- Líder druhej skupiny oznámi, že je líder spojených skupín pomocou Group hello s U_flag príznakom nastaveným.

On-demand multicast routing protocol

ODMRP nevyžaduje multicast strom, t.j. medzi uzlami môže existovať niekoľko ciest.

JOIN REQUEST: ak má uzol dátové pakety na poslanie

JOIN REPLY: ak uzol chce prijímať dátové pakety

Tabuľka členov: uzol v nej ukladá ID členov skupiny a časovú pečiatku každého prijatého JOIN REQUEST.

Smerovacia tabuľka: obsahuje ID a nasledujúci uzol pre cieľový uzol. Ak je prijatý nový JOIN REQUEST, potom je tabuľka aktualizovaná.

On-demand multicast routing protocol

- Ak chce uzol poslať paket do multicast skupiny, potom pošle JOIN REQUEST cez broadcast.

- Uzol, ktorý prijme JOIN REQUEST ho prepošle cez broadcast ďalej. Duplikátne JOIN REQUESTy nie sú preposlané.

- Uzol, ktorý prijme JOIN REQUEST aktualizuje svoju tabuľku členov.

- Uzol s neprázdnou tabuľkou členov prepošle túto tabuľku susedom cez broadcast (Join table).

- Keď uzol prijme Join table, overí či neobsahuje jeho ID. V pozitívnom prípade nastaví FG_flag príznak a pošle vlastnú Join table. Join table je preposielaná, až pokým nedosiahne zdrojový uzol.

ODMRP: soft state

Mäkký stav = soft state

Uzol, ktorý si želá opustiť multicast skupinu, prestane posielať JOIN REQUEST.

Na pristúpenie alebo opustenie skupiny netreba žiadny explicitný paket.

Útoky na ad hoc siete

Prečo: pre získanie prístupu k službám siete, z dôvodu šetrenia vlastných zdrojov, pripadne z dôvodu poškodenia siete.

Ako: útok jediným uzlom alebo skupinou uzlov.

Detekcia: pomocou uzlov, ktoré nie sú ovládané útočníkom.

Útok môže byť prevedený pomocou laptopov, uzly samotnej siete môžu byť v porovnaní výrazne menej výkonné a s obmedzenými zdrojmi (napr. napájané batériou).

Detekcia

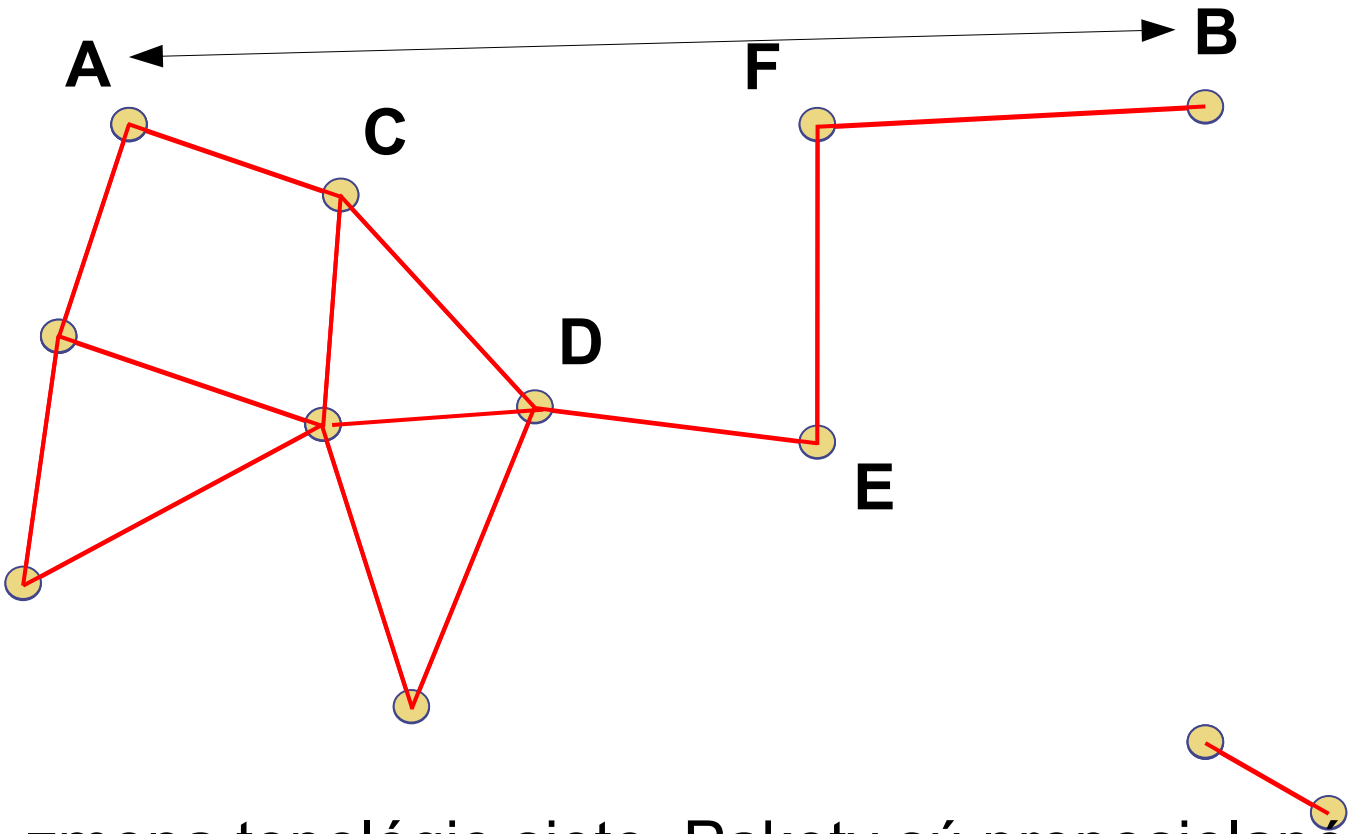
- Signatúra: potrebná distribúcia, čo v prípade ad hoc sietí môže byť energicky náročné.

- Anomálie: systém sa učí, čo je normálne a signalizuje odchýlku od normálneho správania.

Reputačné systémy: výpočet reputácie uzla na základe jeho správania.

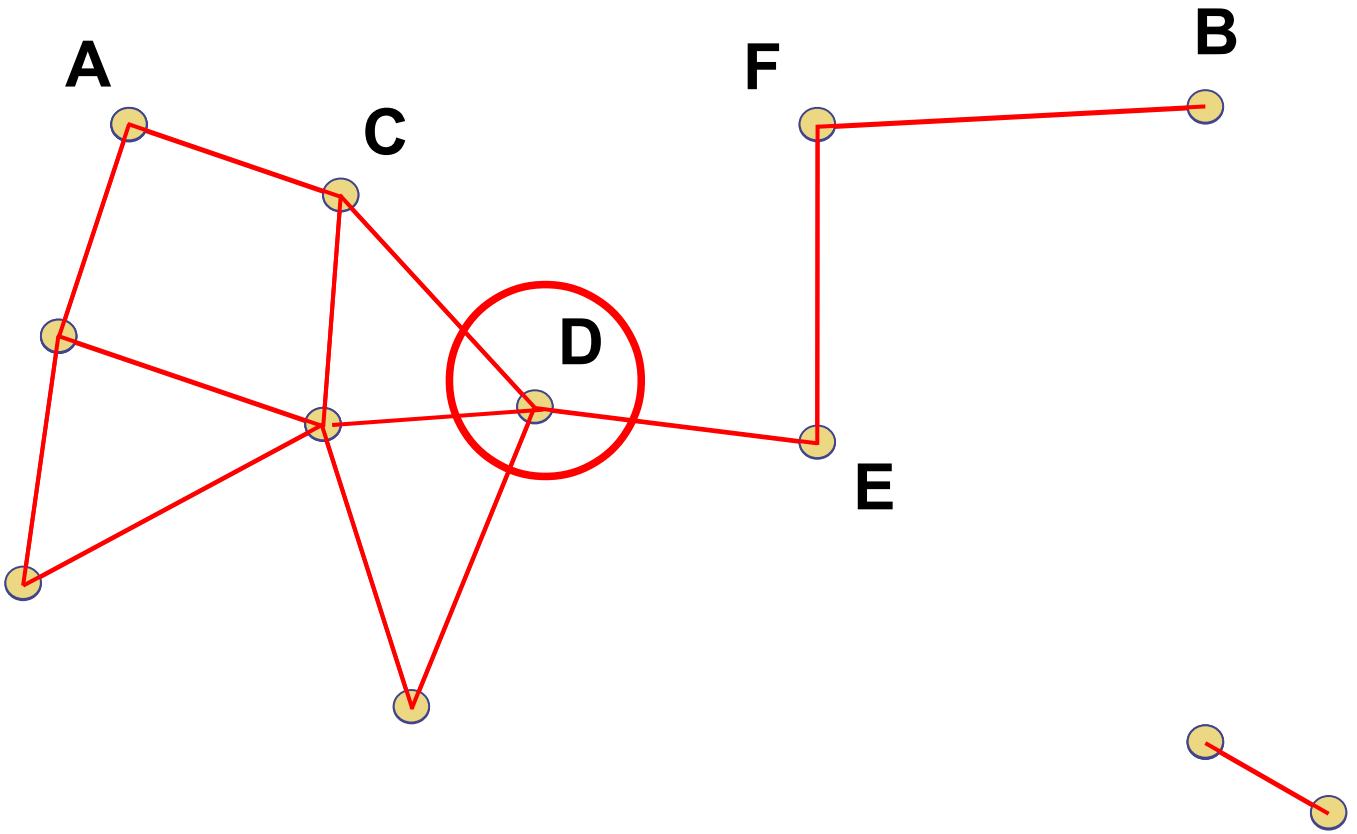
Anomaly (Merriam-Webster): something different, abnormal, peculiar, or not easily classified.

Wormhole (Star trek)



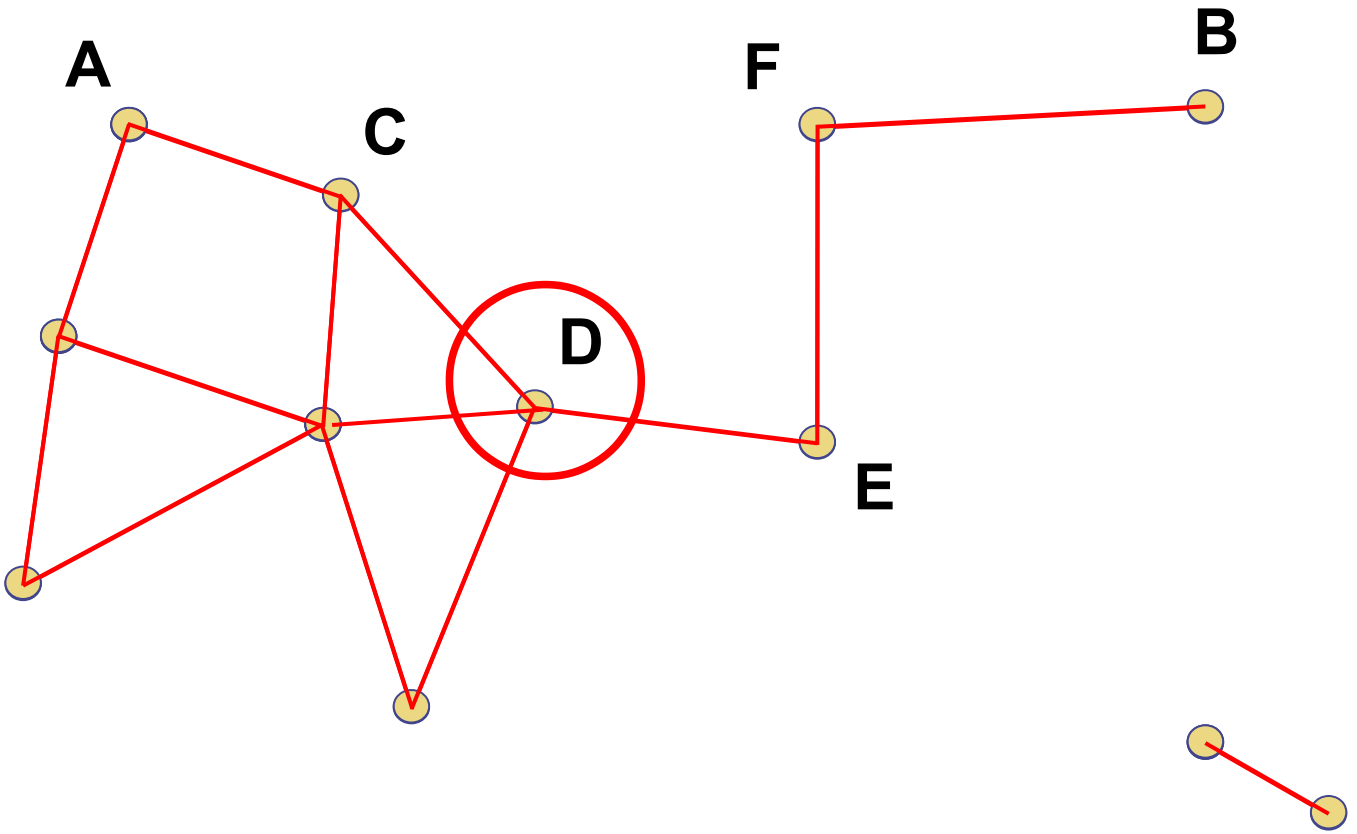
Nastane zmena topológie siete. Pakety sú preposielané cez wormhole (červiu dieru), ktorá je vytvorená útočníkom pomocou privátneho prepojenia dvoch uzlov (A a B). Takéto prepojenie môže byť výrazne rýchlejšie a teda viacej využívané. Wormhole môže byť kedykoľvek vypnutá.

Nepreposielanie paketov



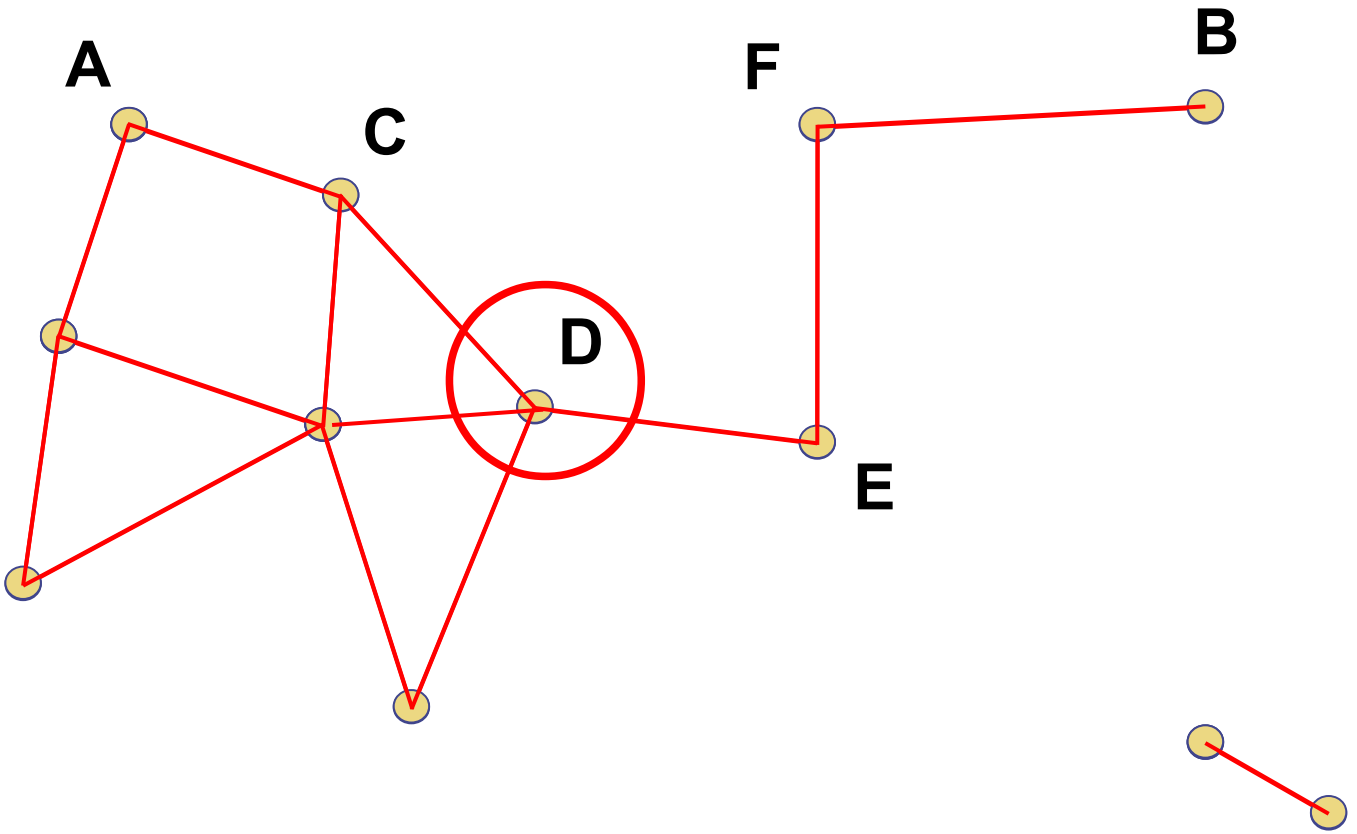
Uzol D neprepošle napr. 30% paketov. Ťažko detegovateľné pre nízku úroveň nepreposielania.

Oneskorovanie preposielania



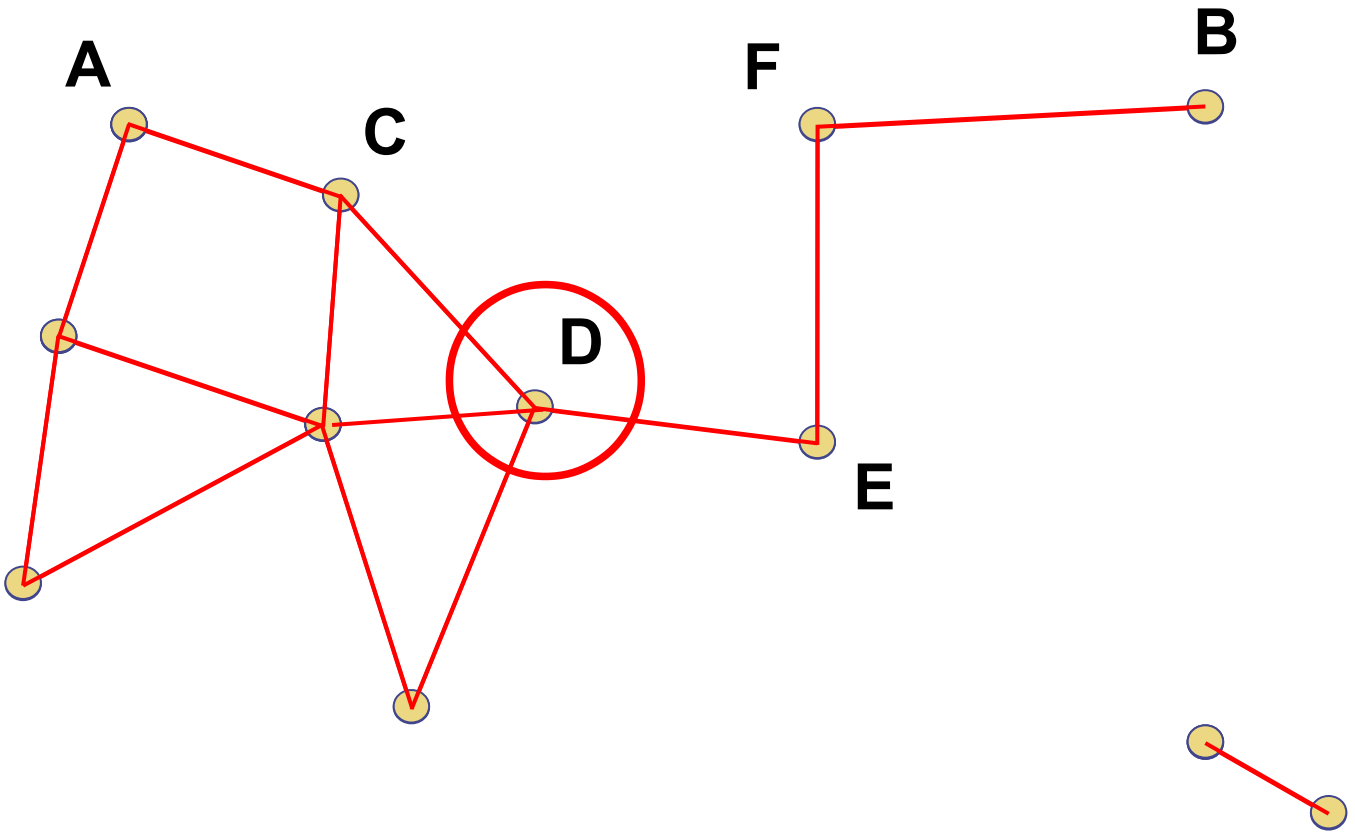
Uzol D oneskoruje preposielanie určitých paketov, čo môže viesť k prioritizácii preposielania.

Black hole



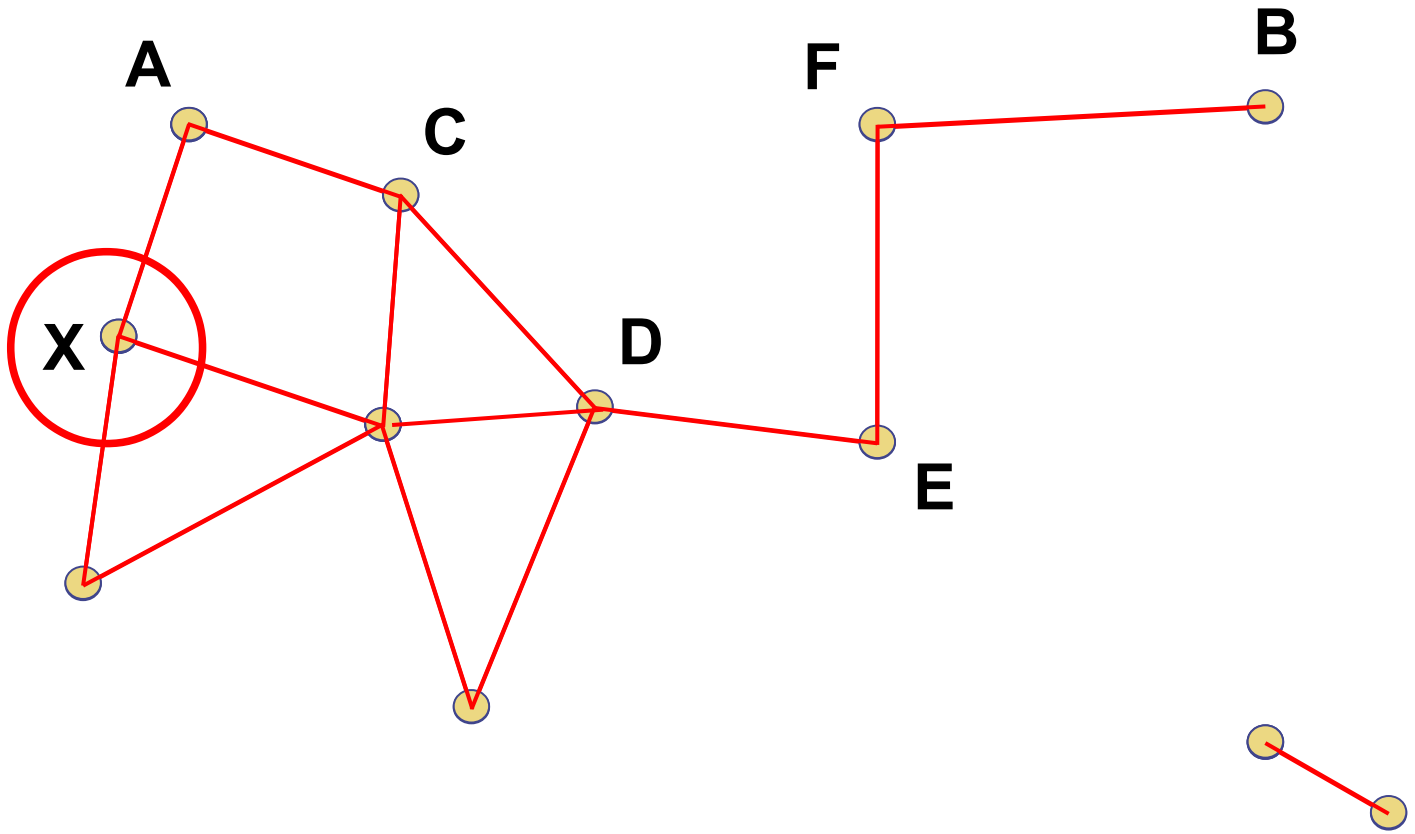
Black hole (čierna diera) je uzol, ktorý odpovie na každý RREQ s RREP, bez ohľadu na to, či cestu k cieľovému uzlu pozná alebo nie.

Gray hole



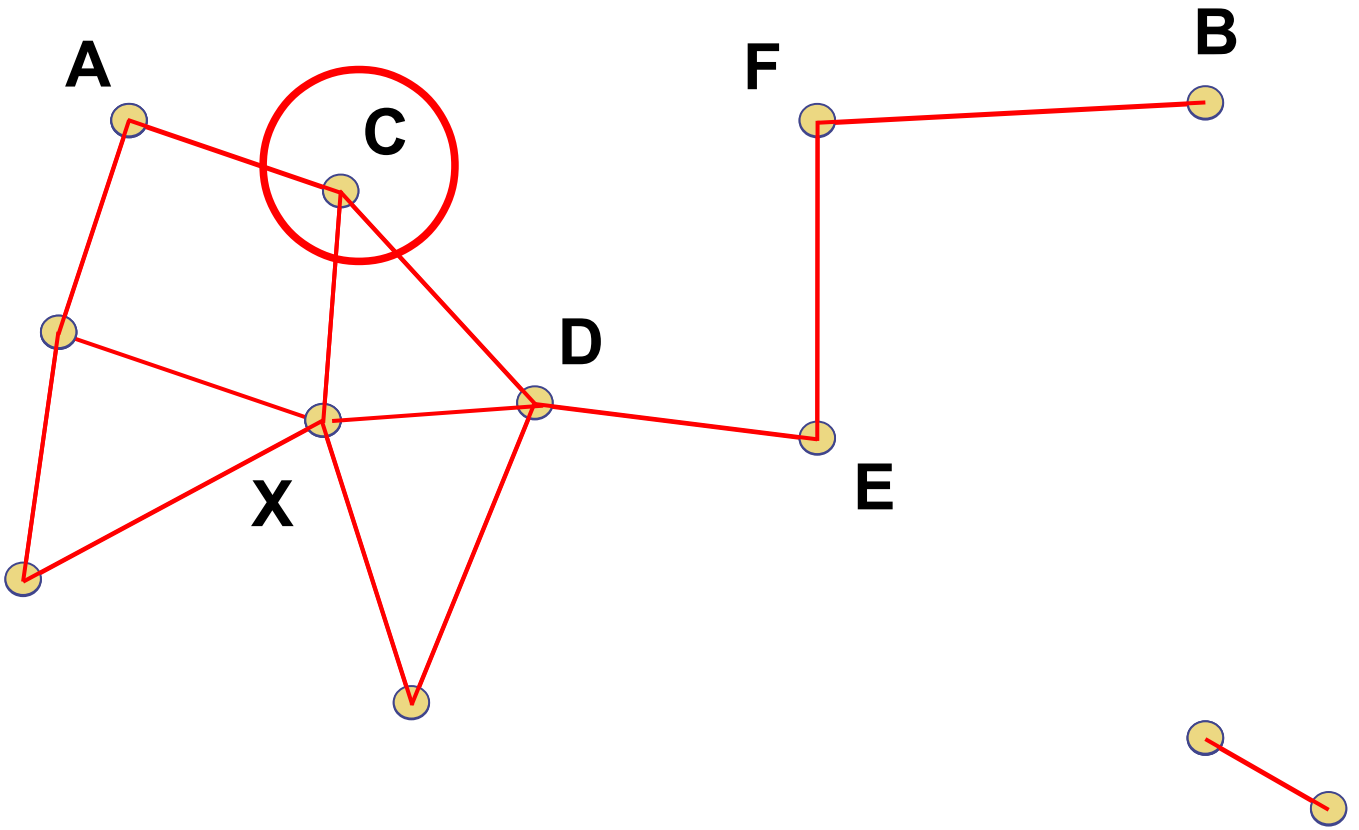
Uzol D sa správa normálne a inokedy ako čierna diera.

Zadržiavanie RREQ



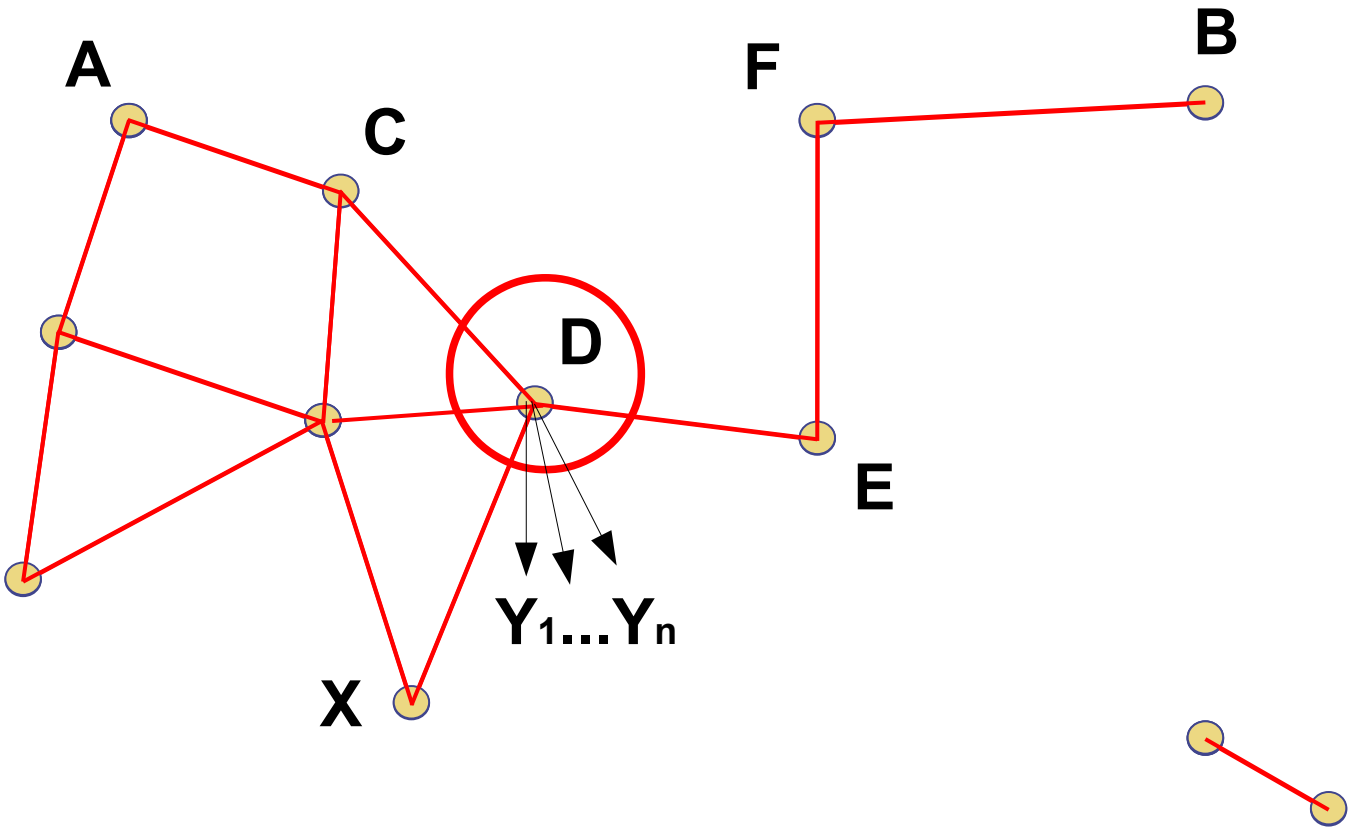
Útočník X preposiela niektoré RREQ skôr, niektoré neskôr. Ak je RREQ preposlaný skôr je väčšia šanca, že cesta bude využitá na preposielanie paketov.

Prepisovanie smerovacej tabuľky



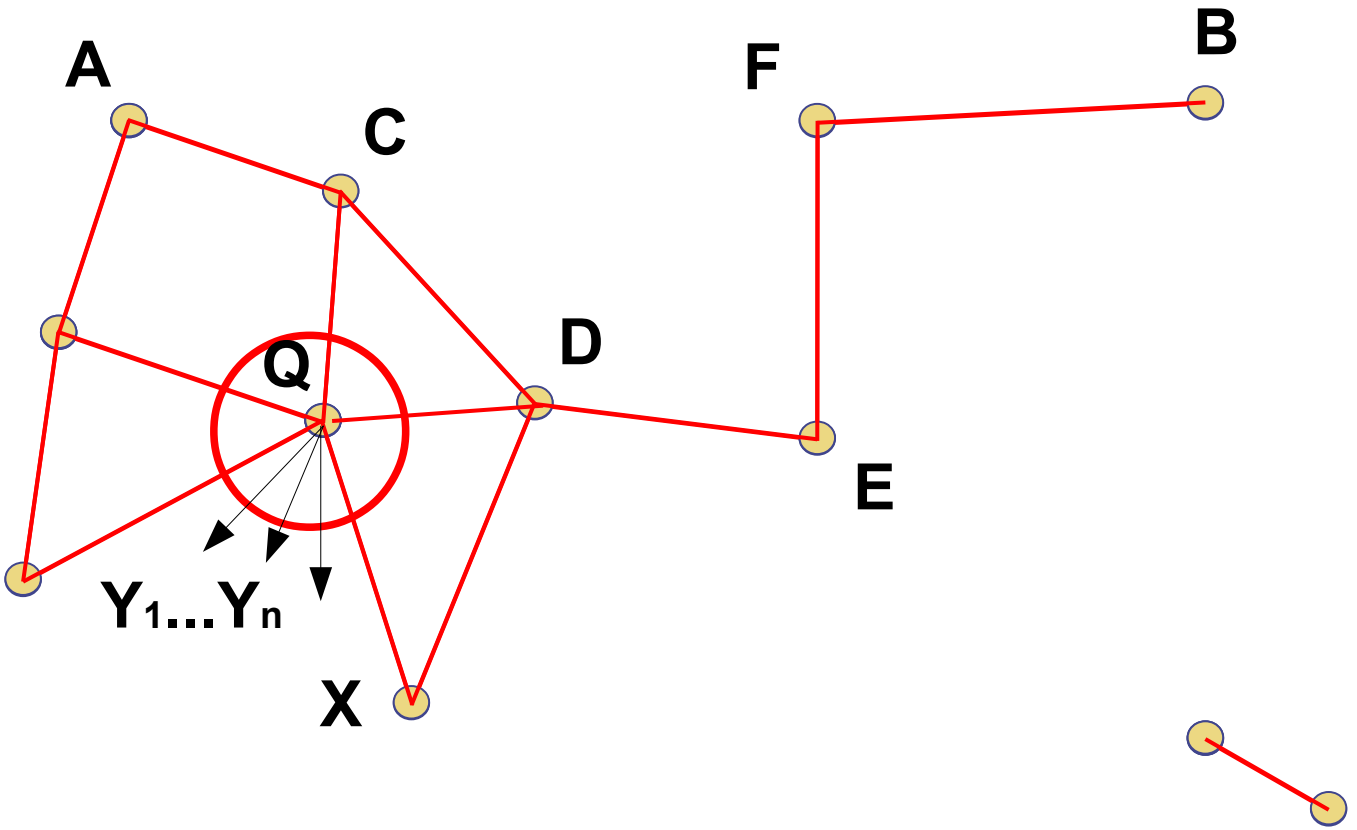
Informácia v smerovacej tabuľke môže byť ľubovolne zmenená, t.j. preposielacie cesty môžu byť zmenené.

Útok Sybil



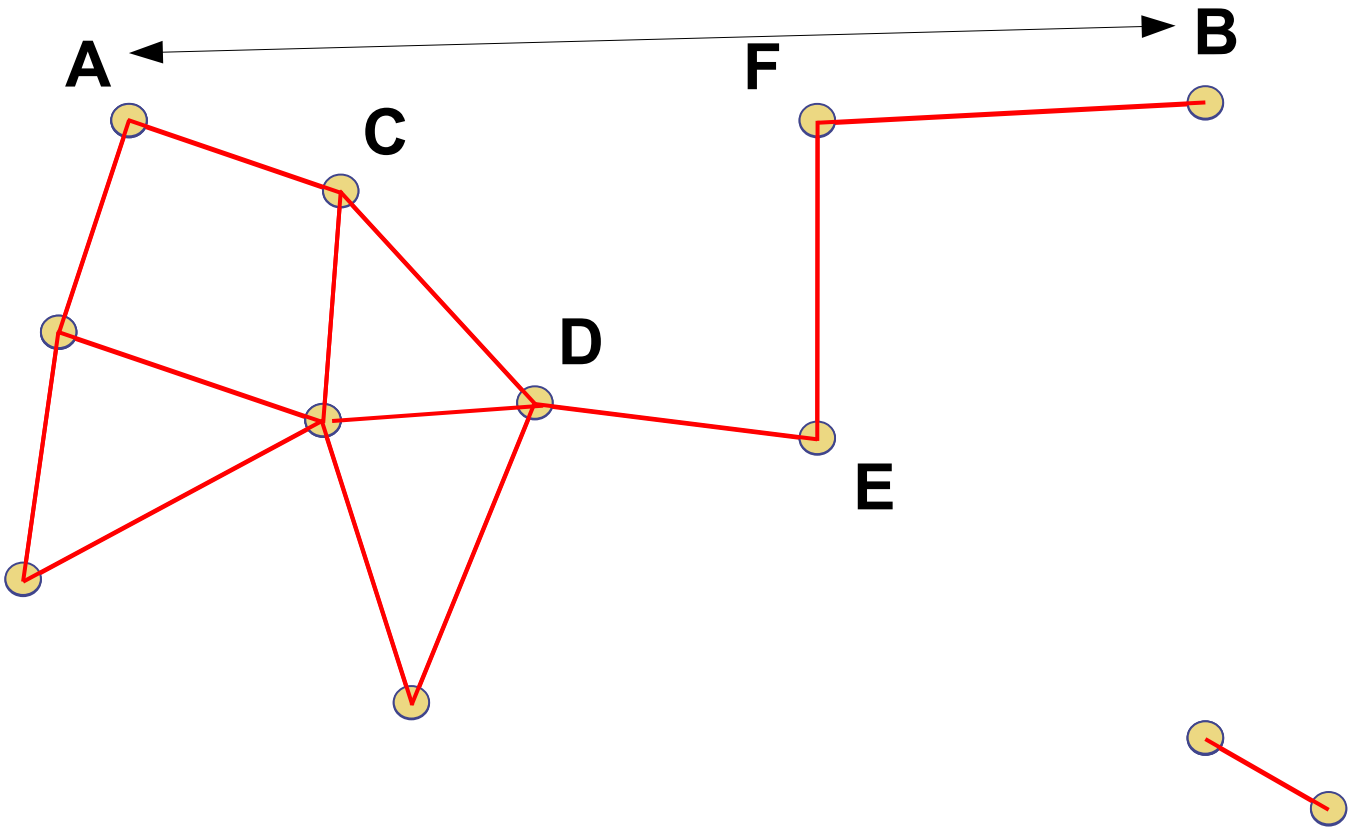
Uzol D vytvorí niekoľko fiktívnych uzlov za účelom získania lepšieho prístupu k médiu.

Virtuálne uzly



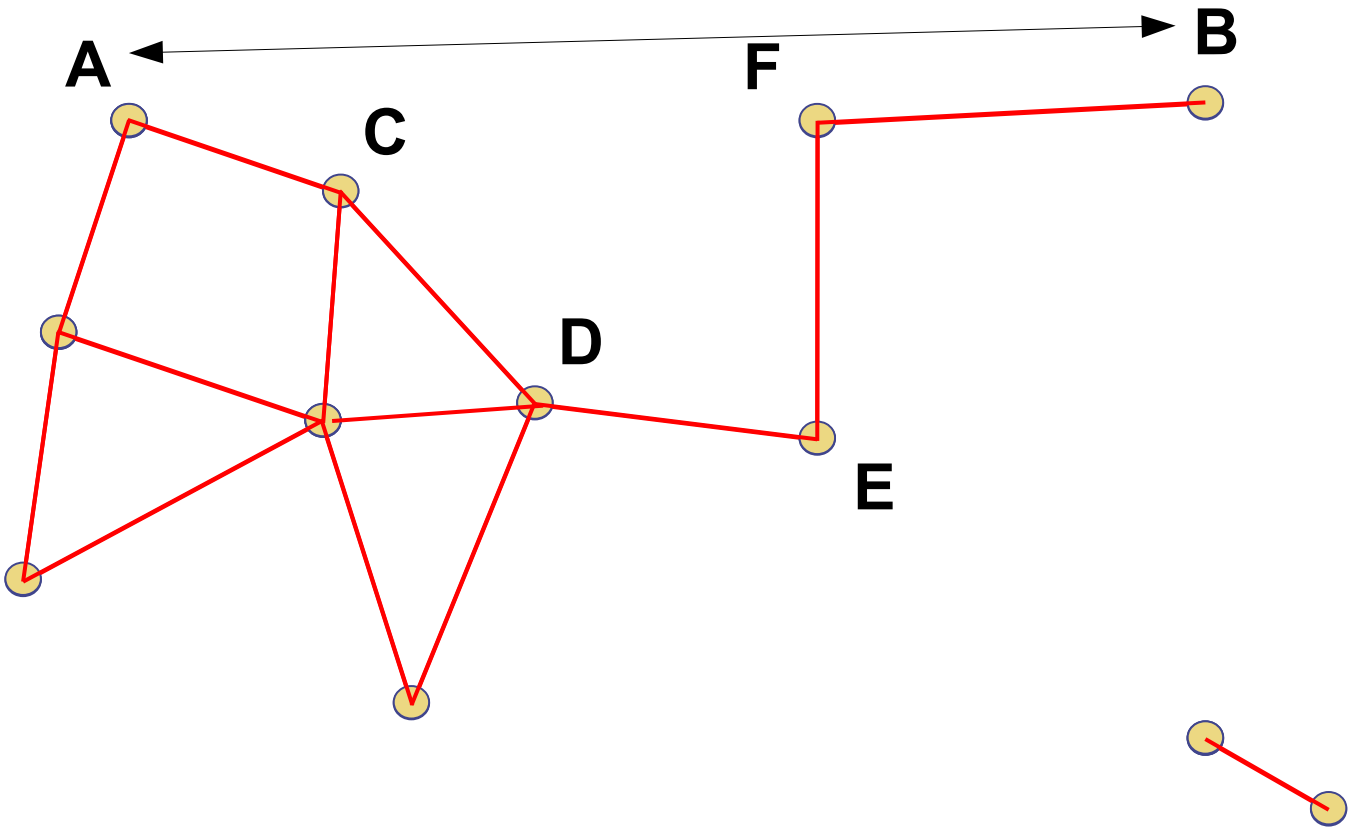
Uzol Q pridá virtuálne uzly Y1...Yn, aby cesta nez neho bola dlhšia. Čím je cesta dlhšia, tým je menšia pravdepodobnosť, že bude využitá na preposielanie.

TCP: duplikátne ACK



Zdrojový uzol opätovne pošle dátový paket pre každý prijatý duplikátny ACK, t.j. môže nastať zahltenie siete.

TCP: SYN útok



Každý SYN paket zapríčiní vznik polootvoreného spojenia, čo je forma DOS (denial of service) útoku.

Útoky na ad hoc siete

- Nepreposielanie paketov: black hole, gray hole
- Vytváranie slučiek v preposielaní
- Vytváranie neoptimálnych ciest na preposielanie
- Rozdeľovanie siete na komponenty
- Zadržiavanie paketov
- Wormhole (červia diera)
- Vytváranie virtuálnych uzlov
- Generovanie paketov bez obsahu za účelom zahltenia siete
- Manipulácie smerovacích tabuliek

Útoky na ad hoc siete

- MAC 802.11: manipulácia NAV
- Uzol neodpovedá na RTS
- Vkladanie nesprávnej informácie do hlavičky paketov
- Sybil útok
- Manipulácia veľkosti okna zahltenia (TCP)
- TCP SYN: vytvorenie polootvorených TCP spojení
- Duplikátny ACK, aj keď bol paket správne prijatý

Literatúra

Elizabeth M. Royer and Charles E. Perkins. Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol. Proceedings of MobiCom '99, Seattle, WA, August 1999, pp. 207-218.