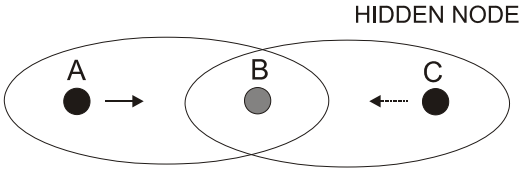
Sdílení rádiového kanálu v sítích MANET

Sítí MANET se rozumí rádiový komunikační systém tvořený mobilními stanicemi, které mají schopnost sebeorganizovat se do dočasné (ad-hoc) sítě s měnící se topologií. Topologie sítě není omezena na přímé spojení mezi stanicemi. Při komunikaci se běžně využívá retranslace přes několik hopů. Z uživatelského hlediska je podstatné, že MANET umožňuje komunikaci v síti stanic bez jakékoli infrastruktury. Proto je také věnována značná pozornost využití protokolů MANET v taktických rádiových sítích. Nezávislost na infrastruktuře je ovšem vykoupena nepříliš vysokou propustností, která je důsledkem toho, že všechny stanice v daném rádiovém kanálu vedle vlastního provozu zajišťují i retranslaci dat pro ostatní stanice a vedou poměrně komplikovanou signalizaci pro potřeby distribuovaného řízení sítě.

Sdílení kanálu v ad-hoc síti

Tradiční metody řízení přístupu do rádiového kanálu vycházejí z předpokladu, že se všechny stanice zúčastněné v rádiové síti navzájem slyší. Při topologii s neúplnou konektivitou, která je v ad-hoc sítích typická, je však situace při řízení přístupu do kanálu podstatně komplikovanější a použití tradičních metod v jejich základní podobě nevede k dobrým výsledkům. Podstatu problémů, které mohou nastat, lze shrnout do dvou kritických scénářů označovaných jako skrytý uzel (Hidden Node) a odkrytý uzel (Exposed Node).

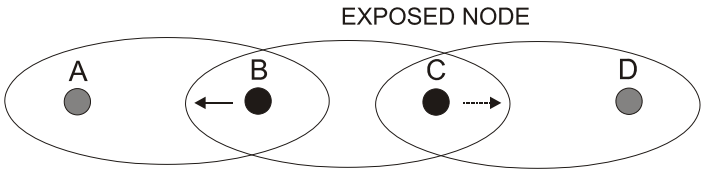
Mějme rádiovou síť tvořenou třemi uzly A, B, C s konektivitou podle obr. 1.



Obr. 1: Skrytý uzel (Hidden Node)

Uzel A má vyslat paket pro uzel B. Aby mohlo dojít k úspěšnému předání paketu, nesmí právě vysílat uzel B ani uzel C. To, zda vysílá uzel B, může uzel A ověřit sledováním provozu v kanálu. Zda vysílá uzel C, ale sám ověřit nedokáže. Hrozí proto, že dojde ke kolizi vysílání uzlu A a C a uzel B nebude schopen paket přijmout. Uzel C se označuje jako *skrytý uzel*.

Mějme rádiovou síť tvořenou čtyřmi uzly A, B, C, D s konektivitou podle obr. 2.



Obr. 2: Odkrytý uzel (Exposed Node)

Uzel B právě vysílá paket pro uzel A a uzel C má vyslat paket pro uzel D. Uzel C sledováním provozu v kanálu zjistí, že kanál je obsazen a proto vysílání nezahájí a čeká, až se kanál uvolní. Přitom to není potřeba. Kdyby začal vysílat hned, nijak neohrozí přenos dat od uzlu B k uzlu A a ani komunikace od uzlu C do uzlu D nebude ohrožena. Uzel C se označuje jako *odkrytý uzel*. Popsaný scénář je méně závažný, protože nevede ke kolizi, ale jen ke zmenšení propustnosti sítě.

Podstatou obou kritických scénářů je skutečnost, že ke kolizím vždy dochází na straně přijímače, nikoli na straně vysílače. Metod, které se více či méně úspěšně pokoušejí řešit problémy řízení přístupu do kanálu v ad-hoc sítích, je značné množství. Jedná se o problematiku, která zdaleka není uzavřená, a k danému tématu se stále objevují nové přístupy.

Nejběžnější jsou postupy založené na signalizaci, která přiměje uzel, který se chystá zahájit příjem paketu, k vyslání nějakého signálu, jenž upozorní sousední uzly, že se mají zdržet vysílání. V nejjednodušší variantě lze takovou signalizaci popsat následovně.

Pokud se uzel A chystá poslat datový paket do uzlu B, vyšle nejprve signalizační paket RTS (Request to Send). Když uzel B přijme RTS a smí vysílat, obratem odpoví signalizačním paketem CTS (Clear to Send). Uzel A po přijetí CTS vyšle datový paket. Ostatní uzly, které přijmou RTS, pozdrží vysílání po dobu potřebnou k vyslání CTS. Jestliže ostatní uzly přijmou CTS, pozdrží vysílání po dobu potřebnou k přenosu datového paketu o délce uvedené v CTS.

Uvedený postup do značné míry řeší problém skrytého uzlu. Pokud skrytý uzel přijme CTS, ví, že některý ze sousedních uzlů se chystá k příjmu datového paketu. Na stanovenou dobu proto pozdrží vysílání, čímž se předejde kolizi. Ke kolizi však stále může dojít, pokud se překryje vysílání RTS dvou uzlů sousedících s B. V tomto případě uzel B paket RTS nepřijme a nevyšle tedy odpověď CTS. Pokud uzel A neobdrží CTS včas, předpokládá, že došlo ke kolizi. Určitou dobu čeká a vyslání RTS zopakuje. Doba prodlevy se přitom určuje vhodným algoritmem. Dále může dojít ke kolizi v případě, kdy skrytý uzel zahájí vysílání RTS v době, kdy jeho soused vysílá CTS. Tato situace nijak ošetřena není a může skončit znehodnocením přenosu dat.

Problém odkrytého uzlu při použití uvedeného postupu vyřešen není. Pokud odkrytý uzel přijme RTS a do stanovené doby nepřijme následný CTS, ví, že adresát datového paketu je mimo jeho dosah. To znamená, že smí zahájit komunikaci, ačkoli jeho soused vysílá. Problém je ale v tom, že po vyslání RTS nebude schopen přijmout odpověď CTS, protože bude rušena krajním uzlem.

Jak je vidět, jednoduchou dvoufázovou signalizací nelze kolize úplně vyloučit, ale pouze snížit jejich pravděpodobnost. Moderní protokoly řízení přístupu do kanálu proto při alokaci kanálu využívají komplikovanější formy signalizace, která probíhá i ve čtyřech či pěti fázích. Situace se ještě více komplikuje v případech, kdy protokol má vedle unicast zajišťovat i multicast či broadcast. Postupná výměna signalizačních paketů se všemi

potenciálními příjemci je časově velmi náročná a možnost současné signalizace několika sousedními uzly zase klade značné nároky na řešení fyzické vrstvy protokolu.

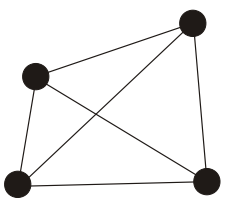
Je zřejmé, že rádiová síť s neúplnou konektivitou vyžaduje poměrně komplikované distribuované řízení přístupu do kanálu. Na druhou stranu je ale možné využít neúplné konektivity k dosažení vyšší propustnosti sítě. Metody, které toto umožňují, se někdy označují jako *Space TDMA*. Pokud je síť tak rozsáhlá, že vzdálenost mezi některými uzly činí tři a více hopů, je možné přidělit tentýž časový slot dvěma či více dostatečně vzdáleným uzlům. Např. při řetězové topologii (obr. 3) vystačíme s třemi časovými sloty při libovolně velkém počtu uzlů. Optimalizace alokace slotů koresponduje s matematickým problémem „vybarvování grafu". Z teorie grafů vyplývá, že počet slotů potřebných k bezkoliznímu sdílení kanálu je zdola omezen $M \geq D + 1$, kde D je nejvyšší počet sousedních uzlů, který se v síti vyskytuje. Pro řetězovou topologii je tedy minimální počet slotů roven 3.

Obr. 3: Při řetězové topologii sítě lze TDMA realizovat ve třech slotech při libovolném počtu uzlů. V síti znázorněné na obrázku mohou vysílat ve stejném slotu dvojice uzlů AD, BE a CF aniž by na sousedních uzlech došlo ke kolizi

Pro síť tvořenou n uzly s úplnou konektivitu je minimální počet slotů roven n. Při obecné topologii sítě pak bude počet slotů potřebných k zajištění TDMA ležet mezi 3 a n. Bohužel pro obecnou topologii výpočetní složitost optimálního řešení této úlohy roste velmi rychle s počtem uzlů. Je ale známo několik heuristických algoritmů, které alespoň částečně optimalizují přidělování slotů při přijatelné výpočetní náročnosti.

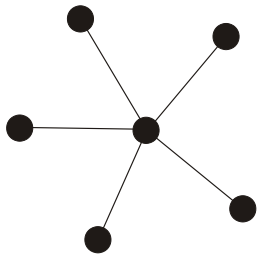
Propustnost ad-hoc sítí

Praktické zkušenosti s provozem ad-hoc sítí ukazují, že jejich propustnost může být překvapivě nízká. Problematice propustnosti se proto věnuje řada teoretických analýz. Pokud předpokládáme rozsáhlou rádiovou síť tvořenou n náhodně rozmístěnými uzly, které posílají pakety k jiným náhodně zvoleným uzlům, přenosová kapacita připadající na jeden uzel sítě je přímo úměrná $W / \sqrt{n \log n}$, kde W je plná přenosová kapacita linky mezi sousedními uzly. Tento výsledek můžeme interpretovat tak, že zdvojnásobení počtu uzlů vede ke snížení propustnosti přibližně $\sqrt{2}$ - krát. Podstatné je zjištění, že s rostoucím počtem uzlů se propustnost sítě limitně blíží k nule. Úzké hrdlo se přirozeně nachází v oblasti kolem středu oblasti pokryté sítí. Uvažovaný scénář ne vždy odpovídá reálnému provozu. V rozsáhlých sítích často probíhá intenzivní provoz pouze lokálně, tj. mezi nepříliš vzdálenými uzly. V takovém případě se s rostoucím počtem uzlů propustnost neblíží k nule, ale zastaví se na úrovni, která závisí na tom, do jaké míry má provoz lokální charakter.



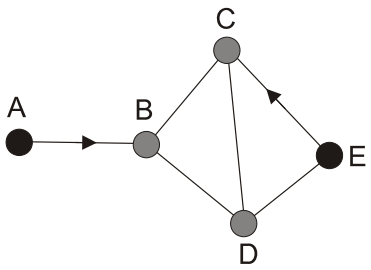
Obr. 4: Příklad sítě s úplnou konektivitou. Současně nelze přenášet více než jeden paket. Veškerá komunikace probíhá na 1 hop

Pokud se zaměříme na taktické rádiové sítě, musíme počítat s častou situací, kdy všechny uzly zúčastněné v síti jsou soustředěny na poměrně malém prostoru a v síti je úplná konektivita (obr. 4). V tomto případě nelze současně přenášet více než jeden paket a na každý uzel připadá přenosová kapacita W / n. Propustnost pak s počtem uzlů klesá podstatně rychleji než v rozlehlé síti podle výše uvedeného modelu. Nejhorší situace však nastane, pokud většina komunikace probíhá na dva hopy. To je např. při hvězdicové topologii (obr. 5).



Obr. 5: Síť s hvězdicovou topologií. Současně nelze přenášet více než jeden paket. Většina komunikace probíhá na 2 hopy

V tomto případě také není možné současně přenášet více než jeden paket, ale přenos většiny paketů trvá dvojnásobnou dobu. Na každý uzel pak připadá přenosová kapacita jen o málo větší než $W / (2n)$. S dalším rozvolňováním topologie sítě se pak propustnost zlepšuje, protože začne být možné přenášet současně více paketů, pokud jejich přenos probíhá v dostatečně odlehlých částech sítě (obr. 6).



Obr. 6: Současný přenos dvou paketů v jedné síti. A vysílá pro B a současně E vysílá pro C. Nedochází přitom ke kolizím

Jak jsme již zmínili, při některých scénářích může být navýšení propustnosti oproti nejméně příznivým scénářům i několika-násobné.

Vzhledem k tomu, že topologii taktické ad-hoc sítě nemůžeme plánovat, nezbývá než zajistit, aby síť měla dostatečnou propustnost i v nejméně příznivých případech. K situacím, kdy významná část komunikace probíhá na dva hopy, přitom v taktických sítích dochází běžně. Dostatečné přenosové kapacity lze pak docílit jen omezením počtu uzlů v síti a zajištěním co nejvyšší přenosové kapacity na linkách mezi sousedními uzly. Předpokladem pro dosažení dostatečné přenosové kapacity je samozřejmě udržení co nejmenšího komunikačního overheadu. To znamená, že signalizace v síti musí probíhat jen v nezbytném rozsahu, což je v síti s distribuovaným řízením dost obtížný úkol.

Ing. Petr Pánek, CSc.
KON, petr.panek@dicom.mesit.cz