

Journal of Cybernetics and Informatics

published by

**Slovak Society for
Cybernetics and Informatics**

Special Issue

**"New Trends in Education of Automation
and Information Technology"**

2004

**PŘÍKLAD APLIKACE PETRIHO SÍTÍ V ANALÝZE BEZDRÁTOVÉ
KOMUNIKACE, Čapek J., 1-4**

<http://www.sski.sk/casopis/index.php> (home page)

ISSN: 1336-4774

PŘÍKLAD APLIKACE PETRIHO SÍTÍ V ANALÝZE BEZDRÁTOVÉ KOMUNIKACE

Josef Čapek

Katedra řídicí techniky, FEL, CVUT, CZ

capekj@fel.cvut.cz

Abstrakt: V tomto článku používáme Stochastické Petriho sítě k modelování a analýze bezdrátových sítí IEEE 802.11.

Klíčová slova: Stochastické Petriho sítě, Simulace, IEEE802.11. Wi-Fi.

1 ÚVOD

V telekomunikacích vystupuje na povrch problém drahé poslední míle. Jako alternativa k metalickým okruhům se zákazníci připojují bezdrátovými technologiemi. U těch ale zejména v husté zástavbě dochází k zaplnění kmitočtových pásem a v řídké zástavbě se objevuje problém časové nestability vlastností kanálu. Vyrůstají tak nároky na komunikační protokoly a na způsob návrhu sítí. Jednou z dnes nejpoužívanějších bezdrátových technologií je IEEE 802.11.

V tomto článku používáme pro modelování Stochastické Petriho sítě. Kvůli usnadnění modelování sítí s určitým konkrétním počtem uzlů jsou použity FPQSPN [Čapek, Hanzálek 2000]. Pro analýzu používáme simulaci. Simulace modelů komunikačních protokolů v Petriho sítích je metoda analýzy, která je názorná při vytváření modelů a mimo jiné poskytuje dobré možnosti pro eliminaci chyb. Petriho sítě usnadňují vytváření přehledných a snadno pochopitelných modelů a umožňují tak validaci protokolů běžnými metodami jako je např. simulace [BILLINGTON J., DIAZ M., ROZENBERG G., Eds., 1999, LNCS 1605]. Podstatnou výhodou použití Petriho sítí pro analýzu komunikačních protokolů je případná možnost verifikace některých vlastností modelů pomocí aplikace metod známých např. z teorie grafů popř. z výzkumu teoretických vlastností Petriho sítí.

2 PŘÍSTUPOVÁ METODA IEEE 802.11

Primární přístupová metoda u IEEE 802.11 je non-persistent CSMA [Kleinrock, 1975]. Všechny uzly jsou připojeny na společné sdílené medium. Uzel, který chce odeslat datový rámec nejprve zjistí stav kanálu a v případě, že tento kanál byl volný po určitou dobu (DIFS) začne vysílat. V opačném případě uzel vysílání odloží na pozdější dobu. IEEE 802.11 je potvrzovaná vrstva – uzel, kterému byl rámec určen posílá potvrzovací rámec ACK. Hlavní zdroj chybovosti této přístupové metody je ve zpoždění mezi změnou skutečného stavu kanálu a okamžikem, kdy je tato informace detekována. Další zdroj chybovosti je zpoždění při přepnutí stanice z režimu přijímání do režimu vysílání. Součet všech zpoždění se nazývá „*vulnerability period*“. Tento parametr hraje klíčovou roli v průchodnosti kanálu a budeme mu věnovat pozornost později.

IEEE 802.11 nemá spolehlivý mechanismus detekce kolizí jako např. IEEE 802.3 (CSMA/CD). Pokud stanice ihned po ukončení svého vysílání detekuje signál vysílaný jinou stanicí, znamená to, že došlo ke kolizi – opačný případ ale neznamená, že ke kolizi nedošlo. Jako zpětná vazba o úspěšnosti odeslání rámce slouží v IEEE 802.11 potvrzování. V případě, že vysílací stanice neobdrží ACK do určitého okamžiku (SIFS + délka ACK rámce včetně hlavičky), předpokládá neúspěšné doručení rámce a rámec je zařazen k opakovanému odeslání za dobu, která se nazývá *backoff time*. Hodnota *backoff time* se mění v závislosti na počtu neúspěšných pokusů o odeslání rámce. V případě, že stanice potřebuje odeslat více než jeden rámec, vkládá mezi tyto rámce také prodlevu *backoff time*. Tomuto parametru se také budeme věnovat později.

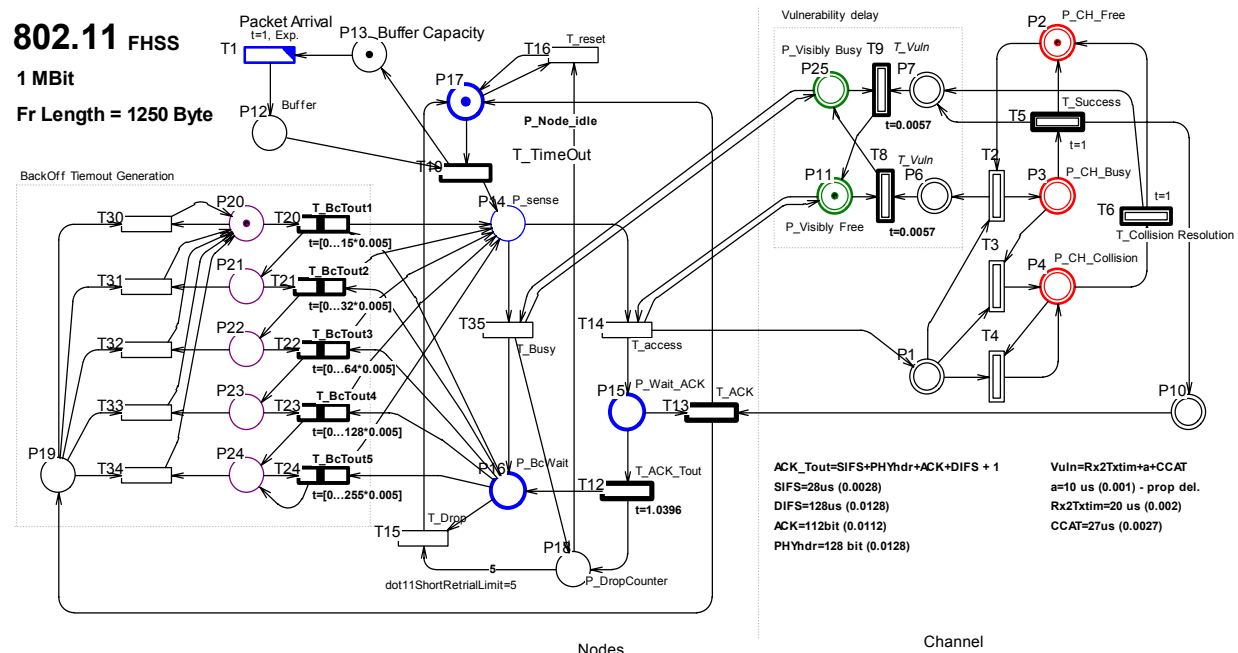
Ve specifikaci IEEE 802.11 je tato přístupová metoda označována *Distributed Coordination Function* (DCF). Dalším významným zdrojem chybovosti je jev známý jako *Hidden Terminal Problem* [Kleinrock 1974, 2], kdy některé stanice nejsou schopny detekovat vysílání některých jiných stanic. Tento známý problém zmiňujeme kvůli doplnění ale v tomto článku jej nemodelujeme.

DCF v IEEE 802.11 rozlišuje dva režimy: 1. *Basic Access*, který funguje tak, jak bylo popsáno – tedy datový rámec následovaný za dobu *SIFS* rámcem ACK. 2. *Request To Send / Clear To Send*, který funguje na základě krátkých *CTS/RTS* rámců. Zde se nejprve odešle rámec RTS, který obsahuje délku datového rámce, který chce vysílající stanice odeslat. Přijímací stanice odpoví rámcem CRT, který obsahuje stejnou informaci. Vysílající stanice pošle datový rámec a přijímací stanice odpoví rámcem ACK. Mezi rámci je prodleva *short interframe space* (SIFS). Který režim je aktuálně použit závisí na délce odesílaného rámce. V případě, že odesílaný rámec je

kratší než *CTS/RTS threshold*, použije sa *Basic Access*. Výhoda použitia *CTS/RTS* je v úspore šírky pásma zabieraného koliziami. V prípade, že dojde ke kolízii spôsobenej *vulnerability period*, dojde ke kolízii krátkych rámců alebo rámců CTS a ne dlouhých rámců které zaberou více času při přenosu. Vzhledem k tomu, že mnoho AP, např. Linksys, má *CTS/RTS threshold* defaultně nastavenou na maximální délku rámcu a tedy tento režim nepoužívá, budeme se díle věnovat DCF pracujícím v *Basic Access* režimu.

3 SPN MODEL IEEE 802.11

Model na obr. 1 se skládá ze dvou hlavních částí: Na pravé straně obrázku je model komunikačního kanálu a na levé straně je model sítě uzlů IEEE802.11 (jejich DCF). Model na obrázku představuje model komunikačního kanálu, ke kterému je propojeno k uzlů, kde k je parametr modelu. Kanál je tvořen sdílenými objekty [Čapek, 2000], které jsou graficky znázorněny dvojitou čarou. Zbytek modelu je tvořen nesdílenými objekty. Pro vysvětlení uvádíme, že kdyby se model na obrázku převedl na low-level Petriho síť, bylo by v modelu k kopií modelu uzlu (k kopií nesdílených objektů) a jeden model komunikačního kanálu. Model předpokládá konstantní délku rámcu, která je kratší než *CTS/RTS threshold* a kanál tedy pracuje v režimu *Basic Access*. Model také předpokládá, že všechny uzly jsou od sebe zhruba stejně vzdáleny a že mají stejné vlastnosti.



Obr. 1 – FPQSPN Model sítě 802.11b -

Komunikační kanál

Místa P2, P3 a P4 reprezentují stavy kanálu: P2 – CH_Free, P3: CH_Busy a P4 CH_Collision. Deterministický časovaný přechod T5 reprezentuje uvolnění kanálu po úspěšném odeslání rámcu. Deterministický časovaný přechod T6 reprezentuje uvolnění kanálu po předcházející kolizi. Umístění tokenu do P1 znamená příchod rámcu na kanál (některý z uzlů právě začal odesílat rámeček). V závislosti na okamžitém stavu kanálu způsobí token v místě P1 povolení jednoho z přechodů T2, T3 nebo T4. Jestliže byl kanál předtím Free, je teď Busy a jestliže byl Busy je teď ve stavu Collision. Jestliže byl kanál ve stavu Collision, odebere přechod T4 token z místa P4 a přechod T7 jej tam zase vrátí. Tím je způsobeno převedení časovaného přechodu T6 do stavu disabled a zpět do stavu enabled a dojde tak k „resetu jeho timeru“. Pro vysvětlení, od okamžiku, kdy je přechod T6 znovu povolen dojde k jeho spuštění za čas, který je mu přiřazen. Například, jestliže T6 je deterministický časovaný přechod s časem $t = 1$, tak mezi okamžikem, kdy začala mít jeho všechna vstupní místa dostatečný marking, do okamžiku jeho spuštění bude vždy jedna časová jednotka (pokud ovšem po celou dobu bude ve všech vstupních místech dostatečný marking).

P6, P7, P11, P25, T8 a T9 modelují zpoždění na kanálu (přesněji *vulnerability delay*). Čas T8 a T9 odpovídá době *vulnerability delay*. Stav markingů P11 odpovídá stavu markingů místa P2 zpožděnému o *vulnerability delay*. Přítomnost tokenu v P11 znamená, že stav kanálu se uzlům jeví jako Free.

Model DCF

V ďalšej časti popíšeme chováni komunikačného uzlu IEEE802.11. Zdôrazníme, že popisujeme chováni jedného uzlu na sieti. Pred simuláciou alebo analýzou modelu sa provede jeho un-folding po ktorom je vytvorené k kopii nesdílené časti modelu a všetky tieto kopie jsou napojeny na sdílenou část modelu. Po un-foldingu tedy např. do místa P1 vede k hran z přechodů odpovídajících T14. Obdobně z místa P10 naopak existuje k hran, které odcházejí do k přechodů T13 (v tento okamžik záměrně neřešíme číslování míst a přechodů po un-foldingu).

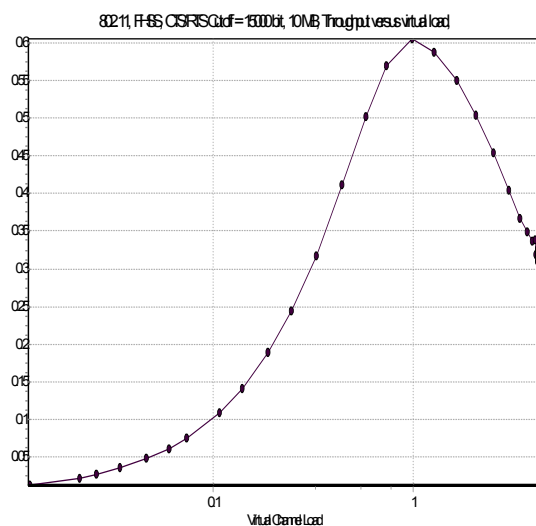
T1, P13, P12 a T10 představují proces příchodu požadavků. T1 je stochastický přechod s exponenciálním rozdělením času. (jestliže je přechod převeden se stavu *disabled* do stavu *enabled* je vygenerováno náhodné číslo, které říká, kdy dojde ke spuštění přechodu pokud mezitím nedojde k jeho převedení do stavu *disabled*). P12 je odesílací buffer a *initial marking* P13 určuje jeho velikost.

T10 představuje začátek MAC procesu. Token v místě P14 znamená, že uzel testuje stav kanálu. Je-li kanál volný dojde ke spuštění T14 a vygenerování tokenu v P1 a P15. Token v P15 znamená čekání na ACK. T13 znamená přijetí ACK (úspěšné odeslání rámce). Jestliže není doručeno potvrzení do času t_ACK_Tout , přejde node do *backoff* stavu. Po pěti neúspěšných pokusech o odeslání rámce dojde k zahození. T15, P18 je počítadlo neúspěšných pokusů o odeslání. Po zahození rámce, stejně tak jako po přijetí ACK je uzel připraven odeslat další rámec- časovaný přechod T18 je ve stavu *enabled*.

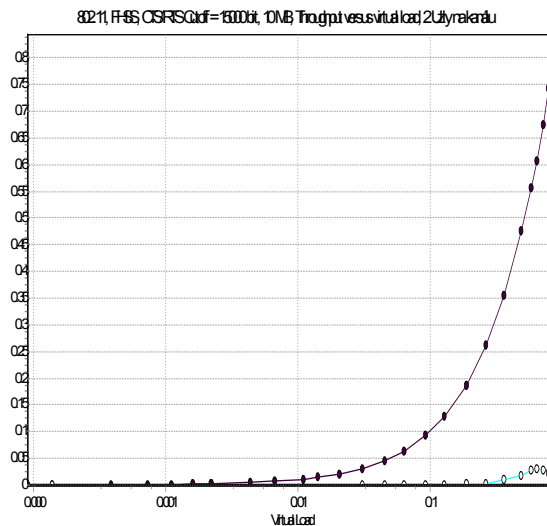
T30-T34, P20-P24 a T20-T24 jsou generátor *backoff* timeout. T20 – T24 jsou stochastické časované přechody. Čas přechodu T20 je určen náhodným celým číslem $<0 - 15> * \text{délka slotu}$. Čas T21 je náhodným celým číslem $<0 - 32> * \text{délka slotu}$. T22, T23 a T24 jsou analogicky - Čas T24 je náhodným celým číslem $<0 - 255> * \text{délka slotu}$. Token v místě P20 až P24 určují stav *backoff* timeru – Token v místě P21 znamená, že aktuálně odesílaný rámec byl jednou neúspěšný, token v P22 znamená že aktuálně odesílaný rámec byl dvakrát neúspěšný apod. Po úspěšném odeslání rámce respektive přijetí ACK je stav generátoru *backoff* timeout resetován jedním z přechodů T30 – T34.

4 VÝSLEDKY SIMULACE

Jako výsledek simulace uvádíme závislost relativní průchodnosti kanálu na virtuální zátěži. Relativní průchodnost je podíl mezi tím do skutečně prošlo a šířkou pásma (tím, co by teoreticky mohlo projít při ideální přístupové metodě). Virtuální zátěž je podíl mezi zatížením kanálu (tím, kolik chceme, aby prošlo) a šířkou pásma. Modely byly simulovány v simulátoru StpnPlay (<http://www.stpnplay.com>). Každý z grafů na Obr. 2 a 3 představuje výsledky sekvence simulací. Pro každý bod v grafu byl nastaven odpovídajícím způsobem čas přechodu T1 a provedena simulace. StpnPlay provádí simulační sekvence automatizovaně.



Obr.2: 802.11 Průchodnost versus zátěž – 100 uzlů



Obr. 3: 802.11 Průchodnost versus zátěž – dva uzly.

Na obr. 3 je patrné, že maximální průchodnost kanálu při zatěžování dvěma uzly je více než 80 šířky pásma. Za daných podmínek nedokázaly dva uzly způsobit reálné přetížení kanálu (na ose X vůbec neexistuje hodnota zátěže jedna nebo větší protože během simulace se nikdy nedostala síť do stavu, že by zátěž byla větší nebo rovna jedné). Na celém zobrazeném intervalu je průchodnost rostoucí funkcí zátěže což znamená, že komunikační protokol je pro dva uzly stabilní. Pro 100 uzlů je situace opačná: Při přetěžování kanálu (zhruba od hodnoty zátěže jedna – tedy 100 % a vyšší) dochází se vzrůstající zátěží k poklesu průchodnosti. Tedy, čím více

je kanál zatěžován, tím méně (a to i skutečně přepočteno absolutně na byte) kanál přenáší. 100 uzlů dokáže vygenerovat i při dané přístupové metodě několikrát větší zátěž, než je průchodnost kanálu.

V současné době probíhá na pracovišti autora analýza novějších perspektivních wire-less standardů jako je 802.16, 802.20.

5 LITERATURA

Y. C. Tay, K. C. Chua, A capacity analysis for the IEEE 802.11 MAC protocol, Wireless Networks Volume 7 , Issue 2 March/April 2001 Pages: 159 - 171 Year of Publication: 2001 ISSN:1022-0038

SINCLAIR B., 2002, Simulation of Computer Systems and Computer Networks: A Process Oriented Approach Rice University, Houston, Texas, January 8, Available by e-mail at bs@rice.edu.

Čapek, J. : “FPQSPN and its application in analysis of Ethernet”, in proc. of IFAC Conference "Control Systems Design", September 7 - 10, 2003, Bratislava, Slovak Republic

Čapek, J. Hanzálek Z.: “StpnPlay a modeling and simulation Petri net tool”, in proc. of PNPM2001, univ. of Dortmund, Germany 2001

Josef Čapek and Zdeněk Hanzálek, “Modelling of Channel Collisions in Petri Nets”, International workshop on Performability Modelling of Computer Communicatio Systems. Erlangen 2001, ISSN 0344-3515

Čapek, J.: Dessertation Thesis “Petri net analysis of Non-deterministic MAC layers of computer communication networks”. ČVUT, FEL 2002.

Kleinrock, L. and Tobagi, F. A., "Packet Switching in radio Channels: Part I—Carrier Sense Multiple Access Modes and Their Throughput Delay Characteristic", IEEE Transactions on Communications., Corn-23, Dec. 1975, pp. 1400-1416