

# Zabezpečení dat při přenosu

Petr Grygárek

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

1

## Komunikace bez spojení a se spojením

- Bez spojení
  - vysílač může datové jednotky (=rámce/pakety) zasílat střídavě různým příjemcům
    - identifikace příjemce součástí datové jednotky
  - datové jednotky vzájemně nezávislé
    - možné změny pořadí a ztráty některých datových jednotek
- Se spojením
  - před zahájením komunikace vysílač žádá o zřízení okruhu ke konkrétnímu příjemci a po ukončení komunikace o jeho zrušení
  - jsou vyhrazeny systémové zdroje pro následný přenos proudu dat (seřazené sekvence) od vysílače k příjemci
    - v síťových prvcích / ve vysílači a příjemci

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

2

## Chápání komunikace bez spojení a se spojením

- Chápáno fyzicky – na úrovni síťové technologie
  - Před zahájením komunikace vysílač žádá síť o zřízení okruhu ke konkrétnímu příjemci
  - Nastavení mezilehlých systémů sítě a předání identifikátoru zřízeného okruhu vysílači
    - síť s přepojováním okruhů, virtuální kanál
  - Po ukončení žádá některá strana síť o zrušení okruhu
- Chápáno logicky – na úrovni software komunikujících stanic
  - Spojení reprezentováno stavem datových struktur ve vysílači a příjemci
  - Síť o logickém spojení neví

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

3

## Kanál vs. okruh

- Kanál – jednosměrný
  - případně half duplex
- Okruh – obousměrný
  - dvojice kanálů

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

4

## Problémy při komunikaci v reálné síti

- ztracení a poškození paketů  
⇒ nutnost zavedení zpětné vazby do přenosu
- duplikace a změna pořadí paketů v sítích s alternativními cestami („přebíhání“)  
⇒ nutnost číslování přenášených paketů

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

5

## Typy zpětné vazby

- potvrzovací - zpět ACK/NAK
- detekční - zpět CRC
- informační - zpět celý rámec

V reálné síti se mohou ztrácet nejen informační pakety, ale i potvrzení.

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

6

## Číslování paketů

- zajištění správného pořadí
- detekce výpadku části sekvence
- chrání před zduplikováním na straně přijímače při opakovaném vyslání (retransmisi)
  - pokud paket došel na přijímač, ale potvrzení se ztratilo

## Komunikační protokol

Soubor syntaktických a sémantických pravidel (včetně definice časových poměrů) pro komunikaci dvou nebo více zařízení.

## Potvrzovací schémata

(Protokoly pro zajištění spolehlivé komunikace dvou stanic)

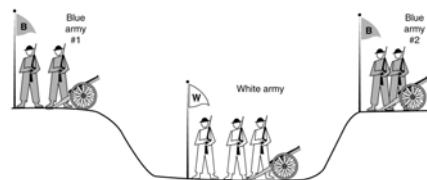
## Typy potvrzování

- pozitivní (ACK) - potvrzuje správné přijetí
  - zablokování vysílače při ztrátě
- negativní (NAK) - informuje o přijetí rámce s chybou
  - samo o sobě nestačí, urychluje však detekci chyb
- kombinované - používá se ACK i NAK

## Potvrzování a časovým limitem (timeout)

- volba vhodného timeoutu řeší problém ztráty pozitivního potvrzení
- komplikuje formální popis protokolu
  - (nutnost zavedení časového kontextu).
- problém volby velikosti timeoutu: snaha o brzké zjištění nutnosti retransmise vs. zbytečné zahlcování kanálu při předčasných retransmisích

## Problém tří armád



Konečným počtem vyměněných zpráv nelze zajistit, aby měl přijímač jistotu, že jeho potvrzení došlo zpět na vysílač.

## Klasifikace potvrzovacích schemat (protokolů)

- Stop-and-wait
  - Vysílač vyšle jediný rámec a čeká na potvrzení.
  - Na kanálech s velkým zpožděním velmi neefektivní
- Skupinové potvrzování (pipelining)
  - Efektivní pro spoje s velkou dobou zpoždění
  - Vysílač smí vyslat více (skupinu) rámců a až poté čekat na potvrzení
  - Lze dosáhnout efektivitu až 100%
    - (na full-duplex spojích)
  - Potvrzení zpravidla inkluzivní
    - potvrzuje vše až do uvedeného sekvenčního čísla
    - chrání před ztrátou předchozího potvrzení

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

13

## Protokoly využívající metody klouzavého okénka (Sliding Window)

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

14

## Sliding Window – základní princip

- Stanice smí vyslat i více rámců bez čekání na ACK
  - (počet dán šířkou vysílacího okna)
- Při odeslání se pro každý rámec nastartuje časovač pro potvrzení.
- Příjímáček posílá ACK po každém přijatém rámcí
  - popř. při vypršení časového limitu od času příchodu prvního dosud nepotvrzeného rámce (ušetření některých ACK)
- Při přijetí rámce s chybou přijímáček ACK nevyšle
  - nebo vyšle NAK
  - bez použití NAK vysílač detekuje chybu vypršením časového limitu na příchod ACK

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

15

## Sliding Window - pojmy

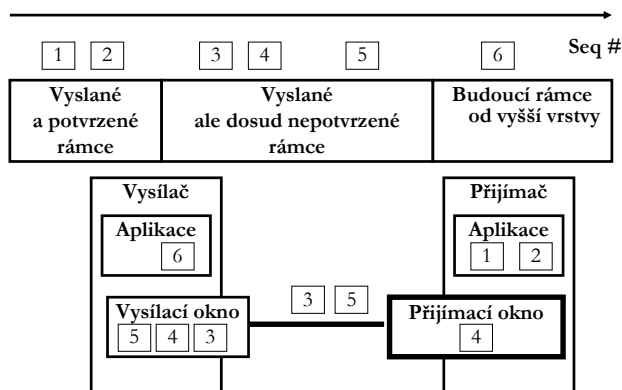
- Vysílací okno - buffer na vysílači s vyslanými rámci, které dosud nebyly potvrzeny a možná budou muset být vyslány znovu
- Příjímáčí okno - buffer na přijímači na přijaté rámce, které ještě nemohly být doručeny vyšší vrstvě přijímače, protože dosud chybí některý z předchozích rámců v řadě

Obě okénka "kloužkou" po sekvenčních číslech

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

16

## Sliding Window: Okna



© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

17

## Varianty obsluhy chyb u Sliding Window

Rozdíl chování podle reakce na chybný nebo ztracený rámec

- ztracený rámec přijímáček pozná podle chybějícího sekvenčního čísla při příchodu následujícího rámce
- Go-Back-N
- Selective Repeat

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

18

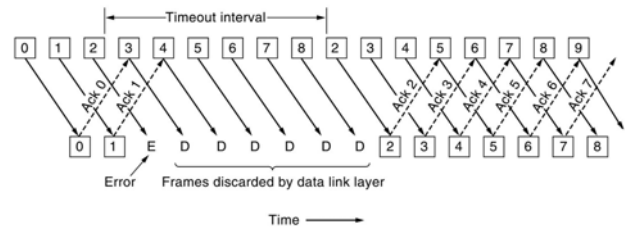
## Go-Back-N

- Přijímač všechny rámce po chybném/nedoručeném zahazuje
  - ani na ně neposílá potvrzení
- Přijímací okno má šířku 1
- Některému rámcu ve vysílacím okně vyprší timeout, vysílač jej opakuje a spolu s ním hned i všechny následující rámce ve vysílacím okně
  - (pokud ty došly na přijímač, přijímač je zahodil)
- Jednoduchá implementace přijímače, ale plýtvá přenosovou kapacitou

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

19

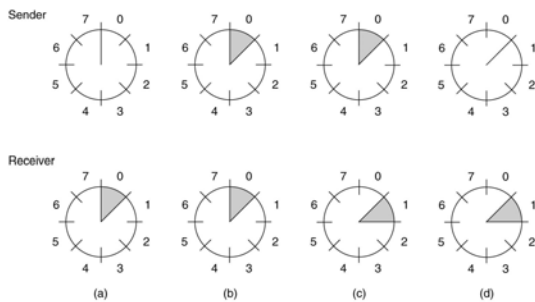
## Go-back-N - příklad



© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

20

## Go-back-N: Vysílací a přijímací okno



© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

21

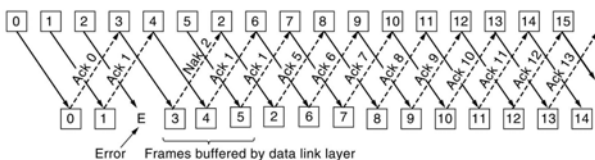
## Selective Repeat

- Rámec s chybou došlý na přijímač se zahodí, ale následující se bufferují
- Pokud vyprší timeout chybného rámce ve vysílacím okně, opakuje se jen on sám
- Když zopakovaný rámec dojde na přijímač, sekvence v přijímacím okně se doplní a může se předat vyšší vrstvě
- ACK z přijímače potvrzuje vždy rámec, který je na konci přijaté spojité sekvence
- Lze zefektivnit zasláním NAK <číslo\_ztraceného> při příchodu chybného rámce nebo rámce mimo pořadí
  - vysílač nemusí s opakováním čekat na vypršení timeoutu

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

22

## Selective Repeat - příklad



© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

23

## Inkluzivní potvrzování

- ACK n potvrzuje všechny rámce se sekvenčními čísly  $\leq n$
- zefektivnění (méně ACK), odolnost proti ztrátě ACK
  - Ztráta potvrzení sekvenčního čísla n nevadí, dojde-li dostatečně brzo potvrzení sekvenčního čísla  $m > n$
  - S vysláním ACK n lze chvilku posečkat, nepřijdou-li další data a pak potvrdit společně ACK m ( $m > n$ )

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

24

## Vztah šířky vysílacího okna a počtu použitých sekvenčních čísel

- Go-back-N  
šířka okna aspoň o jednu menší než počet použitelných sekvenčních čísel
  - (nepoznali bychom ztrátu všech rámců okna)
- Selective repeat:  
šířka nejvýše polovina počtu sekvenčních čísel
  - (z důvodu překrývání vysílacího a přijímacího okna)

## Řízení toku dat (flow control)

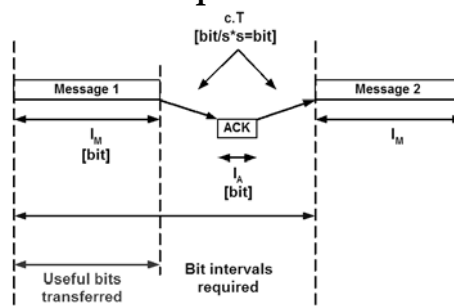
Možnost zbrzdit vysílač, pokud aplikace přijímače nestačí odebírat data

- Inzerování zbývajících šířky přijímacího okna z přijímače na vysílač
- Odpovídající úprava velikosti vysílacího okna na vysílači

Použito např. v TCP protokolu.

## Efektivita potvrzovacích schemat

## Stop and Wait



$$e_f = \frac{l_m}{l_m + cT + l_a + cT} = \frac{l_m}{l_m + l_a + 2cT}$$

## Efektivita Stop and Wait – příklady

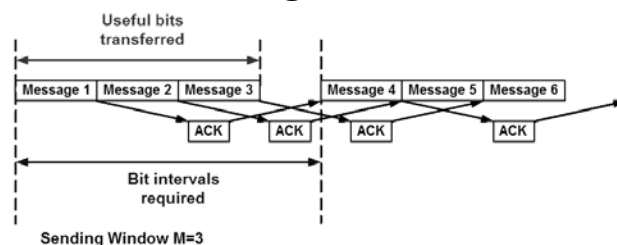
- Modemová linka, pomalá a LAN se spíše větším zpožděním:  
 $l_m=80\text{B}$ ,  $l_a=1\text{B}$ ,  $c=14400\text{ bps}$ ,  $T=1\text{ms}$ ,  $ef=94.56\%$
- Družicový spoj  
 $l_m=80\text{B}$ ,  $l_a=1\text{B}$ ,  $c=14400\text{ bps}$ ,  $T=270\text{ ms}$ ,  $ef=7.6\%$

### Prodloužení rámce 8x:

- Modemová linka, pomalá a LAN se spíše větším zpožděním:  
 $l_m=640\text{B}$ ,  $l_a=1\text{B}$ ,  $c=14400\text{ bps}$ ,  $T=1\text{ms}$ ,  $ef=99.28\%$
- Družicový spoj  
 $l_m=640\text{B}$ ,  $l_a=1\text{B}$ ,  $c=14400\text{ bps}$ ,  $T=270\text{ ms}$ ,  $ef=40.38\%$

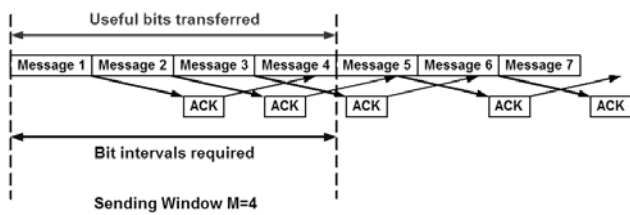
Prodloužení rámce efektivitu zlepši, ale v případě výskytu chyby v rámci se pak zahazuje celý (dlouhý) rámec, oproti např. jen jednomu ze dvou polovičních.

## Sliding Window



$$e_f = \frac{M \cdot l_m}{l_m + cT + l_a + cT} = \frac{M \cdot l_m}{l_m + l_a + 2cT}$$

## Efektivita 100% u Sliding Window



© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

31

## Popřemýšlejte...

Pokuste se vypočítat minimální velikost vysílacího okna pro danou velikost rámce, potvrzení, přenosovou rychlost a zpoždění na kanále

© 2005 Petr Grygárek, FEI VŠB-TU Ostrava, Počítačové sítě (Bc.)

32