Zabezpečení dat při přenosu

Petr Grygárek

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 přijímači a po ukončení komunikace o jeho zrušení
  - jsou vyhrazeny systémové zdroje pro následný přenos proudu dat (seřazené sekvence) od vysílače k přijímači
    - v síťových prvcích / ve vysílači a přijímači

Chápání komunikace bez spojení a se spojením

- Chápáno fyzicky – na úrovni síťové technologie
  - Před zahájením komunikace vysílač žádá síť o zřízení okruhu ke konkrétnímu přijímači
  - 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 přijímači
  - Síť o logickém spojení neví

Kanál vs. okruh

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

Problémy při komunikaci v reálné síti

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

Typy zpětné vazby

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

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

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)

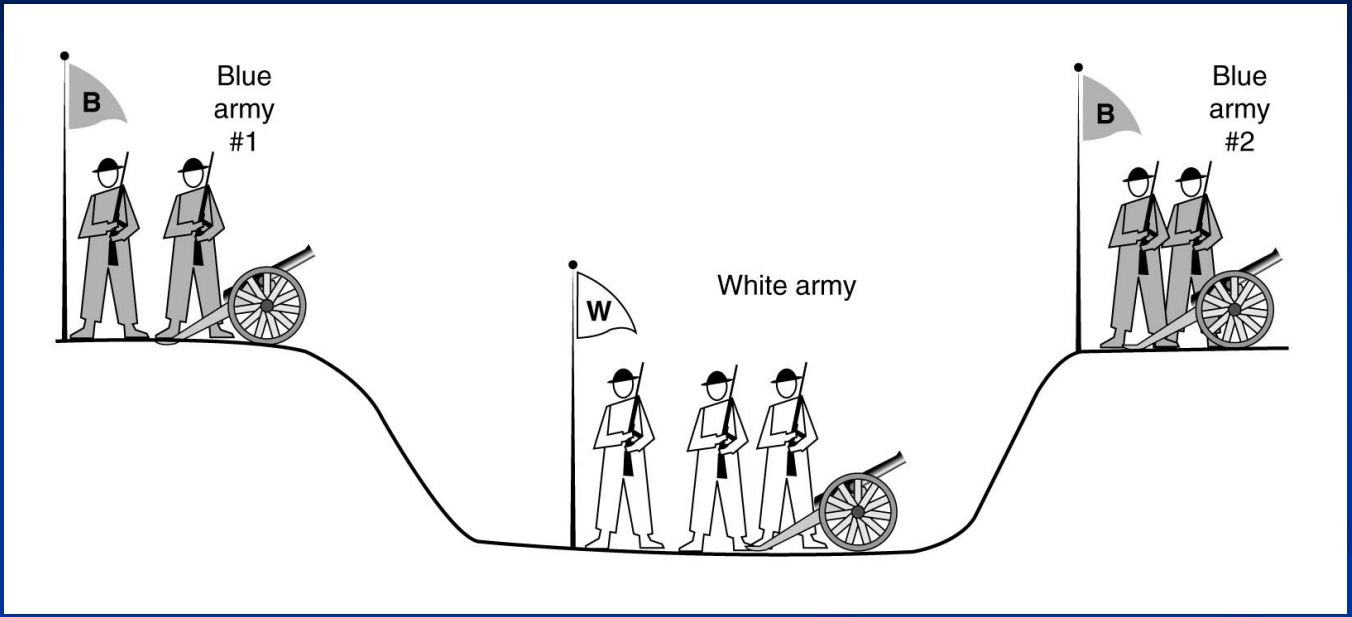
- volba vhodného timeoutu řeší problém ztráty pozitivního potvrzení
- komplikuje formální popis protokolu
  - (nutnost zavedení časového kontextu).
- problém volby velikosti timeoutu:

  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
    - a při komunikaci přes prostředníky - Internet
  - 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, možnost omezení počtu ACK

Protokoly využívající metody klouzavého okénka

(Sliding Window)

Sliding Window – základní princip

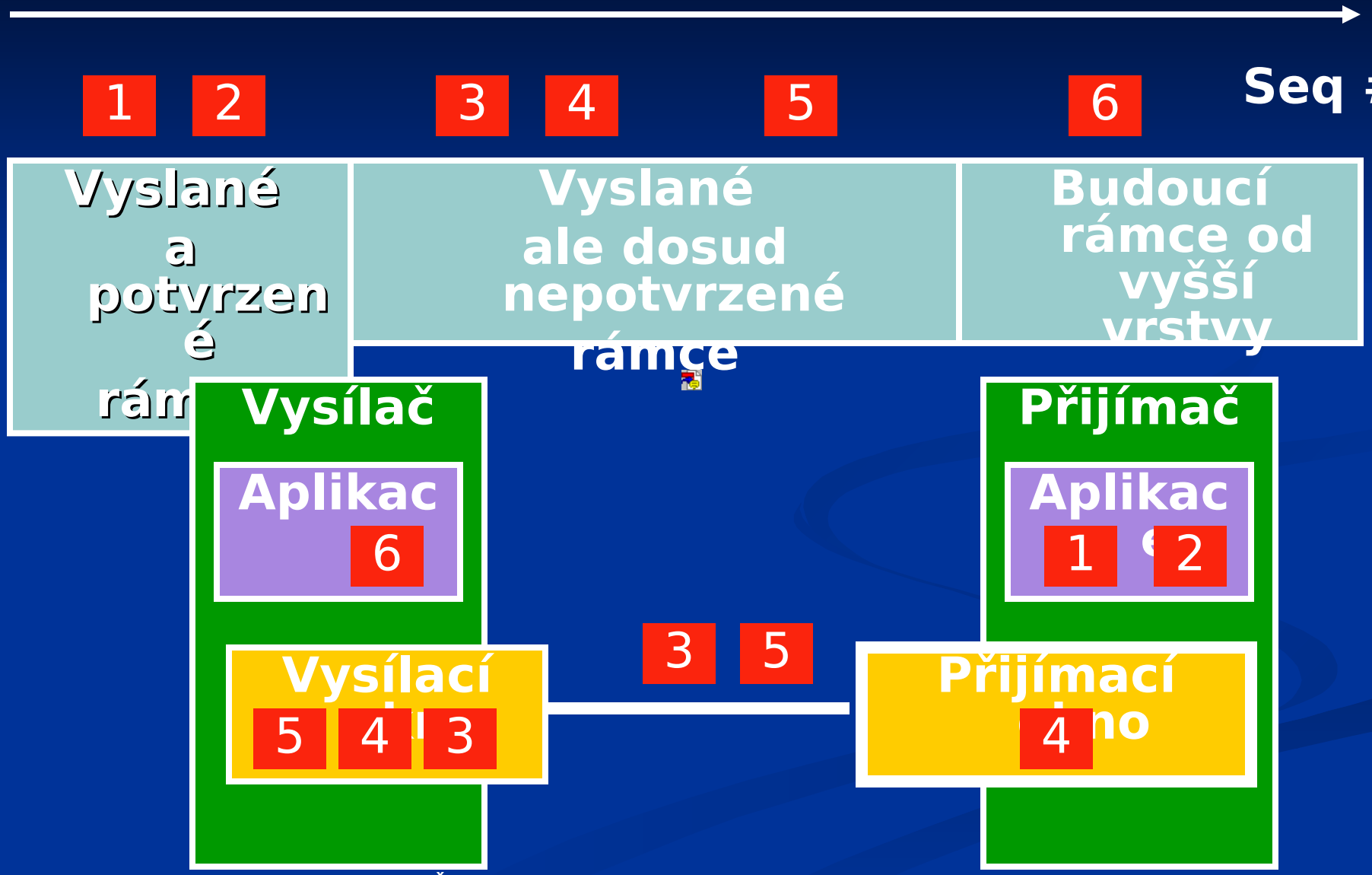
- Stanice smí vyslat i více rámců bez čekání na ACK
  - (počet dán šířkou vysílacího okna)
- Při odeslání se pro každý rámec nastartuje samostatný časovač pro potvrzení
- Přijímač posílá ACK po každém přijatém rámci
- Při přijetí rámce s chybou přijímač ACK nevyšle
  - nebo vyšle NAK
  - bez použití NAK vysílač detekuje chybu vypršením časového limitu na příchod ACK

Sliding Window - pojmy

- Vysílací okno - buffer na vysílači s vyslanými rámci, které dosud nebyly potvrzeny a možná budou muset být vyslány znovu
- Přijímací 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

Sliding Window: Okna



Inkluzivní potvrzování

- ACK n potvrzuje všechny rámce se sekvenčními čísly ≤ 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 chvíli posečkat, nepříjdou-li další data a pak potvrdit společně ACK m (m>n)

Varianty obsluhy chyb u Sliding Window

Rozdíl chování podle reakce na chybný nebo ztracený rámec

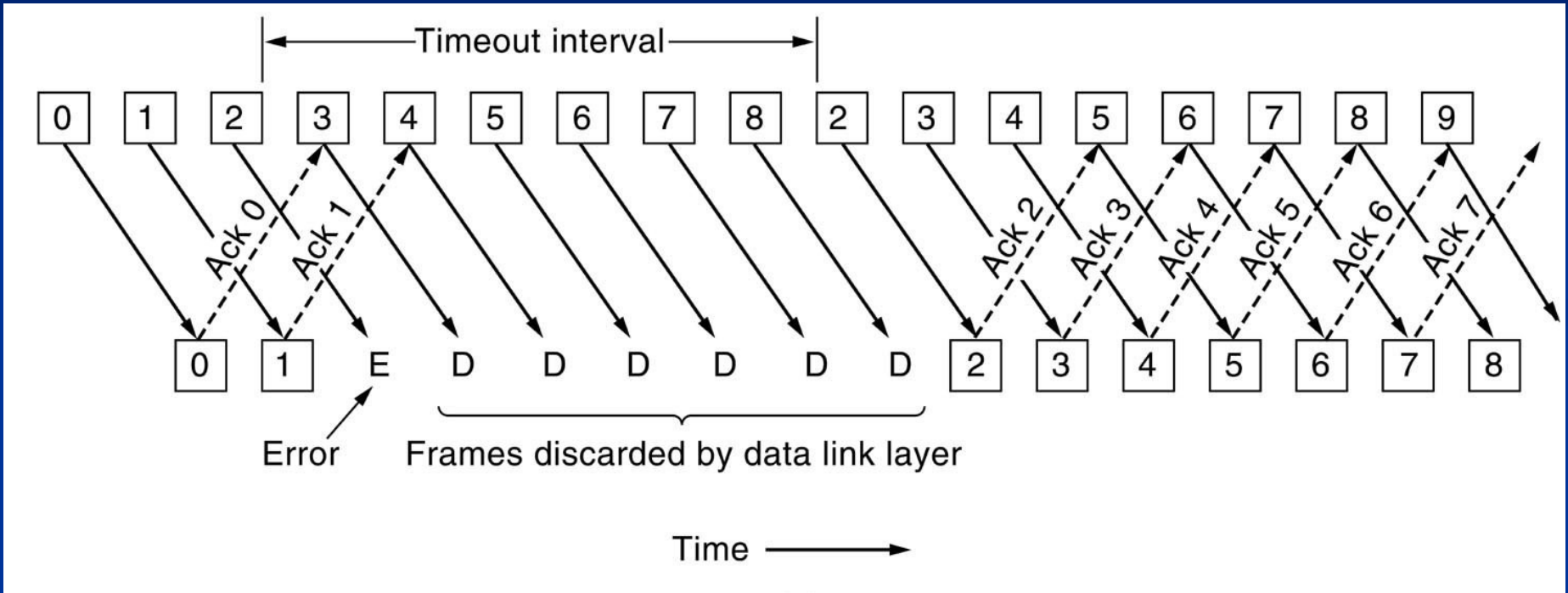
- ztracený rámec přijímač pozná podle chybějícího sekvenčního čísla při příchodu následujícího rámce

- Go-Back-N
- Selective Repeat

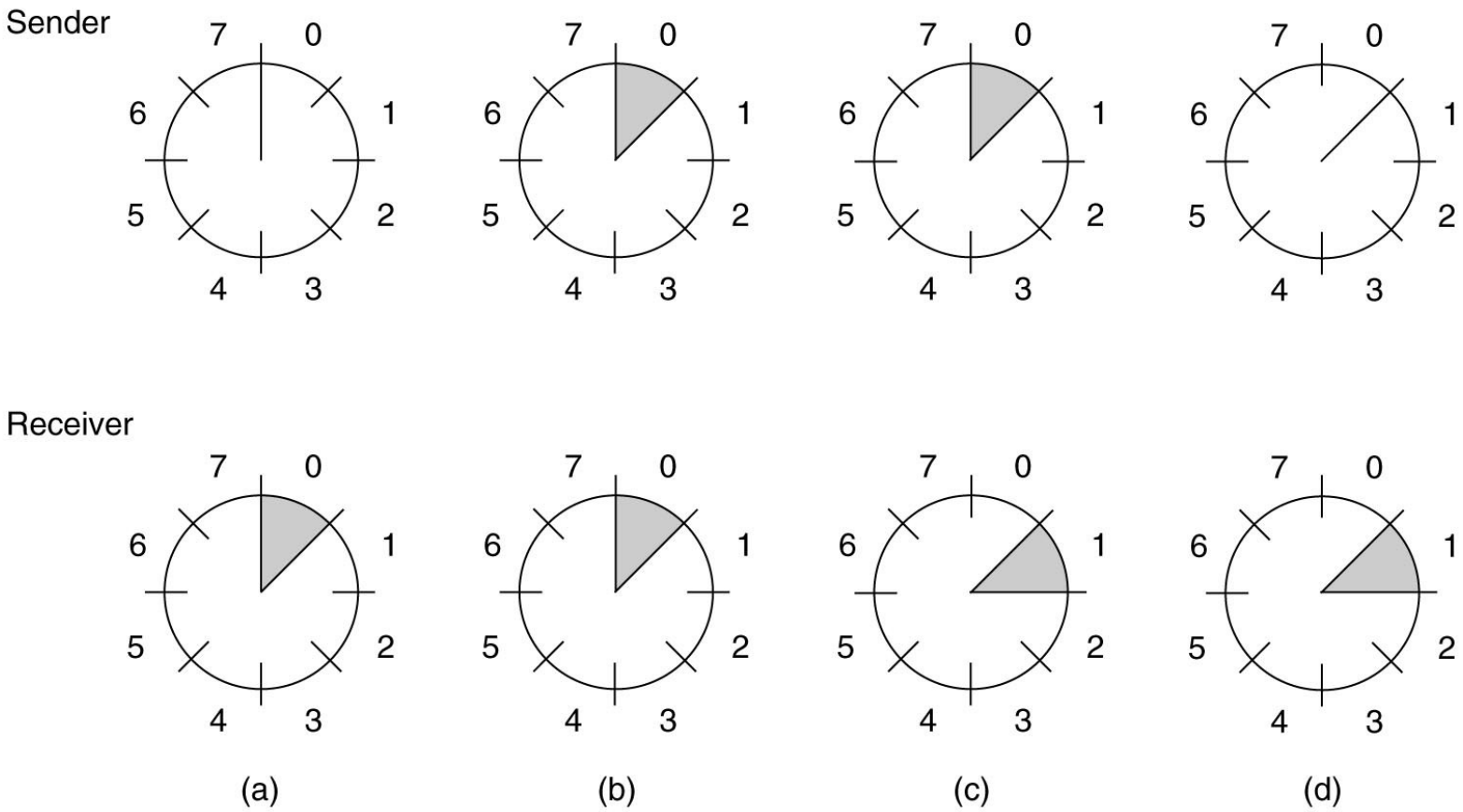
Go-Back-N

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

Go-back-N - příklad



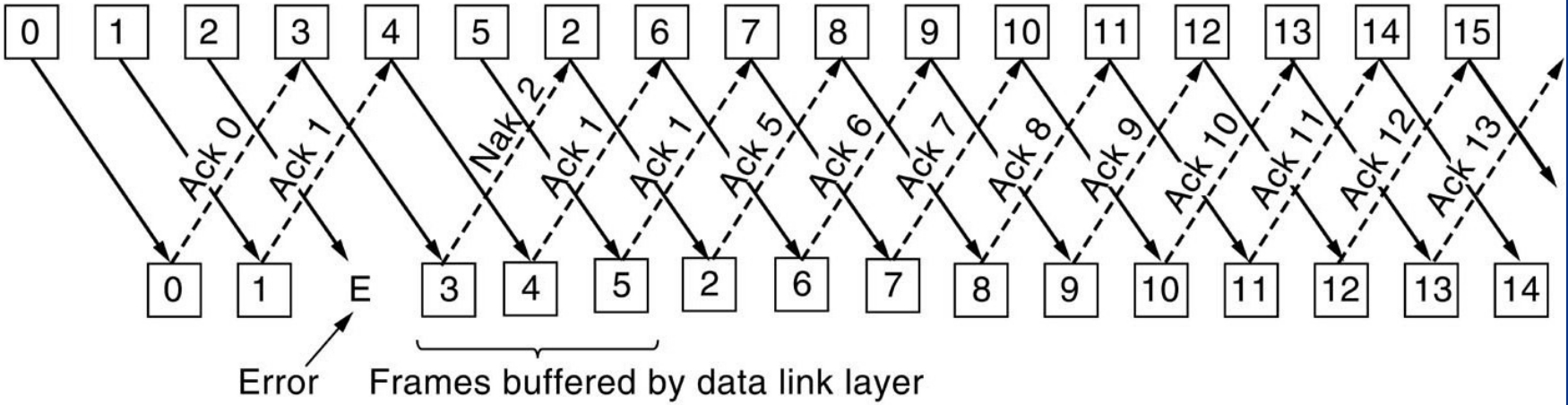
Go-back-N: Vysílací a přijímací okno



Selective Repeat

- Rámec s chybou došlý na přijímač se zahodí, ale následující se bufferují
  - tj. bufferují se i rámce došlé mimo pořadí
- 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

Selective Repeat - příklad



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)

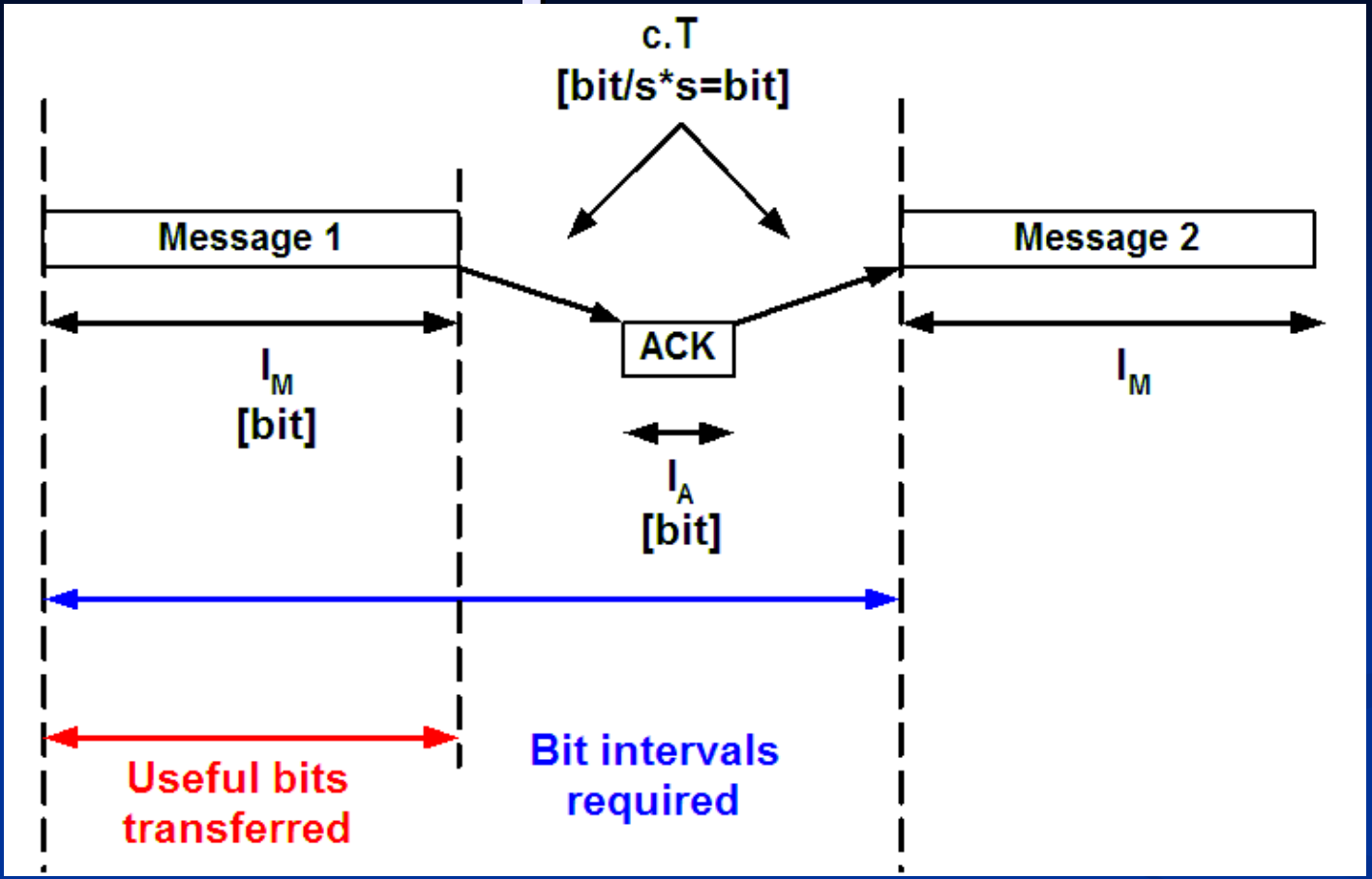
Možnost zbrzdit vysílač, pokud aplikace přijímače nestačí odebírat data

- Inzerování zbývající šířky přijímacího okna z přijímače na vysílač
- Dynamicky 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

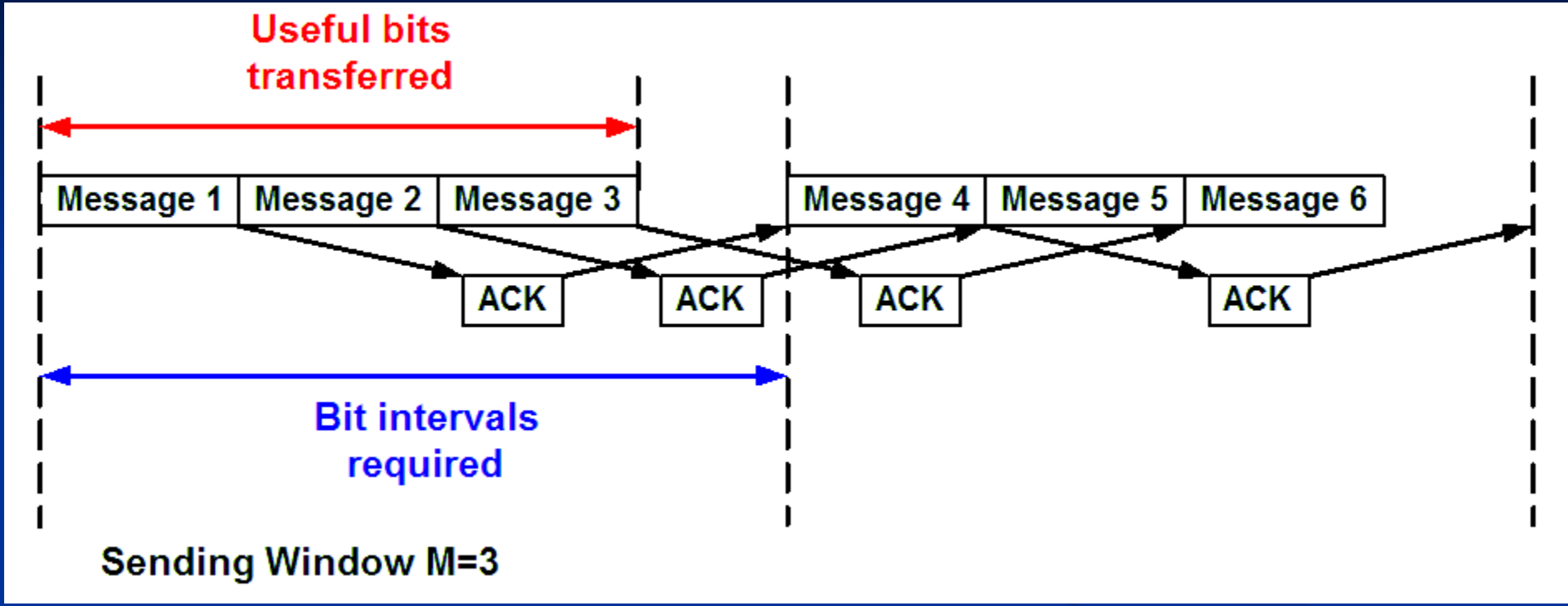
- Modemová linka, pomalá a LAN se spíše větším zpožděním:
  lm=80B, la=1B, c=14400 bps, T=1ms, ef=94.56 %
- Družicový spoj
  lm=80B, la=1B, c=14400 bps, T=270 ms, ef=7.6 %

Prodloužení rámce 8x:

- Modemová linka, pomalá a LAN se spíše větším zpožděním:
  lm=640B, la=1B, c=14400 bps, T=1ms, ef=99.28 %
- Družicový spoj
  lm=640B, la=1B, c=14400 bps, T=270 ms, ef=40.38 %

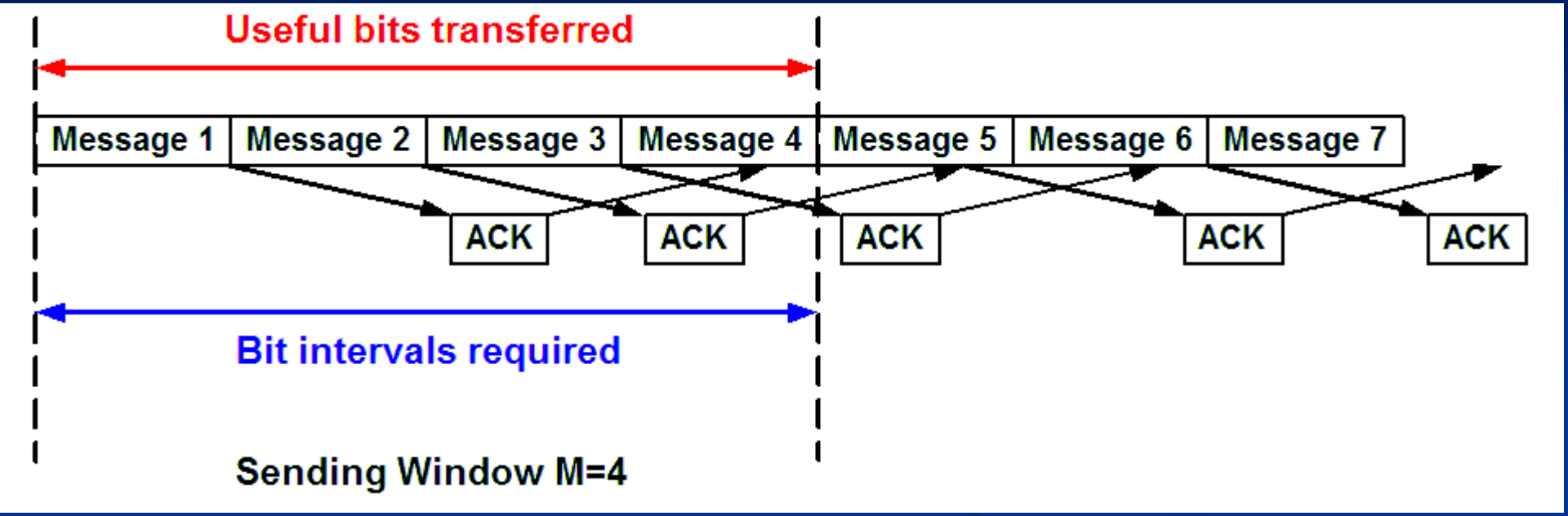
Prodloužení rámce efektivitu zlepší, ale v případě výskytu chyby v rámci se pak zahazuje celý (dlouhý) rámec, oproti např. jen jednomu ze dvou polovičních.

Sliding Window



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

Efektivita 100% u Sliding Window



Popřemýšlejte...

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