



دانشگاه شهید مدنی آذربایجان

Computer Networks

شبکه های کامپیوتری

دانشگاه شهید مدنی آذربایجان
دانشکده فناوری اطلاعات و مهندسی کامپیوتر
دکتر محسن حیدریان

اسلایدهای درس شبکه های کامپیوتری
(رشته مهندسی کامپیوتر)
نیمسال دوم ۱۴۰۰

روشهای مطمئن کردن کانال انتقال داده Reliability

سه ویژگی امنیت Security، ایمنی Safety و اطمینان Reliability در یک سیستم انتقال داده مهم هستند:

۱- امنیت: ابتدا برای کاربران سطح دسترسی مجاز به منابع و داده ها تعیین می شود. یک کاربر فقط به منابع قابل دسترسی اش به صورت مجاز حق دسترسی دارد. کاربرانی که به صورت غیر مجاز قصد دسترسی به داده ها و منابع غیر مجاز دیگران را دارند، حمله کننده یا attacker محسوب می شوند و ناقض امنیت منابع و داده ها هستند. همه روشهای شناسایی و جلوگیری از حمله مانند نصب دزدگیر را امنیت اطلاعات و امنیت منابع می نامند.

۲- ایمنی: سیستم هنگام تعامل با سیستم های دیگر نباید دچار افت کارایی، توقف یا تخریب در خدمات دهی شود. ساختن یک ساختمان بدون سیستم اطفای حریق، نقض ایمنی است. ایمنی با امنیت متفاوت هست.

۳- ارسال و تحویل حتمی و قطعی بسته های کاربر به مقصد، اطمینان کانال نامیده می شود. پروتکل TCP در لایه حمل اینترنت و پروتکل ARQ در لایه پیوند داده OSI، پروتکل های مطمئن کننده کانال هستند.

نقش کنترل جریان و کنترل خطا در مطمئن کردن یک کانال

کنترل جریان مجموعه فعالیت هایی است که فرستنده انجام می دهد تا حجم داده ارسال شده به مقصد کنترل شود. این فعالیت ها قبل از دریافت پیام تصدیق از گیرنده است. اگر خط ارسال و دریافت داده بدون خطا باشد، دو نوع کنترل جریان زیر وجود خواهد داشت:

- Stop-and-Wait flow control
- Sliding-Window flow control

۵ عملیات زیر باعث می شود یک کانال انتقال بسته به یک کانال مطمئن تبدیل شود:

- کنترل خطا نیز به معای کشف خطا در بسته و رفع آن است. که شامل عملیات زیر است:
- تشخیص خطا Error detection

- ارسال پیام تصدیق از طرف گیرنده اگر بسته را بدون خطا دریافت کرده باشد Positive Acknowledgement (ACK):

- ارسال پیام تصدیق منفی اگر گیرنده بسته را با خطا دریافت کرده باشد Negative Acknowledgement (NAK):

- ارسال مجدد بسته توسط فرستنده اگر در یک مدت مشخصی پیام تصدیق منفی یا مثبت را از طرف گیرنده دریافت نکرده باشد.

مجموعه عملیات بالا روش **Automatic Repeat Request (ARQ)** نامیده می شود. معنای این عبارت ارسال کن و منتظر بمان یا به عبارت دیگر ارسال یک بسته و منتظر ماندن برای دریافت تصدیق آن است.

روشهای کنترل خطا و جریان

- کنترل خطا و کنترل جریان برای ایجاد یک کانال مطمئن ترکیب می شوند و ترکیب آنها کنترل در لایه پیوند داده را تشکیل می دهد که یکی سه روش زیر را شامل می شود:

- Stop-and-Wait ARQ
- Go-Back-N ARQ
- Selective repeat ARQ

- روش ARQ یک کانال نا مطمئن را به یک کانال مطمئن تبدیل می کند و از تحویل داده بسته به مقصد اطمینان حاصل می کند. این روش ویژگی های زیر را دارد:

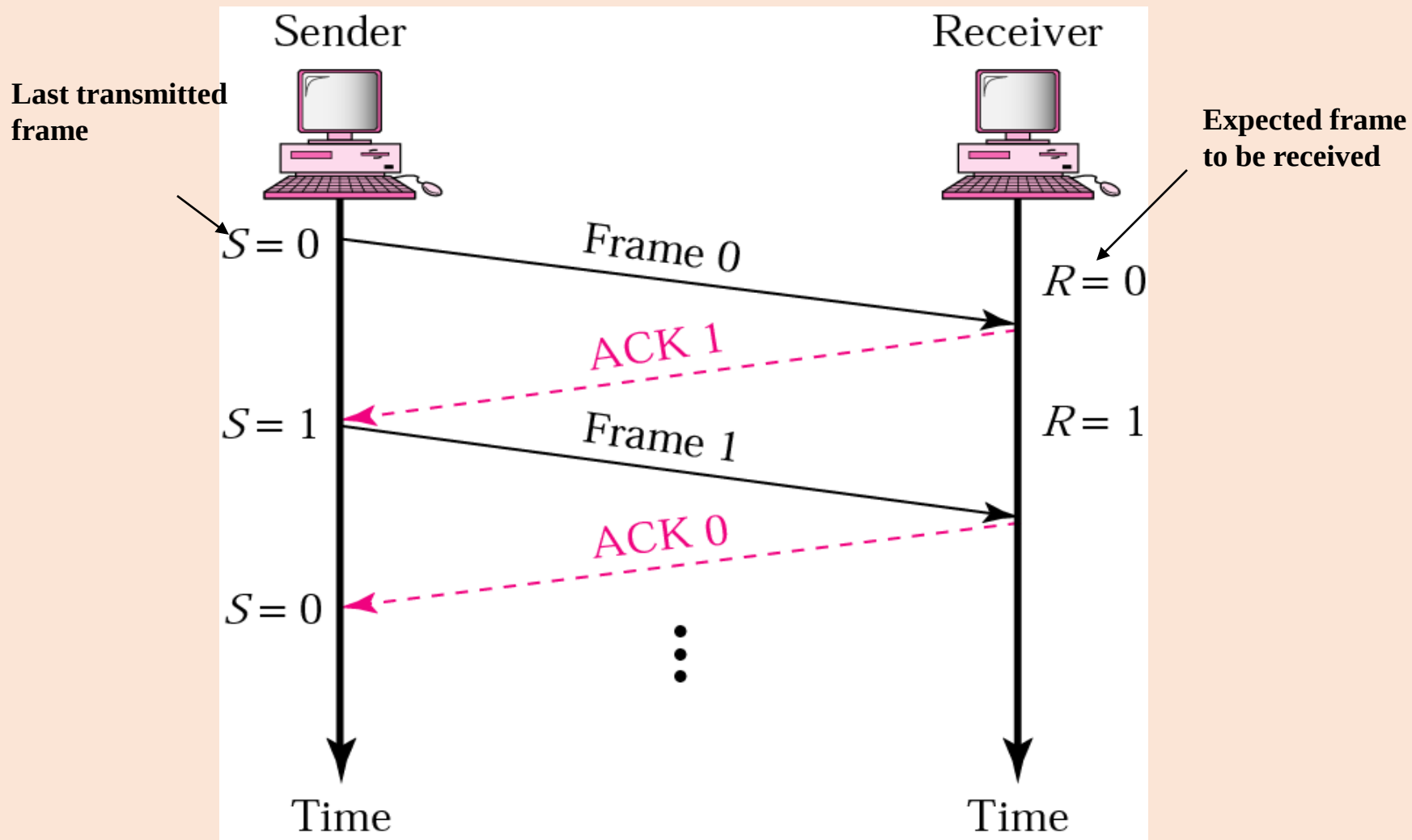
- بدون خطا
- از تحویل دو بار یک بسته به مقصد خودداری می کند
- حفظ ترتیب بسته ها در مبدا و مقصد
- هیچ بسته ای گم نمی شود

تشریح گام های روش Stop-and-Wait ARQ

- ساده ترین روش انتقال بدون خطا است

- بسته های داده و پیام ACK به صورت متوالی با ۰ و ۱ علامت گذاری می شوند
- اگر گیرنده پیام با شماره صفر را دریافت کند، $ACK1$ را بر می گرداند و منتظر دریافت فریم با شماره ۱ خواهد ماند. پیام $ACK0$ بسته دریافت شده با شماره ۰ را تایید می کند و پس از آن گیرنده منتظر دریافت بسته شماره ۱ خواهد ماند.
- اعداد به کار رفته برای شماره گذاری بسته های متوالی به صورت ۰ و ۱ هستند.
- متغیر R در گیرنده به کار می رود و متغیر S نیز در فرستنده. اگر $R=1$ یعنی گیرنده منتظر بسته ۱ است و اگر $S=1$ یعنی بسته ارسالی بعدی بسته با شماره ۱ خواهد بود.

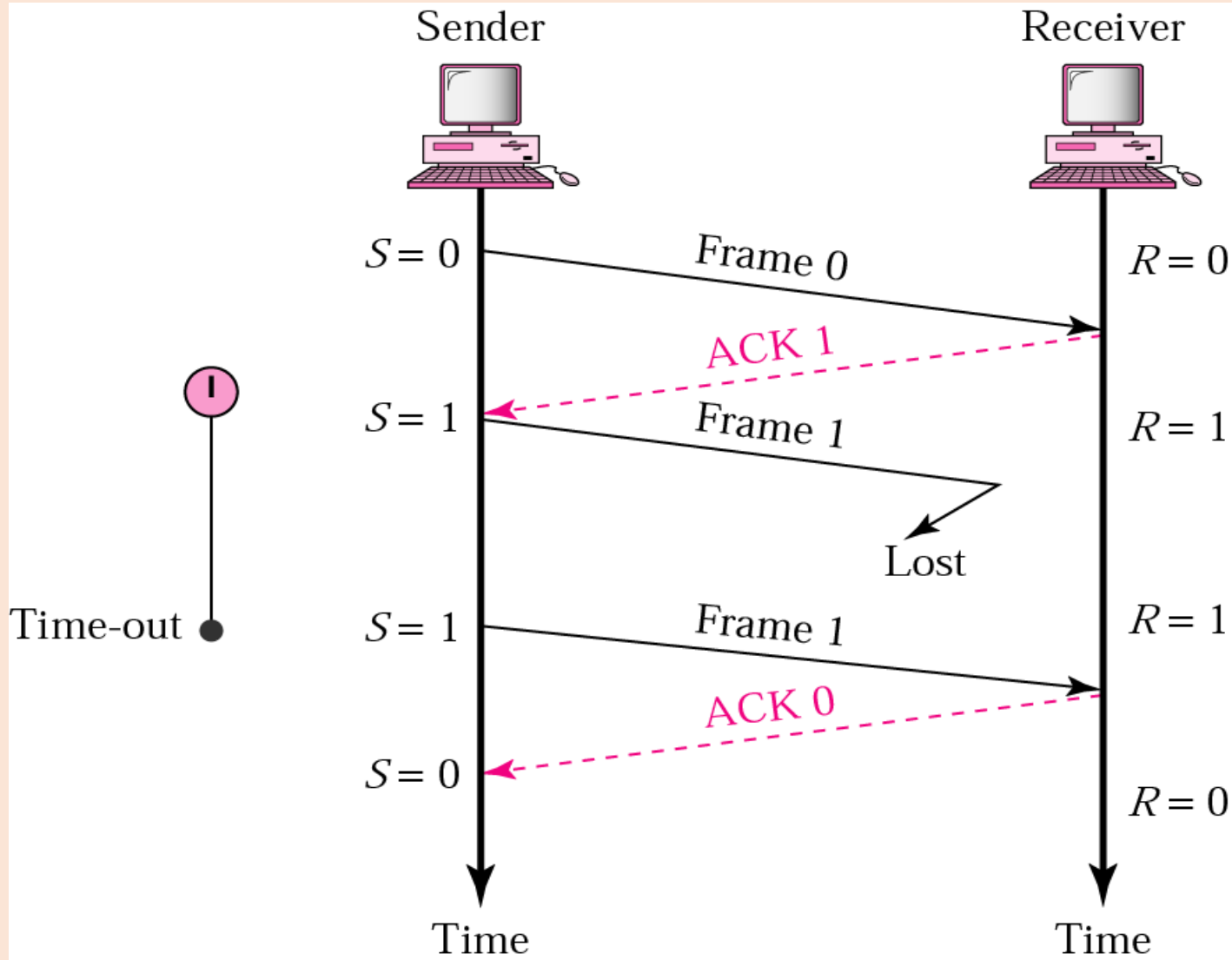
روش عمل کرد ARQ و متغیرهای S، R، ACK

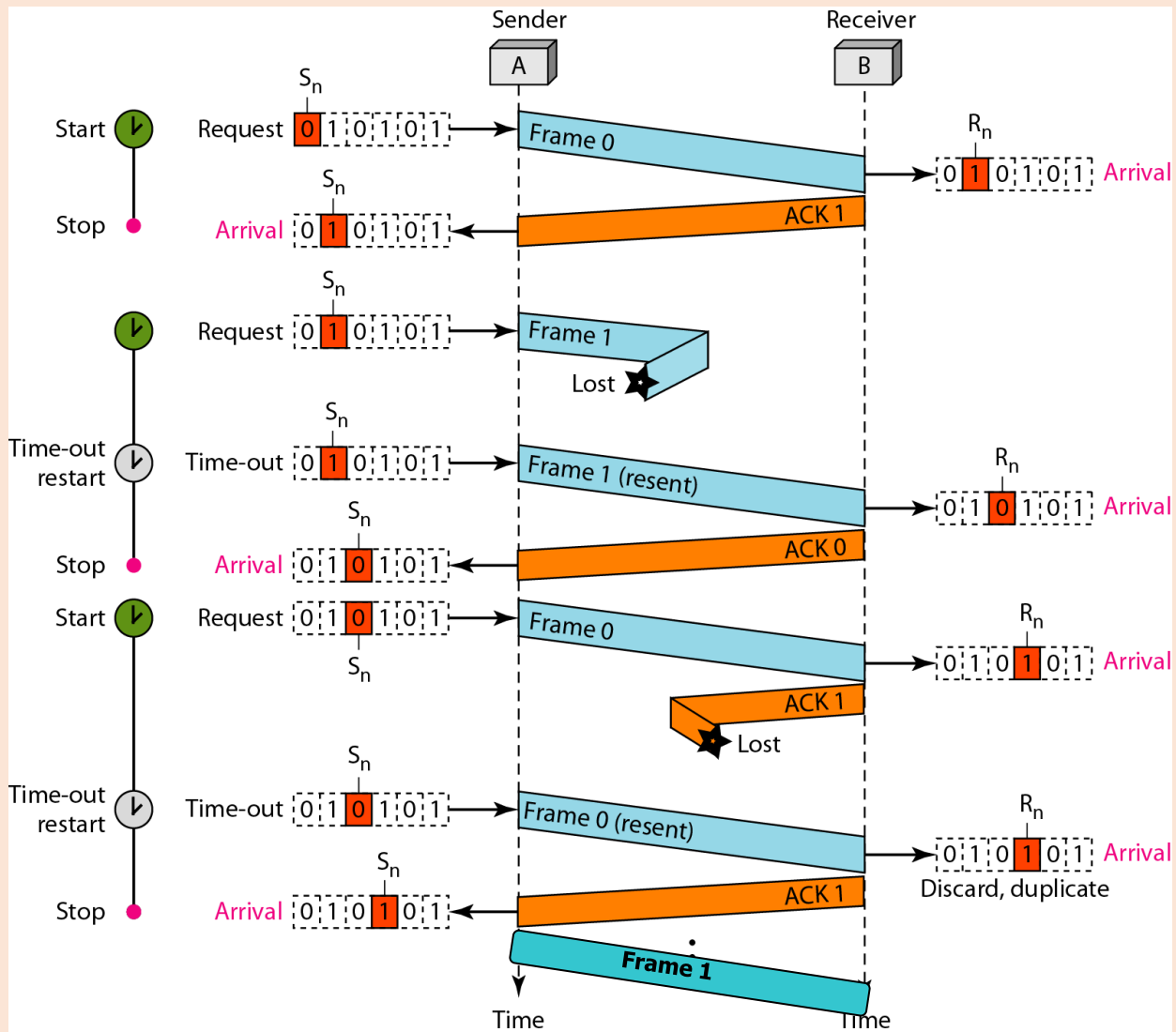


ویژگی های Stop-and-Wait ARQ

- اگر گیرنده خطایی در بسته ببیند، آن را حذف می کند.
- اگر گیرنده بسته خارج از انتظار (مثلا $R=0$ باشد و بسته با شماره 1 را دریافت کند) را دریافت کند آن را حذف می کند و مجدداً تصدیق بسته قبلی را ارسال می کند نه تصدیق بسته اشتباه دریافت شده را.
- اگر گیرنده منتظر تصدیق $ACK0$ یک بسته ارسال شده باشد (مثلا بسته با شماره $S=1$) و تصدیق $ACK1$ متعلق به بسته قبلی را دریافت کند (یعنی تصدیق بسته $S=0$ را دریافت کند)، آن تصدیق را نمی پذیرد و حذف می کند.
- یک کپی از بسته ارسال شده در حافظه ارسال کننده هست و تا زمانی که تصدیق این بسته از طرف گیرنده برنگردد، این بسته مکرراً ارسال شده و از حافظه پاک نخواهد شد.
- فرستنده با ارسال هر بسته، یک تایمر را فعال می کند. اگر تصدیق بسته ارسال شده در طی مدت زمان مشخصی برنگردد، بسته مجدداً ارسال شده و مجدداً تایمر فعال می شود.

گم شدن بسته در روش Stop-and-Wait ARQ





Note:

در روش ARQ شماره گذاری فریم ها از دو بار دریافت شدن
یک فریم جلوگیری می کند

Note:

پیام های ACK شماره گذاری می شوند تا بسته های متناظر آنها توسط مقصد دو بار دریافت نشوند یا بسته های گم شده بتوانند توسط فرستنده دوباره ارسال شوند.

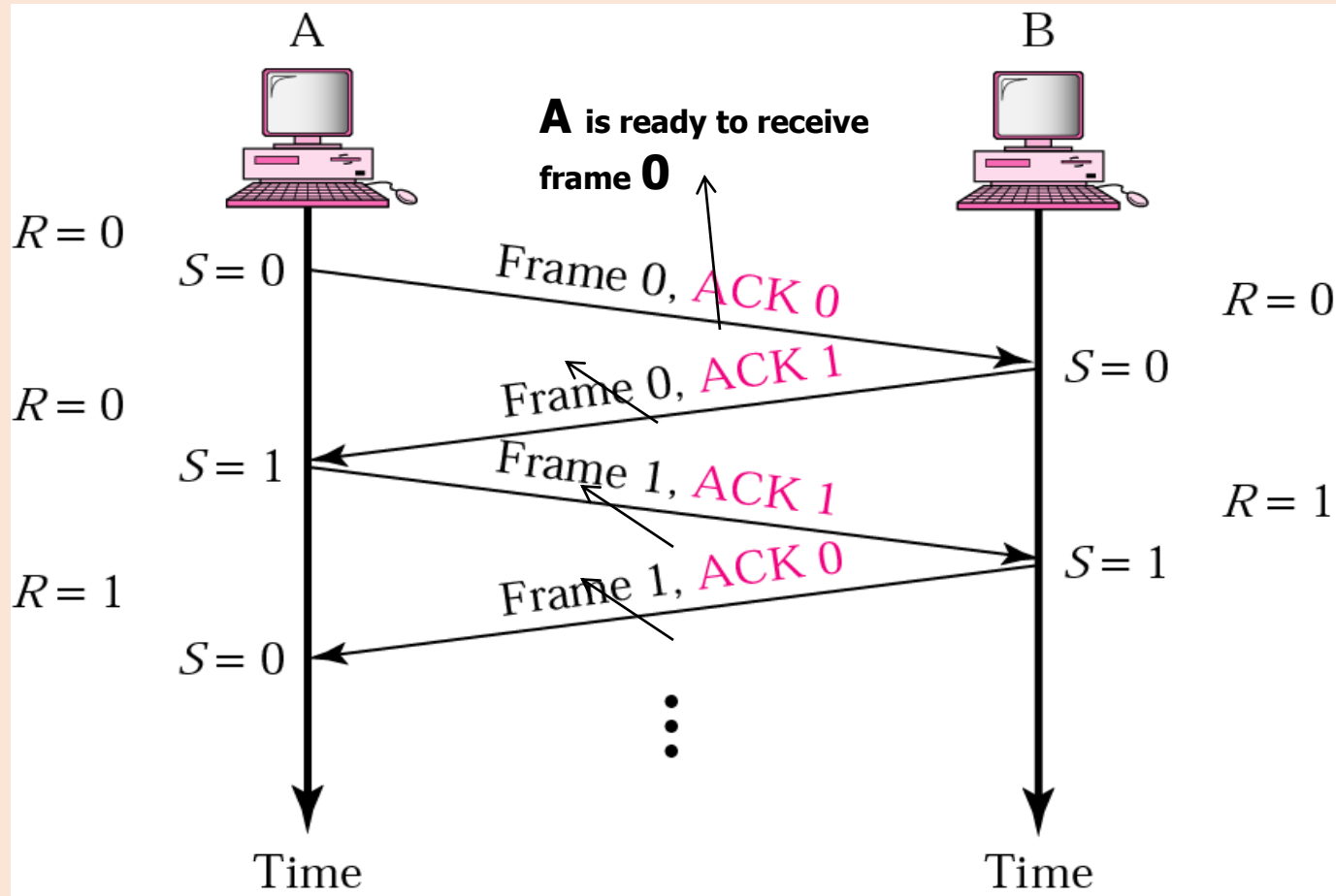
کارایی روش Stop-and-wait

- هر بار یک بسته ارسال می شود و مدت زمانی نیز صرف دریافت تصدیق می شود.
- اگر زمان رسیدن بسته به مقصد خیلی کوتاه باشد، کارایی روش ARQ خوب خواهد بود.
- اگر زمان رسیدن بسته به مقصد طولانی باشد و زمان برگشت ACK نیز طولانی باشد، این روش کارایی خوبی نخواهد داشت زیرا انتظار برای دریافت ACK خیلی طولانی می شود و تلفات زمانی زیاد می شود.
- چون ارسال بسته ها یکی یکی انجام می شود، این روش کارایی بالایی ندارد و تلفات پهنای باند نیز زیاد می شود.

روش ARQ دو طرفه: روشی برای افزایش کارایی ARQ معمولی

- در این روش، هر بسته که توسط گیرنده دریافت می شود، گیرنده همراه با تصدیق آن بسته، یک بسته جدید نیز بر می گرداند و گیرنده نقش فرستنده هم بازی می کند. لذا تلفات زمانی کاهش می یابد.
- در این روش یک تصدیق و یک بسته با یکدیگر ترکیب می شوند و تلفات پهنای باند کاهش می یابد.

روش ARQ دو طرفه



تشریح روش TCP و مقایسه با ARQ

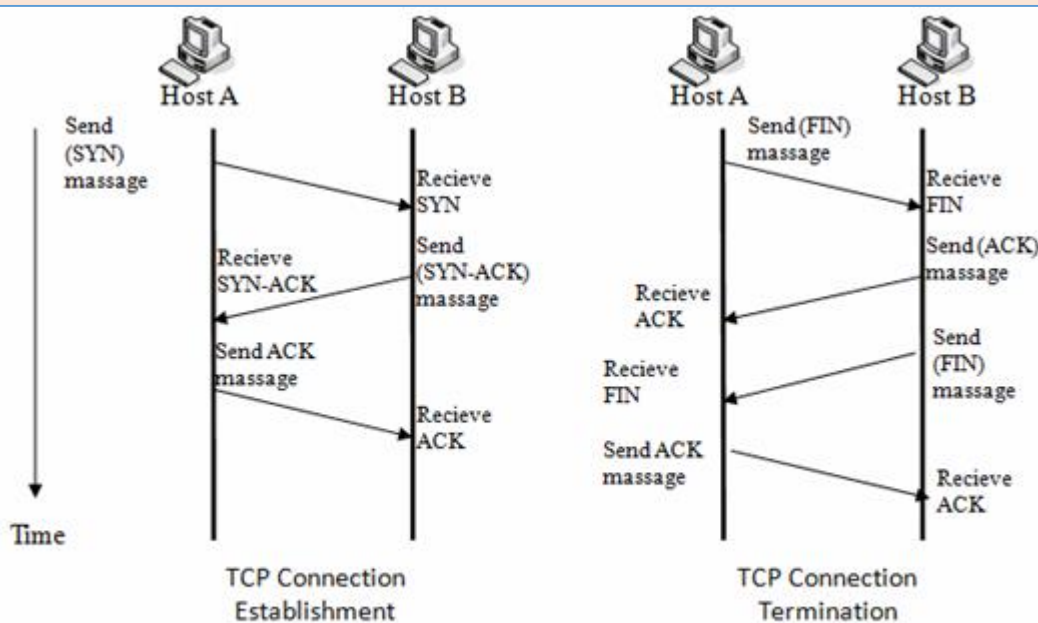
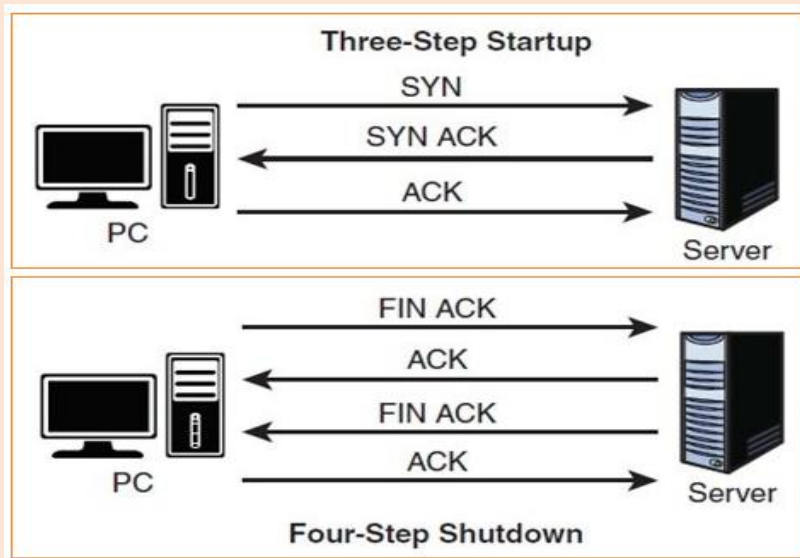


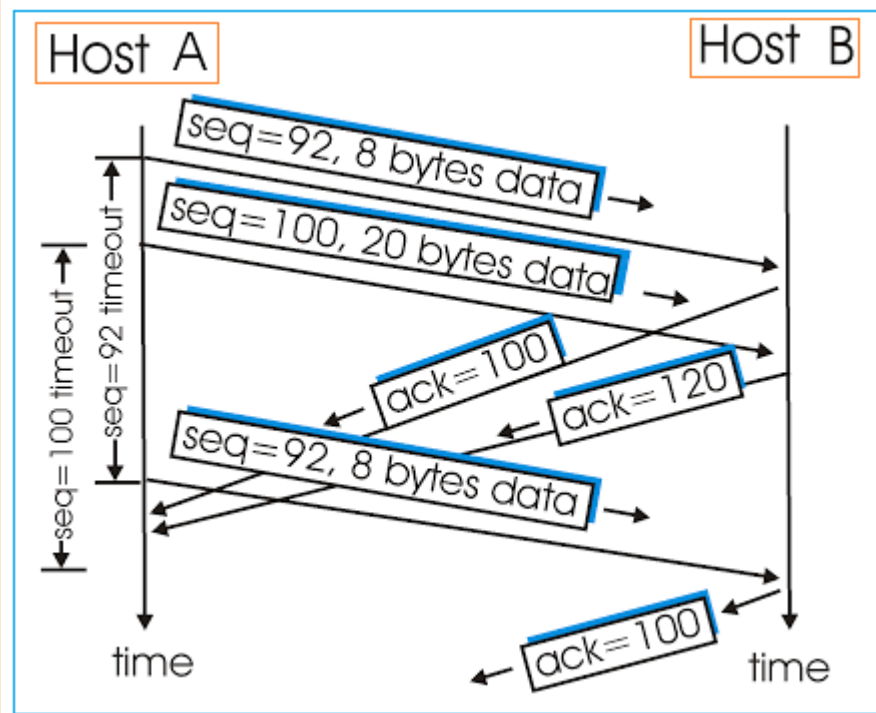
Figure 2.1. TCP session establishment and termination

برای ایجاد اتصال در پروتکل TCP یک Handshake سه مرحله‌ای Three-way Handshaking انجام می‌شود. ابتدا مبدأ، یک پیام SYN به مقصد ارسال می‌کند تا مکالمه شروع شود. سپس مقصد پیام SYN/ACK را به مبدأ ارسال می‌کند تا موافقت خود را برای ایجاد مکالمه ابراز کند و در نهایت نیز مبدأ یک پیام ACK به مقصد می‌فرستد تا پس از آن فرایند انتقال پیام آغاز شود.

برای اتمام اتصال نیز یک Handshake چهار مرحله‌ای Four-way Handshaking لازم است. هر کدام از طرفین مکالمه می‌تواند آغازگر فرایند اتمام اتصال باشند. به این ترتیب، طرف آغازکننده‌ی فرایند، یک پیام FIN به طرف دیگر ارسال می‌کند و طرف دیگر نیز با ACK به آن پاسخ می‌دهد و همچنین یک پیام FIN دیگر را به آن طرف اول می‌فرستد. در ادامه طرف اول با ACK به طرف مقابل پاسخ می‌دهد و پس از مدت زمانی مشخص، اتصال را قطع می‌کند. طرف مقابل نیز با دریافت ACK، اتصال را از سمت خود خاتمه می‌دهد.



تشریح روش TCP و مقایسه با ARQ



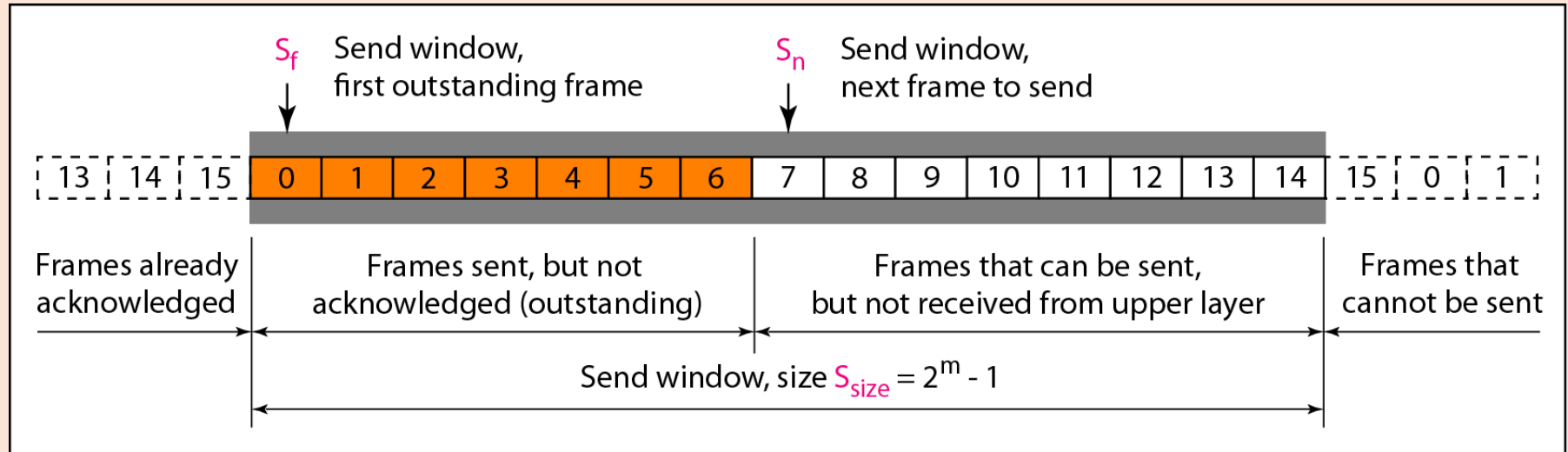
انتقال اطلاعات در پروتکل TCP به این صورت است که بروی هر بسته شماره ای به نام sequence number زده میشود. پس از چندین ارسال، سرویس گیرنده به سرور پیغامی مبنی بر دریافت براساس شماره های بسته ها برای سرویس دهنده ارسال میکند. اگر بسته در انتها آسیب دیده باشد یا به دست مقصد نرسیده باشد، سرویس گیرنده آن شماره را از شماره های تاییدی حذف می کند. به این ترتیب سرور مجددا اقدام به ارسال پکت از بین رفته می کند.

در شکل مقابل دیده می شود بسته شماره 98 توسط مقصد B دریافت نشده است و پس از گذشت مدت زمان لازم و مشخص، تاییدیه آن در A دریافت نشده است. لذا هاست A مجددا آن را برای هاست B ارسال می کند.

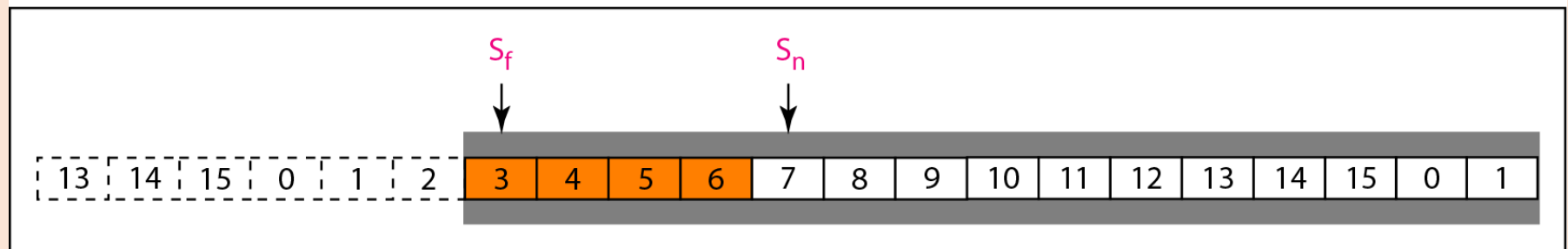
روش Go-Back-N ARQ

- این روش به پنجره لغزان معروف است sliding window
- بسته ها در فرستنده با اعداد به صورت دنباله هایی از اعداد $(2^m - 1) - 0$ شماره گذاری می شوند. مثلاً برای $m=3$ خواهیم داشت:
 $m=3 \rightarrow (0,1,2,3,4,5,6,7,0, 1,2,3,4,5,6,7,...)$
- فرستنده می تواند بسته ها را به صورت گروهی با شماره های بین 0 الی $2^m - 1$ ارسال کند اما تعداد بسته های ارسالی نباید بیشتر از $2^m - 1$ باشد.
- فقط فریم هایی می توانند ارسال شوند که در محدوده پنجره قرار داشته باشند. پنجره شامل 2^m فریم است.
- فریم های سمت چپ پنجره ارسال شده اند و تصدیق آنها نیز دریافت شده است. فریم های سمت راست پنجره نیز در انتظار شدن ارسال هستند.
- فریم های داخل پنجره نیز به سمت گیرنده ارسال شده اند و فرستنده منتظر دریافت تصدیق آنها است. تصدیق هر بسته ارسال شده ای که دریافت شود، آن بسته از پنجره خارج شده و به سمت چپ پنجره منتقل خواهد شد و یکی از بسته های سمت راست پنجره به داخل پنجره اضافه خواهد شد. (این عمل لغزیدن پنجره نام دارد)
- .

پنجره ارسال در فرستنده Go-Back-N ARQ

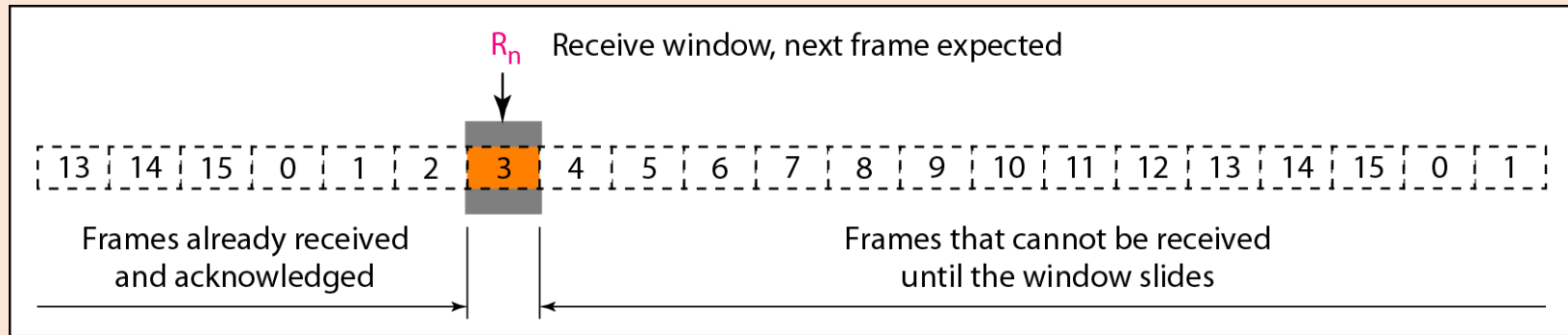


a. Send window before sliding

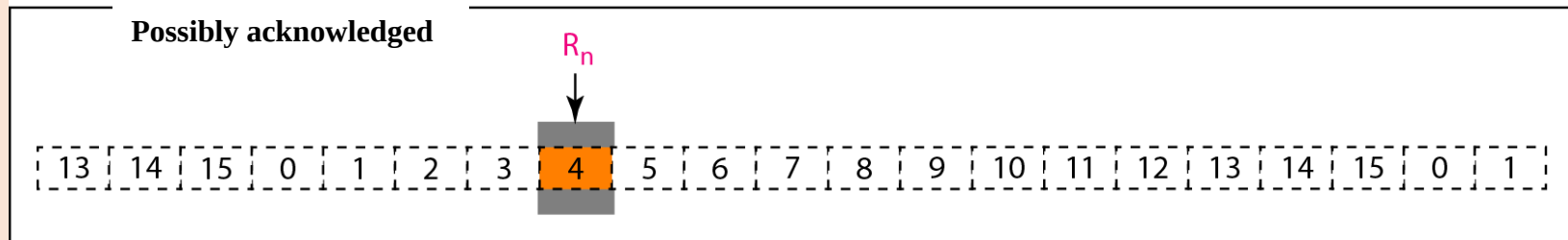


b. Send window after sliding

پنجره به طول یک در سمت گیرنده در روش *Go-Back-N ARQ*



a. Receive window



b. Window after sliding

وقتی که یک بسته بدون خطا و با ترتیب مجاز در سمت گیرنده دریافت می شود، پنجره سمت گیرنده یک واحد به راست خواهد لغزید و تصدیق آن بسته برای فرستنده ارسال خواهد شد. بسته های سمت چپ پنجره دریافت شده و تصدیق شده اند. بسته های سمت راست پنجره نیز هنوز دریافت نشده اند و تصدیق آنها برای گیرنده ارسال نشده است. بسته های سمت راست پنجره ممکن است هنوز در سمت فرستنده باشند، یا در حال آمدن به سمت گیرنده باشند و یا دریافت شده اند اما در حافظه گیرنده قرار دارند و منتظر چک شدن برای خطا و دریافت نهایی و ارسال تصدیق آنها برای مقصد باشند.

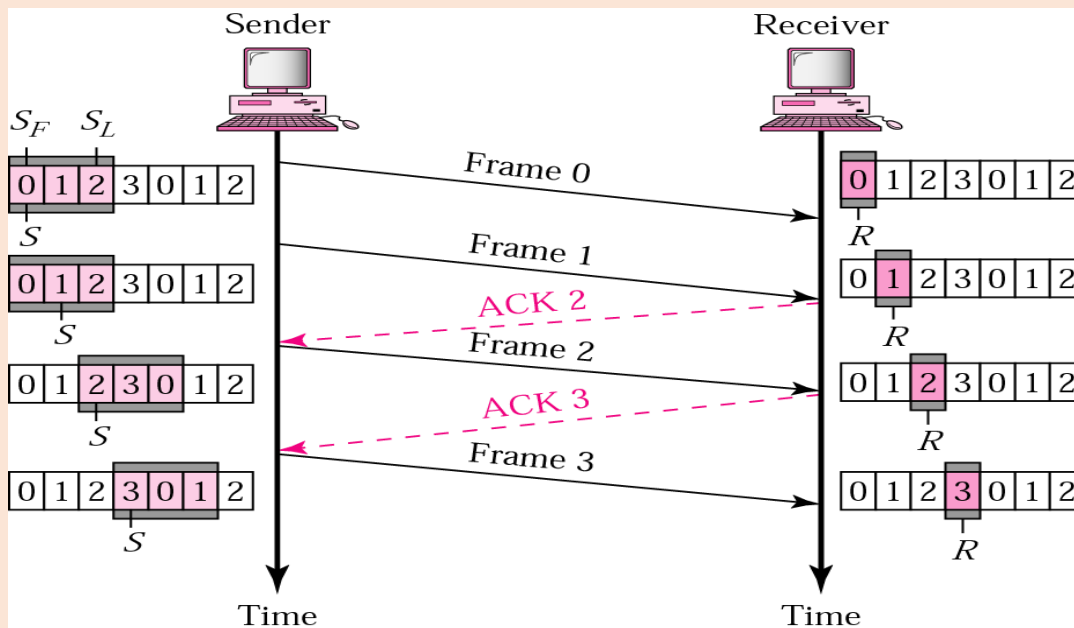
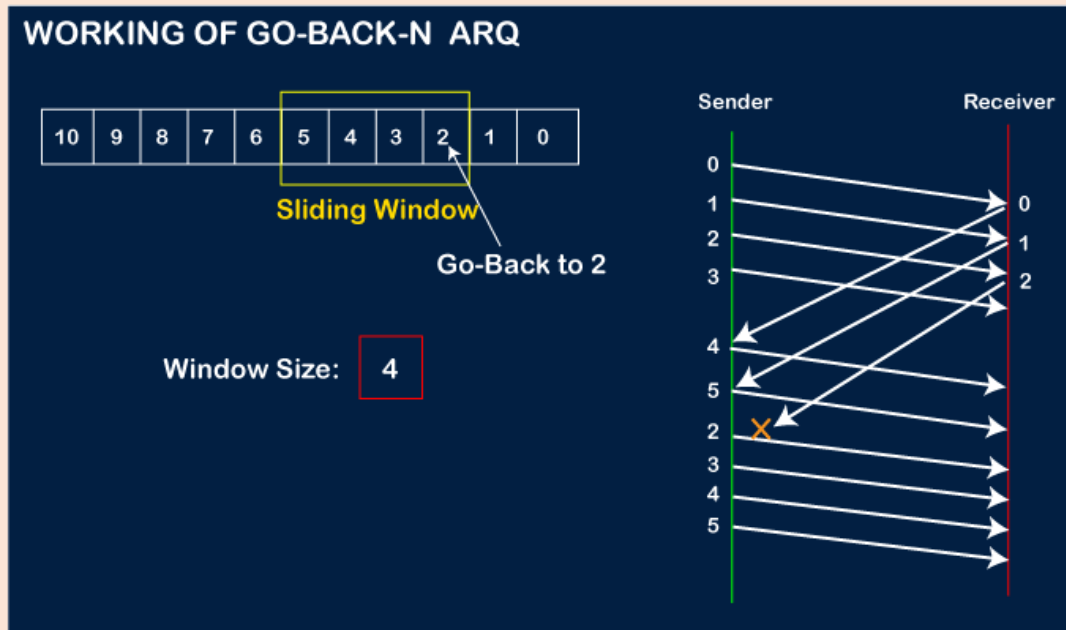
ویژگی های Go-Back-N ARQ

- ساختن پنجره سمت گیرنده
- طول این پنجره یک است و مشخص می کند کدام بسته باید دریافت شود
- بسته بعدی باید طبق شماره و ترتیب اعلام شده در مبدا دریافت شود
- اگر بسته بدون خطا و طبق ترتیب دریافت شود، پنجره یک واحد به راست خواهد لغزید

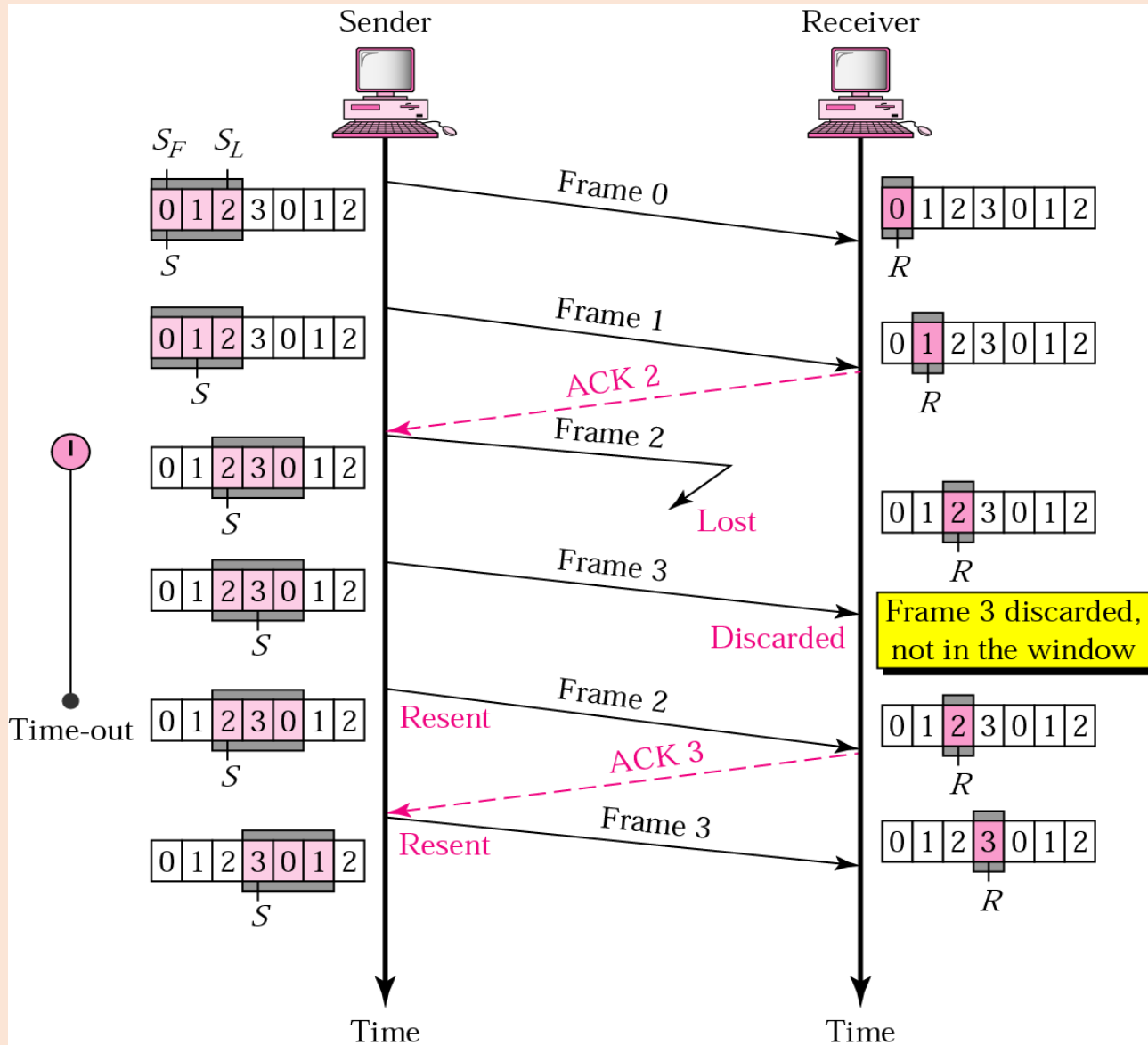
عملیات

- گیرنده می تواند تصدیق را برگرداند اگر بسته بدون خطا و طبق ترتیب دریافت شده باشد
- گیرنده می تواند برای چند فریم متوالی دریافت شده سالم و طبق ترتیب، یک تصدیق برگرداند. مثلاً می تواند ACK5 بسته های شماره ۰، ۱، ۲، ۳ و ۴ را تصدیق کرده و انتظار برای فریم ۵ را اعلام کند.
- بسته های خطا دار یا خارج از ترتیب حذف می شوند و بسته های بعد از آن نیز نمی توانند دریافت و تصدیق شوند.
- فرستنده منتظر دریافت ACK یک بسته باقی می ماند و اگر آن ACK نرسد، فرستنده آن بسته و همه بسته های بعد از آن را نیز ارسال می کند.

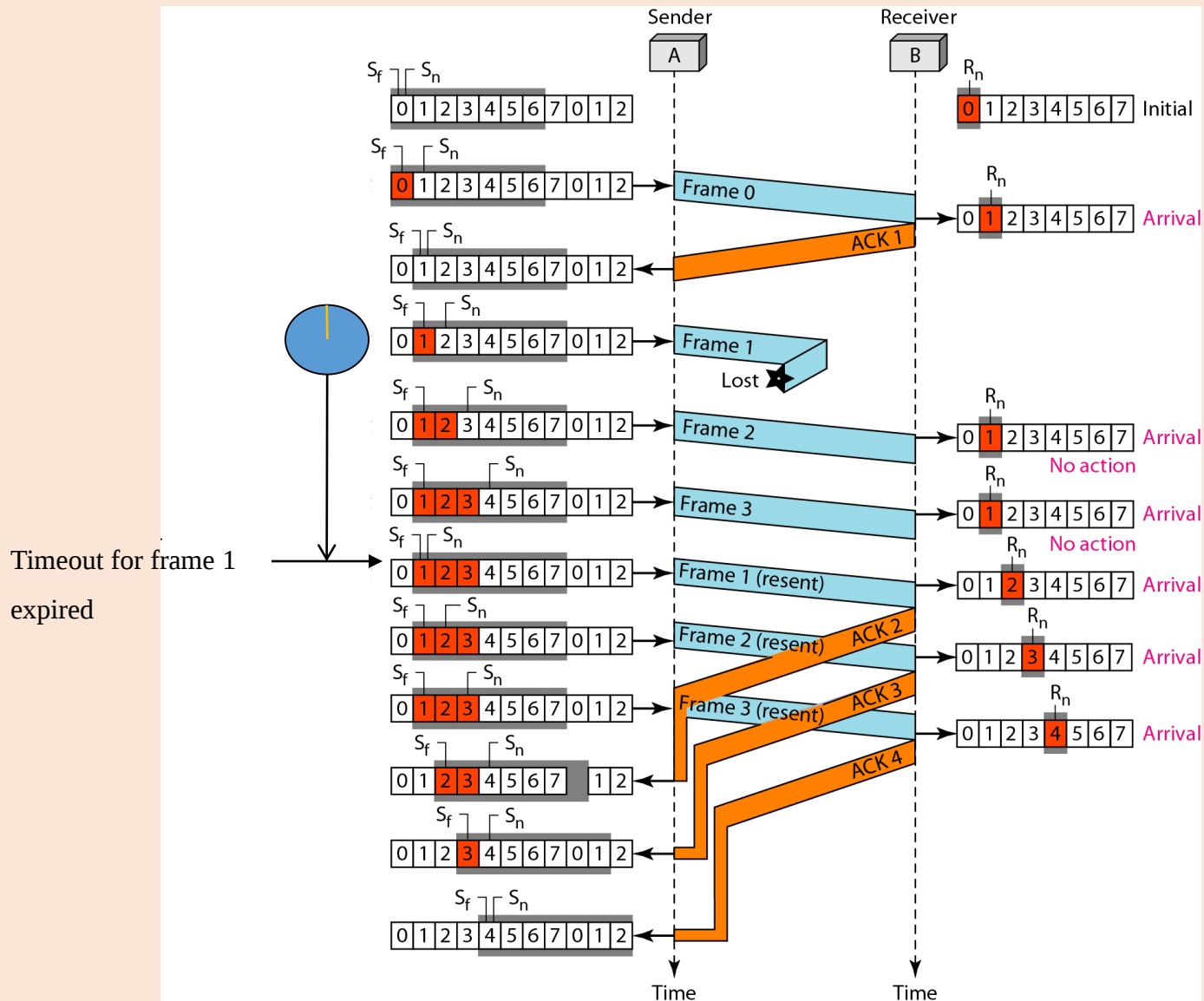
روش ارسال موفق و ناموفق بسته در Go-Back-N ARQ



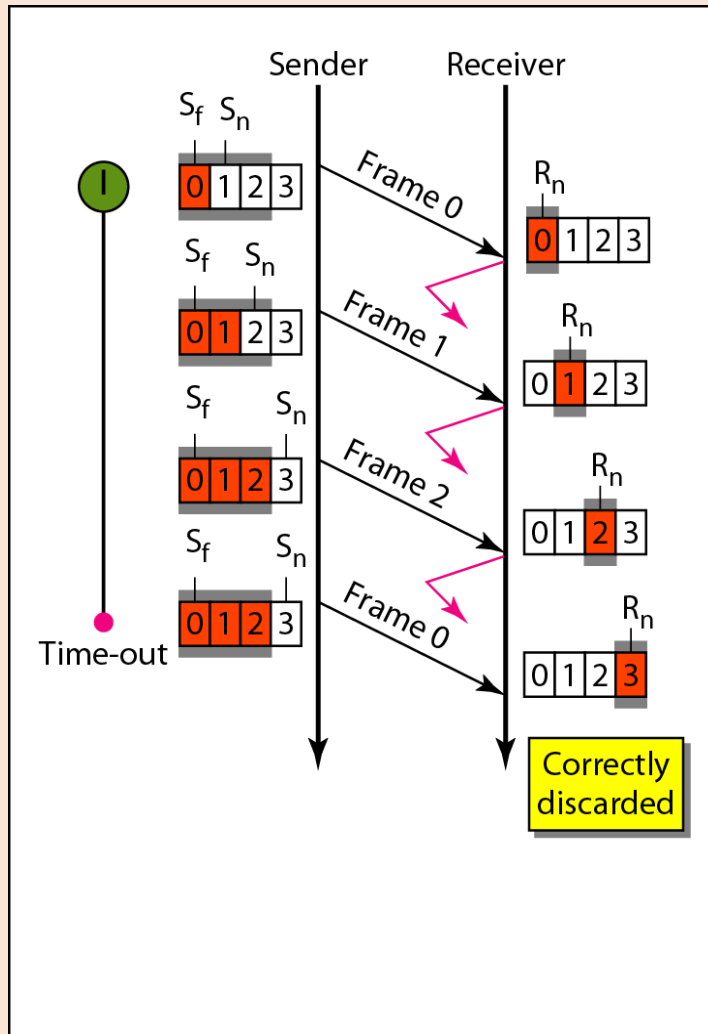
گم شدن بسته در روش Go-Back-N ARQ



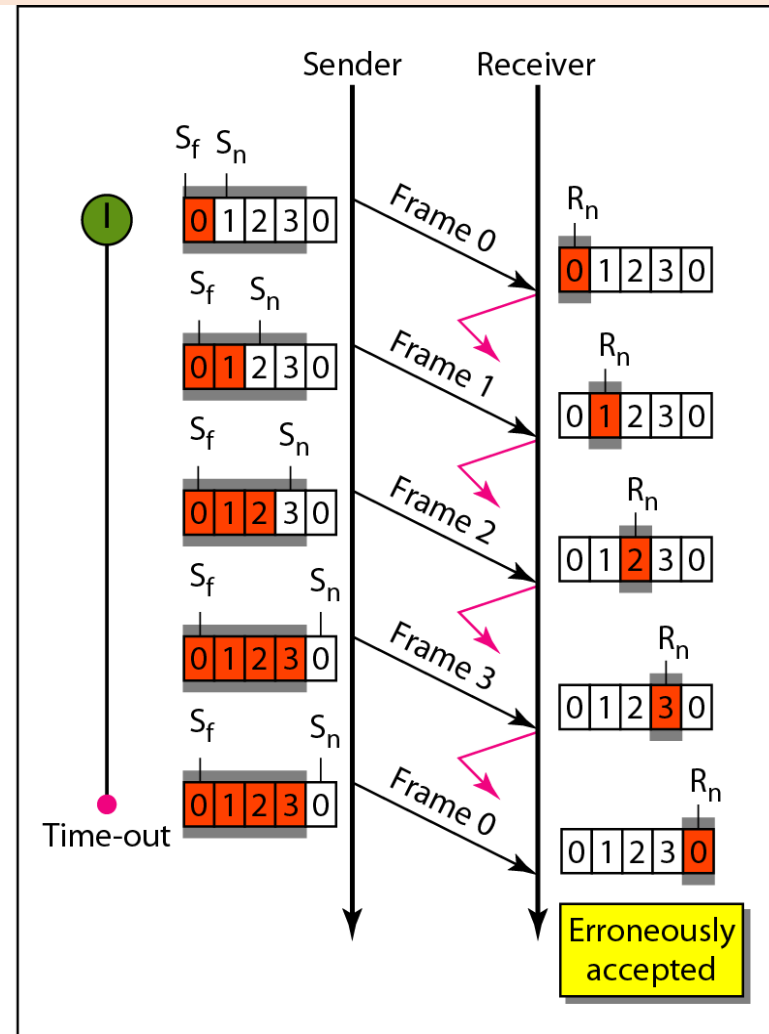
گم شدن بسته در Go-Back-N ARQ



اندازه پنجره در روش Go-Back-N ARQ



a. Window size $< 2^m$



b. Window size $= 2^m$

کارایی روش Go-Back-N ARQ

- بهتر از روش ARQ یک طرفه است
- اگر نرخ خطای کانال بالا باشد، خیلی پهنای باند را هدر می دهد.

