Issues in Ad hoc Wireless Networks

- Medium access scheme
  - **Distributed operation** is required.
  - **Synchronization** is required in TDMA-based systems.
  - **Hidden terminals** are nodes hidden from a sender.
  - **Exposed terminals** are exposed nodes preventing a sender from sending.
  - **Throughput** needs to be maximized.
  - **Access delay** should be minimized.
  - **Fairness** refers to provide an equal share to all competing nodes.
  - **Real-time traffic support** is required for voice, video, and real-time data.
  - **Ability to measure resource availability**, helps in congestion control
  - **Capability for power control** reduces the energy consumption.
  - **Use of directional antennas** has advantages including increased spectrum reuse, reduced interference, and reduced power consumption.

Issues in Ad hoc Wireless Networks

- Routing
  - Mobility (path breaks, packet collision, transient loops, stale roots)
  - Bandwidth constraint
  - Error-prone and shared channel: wireless channel (10^{-5} to 10^{-3}), wired channel (10^{-12} to 10^{-9})
  - Location-dependent contention: (High contention should be avoided by balancing load)
  - Other resource constraints such as computing power, battery power
  - Minimum route acquisition delay
  - Quick route reconfiguration
  - Loop-free routing
  - Distributed routing approach
  - Minimum control overhead
  - Scalability
  - Provisioning of QoS (bandwidth, delay, jitter, packet delivery ration, throughput)
  - Support for time-sensitive traffic: hard real-time and soft real-time traffic
  - Security and privacy

Issues in Ad hoc Wireless Networks

- The objectives of the transport layer protocols include:
  - Setting up and maintaining end-to-end connections
  - Reliable end-to-end delivery of data packets
  - Flow control
  - Congestion control
  - UDP neither perform flow and congestion control nor reliable data transfer
  - Do not take into account the current network status like congestion at intermediate nodes, rate of collision or other factors.
  - Increase the load in the network blindly and degrade performance.
  - TCP faces the problem of dynamic topology, path breaks, stale routing information, high channel error rate, and frequent network partitioned
  - The process of finding an alternate path or reconfiguring the broken path might take longer than the retransmission timeout of the transport layer at the sender, resulting in retransmission of packets and execution of the congestion control algorithm with decreasing congestion window.
  - Due to error, lots of ACK packets and even ACK can loss which intern invoke congestion algorithm

Issues in Ad hoc Wireless Networks

Multicasting. (Point to Multipoint and Multipoint to Multipoint)

- In emergency search-and-rescue operations and military communication applications nodes form groups to carry out certain tasks that require point-to-multipoint and multipoint-to-multipoint voice and data communication
- Wired network multicast protocols such as core based trees (CBT), protocol independent multicast (PIM), and distance vector multicast routing protocol (DVMRP) do not perform well in ad hoc wireless networks because a tree-based multicast structure is highly unstable and needs to be frequently readjusted to include broken links.
- Use of any global routing structure such as the link-state table results in high control overhead.
- Issues in designing multicast protocol
  - Robustness (recover and reconfigure quickly from link breaks)
  - Efficiency (Minimum number of message transfer to convey information to all)
  - Control overhead
  - Quality of service (Support of time sensitive data)
  - Efficient group management
  - Scalability
  - Security (Authentication of session members and preventing of unauthorized information)

Issues in Ad hoc Wireless Networks

- Pricing Schemes need to incorporate service compensation.
- Quality of Service Provisioning
  - QoS parameters based on different applications
    - multimedia applications, the bandwidth and delay are the key parameters, whereas military applications have the additional requirements of security and reliability
    - Emergency search-and-rescue operations, availability is the key parameter
    - For WSN battery life and energy conservation is the parameter
  - QoS-aware routing uses QoS parameters to find a path.
  - QoS framework is a complete system that aims at providing the promised services to each users.

Issues in Ad hoc Wireless Networks

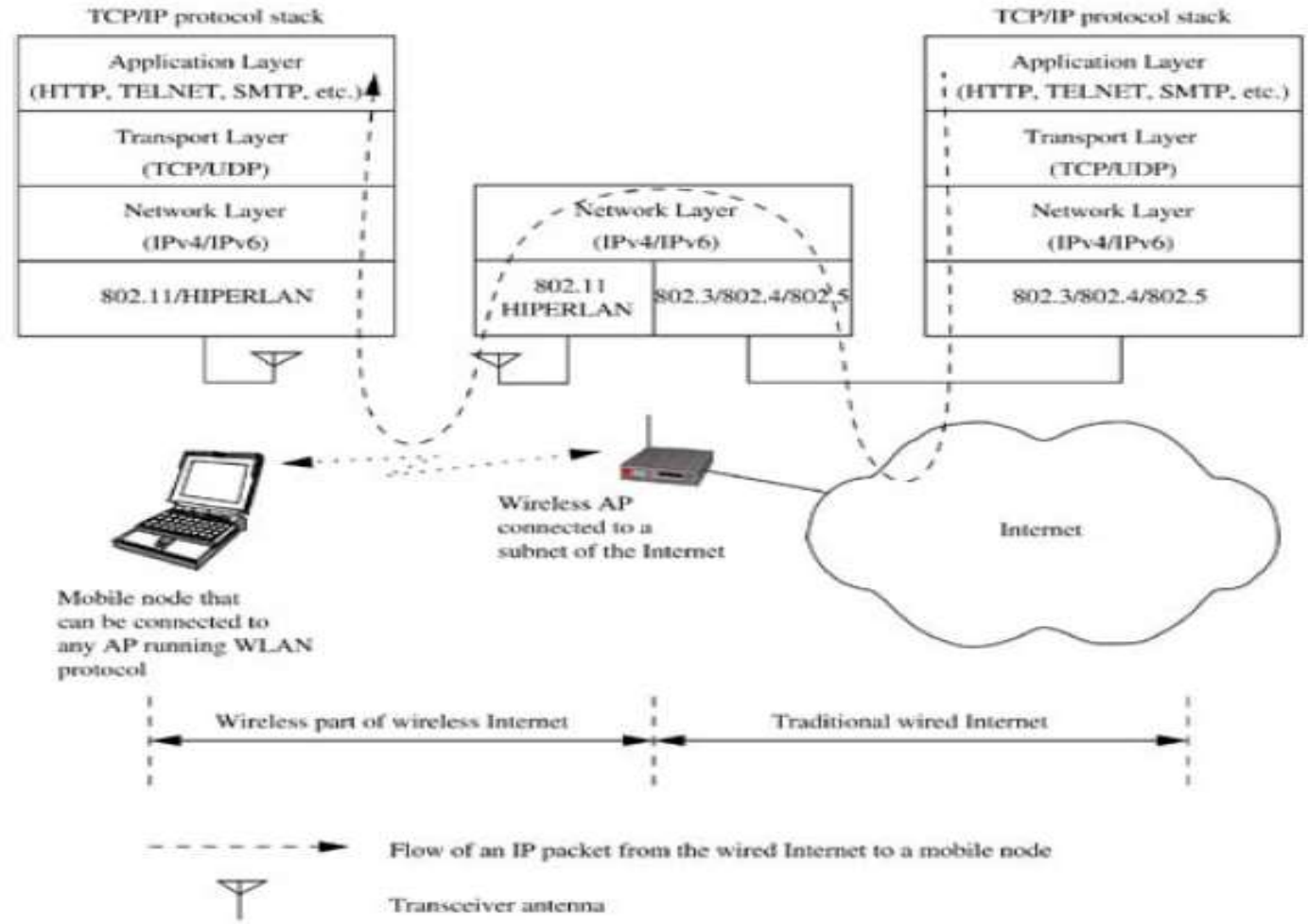
- Self-Organization is required in ad hoc wireless networks:
  - Neighbor discovery (Building local topology)
  - Topology organization (Exchanging topology information)
  - Topology reorganization (Recovery from major topological changes)
  - Network partitioning and recovery
- Security
  - Denial of service
  - Resource consumption
    - Energy depletion: deplete the battery power of critical nodes
    - Buffer overflow: flooding the routing table or consuming the data packet buffer space
  - Host impersonation: A compromised node can act as another node.
  - Information disclosure: a compromised node can act as an informer.
  - Interference: jam wireless communication by creating a wide-spectrum noise.

Issues in Ad hoc Wireless Networks

- Energy Management
  - Transmission power management: The radio frequency (RF) hardware design should ensure minimum power consumption.
  - Battery energy management is aimed at extending the battery life.
  - Processor power management: The CPU can be put into different power saving modes.
- Scalability is expected in ad hoc wireless networks.
- There are issues related to wireless internet also.

What is Wireless Internet?

- The extension of the services offered by the Internet to mobile users enabling them to access information and data irrespective of their location.



Issues

- The major issues to be considered for wireless internet are the following:
  - Address mobility
  - Inefficiency of transport layer protocols
  - Inefficiency of application layer protocols

Address Mobility

- The network layer protocol used in the internet is IP was designed for wired networks with fixed nodes
- IP employs a hierarchical addressing with a globally unique 32-bit address: network id + host id
- The addressing scheme was used to reduce the routing table size in the core routers of the internet
- This addressing scheme may not work directly in the wireless Internet
- Mobile IP is a solution for the mobility problem

Address Mobility

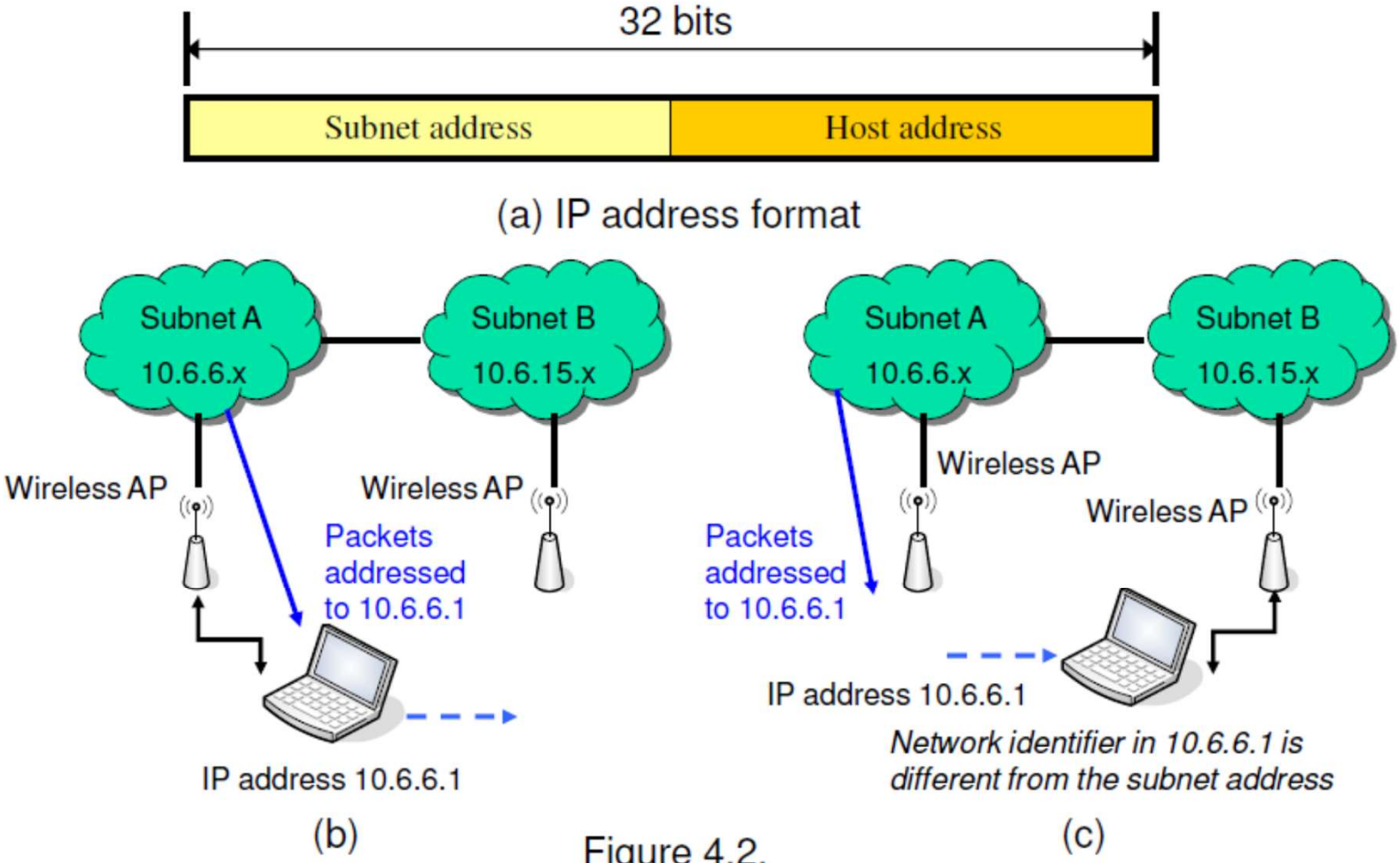


Figure 4.2.

Inefficiency of Transport Layer Protocols (TCPs)

- TCP is very important in the Internet:
  - maintaining end-to-end connections
  - reliable end-to-end delivery of data packets
  - flow control and congestion control
- Congestion control will reduce the size of the congestion window with every successive packet loss
- Link error or collision may lead to very low throughput in wireless network
- Indirect TCP, Snoop TCP and Mobile TCP is the solution.
- Wireless application protocol (WAP) is used to solve the inefficiency of wireless applications

Inefficiency of Application Layer Protocols

- HTTP, TELNET, simple mail transfer protocol (SMTP), and several markup languages such as HTML were designed and optimized for wired networks.
- Not very efficient when used with wireless links.
- HTTP is a stateless protocol opens new TCP connection with every transaction and has high overhead due to character encoding, also redundant information carried in the HTTP requests.
- Not suitable for wireless bandwidth constrained environment and hand held devices.
- Wireless application protocol (WAP) and optimizations over traditional HTTP are some of the solutions for the application layer issues.

Mobile IP

- Some possible solutions are-
  - Change the IP address when the host moves from one subnet to another (Lead to breaking and reestablishment of TCP connection)
  - Use the same IP address and add special routing entries for tracking the current location of the user.

- Solution should enumerate some issues
  - Compatibility: compatible to wired Internet
  - Scalability
  - Transparency

Some Terminologies in Mobile IP

- Mobile Agent (MN):mobile terminal system (end user) or a mobile router.
- Correspondent node (CN): At the other end of the network is the system with which MN communicates may be fixed or mobile. Here it is a fixed node
- Foreign agent (FA): The node or router to which the MN is connected, which currently facilitating to MN, is known as the foreign agent (FA).
- Home Agent (HA):The subnet to which the MN's IP address belongs is the home network, and the router or node under whose domain this IP address lies is the home agent
- Care of Address (COA)

Mobile IP

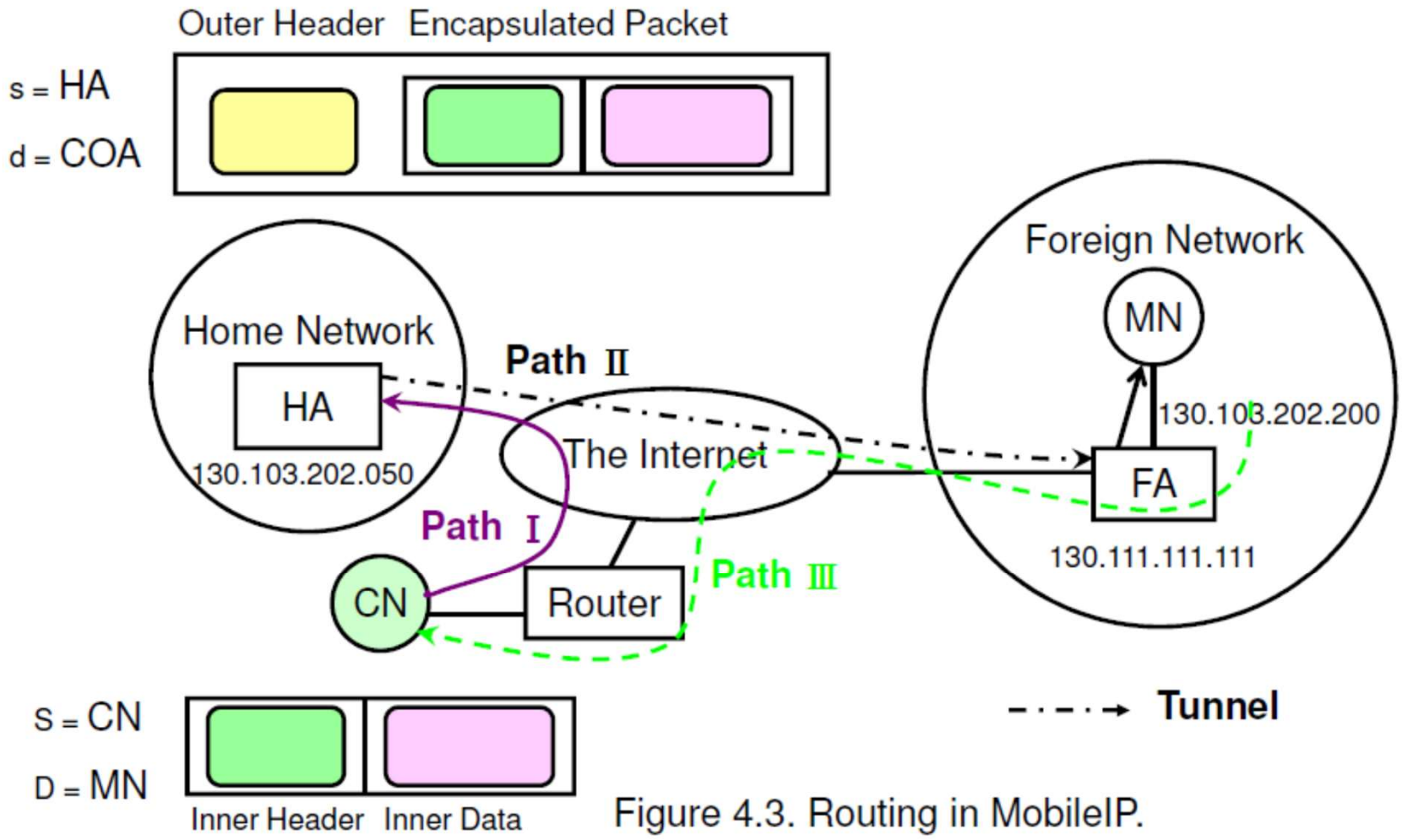


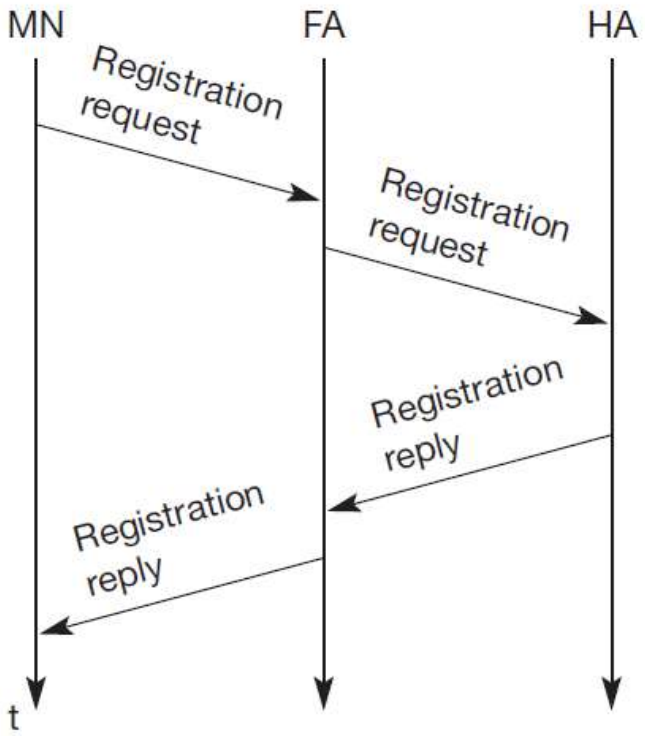
Figure 4.3. Routing in MobileIP.

MobileIP Protocol

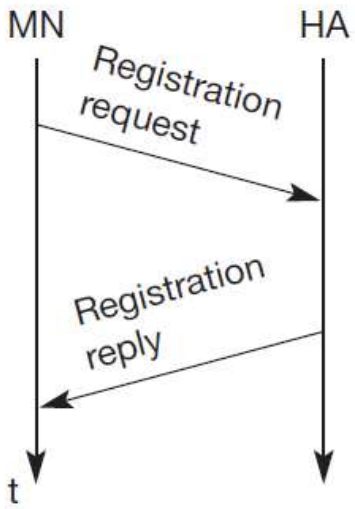
- The essence of mobileIP scheme is the use of old IP with few additional mechanisms, to provide mobility support. MS is assigned a Care of Address (COA) when MN is in the range of a foreign agent (FA)
- COA: Care of Address can be of two types
  - Foreign agent-based COA: address of current FA
    - The FA decapsulates the packet and forwards it to MN
  - Co-located COA: another address of MN
    - MN decapsulates the packet

Registration in Home Network

- The purpose is to send current location to HA
- Two ways to register



Foreign Agent Based COA



Colocated COA

Reverse Tunneling

- Possible problems for sending packet from MN to CN following path III
  - – Ingress filtering: some routers may filter the packets going out the network if the source IP is not the subnet's IP . MN packets may get filtered in foreign network if MN uses its Home IP
  - – Firewalls: filter and drop packets that originate from outside but have a source address belongs to the local network
  - - Multicast is another problem, the foreign network not necessarily has the multicast supposrt
  - – Time to live (TTL)
- Solution: the routing of packet from MN to CN via HA (reverse tunneling)
- The MN encapsulate reply using COA as source and HA address as destination. i.e. MN reply to HA and HA to CN, this is called triangular routing.

Simultaneous Binding and Route Optimization

- Simultaneous binding: HA allows an MN to register more than one COA at the same time
  - To improve the reliability of data transmission
- Route Optimization: (CN to MN bypassing HA)

- CN assumed to be mobility aware, and able to deencapsulate the packet from MN

  – **Binding cache:** CN can keep the mapping of MN's IP and COA in a cache

  – **Binding request and binding update**: find the binding from HA by using a binding request

  – **Binding warning (handoff case):** old FA sends a binding warning to HA, which in turn to informs the CN to use a new binding

TCP IN WIRELESS DOMAIN

Introduction

- **Issues with Wireless Domain**

  - High error rates and low bandwidth

- **Traditional TCP guarantees in-order & reliable delivery in wired network**

- **TCP needs to be modified for wireless domain**

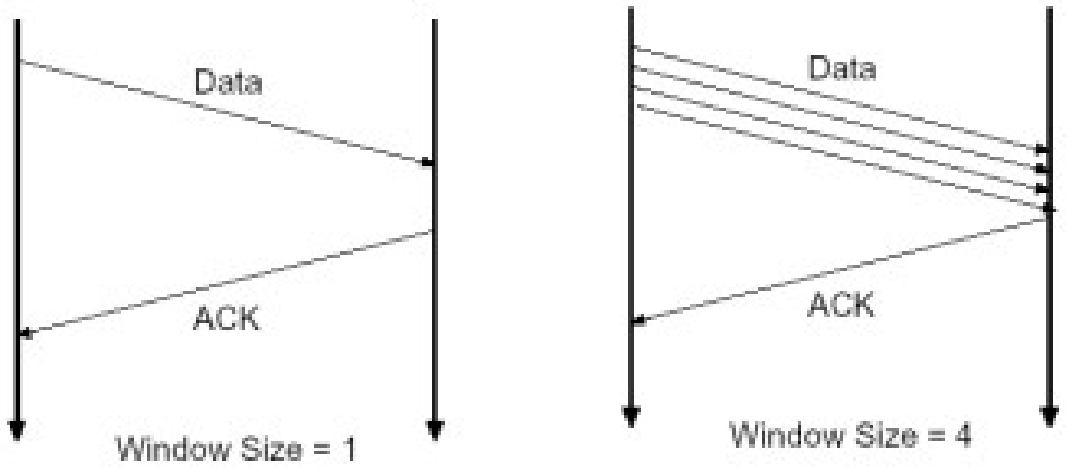
Traditional TCP

- Provides Connection-oriented
  - two applications must establish TCP connection before they can exchange data
- Full duplex protocol
- Includes Flow-control mechanism
  - allow receiver to limit how much data the sender can transmit
- Implements Congestion-control mechanism
- Divides data stream into smaller segments
  - Segment sequence number is used to provide in-order packet delivery and data loss detection

Traditional TCP

Sliding Window (1)

- TCP uses "Window Size" for data transmission.
  - Window Size:
    - The number of data packet which can be sent without waiting for ACKs



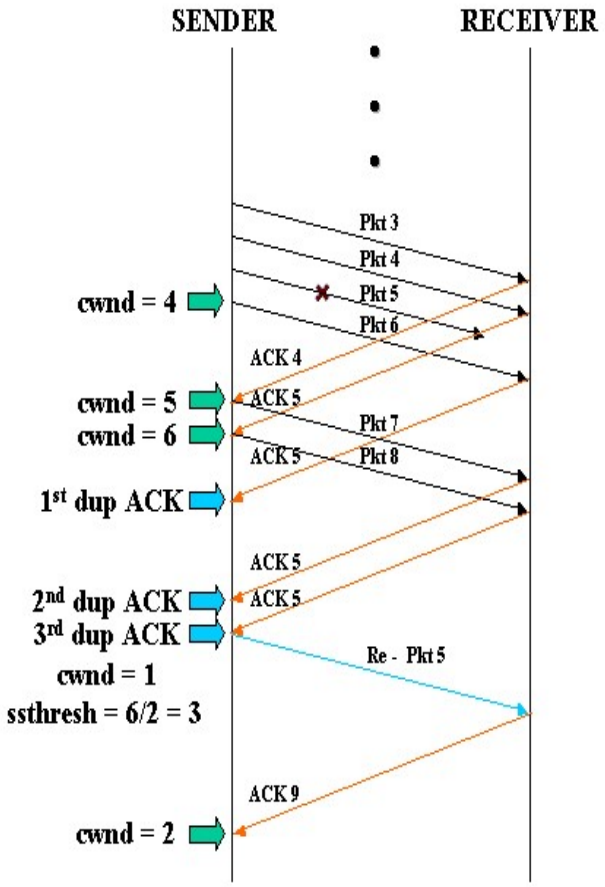
Traditional TCP

Congestion Control Mechanism

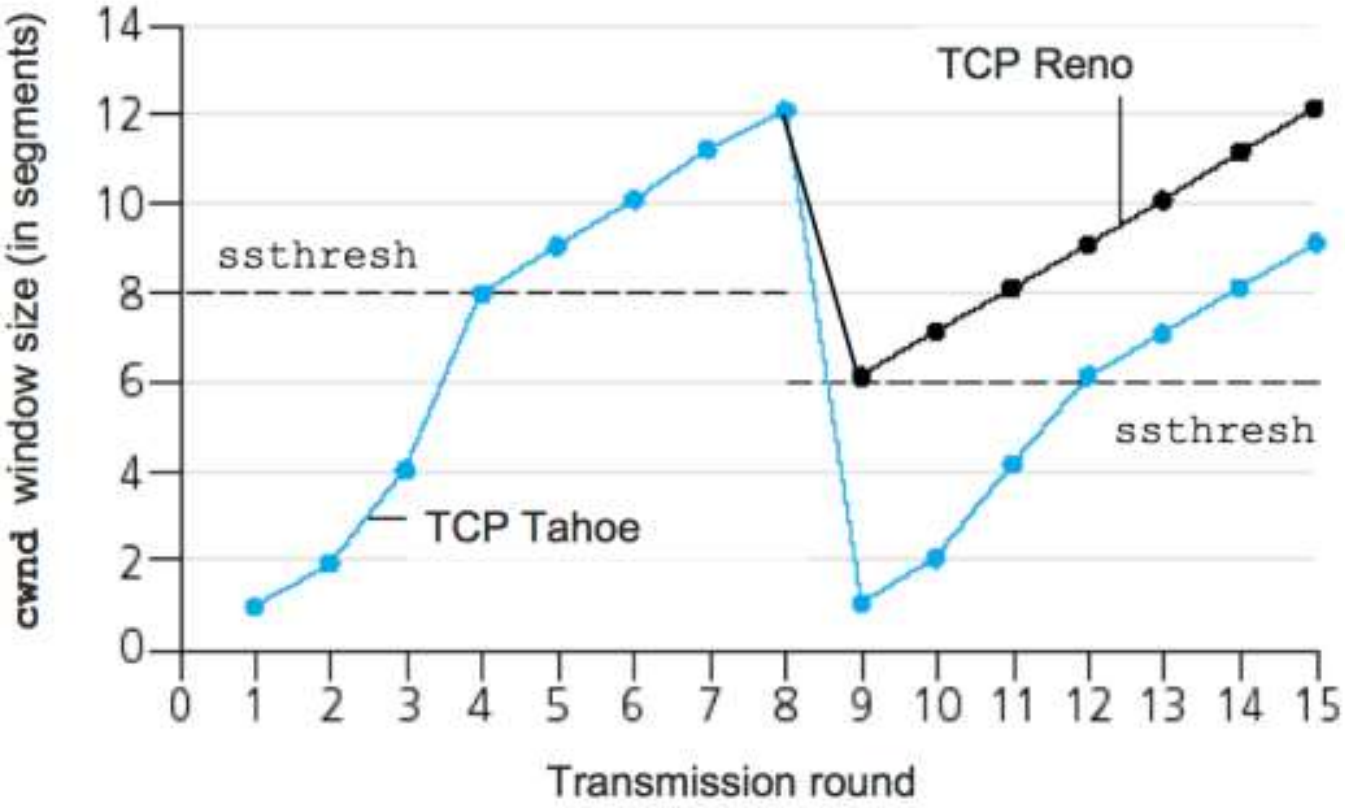
- Initial Window size: Max segment size

- Window get doubled for each successful transmission

-TCP interpret Timeout as congestion
-> initialize Slow Start Threshold as half of current window and reset window as one Max segment size



Traditional TCP



TCP Over Wireless

- TCP Congestion mechanism causes problem in wireless domain
  - Wireless has high packet loss and variable latency, which cause Slow Start and retransmission of lost packets

- Several alternatives are suggested.

  - Let Link Layer correct all errors.
    - FEC (Forward Error Correction): redundancy is encoded into the message.
    - Redundancy is introduced only if error possibility is found.

Implication on mobility

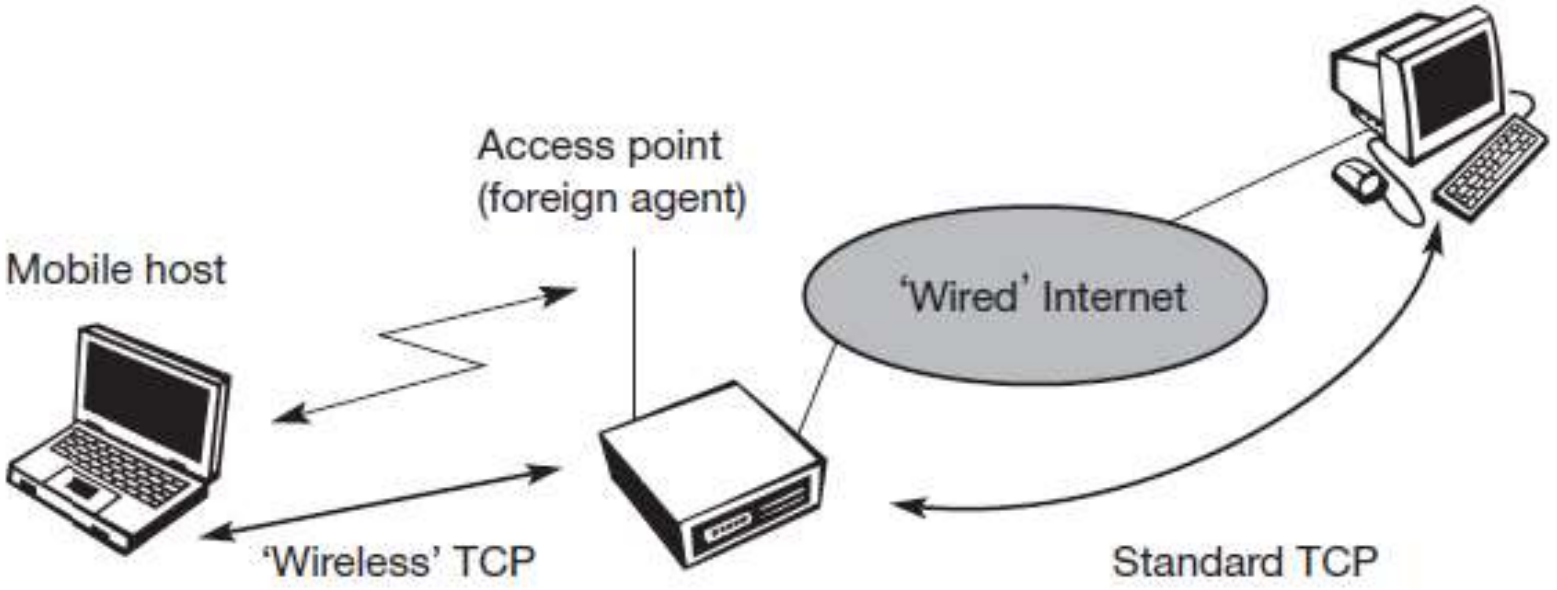
- From a missing acknowledgement, TCP concludes a congestion situation. While this may also happen in networks with mobile and wireless end-systems, it is not the main reason for packet loss.
- Handover: For example, when using mobile IP, there could still be some packets in transit to the old foreign agent while the mobile node moves to the new foreign agent.
- The TCP mechanism detecting missing acknowledgements via time-outs and concluding packet loss due to congestion cannot distinguish between the different causes. This is a fundamental design problem in TCP.

Classical TCP Improvements

Indirect TCP (I-TCP)

- Considers mainly two problems
- One is that TCP performs poorly together with wireless links; the other is that TCP within the fixed network cannot be changed.
- I-TCP segments a TCP connection into a fixed part and a wireless part
- Standard TCP is used between the fixed computer and the access point.
- Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy. This means that the access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host.
- Between the access point and the mobile host, a special TCP, adapted to wireless links, is used.
- The foreign agent controls the mobility of the mobile host anyway and can also hand over the connection to the next foreign agent when the mobile host moves on.

Indirect TCP (I-TCP)



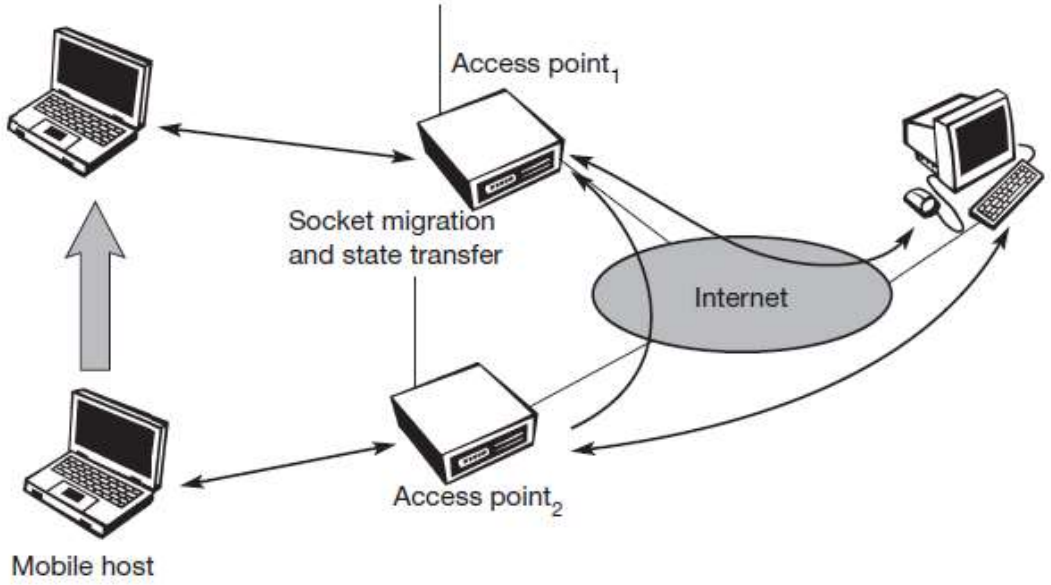
Indirect TCP (I-TCP)

- I-TCP working process
- When a correspondent Node (CN) sends packets to MN then access point (AP), behaving as MN for CN (as proxy of MN) transmit the acknowledgment to CN for all successfully received packets.
- Then AP transmit the packets to MN using an extended version of TCP for warless network.
- Here the loss of packet is high, thus AP retains the packets in buffers till they are not successfully received by MN.
- MN acknowledge to AP alone

Indirect TCP (I-TCP)

Handover Handling

- After the handover, the old proxy must forward buffered data to the new proxy because it has already acknowledged the data.
- Besides buffer content, the sockets of the proxy, too, must migrate to the new foreign agent located in the access point.



Indirect TCP (I-TCP)

- **Advantages**

- I-TCP does not require any changes in the TCP protocol as used by the hosts in the fixed network or other hosts in a wireless network that do not use this optimization
- Due to the strict partitioning into two connections, transmission errors on the wireless link, i.e., lost packets, cannot propagate into the fixed network.
- It is always dangerous to introduce new mechanisms into a huge network such as the internet without knowing exactly how they will behave. However, new mechanisms are needed to improve TCP performance (e.g., disabling slow start under certain circumstances), but with I-TCP only between the mobile host and the foreign agent, the different solutions can be tested or used at the same time
- Partitioning into two connections also allows the use of a different transport layer protocol between the foreign agent and the mobile host or the use of compressed headers etc.

Indirect TCP (I-TCP)

- **Disadvantages**

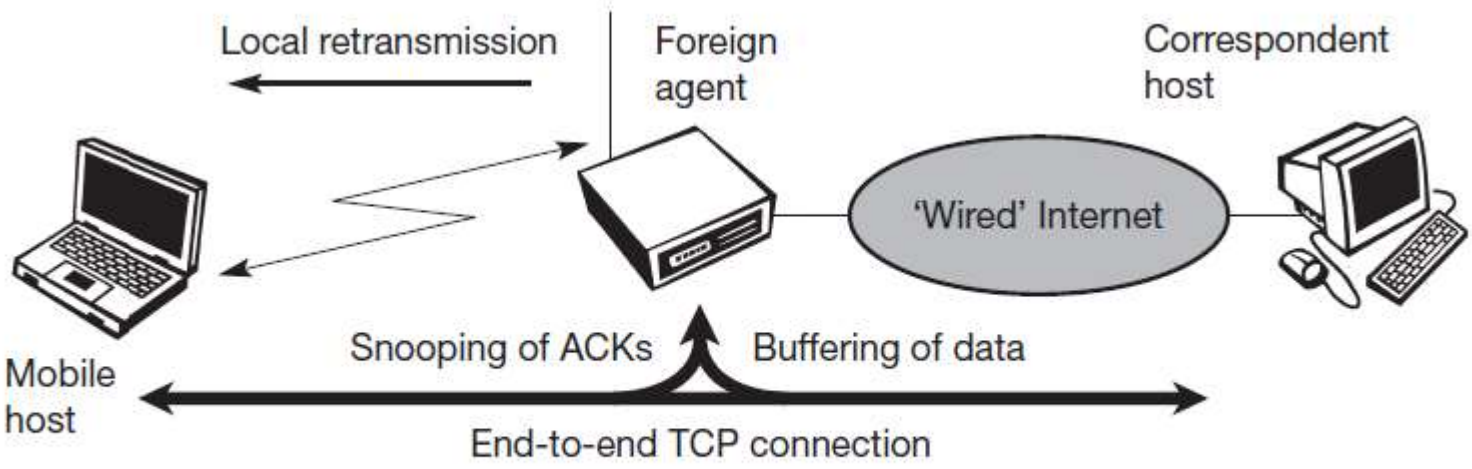
- The loss of the end-to-end semantics of TCP might cause problems if the foreign agent partitioning the TCP connection crashes.
- The correspondent node does not know anything about the partitioning, so a crashing access node may also crash applications running on the correspondent node assuming reliable end-to-end delivery.
- In practical use, increased handover latency may be much more problematic. Too much of buffered data to migrate and handling of new packets during migration can be a problem.
- The access point must be a trusted entity because the TCP connections end at this point.

Snooping TCP

- One of the drawbacks of I-TCP is the loss of original end-to-end TCP semantics.
- Snoop-TCP works completely transparently and leaves the TCP end-to-end connection intact.
- Buffers data close to the mobile host to perform fast local retransmission in case of packet loss. Ex- Buffered at FA.
- Foreign agent buffers all packets with **destination mobile host** and additionally 'snoops' the packet flow in both directions to recognize acknowledgements.
- If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost.
- Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet.
- Then, FA retransmit lost packet from buffer with very shorter acknowledgement time
- To remain transparent, the foreign agent must not acknowledge data to the correspondent host.
- The foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions.
- If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission and if FA now received duplicate packets already sent to MH now discarded

Snoop TCP

- Data transfer from the mobile host with **destination correspondent host** works as follows.
- The foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP.
- As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host. The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the correspondent host by TCP.



Snoop TCP

- **Advantages**

- The end-to-end TCP semantic is preserved. No matter at what time the foreign agent crashes neither the correspondent host nor the mobile host have an inconsistent view of the TCP connection as is possible with I-TCP.
- The correspondent host does not need to be changed; most of the enhancements are in the foreign agent.
- It does not need a handover of state as soon as the mobile host moves to another foreign agent.
- It does not matter if the next foreign agent uses the enhancement or not. If not, the approach automatically falls back to the standard solution.

- **Disadvantages**

- Snooping TCP does not isolate the behaviour of the wireless link as well as ITCP. Assume, for example, that it takes some time until the foreign agent can successfully retransmit a packet from its buffer due to problems on the wireless link.
- Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host. This approach is no longer transparent for arbitrary mobile hosts.
- All efforts for snooping and buffering data may be useless if certain encryption schemes are applied end-to-end between the correspondent host and mobile host.

M-TCP

- Dropping packets due to a handover or higher bit error rates is not the only phenomenon of wireless links and mobility – the occurrence of lengthy and/or frequent disconnections is another problem.
- In case of disconnection, the standard TCP will iteratively increase its acknowledgement waiting time for a certain period and will think that there is a congestion thus go in slow start.
- In I-TCP lots of data will be buffered at FA that required too much storage and retransmission also in Snoop TCP there will be no ACK to snoop so no help of disconnection.
- The **M-TCP (mobile TCP)** approach has the same goals as I-TCP and snooping TCP: to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems. Additionally handles long handovers
- M-TCP splits the TCP connection into two parts as I-TCP does. An unmodified TCP is used on the standard host-**supervisory host (SH)** connection, while an optimized TCP is used on the SH-MH connection. The supervisory host is responsible for exchanging data between both parts similar to the proxy in ITCP

M-TCP

- The M-TCP approach assumes a relatively low bit error rate on the wireless link. Therefore, it does not perform caching/ retransmission of data via the SH. If a packet is lost on the wireless link, it has to be retransmitted by the original sender. This maintains the TCP end-to-end semantics.
- The SH monitors all packets sent to the MH and ACKs returned from the MH. If the SH does not receive an ACK for some time, it assumes that the MH is disconnected.
- It then chokes the sender by setting the sender's window size to 0. Setting the window size to 0 forces the sender to go into **persistent mode**
- As soon as the SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value.
- The wireless side uses an adapted TCP that can recover from packet loss much faster. This modified TCP does not use slow start, thus, M-TCP needs a **bandwidth manager** to implement fair sharing over the wireless link.

M-TCP

Advantages

- It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
- If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0.
- Since it does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

Disadvantages

- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption.
- A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager.

Fast retransmit/fast recovery

Handoff usually leads to packet loss during transit

TCP reacts with slow-start during handoff even when no congestion

Solution: Artificially force fast retransmit mode after handoff. Send duplicate ACK after handoff, instead of entering slow start.

Advantages

- Simple changes result in significant higher performance
- Requires minimal changes to existing TCP structure

Disadvantages

- Scheme doesn't consider fact of losses over wireless links

Transmission / Time-out freezing

- **There are many ideas we presented for short time interruption, error on the channel and long time handovers**.
- Sometime for longer handovers such as while a mobile node is passing through a cell which has not any capacity left or passing through a tunnel where there is no connectivity, etc.
- In such case the TCP try multiple attempts of transmission before disconnection and will move in slow start phase.
- Such situations can be handled in coordination of MAC layer because MAC layer can identify the problem of disconnection early before TCP timeout and can inform to CN and MN about this disconnection.
- Now TCP can freeze its window, and when connection resume, it can start from its current state.

Transmission / Time-out freezing

Advantages

•It offers a way to resume TCP connections even after longer interruptions of the connection.

•It is independent of any other TCP mechanism, such as ACK or sequence numbers so it can used with encrypted data.

Disadvantages

•Require changes in software at MN and CN

•All mechanism rely on the capability of MAC layer to detect future interruption

Selective Retransmission

- A very useful extension of TCP is the use of selective retransmission.
- TCP acknowledgements are cumulative
- If a single packet loss, the sender needs to transmit all following packets again (Go-back-n retransmission), which waste bandwidth.
- TCP can indirectly request a selective retransmission, and receiver can send acknowledgement of single packet.

Advantage

- Lower bandwidth requirement

Disadvantages

- More complex software is needed on receiver side, more buffer is needed for resequencing data and wait for gaps to be filled.

Transaction-Oriented TCP (T-TCP)

TCP connection setup and tear-down is huge overhead for a small amount of data, uses 3-way handshake

3 packets for a single transaction, 2 transactions per connection cycle

3 packets for setup + 1 for data + 3 packets for release = 7 packets minimum

To improve performance use T-TCP for small amount of data.

Integrate connection setup, tear-down, and data transfer combined into single transaction

Usually only 2 or 3 packets are needed

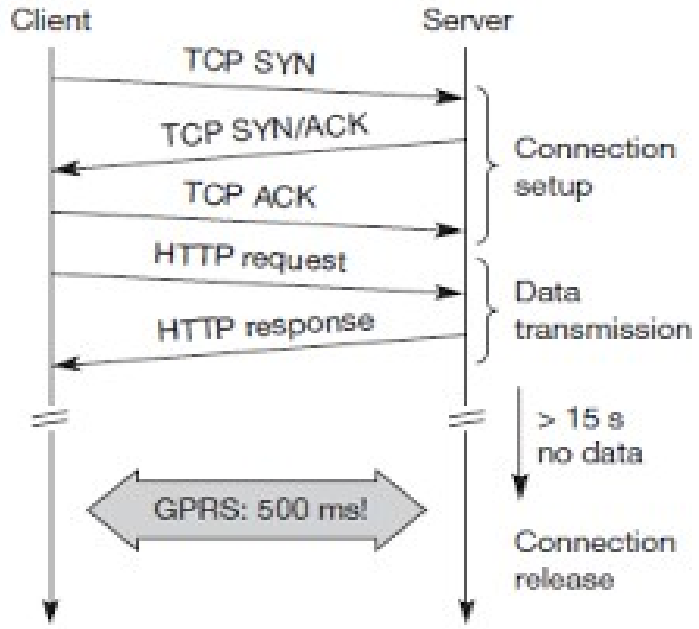
Advantage

Larger efficiency (low overhead)

Disadvantage

Changed TCP

Mobility not transparent, can't affect existing framework



Comparison

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover, security problems
Snooping TCP	Snoops data and acknowledgements, local retransmission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problems
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management, security problems
Fast retransmit/ fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnection	Independent of content, works for longer interruptions	Changes in TCP required, MAC dependent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space needed
Transaction-oriented TCP	Combines connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent, security problems

MAC Protocol for Ad hoc Wireless Networks

Aim of MAC:

- provide fair access to shared broadcast radio channel.

Issues to deal with:

- Bandwidth efficiency: – must be maximized.

The radio spectrum is limited, the bandwidth available for communication is also very limited. The MAC protocol must be designed in such a way that the scarce bandwidth is utilized in an efficient manner. The control overhead involved must be kept as minimal as possible.

Bandwidth efficiency=ratio of the bandwidth used/ Total Bandwidth

- Real-time traffic support: – should be provided.

- QoS support to data sessions in such networks is very difficult. Bandwidth reservation made at one point of time may become invalid once the node moves out of the region where the reservation was made.
- QoS support is essential for supporting time-critical traffic sessions such as in military communications.
- The MAC protocol for ad hoc wireless networks that are to be used in such real-time applications must have some kind of a resource reservation mechanism

- Synchronization: – sometimes needed, e.g. TDMA.

- Exchange of control packets may be required for achieving time synchronization among nodes. Very important for bandwidth (time slot) reservations by nodes.

- Shared broadcast medium: – collisions must be avoided/minimized.

- A node should get access to the shared medium only when its transmissions do not affect any ongoing session.
- Since multiple nodes may contend for the channel simultaneously, the possibility of packet collisions is quite high in wireless networks.
- A MAC protocol should grant channel access to nodes in such a manner that collisions are minimized

- Lack of central coordination: – fully distributed MAC design.

- Nodes must be scheduled in a distributed fashion for gaining access to the channel.
- The MAC protocol must make sure that the additional overhead, in terms of bandwidth consumption, incurred due to this control information exchange is not very high.

MAC Protocol for Ad hoc Wireless Networks

- Mobility of nodes: – loss of connectivity; – network partitioning; – bit errors.
- The protocol design must take this mobility factor into consideration so that the performance of the system is not significantly affected due to node mobility.

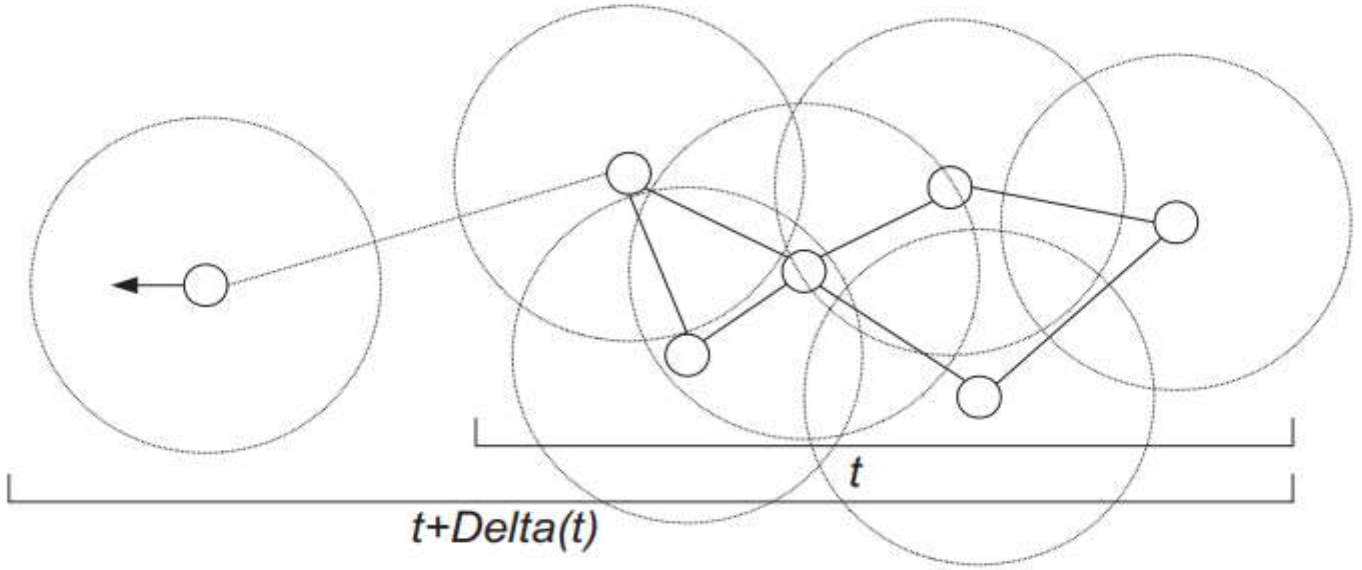


Figure 3: Network partitioning is one of the biggest problem to deal with at MAC sublayer.

MAC Protocol for Ad hoc Wireless Networks

- Hidden terminal problem: – collisions → inefficient bandwidth utilization.

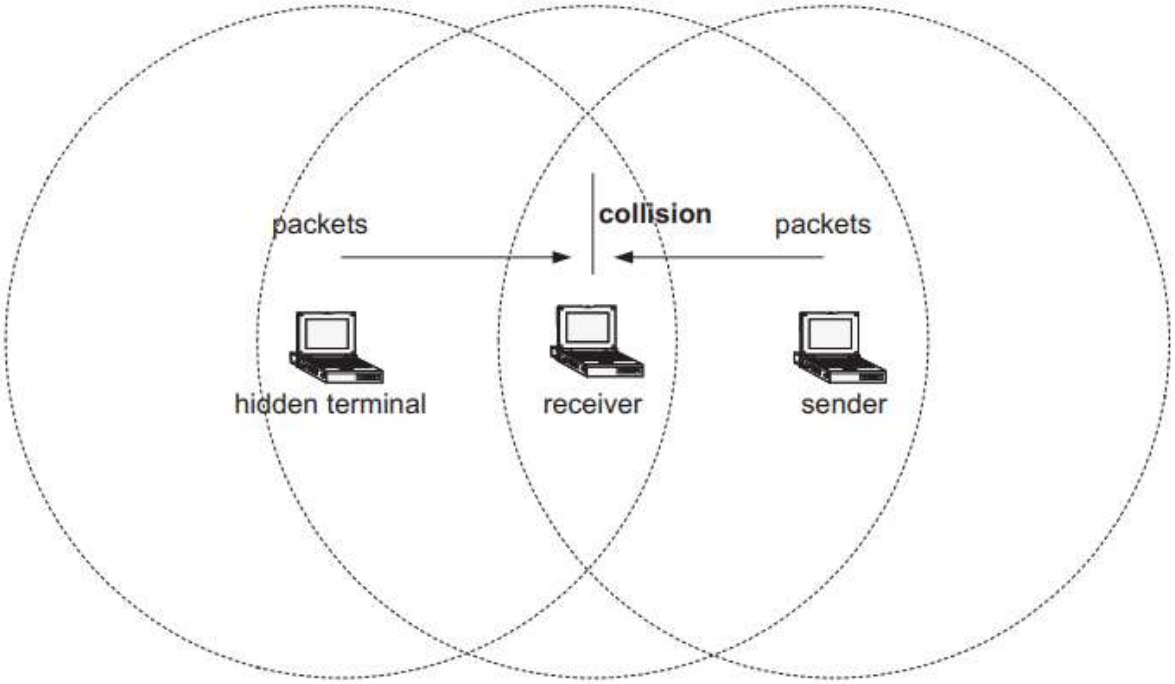


Figure 1: Illustration of the hidden terminal problems.

MAC Protocol for Ad hoc Wireless Networks

- Exposed terminal problem: – inability to transmit → inefficient bandwidth utilization.

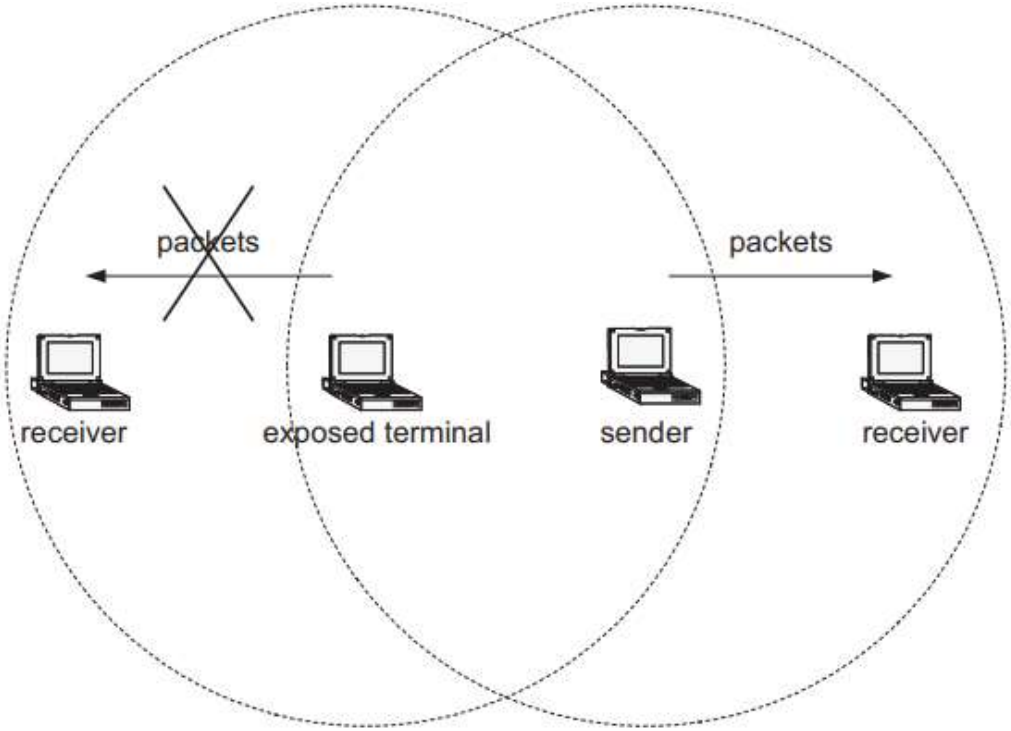


Figure 2: Illustration of the exposed terminal problem.

MAC Protocol for Ad hoc Wireless Networks

Design goals-What we want from MAC protocol?

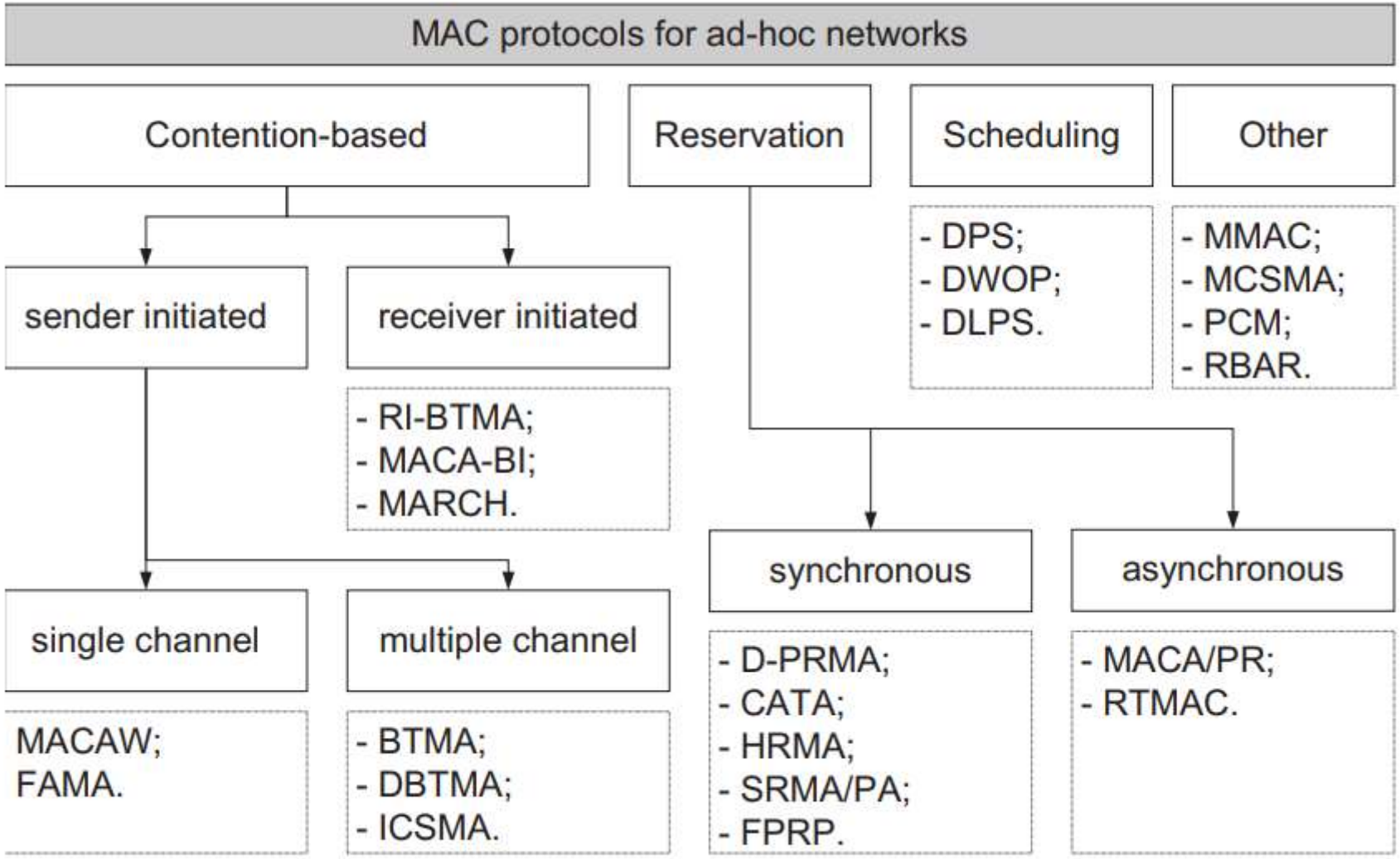
- allow fair access to the shared radio medium;
- operation of the protocol should be distributed;
- should support real-time traffic;
- the access delay must be minimized;
- available bandwidth must be utilized efficiently;
- fair bandwidth allocation to competing nodes;
- control overhead must be minimized;
- the effects of hidden/exposed terminals must be minimized;
- must be scalable;
- should minimize power consumption;
- should provide synchronization between nodes.

MAC Protocol for Ad hoc Wireless Networks

Classification of MAC protocols

- Contention-based protocols without reservation/scheduling:
  - no reservation of the bandwidth is made;
  - guarantees are not possible.
- Contention-based protocols with reservation mechanisms:
  - bandwidth for transmission is reserved in advance.
  - guarantees are possible.
- Contention-based protocols with scheduling mechanisms:
  - distributed scheduling between nodes is used.
  - guarantees are possible.
- Protocols that do not fall to any of these categories:
  - implement several features of different protocol groups or
  - use completely different approach

MAC Protocol for Ad hoc Wireless Networks



MACA

- Contention based protocols w/o reservation/scheduling
  - The basic idea: contention for the resource, winning node transmits.
- **Multiple access collision avoidance (MACA) protocol (Extension of CSMA):**
- **CSMA operates as follows:**
  - the sender sense the channel for the carrier signal;
  - if the carrier is present it retries to sense the channel after some time (exp. back-off);
  - if not, the sender transmits a packet.
- The following shortcomings are inherent to CSMA/CA:
  - hidden terminal problem leading to frequent collisions;
  - exposed terminal problem leading to worse bandwidth utilization.
- To avoid it:
  - virtual carrier sensing;
  - RTS-CTS handshake before transmission.

MACA

- MACA does not make use of carrier-sensing for channel access.
- Two additional signaling packets: the request-to-send (RTS) packet and the clear-to-send (CTS) packet are used.
- When a node has data to transmit, it first transmits an RTS packet.
- The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.

MACA

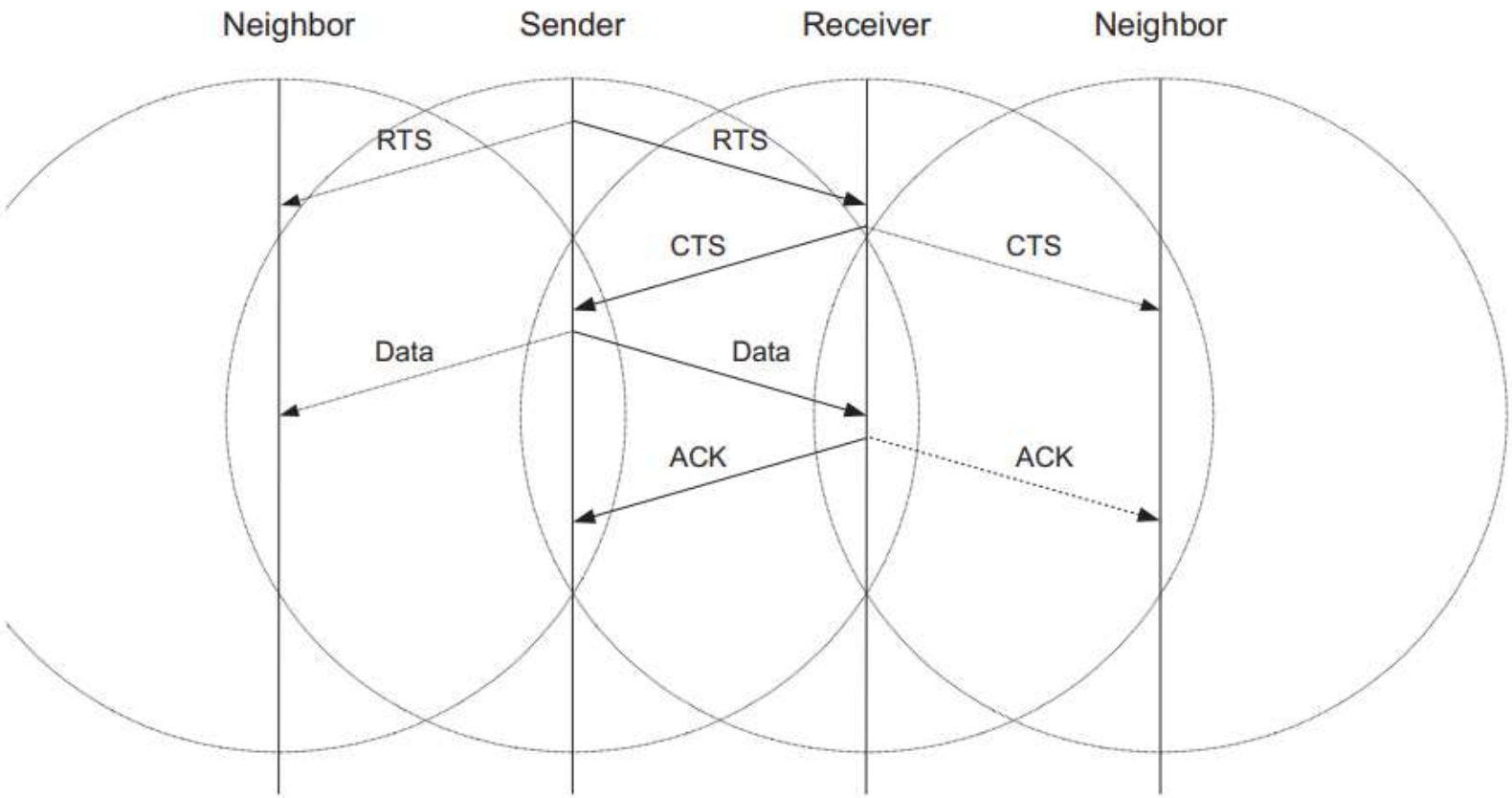


Figure 4: Packet transmission in MACA.

MACA

- If the transmission fails in MACA:
- The node uses the binary exponential back-off (BEB) algorithm
- In the binary exponential backoff mechanism, each time a collision is detected, the node doubles its maximum back-off window.
  - contention window: CW×2;
  - retransmission of RTS.

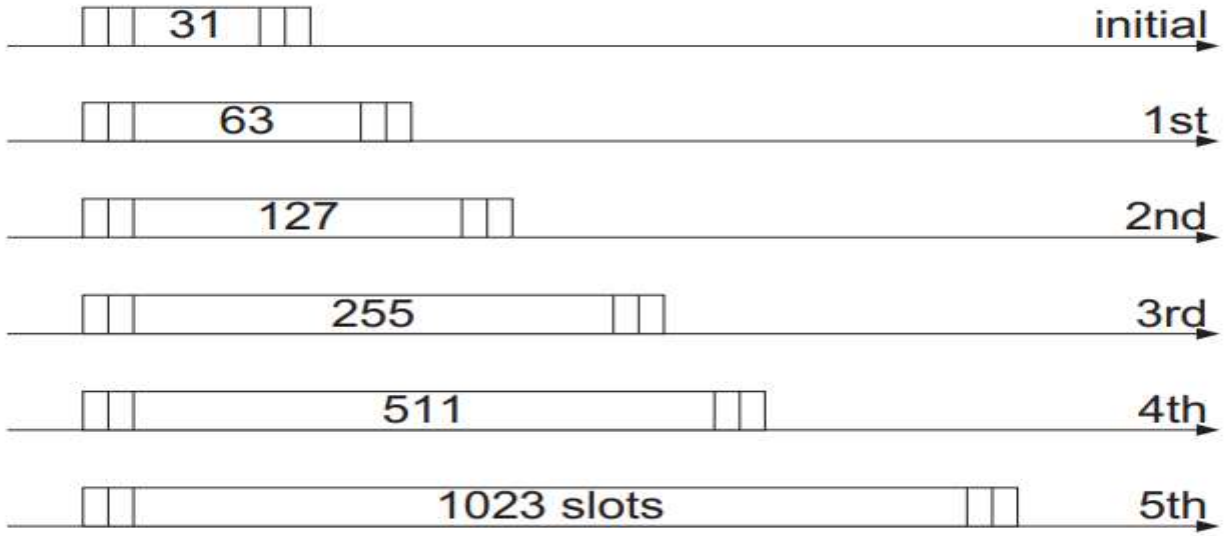


Figure 6: Evolution of the contention window with increasing of transmission attempts.

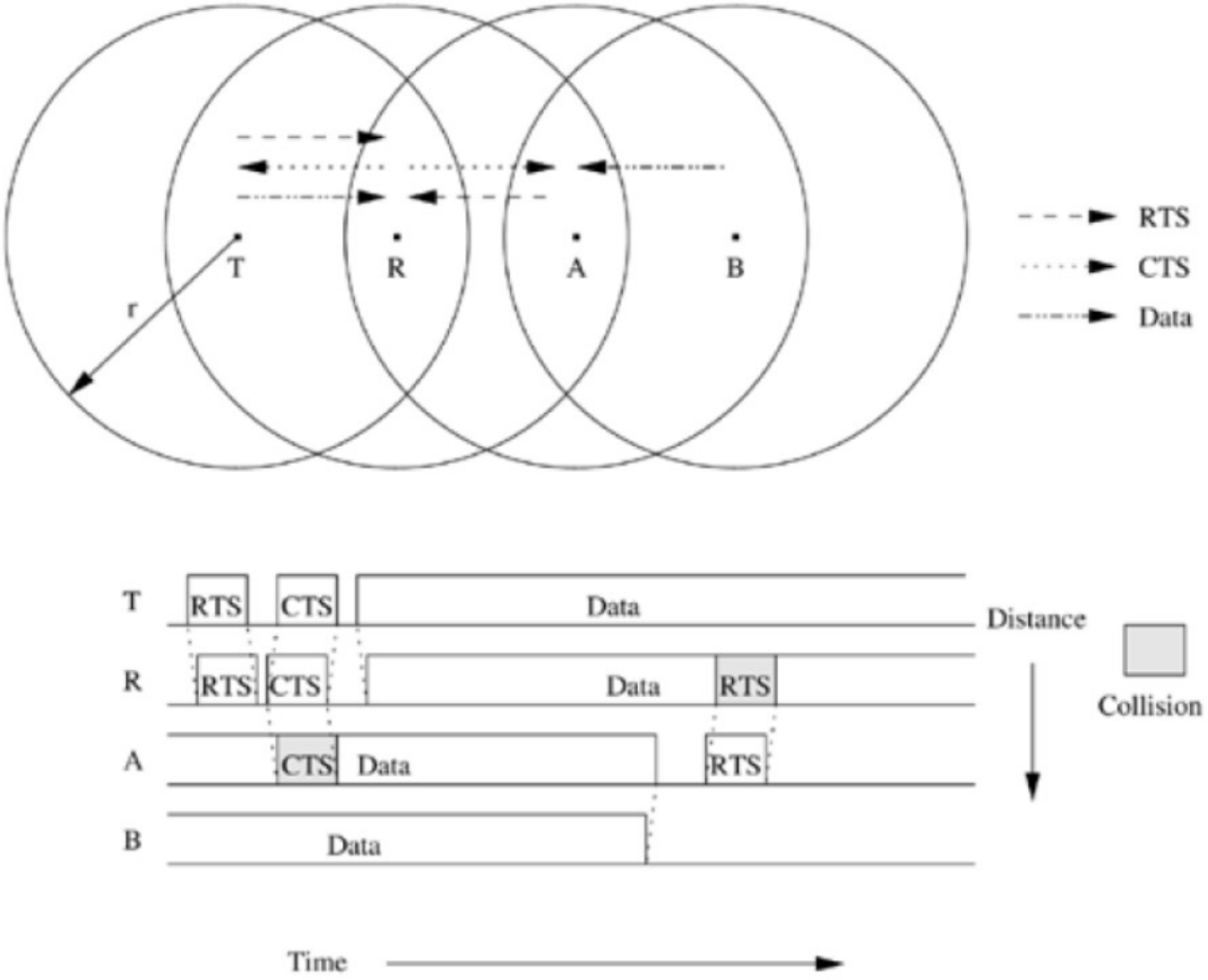
Solving Hidden and Exposed Terminal

- Both the RTS and the CTS packets carry the expected duration of the data packet transmission.
- Neighbor nodes near the sender that hear the RTS packet do not transmit for a long enough period of time so that the sender could receive the CTS packet.
- A node near the receiver, upon hearing the CTS packet, defers its transmission till the receiver receives the data packet. **Thus, MACA overcomes the hidden node**
- Similarly, a node receiving an RTS defers only for a short period of time till the sender could receive the CTS. If no CTS is heard by the node during its waiting period, it is free to transmit packets once the waiting interval is over.
- Thus, a node that hears only the RTS packet is free to transmit simultaneously when the sender of the RTS is transmitting data packets. Hence,
- Thus, the **exposed terminal problem is also overcome in MACA.**
- But MACA still has certain problems, which was why MACAW, described below, was proposed.

Hidden Terminal Problem with RTS-CTS

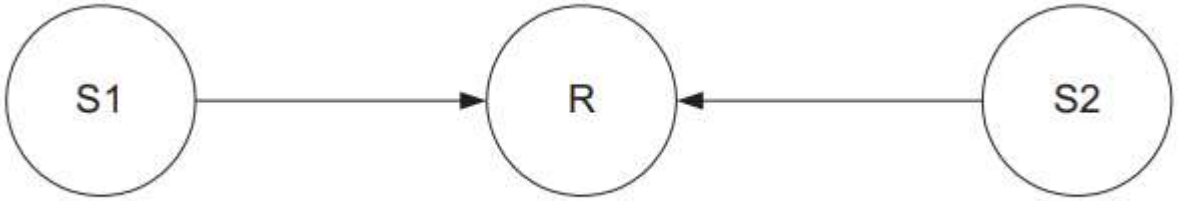
- The RTS-CTS control packet exchange cannot ensure collision-free data transmission that has no interference from hidden terminals.
- One very important assumption made is that every node in the capture area of the receiver (transmitter) receives the CTS (RTS) cleanly.
- Nodes that do not hear either of these clearly can disrupt the successful transmission of the Data or the ACK packet.

Hidden Terminal Problem with RTS-CTS



MACAW (MACA for Wireless)

- There are still some problems in MACA which are resolved by MACAW: an extension of MACA
- **Problem 1 of MACA: starvation of flows:**
  - •both S1 and S2 have the high volume of traffic, S1 seizes the channel first;
  - • packets transmitted by S2 get collided and it doubles CW (CW = 2CW);
  - • the probability that the node S2 seizes the channel is decreasing.



Starvation of the flow from S2.

Solution:

- • the packet header contains the field set to the current back-off value of the transmitting node;
- • a node receiving this packet copies this value to its back-off counter (fairness);

MACAW

- **Problem 2 of MACA: fast adjustment of CW:**
  - when a node successfully transmits a packet;
  - when a collisions is detected by a node.

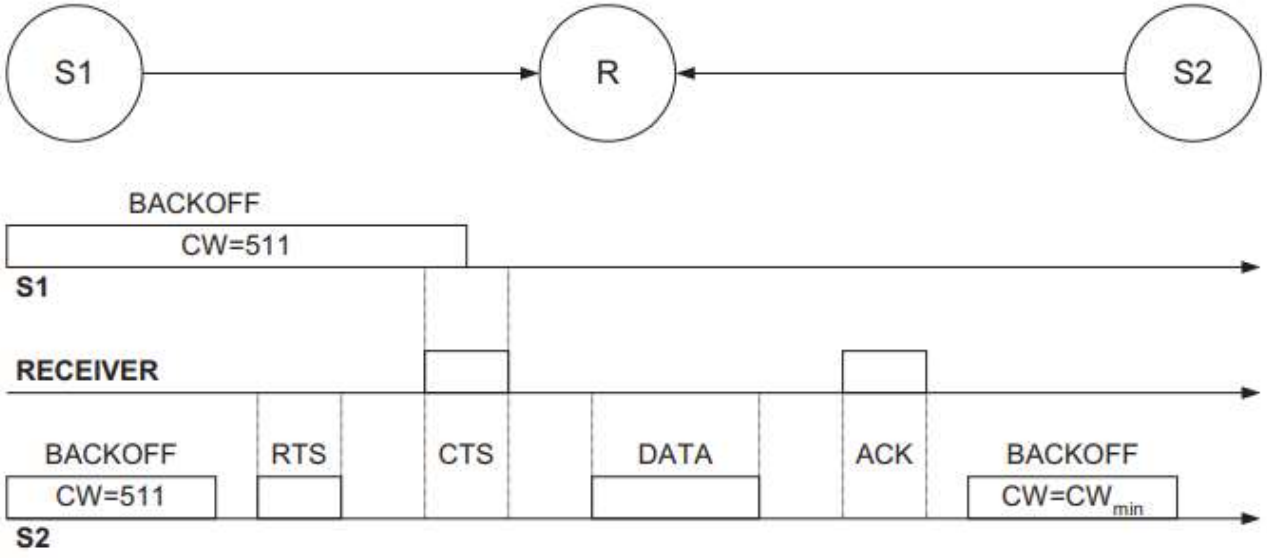


Figure 8: Rapid adjustments of the CW.

Solution: multiplicative increase when collision, linear decrease when success.

BEB in MACAW

- Multiplicative increase, linear decrease (MILD)
- MACAW sender:
  - CW0 = 2 and CWM = 64
  - Upon failed RTS/CTS

    CW =min[1.5CW, CWM]
  - Upon successful RTS/CTS but failed ACK, no change
  - Upon successful RTS/CTS/DATA/ACK

    CW=CW−1

- Another modification related to the back-off mechanism is that the MACAW implements per flow fairness as opposed to the per node fairness in MACA.
- This is done by maintaining multiple queues at every node, one each for each data stream, and running the backoff algorithm independently for each queue.
- A node that is ready to transmit packets first determines how long it needs to wait before it could transmit an RTS packet to each of the destination nodes.
- It then selects the packet for which the waiting time is minimal.

ACK in MACAW

- In MACA, the responsibility of recovering from transmission errors lies with the transport layer. As many TCP implementations have a minimum timeout period of about 0.5 sec, significant delay is involved while recovering from errors. Decreases the network throughput.
- But in MACAW, the error recovery responsibility is given to the data link layer (DLL).
- In MACAW, after successful reception of each data packet, the receiver node transmits an ACK packet.
- If the sender does not receive the ACK packet, it reschedules the same data packet for transmission.
- The sender would retry by transmitting an RTS for the same packet.
- But now the receiver, instead of sending back a CTS, sends an ACK for the packet received, and the sender moves on to transmit the next data packet.

MACAW

- **Problem 3 of MACA: an exposed node is free to transmit.**
  - node S2 hears RTS but not CTS (exposed node);
  - S2 initiates transfer to R2;
  - DATA from S1 and CTS from R2 may collide, CW unnecessary increases at S2.

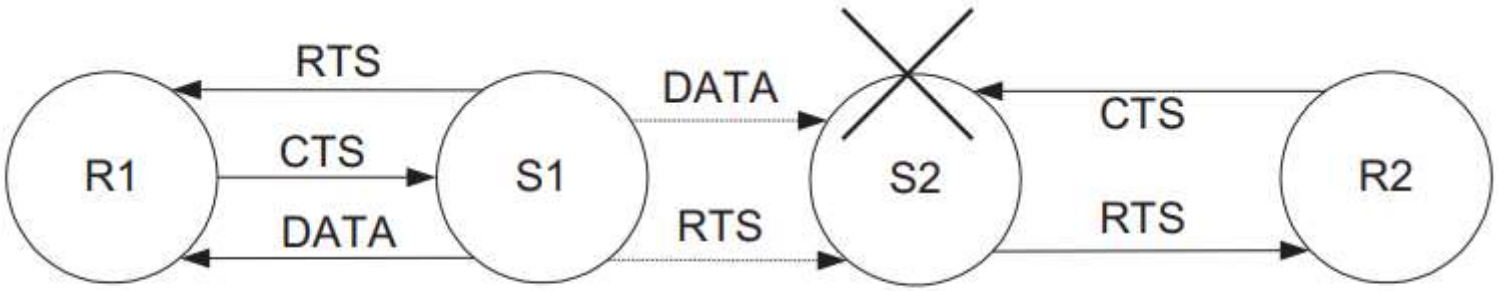


Figure 9: Problems with exposed node.

We conclude from this line of reasoning that S2 should defer transmission while S1 is transmitting data. Note that because S2 has only heard the RTS and not the CTS, station S2 cannot tell if the RTS-CTS exchange between S1 and R1 was a success and so does not know. So to confirm its successfulness a DS packet is used.

Solution: use of small data sending packet (DS) to update information.

MACAW

- **Problem 4 of MACA: neighbour receivers problem:**

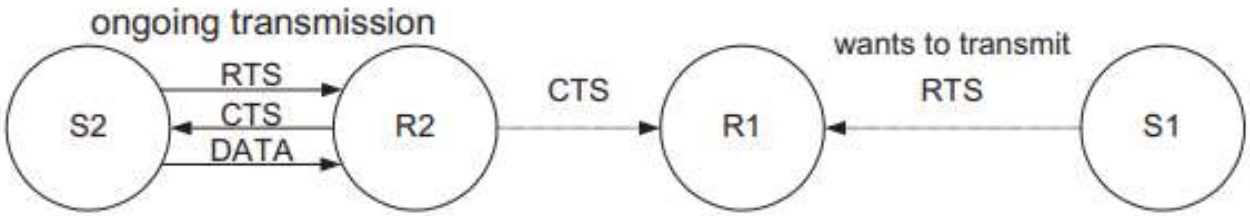


Figure 10: Illustration of the neighbor receivers problem.

- **Solution**: usage of request-for-request (RRTS) to send packets:
  - if R1 had received RTS (S1) and did not respond due to R2-S2 it backs off sends RRTS;
  - R2 hears RRTS waits for successive RTS-CTS between S1 and R1;
  - S1 hears the RRTS, transmits regular RTS and RTS-CTS-DATA-ACK takes place

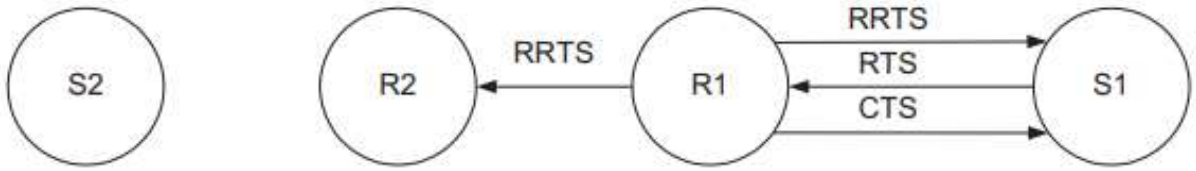


Figure 11: Solution of the neighbor receivers problem.

MACAW

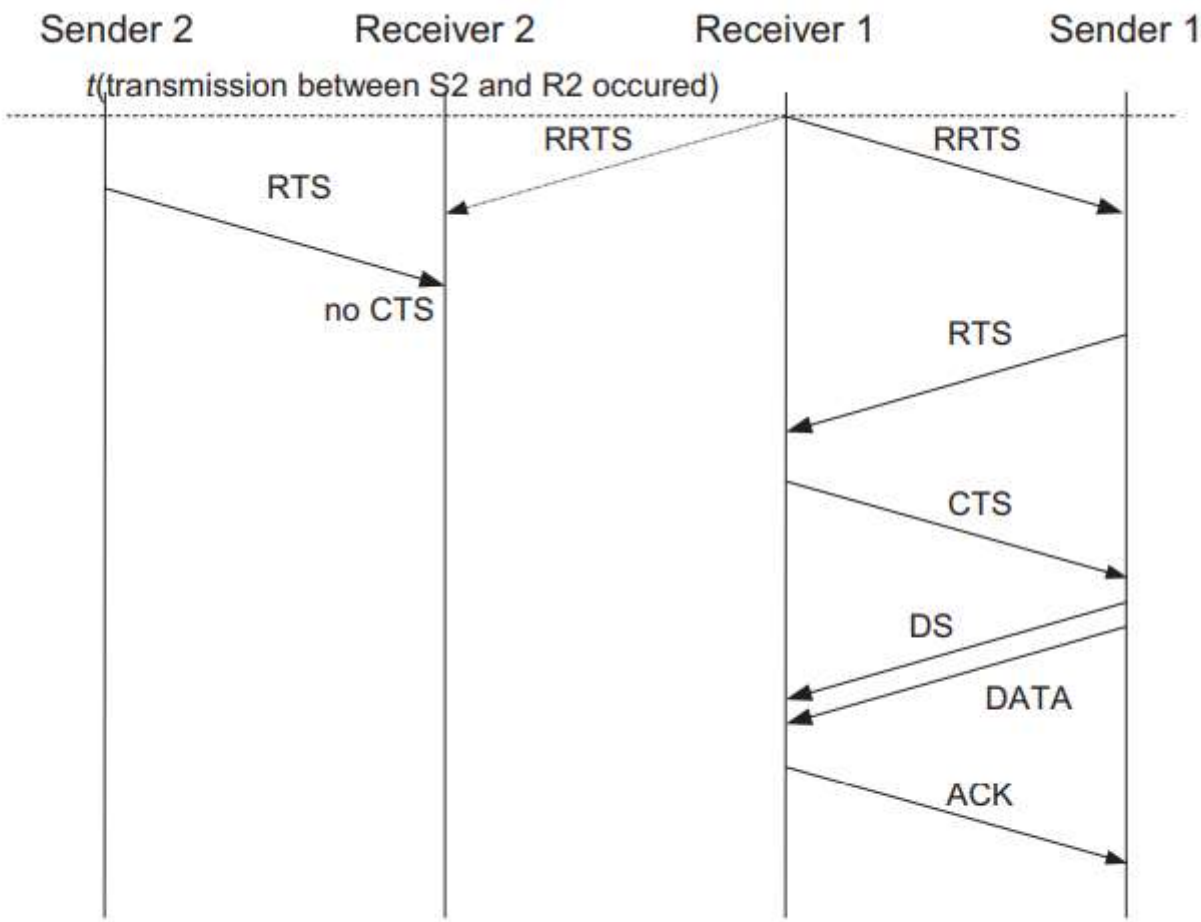


Figure 12: Packets exchange in neighbor receivers problem.

Routing in Ad hoc Wireless Networks

Introduction

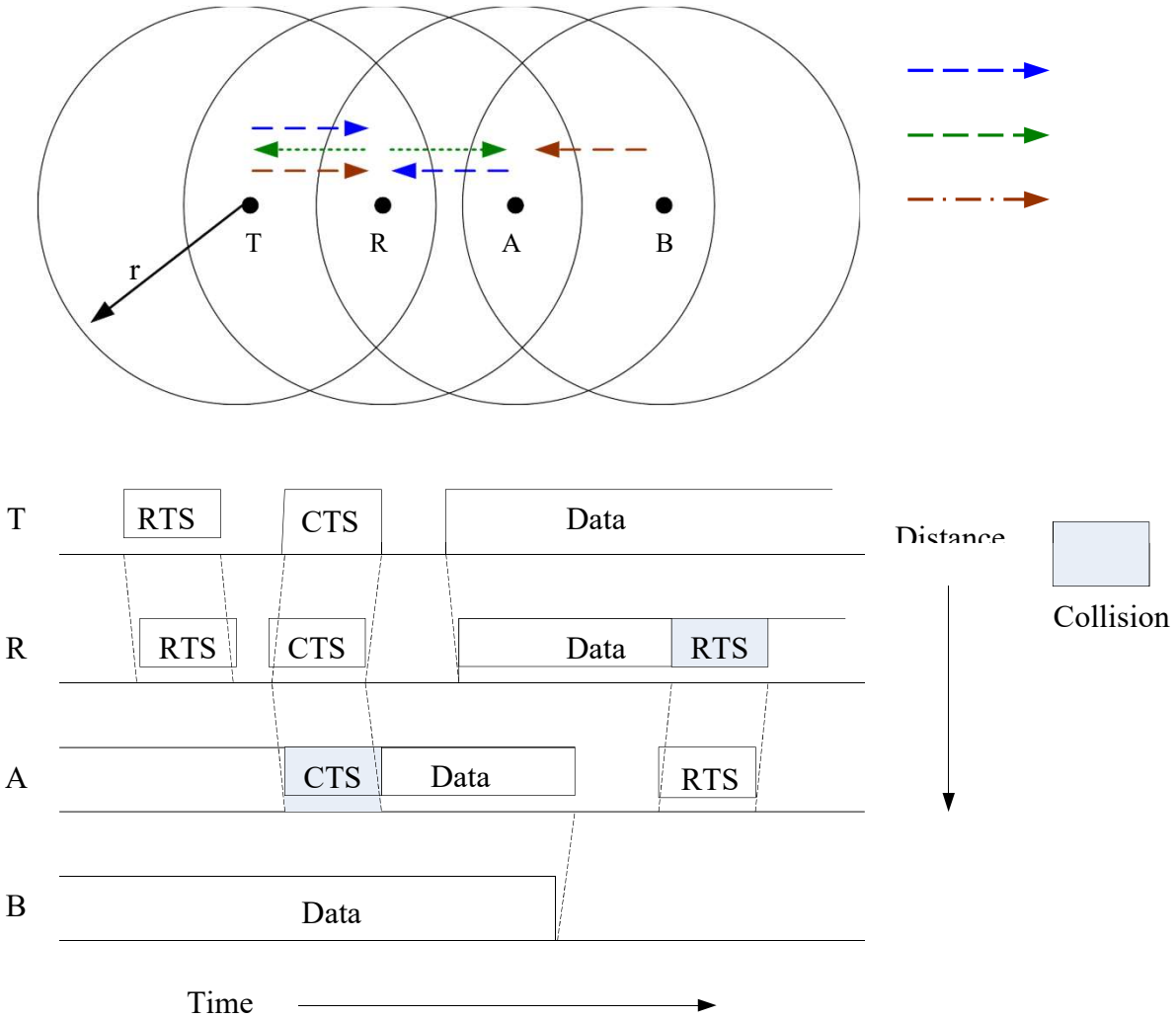
- Routing protocols used in wired networks cannot be directly applied to ad hoc wireless networks
  - Highly dynamic topology
  - No infrastructure for centralized administration
  - Bandwidth constrained
  - Energy constrained
- For the above reasons, we need to design new routing protocols for ad hoc networks

Issues in Designing a Routing Protocol

- Mobility:
  - Ad hoc is highly dynamic due to the movement of nodes
  - Node movement causes frequent path breaks
  - The path repair in wired network has slow convergence
- Bandwidth Constraint:
  - Wireless has less bandwidth due to the limited radio band: Less data rate and difficult to maintain topology information
  - Frequent change of topology causes more overhead of topology maintenance
  - Target: Bandwidth optimization and design topology update mechanism with less overhead

Issues in Designing a Routing Protocol

- Error-prone shared broadcast radio channel:
  - Wireless links have time varying characteristics in terms of link capacity and link-error probability
  - Target: Interact with MAC layer to find better-quality link
  - Hidden terminal problem causes packet collision
  - Target: Find routes through better quality links and find path with less congestion
- Hidden and exposed terminal problems
  - RTS-CTS control packet cannot ensure collision free, see Fig. 7.2
- Resource Constraints:
  - Limited battery life and limited processing power
  - Target: optimally manage these resources



Hidden terminal problem with RTS-CTS-Data-ACK scheme.

Characteristics of an Ideal Routing Protocol for Ad Hoc

- Fully distributed
- Adaptive to frequent topology changes
- Minimum connection setup time is desired
- Localized

– global maintenance involves a huge state propagation control overhead

- Loop free and free from stale routes
- Packet collision must seldom happen

Characteristics of an Ideal Routing Protocol for Ad Hoc (cont.)

- Converge to optimal route quickly
- Optimally use scarce resource

– Bandwidth, computing power, memory, and battery

- Remote parts of the network must not cause updates in the topology information maintained by this node
- Provide quality of service and support for time-sensitive traffic

Classifications of Routing Protocols

- Routing protocol can be broadly classified into four categories :
  - Routing information update mechanism
  - Use of temporal information for routing
  - Routing topology
  - Utilization of specific resource
- These classification is not mutually exclusive

Based on the Routing Information Update Mechanism

- Proactive or table-driven routing protocols
  - Maintain routing information in the routing table
  - Routing information is flooded in the whole network
  - Runs path-finding algorithm with the routing table
- Reactive or on-demand routing protocols
  - Obtain the necessary path while required
- Hybrid routing protocols
  - In the zone of given node : use table-driven
  - Out of the zone of given node : use on-demand

Based on the Use of Temporal Information for Routing

- Using past temporal information
  - Past status of the links or
  - the status of links at the time of routing to make routing decision
- Using future temporal information
  - Expected future status of the links to make decision
  - Node lifetime is also included
    - Ex: remaining battery charge, prediction of location, and link availability

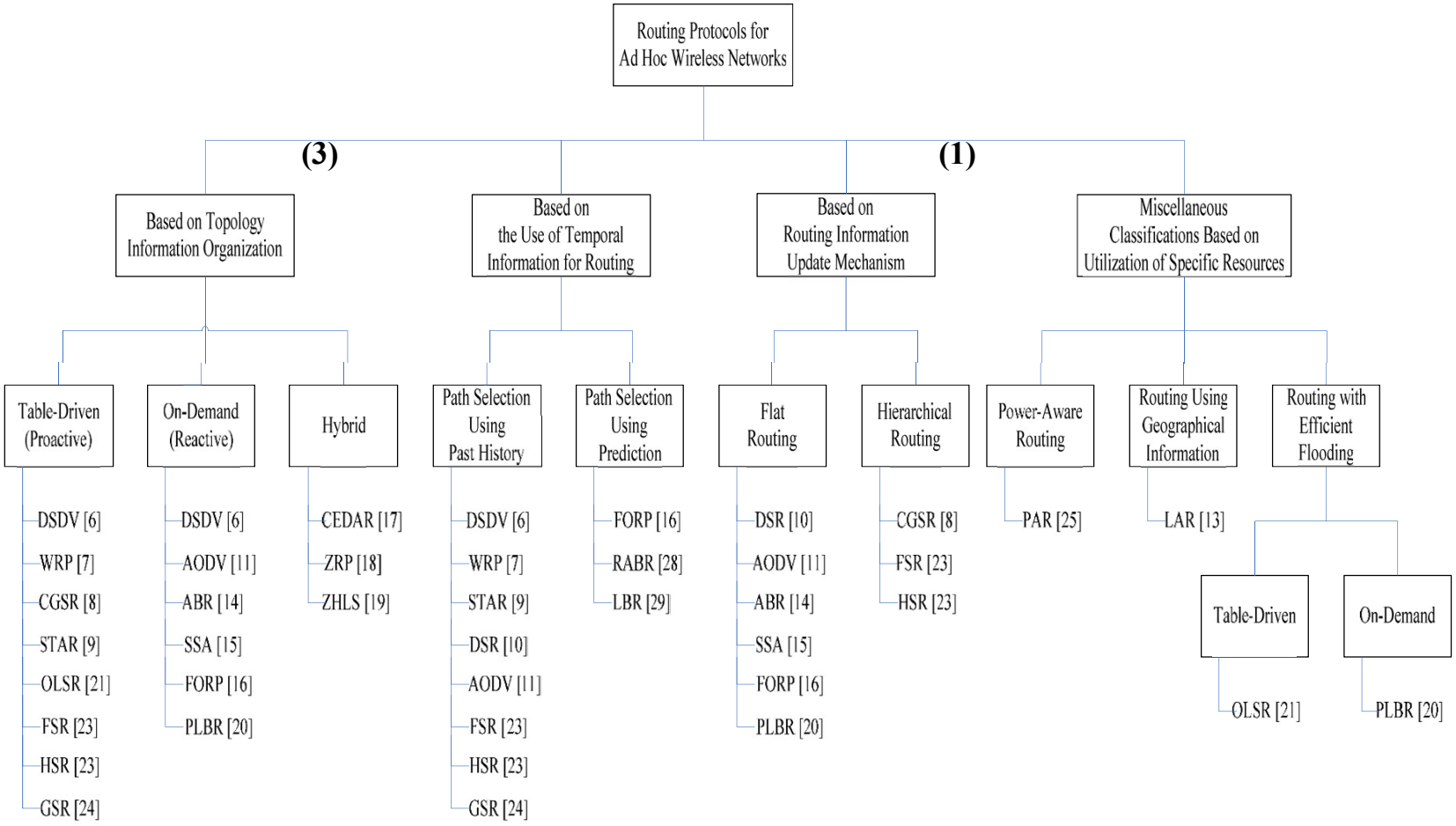
Based on the Routing Topology

- Flat topology routing protocols
  - Flat addressing scheme similar to IEEE 802.3 LANs
  - Globally unique addressing mechanism for nodes
- Hierarchical topology routing protocols
  - Logical hierarchy
  - Associated addressing scheme
  - May based on geographical information or hop distance

Based on the Utilization of Specific Resource

- Power-aware routing
  - Minimize consumption of resource
    - Ex: Battery power
- Geographical information assisted routing
  - Improve the routing performance
  - Reduce control overhead

Classifications of Routing Protocol:



- Table-Driven Routing Protocols
- On-Demand Routing Protocols
- Hybrid Routing Protocols
- Routing Protocol With Efficient Flooding Mechanisms
- Hierarchical Routing Protocols
- Power-Aware Routing Protocols