Wireless Network Protocols

Chapter · March 2017

DOI: 10.1201/b12494-36

2 authors:

Renato M. De Moraes
Federal University of Pernambuco
70 PUBLICATIONS **381** CITATIONS
SEE PROFILE

Hamid R. Sadjadpour
University of California, Santa Cruz
195 PUBLICATIONS **1,914** CITATIONS
SEE PROFILE

Book Chapter on Wireless Network Protocols

Renato M. de Moraes

University of Brasília, Brazil

Hamid R. Sadjadpour

Univeristy of California, Santa Cruz, USA

September 30, 2011

Contents

Chapter 1

Wireless Network Protocols

1.1 Introduction

Wireless networks are characterized by nodes (or stations, or users) that are connected to each other by wireless links. Accordingly, one main feature of such networks is mobility which results in dynamic topology when the position of nodes changes in time. Network setup in mobile wireless ad hoc network is a tedious task because of rapid dynamic nature of these networks while communication in wired networks (internet) or even stationary wireless networks is much easier to manage. In wireless networks, the communication channel is a broadcast medium since the transmitted signal by a node can be received by any other node that is in the transmission range of the transmitter. In some cases, a node transmits to a receiver while another node is also trying to send packet to the same receiver. If these two transmitters are outside of each other transmission range and unaware of the other node existence, it is possible that both nodes try to transmit packets to the same receiver and cause collision. This situation is known as the *hidden terminal problem* and it does not allow the receiver to decode the received signals. Figure 1.1 demonstrates the hidden terminal problem.

Another issue is the related to the fact that in some applications, source and destination

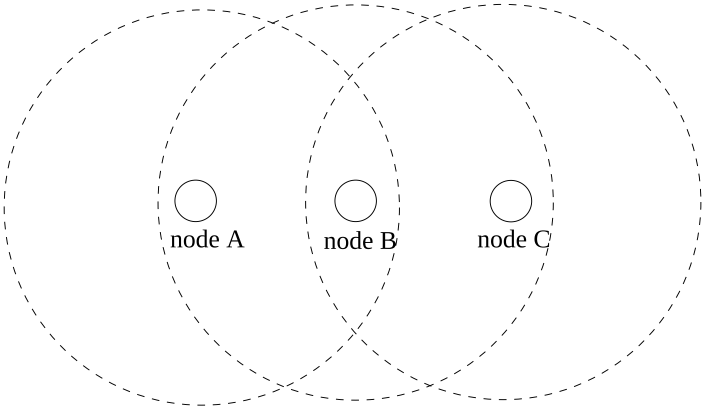


Figure 1.1: Hidden terminal problem. Nodes A and C are within transmission range of node B; however, nodes A and C cannot hear each other. If they both try to simultaneously transmit to node B, a collision will occur at node B.

are not within each other transmission range. Therefore, the source relies on other nodes to relay the message to destination using multihop communications. Since the medium is a broadcast channel, nodes require to coordinate with each other to access the channel in a distributed fashion in order to avoid interference and collision in the network. Consequently, different methods are proposed in literature to coordinate among nodes to access the channel. Such methods are called medium access control (MAC) protocols. Further, once a node can access the communication channel to transmit to its neighbors, it needs to find out the path to destination when there is no base station to route the message to destination. Such networks are called ad hoc networks and MAC and routing protocols are two important ingredients of these networks in order to transport information. This chapter provides a short overview of the main MAC and routing strategies proposed for wireless ad hoc networks.

With respect to the MAC protocols, the random access approaches have gained significant attention due to their simplicity and relatively efficiency to attain the objective of providing channel access in a distributed fashion. In this regard, Aloha and Carrier Sense Multiple Access (CSMA) are by far the most common protocols that are investigated and deployed in wireless ad hoc networks. Section 1.2 will present the Aloha and CSMA protocols with their variants.

With respect to routing strategy, routing protocols can be classified in two types: table-driven (or proactive) and on-demand (or reactive) protocols. In table-driven protocols, the routing algorithm proactively maintains a data base called routing table which includes information about path to each destination node in the network and the next hop in a path from source or relay to destination. In on-demand protocols, the routing algorithm reacts to changes in the network topology to obtain updated routes along multiple hops and as link failures occurs on an active route, the algorithm can search to obtain a new valid path to destination. Once the communication among source and destination is completed and the route is no longer in use, the relay nodes utilized along the path remove the route information from their data base. When a source wants to send data packets to a destination, it initiates the route request. Section 1.3 will present the main features of four important routing protocols for ad hoc networks.

1.2 Medium Access Control Protocols

This section covers the classical Aloha and CSMA protocols proposed in multihop wireless networks. The dynamic aspect of these protocols is due to the random nature of channel access. The stations (or nodes) will compete for the communication medium in a distributed fashion with no coordination in principle. The Aloha protocol was *de facto* the first wireless network protocol implemented in practice and used for transmission of data packets in a wireless network for computer interconnection; however, its low performance prompted other more efficient protocols like the CSMA proposal.

1.2.1 The Aloha Protocol

The Aloha protocol was proposed by Abramson [1] to interconnect the terminals of the University of Hawaii spread on the Hawaiian islands. The proposal was to use a shared broadcast wireless medium employing radio waves to interconnect the host computer in main campus to the other terminals in different islands. One of the key characteristics of this protocol is simplicity and even despite it slow performance, as it will be shown, today the Aloha idea is the fundamental building block for performance analysis of wireless network protocols.

1.2.2 Pure Aloha

The protocol was designed to be distributed such that any node randomly access the shared medium. Consequently, a major advantage of this protocol was simplicity since no coordination is required among nodes.

Whenever a station has data, it transmits immediately without any scheduling with other stations. The receiver acknowledges (ACK) if the packet is received successfully. If no ACK is received after two propagation time period, the transmitter realizes that a collision has occurred. It then waits a random time and retransmits the packet. The station continues this procedure until it receives an ACK for the transmitted packet.

Fig. 1.2 shows the basic behavior of the pure Aloha protocol. During the transmission of the reference packet i, if no other packet from another station is transmitted within the indicated vulnerable period, then the transmission is successful, *i.e.*, no collision happens. If the packet length is constant and equals L (in bits) and the channel transmission rate is R (in bits per second), then the vulnerable period commences $T = L/R$ seconds before the start of the transmission of the reference packet i until the end of its transmission, *i.e.*, a total of $2T = 2L/R$ seconds. Therefore, if other packets from other stations are transmitted during this period, as illustrated in Fig. 1.2, then a collision will happen.

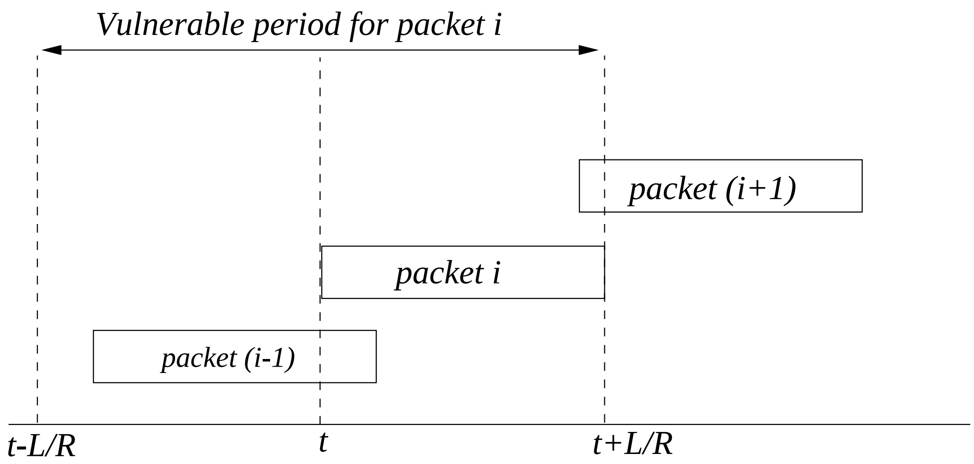


Figure 1.2: Vulnerable period in pure Aloha protocol. For successful transmission of packet i, no other packet can be transmitted within the period starting $T = L/R$ seconds before packet i and during its transmission.

In [1], Abramson assumed that the resulting arrival process of new and retransmitted packets followed a Poisson[1] distribution with mean of G packets per T seconds, in which T is the packet duration in seconds. G is also known as the *offered load* to the network and equals λT, in which λ is the arrival rate of the Poisson process. Thus, the vulnerable period of a packet transmission is $2T$. On the other hand, the throughput X of the system equals the fraction of the arrival flux that is transmitted without collision. The fraction of time that packets are transmitted successfully equals the probability of no collision. No collision happens if no packet arrives during the vulnerable period of a packet that is to be transmitted. Accordingly, the throughput of Aloha is given by [1]

$$\begin{aligned} X &= G \times P\{no\ collision\} = G \times P\{zero\ arrivals\ (i.e.,\ transmissions)\ in\ 2T\ seconds\}, \\ &= G\frac{(2G)^0\, e^{-2G}}{0!}, \\ &= Ge^{-2G}. \end{aligned} \tag{1.1}$$

Fig. 1.2 shows the behavior of X as a function of the offered load. Taking the derivative of X with respect to G and making it equal to zero, one will find that the maximum throughput value is approximately 0.18 attained for $G = 0.5$, which means that the maximum throughput can be attained if on average at every $2T$ seconds one packet is transmitted. If $G < 0.5$ then the throughput of the system is decreased due to dominance of the idle periods, while if $G > 0.5$ the throughput is reduced due to the large number of collision. As figure 1.2 demonstrates, ALOHA only achieves 18% of the maximum throughput which is a very low performance result. A modification proposed to the pure Aloha protocol was called slotted Aloha which double the maximum throughput attained as explained in the next section.

1.2.3 Slotted Aloha

In this approach to multiple access, time is divided into slots of fixed size. The duration of slots equals the packet duration which is $T = L/R$ in which L is the length of the packet and R is the transmission rate. The objective of the slotted Aloha protocol [3] was to reduce

[1] According to a Poisson distribution, the probability of i arrivals in T seconds is given by $\frac{(\lambda T)^i\, e^{-\lambda T}}{i!}$, in which λ is the arrival rate of the process [2].

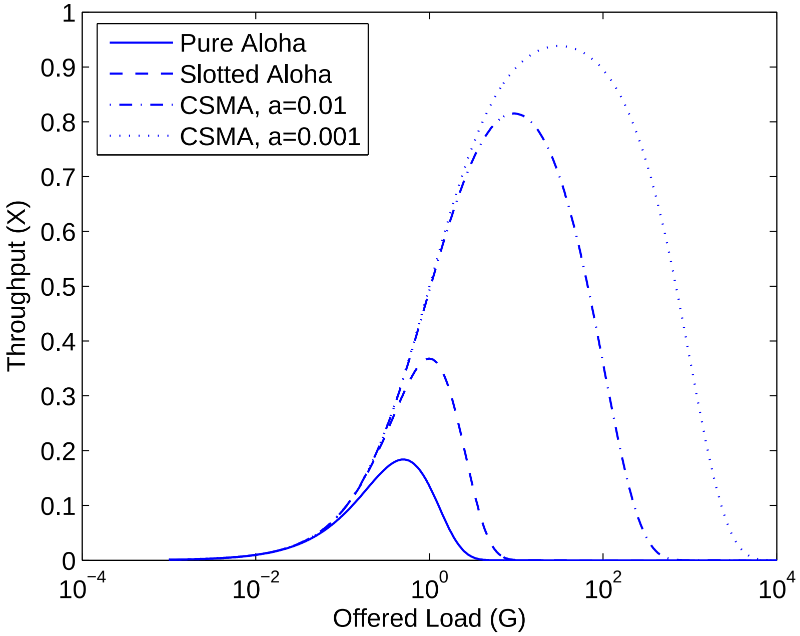


Figure 1.3: Throughput as a function of the offered load (G).

the probability of collisions by forcing all stations to transmit only at the beginning of time slots. Accordingly, the vulnerable period of slotted Aloha is reduced to T.

Stations are synchronized. If a station has a packet to transmit, it does so at the beginning of the next slot. If a collision happens[2], the source node retransmits the packet at the next slot with probability p. It repeats this procedure until a successful transmission occurs.

The throughput analysis of slotted Aloha is obtained by observing that the vulnerable period is now reduced to a slot duration time T. All packets are assumed to be synchronized and only allowed to transmit at the beginning of a slot. Analogous to the pure Aloha analysis, the throughput of slotted Aloha is derived as [3]

$$\begin{aligned} X &= G \times P\{no\ collision\} = G \times P\{zero\ arrivals\ (i.e.,\ transmissions)\ in\ T\ seconds\}, \\ &= G\frac{(G)^0\, e^{-G}}{0!}, \\ &= Ge^{-G}. \end{aligned} \tag{1.2}$$

[2] It is assumed that a feedback from receiver notifies the nodes involved in a collision.

Fig. 1.3 presents the behavior of the throughput of the slotted aloha which maximum value is approximately 0.36 at load $G = 1$. By comparing the behavior, it is clear that the slotted Aloha attains twice the maximum throughput value of the pure Aloha. The increase in performance was obtained by reducing the vulnerable period at the cost of synchronization.

1.2.4 Aloha with Random Backoff

Some wireless communication environments like underwater has different characteristics in which the electromagnetic waves are rapidly attenuated due to energy consumption along the propagation path. In such scenarios, the transmission of acoustic waves are more appropriate. Although the acoustic channel has low speed propagation, it can reach up to 5 kilometres employing frequencies around 50 KHz resulting in transmission rate on the order of 5 kbps [4]. In such case, a modified Aloha protocol was proposed which can readily be incorporated to the off-the-shelf commercial modems [5].

In Aloha protocol with random backoff [6], each node employs a parameter CW representing a contention window size. The backoff time is divided into slotted time of size τ which should be long enough to obtain channel state information. If a node has a packet for transmission, for example, from application running in upper layers, the node randomly selects a slot in the range [0,CW-1] and decrements its timer if there is no activity on the channel. Accordingly, nodes infer the channel use, if busy or idle, every slot boundary and pause their timers if a packet is being transmitted on the channel, *i.e.*, if the channel is determined busy. When the time reaches zero, the node transmits its packet.

In [6], it was shown that Aloha with random backoff is a suitable MAC protocol for underwater communication channel.

1.2.5 The CSMA Protocol

The low performance of ALOHA protocol is due to the large vulnerability period of a packet. In Carrier Sense Multiple Access [7], the stations listen to the channel before transmissions in order to reduce the vulnerability period from the order of a packet length to the maximum channel propagation duration delay (τ). Consequently, the improvement obtained from this approach is based on the fact that τ is assumed much smaller than a packet duration length. By listening before transmition, stations try to reduce the vulnerability period to one propagation delay period. The time required to detect the carrier is negligible. In such approach, if no other node transmits during τ, the sensing station realizes that the medium is free and capture the channel avoiding collision as no other station will transmit thereafter. Depending on the behavior of the stations when it senses that the medium is busy, there are three possibilities (variants) of the CSMA protocol: non-persistent, 1-persistent and p-persistent. Another variation is further obtained if slotted time is used by synchronizing all stations in the network resulting in the slotted CSMA. When a packet is received successfully, the receiver sends and acknowledges (ACK) the packet to the transmitter in order to confirm the delivery of the information.

1.2.6 1-persistent CSMA

The 1-persistent CSMA protocol is the simplest approach to carrier sensing. In such protocol, the station keeps listening and transmits as long the channel is sensed free. If a collision happens the stations involved in the collision run a backoff algorithm and postpones the next attempt to access the channel. Accordingly, if there are more than one node listening to the channel with packets to transmit, a collision will certainly happens because these stations will transmit simultaneously into the channel as long as the medium is idle. Indeed, this variant of the CSMA protocol presents high collision rate due to its greedy nature to capture the channel.

1.2.7 Non-persistent CSMA

In non-persistent CSMA protocol, if the medium is sensed busy, the station waits a random time (running a backoff algorithm) and try again. In Fig. 1.4, a flowchart of the protocol is presented.

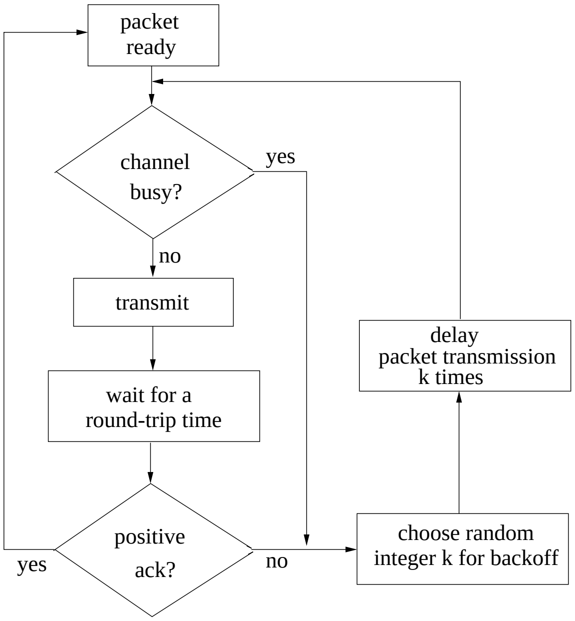

packet ready
channel busy?
yes
no
transmit
wait for a round-trip time
positive ack?
yes
no
choose random integer k for backoff
delay packet transmission k times

Figure 1.4: Flowchart for non-persistent CSMA protocol.

In [7], it is shown that the throughput performance of the non-persistent CSMA is given by

$$X = \frac{Ge^{-aG}}{(1+2a)G + e^{-aG}}, \tag{1.3}$$

where $G = \lambda T$, $a = \tau/T$ and λ is the average arrival rate of packets according to a Poisson process as explained in Section 1.2.2.

Fig. 1.3 presents the behavior of the non-persisten CSMA, which shows the improvement in performance of the wireless medium access protocol due to carrier sensing when comparing with Aloha cases. It is clear that carrier sensing improves significantly the throughput behavior of random wireless medium access networks. Furthermore, the lower is the ratio between maximum propagation delay and packet length, *i.e.* $a = \tau/L$, the better is the maximum throughput performance of the CSMA protocol.

1.2.8 p-persistent CSMA

In the p-persistent CSMA protocol, if the medium is sensed free, the station transmits with probability p and waits with probability $1 - p$ for a backoff time to try again later. Such approach tries to attain a balance between the 1-persistent and the non-persistent cases.

Slotted CSMA

Another variation of the CSMA protocol is to consider the nodes synchronized where sensing is performed at the begining of a slot which has the maximum propagation delay τ.

1.2.9 The CSMA/CA Protocol

Another very important wireless network protocol implemented in the IEEE 802.11 standard [8] is the carrier sense multiple access with collision avoidance (CSMA/CA). This protocol has two modes of operation.

In the first mode, if a station has a packet to transmit, it first senses the channel. If the channel is idle, it transmits its packet. Otherwise, the station will backoff by choosing a random integer to decrement every time it senses the channel is free. If the node perceives the channel busy, the counter value stays frozen. When the counter reaches zero, the station transmits the data packet and waits for the acknowledgement. If the ACK is not received, the sender runs the backoff algorithm again.

In the second mode of operation, the CSMA/CA tries to reserve the channel before transmission. The reservation is accomplished by exchange of short control packets before data packet transmission with CSMA. Fig. 1.5 illustrates packet exchange between nodes A and B. If a source node A has a data packet to transmit, it tries first to negotiate with the intended receiver (node B) to reserve the channel by sending a request-to-send (RTS) control packet. This packet carries the information (duration filed) of how long the other stations (nodes C and D) has to be silent until the end of communication between nodes A and B. This packet has two objectives: first, it warns the nearby nodes of the transmitter that the source node wants to send a data packet; second, it informs the intended receiver to do the same with its neighbors. Accordingly, if the RTS is successfully received at the destination station, it replies by sending a clear-to-send (CTS) control packet informing the duration field in order to warn nearby stations who did not hear the RTS packet[3] that destination is going to receive a data packet such that the destination's neighbors keep silent during the entire communication period. Once the CTS is received by the sender, it transmits the data packet which has length much higher than the RTS/CTS control packets. After the destination successfully receives the data packets, it replies to the sender by transmitting an ACK packet and the communication procedure for this packet is completed. The other stations detecting the duration field adjust their network allocation vector (NAV) to indicate the amount of time the current communication will take place characterizing a virtual channel occupation.

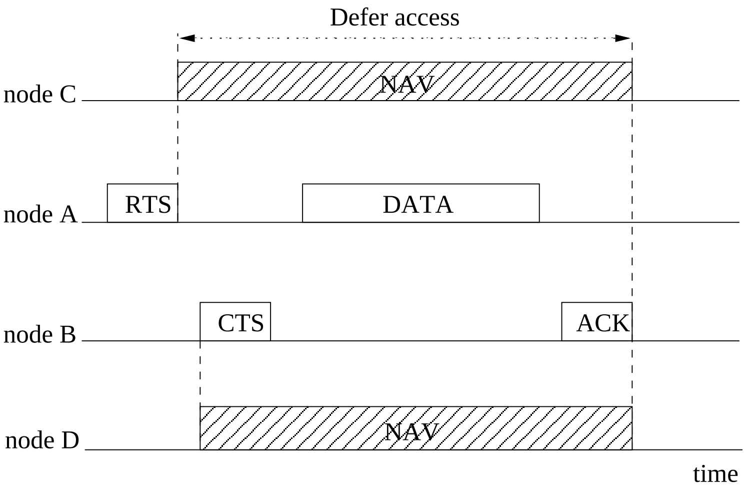


Figure 1.5: Virtual channel detection in CSMA/CA protocol. Node C is close to node A, but does not hear node B, while node D is near node B but does not hear node A. RTS/CTS exchange reserves the channel before transmission of a data packet.

1.3 Routing Protocols

To send information from a source node to a destination node through multi-hop links by implementing one of the above MAC protocols, routing algorithms were proposed which take into consideration the dynamic nature of wireless networks. This section described four important mutli-hop routing protocols: DSR, AODV, OLSR and DSDV. DSR and AODV

[3] The stations that are within the communication range of the destination node but are outside the transmission range of the sender are called the hidden nodes to the transmitter (see Section 1.1).

are on-demand (or proactive) routing protocols whereas OLSR and DSDV are classified as table-driven protocols.

1.3.1 Ad Hoc On-Demand Distance Vector (AODV) Routing

The AODV routing protocol enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network [9]. The AODV algorithm allows mobile nodes to quickly obtain routes for new destinations, and it does not require nodes to maintain routes to destinations that are not in active communication. Also, AODV routing permits mobile nodes to respond to link breakages and changes in network topology in a timely manner. The main objective of this protocol is to rapidly and dynamically adapt itself to changes of conditions in the network links, for example, due to mobility of nodes.

The AODV protocol works as a pure on-demand route acquisition system. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) control packet to its neighbors, which then the first neighbors forward the request to their neighbors, and the RREQ broadcast will continue until either the destination or an intermediate node with a “fresh enough” route to the destination is located.

The AODV protocol utilizes destination sequence numbers to ensure that all routes contain the most recent route information. Each node maintains its own sequence number. During the process of forwarding the RREQ, intermediate nodes record in their routing tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Once the RREQ reaches the destination or an intermediate node with a fresh enough route to destination, the destination or the intermediate node responds by unicasting a route reply (RREP) control packet back to the neighbor from which it first received the RREQ which establishes the route path.

Route Recovery

The AODV protocol employs a neighbor detection mechanism responsible for checking periodically the connectivity between neighbors that keeps a link on an active route. The connectivity is obtained by a node sending local broadcast messages to its one-hop neighbors, called HELLO messages or beacons. When receiving a request HELLO message, the neighbor on a route replies to the sender with information about that route. If a node does not receive a HELLO message from a neighbor on a route during a certain time, it infers that a link breakage occurred.

An active route is defined as a route which has recently been used to transmit data packets. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Alternatively, the algorithm may initiate a local repair mechanism when a link failure happens on an active route and the first node upstream of that break (the predecessor) chooses to repair the link locally if the destination is not too far away. In such case, the node increments the sequence number for the destination and then broadcasts a RREQ for that destination. Thus, local repair attempts will often be invisible to the source node. The node that initiates the repair waits the discovery period to receive RREP in response to the RREQ. During local repair, data packets should be buffered. If, at the end of the discovery period, the repairing node has not received a RREP (or other control message creating or updating the route) for that destination, the node propagates a RERR. When it happens, long delays and huge losses of packets due to exhaustion of the queues will occur. However, if the repairing node receives a RREP, it ensures lower overhead and delay.

In the approach currently implemented on the AODV protocol, it chooses to do either source repair or local repair depending on the number of hops involved on the path. Notice that the choice holds following the condition depicted in Algorithm 1, where *packetForward* is the number of hops from the source node until the upstream node (*i.e.*, the predecessor) before the failure and *predecessorHopCount* is the number of hops from the predecessor node to destination which information is stored in the routing table of the predecessor node. If *packetForward* has more hops than *predecessorHopCount*, the algorithm chooses to make local repair, otherwise the upstream node sends a RERR to the source.

Algorithm 1: AODV Route Recovery Decision.

```
if ($packetForward \geq predecessorHopCount$) then
    localRepair();
end
else
    sourceRepair();
end
```

Summarizing, the main disadvantage of this protocol is the necessity of periodically sending beacon control packets, whereas the main advantage is the protocol adaptability to changes and being able to locally recover from link failure which makes it particularly appropriate for mobile ad hoc networks.

1.3.2 Dynamic Source Routing (DSR) Protocol

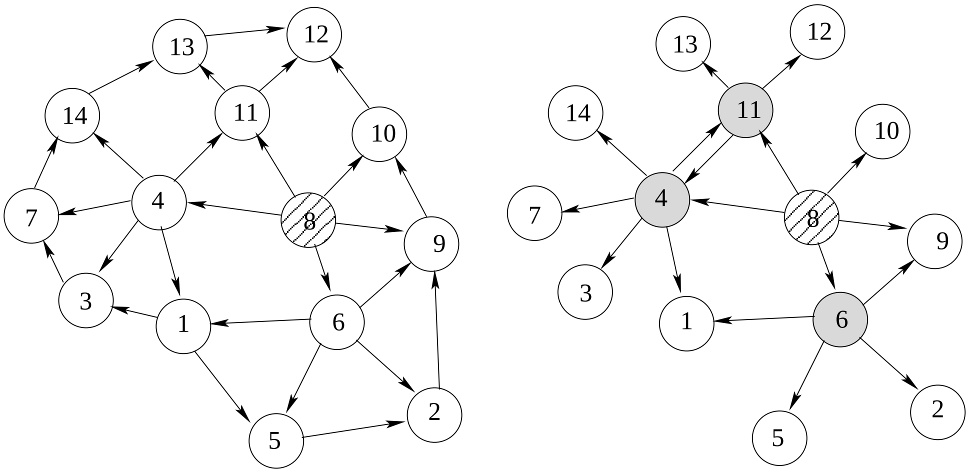
DSR is an on-demand routing protocol [10] designed for mobile ad hoc networks with a simple and efficient approach composed of two main mechanisms: *route discovery* and *route maintenance*, which together allow nodes to, respectively, ascertain and preserve routes to arbitrary destinations in the network. The protocol works well of up to approximately two hundred nodes even with very high rates of mobility. Another important characteristic of DSR is that it does not require periodic messages (like HELLO messages or beacons as in AODV or table-driven protocols). DSR is loop-free, admits multiple routes to destinations and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness.

DSR employs the source routing feature in which the entire route is part of the header of the packet and utilizes caches to store routes on nodes. Consequently, if a node A needs to send a packet to another node B, but it does not have a route to B, then node A initiates a route discovery and broadcasts (floods) a RREQ message. The RREQ packet contains the sender's address, the destinations address and a unique request identification (ID) determined by the sender A. Each node that receives the RREQ message, appends its own identifier (ID) and forwards the updated RREQ. Eventually, a RREQ will reach the destination node with complete reverse path to source which allows the destination to unicast a RREP back to the source establishing the route. After that, the source can unicast the data packet to destination in which the packet header contains the entire path to destination being forwarded by each node along the route.

The main disadvantages of this protocol are that it cannot repair a broken link locally as the AODV protocol does and that overhead of control packets increases with average number of hops in the network.

1.3.3 Optimized Link State Routing (OLSR) Protocol

The OLSR protocol [11] is an optimization of the classical link state algorithm [12] suited to mobile wireless applications. It is a proactive routing using the multipoint relaying mechanism which is an efficient link state packet forwarding scheme. Optimization is attained by reducing the overhead control information by shortening the length of the control packets and by reduction of the amount of links employed to forwarding the link state control packets through entire network. Accordingly, multipoint relays (MPRs) are the nodes responsible to forward the broadcast control messages due to the flooding process necessary to disseminate the link state information. Differently from the classical link state routing algorithm in which the state information is flooded through all nodes of the network, in OLSR scheme only partial link state information is distributed in the network seeking to attain a minimum number of transmissions of control messages but still reaching all nodes in the network. Fig. 1.6 illustrates such behavior for a network with 14 nodes in which node 8 is the source node sending its link state information. In part (a), in classical flooding, all nodes participate in forwarding the message from the source, *i.e.*, the number of control messages are of the order of the number of nodes in the network. However, in part (b), with OLSR, only three nodes are selected as MPRs to forward the control messages reducing the amount of broadcast transmissions needed to flood the entire network. This information is then used for route calculation. OLSR provides optimal routes (in terms of number of hops). The protocol is particularly suitable for large and dense networks as the technique of MPRs works well in this context.



(a) Flooding the network takes as many transmissions as the number of nodes

(b) Source node 8 uses nodes 4, 6 and 11 as MPRs which flood the entire network with four transmissions

Figure 1.6: (a) Classical flooding. (b) OLSR routing protocol employs multipoint relays to reduce the amount of transmissions to flood the entire network.

The main advantage of the OLSR protocol is the reduction of routing overhead compared to other table-driven protocols; however, it is still a table-driven protocol which needs to periodically send control messages through the network to maintain link state update.

1.3.4 Destination Sequenced Distance-Vector (DSDV) Protocol

The DSDV protocol was one of the first routing mechanisms proposed for ad hoc networks [13]. It is proactive and based on the distributed Bellman-Ford algorithm proposed to wired networks [14] which considers the shortest path routing to destination. In DSDV, each node maintains a hop count for each destination and periodically send their routing tables to neighbors which recalculate shortest path upon the receipt of a routing table update. Accordingly, routes to all destinations are promptly available at each node at all times.

When a broken link is detected by a node, it propagates this information to its neighbors such that this information is updated throughout the whole network. Hence, a small change like a single break results in the table update information to be disseminated to the entire network. There are two types of updates: incremental updates and full dumps. The former is used when a node does not observe significant changes in the local topology and the update carries only information changed since last full dump. The latter, full dump, is employed if significant changes in topology is observed and the message conveys all routing table information.

Each entry in the routing table and routing updates is tagged with a sequence number generated by the destination. The destination sequenced number allows identification of stale routes and ensures loop-free operation. In such approach, routing table entries are updated if a new sequence number is observed. If two or more updates contain the same sequenced number, the node chooses the other with better route metric. In order to reduce the dissemination information convergency, a weighted settling time is used to control frequency of new advertisements for a route. Consequently, routing availability to all destinations at all times ensures that small delay is obtained in the route establishment process.

Summarizing the DSDV advantages and disadvantages, it is a protocol with lower route request latency, but higher overhead. It performs best in networks with low to moderate mobility, few nodes and many data sessions. Main problem is poor efficiency for large ad hoc networks in which nodes need to maintain a complete list of destination routes.

1.4 Summary and Conclusion

Wireless networks are characterized by a broadcast access medium that should be appropriately shared among nodes trying to communicate. Furthermore, in infrastructureless scenarios, the channel access and information forwarding tasks must be distributed among the nodes themselves to make communication feasible among nodes separated by multiple hops. Such networks are classified as ad hoc networks.

Aloha and CSMA with their variants were presented for medium access in which it was shown that CSMA has better performance than Aloha, due to fact that in CSMA carrier sense before transmission is essential in order to reduce the occurrence of collision.

This chapter also presented four important routing schemes proposed for wireless ad hoc networks that try to make the relaying of messages from source to destination an efficient procedure even under the situation of mobility which can cause constant topology changes. Two table-driven routing protocols, DSDV and OLSR, were described which provided nodes with routes to their destinations in the network. These two protocols have high overhead in terms of exchange of control messages in order to keep table entries updated. On the other hand, two reactive routing protocols, AODV and DSR, were reviewed where it was reported that routes are obtained on-demand, *i.e.*, paths to destinations are obtained upon sources requests causing a smaller control message overhead while requiring longer setup time to establish the route when compared to proactive protocols.

References

[1] N. Abramson, “The ALOHA System: Another Alternative for Computer Communications,” *Proc. of Fall Joint Computer Conference*, Houston, TX, USA, Nov. 1970.

[2] A. Papoulis and S. U. Pillai, “Probability, Random Variables and Stochastic Processes,” Mcgraw Hill, Inc., 2002.

[3] L. G. Roberts, “ALOHA Packet System with and without Slots and Capture,” *Computer Communications Review*, vol. 5, No. 2, pp. 28-42, April 1975.

[4] M. Stojanovic, On the relationship between capacity and distance in an underwater acoustic communication channel, *Proc. of ACM WUWNet*, September 2006.

[5] L. Freitag, M. Johnson, M. Grund, S. Singh, and J. Priesig, Integrated Acoustic Communication and Navigation for Multiple Uuvs, *Proc. of IEEE OCEANS*, November 2001.

[6] N. Parrish, L. Tracy, S. Roy, P. Arabshahi and W. L. J. Fox, “System Design Considerations for Undersea Networks: Link and Multiple Access Protocols”, *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 9, pp. 1720-1730, December 2009.

[7] L. Kleinrock and F. Tobagi, "Packet Swithc in Radio Channels: Part I - Carrier Sense Multiple Access Modes and Their Throughput-Delay Characteristics," *IEEE Transactions on Communications*, vol. com. 23, No. 12, pp. 1400-1416, December 1975.

[8] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[9] C. E. Perkins, E. M. Belding-Royer and S. R. Das, "Ad Hoc On-Demand Distance Vector Routing." *Request for Comments*: 3561, July 2003.

[10] D. Johnson, Y. Hu and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4." *Request for Comments*: 4728, Feb 2007.

[11] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," *Request for Comments*: 3626, October 2003.

[12] J. M. McQuillan, I. Richer and E. C. Rosen, "The New Routing Algorithm for the ARPANet," *IEEE Transactions on Communications*, vol. com. 28, No. 5, pp. 711-719, May 1980.

[13] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proc. of ACM SIGCOMM*, Aug. 1994.

[14] C. Hedrick, "Routing Information Protocol." *Request for Comments*: 1058, June 1988.

Further Information

Readers interested in wireless ad hoc network protocols are recommended the following overview books:

- C. S. R. Murthy and B. S. Manoj, "Ad Hoc Wireless Networks Architectures and Protocols," Prentice Hall, 2004.
- P. Mohapatra and S. Krishnamurthy, "AD HOC NETWORKS: Technologies and Protocols," Springer, 2010.

More information on this topic can be found in *IEEE Transactions on Communications*, *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Vehicular Technol-*

ogy, *Elsevier Ad Hoc Networks* and issues of *IEEE Journal on Selected Areas in Communications* covering wireless ad hoc networks.