CHAPTER 3

CROSS LAYER BASED ROUTING PROTOCOL WITH POWER SAVING TECHNIQUE (CBRP-PS)

3.1 INTRODUCTION

The routing protocol is used to establish a path between the source node and destination node to relay the traffic. The traffic is generated at the sender and relayed towards the receiver. This traffic flows through Multi hop path which involves many intermediate nodes. The queuing delay, contention delay, transmission delay, and available bandwidth at every intermediate node determine the performance of the routing protocol. The routing protocols use the routing metric for choosing a path between the sender and receiver. A new routing metric is introduced in the AODV routing protocol. The routing metric includes queuing delay, contention delay, transmission delay, and available bandwidth in the route selection process. This chapter describes about how the AODV is modified to optimize the performance of UWB ad hoc networks. This chapter also illustrate about how the power saving technique can be applied to optimize the performance of UWB ad hoc networks.

3.2 REVIEW OF AD HOC NETWORK ROUTING PROTOCOLS
3.2.1 Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV routing protocol is an on demand protocol that is a route is established only when the source node wants to send the data. The AODV is
the improved version of Destination Sequenced Distance Vector (DSDV)
routing protocol. DSDV operates efficiently in small networks only because it
requires frequent broadcast of connectivity information. The difference
between AODV and DSR is that the DSR uses source routing in which the
data packets carry the complete route to be traversed to reach the destination
whereas in AODV, the source node and all the intermediate nodes maintains
the next hop information corresponding to each flow for data packet
transmission. The main advantages of AODV are that the routes are
established on demand and the destination sequence number is used to find
the freshness of the route to the destination.

3.2.1.1 Route discovery

The route discovery process is initiated by the source node only
when the route is not available to the destination. The source node floods the
route Route Request (RREQ) packet in the network. Each intermediate node
receiving RREQ either forwards the RREQ to the neighbor node or reply with
Route Reply (RREP). The intermediate node forwards the RREQ if it does
not have a recent route to the destination. The intermediate node replies with a
RREP if it has a fresh route to the destination.

A RREQ carries the source identifier, the destination identifier, the
source sequence number, the destination sequence number, the broadcast
identifier, and the time to live field. The broadcast identifier is incremented
for every RREQ packet generated by the source node. Sometimes the
intermediate node may receive the same RREQ from multiple neighbors. In
this case, the intermediate node checks the source identifier and the broadcast
identifier, if it matches with the previously received RREQ, then it discards
RREQ packet as a duplicate copy. When an intermediate node receives a
RREQ, it stores the neighbor identifier from which it has received the RREQ
packet. This information is used by the intermediate nodes to establish the reverse path to reach the source node. The propagation of RREQ packets is illustrated in figure 3.1 (a).

The RREP is sent by either the intermediate node or the destination node. If the intermediate node has a recent path to the destination, it responds with a RREP, otherwise the RREP is sent by the destination. The intermediate node sends RREP to the source node only if the destination sequence number of the route to the destination is equal to or greater than the destination sequence number carried by RREQ. When the RREP is sent back to the source, all the intermediate nodes sets forward route entry in the routing table. The figure 3.1 (b) shows the propagation of RREP packet towards source node S.

3.2.1.2 Route maintenance

The link break in AODV is determined by observing the periodical beacon messages or through link level acknowledgements. The end nodes are informed about the link failure. Suppose an intermediate node along the forward path moves away, the upstream neighbor notices the move and forwards the link failure notification towards the source node. The link failure notification is forwarded by all the upstream neighbors until it reaches the source node as shown in figure 3.2. The source node reinitiates the route discovery process with the new broadcast identifier and the previous destination sequence number.
(a) Flooding of RREQ packets by the source node S

(b) Propagation of a RREP packet towards the source node S

Figure 3.1 AODV Path Discovery Process
Figure 3.2  AODV Route Maintenance

3.2.2 Dynamic Source Routing (DSR) Protocol

The DSR protocol is an on demand protocol designed to reduce the bandwidth consumed by control packets in ad hoc networks. DSR eliminates the periodic table update messages required in the table driven routing protocols. In DSR, the nodes do not require periodic hello packet (beacon) transmissions to inform its neighbors of its presence. DSR is a source routing protocol in which the source node determines the sequence of nodes through which the packets can be forwarded.

3.2.2.1 Route discovery

Assume that the source node has data packets to send and does not have route to destination. The source node initiates the route request (RREQ) which is flooded throughout the network. Each intermediate node receiving
the RREQ packet rebroadcast the packet towards the destination node. A node upon receiving the RREQ packet, checks the sequence number in the packet before forwarding it. This process is used to avoid the propagation of duplicate RREQ. All the nodes except the destination node forwards the RREQ during the route discovery phase. The destination upon receiving the RREQ sends the route reply (RREP) through the reverse path that RREQ had travelled. Every node in the network maintains a route cache in which all the routes learned by the node are maintained. This route cache is used in route discovery phase also. If an intermediate node receiving a RREQ has a route to the destination node in its route cache, then it sends a RREP with a entire route information from source to destination.

The route record building process is shown in Figure 3.3 (a) in which the arrows indicate the direction of flow of route request towards the destination. The numbers on the arrow indicate route record (i.e. the list of nodes through which the route request has travelled). For example, the route record 1-2-5-9 indicates that the route request has travelled through nodes 1, 2, 5 and 9. The propagation of route reply is shown in Figure 3.3 (b). The arrows in the diagram indicate the direction of flow of the route reply. The numbers on the arrow indicate the complete path from source to destination. For example, the route record 1-3-6-8-12-13 indicates the path form source to destination flows through node 1, 3, 6, 8, 12 and 13.

3.2.2.2 Route maintenance

A wireless link in the path breaks due to the movement of the intermediate node. The node adjacent to the link break generates the route error (RERR) message and informs the source node about the link break. The route cache entries in the intermediate node and the source node are updated. Then the source node reinitiates the path discovery process. If the link break
is due to the movement of end nodes, the source node again initiates the route discovery process.

(a) Building of the route record

(b) Propagation of the route reply

Figure 3.3 DSR Route Discovery Process
3.2.3 Location-Aided Routing (LAR)

The different variations of route request flooding is used in AODV and DSR, which creates excess routing overhead. The LAR has been developed to minimize the routing overhead with the help of location information. In LAR, the flooding process is restricted to a certain area using the position information. The RREQ and RREP in LAR are similar to DSR and AODV.

Location Information: The exact physical location of a node is obtained using Global Positioning System (GPS). The information provided by the GPS is always with a small error. The differential GPS offers position information with some reasonable accuracy of few meters.

Expected Zone: Consider a source node S wants to send data to destination node D. Before finding a path to the destination, the source node tries to guess the location of D. Assume that the source node S knows the location of D at time $t_0$ (P) and speed of movement of D (v). At time $t_1$, the source nodes expect that D to be in a circle around point P with a radius of $v (t_1-t_0)$ as shown in figure 3.4. This expected zone only gives the possible location of D at any given time. This expected zone may not be correct under two circumstances: (i) if the source node did not have a correct location of D at time $t_0$ and (ii) if D is moved away with higher speed than the speed expected by S. In this situation, the entire ad hoc network is considered as an expected zone.
Request Zone: The request zone is defined as the zone where RREQ should be forwarded. The request zone is different from the expected zone. The RREQ packets are forwarded by the intermediate nodes only, if they belong to request zone. The request zone should include the expected zone then only the route request will reach the destination.

In Figure 3.5 (a) both source node S and destination node D are part of request zone. In Figure 3.5 (b), both S and D are contained in the request zone but there is no route between S and D through the nodes in the request zone. In this case, the route is established through the nodes that are near but are outside the request zone. Assume that after sometime there is no direct route from S to D. The request zone is expanded and then the source node reinitiates the route discovery process as shown in Figure 3.5 (c).
Figure 3.5 LAR - Different Request Zones
3.2.3.1 LAR Request Zone Types

When an intermediate node receives a data packet, it uses an algorithm to determine whether to forward the packet or not. The packet is forwarded by the node only if it is a member of the request zone. To perform this task, LAR defines two types of request zones:

LAR Type 1 (LAR 1)

In LAR 1, a rectangular shaped request zone is defined as shown in Figure 3.6. Let ‘P’ be the previous location of D at time $t_0$ and $v$ be the average speed at which D is moving and these two values are known to S. At time $t_1$, the expected zone is defined as a circle with P as a center point and $v(t_1-t_0)$ as a radius. Now the rectangular request zone is defined in such a way that it is a smaller possible rectangular which includes the source node S and the circular expected zone. In addition, the sides of the rectangular request zone should be parallel to x and y axis. The source node can able to determine the four corners of the rectangular request zone.

When S sends a route request it includes all the four corners of the request zone. The RREQ flows through all the intermediate zones, and the intermediate zone forwards the RREQ only if they are within the four corners of the rectangular request zone, otherwise, it drops the RREQ packet. Finally, the RREQ reaches the destination. Then the destination sends the RREP along with its current position, the actual time and average speed at which D is moving. This information is used by source node during the future route discovery phase.
LAR Type 2 (LAR 2)

In LAR 2, when the source node $S$ sends a RREQ, it includes the estimated coordinates of destination $(x_d, y_d)$ and the distance to destination. The intermediate node forwards the RREQ only if it is located at most $\delta$ distance from the previous node. The parameter $\delta$ is dependent on the implementation. The intermediate nodes forward the RREQ by overwriting the distance field with its current distance to $D$.

![Figure 3.6 LAR Type 1 - Request Zone](image)

3.2.4 Zone Routing Protocol (ZRP)

The zone routing protocol is a hybrid routing protocol which combines the best features of proactive and reactive routing protocols. The zone routing protocols works based on the fact that in a mobile ad hoc network most of the communication takes place between nodes that are close to each other. The ZRP divides the entire network into a number of
overlapping zones. Within a zone, proactive routing protocol is used to find the neighbors by sending the hello messages. The reactive routing protocol is used beyond the zone to establish the route between source and destination. The size of a zone is defined by each node. The size is defined in terms of number of hops to reach the perimeter of the zone. The zone size depends on the various features such as available power, reliability of different nodes etc.

Figure 3.7 shows an example routing zone of node A in which the zone is indicated by a dotted circle. The nodes on the dotted circle (dark grey colour) are called as perimeter nodes, which builds the border of A’s zone. The node A can reach border nodes with number of hops or radius $\rho = 2$. The Neighbor Discovery Protocol (NDP) helps to determine the perimeter nodes and also to build a zone.

![Figure 3.7 ZRP - Routing Zone of Node A, $\rho = 2$](image)

### 3.2.4.1 Intra zone Routing Protocol (IARP)

An IARP is employed in the zone where a particular node employs a proactive routing to find the neighbors within the same zone. Each node
builds a routing table by exchanging the periodic update packets and maintains the route to all nodes within the routing zone.

3.2.4.2 Inter zone Routing Protocol (IERP)

The IERP is used for finding paths to reach the nodes which are not members of the routing zone. The IERP makes use of the information available at every node's routing zone and establishes the route. Consider a source node S wants to send data packets to destination node D. If the node D is within the own zone then the packets are delivered to it directly. Otherwise, the node S broadcast (uses unicast to send the packets to peripheral nodes) the RREQ to its peripheral nodes. If any one of the peripheral node has destination in its zone then, it sends a RREP back to node S. Otherwise, the RREQ is re broadcasted to the peripheral nodes. This process is repeated until the node D is located. Then the node D sends RREP to node S. When RREQ is forwarded each node appends the address to it. This information helps to send the RREP back to sender S.

When the intermediate node in the path detects a broken link, it performs a local reconfiguration to find a short alternate path to bypass the broken link. The sender node is informed about the change in the path. This path is a sub optimal path only. To find an optimal path, the sender reinitiates the path discovery process once again.

3.3 PROPOSED CBRP-PS

The CBRP-PS is a modified version of the existing AODV routing protocol. The CBRP-PS is a cross layer based routing protocol in which the cross layer parameters such as queuing delay, contention delay, transmission delay, and available bandwidth at every intermediate node are considered in
the route selection process. The CBRP-PS uses the four MAC level queues for Access Categories (AC) introduced by IEEE 802.11e to improve the QoS.

3.3.1 Formation of Routing Metric (RM)

A new routing metric value is proposed in the CBRP-PS which plays a crucial role in determining a path for relaying a particular type of traffic from source node to destination node. The key parameters that determine the routing metric includes available bandwidth, queuing delay, contention delay and transmission delay. Each one of these parameters and the routing metric are explained in the next section.

3.3.1.1 Bandwidth estimation

Direct range is the area within transmission range and indirect range is the area between transmission range and interference range. The total number of these two areas represents the number of competitive nodes. Hence each node maintains two tables namely Direct Range Members (DRM) and Indirect Range Members (IRM). DRM is established from the first hop and the IRM is established from two or more hops nodes or hidden nodes. The bandwidths of the neighboring nodes are obtained proactively or reactively. For obtaining the bandwidth information at neighboring nodes, the proposed scheme selects the proactive approach. In this mode, in order to decrease collision and to deliver bandwidth information, every node issues a signal at its own defined interval, which can be coordinated with neighboring nodes. All the neighboring nodes send their own bandwidth data by one-hop with double power for collecting neighboring nodes information.

Nodes that perform active attacks with the aim of damaging other nodes by causing the network interruptions are considered as malicious. The
malicious nodes may try to send incorrect bandwidth information to nearby nodes to slow down the network communication. The task of identifying and isolating the malicious nodes using the routing layer information in ad hoc network is a big research area. In our research work, we have not proposed any technique to deal with the malicious nodes. We assume that the network is fully secured.

In order to prevent the nodes in a UWB ad-hoc networks from simultaneous transmission, a randomization of the transmission time of packets by nodes, known as jitter has been employed. Three jitter mechanisms, which addresses different aspects of this problem has been employed. The aim of these jitter mechanisms is to reduce the likelihood of simultaneous transmission, and if it occurs preventing it from continuing. Three cases of sending messages are given below:

- Periodic message generation
- Externally triggered message generation
- Message forwarding

For the first case, jitter is used to reduce the interval between successive message transmissions by a random amount. For the second and third cases, jitter is used to delay a message being generated or forwarded by a random amount.

The proposed scheme should assure that each node within the interference range has enough bandwidth for transmitting the data without congestion. Hence the identification of local and the neighboring nodes within the interference range should be accurate. A node transmitting data considers both its local bandwidth and the bandwidth of all interference range nodes. In the proposed system, every node transmits a particular signal with double
power at a predefined interval. Each node collects all the signals from its neighboring nodes and updates its DRM and IRM tables.

The local bandwidth and neighboring node's bandwidth are determined as below. Since bandwidth is shared among neighboring nodes, a node listens to the channel and estimates bandwidth based on the ratio of idle and busy times for a predefined interval.

The local bandwidth $L_{BW}$ is estimated as given in equation (3.1)

$$L_{BW} = \left(\frac{1}{I_t - CU}\right) * C_{BW}$$

(3.1)

where $I_t$ denotes the predetermined time interval, $C_{BW}$ denotes the channel capacity, and $CU$ denotes the channel utilization rate for predefined interval $I_t$.

The channel utilization rate is given by equation (3.2)

$$CU = \frac{B_t}{I_t}$$

(3.2)

$B_t$ denotes the channel busy time in a predefined interval $I_t$. The neighboring nodes bandwidth is given by $NM_{BW}$ which is collected from the neighboring nodes.

So the residual bandwidth $RBW$ is calculated as given in equation (3.3)

$$RBW = NM_{BW} - L_{BW}$$

(3.3)

When the idle time increases the busy time is reduced therefore channel utilization is decreased. Because of this $L_{BW}$ is increased and $RBW$ is
decreased. The routing metric is indirectly proportional to the RBW, hence RM is increased.

3.3.1.2 Estimation of queuing delay (DQ)

Queuing delay represents the time spent by a packet in the MAC sub-layer queues after passing through the MAC-service access point, till it is marked ‘ready’ for transmission. The arrival and service rate of the queue affects the queuing delay. Packets arriving in the queue are from two different sources,

- Packets received from other nodes which are further relayed,
- Packets generated by host applications.

Service rate is tied up with the channel conditions, transmission rate and contention levels within a BSS and the internal contention within the queues at every node.

3.3.1.3 Contention delay (DC)

The time which a node spends while competing for acquiring access to the medium is known as contention delay. When an MSDU is marked ‘ready’ the contention period starts for transmission. According to IEEE 802.11 rules whenever a medium is busy the node will wait. While the medium is in idle state, a node waits further for predefined distributed inter-frame space (DIFS) duration and then waits for a random number of timeslots depending on the value of back-off. If there is an activity on the medium all nodes set their back-off counters.
The outcome of previous transmissions has an impact in the value of back-off counter. Retransmissions effect higher values of back-off counters (by incrementing the Contention Window size). The nodes would set their back-off counters a number of times before they finally find their turn for transmission in the case of highly congested nodes. To expose the significance of back-off and the overall medium access delay various scenarios with varying node density are simulated. We also configured the nodes to communicate whenever they acquire access to the medium.

3.3.1.4 Transmission delay (DT)

Transmission and propagation time for delivery of MSDUs between MAC level nodes along with the time spent in the retransmissions is given by $T_{t}$. The decisions of statistics based rate adaptation schemes are extensively affected by the MAC level retransmissions. So, after frame failures, higher transmission delay occurs because retransmission attempts are made using a lower transmission rate. The per frame $T_{c}$ and $T_{t}$ is given by equation (3.4):

$$T_{c} + T_{t} = \sum_{n=1}^{\text{Retrans}} (T_{cn} + T_{ln})$$

(3.4)

In other words, every value of $T_{c}$ and $T_{t}$ represents the total contention and transmission delay experienced till a frame is successfully transmitted.
3.3.1.5 Routing metric (RM)

The routing metric of CBRP-PS at a node represents the sum of the average queuing, medium access contention and transmission delays experienced by a frame and available bandwidth. For a destination node ‘x’, a node running CBRP-PS would have the following route metric defined by equation (3.5) in its routing table:

\[ RM = \sum_{i=1}^{HNO} \frac{(DQ_i + DC_i + DT_i)}{RBW_i} \]  

(3.5)

where, DQ, DC and DT are queuing, contention and transmission time at each link of a route to destination ‘x’ respectively and RBW is the residual bandwidth of a node. ‘HNO’ is the total number of hops between a source and destination nodes.

3.3.2 CBRP-PS Operation

We have modified the structure of AODV routing table by including the AC parameters as route entry parameters. For the CBRP-PS, the route entry structure has four next-hop address fields for the same destination address, each of the four correspond to a one of the four AC-routes. Depending on the metric values, for a unique destination address, a node running the CBRP-PS routing table has such a provision for maintaining per AC route information. An instance of the structure of CBRP-PS routing table is as given in Table 3.1.
Table 3.1 An instance of CBRP-PS routing table

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>AC_BK Next hop for AC_BK</th>
<th>CBRP-PS for AC_BK</th>
<th>AC_BE Next hop for AC_BE</th>
<th>CBRP-PS for AC_BE</th>
<th>AC_VI Next hop for AC_VI</th>
<th>CBRPPS for AC_VI</th>
<th>AC_VO Next hop for AC_VO</th>
<th>CBRP-PS for AC_VO</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.15</td>
<td>192.168.100.15</td>
<td>0.06</td>
<td>192.168.100.15</td>
<td>0.055</td>
<td>192.168.100.13</td>
<td>0.04</td>
<td>192.168.100.12</td>
<td>0.035</td>
</tr>
</tbody>
</table>
The AODV with slight variations gives us the CBRP-PS for route discovery and maintenance, which is used for integrating the new route metric for route selection. The route request (RREQ) initiated by the source and the route reply (RREP) initiated by the destination/intermediate nodes executes the route discovery. Only if the node has a knowledge about the current contention delay experienced at its MAC layer, the CBRP-PS route metric can be included. Average queuing delay information is also required by the nodes for each of the four ACs. The contention and queuing delay are specific to the current node and independent of the next hop.

3.3.2.1 Generation of RREQ

Consider a source node N1 want to send data to the destination node N9. The source node N1 initiates the route discovery process if it does not have a route to the destination N9. The source node generates and floods the RREQ packets. The source sequence number in RREQ is N1’s sequence number and the destination sequence number field in RREQ is the last known destination sequence number for the destination N9. The flooding identifier field in RREQ is incremented by one from the last flooding.

3.3.2.2 RREQ propagation

The current node after receiving an RREQ message, first checks if it has recent (in the past 10 seconds time-window) communication with the node sending the RREQ message. It is important to notice that the propagation delay calculated by ‘N4’ is not based on the transmission rate at which ‘N2’ sent the latest RREQ message, which is sent by the MAC layer of IEEE 802.11 at a lower rate than the transmission rate which is used for actual transmission of data frames.
A local cache of neighboring nodes (MAC addresses) and the transmission rates used for communication with each of the neighboring nodes is maintained. It is also possible for the node to maintain a similar field in the local cache to indicate the transmission rates used while communication with the node which transmitted the RREQ message. Therefore, if there is a recent communication with the RREQ-sending node, a simple table look up (fetching the transmission rate using the source MAC address) provides the transmission rate information of the node which transmitted the RREQ message.

A node receiving a RREQ message fills the propagation delay field by using the transmission rate information from its local tables. However, in case of no recent communication between the nodes sending and processing the RREQ; the receiving node uses a default transmission rate of 11 Mbps and using this rate it estimates the propagation delay. Considering the propagation delay from the current node to the RREQ-sending node provides the accurate measure of the propagation delay which would be experienced on this hop of the route.

An RREQ message which is propagated in this manner provides information about the route from the destination to the source node in terms of the selected metric parameters.

3.3.2.3 Generation of RREP

A RREP message is generated in response to a RREQ message. A RREP indicates the residual bandwidth, queuing, contention and transmission delay from the destination to the source. The destination node after receiving a RREQ message, increments the sequence number if the destination sequence number in the received RREQ message is higher than the current
sequence number. Otherwise, it does not change its sequence number. The destination node places the sequence number in the corresponding field in the RREP message and assigns NULL to the routing metrics.

If the current node generating the RREP message is an intermediate node, it simply places the destination sequence number that it has maintained for the destination into the corresponding field in the RREP message. The intermediate node fetches the routing metric values that it has for the destination and adds its corresponding routing metrics values for inclusion in the RREP message. The rest of processing remains the same as in the case of AODV i.e. the lifetime field in the RREP is calculated by subtracting the current time from the route expiration time value that the intermediate node has for the current route.

Node N1 communicates with node N9 through intermediate nodes in an ad-hoc network. The values at each node represent the link metric values for AC_VO, AC_VI, AC_BE and AC_BK respectively. For example, N1 has a link metric of 0.5 for AC_VO when it communicates with N3. The link metric values are higher for AC_BE and AC_BK at N3, N5 and N7 which may reflect the possibility that these nodes either generate or forward packets most of which belong to either AC_VO or AC_VI. As a consequence, packets which fall into other ACs would experience higher queuing delays at these nodes. According to the forwarding table of N1 and the metric values as depicted at various nodes in the topology shown in the Figure 3.8, the routes used by various ACs from N1 to N9 are:

AC_VO:  N1 → N3 → N6 → N8 → N9
AC_VI:  N1 → N3 → N5 → N8 → N9
AC_BE:  N1 → N2 → N4 → N7 → N9
AC_BK:  N1 → N2 → N4 → N7 → N9
The RM values computed using the equation 3.5 at different nodes in the topology is shown in the Figure 3.8. The values at each node represent the link metric values for AC_VO, AC_VI, AC_BE and AC_BK respectively. For example, the link metric value 1, 1.5, 2, 2 represent the link metric value for AC_VO, AC_VI, AC_BE and AC_BK respectively.

A source node may receive more than one RREP messages for the same destination node, each of the RREP messages may possibly give a different value of the route metric (RM). The source node selects a route based on the comparison of the received values of RM in the corresponding RREP messages. It is important to notice that such comparison is made individually for each AC. Assume that the source node receives two RREP messages indicating two different route metrics (i.e. RM1 and RM2), we simply name the route: N1_N2_N4_N7_N9 as route-1 and route: N1_N3_N6_N8_N9 as
route-2. Assume that the route-2 offers higher queuing delay for traffic category belonging to AC_BK, and less for traffic belonging to AC_VO and AC_VI such that:

\[
(Q_{AC\_BK} + C + P)_{route\_1} \leq (Q_{AC\_BK} + C + P)_{route\_2} \\
(Q_{AC\_VI} + C + P)_{route\_2} \leq (Q_{AC\_BK} + C + P)_{route\_1} \\
(Q_{AC\_VO} + C + P)_{route\_2} \leq (Q_{AC\_BK} + C + P)_{route\_1}
\]

In this case, the node ‘N1’ would use route-1 for packets tagged with delivery service ‘Background’ and update its routing table entries at time instance t1 (when it receives RREP for route-2), to use route-2 only for packets tagged with ‘AC_VO’ and ‘AC_VI’ delivery service. The source’s decision for selecting a route is based on the comparison, according to which the route having route metric RM2 will be selected if RM2 < RM1. The route with lowest metric value will be chosen to send a particular type of traffic.

3.4 POWER SAVING (PS) TECHNIQUE

Power saving is an important issue for almost all kinds of portable devices. In this section, we consider the design of power-saving technique for UWB ad hoc networks. UWB ad hoc network is one consisting of a set of mobile hosts which can communicate with one another and roam around randomly. Hence, the mobile nodes should be able to communicate in multi hop fashion without the support of base station. The mobile device will become useless if the power is drained completely. Battery power is a limited resource, and it must be managed efficiently. Hence, how to lengthen the lifetime of batteries is a critical issue, especially for UWB ad hoc networks. Solutions addressing the power-saving issue in UWB ad hoc networks can generally be classified into three categories as follows:
Transmission Power Control: In wireless communication, transmission power has strong influence on bit error rate, transmission rate, and inter-radio interference. The transmission power control can be used to reduce the interference and improve throughput on the MAC layer. How to determine transmission power of each mobile host so as to determine the best network topology is known as topology control.

Power-Aware Routing: Power-aware routing does not allow a mobile node to forward the data packets, when a mobile host’s battery level is below a certain threshold. The route is chosen between the source and destination based on the power level of the intermediate nodes.

Low-Power Mode: Many wireless devices are designed nowadays to support low-power sleep modes. IEEE 802.11 has a power saving mode in which a radio only needs to be awake periodically. Hyper LAN allows a mobile host in power-saving mode to define its own active period. An active host may save powers by turning off its equalizer according to the transmission bit rate.

This work focuses on the management of power-saving (PS) modes for IEEE 802.11 -based UWB ad hoc networks and thus falls into the last category of the above classification. We consider the UWB ad hoc networks which are characterized by multi-hop communication, unpredictable mobility, no plug-in power, and no clock synchronization mechanism. In particular, the last characteristic would complicate the problem since a host has to predict when another host will wake up to receive packets. Thus, the protocol must be asynchronous. Existing standards, such as IEEE 802.11 and HYPERLAN, do support PS modes, but assume that the MANET is fully connected. Bluetooth also has low-power modes, but is based on master-slave architecture, so time synchronization is trivial.
3.4.1 Power-Saving Modes in IEEE 802.11

IEEE 802.11 supports two power modes: active and power saving (PS). Under the PS mode, a host can reduce its radio activity by only monitoring some periodical signals (such as beacons) in the network. Tuning a host to the PS mode can save a lot of energy. However, PS mode should be used cautiously so that the network throughput and delay do not get hurt.

Under the ad hoc mode, IEEE 802.11 divides the time axis into equal-length beacon intervals, each of which starts with an ATIM (Ad hoc Traffic Indication Map) window. The ATIM window is relatively small compared to the beacon interval. PS hosts must remain active during the ATIM window so as to be notified by those intending senders, and may go to doze in the rest of the beacon interval if no one intends to send packets to it. It is assumed that the ad hoc network is fully connected, so time synchronization is not an issue.

In the beginning of a beacon interval, each mobile host will contend to send a beacon frame. Any successful beacon serves the purpose of synchronizing mobile host’s clocks as well as inhibiting other hosts from sending their beacons. To avoid collisions, each beacon is led by a random back off between 0 and $2^{CW_{\text{min}}} - 1$ slots.

After the beacon, a host with buffered packets can send a direct ATIM frame to each of its intended receivers in the PS mode. ATIMs are transmitted by contention in accordance with the DCF (Distributed Coordination Function) access procedure. A receiver, on hearing the ATIM, should reply an ACK and remain active. After the ATIM window, hosts having neither packets to send nor packets to receive can go back to the PS mode to save energy. The buffered unicast packets are then sent based on the DCF access procedure after the ATIM window. If the sender does not receive an ACK, it should retry in the next ATIM window. If a mobile host is unable to transmit its ATIM frame in the current ATIM window or has extra buffered
packets, it should retransmit ATIMs in the next ATIM window. To protect PS hosts, only RTS (request to send), CTS (clear to send), ACK, Beacon, and ATIM frames can be transmitted during the ATIM window.

3.4.2 Review of Quorum-based PS Protocol

IEEE 802.11 only considers single-hop MANETs. For multi-hop MANETs, the following two issues have to be addressed: wakeup prediction and neighbor discovery. Three solutions are proposed to solve these problems: the dominating awake-interval, the periodically-fully-awake-interval, and the quorum-based protocols. Among them, the quorum-based one has the merit of sending the fewest beacon signals. Below, we briefly review the quorum-based protocol. Still, the time axis is divided evenly into beacon intervals. Hosts can be arbitrarily asynchronous in their clocks. Beacon intervals are classified into two types:

- Quorum interval. It starts with a beacon window followed by a MTIM window. After the MTIM window, the host remains active (in monitor mode) for the rest of the beacon interval.

- Non-quorum interval. It starts with a MTIM window. After the MTIM window, the host may go to the PS mode if it has no packets to send or receive.

Similar to IEEE 802.11, the beacon window is for hosts to compete sending their beacons. The MTIM window is similar to the ATIM window – a host with buffered packets can compete to send notifications to intended receivers in the PS mode to wake them up. It is named so to reflect that it is used for multi-hop ad hoc networks.
3.4.3 Proposed Power Saving Technique

Two important things that must be viewed seriously when designing power-saving protocols are: clock synchronization and the neighbor discovery. Clock synchronization in a multi-hop UWB ad hoc network is really a tough task since there is no central control and packet delays may vary due to unpredictable mobility and radio interference. PS modes are typically supported by allowing low-power hosts wake up only in specific time. Without precise clocks, a host may not be able to know when other PS hosts will wake up to receive packets. Further, a host may not be aware of a PS host at its neighborhood since a PS host will reduce its transmitting and receiving activities. Such incorrect neighbor information may be detrimental to most current routing protocols because the route discovery procedure may incorrectly report that there is no route even when routes actually exist with some PS hosts in the middle.

Optimizing the power consumption is a tough task in UWB ad hoc networks. Due to technological advancements several low power hardware designs have been proposed for mobile devices. The wireless network interface consumes large amount of power. Since the wireless interface is often idle, this power could be saved by switching off the devices. Practically this is not an easy task. A node must be turned on not just to send packets but also to receive packets addressed to it and also to participate in higher layer routing protocols and control protocols. The cooperation between routing protocol and power saving technique is particularly very important to improve the performance of UWB ad hoc networks.

An efficient power saving technique should allow as many nodes to turn their receivers off, since even an idle receiver consumes as much power as an active receiver consumes. On the other hand, it should forward all the
packets from source to destination. To help this, enough nodes must stay awake to form a connected backbone. The power saving technique presented in this work allows the nodes to make periodic, local decisions on whether to sleep or stay awake.

### 3.4.3.1 Power saving modes

The power saving technique proposed in this work employs a channel condition estimator (CCE) to study the condition of the channel. For channel condition checking, the responses from the neighbor nodes are used as the basis. There could be three types of response from the neighbor nodes.

- CCE receives data correctly without error.
- CCE receives an erroneous packet.
- The node does not respond.

According to responses from a node, we can classify the channel into three classes:

- Good channel with data (GD),
- Good channel with no data (GN),
- No response (NR).

We define a sleep-awake duty cycle for a node based on the above 3 states of the nodes as given in equation (3.6).

\[
\text{Power save mode} = \begin{cases} 
  \text{sleep, if status = GN} \\
  \text{awake, if status = GD or NR}
\end{cases}
\]
3.4.3.2 Super frame structure

According to IEEE 802.11 terminology UWB ad-hoc networks are termed as Independent Basic Service Set (IBSS). An IBSS enables two or more mobile devices to communicate directly without the intervention of a centralized Access Point (AP). In an IBSS, the beacon frames, which contain the timing information, are managed using a distributed process. At the start of the beacon interval, all the mobile devices wake up and randomly contend to transmit the synchronization beacon. All the mobile devices in the IBSS, schedule the transmission of a beacon frame at a random time just after the target time identified by the beacon interval. After the first successful transmission of the beacon, all the other transmissions are cancelled. The mobile devices synchronize themselves with the first beacon they receive.

We assume a super frame consists of n beacon intervals. Each mobile node will enter the listen mode, only at one beacon interval during a super frame and will stay in PS mode during the rest of intervals (n-1). Each mobile node uses its MAC address as the input to a pre-chosen hash function, such as Secure Hash Algorithm-1 (SHA-1). Each beacon interval consists of three windows: Beacon Window (BW), Multi-hop Traffic Indication Map (MTIM) Window, and Data Window (DW). A mobile node will be active during MTIM and DW if it is in listen mode, or it is in PS mode.

To determine the beacon interval to enter into the listen mode, the power saving mechanism is based on the super frame structure and the use of hash function for a mobile node. It can be recalled that a mobile node will always awake and keep listening to the channel or transmit packets in the listen mode. In Power Saving mode, the mobile node will be awake in BW to send a beacon. If there is a packet to send, the mobile node will be awake in
the suitable MTIM window to send a MTIM frame to the destination and transmit the packet in the next DW.

Whenever a node want to send data to its neighbor node it should predict the time slot during which the neighbor node will be awake. The wake up prediction problem is solved in the proposed PS technique by using MAC address of neighbor node and hash function. Same hash function is shared by all mobile nodes and the next hop nodes in the routing table of a mobile node are neighbors of the node. So, the next hop node is checked from the routing table for a mobile node to transmit a packet. While the next hop being its neighbor of the mobile node, it can also make out the MAC address of the next hop. It then uses the hash function to get the beacon interval so that the next hop enters the listen mode which is the $i^{th}$ interval of the super frame. Then the MTIM frame and the packet in the MTIM window and DW window of the $i^{th}$ interval are sent by the mobile node. The mobile node will be able to listen to the MTIM frame since it will enter into the listen mode at the $i^{th}$ interval and the packets are received in the DW window.

Each node uses its MAC id to create a hash value. This hash value is mapped to the beacon interval for listening. When a node wants to transmit a packet, it first looks up the MAC id of next hop node from the routing table. It can then derive the hash value of that node which is common to all. By looking up the hash value, the node can get the beacon interval that the next hop will enter the listen mode.
Figure 3.9 Super frame

The Figure 3.9 illustrates the example of how a mobile node communicates with a neighbor node. Node A, B, C will enter the listen mode at beacon interval a, b and b, respectively. If node B wants to transmit a data frame to node C, it first calculates the interval that node C will enter the listen mode by the hash table. During the MTIM window of the beacon interval b, node B sends the MTIM frame to notice node C that a data frame will be sent to it. Upon receiving the MTIM frame, node C replies an ACK to node B. Since node A does not have any packets to send, it enters the sleep mode after BW window of interval b. Node B will enter the sleep mode after sending the
packet while node C can also enter the sleep mode if all data, notified in the MTIM window, have been received.

3.5 SUMMARY

This chapter described about the CBRP-PS, a cross layer based routing protocol with power saving scheme for UWB ad hoc networks. This protocol is a modification of AODV protocol by introducing a new routing metric in the route selection process. The routing metric includes parameters such as queuing delay, transmission delay, contention delay and available bandwidth. This protocol chooses different route for each of the four access categories mentioned in IEEE 802.11 since the requirements for each of the access categories are different form one another. For each of the four access categories the routing protocol chooses a path with low delay and high bandwidth among the available route to the destination. In addition to this a power saving technique has been proposed, which cooperates with the routing protocol to optimize the performance of UWB ad hoc networks. The power saving technique uses sleep and awake duty cycle based on the channel condition of the node. The node will be maintained in the awake mode only if it has the data to send otherwise, it will be maintained in the power saving mode.