Chapter 9
EPC: Efficient Gateway Selection for Passive Clustering in MWSNs

Abstract Passive clustering does not employ control packets to collect topological information in a Mobile Wireless Sensor Networks (MWSNs). The primary objective is to make Passive Clustering more practical, robust, and to minimize the quantity of cluster information on the data packets. In this chapter, we propose an intelligent gateway selection heuristic along with a time-out mechanism and an efficient passive clustering algorithm that employs an optimal number of gateways to reduce the number of rebroadcast and improve the QoS of the network. In this proposal, we avoid making frequent changes in cluster architecture, caused due to repeated election and re-election of cluster heads and gateways.

9.1 An Introduction to Clustering

Clustering is based on partitioning of a network into logical substructures called *clusters*. A cluster is a set of nodes which can be treated as a single entity during packet transmission. Each node in a cluster assumes a role depending on its position in the cluster and other topological information. The most important role in a cluster is played by the *Clusterhead*. A cluster cannot exist without a cluster head, as it is the only node which interacts with other clusters. In the clustering scheme, a node can send packets to other nodes of the same cluster, without the help of a cluster head. A node that belongs to more than one cluster becomes a *Gateway*. A gateway is responsible for routing packets across two clusters as they are reachable from both the clusters in a single hop. The remaining nodes are known as *Ordinary nodes*, and they do not have the privilege of routing packets to nodes of the other cluster. The cluster architecture is shown in Fig. 9.1.

The stability of the cluster architecture is primarily determined by the rules used for selecting cluster heads and gateways. These rules must be so designed, as to make minimal architectural changes in the network whenever its topology changes. The

---

K. R. Venugopal et al., *QoS Routing Algorithms for Wireless Sensor Networks*,

Fig. 9.1 Cluster architecture in MWSNs
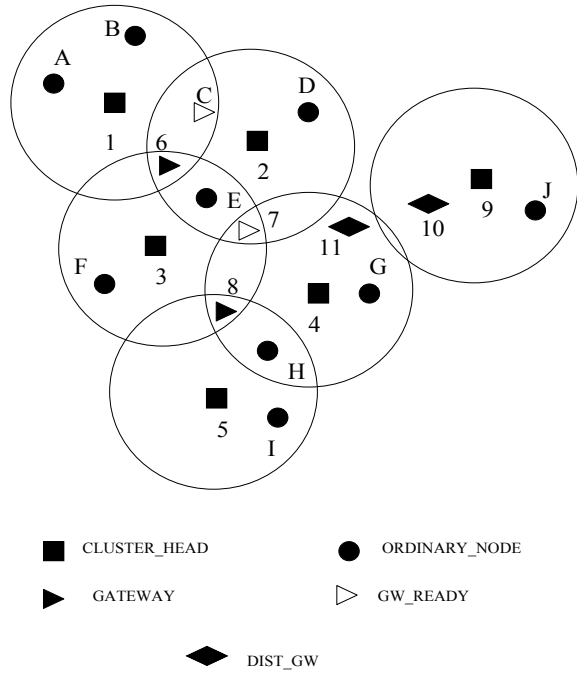
two most popular heuristics for cluster head or gateway selection are *Least Id* [1] and *First declaration wins rule* [2].

Routing protocols for WSNs can either be *flat or hierarchical*. Hierarchical routing protocols can reduce routing table storage and processing overhead, and therefore achieve better scalability. The most widely used two-level infrastructures are Dominant Set Pruning [3] and Clustering [1]. This work addresses the issue of scalability with respect to an increase in the number of control packets using passive clustering. This form of clustering is employed to reduce the number of rebroadcasts. Further, passive clustering works well only under ideal conditions. This can be justified by a number of peculiar cases of network topology, which are frequent in a WSN environment. These cases show that the control information piggy-backed on the data packets is alone not sufficient to maintain the cluster at all times. A survey [4] of different clustering algorithms for WSNs highlights their objectives, features, complexity, etc, and allso comparison of these clustering algorithms based on metrics such as convergence rate, cluster stability, cluster overlapping, location-awareness ,and support for node mobility.

9.2   Related Works

The problem of blind flooding is addressed in [5–8]. Several ideas have been proposed on reducing broadcast redundancy in wireless networks [9]. One of the most popular algorithm is *max-min d*-cluster formation [10]. This algorithm assumes that all links are bidirectional. It uses beacons to detect the presence of neighbors. If a node does not send beacons for a long time, it is assumed that it has either moved out or it has gone down. Though this algorithm works well, it should be triggered whenever the topology changes.

Bandwidth is a scarce resource in WSNs primarily because the nodes behave as routers in addition to being sources and destinations for the packets. Gupta and Kumar [11] proved that the performance of a wireless network decreases significantly with the increase in the number of nodes. This can be mainly attributed to the increase in the number of control packets with an increase in the number of nodes in the network. Also, movement of nodes causes failure of existing routes and fresh control packets will have to be used to detect new routes.

Grossglauser and Tse have proposed a mechanism to employ mobility of nodes to increase the capacity of WSNs using a different kind of packet-relaying approach. In this approach, a node hands-off packets to the destination only when it gets close to the packet's destination [12]. However, the packet-transit delay cannot be predicted as the nodes do not move in a predetermined way. Also, this approach cannot be used for real-time applications. Passive clustering uses ongoing data packets to extract information about the network. Thus, use of control packets is reduced. Passive clustering can be used to ensure scalability in a wireless network without resulting in a decline in its performance. Since bandwidth is limited in a wireless network, it is important to construct a virtual backbone consisting of only a subset of nodes that have the privilege to forward packets. Such a virtual backbone called *spine* plays an important role in routing, broadcasting, and connectivity management. An effort should be made to keep this backbone thin and connected [13–15].

Wan et al. [16] have described the formation of virtual backbone in ad hoc networks by means of a connected dominating set of nodes. In a connected dominating set (CDS), the number of nodes responsible for routing is reduced to the number of nodes in a CDS. Several heuristics have been put forth to find a minimum connected dominating set. Finding a minimum connected dominating set in a graph is NP-complete [17].

Clustering provides a mechanism to group the nodes. Clustering causes improvement in channel access, routing capabilities, code separation (among clusters), and bandwidth allocation [18, 19]. Clustering is classified into two types, active and passive. Some of the common algorithms employed in clustering are Least_ID, Highest_ID [20], Highest_connectivity [18], and LCC (Least cluster head change) [21].

The basic clustering algorithm was proposed by Lin and Gerla [1] based on the Least Id principle. It uses periodic control messages to maintain clusters and is known as active clustering. An innovative mechanism for cluster formation is provided in [2]. This method does not use any explicit control messages. Instead, it piggybacks

the control information on the out-going data packets and has the advantage of reducing the control overhead. But, relying only on data packets for control information introduces a number of problems.

Williams et al. [22] classified the protocols as Simple Flooding, Probability-Based Methods, Area-Based Methods, and Neighbor knowledge methods based on algorithmic complexity and each node's state need. The existing reactive protocols like DSR [23], AODV [24] have high rebroadcast messages and control overhead.

Jin et al. [25] develop a clustering protocol in which passive clustering is implemented in the first round followed by active clustering in the next rounds, this helps to satisfy the requirements of energy efficiency and QoS in WMSNs. A smart delay approach helps to distribute the cluster uniformly along with cluster head based on a node disjoint many to one multipath routing discovery algorithm, which is comprised of an optimal path searching process and multipath expansion process.

Liu et al. [26] develop an innovative vehicular clustering design combining hierarchical clustering using classical routing algorithms. The results are compared with Direct, LEACH, and DCHS and the new protocol reduces hot stops in WSNs.

Chen et al. [27] propose a directional geographical routing (DGR) with forward error correction (FEC) coding aimed at real-time videos transmitted over energy and bandwidth limited unreliable WSNs. The protocol employs multiple disjointed paths for video sensor node using H.26L and helps in load balancing, bandwidth aggregation, and fast packet delivery.

Xiao et al. [28] investigate the fundamental performance limits of medium access control (MAC) protocols for particular multi-hop, RF-based wireless sensor networks, and underwater sensor networks. A key aspect of this study is the modeling of a fair-access criterion that requires sensors to have an equal rate of underwater frame delivery to the base station. Tight upper bounds on network utilization and tight lower bounds on the minimum time between samples are derived for fixed linear and grid topologies.

Xiao et al. [28] study the working boundaries of medium access control (MAC) protocols in RF underwater sensor nodes. Modeling of a fair access benchmark is conducted that considers that sensors have an equal rate of underwater frame delivery to the base station. Derivation of upper and lower limits of network utilization and minimum time between samples for fixed linear and grid topologies are conducted.

In [29], sensor nodes are segregated into important and non-critical nodes without any extra transmission. This Passive clustering uses 2-b piggybacking and monitoring user traffic making initial flooding efficient. Also, Passive clustering aids in density adaptation and minimizes control overhead of sensor routing protocols and improves scalability.

In [31], the proposed HMR-LEACH algorithm (Hierarchical Multipath Routing-LEACH) improves election of cluster head and adopts multi-hop algorithm instead of one hop transmission data. When chooses transmission path, HMR-LEACH algorithm takes energy and distance into account and assigns a probability to each transmitting path by weight. Simulation result indicates that HMR-LEACH outperforms the LEACH algorithm and prolongs the life of the network dramatically.

Wang et al. [30] propose trust-based clustering called LEACH-TM; here, trust is used to select the cluster heads and CHs are used as routers. Results indicate improvement in reliability of data transmission and lifetime of networks. Hierarchical Multipath Routing-LEACH (HMR-LEACH) is proposed in [31]; the protocol improves cluster head selection and uses multi-hop approach instead of one-hop transmission. HMR-LEACH algorithm considers energy and distance and assigns a probability to each transmitting path by weight. Simulation result proves that HMR-LEACH exceeds the LEACH algorithm and increases the life of the network.

A cluster-based QoS multipath routing protocol (CQMRP) is proposed by Lu et al. [32], the protocol provides QoS responsive routes in a scalable and flexible way in WSNs by maintaining local routing information of other clusters rather than a global state data. A cluster-based multipath delivery scheme (CMDS) is proposed by Jing et al. [33], which uses cluster and multipath to boost the capability of load balance, and prolong the network lifetime.

Bhatia et al. [34] present an improved version of AODV called Multipath Energy Aware AODV routing (ME-AODV), which utilizes the topology of network to divide it into one or more logical clusters and restricts the flooding of route request outside the cluster. The mesh links created at the time of cluster formation are used to decrease the routing path. ME-AODV uses nodes of the same cluster to share routing information, which significantly reduces the route path discovery. Since ZigBee routing is based on the shortest-hop count, which causes overuse of a small set of nodes and hence decreases node as well as network lifetime. They also propose a mix of Ad hoc On-demand Multipath Distance Vector routing (AOMDV) and Minimal-Battery Cost Routing (MBCR) as an extension to AODV to increase the lifetime of network. Bidai et al. [35] propose a multipath routing where multiple paths are used simultaneously to transfer data between a source and the sink. Also they propose Z-MHTR, a node disjoint multipath routing extension of the ZigBee hierarchical tree routing protocol in cluster-tree WSN.

A augmented version of AODV called Multipath Energy Aware AODV routing (ME-AODV) is proposed by Bhatia et al. [34]; here; the algorithm uses the topology of network to partition it into one or more logical clusters and diminish the flooding of route request outside the cluster. The mesh links built at cluster formation are used to reduce the routing path length. ME-AODV uses nodes of the same cluster to distribute routing information, this naturally reduces the route path exploration. The protocol uses Ad hoc On-demand Multipath Distance Vector routing (AOMDV) and Minimal-Battery Cost Routing (MBCR) as an expansion to AODV to boost the lifetime of network.

A Secure Cluster-based Multipath Routing protocol was proposed by Almalkawi et al. [36] for multimedia traffic that needs to deliver different data types of high data rate. The protocol uses the cluster heads and the optimized multiple paths to maintain timeliness and reliability of multimedia data communication with minimum energy requirements, additionally a secure key handling scheme prevents against attacks.

An innovative heuristics is proposed by Hafid et al. [37] which used passive clustering and achieves balanced energy consumption among the network nodes. The proposed scheme does not have stringent requirements such as clock synchronization

and does not generate extra control traffic and can be seamlessly used with other clustering protocols.

Bandyopadhyay et al. [38] have used stochastic geometry with a distributed, randomized algorithm for generating clusters of sensors. This helps in reducing the total transmissions required to gather one sample from each sensor. The proposed protocol performs better with respect to energy costs than the max-min d-cluster algorithms.

9.3   Network Model

9.3.1   Definitions

- A Free Tree or an *Unrooted Tree* in a Mobile Wireless Sensor Network is defined as a connected graph with no cycles. A graph $G(V, E, n)$ is a free tree if G is connected, contains no cycles, and has n-1 edges.
- A Cluster is a group of nodes that is treated as a single entity, with reference to routing of packets.
- A Cluster Set is the set of all Cluster IDs to which a node belongs.
- A Cluster Head is a representative of the cluster, holding the privilege of forwarding packets to other members in that cluster.
- A Gateway is a node that connects overlapping clusters, capable of receiving/forwarding packets from/to the Cluster Heads of all the clusters to which it belongs.
- A Gateway Ready node (*gw_ready*) is a candidate gateway that has not yet detected enough gateways, it can become an ordinary node with the discovery of enough gateways.
- A Critical Path is a link between any two nodes or any two clusters, the loss of which results in loss of connectivity between the participating nodes or clusters.
- The Control Overhead is defined as the ratio of the number of control packets and the number of packets received by the destination node.
- The Competition Count (C_c) of a node is defined as the number of times a node competes for the Gateway status. It is set to zero, each time a node acquires either *initial or cluster head* status.
- The Redundancy Factor (R_f) of the network is defined as the maximum number of common clusters that any two neighboring gateways can connect. It has a minimum value of one and a maximum value of five, since a node cannot be a member of more than six clusters.

Fig. 9.2 Simple wireless
network
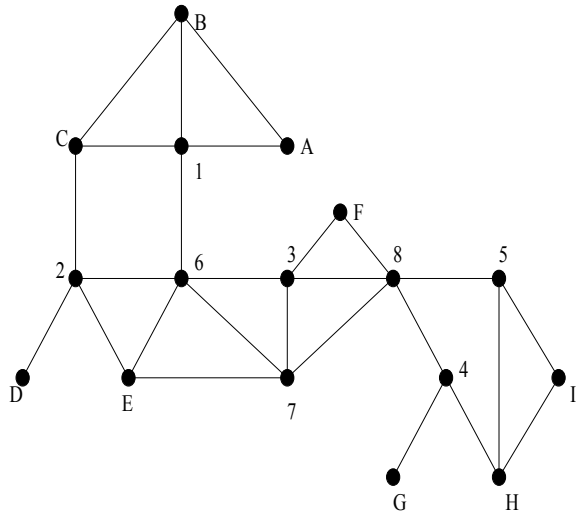
### 9.3.2   Mobile Wireless Sensor Network as a Graph

Let $G = (V, E)$ be a graph representing the topology of the network of mobile nodes,
where E is a subset of $\{(v_i, v_j) \mid v_i, v_j \in V \wedge v_i \neq v_j \}$, set of finite links.

Figure 9.2, is an undirected graph representing a wireless network. A bidirectional
link exists between two nodes if they are within the transmission range. Further, the
network becomes a free tree [39] after passive clustering is applied to the network.
This is the case when there are no redundant gateways. Only the nodes that lie in
the path from source to destination in a free tree forward packets, while all the other
nodes in the network are passive. In Fig. 9.3, the cluster heads are (1, 2, 3, 4, 5) and
the gateways are (6, 8). Packets are routed through a series of ClusterHeads and
Gateways between the source and destination.

9.4   Problem Definition

Given a wireless sensor network $G_w(V, E, n)$ of a finite set of nodes, V = {
$v_1, v_2, ..., v_n$ } and a finite set of links E = { $(v_i, v_j) \mid v_i, v_j \in V \wedge v_i \neq v_j$ }, a
link is said to exist between two nodes v_i and v_j if they are within the transmission
range of each other. The objectives are to

- account for mobility among nodes and to avoid loss of connectivity,
- reduce the number of rebroadcasts by reducing the number of redundant gateways
  between the overlapping clusters,

Fig. 9.3 Free tree
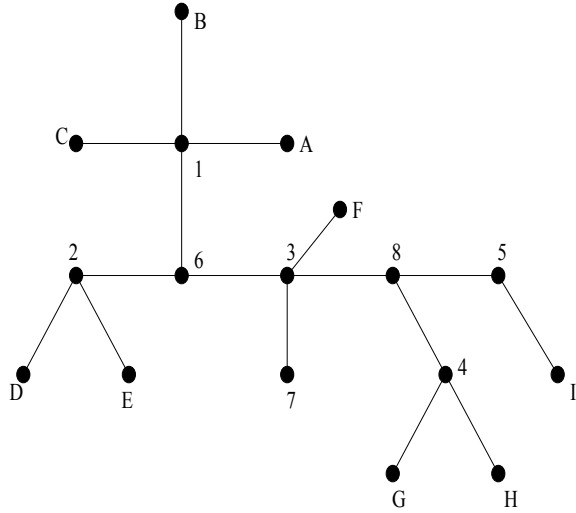
- ensure full coverage of all nodes within the given area using minimum number of clusters,
- reduce the quantity of control information loaded on the data packets,
- make the cluster architecture more stable,
- improve the QoS of the network.

   The assumptions are

- The network model assumes that the sensor nodes move in a two-dimensional area.
- The logical link layer is assumed to be free from errors.
- Each node is a unit disk. All nodes have equal transmission range.
- All transmitted packets are received in the order of their transmission.

9.4.1 Topological Problems Associated with Passive Clustering

Problem 1: An ordinary node may move into other clusters and generate a spurious gateway.

   In Fig. 9.4, *w* belongs to C_2 and has information about head of C_2. If it moves to C_1 as shown in Fig. 9.4, it starts receiving packets from the head of $C_1(Ch1)$, and updates its cluster table to have information about C_1 while retaining information about C_2. In this situation, it enters into *gw_ready* state and further, it may become a Gateway.

Fig. 9.4 Ordinary node
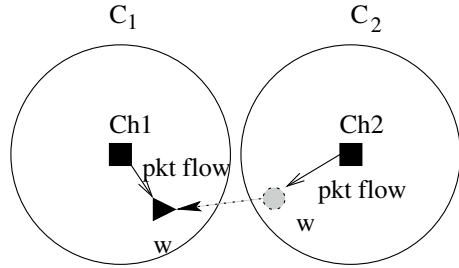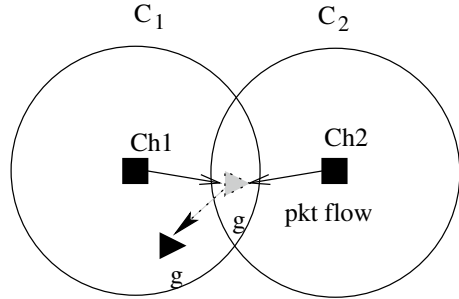moving into other cluster

Fig. 9.5 Movement of
gateway

This is highly unacceptable, because (i) it may cause the real gateway candidate
to become *ordinary*, resulting in the loss of connectivity between two clusters. (ii)
it will have privilege to rebroadcast, which it should not have, resulting in an increase
in the number of rebroadcasts and hence an increase in the traffic.

*Problem 2: A gateway may move from the intersection area to a single cluster without
relinquishing the status of the Gateway.*

In Fig. 9.5, g is a gateway between $Ch1$ and $Ch2$ and it receives packets from both
these cluster heads. Suppose g moves into C_1, now it belongs to only one cluster and
hence must become an ordinary node. Instead, it continues to assume that it belongs
to two clusters and hence will stay in gateway state, rebroadcasting the incoming
packets. In passive clustering, a node gets good news (addition of new nodes or
clusters) more easily than the bad news (a node going down or cluster head going
out of the cluster).

Problem 3: Spurious generation of multiple gateways.

In a dense network, there will be a number of nodes in the intersection region
of any two clusters. All of them compete for the *Gateway* status and the one with
the *least id* wins. However, if the cluster sets of all the competing gateways are not
exactly the same, then all of them become gateways. This creates redundant gateways
and causes a broadcast storm in the wireless network.

Problem 4: Formation of redundant clusters.

During the initial setup, all the nodes that receive packets from the ordinary nodes
become cluster heads. This results in dense and overlapped clusters.

Problem 5: Problems associated with the cluster head moving out of a cluster.

If an ordinary node does not receive packets from its cluster head for a long time, it assumes that cluster head is still present but it has no packets to send. An ordinary node has no privilege to rebroadcast, hence it relays on its cluster head to route packets to a distant node. Now, the ordinary node knows nothing about its cluster head's absence continues to send packets to the cluster head to route them to the destination resulting in the loss of packets and redundant broadcasts by the source. This problem can be solved only by electing a new cluster head among the other members of that cluster. This will not happen, because a node changes its state only on receiving packets from the other nodes. This is the case of a deadlock.

9.5   Algorithm EPC (Efficient Passive Clustering)

In the cluster architecture, a node can be in any of the following states: *initial, ordinary_node, gw_ready, gateway, dist_gw, cluster_head* as in Fig. 9.1. The algorithm is as follows:

  (i) At the start, all the nodes are in the *initial* state and they are assigned a unique ID.
 (ii) The source node sends a packet to all its neighbors and declares itself as a Cluster Head.
(iii) If the *initial* node hears from a *cluster_head*, it becomes an *ordinary_node*.
(iv) If a node (other than *initial* and *cluster_head*) hears from a non-Cluster Head,

   (a) It checks whether the sender node was a Cluster Head before. This check is carried out by scanning its cluster table in search of the sending node's ID. (Cluster Table maintains a list of Cluster Heads reachable from the node).
   (b) If the sender node was a Cluster Head before, then its entry is cleared from the cluster table of the receiving node. Packets from this node are not forwarded henceforth.
   (c) If the cluster set of the node becomes null, the node changes its state to *cluster_head*.

  (v) Contention between the Cluster Heads is resolved by the Least ID method. This is because the Cluster Head does not monitor the cluster.
 (vi) An *ordinary_node* receiving packets from more than one *cluster_head* enters into *gw_ready* (gateway ready) state.
(vii) A *gw_ready* node becomes a *gateway* based on the *Intelligent Gateway Selection Heuristic.*
(viii) A *gateway* on receiving packets from other *gateway* or *gw_ready* nodes may change its state based on *Intelligent Gateway Selection Heuristic*.
 (ix) If an *ordinary_node* hears from another *ordinary_node* or *dist_gw* of another cluster, and if there are no gateways in the intersection area, it becomes a Distributed Gateway (*dist_gw*).
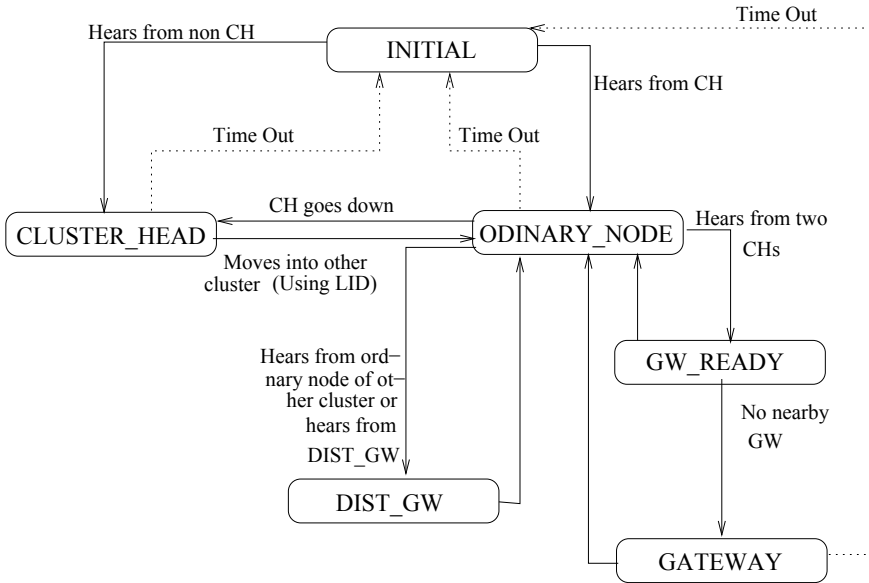
Fig. 9.6   State diagram of efficient passive clustering algorithm

  (x) If a *dist_gw* hears from *gateway* or *gw_ready* of the same cluster-pair, it becomes *ordinary_node*.
 (xi) No node remains in the intermediate state for a long time.
(xii) If the node times out (using *Special Time-out Mechanism*), its state is set to *initial*.

The nodes change their states based on the status of the last sending node. A node increments its Competition Count whenever it enters into gateway selection process. Unlike the role played by the Cluster Head in other prevailing clustering algorithms, the Cluster Head does not monitor the cluster and it does not contain any extra information. The Cluster Head is different from the other nodes; in that, only the cluster head has the privilege to rebroadcast. The Cluster Head does not monitor the cluster members. If it does, it may become a bottleneck in the cluster architecture. There is an intermediate gateway ready state (*gw_ready*), which reduces the chances of more than one node becoming *gateway* between the same clusters. Figure 9.6 shows the state diagram of Efficient Passive Clustering Algorithm.

9.5.1   Intelligent Gateway Selection Heuristic

Gateways are the intermediate nodes that connect clusters and they have the ability to rebroadcast. The number of rebroadcasts is directly proportional to the number of

gateways. Redundant gateways increase the number of rebroadcasts. This is undesirable in WSNs because of the limited bandwidth, power, and Qos constraints. Hence selection of an optimal number of gateways is very essential. Here, we give a heuristic that selects an optimum number of gateways. The original Passive Clustering algorithm selects gateways using the Least_ID principle. This means whenever there is a contention, the one with the lesser ID wins. This method does not consider the topological situation at the time of the decision.

Given that the nodes are mobile, there is a high probability that well-connected gateways will lose their *gateway* status when they compete against the ones having Least_ID. Also, simulation results show that there are generally four or five clusters sharing the same gateway in a dense Wireless Sensor Network. It would be disadvantageous to lose such a well-connected gateway. The Intelligent Gateway Selection Heuristic takes into account the history of competitions a node underwent using Competition Count (C_c) while deciding its status. The Competition Count (C_c) of a node is the number of times a node competes for the *gateway* status. It is set to zero, each time a node acquires either *initial* or Cluster Head status.

Sometimes, it may be necessary to incorporate redundant gateways between clusters in a mobile network. This may be done to ease the traffic flow between clusters to control congestion. This is done by setting the Redundancy Factor (R_f) to a higher value. The Redundancy Factor (R_f) of the network is the maximum number of common clusters that any two neighboring gateways can connect. Since competing gateways can hear each other, they will not compete until the number of gateways in the intersection area is greater than the Redundancy Factor (R_f). Thus, there is a trade-off between optimal connectivity and congestion in Wireless Sensor Networks. For a thin backbone wireless network, Redundancy Factor (R_f) must be set to 1.

To accommodate this heuristic, the information about cluster set of the node (i.e., the set of clusters to which it belongs in case of gateways and distributed gateways), *id* of the node, type of the node, and NOC (size of cluster set) are included in both the packets and the nodes. Competition Count (C_c) and Redundancy Factor (R_f) have to be set in the individual nodes in the WSN. Competition Count (C_c) is reset as soon as the node takes up the *initial* or the Cluster Head state. It is used only when the node is in the other states. It does not make the algorithm inefficient when there is mobility in the network because when a gateway goes far away from the clusters due to its movement, it has a high probability of acquiring either the *initial* or the Cluster Head state. And, the process starts all over again. The heuristic is divided into four cases. In the gateway selection process, these cases do not occur simultaneously.

Case 1: Only node in the intersection area: When the node receives packets from two cluster heads, it enters into the *gw_ready* state and it becomes a gateway.

Case 2: Two or more nodes in the region of intersection of clusters: When a node receives packets from the other Gateway or *gw_ready*, it compares the cardinality of its cluster set with that of the sending node. If both the sets are equal, then the one with the least ID becomes the gateway.

Case 3: The cluster-set of one node in the intersection area is a subset of the cluster-set of another node: Suppose there are two nodes in the intersection area of clusters

such that the cluster-set of one node is a subset of the cluster-set of another node. Then the node with the superset will be selected as the gateway. Every gateway performs this comparison by intercepting the packets from its neighboring gateways.

Case 4: When two nodes such that cluster-set(node1)~cluster-set(node2)≠0: In this case, both the nodes have a tendency to declare themselves as gateways when they receive packets from each other. But this may not be optimal, since there may be a difference of just one cluster between the cluster-sets. This leads to the creation of redundant gateways. Clusters are said to possess redundant Gateways, when a cluster is connected to its neighboring cluster by more than one Gateway. The receiving node computes the number of clusters that are common to both the sending node's and receiving node's cluster-sets. If this value is less than or equal to the Redundancy Factor (R_f), then both nodes are designated as Gateways. Otherwise, the node with the least Competition Count (C_c) is designated as the Gateway.

The logic is that, if a node has competed at least once, then there must be one more node in that intersection area, which is capable of covering most of the clusters the former node could connect to. Thus, the other node is given a chance to become a Gateway and extend the connectivity. This heuristic is adaptable to the changes in network topology and network density. The heuristic intelligently selects the best gateway in the intersection area of the two or more clusters.

For instance, in Fig. 9.3, consider the following gateways and their cluster-sets: $G_1(1, 2, 3, 4, 5)$, $G_2(2, 3, 4, 5, 6)$, $G_3(3, 4, 5, 6, 7)$, $G_4(4, 5, 6, 7, 8)$, and $G_5(5, 6, 7, 8, 9)$. If the gateway redundancy factor, R_f is set to 1, only G_1 and G_5 remain as gateways because there is only one cluster common between their cluster-sets ($R_f = 1$). Otherwise, all five would be chosen as gateways. Therefore, there is a reduction in the number of gateways by three. We analyze the proposed heuristics and prove that the heuristics are optimal. And we also analyze the time complexities of our algorithm.

Lemma 1: The EPC algorithm maintains connectivity.
Proof: The number of gateways selected by the EPC algorithm is optimal, since it satisfies the following conditions.

(i) Only one gateway is selected between each cluster pair, unless there is a loss of critical path between a cluster pair. According to *Case 1* and *Case 2* when the cluster sets of more than one node are same, only one of them is selected as the gateway. Also, according to *Case 3* when the cluster set of one node is a subset of the cluster set of the other node, the node having the superset as the cluster set is elected as a gateway.

(ii) At least one gateway is selected between each cluster pair, unless there is no node common to both the clusters.

According to the *Cases 1, 2, and 3* at most one node is selected between cluster pairs. *Case 4* guarantees that optimal number of gateways are chosen between overlapping clusters, by setting the Redundancy Factor (R_f) to a suitable value.

Lemma 2: Number of gateways selected by our algorithm is minimal when $R_f = 1$.
Proof: This is proved by contradiction. Assume that there are two or more gateways between two clusters. If this happens, then the Gateway Selection Heuristic will

ensure that only one of competing gateways retains the *gateway* status as R_f is set to 1. A distributed gateway is selected between a cluster pair only when there is no node in the intersection area of the clusters. Thus, minimum number of gateways are selected to maintain overall connectivity. Because of the nature of passive clustering, more than one node can become gateway simultaneously. But, this situation is overcome by using an intermediate state, between ordinary and gateway states, known as *gw_ready*. A node in *gw_ready* state changes its status to *initial*, if it receives packets from another gateway.

Time Complexity:

When each node receives the packets from at least one of its neighbors, the network becomes stable. The time taken in the worst case is $O(L + Avg\_neighbor)$, where L is the diameter of the network, and $Avg\_neighbor$ is the average number of neighbors of each node. The time complexity of our algorithm is $O(N)$.

9.5.2   Time-out Mechanism

There is no special thread for implementation of time-out mechanism in the nodes and the system clocks of all the nodes need not be synchronized. Every node calculates the time interval between reception of successive packets, asynchronously. If this interval is greater than Time-out, the node goes into the *initial* state and it clears all the stored information. This recalculation and re-clustering is significant as the node may have been isolated for a long time. It may be necessary to change its state relative to its immediate neighbors.

The algorithm provides solutions to all the problems mentioned in the previous section. The solution for the movement of ordinary nodes and gateways is to allow the gateways to send periodic messages to all the cluster heads to check whether the cluster heads have moved. If not, the information corresponding to each non-existing cluster head is removed from the node's cluster table. This will change the status of the sending node, which is desirable. Although control packets are used, they are restricted to gateways only and specifically for collecting information about cluster heads. So, exchanging a small number of control packets does not disturb the passiveness of the algorithm. The advantages gained through incorporating this flexibility in passive clustering are significant. Especially, if the clustering is built on *reactive* protocols like AODV, there is no need to send *hello packets*. There is no way to avoid the formation of redundant clusters during the initial setup. But once this happens, clusters are reformed by making use of the EPC algorithm. The algorithm reduces the number of clusters and also makes each of the clusters thus formed, more stable. A special time-out mechanism is used to solve the problem of cluster head moving out of the cluster.

9.6 Performance Analysis

Passive clustering is simulated in the *ns*-2 simulation environment. The efficiency of the EPC algorithm in reducing the number of rebroadcasts is illustrated. Simulation results reveal that there is a reduction in the control overhead by the application of EPC algorithm. Also, the number of gateways and the number of cluster heads are reduced. The IEEE 802.11 DCF and two-ray propagation model is employed for simulation. The broadcast range for each node is 250 meters. Both the simple passive clustering and improved passive clustering algorithm are implemented on AODV.

By employing the efficient gateway selection heuristic, with the Redundancy Factor set to one, a minimal number of gateways are chosen. Not more than one gateway is chosen between two clusters. The gateways form a *thinner* backbone while maintaining the connectivity among all the clusters within the designated area.

Also, inclusion of more nodes will not increase the number of clusters and the number of gateways will remain fairly constant. Hence, the gateway curve of our algorithm is linear compared to that of the simple passive clustering as shown in Fig. 9.7. The EPC algorithm forms and reforms the clusters in such a way that there will be no two cluster heads that are reachable in one hop. This reduces the number of cluster heads and thus reducing the number of overlapped clusters in the wireless sensor network. Figure 9.8 shows that the EPC algorithm reduces the number of cluster heads compared to simple passive clustering.

The Number of Rebroadcasted Packets (NRP) is the total number of packets that are broadcast and rebroadcast from all the nodes, irrespective of their states. This is a very important parameter because an increase in NRP results in the broadcast storm. The number of rebroadcasts is directly proportional to the total number of cluster
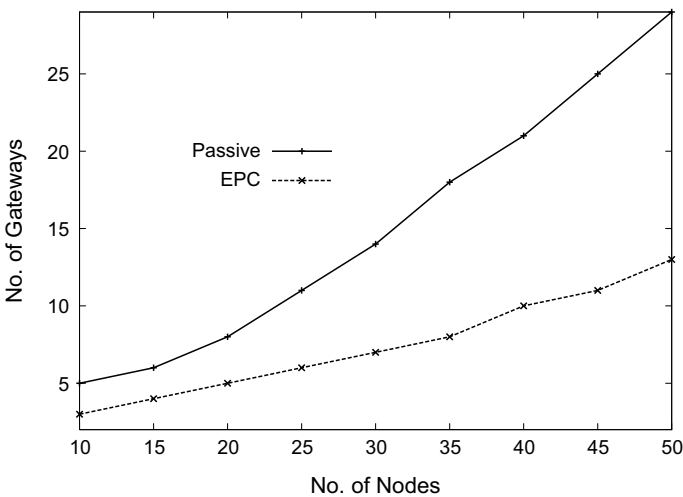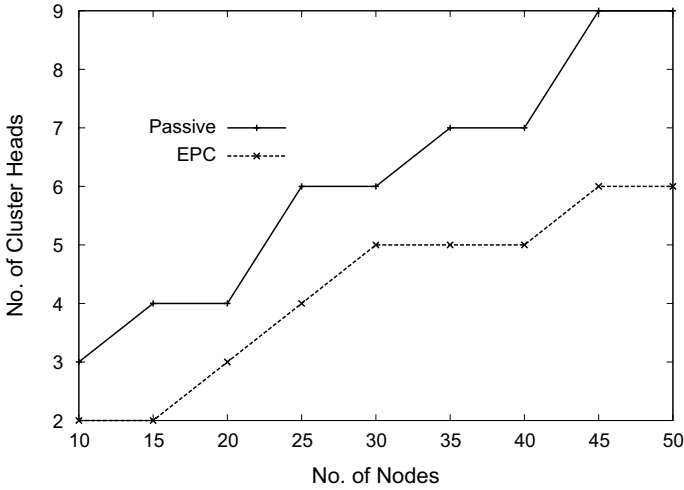

Fig. 9.7 No. of gateways versus no. of nodes

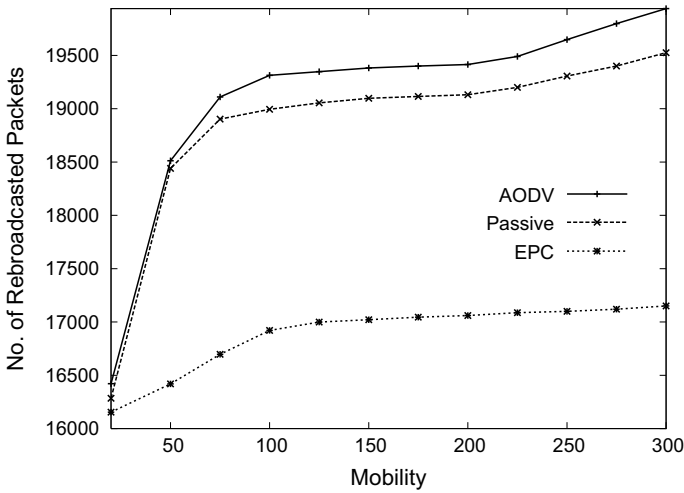**Fig. 9.8** No. of cluster heads versus no. of nodes

Fig. 9.9 No. of rebroadcasted packets versus mobility

heads, gateways, and distributed gateways in the wireless network. This is because in passive clustering, only the cluster heads, gateways, and distributed gateways of a cluster have the privilege to forward the packets they receive. As depicted in Fig. 9.9, the number of rebroadcasts is the lowest for EPC. With the application of the gateway selection heuristic and other improvements over passive clustering, the number of rebroadcasts is reduced considerably. The curve corresponding to our EPC algorithm is more stable (flatter) than others. The number of rebroadcasts is the highest for AODV since every node forwards the incoming packets. The number
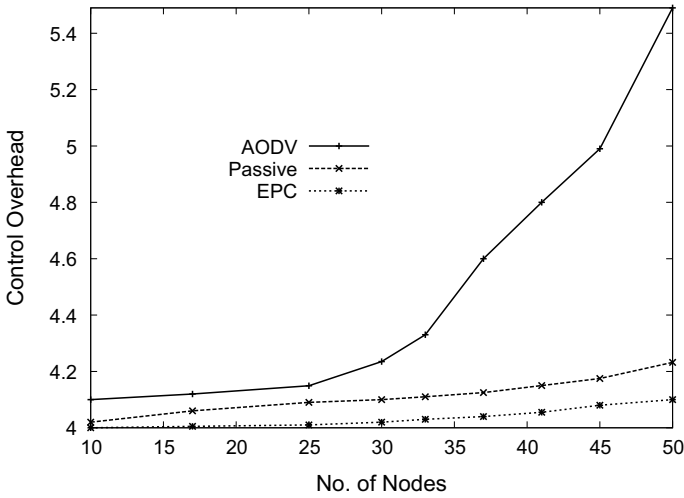
Fig. 9.10 Control overhead versus no. of nodes

of rebroadcast messages in passive clustering is lower than AODV, but much higher than EPC, and obtain better QoS in the network.

As Fig. 9.10 shows, in the EPC algorithm, control packets are employed only by the gateways. Even though we are using explicit control messages, the result of these messages is to make the clustering much more stable and hence reduce the control messages. Thus, the total control overhead of the EPC algorithm is lower than the other cases. In passive clustering, there are no explicit control packets, but the clustering mechanism reduces the generation of control packets. The control overhead is higher than the EPC algorithm. The control overhead curve for AODV is steep, since every node sends control packets to its neighbors and as the number of nodes increase, the number of control packets also rises exponentially.

9.7 Summary

The simulation results show that the EPC Algorithm is inexpensive, efficient, and stable. The number of clusters is found to be optimal in dense wireless sensor networks. This work has proved that Passive Clustering becomes practically possible by implementing the intelligent gateway selection heuristic and on-demand timeout mechanism. Frequent changes in cluster architecture are avoided by precluding repeated re-election of cluster heads. This improves the QoS network performance. Future work can be carried out by employing distributed gateways to route packets.

References

1. C.R. Lin, M. Gerla, Adaptive clustering for mobile wireless networks. In: IEEE J. Select. Areas Commun. 1265–1275 (1996)
2. Y. Yi, M. Gerla, T.-J. Kwon, *Efficient flooding in Ad Hoc networks using on-demand (passive) cluster formation* (Proc, MobiHoc, 2002)
3. F. Dai, J. Wu, Distributed dominant pruning in Ad hoc wireless networks. Florida Atlantic University, Technical Report TR-CSE-FAU-02-02 (2002)
4. A.A. Abbasi, M. Younis, A survey on clustering algorithms for wireless sensor networks. Comput. Commun. **30**(14), 2826–2841 (2007)
5. Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, J.-P. Sheu, The broadcast storm problem in a mobie Ad Hoc network, in *Proceedings of the Mobicom* (1999)
6. Y.-C. Tseng, S.-Y. Ni, E.-Y. Shih, Adaptive approaches to relieving broadcast storms in a wireless multihop mobile Ad Hoc network, in *Infocom* (2001)
7. A. Qayyum, L. Viennot, A. Laouiti, Multipoint relaying: an efficient technique for flooding in mobile wireless networks, in *INRIA Report* (2000)
8. H. Lim, C. Kim, *Flooding in wireless Ad hoc networks* (IEEE Comput, Commun, 2000)
9. W. Lou, J. Wu, On reducing broadcast redundancy in Ad hoc wireless networks. IEEE Trans. Mob. Comput. **1**(2), 111–123 (2002)
10. A.D. Amis, R. Prakash, T.H.P. Voung, D.T. Huynh, Max-min D-cluster formation in wireless Ad Hoc networks, in *IEEE INFOCOM* (2000)
11. P. Gupta, P.R. Kumar, The capacity of wireless networks. IEEE Trans. Inform. Theory **46**, 388–404 (2000)
12. M. Grossglauser, D.N.C. Tse, Mobility increases the capacity of Ad Hoc wireless networks, in *IEEE/ACM Transactions on Networking*, vol. 10 (2002)
13. V. Bhargavan, B. Das, Routing in Ad Hoc networks using minimum connected dominating sets, in *International Conference on Communications'97* (1997)
14. B. Das, R. Shivakumar, V. Bhargavan, Routing in Ad Hoc networks using a spine, in *International Conference on Computers and Communication Networks'97* (1997)
15. R. Shivakumar, B. Das, V. Bhargavan, An improved spine-based infrastructure for routing in Ad Hoc networks, in *IEEE Symposium on Computers and Communication Networks'98* (1998)
16. P.-j. Wan, K.M. Alzoubi, O. Frieder, Distributed construction of connected dominating set in wireless Ad Hoc networks, in *Proceedigs of IEEE INFOCOM '02* (Chicago, USA, 2002)
17. M.V. Marathe, H. Breu, H.B. Hunt III, S.S. Ravi, D.J. Rosenkrantz, *Simple Heuristics for Unit Disk Graph* (Addison-Wesley, Narosa, 1995)
18. M. Gerla, J.T.-C. Tsai, Multicluster, mobile, multimedia radio network. ACM J. Wirel. Netw. **1**(3), 255–265 (1995)
19. K. Gilhousen, I.M. Jacobs et al., On the capacity of a cellular CDAM system. IEEE Trans. Vehicul. Technol. 303–312 (1991)
20. A. Ephremides, J. E. Wieselthier, D.J. Baker, A design concept for reliable mobile radio networks with frequency hopping signaling, in *Proceedings of the IEEE* (1991), pp. 56–73
21. C.C. Chiang, H.K. Wu, W. Liu, M. Gerla, Routing in clustered multihop, mobile wireless networks with fading channel, in *The Proceedings of the IEEE Singapore International Conference on Networks* (1996), pp. 197–211
22. B. Williams, T. Camp, *Comparison of broadcasting techniques for mobile Ad Hoc networks, in Proceedings of the MOBIHOC'02* (Colorado School of Mines, Golden, Colorado, 2000)
23. D.B. Johnson, D.A. Maltz, Dynamic source routing in Ad Hoc networks. Mob. Comput. 153–181 (1996)
24. C. Perkins, E. Royer, S. Das, *Ad hoc on Demand Distance Vector (AODV) Routing* (Internet draft, IETF, 1999)
25. R.C. Jin, T. Gao, J.Y. Song, J.Y. Zou, L.D. Wang, Passive cluster-based multipath routing protocol for wireless sensor networks. Wirel. Netw. **19**(8), 1851–1866 (2013)
26. Y. Liu, N. Xiong, Y. Zhao, A.V. Vasilakos, J. Gao, Y. Jia, Multi-layer clustering routing algorithm for wireless vehicular sensor networks. IET Commun. **4**(7), 810–816 (2010)

27. M. Chen, V.C. Leung, S. Mao, Y. Yuan, Directional geographical routing for real-time video communications in wireless sensor networks. Comput. Commun. **30**(17), 3368–3383 (2007)
28. Y. Xiao, M. Peng, J. Gibson, G.G. Xie, D.Z. Du, A.V. Vasilakos, Tight performance bounds of multihop fair access for MAC protocols in wireless sensor networks and underwater sensor networks. IEEE Trans. Mob. Comput. **11**(10), 1538–1554 (2012)
29. T.J. Kwon, M. Gerla, V.K. Varma, M. Barton, T.R. Hsing, Efficient flooding with passive clustering-an overhead-free selective forward mechanism for Ad hoc/sensor networks. Proc. IEEE **91**(8), 1210–1220 (2003)
30. W. Wang, F. Du, Q. Xu, An improvement of LEACH routing protocol based on trust for wireless sensor networks, in *5th International Conference on Wireless Communications, Networking and Mobile Computing* (2009), pp. 1–4
31. G. Liu, C. Wei, A new multi-path routing protocol based on cluster for underwater acoustic sensor networks, in *2011 International Conference on Multimedia Technology* (2011), pp. 91–94
32. X.C. Lu, H.Y. An, Y.X. Peng, W. Peng, A cluster-based QoS multipath routing protocol for large-scale MANET. Ruan Jian Xue Bao (J. Softw.) **18**(7), 1786–1798 (2007)
33. Y. Jing, X. Mai, X. Jinfu, X. Baoguo, H. Lu, A cluster-based multipath delivery scheme for wireless sensor networks, in *2nd IEEE International Conference on Broadband Network Multimedia Technology* (2009), pp. 286–291
34. A. Bhatia, P. Kaushik, A cluster based minimum battery cost AODV routing using multipath route for Zigbee, in *2008 16th IEEE International Conference on Networks* (2008), pp. 1–7
35. Z. Bidai, H. Haffaf, M. Maimour, Node disjoint multi-path routing for ZigBee cluster-tree wireless sensor networks, in *2011 International Conference on Multimedia Computing and Systems* (2011), pp. 1–6
36. I.T. Almalkawi, M. Guerrero Zapata, J.N. Al-Karaki, A secure cluster-based multipath routing protocol for WMSNs. Sensors **11**(4), 4401–4424 (2011)
37. A.S. Hafid, F. Chender, T.J. Kwon, Energy aware passive clustering in wireless mobile networks. in *2008 International Wireless Communications and Mobile Computing Conference* (2008), pp. 535–540
38. S. Bandyopadhyay, E.J. Coyle, Minimizing communication costs in hierarchically-clustered networks of wireless sensors. Comput. Netw. **44**(1), 1–16 (2004)
39. D.E. Knuth, *Fundamental Algorithms* (Addison-Wesley, Narosa, 1985)