Summary of Thesis

on

A Multipath Routing Protocol for Ad Hoc Networks

Submitted for the award of
DOCTOR OF PHILOSOPHY
in
COMPUTER ENGINEERING

By

RAJ KUMAR MANOCHA
(Registration Number:SU/SCE&IT/Ph.d./PT/09/03)
(Enrollment Number: 2009060003)

Under Supervision of

Dr. A. K. Srivastava
Principal General,
Institute of Engineering & Technology,
Alwar, Rajasthan

Dr. R. P. Agarwal
Vice Chancellor,
Shobhit University
Meerut, U.P.
In this thesis two protocols have been proposed, one at Medium Access Control (MAC) layer and the other at Network Layer of Open System Interconnection (OSI) Model. The protocol at MAC layer aims to prevent collisions due to interference at MAC layer with some modifications in IEEE 802.11 when operating over Frequency Hop Spread Spectrum (FHSS). The protocol at network layer is an AODV-based Node-Disjoint Multipath routing protocol for Ad Hoc Networks which computes paths that are out of each other’s interference range, that avoid congestion in all paths and have a good stability against mobility of nodes. Simulation on network simulator ns-2 shows that when both these protocols operate in conjunction with each other, the throughput of the system increases by approximately 22% as compared to AODV operating over 802.11.

The MAC layer protocol named as MAC-CPI.A prevents collisions due to interference by ensuring that no node begins its transmission i.e., Request To Send (RTS) frame if any of current transmitter-receiver pair is within its ‘maximum interference range’. Interference is sum of signals at a receiver node due to other transmitters operating con-currently within its carrier sensing range (CSR). The ‘maximum interference range’ is a non-linear function of five parameters: average distance between a transmitter and its next hop receiver – ‘hd’, minimum path-loss constant in any part of network – $\alpha$, minimum acceptable Signal to Interference and Noise Ratio (SINR) threshold ($\beta$) so that a receiver can always decipher the signals of its transmitter, the carrier sensing range – which limits the maximum number of transmitter-receiver pairs that can exchange data in parallel, and maximum Noise (N) in any part of the network. The values of ‘maximum interference range’ have been computed and tabulated for different values of above five parameters. The only assumptions made for computing ‘maximum interference range’ are that (i) all transmitters have the same transmission range, i.e., all transmitters operate at same power level; (ii) all receivers have a uniform carrier sensing range, (iii) all transmitters use Omni-directional antennas, and (iv) free space wireless propagation model is used. Every node not currently involved in transmission or receipt of data from its transmitter senses two elements of the
received signals – average signal value arriving at the node and the sudden increase or decrease in its received signal above a ‘significant’ value. The magnitude of ‘significant’ value of sudden change in received signal has been defined as inverse of path-loss constant power of the ‘maximum interference range’. Further, necessary modifications in IEEE 802.11 have been suggested which enable every node to count the number of nodes involved in data transfer within carrier sensing range (CSR) of the node planning to begin its transmission or planning to receive data from its transmitter. The changes in 802.11 are designed keeping an eye on the signals observed by a node when physical layer transmission is using Frequency Hopping Spread Spectrum (FHSS). By observing the pattern of received signals for FHSS, a method has been designed to identify ‘significant’ sudden positive and negative changes in received signal. This enables every node to infer whether nearest transmitter or receiver is within or outside of its ‘maximum interference range’. When no other node within its ‘maximum interference range’ is currently involved in data transfer, the node would begin its RTS frame after a wait of Differential Inter-Frame Space (DIFS) and Contention Window (CW), where DIFS and CW are as per IEEE 802.11 standard.

Analysis of ‘maximum interference range’ shows that it comprises of approximately 5-hops for an average spacing of nodes as 0.8 times the transmission range for $\beta=6$ and CSR values of 6, or 8, or 12, and it comprises of approximately 4-hops for $\beta=4$. Thus network layer estimates the ‘maximum interference range’ as the average number of hops. Note that at MAC layer a node can easily maintain a distance of ‘maximum interference range’ by observing the magnitude of sudden change in its received signal where at network layer every node assumes that the nodes within its ‘interference range’ are at a distance of up to 5-hops from it when $\beta=6$ or within 4-hops for a distance of $\beta=4$. Thus MAC layer can assess the nodes that are within its ‘maximum interference range’ by observing magnitude of sudden change in its received signal in a far more accurate way as compared to network layer which assumes that nodes up to 5-hops for $\beta=6$ are within its ‘interference range’ referred to as ‘safe-distance’. The network layer uses this property to ascertain load at a node, i.e.,
number of packets in four standard sizes of 256, 512, 1024 and 2048 Bytes awaiting transmission at MAC layers of all nodes within its ‘safe distance’. Therefore, every node maintains a database of number of packets in four standard sizes awaiting transmission at MAC layers of all nodes that are up to 5-hops from it by gathering such information from its 1-hop neighbors in form of special data packets broadcasted by each node periodically.

Since only one node within ‘maximum interference range’ of any node can begin its data transfer, therefore whenever a node pair completes its data transfer more than one nodes within its ‘safe-distance’ will compete for media. It is obvious that most of the nodes within ‘safe-distance’ of the node pair cannot compete for media as majority of them fall under ‘safe-distance’ of other transmitter-receiver pairs that are transferring their data concurrently. However, the number of nodes that would compete for media around the node pair just completing its data transfer in the proposed MAC layer protocol may be marginally higher than in case of standard 802.11 protocols at medium and high loads.

The proposed protocol at MAC layer prevents collisions due to interference completely which results in saving of substantial time that was lost due to such collisions in IEEE 802.11. The time lost due to slight increase in number of direct collisions may increase marginally as compared to similar time lost in IEEE 802.11 but that loss of time would be insignificant as compared to the time saved due to indirect collisions at medium and high loads; at low load the increase in number of direct collisions for the proposed MAC-CPI.A protocol would not be there and there may be slight savings of time due to a stray case of indirect collision.

At network layer an AODV-based Node-Disjoint Multipath routing protocol has been proposed that has features of Collision Prevention due to Interference, and has been named as AODV-MCPI. Every node maintains a database comprising of IDs of all nodes that are up to 5-hops in all directions along with the number of frames of different sizes awaiting transmission at MAC layers of all these nodes. Every node
broadcasts its database periodically. By listening to the similar periodic ‘Beacons’ of its 1-hop neighbors, every node updates its own database. From this database every node estimates the time to clear all frames awaiting transmission at MAC layers of all nodes within 5-hops; this time is treated as the ‘total delay time’ at that node. A node planning to send data to a destination node that is more than 1-hop away estimates the total load at it. If total load (in terms of time) with the node is less than the time between successive ‘beacons’, then it can generate a Route Request (RREQ) for any destination node, else source node cannot generate a RREQ. The RREQ in proposed protocol has two additional fields as compared to AODV, first is the path accumulation feature that has IDs of all nodes that RREQ traverses, and second is ‘Delay Time’ field that shows the load with nodes starting from source till the node that forwarded RREQ; the load is assessed in units of time. When a source node generates a RREQ message, the ‘Delay Time’ field of RREQ is filled with the estimated ‘total delay time’. When an intermediate node receives first copy of RREQ, it computes its ‘total delay time’ by assuming an additional load of 4 packets of 256 bytes due to RREQ. If the ‘total delay time’ at an intermediate node is more than the time between its two successive beacons, then it drops the RREQ, otherwise it proceeds with processing of RREQ. The intermediate node then makes a reverse-route entry along with the ‘Delay Time’ field of RREQ and computes the additional delay time at it; the additional delay time is the time to clear frames at MAC layers of nodes that are within 5-hop distance from the intermediate node but are at more than 5-hops from the node that forwarded RREQ. The estimation of delay and additional delay times takes into account the time lost in direct collisions and the average number of back-off time slots a transmitter node has to wait when it does not receive ‘Clear To Send’ (CTS) signal either due to direct collision or the receiver was busy due to some other data transfer. The intermediate node adds the additional delay time to ‘Delay Time’ field of RREQ and forwards the same. When the intermediate node receives duplicate copies of same RREQ, and the ‘Delay Time’ field of RREQ has smaller value as compared to value recorded in its routing table, it updates its routing table accordingly and forwards the RREQ by adding additional delay time to ‘Delay Time’ field of RREQ, otherwise drops the RREQ. When destination node receives first copy
of RREQ it waits for some more copies of RREQ to arrive. After the expiry of wait time it generates first RREP towards source for the RREQ that had the least ‘Delay Time’; the route taken by RREP is the reverse path that was recorded in the RREQ. After receiving confirmation from source node regarding receipt of RREP, the destination node generates the next RREP for a RREQ that does not have any common node with RREPs previously received by destination and has minimum ‘Delay Time’. The subsequent RREPs contain the list of nodes that form a path from source to destination in previous RREPs. The intermediate nodes that are out of ‘safe-distance’ from source and destination nodes forward RREP towards source only if none of the nodes in previous RREPs is within ‘safe-distance’ of the intermediate node, otherwise the intermediate sends a RREP Returned (RREPR) packet towards destination. If destination receives a RREPR packet, then it sends another RREP to source that satisfies node-disjointness. After receiving acknowledgement from source for each of the RREP for which RREPR has not been received by destination, the destination generates next RREP. The source can start data transfer to destination along all the computed paths to destination and can be sure that all paths are out of each other’s interference range, except for some nodes within ‘safe-distance’ of either the source or the destination.

Whenever an intermediate node cannot forward a data packet to next hop towards destination, it identifies an ‘alternate node’ to 2nd hop node from it towards destination from its database. The intermediate node sends a Route Modification (RMOD) control packet to the ‘alternate node’ for modification of existing path to destination. The ‘alternate node’ confirms the same to intermediate node by sending another RMOD control packet. Thus if any path breaks due to mobility of nodes then the intermediate nodes immediately repair the path without involving the source node. Thus the proposed routing protocol AODV-MCPI has a special and powerful feature of fast ‘local repair’ as compared to any other existing protocol.

Simulation of the MAC layer MAC-CPI.A protocol on ns-2 shows that it gives better throughput (bytes received by destination node) approximately by 12% as compared to
IEEE 802.11b protocol when operating over Frequency Hop Spread Spectrum (FHSS) under medium and heavy load conditions. The proposed network layer protocol AODV-MCPI operating over IEEE 802.11 gives approximately 11% higher throughput as compared to AODV protocol under medium and heavy load conditions. However when AODV-MCPI operates over MAC-CPLA protocol, it gives an approximately 21% improvement in throughput as compared to AODV operating over IEEE 802.11 protocol.