# A Novel Cross-layer Node-Disjoint Multipath Routing Protocol for Ad Hoc Networks

R. K. Manocha
Institute of Management Studies, Lal Kuan, Ghaziabad, U.P. 201009, India

R. P. Agarwal
Shobhit University, Meerut, U.P., 201010 India

Anoop Srivastava
Institute of Engineering & Technology, Alwar, Rajasthan, 301030, India

## ABSTRACT
Finding multipath routes for Ad Hoc networks is a challenging task due to mobility of nodes. In this paper, we propose a cross-layer node disjoint multipath routing protocol AODV-MCPI. This routing protocol works in conjunction with MAC-CPI protocol at MAC layer. The protocol at MAC layer ensures that there are no collisions due to interference as every node ensures a minimum of 'safe-distance' from its nearest parallel transmitter-receiver pair before beginning its transmission. At routing layer every node gathers the number of packets and bytes awaiting transmission at MAC layers of nodes that are located within its circle of 'safe-distance' and then finds congestion free routes. In addition, the routing layer protocol finds multiple node-disjoint paths for every source destination pair that is separated by a minimum of 'safe-distance' except for the nodes located within 'safe-distance' of source and destination nodes. The protocol also perform local repair of existing routes thus providing a good degree of safeguard against mobility of nodes.

## General Terms
Mobile ad hoc networks, multi-hop wireless networks, multipath routing, disjoint paths. Interference-free routing

## Keywords
Multi-path routing in ad hoc networks, interference, SINR, AODV, load-aware routes.

## 1. INTRODUCTION
Ad Hoc networks consist of mobile nodes that do not have provisions of an access point and therefore are multi-hop networks. Mobility of nodes and channel fading make it a challenging job to find routes for a source destination pair. In order to decrease overhead of finding routes for any source-destination pair in case of reactive protocols, multiple node-disjoint routes are found with a single route request.

AODV [1] and DSR [2] are the two main reactive protocols that have been studied in detail. In this paper we concentrate on node-disjoint multipath routing protocols based on AODV. Some of the metric used for finding node-disjoint multi-path routes can be any combination of the following: (i) minimum hop-count, (ii) minimization of collisions due to interference, (iii) load balancing at nodes in various paths, (iv) paths with minimum congestion (load-aware paths), (v) route stability with reference to mobility of nodes, (vi) energy or power-aware routes and so on. This paper concentrates on (i) prevention of collisions due to interference at MAC layer, (ii) finding congestion-free node-disjoint multi-paths, and (iii) that these paths are out of each other's interference range. In this paper we discuss a different concept of maximum load at a node and hence find paths that are congestion-free.

## 2. RELATED WORKS
Earlier work in node-disjoint multi-path routing protocols based on AODV for MANETS used minimum hop count as the main metric. Two such important protocols are NDMR [3] and AODVM [4]. Both the protocols compute node-disjoint multi-paths with a single RREQ. MAMR protocol [5] requires an incremental RREQ to find a find new path for the same source-destination pair, if possible; the protocol may alter any of existing paths if necessary. All these protocols have minimum hop count as the main criteria for finding routes and do not consider any of the parameters like interference, load on nodes, mobility of nodes and energy with nodes etc.

In [6] authors proposed Greedy-based Interference Avoidance Multipath Routing (GIMR) protocol which finds interference free routes but uses GPS to discover the paths. In [7] authors present a multipath routing protocol with minimum routing control overhead and three route maintenance methods. In [8] authors present a node-disjoint multipath routing protocol that focuses on low routing overhead during route discovery and also considers residual energy of nodes.

In [9] authors present a Node-disjoint multipath routing protocol MP-AODV which uses the modified RREQ and RREP packet and a flag to identify packets in main or backup route in route discovery process. Unlike a conventional AODV, intermediate nodes that receive the RREP packet increment the RREQ ID value in the seen table. By incrementing the RREQ ID value, the protocol ensures that a backup route will not use any nodes that belong to the main route. Nodes belonging to the main route always have a RREQ ID value one higher than nodes in the backup route for the route maintenance process when the backup route has been broken. New field named "Route_flag" is added to the routing table for the source node to distinguish between main and backup routes, a value of zero for "Route_flag" indicates the main route, and a value of one indicates the backup route. MP-AODV also modifies the routing table of conventional AODV and adds a 'Source' field, that records information about the source node. In [10] authors propose a New multipath node-disjoint based on AODV (NMN-AODV) which requires three control packets for two node-disjoint routes while MP-AODV uses five control packets. Similar to MP-AODV, this protocol uses a flag in the RREQ and RREP packets to distinguish the main or backup route packets in route discovery processes. In [11] authors propose a Node-disjoint minimum interference Multipath (ND-MIM) protocol.

In [12] authors propose an Interference-minimized multipath routing with congestion control and also propose a congestion control scheme for load balancing at the highest supoortable rates. To the best of our knowledge only authors of [13] have presented the first collision prevention protocol, BROADEN

for Ad Hoc networks. But it requires prior reservation to be made allocation of media.

In [14] authors propose a MA-AODV protocol which quantifies mobility of nodes so that stability of routes can be improved. In [15] authors analyze the stability of multipath routes against mobility of nodes. In [16] authors propose a MLR protocol that finds paths by excluding nodes with high mobility based on Markovian model.

In [20] authors introduce a concept of Interference range and Interference zones to express the probability of successful transmission as a function of network density, node transmission probability, radio propagation environment and network card sensitivity. The main theme of this and many other papers is that interference range or interference zone is a complex function of node pairs operating in parallel at present and this information pertaining to a node cannot be gathered or computed by another node which plans to begin its transmission. Therefore when another node, which is outside the transmission ranges of nodes transmitting at present but inside the interference range of any of nodes transmitting at present, begins its transmission, it causes a collision with on-going transmission.

Thus there is a need of a protocol which finds node-disjoint multipath congestion-free routes that have no collisions due to interference. In this paper we present a node-disjoint multi-path routing protocol AODV-MPCI that ensures (i) proposed and already admitted flows do not cause congestion in any part of network, (ii) collisions due to interference are prevented, (iii) parallel data transfers via multiple paths is possible, except at the nodes that are located within 'safe-distance' of the source or the destination nodes, and (iv) the routes can adapt to mobility of nodes. The rest of the paper is organized as follows: Section 3 describes the MAC-CPI protocol at MAC layer and its implications that pave the way for designing AODV-MCPI protocol at routing layer, section 4 describes the routing protocol AODV-MCPI, section 5 discusses critical real life situations with respect to the proposed protocols, and section 6 concludes the paper.

## 3. MAC-CPI Protocol at MAC Layer

Authors in [17] and [18] had proposed and analysed in detail suitable protocol for MAC layer. It has been named as MAC-CPI protocol and its main features have been described below.

When all transmitter-receiver pairs engaged in data transfer at any instant of time have a minimum of 'safe-distance' between each other, then interference at all receivers in the network would be below the maximum value that can cause collision due to interference, that is, $S/(I+N) \geq \beta$. Thus, if all nodes before beginning their data transfer ensure a minimum of 'safe-distance' from the nearest parallel transmitter-receiver pair, then collision due to interference can be completely prevented at all other receivers in the network. Two questions arise, first, what is the magnitude of 'safe-distance' and second, how does a node ensure a minimum of 'safe-distance' from its nearest transmitter-receiver pair. We derive the answers to both these questions one by one.

### 3.1 Computation of 'safe-distance'

Signal S at a receiver R due to a transmitter T with Omni-directional antenna is given by equation (1).

$$S = G.\ Pt / d^{\alpha} \quad \text{.....} \quad (1)$$

Where G is a constant of proportionality, Pt is the transmission power of the transmitter, 'α' is the path-loss factor, 'd' is distance between transmitter and the receiver. The signal at receiver R due to other parallel transmitters in the network is the interference signal. If 'N' is the noise at R and 'I' is the sum of signals at R due to all other parallel transmitters in the network, then R can decipher the signal S from T only if S is greater than β times (I + N) as given in equation (2).

$$S/(I + N) \geq \beta \quad \text{.....} \quad (2)$$

In order to simplify the computations of 'safe-distance', let us assume that (i) all transmitters in the network have same transmission power and hence the same transmission range, (ii) all distances are expressed as a multiple of transmission range, (iii) noise N is constant throughout the network and (iv) the constant G*Pt is replaced by one for brevity for all received signal values. R is always within transmission range of T, therefore, distance between any transmitter-receiver pair should be less or equal to one unit normalized distance. With the above assumptions, the minimum signal at R due to its T would be one unit as G*Pt has been replaced by one and maximum distance between any T-R can be one unit of normalized distance. Equation (2) puts a limit on the value of total interference due to all parallel transmitters and has been shown in equation (3).

$$I < (1/\beta - N) \quad \text{.....} \quad (3)$$

The value of 'I' as computed from equation (1) is the sum of signals due to each of the transmitter-receiver pairs operating in parallel in the network. In order to arrive at the maximum number of parallel transmitters in the network while maximizing interference let us assume that all transmitter-receivers operating in parallel have an exact distance as 'safe-distance' from their nearest transmitter-receiver pair. Figure 1 shows locations of transmitter-receiver pairs operating in parallel and having an exact distance equal to 'safe-distance' from their nearest transmitter-receiver pair with reference to a node pair T-R at the centre of the network. This figure does not show the other nodes in the network. Let these transmitter-receiver pairs operating in parallel be named as T101-R101, T102-R102, T103-R103, T104-R104, T105-R105, T106-R106, T201-R201, T202-R202, T203-R203 and so on. Let us denote 'safe-distance' as 'a' and assume that all nodes in the network are placed in grid form with grid spacing of 'hd'. Thus distance between a transmitter and its receiver is 'hd', i.e., average hop distance.

Equations for computation of maximum interference at R due to each of these transmitter-receiver pairs by using equation (1) has been listed out in equations (4) to (12).

The interference at R due to each of R101, R104, R105 and R106 is $1/a^{\alpha}$. Similarly interference at R due to R102 and R103 is

$$2/[(0.5*a)\text{^}2 + (0.5*a*\sqrt{3}+hd)\text{^}2)]\text{^}(0.5*\alpha) \quad \text{.....} \quad (4)$$

Interference at R due to R201 to R206 nodes is

$$2/[a*\sqrt{3}]\text{^}\alpha + 2/[(1.5*a)\text{^}2 + (hd+0.5*a*\sqrt{3})\text{^}2]\text{^}(0.5*\alpha) + 1/[a*\sqrt{3}+hd]\text{^}\alpha + 1/[a*\sqrt{3}+2*hd]\text{^}\alpha \quad \text{.....} \quad (5)$$

Interference at R due to R301 to R306 nodes is

$$2/[2*a]\text{^}\alpha + 2/[a*a+(a*\sqrt{3}+2*hd)\text{^}2]\text{^}(0.5*\alpha) + 2/[a*a+(a*\sqrt{3}+hd)\text{^}2]\text{^}(0.5*\alpha) \quad \text{.....} \quad (6)$$

Interference at R due to R401 to R412 nodes is

$$2/[(2.5*a)\text{^}2+(0.5*a*\sqrt{3}+hd)\text{^}2]\text{^}(0.5*\alpha) + 2/[a*\sqrt{7}]\text{^}\alpha + 2/[4*a*a+(a*\sqrt{3}+2*hd)\text{^}2]\text{^}(0.5*\alpha) + 2/[4*a*a+(a*\sqrt{3}+hd)\text{^}2]\text{^}(0.5*\alpha) +$$

2/[0.25*a*a+(1.5*a*√3+2*hd)^2]^(0.5*α) +
2/[0.25*a*a+(1.5*a*√3+3*hd)^2]^(0.5*α) …….…….. (7)

Interference at R due to R501 to R506 nodes is

2/[(1.5*a)^2+(1.5*a*√3+3*hd)^2]^(0.5*α) + 2/[a*3]^α +
2/[(1.5*a)^2+(1.5*a*√3+2*hd)^2]^(0.5*α) …….…….. (8)

Interference at R due to R601 to R606 nodes is

2/[(3*a)^2+(a*√3+2*hd)^2]^(0.5*α) +
2/[(3*a)^2+(a*√3+*hd)^2]^(0.5*α) + 2/[2*a*√3+4*hd]^α +
2/[2*a*√3+3*hd]^α …….…….. (9)

Interference at R due to R701 to R712 nodes is

2/[(3.5*a)^2+(0.5*a*√3+*hd)^2]^(0.5*α) + 2/[a*√13]^α +
2/[6.25*a*a+(1.5*a*√3+3*hd)^2]^(0.5*α) +
2/[6.25*a*a+(1.5*a*√3+2*hd)^2]^(0.5*α) +
2/[a*a+(2*a*√3+4*hd)^2]^(0.5*α) +
2/[a*a+(2*a*√3+3*hd)^2]^(0.5*α) …….…….. (10)

Interference at R due to R801 to R806 nodes is

2/[(2*a)^2+(2*a*√3+4*hd)^2]^(0.5*α) + 2/[a*4]^α +
2/[(2*a)^2+(2*a*√3+3*hd)^2]^(0.5*α) …….…….. (11)

Interference at R due to R901 to R912 nodes is

2/[(4*a)^2+(a*√3+2*hd)^2]^(0.5*α) +
2/[(4*a)^2+(a*√3+*hd)^2]^(0.5*α) +
2/[(3.5*a)^2+(1.5*a*√3+3*hd)^2]^(0.5*α) +
2/[(3.5*a)^2+(1.5*a*√3+2*hd)^2]^(0.5*α) +
2/[(0.5*a)^2+(2.5*a*√3+5*hd)^2]^(0.5*α) +
2/[(0.5*a)^2+(2.5*a*√3+4*hd)^2]^(0.5*α) …….…….. (12)

The sum of interference at R given by equations (4) to (12) must be less than or equal to the value of 'I' given by equation (3). If the signal at R as computed in any of the equation (4) to (12) is below the value that can be sensed by R (that is, the lowest value of carrier signal that can be sensed by any receiver) then those signals must not be summed up. From the two equations of 'I' at R, one can observe that 'a' is a non-linear function of (i) α – the path propagation constant, (ii) β, threshold value of SINR, (iii) average hop-distance 'hd', and (iv) the maximum noise around the receiver and it is assumed that it is the maximum value of noise in any part of the network, (v) the number of transmitter-receivers operating in parallel in the network.

Consider three circular networks of radii 12, 8 and 6 normalized units of distance; if the transmission range is 250m., then these radii get translated to radii of 3Km., 2Km. and 1.5 Km. respectively. The signal strength at the perimeter of these networks due to a transmitter at the centre would be 0.00422475 (-23.942 dBm), 0.01030865555 (-19.868 dBm) and 0.0194118644 (-17.119 dBm) respectively. Authors have already proved in [17] and [18] that 'safe-distance' decreases non-linearly as α increases and it increases non-linearly as N increases. So we consider a value of α = 2.2 which is path loss exponent in free air, β varying as 2, 4 and 6, 'hd' from 0.6 to 1.0 in steps of 0.1, two values of N as 0.5 and 1.5 times of the signal at the perimeter for all three network in order to arrive at highest possible values of 'a'. Computed values of 'a' for these three networks have been tabulated in Tables 1 to 3 respectively.

The magnitude of interference as computed from equations (4) to (12) decreases sharply with higher equation numbers as the interference is inversely proportional to higher powers of 'a'.

**Table 1. Computed values of 'Safe-Distance' for a circular network of radius 12 units normalized distance (in multiples of transmission range) for α=2.2**

| N | Hop distance 'hd' | β | | |
|---|---|---|---|---|
| | | 2 | 4 | 6 |
| 0.002 (-26.9897 dB) | 0.6 | 2.26700 | 3.12725 | 3.66965 |
| | 0.7 | 2.66435 | 3.55345 | 4.20195 |
| | 0.8 | 3.05240 | 4.00460 | 4.65865 |
| | 0.9 | 3.36465 | 4.40235 | 5.18090 |
| | 1.0 | 3.71475 | 4.85445 | 5.56180 |
| 0.006 (-22.2185 dB) | 0.6 | 2.26995 | 3.13525 | 3.68360 |
| | 0.7 | 2.66915 | 3.56610 | 4.22430 |
| | 0.8 | 3.05975 | 4.00460 | 4.69195 |
| | 0.9 | 3.37510 | 4.42955 | 5.19620 |
| | 1.0 | 3.72925 | 4.89230 | 5.56290 |

**Table 2. Computed values of 'Safe-Distance' for a circular network of radius 8 units normalized distance for α=2.2**

| N | Hop distance 'hd' | β | | |
|---|---|---|---|---|
| | | 2 | 4 | 6 |
| 0.005 (-23.0103 dB) | 0.6 | 2.16145 | 2.87885 | 3.30165 |
| | 0.7 | 2.49480 | 3.19760 | 3.79880 |
| | 0.8 | 2.81680 | 3.60000 | 4.00005 |
| | 0.9 | 3.03830 | 3.93190 | 4.39705 |
| | 1.0 | 3.34210 | 4.04105 | 4.92285 |
| 0.015 (-18.2391 dB) | 0.6 | 2.16845 | 2.88170 | 3.33320 |
| | 0.7 | 2.50605 | 3.22615 | 3.84985 |
| | 0.8 | 2.83385 | 3.64320 | 4.00005 |
| | 0.9 | 3.06205 | 3.93190 | 4.50265 |
| | 1.0 | 3.37485 | 4.12200 | 5.07395 |

The maximum signal strength at R due to each of parallel transmitters and receivers in the network that has a radius of 8 normalized units, minimum α=2.2, β=6, 'hd'=1.0, N=0.015 (-18.2391 dB) can be computed as $1/(\text{distance from R})^{\alpha}$ and is as shown in Table 4. From the signal values in Tables 4 it can be easily verified that the interference is maximum at nodes around the centre of the network.

**Table 3. Computed values of 'Safe-Distance' for a circular network of radius 6 units normalized distance for α=2.2**

| N | Hop distance 'hd' | B | | |
|---|---|---|---|---|
| | | 2 | 4 | 6 |
| 0.01 | 0.6 | 2.02955 | 2.66285 | 2.98030 |

| | | | | |
|---|---|---|---|---|
| (-30.0 dB) | 0.7 | 2.29155 | 2.88560 | 3.38445 |
| | 0.8 | 2.58615 | 3.20380 | 3.91185 |
| | 0.9 | 2.73930 | 3.63920 | 4.44885 |
| | 1.0 | 3.00005 | 4.08090 | 4.99655 |
| 0.029 (-15.3760 dB) | 0.6 | 2.04195 | 2.69535 | 3.00005 |
| | 0.7 | 2.31115 | 2.93560 | 3.47455 |
| | 0.8 | 2.61585 | 3.27960 | 4.05445 |
| | 0.9 | 2.73930 | 3.75250 | 4.66450 |
| | 1.0 | 3.00005 | 4.24420 | 5.11315 |

**TABLE 4. Magnitude of signal at Tx & Rx due to all 12 parallel transmitter-receiver pairs in a circular network of radius 8 units normalized distance with for α=2.2, β=2, N=0.015 when all parallel receivers have minimum distance from Rx; 'a'=3.37485, Mag2=0.0280697, $R_T$=0.484987**

| Node | Magnitude of signal at Tx | Magnitude of signal at Rx |
|---|---|---|
| T101 | 0.068840 | 0.062753 |
| R101 | 0.062753 | 0.068840 |
| R102 | 0.068840 | 0.041021 |
| T102 | 0.041021 | 0.026551 |
| R103 | 0.068840 | 0.026551 |
| T103 | 0.041021 | 0.041021 |
| T104 | 0.068840 | 0.062753 |
| R104 | 0.062753 | 0.068840 |
| R105 | 0.041021 | 0.068840 |
| T105 | 0.026551 | 0.041021 |
| R106 | 0.041021 | 0.068840 |
| T106 | 0.026551 | 0.041021 |
| R201 | 0.020559 | 0.016818 |
| T201 | 0.016818 | 0.013567 |
| R203 | 0.020559 | 0.016818 |
| T203 | 0.016818 | 0.013567 |
| R204 | 0.016818 | 0.020559 |
| T204 | 0.013567 | 0.016818 |
| R206 | 0.016818 | 0.020559 |
| T206 | 0.013567 | 0.016818 |
| R301 | 0.014629 | 0.014982 |
| T301 | 0.014982 | 0.014629 |
| R304 | 0.014629 | 0.014982 |
| T304 | 0.014982 | 0.014629 |

## 3.2 Ensuring a minimum of 'safe-distance' between parallel transmitter-receiver pairs

Signal at a node would suddenly increase or decrease by $1/a^{\alpha}$ if a node located at 'safe-distance' from it begins or completes its frame. If the sudden increase in signal at a node is greater than $1/a^{\alpha}$ then the node infers that another node within its 'safe-distance' has begun transmission and therefore it should defer its transmission till it observes a sudden decrease in its received signal of magnitude > $1/a^{\alpha}$. Whenever a node observes a sudden increase greater than $1/a^{\alpha}$ then it defers its transmission by starting a new timer for a period equal to sum of time for transmitting RTS, CTS, $DATA_{MAX}$ & ACK frames plus three SIFS periods, where $DATA_{MAX}$ represents a time for transmitting the longest DATA frame. If the node observes a sudden decrease greater than $1/a^{\alpha}$ in its received signal and it has an active timer, then it resets the timer. If the sudden increase or decrease in its received signal is less than $1/a^{\alpha}$, then node infers that it has more or equal to 'safe-distance' from the node beginning or completing its frame and hence does not begin or reset any timer. Moreover, a node observes a sudden increase of magnitude $\geq 1/a^{\alpha}$ twice due to a transmitter or a receiver if it has less than 'safe-distance' from the transmitter or the receiver or both. Therefore, a new timer is set only when the node observes an odd (1 or 3 or 5 or ..) jump of magnitude > $1/a^{\alpha}$ and the node resets its timer with the even (2 or 4 or 6..) negative jump of magnitude > $1/a^{\alpha}$. A node begins its transmission only if it has no active timer.

### *3.2.1 Interpretation of node positions as shown in figure 1*

Figure 1 depicts node pairs presently engaged in data transfer have 'hd' as the distance between transmitter and its corresponding receiver. i.e., distance between T and its R is 'hd'. All these node pairs are separated by a minimum of 'safe-distance' from their nearest node pair. Three dark circles indicate the periphery of circles with radius of 12 unit's normalized distance for values of β = 2, 4, 6, α=2.2, and N=1.5 times the signal at periphery of circle due to a transmitter located at centre of the circle. The diagram also shows the location of transmitter-receiver pairs operating in parallel. For example, a circular network of normalized 12 units radius from centre of T-R pair has 'safe-distance' of 3.72925 normalized units for β=2 and 'hd=1, refer Table 3 last row column three. This implies that a radius of 12 units is equivalent to 12/3.72925 ≈ 3.2178 times the 'safe-distance' and therefore periphery of the network is represented by a thick dark outermost circle as shown in figure 1. The circle passes between node pairs T501-R501 and T801-R801. Nodes beyond the circle do not form a part of the network of radius 12 when β=2. For β = 4, 'a' has a value 4.89230, refer Table 3 last row column four. This implies that a radius of 12 units is equivalent to 12/4.8923 ≈ 2.4528 times the 'safe-distance' and therefore, periphery of the network is represented by a thick dark middle circle as shown in figure 1. This circle passes between node pairs T301-R301 and T501-R501; nodes beyond this circle do not form a part of the network of radius 12 for β=4. This is so because the 'safe-distance' has increased substantially from 3.72925 to 4.89230. Similarly, for β=6, the radius of 12 units is represented by a thick dark inner circle as shown in figure 1 and it is closer to T301-R301 node pair as compared to when β=4.

Three circles with dotted lines show size of networks with radii = 12, 8 and 6 for β=6, α=2.2 and N=1.5 times the signal at the periphery of the network from an imaginary node placed at centre of circles; the outermost circle with dotted line corresponds to a network of 12 units normalized radius and innermost dotted circle corresponds to 6 units normalized radius.

### *3.2.2 Number of node pairs that can transmit in parallel in networks of different sizes*

In Table 5 columns 3 to 5 odd numbered rows have the computed values of normalized radius of network divided by the respective 'safe-distance'. With reference to T-R pair at centre of the network in figure 1, it is possible to identify the number of transmitter-receiver pairs that can operate in parallel with T-R pair; all such nodes must be located within a radius as shown in Table 5, columns 3 to 5 with odd numbered rows. For example, for a network with normalized radius = 6, the values of 'safe-distance' for node spacing ('hd') of 0.8 with varying β as 2, 4 and 6 can be read from

Table 3 eighth row columns 3 to 5 as 2.61585, 3.27960 and 4.05445 respectively; Division of radius of network = 6 with 'a' = 2.61585 yields 2.29371 and this value is depicted in first row of Table 5 for β = 2. With reference to figure 1, when one move to the right of T-R pair located at the centre of network by 2.29371*'a' units of distance, one cross transmitter-receiver pairs T101-R101 and T301-R301 but stop short of T501-R501 pair. Similarly, as one move to the left of T-R pair in figure 1 by 2.29371*'a' units of distance, one cross transmitter-receiver pairs T104-R104 and T304-R304 but stop short of T504-R504 pair. Thus, the node pairs that can operate in parallel along the centre line of network joining nodes T504 to T501 are T304, T104, T, T101 and T301. By drawing a circle of radius 2.29371*'a' units from centre point of T-R, one observes that the circle will encompass node pairs T203-R203, T103-R103, T102-R102, T201-R201, T204-R204, T105-R105, T106-R106 and T206-R206 but not node pairs T202-R202 and T205-R205. Thus for β=2, 'hd' = 0.8, α = 2.2 only a maximum of 13 transmitter-receivers can operate in parallel as specified above in a circle with 6 normalized units radius. The number has been shown in Table 5, column 3, row 2. The other values in the Table 5 have been computed exactly in same manner by varying size of network as 8 and 12 and β from 2 to 6 in steps of 2.

**Table 5: Maximum number of transmitter-receiver pairs that can N operate in parallel in networks of different sizes with uniform node spacing ('hd') of 0.8 normalized units**

| Radius of network | Normalized radius of network / 'safe-distance' / Maximum number of node pairs that can operate in parallel | β = 2 | β = 4 | β = 6 |
|---|---|---|---|---|
| 6 | | 6 / 2.61585 = 2.29371 | 6 / 3.27960 = 1.82949 | 6 / 4.05445 = 1.47985 |
| | | 13 | 7 | 7 |
| 8 | | 8 / 2.83385 = 2.82301 | 8 / 3.6432 = 2.19587 | 8 / 4.00005 = 1.99997 |
| | | 15 | 13 | 7 |
| 12 | | 12 / 3.05975 = 3.92189 | 12 / 4.0046 = 2.9965 | 12 / 4.69195 = 2.55757 |
| | | 33 | 19 | 15 |

Proceeding in a similar fashion, it can be easily verified from figure 1 that the various node pairs that can operate in parallel are as follows: Seven node pairs as specified in Table 5, columns 4 and 5, row 1 are T103-R103, T102-R102, T104-R104, T-R, T101-R101, T105-R105 and T106-R106. A list of thirteen node pairs as specified in row 2 column 5 of Table 5 includes the above seven node pairs and T203-R203, T201-R201, T304-R304, T301-R301, T204-R204 and T206-R206. The list of 15 node pairs that can operate in parallel are thirteen nodes mentioned above plus two additional node pairs T202-R202 and T205-R205. For nineteen node pairs four more node pairs T303-R303, T302-R302, T305-R305, and T306-R306 get added to the list of fifteen nodes. List of 33 node pairs that can operate in parallel includes additional fourteen node pairs as T401 to T412, T501 and T504.

## 3.3 More details of MAC-CPI protocol

At physical layer every node in the network should meet the following requirements:

1. When a node observes an odd ($1^{st}$ or $3^{rd}$ or $5^{th}$) sudden increase of > $1/a^{\alpha}$ magnitude in its received signal it starts a timer for period RTS + CTS + DATA(Max) + ACK + 3SIFS and also sets a flag named as flag1 where DATA(Max) is the time to transmit the longest DATA frame, SIFS is Short Inter-Frame Space and RTS, CTS and ACK are the timings to transmit these frames as used in IEEE 802.11. If the sudden increase in received signal is > $k/a^{\alpha}$ where 'k' is an integer, then node starts 'k' timers subject to a maximum of six timers. Whenever a node observes the even ($2^{nd}$ or $4^{th}$ or $6^{th}$) sudden increase > $1/a^{\alpha}$ magnitude in its received signal, it resets flag1. Thus flag1 indicates even or odd sudden increases of > $1/a^{\alpha}$ in received signal.
2. When a node observes an odd sudden decrease of > $1/^{a\alpha}$ magnitude in its received signal, it sets flag2. With even sudden decrease of > $1/a^{\alpha}$ magnitude in its received signal, the node resets flag2 and its oldest timer, if any. A sudden decrease of > $k/a^{\alpha}$ magnitude resets only one timer.
3. If a node observes that the received RTS frame has its address as next hop, then it complements its flag1 and flag2 and resets its latest timer. Further, if it does not have any active timer after resetting its latest timer, then it can reply with CTS after SIFS period.
4. Timers of a node can either time out or are reset due to sudden decrease of > $1/a^{\alpha}$ in its received signal. A node starts its RTS or CTS frame only if it has no active timer and does not observe an odd sudden increase of > $1/a^{\alpha}$ magnitude in its received signal for a continuous period of DIFS+CW, where DIFS and CW have the same meaning as used in IEEE 802.11. If the node observes an odd sudden increase of > $1/a^{\alpha}$ magnitude in its received signal during DIFS+CW period, it has to start a fresh timer, wait for timer to timeout or get reset and then start another wait for a period of DIFS+CW afresh; however, if the node has already waited for some slots of CW, then reduced CW would be used for the next wait cycle as is done in IEEE 802.11.
5. When a node resets its last active timer or the last timer times out, it resets flag1 and flag2 as well. This helps in restoration of correct status of flags in case it gets disturbed.
6. Whenever a direct collision occurs, exponential back-off as used in IEEE 802.11 is applicable for CW.

A node does not start any timer when it is in the process of transmitting or receiving DATA or ACK frame. If received frame is for the node, then it complements the flag1 and resets the timer.

## 3.4 Implications of the proposed MAC protocol

The MAC-CPI protocol requires that only one node pair in any circle of 'safe-distance' should exchange data at any time. Let us estimate the number of nodes inside a circle of 'safe-

distance' as well as the number of hops from centre of network to the periphery of the 'safe-distance'.

### *3.4.1 Estimation of number of nodes inside a circle of 'safe-distance'*

Let us assume that nodes in the network are organized in a grid form with node spacing equals to 'hd'. This assumption will bring us closer to a better estimation of the number of nodes inside a circle of 'safe-distance' in real life.

The average number of nodes within the 'safe-distance' for the values of 'safe-distance' in Tables 1, 2 and 3 have been computed as $\pi(\text{safe-distance})^2/\text{hd}^2$ and recorded in Tables 6, 7 and 8 respectively for varying values of hop-distance and β; a higher value of N from both tables was selected as 'safe-distance' increases non-linearly with increasing N. In a similar way the total number of nodes in entire network has been estimated for networks with node placement in grid form and having radii of 12, 8 and 6 units of distance.

**Table 6: Number of nodes in 'safe-distance' & in a network of radius 12 units normalized distance for α=2.2 and N=0.006 equivalent to -22.2185 dBm**

| β | Number of nodes in 'Safe-distance' for average Hop Distance | | | | |
|---|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
| 2 | 44 | 45 | 45 | 44 | 43 |
| 4 | 85 | 81 | 78 | 76 | 75 |
| 6 | 118 | 114 | 108 | 104 | 97 |
| Number of nodes in network | | | | | |
| | 1256 | 923 | 706 | 558 | 392 |

**Table 7: Number of nodes in 'safe-distance' & in network of radius 8 units normalized distance for α=2.2 and N=0.015 equivalent to -18.2391 dBm**

| β | Number of nodes in 'Safe-distance' for average Hop Distance | | | | |
|---|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
| 2 | 41 | 40 | 39 | 36 | 35 |
| 4 | 72 | 66 | 65 | 59 | 53 |
| 6 | 96 | 95 | 78 | 79 | 80 |
| Number of nodes in network | | | | | |
| | 558 | 410 | 314 | 248 | 201 |

**Table 8: Number of nodes in 'safe-distance' & in network of radius 6 units normalized distance for α=2.2 and N=0.029 equivalent to -15.3760 dBm**

| Number of nodes in 'safe-distance' For β | Number of nodes in 'Safe-distance' for average Hop Distance | | | | |
|---|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
| 2 | 41 | 40 | 39 | 36 | 35 |
| 4 | 72 | 66 | 65 | 59 | 53 |
| 6 | 78 | 77 | 80 | 84 | 82 |
| Number of nodes in network | | | | | |
| | 314 | 230 | 176 | 139 | 113 |

### *3.4.2 Estimation of average number of hops in redius of 'safe-distance'*

The average number of hops from a node to periphery of 'safe-distance' has been computed as 'safe-distance' divided by average hop distance 'hd' and recorded in tables 9 to 11 by varying β and 'hd'. A closer look at the number of hops within a 'safe-distance' as computed in Tables 8 to 10 indicates that it is close to five for any size of network when β = 6, i.e., SINR=-7.7815 dBm, and it is closer to 4 when β = 4, i.e., SINR=-6.021 dBm.

**Table 9: Number of hops in 'safe-distance' for a circular network of radius 12 units normalized distance (3.0 Km. radius with transmission range = 250 m.), α=2.2 and N=0.006 (-22.2185 dBm); all distances are in multiples of Transmission range**

| B | Average Hop Distance | | | | |
|---|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
| 2 | 3.78 | 3.81 | 3.82 | 3.75 | 3.73 |
| 4 | 5.23 | 5.09 | 5.01 | 4.92 | 4.89 |
| 6 | 6.14 | 6.03 | 5.86 | 5.77 | 5.56 |

**Table 10: Number of hops in 'safe-distance' for a circular network of radius 8 units normalized distance, N=0.015 (-18.2391 dBm) and α=2.2**

| β | Average Hop Distance | | | | |
|---|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
| 2 | 3.61 | 3.58 | 3.54 | 3.40 | 3.37 |
| 4 | 4.80 | 4.61 | 4.55 | 4.37 | 4.12 |
| 6 | 5.56 | 5.50 | 5.00 | 5.00 | 5.07 |

**Table 11: Number of hops in 'safe-distance' for a circular network of radius 6 units normalized distance, N=0.029 (-15.3760 dB) and α=2.2**

| β | Average Hop Distance | | | | |
|---|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
| 2 | 3.40 | 3.30 | 3.27 | 3.42 | 3.00 |
| 4 | 4.49 | 4.19 | 4.10 | 4.17 | 4.24 |
| 6 | 5.00 | 4.96 | 5.07 | 5.18 | 5.11 |

### *3.4.3 Design values of β, 'hd' (average hop-distance) and 'a' ('safe-distance')*

If the design values of β and average hop-distance for all parallel transmitter-receiver pairs in any size of network are fixed as 6 and 0.8 respectively, then the actual value of SINR for a parallel transmitter receiver pair having a distance of 1.0

unit would drop to $(0.8)^{2.2}*6 = 3.672$, i.e., SINR=-5.649 dB. This value of SINR is very close to -6dB where packet drop ratio remains below 10% [19]. If the distance between a transmitter and its receiver in real life is less than the design value of 0.8, then the actual SINR would be larger than the design value of 6, thus further reducing the probability of packet drop due to interference.

Load at a node is logically the sum of the time required by all nodes within its 'safe-distance' to transmit all the frames awaiting transmission at their MAC layers plus the time required to periodically broadcast their beacons. In other words, load at a node or the time required to transmit all packets waiting at MAC layers of all nodes located within a circle of 'safe-distance' must not be more than a prededined value in order to find congestion-free routes at network layer.

*3.4.4 Estimation of time for forwarding all packets awaiting transmission at MAC layers of all nodes within its 'safe-distance'*

Time required to transmit a frame at MAC layer by a node comprises of three parts, (a) time lost due to collisions of RTS packets, that is, direct collisions, (b) time lost in backoff slots due to multiple direct collisions, if any, and (c) time taken to transmit the data bytes at the appropriate data rates. When RTS CTS exchange takes place safely, the data transfer would be successful and there would be no collisions due to interference. A transmitter will not receive CTS from its receiver only if (i) RTS have direct collision, or (ii) the receiver is within 'safe-distance' of another transmitter, or (iii) the intended receiver has moved out of transmission range (either mobility of node or link failure due to channel fading), (iv) more than one nodes begin their CTS in parallel.

For estimation of time for above mentioned parts (a) and (b), it has been assumed that average number of collisions per data frame successfully transmitted is 4, 3, 2 and 2 for data packets of sizes ≤ 250, > 250 and ≤500, > 500 and ≤1000 and > 1000 and ≤ 2000 bytes respectively, and the average number of backoff slots per collision is 8, 4, 2 and 2. Computation of time required for transmitting RTS, CTS, DATA and ACK frames at 2Mbps, 5.5Mbps and 11Mbps IEEE 802.11b rates has been detailed in Table 12 with SIFS, DIFS and time for one backoff slot of 10, 50 and 20μseconds respectively. Thus time required to forward one DATA packet without any direct collision of size 250, 500, 1000, 1400 or 2000 bytes at 2, 5.5 and 11Mbps including DIFS, RTS, CTS, ACK and three SIFS periods can be summed from last column of Table 12 as 1792, 2792, 4792, 6392, 8792, 1070, 1433, 2160, 2742, 3525, 863, 1045, 1408, 1699 and 2136 micro-seconds respectively. With the above assumption of average number collisions and back-off slots per packet, the estimated time required to transmit 152,000 bytes of DATA packets in sizes of 250, 500, 1000 and 2000 bytes has been worked out in Table 13. The relevance of 152,000 bytes has been explained in section 4.1.

In order to estimate time to transmit all frames at MAC layers of all nodes within its 'safe-distance', a node should consider the number of packets awaiting transmission at MAC layers of all.

# 4. Proposed protocol at Routing Layer

At routing layer every node finds and maintains routes for the desired source destination pairs and also broadcast periodic beacons with specific information as has been detailed below.

## 4.1 Special periodic beacons

It is proposed that all nodes periodically transmit a special beacon packet with following information:

(i) ID of all nodes within its 'safe-distance',
(ii) The number of hops for all nodes recorded above from the node transmitting beacon,
(iii) Transmission time required by the node to clear all its packets and bytes awaiting transmssion at MAC layer on different links, and
(iv) The time stamp when the node transmits beacon with the above information.

These beacons must be broadcasted periodically. All nodes listen to the beacons of their 1-hop neighbours and update their database with the said information; it is implied that a node recalculates its minimum hop distance for every node as it listens to the beacons of its 1-hop neighbours. A node restricts its database to the number of nodes which are located within its 'safe-distance', i.e., up to 5-hop distance from it.

Beacon is a variable length packet. The first three fields of the proposed beacon are (a) Two bytes as ID of the node transmitting beacon, (b) Four one byte sub-fields indicate the number of packets waiting at MAC layer for transmission with ≤ 250 bytes, with > 250 & ≤ 500 bytes, with > 500 bytes and ≤ 1000 bytes and with > 1000 bytes and ≤ 2312 bytes respectively, (c) six bytes to indicate the time beacon is transmitted, and (d) one byte to represent the number of nodes within its 'safe-distance'. The next four fields are repeated as per value in field (d). These four fields are (e) ID of the node within 'safe-distance' of the node transmitting beacon (2 bytes), (f) one byte for hop number from the node transmitting beacon, (g) six bytes to represent time of transmission of last beacon by the node, (h) four one byte sub-fields to indicate number of packets awaiting transmission at MAC layer with ≤ 250 bytes, with > 250 & ≤ 500 bytes, with > 500 bytes and ≤ 1000 bytes, with > 1000 bytes and ≤ 2312 bytes respectively.

It can be observed from Table 6 row 3 column 4 that the maximum number of nodes within a circle of 'safe-distance' can be 108 for β = 6 and hop-distance = 0.8. Thus, if the number of nodes in a circle of 'safe-distance' is 108, then every beacon packet will have 1404 bytes. It must be observed that these beacons are transmitted as data packets and are broadcasted.

## 4.2 Time between two successive beacons

During the period between two successive beacons by a node, all nodes within its 'safe-distance' would transmit their periodic beacons once and some or all of the data bytes awaiting transmission at their MAC layers. It will be desirable to keep the overhead due to large size of beacons below 50%, that is, the number of bytes in all beacons should be less than or equal to the number of data bytes transmitted between two successive beacons in any circle with radius of 'safe-distance'. In other words, if there are approximately 108 nodes within a circle of 'safe-distance' and each of these nodes transmits beacons of 1404 bytes, then approximately 152,000 bytes would be transmitted in the form of beacons during two successive beacons by same node. In order to keep the overhead due to beacons below 50%, at least the same number of bytes in form of data packets must be transmitted during same period, which implies that at least 76, 152, 304 or 608 data packets with 2000, 1000, 500 or 250 bytes respectively should be transmitted between two consecutive beacons. Table 13 shows the computation of time between two successive beacons for these sizes of data packets at 2, 5.5 and 11Mbps data rates. Row one column six of Table 13 shows that the maximum time between two successive

beacons for 250 bytes data packets is 1.84234seconds with data transfer rate of 11Mbps. So let us fix the design value of time between two successive beacons as 2.0 seconds for data rates of 11Mbps.

If 'w', 'x', 'y' and 'z' represent the number of data packets of 250, 500, 1000 and 2000 bytes respectively that can be transmitted in 2.0 seconds at 11Mbps, then these values can be computed from equations (13) to (16) while assuming that the average number of collisions per packet (data or beacon) is 4, 3 and 2 for number of packets $\geq 500$, $\geq 260$ & $< 500$, and $< 260$ respectively and number of backoff slots per collision is 8, 4 and 2 respectively.

(0.863*w + 1.699*108 + (w+108)*4*(176+50+10)/1000 + (w+108)*4*8*0.02) msec = 2000 msec ……..……. (13)

(1.045*x + 1.699*108 + (x+108)*4*(176+50+10)/1000 + (x+108)*4*8*0.02) msec = 2000 msec ……..……. (14)

(1.408*y + 1.699*108 + (y+108)*4*(176+50+10)/1000 + (y+108)*4*8*0.02) msec = 2000 msec ……..……. (15)

(2.136*z + 1.699*108 + (z+108)*4*(176+50+10)/1000 + (z+108)*4*4*0.02) msec = 2000 msec ……..……. (16)

Solving for 'w', 'x', 'y' and 'z' and taking integer parts yield 'w' = 672, 'x' = 625, 'y'=549, and 'z' = 494. This implies that on the average a node can transmit 672/108 ≈ 6.222 data packets of 250 bytes each or 625/108 ≈ 5.787 data packets of 500 bytes each, or 549/108 ≈ 5.083 data packets of 1000 bytes each, or 494/108 ≈ 4.574 data packets of 2000 bytes each in addition to its beacon packet of ≈ 1404 bytes in the period between two successive beacons by any node. The overhead due to 1404 bytes beacons for 250, 500, 1000 or 2000 bytes packets is 47.44%, 32.67%, 21.64%, 13.305% respectively when computed as bytes in beacon packets/(bytes in beacon plus data packets)*100. The above computations assume that media is not idle except for the estimated number of backoff slots required due to collision, i.e., maximum load conditions.

## 4.3 Generation of RREQ

It is proposed that RREQ has additional fields for (i) total estimated delay time including the delay caused by intermediate, and (ii) the ID of all nodes through which this copy of RREQ has reached the intermediate node, as used in DYMO and DSR protocols.

A node generates a RREQ for a route to desired destination node only if the time to clear its existing as well as the proposed load is less than the time between two beacons.

When a source node starts a RREQ it fills the 'delay' field of RREQ with the estimated time to clear all frames awaiting transmisssion at MAC layers of all nodes within its 'safe-distance'.

An intermediate node performs following steps when it receives a RREQ.

1. It computes the estimated time to forward all frames in queue at MAC layers of all nodes within its 'safe-distance' and assumes a new load of four packets of 250 bytes each. If this time is more than the time between two beacons, it drops the RREQ.
2. It also computes the delay time introduced at the intermediate node as explained in section 4.3.1.
3. The delay time computed above is added to the value in delay field of RREQ. For the first copy of RREQ received by intermediate node, it records ID of source node, its RREQ-ID and the delay time up to this node in another table known as RREQ table.
4. Forwards the RREQ after appending its own ID along with the updated delay field of RREQ as explained in step 3 above.
5. If intermediate node is within 'safe-distance' of destination node, it skips following actions. For duplicate copies of RREQ, it compares the delay up to the intermediate node with the delay time recorded in RREQ table. If delay time up to intermediate node is more than the previously recorded delay time, it drops the RREQ. Otherwise, it updates the new delay time in RREQ table, forwards RREQ after appending its own ID and updating delay field of RREQ with delay up to intermediate node.

### *4.3.1 Estimation of Delay Time by Intermediate Nodes*

A source node estimates the average delay time as the sum of time taken by all nodes within its 'safe-distance' to transmit their existing packets awaiting transmission at MAC layer. An intermediate node computes the additional delay time introduced at it as the time to forward frames awaiting transmission at the MAC layer of nodes which are not in the 'safe-distance' of previous hop but are within 'safe-distance' of the intermediate node.

Every node should record the latest beacons of its 1-hop neighbors and a beacon has the information of all nodes which are up to 5-hop from it. From these recorded beacons a node can retrieve the nodes which are not in the 'safe-distance' of previous hop but are within 'safe-distance' of the intermediate node.

This process continues for all those intermediate nodes which do not have destination node as the next hop.

## 4.4 RREP generation

As first RREQ reaches its destination, the destination node records the route to source and replies with first RREP after incrementing its sequence number. RREP has the ID of all nodes through which RREQ had travelled up to destination node. It has an additional field of delay time from source to destination as this would allow source node to choose a path with minimum delay up for sending data packets to destination. For first RREQ destination node need not check for node-disjointness or loop free route. The source node, however, must send an acknowledgement for the RREP.

For all subsequent copies of RREQ received by destination which satisfy node-disjoint ness as verified by destination node, it increments its sequence number and sends another RREP. These additional RREPs contain a list of nodes through which earlier RREPs were sent. Each intermediate node which is more than 5-hop from source or destination verifies that any of the nodes specified in the previous RREPs is not within its 'safe-distance, otherwise intermediate node drops the RREP and sends a special message to destination node along the route specified in RREP. This new message is christened as RREPR (RREP returned).

The intermediate node after ensuring that none of the nodes in the previous RREPs is within its 'safe-distance' when it is more than 5-hop away from source or destination, it records the route to destination and forwards the RREP towards source.

No intermediate node generates RREP for any RREQ.

## 4.5 RERR generation

It is proposed that all nodes record ID of nodes which fall within their 'safe-distance' and are a part of the route to a destination node as shown in Table 13. When an intermediate node while forwarding data packet finds that next hop to destination is not available, it attempts to route the data through any of the nodes which form a path to destination from it as recorded in Table 14.

All nodes record latest beacons of their 1-hop neighbors. From these beacons the intermediate node can identify it's another 1-hop neighbor which has 2nd hop of intermediate node as its 1-hop neighbor. If the intermediate node cannot find any other node for forwarding packets data packets to destination, it sends a RERR packet as per AODV protocol towards source node and to all nodes in the precursor list.

**Table 14: Nodes within 'safe-distance' which form a route to a destination**

| ID of destination nodes which have a route through this node | ID of nodes which are within 'safe-distance' and form a route to the destination. |
|---|---|
| ID of destination node | ID of 1st hop node from intermediate node towards the destination<br>ID of 2nd hop node from intermediate node towards the destination<br>ID of 3rd hop node from intermediate node towards the destination<br>ID of 4th hop node from intermediate node towards the destination<br>ID of 5th hop node from intermediate node towards the destination |

# 5. Discussion

Here we analyze that how the proposed protocol responds to some real life situations.

## 5.1 Values of 'Safe-Distance' as a function of N, α and β

If noise in real life is more than the assumed maximum N, that is, more than 1.5 times minimum carrier sensing range, refer values of N in Tables 1 to 3, then the 'safe-distance' would be marginally higher than the computed values as given in Tables. A higher value of N in real life can be compensated by values of $\alpha > 2.2$ (its design value) or by values of β lower than its design value.

Smaller value of 'safe-distance' would be required if path-loss constant α in most parts of network is more than the design value of 2.2. This would improve the ratio of network radius to 'safe-distance' and allowing higher number of parallel transmitter-receiver pairs in the network, refer Table 5.

The magnitude of sudden increase or decrease in received signal at a node for changing state of one of its flags (flag1 or flag2) is $>1/a^{\alpha}$. The ratio of this signal strength to maximum noise N level while computing the value of 'safe-distance' in Tables 1 to 3 turns out be 5.55, 3.1576 and 1.585 for networks with radii of 12, 8 and 6 normalized units; recall that maximum noise level used in computation of 'a' is 1.5 times the signal strength at the periphery of the network due to a imaginary transmitter located at centre of the circle. It is obvious that a sudden change in noise level in any part of network does not change the state of any node (that is, state of either of flag1 or flag2 does not change and there is no change in number of timers).

## 5.2 Placement of Nodes in the network

In real life node pairs engaged in parallel communication need not be placed at an exact distance of 'safe-distance' from each other. Only for the purpose of calculations of maximum interference at any node in the network, an exact distance equal to 'safe-distance' between two nearest parallel transmitter-receiver pairs was used.

In sections 3.1 and 3.4.1 we had assumed that nodes in the network be organized in a grid form, that is, having equal spacing of 'hd' from the nearest node. Such s placement of nodes is used only to get a fair idea of the number of nodes within a circle 'safe-distance' and the other design parameters (e.g., time between two successive beacons by a node) dependent on it.

If overall density of nodes is much higher than the density with assumed grid spacing then majority of nodes will have direct collisions most of time when attempting to forward their packets. In such a situation it would be advisable to lower the transmission power of all nodes, which implies increasing logical distance between nodes as all distances are defined as multiples of transmission range. It effectively increases the logical size of the network and therefore more number of node pairs can transfer data in parallel in the network. In other words, the number of nodes within a circle of radius equal to 'safe-distance' would decrease and approach the design value. Therefore, the assumption of placement of nodes in the network in a grid form was only to carry on the analysis by estimating (i) the number of nodes within any circle of radius equal to 'safe-distance', (ii) the number of hops in a distance of 'safe-distance', (iii) size of beacon packet and (iv) time between two successive beacons by same node. The above said analysis would apply to any placement of nodes within network.

This brings out an important conclusion that the transmission power of nodes controls the number of nodes that can transmit in parallel within a network. However, the increase in number of transmitter-receiver pairs is not linear with change in transmission power; the number of node pairs that can transmit in parallel as shown in Table 5 also point to this fact; as increase in size of network does not yield a linear increase in number of node pairs that can transmit in parallel for same values of β (refer values in Table 5 column wise). However, these numbers do not take into account the delays introduced due to queuing delays at nodes and hence optimization of throughput in the network requires some more factors as well.

## 5.3 Shape of Network

For computing the value of 'safe-distance' we had assumed a circular network. This assumption was made to ascertain the maximum number of transmitter-receiver pairs that can operate in parallel and interfere with the transmission at the centre of network, and therefore, affect the value of 'safe-distance'. Any shape or size of the network can be mapped on to an imaginary circle which can accommodate all nodes of network; this would help in ascertaining the maximum

number of node pairs that can operate at any time and therefore add to the interference at any node in the network.

## 5.4 Congestion-Free Routes

Congestion free routes are decided on the basis of load on nodes at time of route formation. However, if the source nodes start sending higher number of data packets than what was assumed at the time of deciding routes (8 packets of 250 bytes each), then the congestion-free routes may get chocked subsequently. Thus for routes to remain always congestion-free, it is essential that routes are formed when source nodes define the maximum number of packet it plans to send during a period between two successive beacons, then the routes will always be congestion and interference free. In other words, if RREQ can be further modified to include a field of maximum number of data bytes to be transmitted by the node during two successive beacon periods, then it would be possible to ensure that every node can estimate its total load (including that of nodes within its 'safe-distance', then routes computed after this information would be congestion-free throughout the network.

## 5.5 Multiple RREQs received in the duration between two beacons

Every node has a counter to indicate the number of RREQs received by the node during a period between two successive beacons. For first copy of RREQ received by the node, it increments the said counter. Each RREQ is assumed to generate an additional flow of eight 250 bytes packets to forward while calculating the revised load and delay time. If the revised load in units of time does not exceed the design time interval between two successive beacons, then node forwards RREQ, otherwise it is dropped. The said counter is reset as a node transmits its beacon.

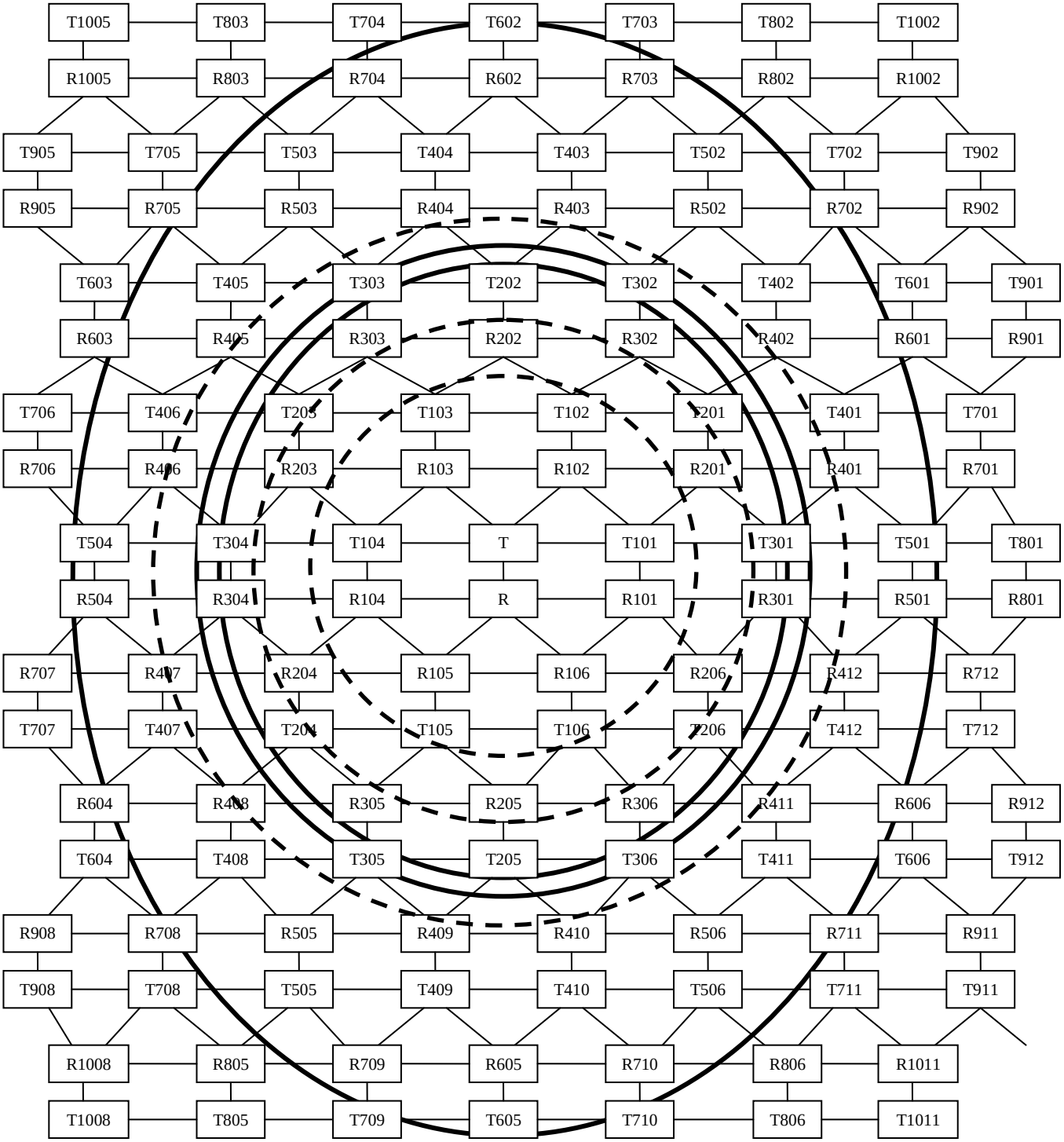
## 5.6 Load with nodes within a circle of 'safe-distance'

The average load with nodes within a circle of 'safe-distance' is a function of the number of routes passing through the circle and rate of the flows passing through these routes.

In case there is only one flow (route) passing through a node, then the average load is the sum of the number of packets awaiting transmission at MAC layers of nodes along the path and within 'safe-distance' of the node. The average load for all nodes that are within 'safe-distance' and perpendicular to the direction of flow approximately remains the same.

If more than one flows (route) pass through a node, then load at nodes within its 'safe-distance' would increase and would reach its maximum value around the common node between two flows. Further, the load at a node located at cross section of two flows would decrease when the frames awaiting transmission at its MAC layer move five hops along the direction of flow. Further, it has been proved in section 4.2 that every node can transmit approximately 5 data packets during a period between its two successive beacons. Therefore, the information of load with nodes passed through periodic beacons will not be that obsolete for 5-hop nodes even if the latest information reaches a node after 5 successive beacons.

The average load at a node within a 'safe-distance' may become more than the time interval between two beacons if (i) any of the flow continues to increase its number of bytes and/or packets to be transmitted, or (ii) the number of frames moving out of a circle of radius of 'safe-distance' are outnumbered by the number of frames coming into the circle. Any one or both such situations may occur for a few circles of 'safe-distance' within a network for a few consecutive periods between two successive beacons.




Nodes connected with vertical lines have one unit of normalized distance from each other and those connected with horizontal lines or lines at an angle are separated by a 'safe-distance'. Innermost dark circle shows parallel transmitter-receiver pairs for β=6, next dark circle for β=4 and outermost dark circle is for β=2 for a network with 12 units of normalized radius with α=2.2, N=0.006 (-22.2185dB). Innermost circle with dotted lines is for network with 6 units normalized radius, next dotted circle is for 8 units of radius and outermost circle is for 12 units normalized radius for β=6, α=2.2, node spacing in grid form = 0.8 and maximum noise as 1.5 times the signal at the periphery of circle.

**Fig 1: Placement of maximum number of parallel transmitter-receiver around T-R pair at the centre of the network for varying values of β.**

**Table 12: Transmission time of RTS, CTS, DATA and ACK frames**

| Type of frame | | Network layer | MAC layer | Physical Layer | | Total Transmission time in micro-seconds |
|---|---|---|---|---|---|---|
| | | | | PLCP Preamble | PLCP Header | |
| RTS | Size of data | | 20B | 9B | 6B | |
| | Transmission time | 80 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 176 µs @ 2Mbps |
| CTS & ACK | Size of data | | 14B | 9B | 6B | |
| | Transmission time | 56 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 152 µs @ 2Mbps |
| Data | Size | 2000B | 34B | 9B | 6B | |
| | Transmission time | 8136 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 8232 µs @2Mbps |
| | | 2869 µs @5.5 Mbps | | | | 2965 µs @ 5.5Mbps |
| | | 1480 µs @11 Mbps | | | | 1576 µs @ 11Mbps |
| Data | Size | 1400B | 34B | 72b | 6B | |
| | Transmission time | 5736 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 5832 µs @ 2Mbps |
| | | 2086 µs @5.5 Mbps | | | | 2182 µs @ 5.5Mbps |
| | | 1043 µs @11 Mbps | | | | 1139 µs @ 11Mbps |
| Data | Size | 1000B | 34B | 72b | 6B | |
| | Transmission time | 4136 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 4232 µs @ 2Mbps |
| | | 1504 µs @5.5 Mbps | | | | 1600 µs @ 5.5Mbps |
| | | 752 µs @11 Mbps | | | | 848 µs @ 11Mbps |
| Data | Size | 500B | 34B | 72b | 6B | |
| | Transmission time | 2136 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 2232 µs @ 2Mbps |
| | | 777 µs @5.5 Mbps | | | | 873 µs @ 5.5Mbps |
| | | 389 µs @11 Mbps | | | | 485 µs @ 11Mbps |
| Data | Size | 250B | 34B | 72b | 6B | |
| | Transmission time | 1136 µs @2 Mbps | | 72 µs @ 1Mbps | 24 µs @ 2Mbps | 1232 µs @ 2Mbps |
| | | 414 µs @5.5 Mbps | | | | 510 µs @ 5.5Mbps |
| | | 207 µs @11 Mbps | | | | 303 µs @ 11Mbps |

**Table 13: Computation of minimum time between two successive Beacons by same node**

| Size of data packet | Time wasted due to RTS collisions | Time wasted in backoff slots | Minimum time between beacon packets | | |
|---|---|---|---|---|---|
| | | | 2Mbps | 5.5Mbps | 11Mbps |
| 250B | Number of packets * Estimated number of collisions per packet * (Time for RTS + DIFS + SIFS) = 716 * 4 * (176+50+10) / 1000 = 675.904 msec | Estimated Number of collisions * time for estimated number of backoff slots per collision = (716*4)*(8*20 / 1000) = 458.24 msec | Transmission time for 108 beacons & 608 data packets + time wasted due to RTS collisions + time wasted due to backoff slots (1.792*608 + 6.392*108 + 675.904 + 458.24) msec = 2.914016 seconds | Transmission time for 108 beacons & 608 data packets + time wasted due to RTS collisions + time wasted due to backoff slots (1.07*608 + 2.742*108 + 675.904 + 458.24) msec = 2.08084 seconds | Transmission time for 108 beacons & 608 data packets + time wasted due to RTS collisions + time wasted due to backoff slots (0.863*608 + 1.699*108 + 675.904 + 458.24) msec = 1.84234 seconds |
| 500B | 412 * 3 * (176+50+10) / 1000 = 291.696 msec | (412*3)*(4*20 / 1000) = 98.88 msec | {304 data packets} (2.792*304 + 6.392*108 + 291.696 + 98.88) msec = 1.92968 seconds | {304 data packets} (1.433*304 + 2.742*108 + 291.696 + 98.88) msec = 1.122344 seconds | {304 data packets} (1.045*304 + 1.699*108 + 291.696 + 98.88) msec = 0.891748 seconds |
| 1000B | 260 * 2 * (176+50+10) / 1000 = 122.072 msec | (260*2)*(2*20 / 1000) = 20.8 msec | {152 data packets} (4.792*152 + 6.392*108 + 122.072 + 20.8) msec = 1.561591 seconds | {152 data packets} (2.160*152+ 2.742*108 + 122.072 + 20.8) msec = 0.767328 seconds | {152 data packets} (1.408*152 + 1.699*108 + 122.072 + 20.8) msec = 0.54038 seconds |
| 2000B | 184 * 2 * ((176+50+10) / 1000) = 86.848 msec | (184*2)*(2*20 / 1000) = 14.72 msec | {76 data packets} (8.792*76 + 6.392*108 + 86.848 + 14.72) msec = 1.460096 seconds | {76 data packets} (3.525*76 + 2.742*108 + 86.848 + 14.72) msec = 0.665604 seconds | {76 data packets} (2.136*76 + 1.699*108 + 86.848 + 14.72) msec = 0.447396 seconds |

## 6. CONCLUSION

Proposed cross-layer node-disjoint multi-path routing protocol finds routes that do not get congested throughout the network and are outside the interference range of other routes for the same source-destination pair. At MAC layer, it prevents collisions due to interference. The proposed protocol derives a static value of maximum load at any node by provisioning for multiple collisions per packet and number of backoff slots per collision.

The design process of proposed cross-layer routing protocol assumes near worst situations in real life for computing maximum interference signal and load at any node. However, adoption of static value of the maximum load on any node may tend to decrease the maximum achievable throughput.

## 7. ACKNOWLEDGMENTS

Our sincere thanks to Professors Divya Gupta and Sandhya Rai of IMS Ghaziabad for their valuable discussions during the development of this paper.

## 8. REFERENCES

[1] Perkins C. E. et al.: "Ad Hoc On Demand Distance Vector (AODV) Routing", RFC 3561, July.2003.

[2] D. Johnson,Yi Hu and D. Maltz: "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", RFC 4728, draft-ietf-manet-dsr 2007.

[3] Li X. and Cuthbert L., On-demand Node-Disjoint Multipath Routing in Wireless Ad hoc Networks, In Proceedings of the 29th Annual IEEE Conference on Local Computer Networks, LCN 2004, Tampa, Florida, U.S.A., November 16-18, 2004, pages 419-420.

[4] Ye Zhenqiang, Krishnamurthy Srikanth V., Tripathi Satish K., "A Framework for Reliable Routing in mobile Ad Hoc Networks"; 22nd Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies, March 30 – April 3, 2003, pages 270-280 vol.1.

[5] Abbas A.M., Abbasi T.A.; "An Improvement over Incremental Approach for Guaranteed Identification of Multiple Node-Disjoin Paths in Mobile Ad hoc Networks" International Conference on Communications Systems Software and Middleware, Bangalore, COMSWARE 2007, 7-12 an. 2007.

[6] Yang Wenjing, Xinyu Yang, Guozheng Lu, Wei Yu, "An Interference Avoidance Multipath Routing protocol based on greedy forwarding in MANETS" IEEE International conference on Wireless Communications, Networking and Information Security (WCNIS), June 25-27, 2010, pages 483-487.

[7] Lal Chhagan, Laxmi V., Gaur M.S. "A Node-Disjoint Multipath Routing Method based on AODV protocol for MANETs"; 26th IEEE International Conference on Advanced Information Networking and Applications, 26-29 March, 2012, pages 399-405.

[8] Shunali Deng, Liping Liu, "A Node-disjoint Multipath Routing protocol based on AODV" Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), 10-12 Aug., 2010, pages 312-316

[9] Chang-Woo Ahn, Sang-Hwa Chung, Tae-Hun Kim, Su-Young Kang, "A Node-Disjoint Multipath Routing Protocol Based on AODV in Mobile Ad-hoc Networks", Seventh International Conference on Information Technology: New generation (TING), 12-14 April 2010, pages 828-833, IEEE Explore, 2010.

[10] Zangeneh, S. Mohammadi, "New Multipath Node-Disjoint Routing Based on AODV Protocol": World Academy of Science, Engineering and Technology 76 2011

[11] Gupta Rajendra Kumar, "Node Disjoint Minimum Interference Multipath (ND-MIM) Routing Protocol for Mobile Ad hoc Networks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012.

[12] Teo J.Y., Ha Y. Tham C.K., "Interference-Minimized Multipath routing with Congestion Control in Wireless Sensor Network for High-Rate Streaming", IEEE Transactions on Mobile Computing, Vol.7, No.9, September 2008, pages 1124-1137.

[13] Tiantong You , Chi-Hsiang Yeh , Hossam Hassanein "A New Class of Collision Prevention MAC Protocols for Wireless Ad Hoc Networks" IEEE International conference on Communications, ICC 2003, May 11-15, 2003, pages 1135-1140, vol.2.

[14] Khamayseh Yaser, Darwish O.M., Wedian S.A.,"MA-AODV: Mobility aware Routing Protocols for Mobile Ad Hoc Networks", Fourth International Conference on Systems and Network Communications, 20-25 Sept. 2009, pages 20-25.

[15] Sarma Nityananda, Nandi Sukumar, "A Multipath QoS Routing with Route Stability for Mobile Ad Hoc networks". In IETE Technical Review 2010, volume 27, issue 5, pages 380-397.

[16] Yaser Khamayesh, Ghadeer Obiedat, Munner Bani Tassin, "Mobility and Load aware Routing protocol for ad hoc networks", Journal of King Sahd University – Computer and Information Sciences, Volume 23, Issue 2, July 2011, Pages 105-113.

[17] Manocha R. K., Agarwal R. P., Srivastava A. "A MAC Protocol to prevent Collisions due to Interference for MANETS" International Journal of Computer Science and Systems, volume 2, Issue 2, pages 92-107.

[18] Manocha R. K., Agarwal R. P., Srivastava A. "Modifications in IEEE 802.11 to prevent Collisions due to Interference in MANETS"; International Journal of Computer Applications, volume 50(17):11-18, July 2012.

[19] R. Maheshwari, S. Jain and S. R. Das; "A measurement study of interference modeling and scheduling in low power wireless networks"; In SenSys, pages 141–154, 2008.

[20] Georgios P., Merkourios K., Martin M., Thrasyvoulos S., Bernhard P.; "Interference in Wireless Multihop Networks: A Model and its Experimental Evaluation" International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM, Newport Beach, CA, 23-26 June 2008, pp. 1 – 12.