Route Discovery by Cross Layer Approach for MANET

Mehajabeen Fatima	Roopam Gupta	T.K. Bandhopadhyay
RGPV, Bhopal, India	RGPV, Bhopal, India	BIST, Bhopal, India

ABSTRACT

Link breakage is of high probability in mobile wireless adhoc networks because of highly dynamic nature of MANET. This is because of limited transmission range, mobility and limited battery power. It becomes difficult to maintain continuous links in the networks. In AODV, node generates a RERR message for the given destination when it noticed that a link breakage has taken place. This hampers the continuity of the link and results in link breakage, in loss of some packets and increase in delay and overhead. Link breakage, delay and packet loss is not tolerable in real time communication and loss of packets, more overhead is not tolerable in non real time communication. So AODV is modified to cope up with these problems. An algorithm using cross layer approach is proposed which helps in maintaining the continuity of the network resulting in more throughput, less delay, less overhead and less battery power consumption which can be used for both real time and non real time communication.

KEYWORDS: MANET, AODV, Battery power consumption, Link breakage, Critical node, Hello warning message.

1. INTRODUCTION

A MANET is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. Some or possibly all of these nodes are mobile. This network can be deployed rapidly and flexibly. Every node has its own transmission range and every node acts as a router used for data transmission of all nodes with data of itself[1]. The mobile ad hoc networks provide new applications, but also face significant technical challenges. Comparing with wired networks, wireless adhoc networks have less bandwidth, longer paths, and less stable connectivity, routing protocols of wired networks are less suitable for the wireless. So more strong routing protocols are required keeping all parameters of MANET in view. For searching of path, a number of MANET routing protocols are available. Types of routing protocols and overview of AODV are discussed in Part 2 and Part 3 respectively. In part 4 cross layer approach is considered. In part 4 and part 5 transmission power, channel model and Received signal strength is discussed respectively. Part 6 has taken Battery Power consumption. Battery models and Energy systems, models are discussed in Part 7 and Part 8 respectively. Fuzzy logic and Proposed algorithm is given in part 9 and 10 respectively. In Part 11 message formats are given. Part 12 discussed performance parameter.

2. TYPES OF ROUTING PROTOCOL

For searching of path, a number of MANET routing protocols are available as given below.

2.1 Table-driven or Proactive routing protocols:

In this type of protocols like DSDV and OLSR, each node maintains individual routing table for every node in the network containing routing information. Each node maintains current routing information by listening and sending control messages periodically among the nodes which update their routing tables. The drawback of this protocol large overhead.

2.2 Reactive or On Demand Routing Protocol:

In this type of routing protocols like DSR and AODV, whenever a node wants to send packets to a destination, it starts the route discovery mechanisms to find the route to the destination. It does not maintain any previous route information for long time and no need to maintain up-to-date routing information as in proactive routing protocol. This reduces overhead. It has more delay.

2.3 Hybrid Routing Protocol:

Hybrid routing protocol like ZRP and TORA, combines the advantages of both proactive and reactive routing protocols. The route is initially established with help of routing tables in which route path is already available and then serves the demand from additionally activated nodes through reactive flooding. A brief summary of routing protocols is given in table 1

Table 1 Advantage and disadvantage of different types of protocols

Protocol type	Advantage	Disadvantage
Proactive	Uptodate routing information Quick establishment of routes Small delay Uptodate routing information Less overhead	Tendency of creating loops Large amount of resources required Routing information not fully used

Reactive	Less memory requirement Reduction of routing load Loop free	Large delay More overhead More power consumption
Hybrid	Scalability Limited search cost Up to date routing Information within zone	proactive scheme within zones More resources needed for large size zones

3. OVERVIEW OF AODV

AODV is on-demand routing protocol. Whenever it is required to send the data, route is discovered. The route discovery and route maintenance is done by four messages in AODV. These messages are Route Request (RREQ) and Route Reply (RREP), Route Error (RERR) and HELLO messages. Route Request (RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and HELLO messages are used for route maintenance.

Whenever a node wants to communicate, source determines a route to a destination node. The source node floods the network with a Route Request (RREQ) message. The source node broadcasts a RREQ message to its neighboring nodes which in turn broadcast the message to their neighbors and so on as shown in Fig.1. Each node stores latest forwarded route requests in register of route request. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count. When a node receiving the request either knows of a "fresh enough" route to the destination or is itself the destination, the node generates a Route Reply (RREP) message as shown in Fig. 2 and sends this message along the reverse path back towards the originating node. As the RREP message passes through
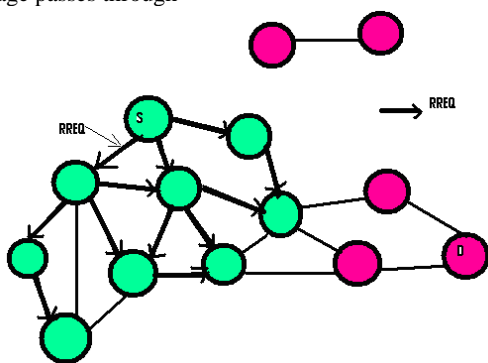

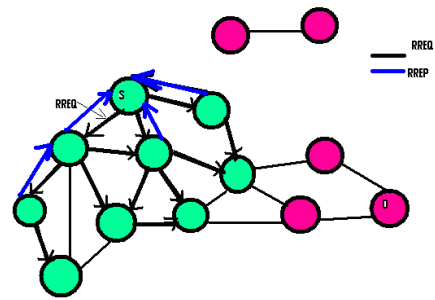**Fig 1 Route Requests in AODV**

Fig 2 Reverse Path Setup in AODV

intermediate nodes, these nodes update their routing tables. So in the future, messages can be routed through these nodes to the destination. It is possible for the RREQ originator to receive a RREP message from more than one node as shown in Fig.3. In this case, the RREQ originator will update its routing table with the most recent routing information means it uses the route with the greatest destination sequence number.
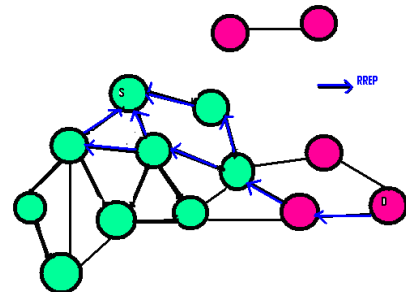

Fig 3 The destination will reply the source by RREP message

Each node periodically sends HELLO messages to its precursors. If a node has received no messages from some outgoing node for some fixed period of time then that node is presumed to be no longer reachable. Whenever a node determines one of its next- hop to be unreachable, it generates a Route Error (RERR) message. The node sends the RERR to each of its precursors. These precursors update their routing tables and in turn forward the RERR to their precursors and so on.

P.Kuppusamy et.al has given a comparison of three different types of protocols OLSR, AODV and TORA. These protocols are compared for Low mobility, Low traffic and High mobility, High traffic as given in table 2 and 3 respectively. As per table 2 and 3, the performance of TORA is better for dense networks, AODV performs well for moderately dense networks and OLSR is better in sparse networks[2].

Table2[2]

Low Mobility and Low Traffic				
Protocol	End to End delay	Packet delivery ratio	Path optimality	Routing overhead
OLSR	Low	High	Good	Low
AODV	Average	High	Average	Low
TORA	Low	High	Good	Average

Table3[2]

High Mobility and high Traffic				
Proto col	End to End delay	Packet delivery ratio	Path optim ality	Routin g overhe ad
OLS R	Low	Average	Avera ge	Low
AOD V	Avera ge	Average	Avera ge	Low
TOR A	High	Low	Avera ge	Averag e

DSDV is more suitable for small networks with limited changes in the topology. DSDV could be considered for delay constraint networks. DSR is suitable for moderate speeds mobile node networks. It is suitable for power constrained network. AODV is better than DSR and TORA[3] but AODV performance degraded when the node density is increased. This is because of its poor routing strategy in a network that has relatively static topology. It also scaled poorly when the density is in the region of 100 nodes or more[4]. In AODV protocol, delay is more and it is always discussed but link breakage probability, power consumption, control packets are also more and these parameters are not discussed till now. That's why AODV is taken for the improvement MANET uses traditional architecture which does not give optimized results. Better improvement can be done using new approach instead of traditional architecture. This new approach is cross layer approach.

4. CROSS LAYER APPROACH

In fourth generation (4G) communication, wireless networks and other networks is expected that Mobile Ad hoc Network (MANET) can be used economically anywhere at anytime i.e. pervasive computing. But before moving to pervasive computing MANET face lots of technical challenges. One of them is traditional architecture. The Traditional architecture is hierarchical model of TCP\IP which is used for networking and traditional hierarchical layered design of network protocols is inflexible to cope with the dynamics of Mobile Adhoc Network. Cross-layer design breaks away from traditional network design. In traditional network design, each layer of the protocol stack operates independently and information is exchanged only between adjacent layers of the protocol stack[5] as shown in Fig. 4. Because of the direct dependencies between the physical layer and the upper layers, the traditional protocol stack is not sufficient for Mobile Adhoc Networks. The careful exploitation of some protocol interactions that cross the normal layer boundaries can improve the performance of the communication and hence better application-layer performance. The dependent design between the layers blur the boundary between two adjacent layers[6].
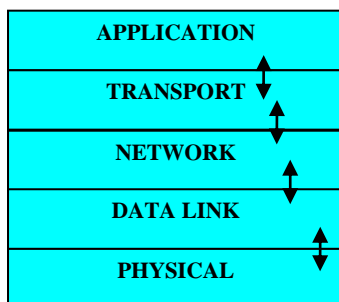

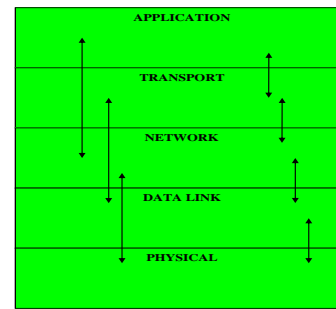**Fig. 4 Traditional Approach- Information exchange**

Fig. 5 Cross layer approach - Information exchange

In Cross-layer design, the information is exchanged between different protocol layers dynamically[7]. The information can be exchanged between any different layers of the protocol stack directly as shown in Fig. 5 In a wireless network, physical layer, MAC layer and routing layer together contend for the network resource. At physical layer transmission power and data rate is decided affects MAC and routing decisions. The MAC layer is responsible for scheduling and allocating the wireless channel, it will determine the available transmitter bandwidth and the packet delay. Routing layer also depends on bandwidth and delay to select the link. The routing layer chooses the route to send the data packets to the destination. The routing decision will change the contention level at the MAC layer and accordingly the physical layer parameters [8]. Because of adaptation of layers end to-end performance can be optimized. Any design changes in the protocol stack when adding interaction between different layers may have effect on the whole system, which may lead to spaghetti design[9]. So cross layer design use with caution.

5. TRANSMISSION POWER AND CHANNEL MODEL

Channel or physical layer decides the transmission power, data rate, bandwidth etc. There is some power loss in a channel during transmission. To model this loss, path loss channel models are available. They are free space, two ray model, Irregular Terrain model, OKUMARA-HAA, path loss matrix, Suburban, Urban model, street model, irregular terrain model e.t.c. With the help of these models minimum required transmission power, reception power, distance, gain of antenna etc can be calculated. All models have different parameters and suit to different environment. Two radio propagation models are the Friis free Space Attenuation model and the Two-Ray Ground Reflection model. At near distances, the Friis free space attenuation model holds true where the received signal strength is inversely proportional to the square of the distance (d) between the transmitting antenna and the observing point while at far distances the received signal strength varies in accordance with the Two-Ray Ground propagation model (inversely proportional to d^4). For distances less than the reference point, the Friis model is used and beyond the reference point the two-Ray model is used. The Free-space propagation model relation given by equ.1

$$P_R = P_T \left(\frac{\lambda}{4\pi d} \right)^2 G_T G_R \text{ ---------(1)}$$

where λ is wavelength of carrier, d is distance between sender and receiver, G_T and G_R are gain of transmitting and receiving antennas respectively. The effects of noise and fading are not considered[3]. The receiving node calculates the path loss by equ.2.

$pathloss = P_T - P_R$ ----------(2)

So the minimum required transmission power (P_{Tmin}) can be calculated by equ.3

$P_{T\min} = k * (Pathloss + R_{TH})$ ----------(3)

where R_{TH} is receiver threshold, the minimum received power required for proper signal detection. The multiplication factor "k" is considered to provide marginal hike in minimum required transmission power to withstand against the effect of interference on packet reception.

So P_{Tmin} is minimum transmission power required to transmit such that it should be receive on other node.

Free space propagation considers the wavelength or frequency used for transmission and reception. It can be used to determine minimum required transmission power, minimum required reception power, distance. If distance is calculated then speed can also be calculate. In this paper equ. 3 is used to calculate speed.

6. RECEIVED SIGNAL STRENGTH (RSS)

In cross-layer designs, RSS is measured at physical layer and can be made available to the top layers. RSS information can be used to judge whether the nodes are approaching or leaving the transmission range. RSS can be used to compute the minimum sufficient transmit power to obtain energy conservation, interference reduction, and spatial reuse. RSS information is also used to compute path loss incurred in order to identify and reject the unidirectional links. RSS is also used to choose reliable links to form stable routes by monitoring the signal quality to judge whether the neighbors are approaching or leaving [10]. Consider the signal strength of two devices D_1 and D_2 with possible signal from very low to excellent. The change (ΔD_1, ΔD_2) is considered within an observation time. This observation time can be found on an empirical basis and ranges from seconds to a few minutes. If Device D_2 has stronger signal strength at current time and device D_1 has a more stable signal strength at all time[11]. The device with more stable signal strength is better than the another device may currently have a stronger signal strength.

In this paper RSS is used to see the direction of node whether the node is coming inside of transmission range or moving away from transmission range. When a node receives a particular value of signal strength of a packet then only it can be received by receiver node but if the packet signal strength is less than a particular value the node willn't be able to receive it. This sets a threshold, RSS threshold used in AODV is −78 dBm and AODV - Adaptive uses a value from the set of values (−81, −80.5, −80, −79, −78 dBm) that depends on the maximum speed of nodes in the range of 0-25 m/s[11]. In this paper range of RSS is taken from -30dbm to -70dbm and the threshold is considered at   -70dbm.

7. BATTERY POWER CONSUMPTION

The choice of the power level affects operation of the network like the transmit power level determines the quality of the signal received at the receiver, it determines the range of a transmission, it determines the magnitude of the interference create for the other receivers[12]. The power consumption can be control by choosing the transmit power for each packet in a distributed fashion at each node in ad hoc networks and the impact of power control on a variety of parameters and phenomenon can lead to fundamental design principles [12].

The total battery power consumption (BPC) can be given by

$BPC = (N_t * I * P_t) + (N_r * J * P_r) + (P_{idel}) + (P_{sleep})$ ---(4)

Where N_t is number of times packet transmitted, I is size of transmitted packet, P_t is battery power consumption in transmission of a packet, N_r is number of times packet is received, J is size of received packet, P_r is battery power consumption in reception of a packet, P_{idel} is battery power consumption in ideal mode, P_{sleep} is battery power consumption in sleeping mode.

Most of the power consumes in transmission of packet. The power also consumed in discarding of packets, in collision of packets and in interference[13]. Whatever is the mode of packet, the power consumed either in transmission or in reception of packets[14]. Equation 4 shows that battery power consumption can be reduced if less number of packet transmitted or received. So instead of sending Hello message periodically as in basic AODV, only one Hello message as HWM sends in proposed protocol of route discovery by cross layer approach routing protocol (RDCLRP)[14]. Because of HWM, no need to send Hello message again and again, the RERR messages have not to send back to source and no need to flood RREQ. This saves lots of battery.

8. BATTERY MODEL

MANET is battery constraint device. Most cell phones, laptops, tablet laptops etc can take anywhere, anytime use rechargeable electrochemical batteries like, lithium-ion batteries. These batteries take approx. 1 to 4 hours to charge fully but they can run for only a few hours[15]. So it is required to reduce battery power consumption as minimum as possible. For calculation of battery power consumption battery power models are required. For this number of battery models are available as shown in Fig. 7
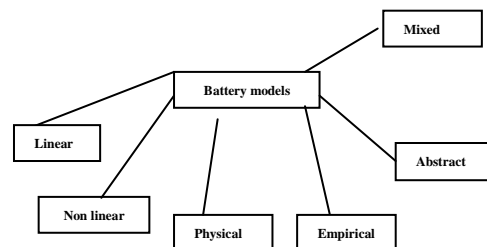
Battery discharge behavior is sensitive to the discharge rate, temperature and the number of charge-recharge cycles[16]. So battery discharge deviates from its ideal linear behavior. Lower efficiency means less battery energy remains and thus the battery lifetime is proportionally lower. Example, if battery efficiency is 60% and its rated capacity is 100 mAhr at 1 V, then the battery would be drained in 12 min at an average DC-DC current of 300 mA. With efficiency of 100% the battery would last 1 h[17, 18].

9. ENERGY AND SYSTEM MODEL

Battery provides voltage and current for the components attached to the battery such as radio interfaces, CPU, Memory blocks, sensing core etc. A DC-DC converter regulates voltage for different components as in Fig. 6. Battery is a repository of electrical charges which losses its charge when a load (electrical current) is taken off from it. The loss rate is a function of the load.
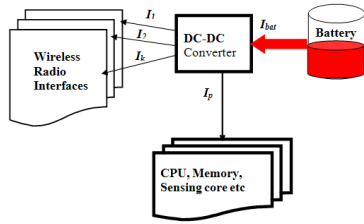
Fig.6 System Level Block of Smart Batteries

$$E_{cycle} = E_{trans} + E_{CPU} + E_{DC} + E_{BAT} \text{-------(5)}$$

The total energy consumed by the system per cycle (E_{Cycle}) is the sum of energies consumed by the radio transceivers(E_{Trans}), protocol processor (E_{CPU}), the DC-DC converter (E_{DC}) and the efficiency losses in the battery (E_{Bat}). Several high level simulation based models have been reported like pspice equivalent circuits, a discrete time VHDL model and markov chain model. Some battery models are also available for simulation like service life battery model and residual life battery model.

9.1 Service Life Battery Model:

This model estimates the total service life of the battery (i.e. the time it takes the battery charge to reach zero from the start).The battery model is a modular approach for enhancing event-driven simulator with precise high battery level which can accurately estimate service life of a battery-operated device with a given -time-varying load.

Parameter Estimation done by Rakhmatov's model. This model is an abstraction of a real battery. For the model to adequately mimic real behavior of the batteries, it is recommended to choose the appropriate parameters so that the predicted and observed lifetimes match closely. Thus, before one can use the proposed model, the parameters need to be estimated from experimental data for the modeled battery. Simple experiments with constant loads are sufficient for estimation purposes and one can utilize the equation 6.

$$\alpha \approx I \left[L + 2 \sum_{m=1}^{10} \frac{1 - e^{-\beta^2 m^2 L}}{\beta^2 m^2} \right] \text{--------(6)}$$

For a given battery under a given load, the battery voltage changes over time from the open-circuit value, V_{open}, to some cutoff value, V_{cutoff}. The observed lifetime is defined as the time when the battery voltage reaches V_{cutoff}. The predicted lifetime is defined as the time for which the equality (6) holds. For a given set of constant loads $\{I(1),I(2),...,I(M)\}$, the corresponding set of observed lifetimes is $\{L(1),L(2),...,L(M)\}$. The objective is to find and such that the predicted lifetimes match the observed lifetimes as closely as possible. However this objective is hard to pursue directly, since (6) is hard to solve for the unknown L. Alternatively one can estimate parameters by fitting the load values for a given set of observed lifetimes.

9.2 Residual Life Battery Model

This model estimates the remaining service life of the battery at any time in the simulation.

Battery Capacity and Efficiency

One important characteristic of the battery is that some amount of energy will be wasted when the battery is delivering the energy required by the circuit. In analytical form, given a fixed battery output voltage, if the circuit

current requirement for the battery is 1, the actual current that is taken out of the battery is

$$I^{act} = \frac{I^{bat}}{\mu}, 0 \langle \mu \leq 1 \text{-----------(7)}$$

where μ is called the battery efficiency (or utilization) factor. I^{act} is always larger than or equal to I^{bat}. Defining CAP^0 as the amount of energy that is stored in a new (or fully charged) battery and CAP^{act} as the actual energy that can be used by the circuit, (7) is equivalent to:

$$CAP^{act} = \mu . CAP^o \text{------------(8)}$$

The efficiency factor is a function of discharge current I^{bat}:
$$\mu = f\left(I^{bat}\right)$$

where, $f(.)$ is a monotonically decreasing function. Only the low-frequency part of the current is relevant to changing the battery efficiency. Therefore, I^{bat} must be the average output current of the battery (denoted by i(t) over certain amount of time, which can be represented as $N.T$, where N is some positive integer and T is the clock cycle, as shown in the equation 9. $N.T$ may be as large as a few seconds.

$$I^{bat} = \frac{1}{N.T} \int_{0}^{N.T} i(t).dt \text{-------(9)}$$

10. FUZZY LOGIC

Fuzzy logic is a set of classical logic with degree of membership. Fuzzy Logic set was particularly designed to mathematically represent fuzziness and vagueness and to provide the fundamental concept for handling the imprecision intrinsic to the problems of subjective evaluation and measurement. Fuzzy set is based on possibility instead of probability. A Fuzzy logic differs from classical logic systems in that it aims modeling the imprecise modes of reasoning that play an essential role in the human ability to make rational decisions in uncertainty and imprecision. This depends on ability to infer an approximate answer to a question based on a store of knowledge that is incomplete or totally not available. Fuzzy logic comprises fuzzy sets which are methods of representing non statistical uncertainty and approximate reasoning including the operations used to make inferences. Uncertainties are presented as fuzzy sets (**Ai**), which are often expressed by words and interpreted by their membership functions μ_A. A fuzzifier is used at the input of the system to convert crisp to fuzzy data while a defuzzifier - from fuzzy to crisp data.

It is a tool for mapping the input features to the output based on data in the form of "IF – Then" rules controller. Fuzzified input data trigger one or several rules in the fuzzy model to calculate the result. IF-THEN rules map the input values to the output space in terms of implication relation between fuzzy sets in "IF" and "THEN" parts. Fuzzy reasoning is numerically processing of the information in the fuzzy rules.

$$f = \frac{\sum_{i=1}^{p} x_i * \mu(x_i)}{\sum_{i=1}^{p} \mu(x_i)} \text{----------(10)}$$

Equ.10 shows the defuzzification functions for *f*. The defuzzification method uses the center-of-maximum (CoM), where x_i is the input, p is the number of rules, and *f* is the output[19]. Mamdani type fuzzy controller uses a range of input variables for making membership function[20] as shown

in Fig. 7. Whereas Takagi-Sugeno type fuzzy controller is also available in which a constant value is taken instead of range for making membership function. The Mamadani's fuzzy logic is used in this paper. A fuzzy rule is a conditioned rule where all inputs must be initiated simultaneously and will affect the output. In this paper three inputs are taken and each has membership functions then 36 conditions can be cited and used simultaneously.
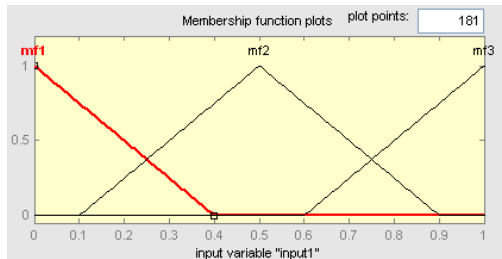
Fig 7 fuzzy membership functions

In the proposed algorithm three input variables are taken and one output variable. Three input variables are Battery power(P_B), Received signal strength(RSS) and Speed(S) of a node. The output is a crisp value for Hello Warning message interval(HI)

A message called HWM has to be sent when a node finds out that it may not be able to provide proper connectivity between source and destination. This node is called critical node. HWM can be generated by only critical nodes when criticality is reached. The criticality is decided based on RSS received (threshold value = -25 dbm)and battery power (3W). Once criticality is decided the HWM is not sent instantaneously but after a time HI which is decided by the fuzzy logic table.

11. PROPOSED ALGORITHM FOR ROUTE DISCOVERY BY CROSS LAYER APPROACH

In basic AODV the path is searched when it is required to send the packets. The path is searched by RREQ and RREP messages, after searching of path, route has to be maintained. Route is maintained by periodic Hello messages. Every path which participate in transmission of packets acts as active path or active route and every node which participate in transmission of packets acts as active node send Hello message shows its presence in the transmission range and if a node does not send the Hello message for long time then it is assumed that it is die. Then a RERR message is sent back to source. Then source will reinitiate the route discovery procedure. Hello   message sends after every one second in basic AODV it increases overhead and traffic inturn increases possibility of congestion, consumes bandwidth unnecessarily and most important consumes battery power. So it is proposed that instead of this periodic Hello message, non periodic Hello message can be send as Hello warning message(HWM). HWM send only when a node touches the threshold of battery power(Bp) and received signal strength(RSS). If speed(S), transmission range varies then a node will go out of transmission range in different times, so HWM should be

$$HI\alpha B_P$$

$$HI\alpha RSS$$

$$HI\alpha \, 1/S$$

given adaptively. HWM depends on prediction of direction of node and remaining battery power. Direction of a node can be predicted by RSS, it is present at Physical layer. The value of RSS call on network layer from physical layer directly. The position of a node also depends on speed of a node and this speed is available at physical layer and this is also call on network layer - cross layer approach.

In proposed algorithm, the path is searched by RREQ and RREP. RREPAck should broadcast and it consist of address of origination node and the address of the node to which it has to be given. The neighbouring node will do the entry of these active nodes addresses in its routing table. Once path is established the data is communicated. But when a node is going out of transmission range or if its battery power touches threshold called critical node send a HWM to warn the nodes that the link is going to break after sometime. So warning has to be given before link breakage This warning is given by Hello warning message (HWM) and it should be broadcasted so that neighbour node can listen it[14]. HWM consist of addresses of its both active neighbours which are participating in transmission of packets. Neighbour nodes listen the warning message and they will see the address of HWM in its routing table. If neighbour node is having addresses of both active neighbours then it will reply to critical node by sending Hello reply message (HRM). The node which reply first will participate in new route. The critical node will reply service replicate (SRM) message consist of new node id to its active neighbour node. Now the old route will replace by new route before link breakage. So a new route is discovered through HWM locally. Critical node search the route locally and try to find out the route before link breakage. So instead of sending Hello message periodically, Hello sends as HWM only once whenever it is required. Because of this power will be less consumed, delay will be less and overhead reduces.   HWM interval is decided according to fuzzy logic.

A message called HWM has to be sent when a node finds out that it may not be able to provide proper connectivity between source and destination. This node is called critical node. HWM can be generated by only critical nodes when criticality is reached. The criticality is decided based on RSS received (threshold value = -25 dbm), and battery power (3W). Once criticality is decided the HWM is not sent instantaneously but after a time HI which is decided by the fuzzy logic table. Flow chart of the algorithm is shown in Fig.8

If transmission range T_r is more, less number of Hello are acceptable or more HWM interval (HI)is acceptable. If battery power B_p is more, more number of Hello messages are not required, more Hello warning message interval (HI)is acceptable. If speed increases then more number of Hello message are required. so HI should be reduced[14]. If RSS is more, no need to send hello messages again and again HI can be kept large. HI is directly proportional to transmission range T_r , Battery power B_p , received signal strength RSS and inversely proportional to speed S . Therefore,

Therefore

$$HI = \frac{KB_P RSS}{S} \text{---------(11)}$$

Where K is proportionality constant can be taken equal to one. Equation 11 shows the dependency of HI on transmission range, speed of node, battery power and received signal strength.

Table 4[14] Rule table for HI

S	B_p Low(L)			B_p Medium(M)			B_p High(H)		
	RSS			RSS			RSS		
	L	M	H	L	M	H	L	M	H
L	L	L	L	H	M	H	H	H	H
M	L	L	L	M	M	H	M	M	H
H	L	L	L	L	L	M	L	L	M

HI is made adaptive w.r.t. speed, RSS, transmission range and battery power. Low(L), medium(M) and high(H) values are taken for speed, transmission range, Received signal strength, battery power for making of fuzzification rules. Membership functions for different parameters consider different ranges. Rules for making HI adaptive are given in Table 4. With the fuzzy, HI is calculated and is given in table 5.
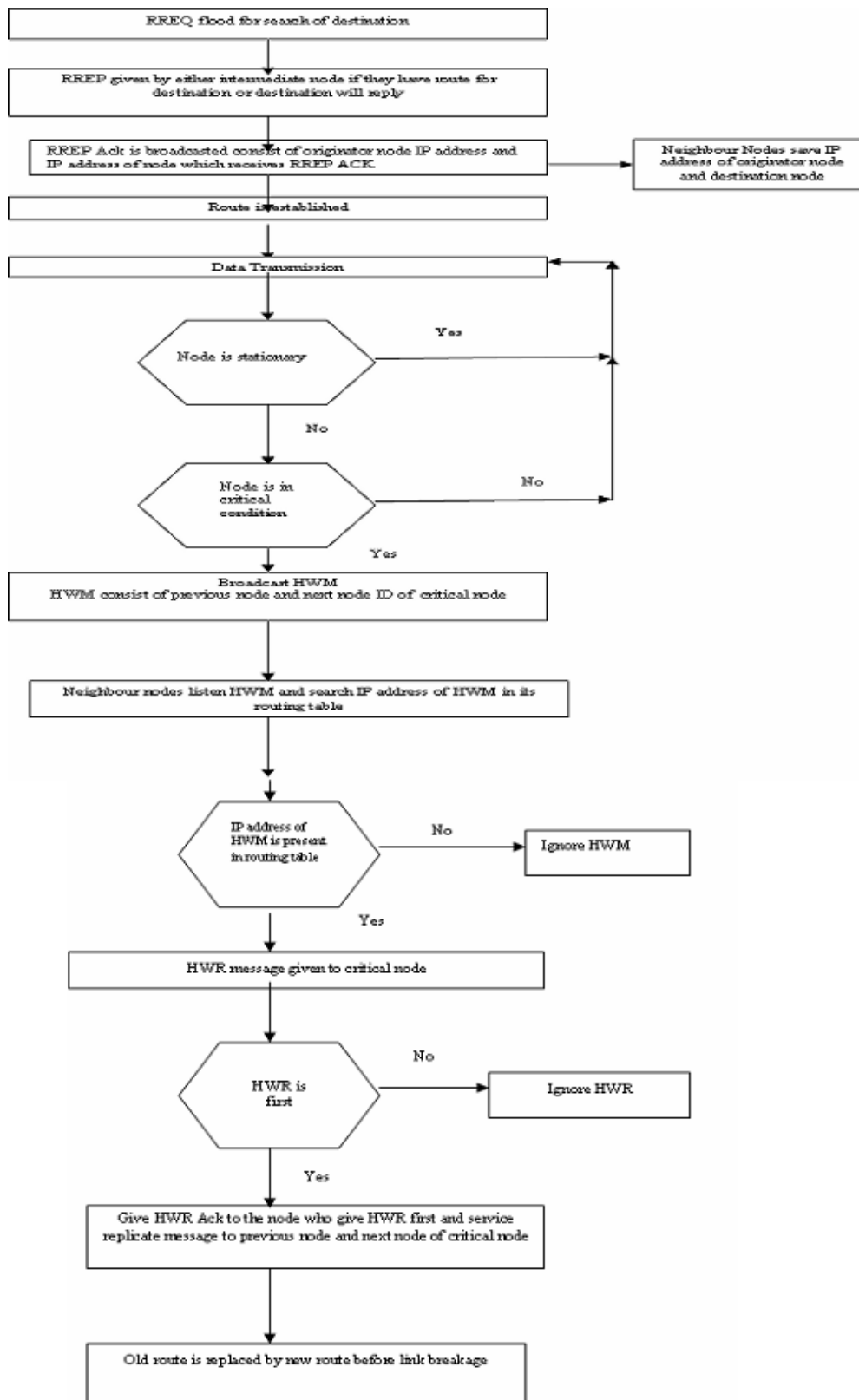
Table 5 Ranges for L, M, H values

Range	Speed((mps)	Transmission Range (m)	Battery Power(W)	Received signal strength(-dbm)	HI(s)
Low(L)	0-6	0-100	1-2	60-70	0-4
Medium(M)	6-12	100-200	2-3	50-60	4-8
High(H)	12-18	200-300	3-4	40-50	8-12

Table 6 *HI* calculated by fuzzy method for *B_p=H*

S (mps)	If RSS= H, B_p=M HI (s)	If RSS= M, B_p=M HI (s)	If RSS= M, B_p= M HI (s)
2	10.7	6	10.7
4	10.5	6	10.5
6	10.7	6	6
8	10.7	6	6
10	10.7	6	6
12	6	6	6
14	6	1.54	1.54
16	6	1.21	1.34
18	6	1.13	1.34

Table 7 *HI* calculated by fuzzy method for *B_p= M*

S (mps)	If RSS= H, B_p= H HI (s)	If RSS= M, B_p= H HI (s)	If RSS= M, B_p= H HI (s)
2	10.7	10.7	10.7
4	10.5	10.5	610.5
6	10.7	6	6
8	10.7	6	6
10	10.7	6	6
12	6	6	6
14	6	1.54	1.54
16	6	1.34	1.34
18	6	1.34	1.34

Fig 8 Flow chart of proposed algorithm

Table 8 *HI calculated by fuzzy method for $B_p= L$*

S (mps)	If RSS= H, B_p=L HI (s)	If RSS= M, B_p=L HI (s)	If RSS= M, B_p= L HI (s)
2	1.34	1.34	1.34
4	1.54	1.54	1.54
6	1.54	1.54	1.54
8	1.34	1.34	1.34
10	1.34	1.34	1.34
12	1.34	1.34	1.34
14	1.54	1.54	1.54
16	1.34	1.34	1.34
18	1.34	1.34	1.34

Fuzzy logic will incorporate in Network Simulator such that it calculate all above values if node is in critical condition to generate HWM.

12. MESSAGE FORMATS

Number of messages are used in the proposed algorithm. Its formats are given below in which format of RREP Ack is changed and some new messages like HWM, HWR, SRM are introduced.

Route Request (RREQ) Message Format[21]:

```
0               1               2               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|   Type    |J|R|G|D|U|  Reserved      |   Hop Count   |
                        RREQ ID
                  Destination IP Address
              Destination Sequence Number
                  Originator IP Address
              Originator Sequence Number
```

The format of the Route Request message is illustrated above, and contains the following fields:

Type   1

J   Join flag; reserved for multicast.

R   Repair flag; reserved for multicast.

G   Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field

D   Destination only flag; indicates only the destination may respond to this RREQ

U   Unknown sequence number; indicates the destination sequence number is unknown

Reserved   Sent as 0; ignored on reception.

Hop Count   The number of hops from the Originator IP Address to the node handling the request.

RREQ ID   A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.

Destination IP Address   The IP address of the destination for which a route is desired.

Destination Sequence Number   The latest sequence number received in the past by the originator for any route towards the destination.

Originator IP Address   The IP address of the node which originated the Route Request.

Originator Sequence Number   The current sequence number to be used in the route entry pointing towards the originator of the route request.

Route Reply (RREP) Message Format[21]:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    Type    |R|A|   Reserved    | Prefix Sz|
                        Hop Count
              Destination IP address
            Destination Sequence Number
                Originator IP address
```

The format of the Route Reply message is illustrated above and contains the following fields:

Type   2

R   Repair flag; used for multicast.

A   Acknowledgment required.

Reserved   Sent as 0; ignored on reception.

Route Reply Acknowledgment (RREP-ACK) Message Format:

The Route Reply Acknowledgment (RREP-ACK) message must be sent in response to a RREP message. This message should broadcast.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|   Type    |              Reserved
              next hop IP address
              Originator IP address
```

Type   3.

Reserved   Sent as 0; ignored on reception.

Next hop IP Address
        Next hope IP address to which RREP ack has to be given. It is broadcasted so that the neighbours can save address in its routing table.

Originator IP Address
        The IP address of the node which originated the RREQ. It is also broadcasted so that the neighbours can save address in its routing table.

Hello Warning Message(HWM) Format:

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Type | Reserved
Previous active node IP address
next active node IP address

Type   4

Previous active node IP address
        It is given so that neighbours can check their routing table whether it is present in its routing table or not.

 Next active node IP address
It is given so that neighbours can check their routing table whether it is present in its routing table or not.

Hello Warning Reply (HWR) Message Format:

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Type |A|G| Reserved | Hop Count
Destination IP address
Originator IP address

Type   5
A   Acknowledgment required

G
Gratuitous HWR flag; indicates whether a gratuitous HWR should be unicast to the node specified in the Destination IP Address field

Hop Count
The number of hops from the Originator IP Address to the critical node handling the reply.

Destination IP address
The IP address of the destination for which a reply is desired. HWR goes to critical node. This message is unicast

Originator IP address
The IP address of the node which originated the HWR.

Service Replicate Message (SRM) Format:
This message is given to previous active node and next active node of critical node.

Type   6

G
Gratuitous HWR flag; indicates whether a gratuitous HWR should be unicast to the node specified in the new node IP Address field.

New node IP address
This IP address is given to previous and next node of critical node.

Originator IP address
This IP address is the address of critical node who wants to resume its services and given to another node.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Type |G| Reserved
Originator IP address
New node IP address

13. PERFORMANCE PARAMETERS

Proposed algorithm improves following parameters, their formulae are given below. With the help of these formulae can see the improvements.

Throughput = Total number of arrival packets/ Simulation time

End to End delay = Total delay of arrival packets/ Number of arrival packets

Control Overhead= Total number of bits of sent control packets/ Total number of bits of sent packets

Total Overhead = Total number of bits of sent data packets/ Total number of bits of sent packets.

Packet delivery ratio= Total number of bits of received packets/   Total number of bits of sent packets

Link breakage ratio= Total number of link breakage/ Simulation time

Battery Power Consumption $=\{(N_t \times I \times P_t) + (N_r \times J \times P_r) + (P_{idel}) + (P_{sleep})\}$

14   CONCLUSION
Hello message of AODV is used as HWM for searching of route before link breakage to keep continuity of route. HWM Interval decided by fuzzy logic. This method tries that the active link should not break and move to another route before link breakage. So RERR of AODV is eliminated in this modified algorithm. Because of this no need to flood RREQ again inturn no need to give RREP, RREPAck, Hello

message. With transmission and reception of less number of control packets reduces overhead, this reduces battery power consumption, with this number of times link breakage reduces, so more number of packets arrives at destination in less time, this decreases delay and increases throughput. It increases bandwidth and reduces congestion. It can be done with the help of cross layer approach.

15. REFERENCES

[1] Mehajabeen Fatima, Roopam Gupta, and T.K. Bandhopadhyay, "RDCLRP-Route Discovery by Cross Layer Routing Protocol for Manet Using Fuzzy Logic", AIM, CCIS 147, pp. 348–351, 2011, Springer-Verlag Berlin Heidelberg 2011.

[2] P.Kuppusamy, Dr.K.Thirunavukkarasu "A Study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks", 978-1-4244-8679-3 /11/, 2011 IEEE

[3] M.Ramakrishnan1, S.B.M.Priya, S.Shanmugavel "Mathematical Modeling of Routing Protocol Selection for Optimal Performance of MANET" Second International Conference on Computer and Network Technology, IEEE, 2010

[4] Pore Ghee Lye and John C. McEachen "A Comparison of Optimized Link State Routing with Traditional Routing Protocols in Marine Wireless Ad-hoc and Sensor Networks", Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07),0-7695-2755-8/07, 2007

[5] Mohammad Abdur Razzaque, Simon Dobson, and Paddy Nixon, "Cross-Layer Architectures for Autonomic Communications", Journal of Network and Systems Management , 2006 DOI: 10.1007/s10922-006-9051-8.

[6] Vineet Srivastava and, Mehul Motani, Cross-Layer Design:A Survey and the Road Ahead 0163-6804/05, IEEE Communications Magazine, December 2005

[7] V. Srivastava and M. Motani, "Cross-layer design: A survey and the road ahead", IEEE Communications Magazine, Vol. 43, No. 12, pp. 112–119, Dec. 2005.

[8] Liang Qin and Thomas Kunz "Survey on Mobile Ad Hoc Network Routing Protocols and Cross-Layer Design", Carleton University, Systems and Computer Engineering, Technical Report SCE-04-14, August 2004

[9] Vikas Kawadia, P. R. Kumar, "A Cautionary Perspective On Cross-Layer Design", IEEE Wireless Communications, February 2005.

[10] B Ramachandran and S Shanmugavel "Received Signal Strength-based Cross-layer Designs for Mobile Ad Hoc Networks", IETE Technical Review, DOI10.4103/0256-4602.42811

[11] Guenter Prochart and Reinhold Weiss Reiner Schmid and Gerald Kaefer, "Fuzzy-based Support for Service Composition in Mobile Ad Hoc Networks", 1-4244-1 326-51071, 2007 IEEE

[12] V. Kawadia, and P. R. Kumar, "Principles and protocols for power control in wireless ad-hoc networks," IEEE Journal on Selected Areas in Communication, Part I, Vol. 23, No. 1, pp. 78-88, January 2005.

[13] Laura Marie feeney, Martin Nilson "Investigating the energy consumption of a wireless network interface in an adhoc networking environment", In Proceedings of IEEE INFOCOM, Anchorage, AK, 2001

[14] Mehajabeen Fatima, Roopam Gupta, T.K. Bandhopadhyay "RDCLRP-Route Discovery by Cross Layer Routing Protocol for Performance Improvement" V5-306, 978-1-4244-8679-3 /11/C 2011 IEEE .

[15] Ravishankar Rao, S. Vrudhula, D. Rakhmatov "Battery Modeling for Energy-Aware System Design" 0018-9162/03/, 2003 IEEE

[16] Daler N. Rakhmatov, Sarma B.K.Vradhula "Battery Modeling for Energy-Aware System Design", 0018-9162/03 , December, 2003, IEEE

[17] D. Rakhmatov, S. Vrudhula, and D. Wallach. "A model for battery lifetime analysis for organizing applications on a pocket computer." IEEE Transactions on VLSI. Vol. 11, 2003, 1019-1030.

[18] Daler N. Rakhmatov, Sarma B.K.Vradhula "An Analytical High level Battery Model for Energy-management of portable Electronic systems" 0-7803-7247-6/01, pn- 488-493, 2001, IEEE

[19] Anna Lekova, Katrine Skjelsvik, Thomas Plagemann, Vera Goebel, "Fuzzy Logic-Based Event Notification in Sparse MANETs", 0-7695-2847-3/07, 2007, IEEE Computer society.

[20] J. Martin Leo Manickam, S.Shanmugavel, "Fuzzy based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET", 0-7695-2889-9/07, 2007, IEEE Computer Society

[21] C. Perkins, E. Belding-Royer and S. Das, 'Ad hoc On-Demand Distance Vector (AODV) Routing", IETF, RFC: 3561, July 2003