IPHV7I10009X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

LOCATION-BASED PROBABILISTIC REBROADCAST FOR AVOIDING RE- ROUTING LOAD IN MANETS

[1]**M.Madhumitha Reddy**, [2]**V.Sowmya Devi**
Dept of CSE
GITAM University, Hyderabad

Abstract:- In mobile ad hoc networks, nodes are dynamically changing their locations. MOBILE ad hoc networks (MANETs) consist of a collection of mobile nodes which can move freely. These nodes can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. A mobile ad hoc network consists of wireless hosts that may move often. Movement of hosts results in a change in routes, requiring some mechanism for determining new routes. Several routing protocols have already been proposed for ad hoc networks. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. In this paper, we propose a neighbor coverage-based probabilistic rebroadcast protocol for reducing routing overhead in MANETs. In order to effectively exploit the neighbor coverage knowledge, we propose a novel rebroadcast delay to determine the rebroadcast order, and then we can obtain the more accurate additional coverage ratio by sensing neighbor coverage knowledge. We also define a connectivity factor to provide the node density adaptation. By combining the additional coverage ratio and connectivity factor, we set a reasonable rebroadcast probability. We propose Establishing a trust hierarchy path MUST be performed to verify authenticity and usability of certificates within IMEP(Internet MANET Encapsulation Protocol).

Keywords —*Manet, Aodv, Dsr, Rreq, Rerr, Mac, IEEE 802.11 Protocols.*

I. INTRODUCTION

Mobile Ad-Hoc Networks (referred to as MANETs), are impromptu wireless communication networks increasingly appearing in the Commercial, Military, and Private sector as portable wireless computers become more and more ubiquitous. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. However MANETs are not perfect. The challenges of scalability, mobility, bandwidth limitations, and power constraints of these networks have not been completely alleviated to date. Using location information to help routing is often proposed as a means to achieve scalability in large mobile ad hoc networks. However, location-based Probabilistic Rebroadcast for avoiding Re- Routing load is difficult when there are holes in the network topology and nodes are mobile or frequently disconnected to save battery. Terminode routing, presented here, addresses these issues. In smaller networks; the performance is comparable to MANET routing protocols. In larger networks that are not uniformly populated with nodes, existing location-based Probabilistic Rebroadcast for avoiding Re- Routing load or MANET routing protocols.

Since a MANET has no underlying information infrastructure and is multihop in nature, every node in the network functions as a router. The nodes are free to move arbitrarily, and the topology of the network can be considered to be dynamic. Mobility of the nodes also results in limited power supply and the dependence on batteries or exhaustible means of power. However, the advantages are numerous. Firstly, deployment is easy and speedy. Secondly, because there is no dependence on infrastructure, the network is robust and low-cost.

In this paper, we proposed two routing protocols like AODV(Ad hoc On-demand Distance Vector Routing), DSR(Dynamic Source Routing). Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes cooperate to forward packets for each other to allow communication over multiple "hops" between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol. Since the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing.

The DSR protocol is composed of two main mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

- Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.

Route Discovery and Route Maintenance each operate entirely on demand. DSR also supports internetworking between different types of wireless networks, allowing a source route to be composed of hops over a combination of any types of networks available. The conventional on-demand routing protocols use flooding to discover a route. They broadcast a Route REQuest (RREQ) packet to the networks, and the broadcasting induces excessive redundant retransmissions of RREQ packet and causes the broadcast storm problem, which leads to a considerable number of packet collisions, especially in dense networks . Therefore, it is indispensable to optimize this broadcasting mechanism. Some methods have been proposed to optimize the broadcast problem in MANETs in the past few years. We categorized broadcasting protocols into four classes: "simple flooding, probability-based methods, areabased methods, and neighbor knowledge methods." For the above four classes of broadcasting protocols, they showed that an increase in the number of nodes in a static network will degrade the performance of the probability-based and area-based methods . we indicated that the performance of neighbor knowledge methods is better than that of area-based ones, and the performance of area-based methods is better than that of probability-based ones.

We now obtain the initial motivation of our protocol: Since limiting the number of rebroadcasts can effectively optimize the broadcasting, and the neighbour knowledge methods perform better than the area-based ones and the probability-based ones , then we propose a Location based probabilistic rebroadcast (LBPR) protocol. Therefore, 1) in order to effectively exploit the neighbour coverage knowledge, we need a novel rebroadcast delay to determine the rebroadcast order, and then we can obtain a more accurate additional coverage ratio; 2) in order to keep the network connectivity and reduce the redundant retransmissions, we need a metric named connectivity factor to determine how many neighbors should receive the RREQ packet. After that, by combining the additional coverage ratio and the connectivity factor, we introduce a rebroadcast probability, which can be used to reduce the number of rebroadcasts of the RREQ packet, to improve the routing performance.

The main contributions of this paper are as follows:

1. We propose a novel scheme to calculate the rebroadcast delay. The rebroadcast delay is to determine the forwarding order. The node which has more common neighbours with the previous node has the lower delay. If this node rebroadcasts a packet, then more common neighbours will know this fact. Therefore, this rebroadcast delay enables the information that the nodes have transmitted the packet spread to more neighbours, which is the key to success for the proposed scheme.

2. We also propose a novel scheme to calculate the rebroadcast probability. The scheme considers the information about the uncovered neighbours (UCN), connectivity metric and local node density to calculate the rebroadcast probability. The rebroadcast probability is composed of two parts:

- additional coverage ratio, which is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbours; and
- connectivity factor, which reflects the relationship of network connectivity and the number of neighbours of a given node.

3. we calculate the rebroadcast delay and rebroadcast probability of the proposed protocol. We use the upstream coverage ratio of an RREQ packet received from the previous node to calculate the rebroadcast delay, and use the additional coverage ratio of the RREQ packet and the connectivity factor to calculate the rebroadcast probability in our protocol, which requires that each node needs its 1-hop neighbourhood information.

4. The average delay of successfully delivered CBR packets from source to destination node. It includes all possible delays from the CBR sources to destinations. We will calculate Given Time , Rebroadcast Delay, Replica Status , Data & time.

The rest of this paper is organized as follows: Section 2 introduces the related previous work. Section 3 proposes a Neighbour Coverage-based

Probabilistic Rebroadcast protocol for reducing routing overhead in route discovery. Section 4 presents simulation parameters and scenarios which are used to investigate the performance of the proposed protocol. Section 5 concludes this paper.

II. RELATED WORK

Broadcasting is an effective mechanism for route discovery, but the routing overhead associated with the broadcasting can be quite large, especially in high dynamic networks. We studied the broadcasting protocol analytically and experimentally, and showed that the rebroadcast is very costly and consumes too much network resource. The broadcasting incurs large routing overhead and causes many problems such as redundant retransmissions, contentions, and collisions . Thus, optimizing the broadcasting in route discovery is an effective solution to improve the routing performance. Here We proposed a gossip based approach, where each node forwards a packet with a probability. They showed that gossip-based approach can save up to 35 percent overhead compared to the flooding. However, when the network density is high or the traffic load is heavy, the improvement of the gossip-based approach is limited . Kim et al. proposed a probabilistic broadcasting scheme based on coverage area and neighbour confirmation. This scheme uses the coverage area to set the rebroadcast probability, and uses the neighbour confirmation to guarantee reach ability. We proposed a neighbour knowledge scheme named Scalable Broadcast Algorithm (SBA). This scheme determines the rebroadcast of a packet according to the fact whether this rebroadcast would reach additional nodes. We proposed a Dynamic Probabilistic Route Discovery (DPR) scheme based on neighbour coverage. In this approach, each node determines the forwarding probability according to the number of its neighbours and the set of neighbours which are covered by the previous broadcast. This scheme only considers the coverage ratio by the previous node, and it does not consider the neighbours receiving the duplicate RREQ packet. Thus, there is a room of further optimization and extension for the DPR protocol. Several robust protocols have been proposed in recent years besides the above optimization issues for broadcasting. we proposed an AODV protocol with Directional Forward Routing (AODV-DFR) which takes the directional forwarding used in geographic routing into AODV protocol. While a route breaks, this protocol can automatically find the next-hop node for packet forwarding. Keshavarz-Haddad et al. proposed two deterministic timer-based broadcast schemes: Dynamic Reflector Broadcast (DRB) and Dynamic Connector-Connector Broadcast (DCCB). They pointed out that their schemes can achieve full reach ability over an idealistic lossless MAC layer, and for the situation of node failure and mobility, their schemes are robustness. We proposed a Robust Broadcast Propagation (RBP) protocol to provide near-perfect reliability for flooding in wireless networks, and this protocol also has a good efficiency. They presented a new perspective for broadcasting: not to make a single broadcast more efficient but to make a single broadcast more reliable, which means by reducing the frequency of upper layer invoking flooding to improve the overall performance of flooding. In our protocol, we also set a deterministic rebroadcast delay, but the goal is to make the dissemination of neighbor knowledge much quicker.

The Internet MANET encapsulation protocol (IMEP) is a mechanism to aggregate and encapsulate control messages. Also, IMEP provides a generic multi-purpose layer containing various common functionalities for MANET routing protocols. However, in the IMEP speci_cation no consideration for signal strength was presented. It may be possible to use IMEP for _ltering neighbors based on link stability rather than just to list neighbors that are in range. Given the observations obtained from our experiments, one possible area of work is to extend upon IMEP's functionalities to incorporate mechanisms to shield wireless defects, and also o_er various routing metrics which could be used by routing protocols.

Probabilistic flooding scheme :-

The basic idea of probabilistic flooding schemes is that each node forwards a flooding message with probability P upon receiving it for the first time. Clearly, when P=1, this scheme is equivalent to pure flooding. The probabilistic schemes can be classified into four types: counter-based, distance-based, location-based and cluster-based. These schemes differ in how a node estimates redundancy and how it accumulates knowledge to assist its decision. Except the last scheme, which relies on some local connectivity information, all schemes operate in a fully distributed manner.

Counter based scheme:- when a node tries to rebroadcast a message, the rebroadcast message may be blocked by busy medium, back off procedure, or other queued messages. There is a chance for the node to hear the same message again and again from other rebroadcasting nodes before the node actually starts transmitting the message.

Distance-based scheme:- This scheme uses the relative distance between hosts to make the decision.

Location-based:- This scheme uses the location information of the broadcasting nodes to make the decision. The location information may be supported by positioning devices such as GPS (Global Positioning System) receivers, it is also used to facilitate route discovery in a MANET .

Cluster-based:- Further investigate the probabilistic scheme and show that the success rate curves for probabilistic flooding tend to become linear for the network with low average node degree, and resemble a bell curve for the network with high average node degree.

In these schemes, a non-redundant transmission might be dropped out, without being forwarded further. Therefore, it will make some nodes in the network fail to receive the flooding message(i.e., these nodes are not reached by the flooding). Besides this deliverability problem, another major concern of these techniques is the difficulty in setting the right threshold value in various network situations .

III. LOCATION -BASED PROBABILISTIC REBROADCAST PROTOCOL

In this section, we calculate the rebroadcast delay and rebroadcast probability of the proposed protocol. We use the upstream coverage ratio of an RREQ packet received from the previous node to calculate the rebroadcast delay, and use the additional coverage ratio of the RREQ packet and the connectivity factor to calculate the rebroadcast probability in our protocol, which requires that each node needs its 1-hop neighbourhood information.

1-Hop Neighbor Knowledge Methods :-

Schemes in this category assume that each node keeps the information of 1-hop neighbors. The 1-hop neighbor information can be obtained by exchanging the HELLO message in MAC layer protocols. A major issue in the schemes that use 1-hop or 2-hop (discussed in the next section) information is the selection of a subset of neighbors for forwarding the flooding message. There are two strategies for choosing forwarding nodes: sender-based, where each sender nominates a subset of its neighbors to be the next hop forwarding nodes, and receiver-based, where each receiver of a flooding message makes its own decision on whether it should forward the message or not.

3.1 Uncovered Neighbours Set and Rebroadcast Delay:

When node ni receives an RREQ packet from its previous node s, it can use the neighbour list in the RREQ packet to estimate how many its neighbours have not been covered by the RREQ packet from s. If node ni has more neighbours uncovered by the RREQ packet from s, which means that if node ni rebroadcasts the RREQ packet, the RREQ packet can reach more additional neighbour nodes. To quantify his, we define the Uncovered Neighbours set U(ni) of node ni as follows:

$$U(n_i) = N(n_i) - [N(n_i) \cap N(s)] - \{s\},$$

where $N(s)$ and $N(n_i)$ are the neighbours sets of node s and respectively. s is n_i. the node which sends an RREQ packet to node n_i.

we obtain the initial UCN set. Due to broadcast characteristics of an RREQ packet, node n_i. can receive the duplicate RREQ packets from its neighbours. Node n_i. could further adjust the $U(n_i)$ with the neighbour knowledge. In order to sufficiently exploit the neighbour knowledge and avoid channel collisions, each node should set a rebroadcast delay. The choice of a proper delay is the key to success for the proposed protocol because the scheme used to determine the delay time affects the dissemination of neighbour coverage knowledge. When a neighbour receives an RREQ packet, it could calculate the rebroadcast delay according to the neighbour list in the RREQ packet and its own neighbour list. The rebroadcast delay $T_d(n_i)$ of node ni is defined as follows:

$$T_p(n_i) = 1 - \frac{|N(s) \cap N(n_i)|}{|N(s)|}$$
$$T_d(n_i) = MaxDelay \times T_p(n_i),$$

where $T_p(n_i)$ is the delay ratio of node n_i., and MaxDelay is a small constant delay. $|\cdot|$ is the number of elements in a set.

The above rebroadcast delay is defined with the following reasons: First, the delay time is used to determine the node transmission order. To sufficiently exploit the neighbour coverage knowledge, it should be disseminated as quickly as possible. When node s sends an RREQ packet, all its neighbours $n_i, i = 1, 2, \ldots, |N(s)|$ receive and process the RREQ packet. We assume that node n_k has the largest number of common neighbours with node s, according to , node n_k has the lowest delay. Once node n_k rebroadcasts the RREQ packet, there are more nodes to receive it, because node n_k has the largest number of common neighbours. Then, there are more nodes which can exploit the neighbour knowledge to adjust their UCN sets. Of course, whether node n_k rebroadcasts the RREQ packet depends on its rebroadcast probability calculated in the next section. The objective of this rebroadcast delay is not to rebroadcast the RREQ packet to more nodes, but to disseminate the neighbour coverage knowledge more quickly. After determining the rebroadcast delay, the node can set its own timer.

3.2 Neighbours Knowledge and Rebroadcast Probability

The node which has a larger rebroadcast delay may listen to RREQ packets from the nodes which have lower one. For example, if node n_i receives a duplicate RREQ packet from its neighbour n_j, it knows that how many its neighbours have been covered by the RREQ packet from n_j. Thus, node ni could further adjust its UCN set according to the neighbour list in the RREQ packet from n_j. Then, the $U(n_i)$ can be adjusted as follows:

$$U(n_i) = U(n_i) - [U(n_i) \cap N(n_j)].$$

After adjusting the $U(n_i)$, the RREQ packet received from nj is discarded.

We do not need to adjust the rebroadcast delay because the rebroadcast delay is used to determine the order of disseminating neighbour coverage knowledge to the nodes which receive the same RREQ packet from the upstream node. Thus, it is determined by the neighbours of upstream nodes and its own.

When the timer of the rebroadcast delay of node ni expires, the node obtains the final UCN set. The nodes belonging to the final UCN set are the nodes that need to receive and process the RREQ packet. Note that, if a node does not sense any duplicate RREQ packets from its neighbourhood, its UCN set is not changed, which is the initial UCN set. Now, we study how to use the final UCN set to set the rebroadcast probability.

We define the additional coverage ratio $(R_a(n_i))$ of node n_i as $R_a(n_i) = \frac{|U(n_i)|}{|N(n_i)|}$.

This metric indicates the ratio of the number of nodes that are additionally covered by this rebroadcast to the total number of neighbours of node ni. The nodes that are additionally covered need to receive and process the RREQ packet. As Ra becomes bigger, more nodes will be covered by this rebroadcast, and more nodes need to receive and process the RREQ packet, and, thus, the rebroadcast probability should be set to be higher.

we derived that if each node connects to more than 5:1774 log n of its nearest neighbours, then the probability of the network being connected is approaching 1 as n increases, where n is the number of nodes in the network. Then, we can use 5:1774 log n as the connectivity metric of the network. We assume the ratio of the number of nodes that need to receive the RREQ packet to the total number of neighbours of node n_i is $(R_a(n_i))$. In order to keep the probability of network connectivity approaching 1, we have a heuristic formula: $|N(n_i)| \cdot F_c(n_i) \geq 5.1774 \log n$. Then, we define the minimum $F_c(n_i)$ as a connectivity factor, which is

$$F_c(n_i) = \frac{N_c}{|N(n_i)|},$$

where $N_c = 5.1774 \log n$, and n is the number of nodes in the network.

From (5), we can observe that when $|N(n_i)|$ is greater than N_c, $F_c(n_i)$ is less than 1. That means node ni is in the dense area of the network, then only part of neighbours of node ni forwarded the RREQ packet could keep the network connectivity. And when $|N(n_i)|$ is less than N_c, $F_c(n_i)$ is greater than 1. That means node ni is in the sparse area of the network, then node ni should forward the RREQ packet in order to approach network connectivity.

Combining the additional coverage ratio and connectivity factor, we obtain the rebroadcast probability $P_{re}(n_i)$ of node n_i :-

$$P_{re}(n_i) = F_c(n_i) \cdot R_a(n_i),$$

where, if the $P_{re}(n_i)$ is greater than 1, we set $P_{re}(n_i)$ the to 1.

The above rebroadcast probability is defined with the following reason. Although the parameter R_a reflects how many next-hop nodes should receive and process the RREQ packet, it does not consider the relationship of the local node density and the overall network connectivity. The parameter F_c is inversely proportional to the local node density. That means if the local node density is low, the parameter F_c increases the rebroadcast probability, and then increases the reliability of the LBPR in the sparse area. Note that the calculated rebroadcast probability $P_{re}(n_i)$ may be greater than 1, but it does not impact the behaviour of the protocol. It just shows that the local density of the node is so low that the node must forward the RREQ packet. Then, node ni need to rebroadcast the RREQ packet received from s with probability $P_{re}(n_i)$.

3.3 Algorithm Description

The formal description of the Location -based Probabilistic Rebroadcast for reducing routing overhead in route discovery is shown in Algorithm 1.

Algorithm 1:- LBPR

Definitions:
$RREQ_v$: RREQ packet received from node v.
$R_v.id$: the unique identifier (id) of $RREQ_v$.
$N(u)$: Neighbor set of node u.
$U(u, x)$: Uncovered neighbors set of node u for RREQ whose id is x.
$Timer(u, x)$: Timer of node u for RREQ packet whose id is x.
{Note that, in the actual implementation of LBPR protocol, every different RREQ needs a UCN set and a Timer.}

if n_i receives a new $RREQ_s$ from s **then**
  {Compute initial uncovered neighbors set $U(n_i, R_s.id)$ for $RREQ_s$:}
  $U(n_i, R_s.id) = N(n_i) - [N(n_i) \cap N(s)] - \{s\}$
  {Compute the *rebroadcast delay* $T_d(n_i)$:}
  $T_p(n_i) = 1 - \frac{|N(s) \cap N(n_i)|}{|N(s)|}$
  $T_d(n_i) = MaxDelay \times T_p(n_i)$
  Set a Timer(n_i, $R_s.id$) according to $T_d(n_i)$
end if

while n_i receives a duplicate $RREQ_j$ from n_j before Timer(n_i, $R_s.id$) expires **do**
  {Adjust $U(n_i, R_s.id)$:}
  $U(n_i, R_s.id) = U(n_i, R_s.id) - [U(n_i, R_s.id) \cap N(n_j)]$
  discard($RREQ_j$)
end while

if Timer(n_i, $R_s.id$) expires **then**
  {Compute the *rebroadcast probability* $P_{re}(n_i)$:}
  $R_a(n_i) = \frac{|U(n_i, R_s.id)|}{|N(n_i)|}$
  $F_c(n_i) = \frac{N_c}{|N(n_i)|}$
  $P_{re}(n_i) = F_c(n_i) \cdot R_a(n_i)$
  if Random(0,1) $\leq P_{re}(n_i)$ **then**
    broadcast($RREQ_s$)
  else
    discard($RREQ_s$)
  end if
end if

IV. PROTOCOL IMPLEMENTATION AND PERFORMANCE EVALUATION

4.1 Protocol Implementation :

We modify the source code of AODV in NS-2 (v2.30) to implement our proposed protocol. Note that the proposed LBPR protocol needs Hello packets to obtain the neighbour information, and also needs to carry the neighbour list in the RREQ packet. Therefore, in our implementation, some techniques are used to reduce the overhead of Hello packets and neighbour list in the RREQ packet, which are described as follows:

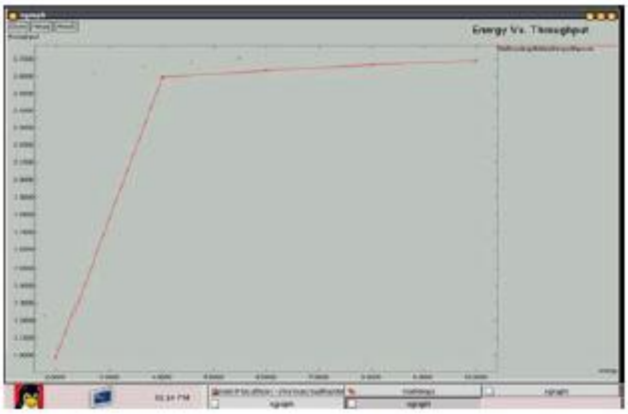
In order to reduce the overhead of Hello packets, we do not use periodical Hello mechanism. Since a node sending any broadcasting packets can inform its neighbours of its existence, the broadcasting packets such as RREQ and route error (RERR) can play a role of Hello packets. We use the following mechanism to reduce the overhead of Hello packets: Only when the time elapsed from the last broadcasting packet (RREQ, RERR, or some other broadcasting packets) is greater than the value of Hello Interval, the node needs to send a Hello packet. The value of Hello Interval is equal to that of the original AODV. In order to reduce the overhead of neighbour list in the RREQ packet, each node needs to monitor the variation of its neighbour table and maintain a cache of the neighbour list in the received RREQ packet. We modify the RREQ header of AODV, and add a fixed field num_ neighbours which represents the size of neighbour list in the RREQ packet and following the num_ neighbours is the dynamic neighbour list. In the interval of two close followed sending or forwarding of RREQ packets, the neighbour table of any node ni has the following three cases:if the neighbour table of node ni adds at least one new neighbour nj, then node ni sets the num_- neighbours to a positive integer, which is the number of listed neighbours, and then fills its complete neighbour list after the num_ neighbours field in the RREQ packet. It is because that node nj may not have cached the neighbour information of node ni, and, thus, node nj needs the complete neighbour list of node ni; if the neighbour table of node ni deletes some neighbours, then node ni sets the num_ neighbours to a negative integer, which is the opposite number of the number of deleted neighbours, and then only needs to fill the deleted neighbours after the num_ neighbours field in the RREQ packet;

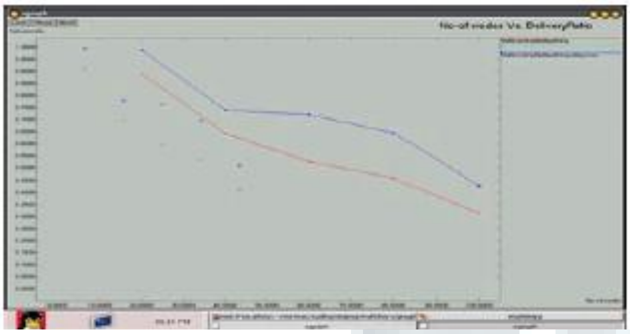
The nodes which receive the RREQ packet from node ni can take their actions according to the value of num_ neighbours in the received RREQ packet:

- if the num_ neighbours is a positive integer, the node substitutes its neighbour cache of node ni according to the neighbour list in the received RREQ packet;

ISSN Online: 2319 – 9253
Print: 2319 – 9245

- if the num_ neighbours is a negative integer, the node updates its neighbour cache of node ni and deletes the deleted neighbours in the received RREQ packet;
- if the num_ neighbours is 0, the node does nothing. Because of the two cases 2 and 3, this technique can reduce the overhead of neighbour list listed in the RREQ packet.





Pause-time is the time for which a packet stops in when it reached a destination after a travel from the place of origination. The unit of pause-time is seconds. Mobility is the velocity with which a node moves from the source to destination. Dropped packets are number of packets dropped due to the effect of link breaks. The dropped packets may be a control packets or data packets.

Normalized routing overhead: the ratio of the total packet size of control packets (include RREQ, RREP, RERR, and Hello) to the total packet size of data packets delivered to the destinations. For the control packets sent over multiple hops, each single hop is counted as one transmission. To preserve fairness, we use the size of RREQ packets instead of the number of RREQ packets, because the DPR and NCPR protocols include a neighbour list in the RREQ packet and its size is bigger than that of the original AODV.

Packet delivery ratio: the ratio of the number of data packets successfully received by the CBR destinations to the number of data packets generated by the CBR sources.

.*Average end-to-end delay:* the average delay of successfully delivered CBR packets from source to destination node. It includes all possible delays from the CBR sources to destinations.

The experiments are divided to three parts, and in each part we evaluate the impact of one of the following parameters on the performance of routing protocols: Number of nodes. We vary the number of nodes from 50 to 300 in a fixed field to evaluate the impact of different network density. In this part, we set the number of CBR connections to 15, and do not introduce extra packet loss. Number of CBR connections. We vary the number of randomly chosen CBR connections from 10 to 20 with a fixed packet rate to evaluate the impact of different traffic load. In this part, we set the number of nodes to 150, and also do not introduce extra packet loss. Random packet loss rate. We use the Error Model provided in the NS-2 simulator to introduce packet loss to evaluate the impact of random packet loss. The packet loss rate is uniformly distributed, whose range is from 0 to 0.1. In this part, we set the number of nodes to 150 and set the number of connections to 15.

V. CONCLUSIONS

Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. In this paper, we propose a neighbor coverage-based probabilistic rebroadcast protocol for reducing routing overhead in

MANETs. In order to effectively exploit the neighbor coverage knowledge, we propose a novel rebroadcast delay to determine the rebroadcast order, and then we can obtain the more accurate additional coverage ratio by sensing neighbor coverage knowledge. We also define a connectivity factor to provide the node density adaptation. By combining the additional coverage ratio and connectivity factor, we set a reasonable rebroadcast probability. We propose Establishing a trust hierarchy path MUST be performed to verify authenticity and usability of certificates within IMEP(Internet MANET Encapsulation Protocol). The meaning of the concepts is also taken into consideration, , by applying any linguistic analysis.. The main advantages of the proposed framework can be summarized in terms of extensibility and flexibility.Furthermore we could improve the system by integrating the constraints evaluation directly in the algorithm.

VI. REFERENCES

[1] Y. Sebastian, H. H. Then Patrick, "Domain-driven KDD for mining functionally novel rules and linking disjoint medical hypotheses", Knowledge-Based Systems, Vol. 24, No. 5, 2011, pp. 609-620.

[2] J. H. Feng, G. L. Li, "Efficient fuzzy type-ahead search in XML data", IEEE Transactions on Knowledge and Data Engineering, Vol. 24, No. 5, 2012, pp. 882-895.

[3] Y. Lou, Z. H. Li, Q. Chen, "Semantic relevance ranking for XML keyword search", Information Science, Vol. 190, 2012, pp. 127-143.

[4] Y. H. Chang, C. Y. Wu, C. C. Lo, "Processing XML queries with structural and full-text constraints", Journal of Information Science and Engineering, Vol. 28, No. 2, 2012, pp. 221-242.

.[5] Broekstra, J., Kampman, A., van Harmelen, F.: Sesame: A Generic Architecture for Storing and Querying RDF and RDF Schema. In Ian Horrocks and James Hendler, editors, *Proceedings of the first International Semantic Web Conference (ISWC 2002), number 2342 in Lecture Notes in Computer* Science, pages 5468, Sardinia, Italy, June 9 12, 2002. Springer Verlag, Heidelberg Germany.

[6] Chen, X., Zhou, X., Scher, R., and Geller, J.: Using an interest Ontology for Improved Support in Rule Mining. In Proceedings of the 5th International Conference of Data Warehousing and Knowledge Discovery (DaWaK 2003), Prague, Czech Republic, pp. 320–329

[7] Han, J., and Fu, Y.: Discovery of multiple-level association rules from large databases. In Proceedings of the 21st International Conference on Very Large Data Bases (VLDB '95) San Francisco, CA, pp. 420–431

[8] Hou, X., Gu, J., Shen, X., and Yan, W.: Application of Data Mining in Fault Diagnosis Based on Ontology. In Proceedings of the 3rd Conference on Information Technology and Applications (ICITA '05), Sydney, Australia, pp. 260–263.

[9] Ng, R., T., Lakshmanan, L., V., S., Han, J., and Pang A.: Exploratory mining and pruning optimizations of constrained associations rules. In Proceedings of the 1998 ACM SIGMOD international conference on Management of data (SIGMOD Seattle, WA, pp. 13–24.

AUTHOR'S PROFILE:

1. Ms.Madhimitha Reddy student in GITAM University, Hyderabad pursuing her M-Tech in dept of CST, and research area in the field of Networking.

2.Vallala Sowmya Devi, B.Tech.,M.Tech, (Ph.D.), MIEEE, MISTE, MIETE. Currently, she is a Assistant professor in CSE department in GITAM University, Hyderabad. Her specializations include networking, MANET, Network Security. Her current research interests are wireless communications and networking, MANET, Network Security.