A Selfishness Aware Neighbor Coverage Based Probabilistic Rebroadcast Protocol For Manets

Deepthi Sivaraj

University of Calicut India

***Abstract*— Broadcasting is a fundamental and effective data dissemination mechanism for route discovery, address resolution and many other network services in ad hoc networks. While data broadcasting has many advantages, it also causes some problems such as the broadcast storm problem, which is characterized by redundant retransmission, collision, and contention. To discover the route better than broadcasting methodology, rebroadcast can be done with the help of neighbor knowledge methods. In order to effectively exploit the neighbor coverage knowledge, we propose a novel rebroadcast delay and a connectivity factor to provide the node density adaptation. This paper proposes new reputation based neighbor coverage based probabilistic rebroadcast protocol based on AODV (Ah hoc On demand Distance Vector). This approach can significantly decrease the number of retransmissions so as to reduce the routing overhead and also improve the routing performance.**

***Keywords*— Mobile ad hoc networks, neighbor coverage, network connectivity, probabilistic rebroadcast, routing overhead, reputation.**

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a multi-hop wireless network formed by a group of mobile nodes that have wireless capabilities and are in proximity of each other. It is usually referred to a decentralized autonomous system. Ad-hoc wireless networks are self-creating, self-organizing, and self-administering by communicating among their component mobile nodes they inherit from being exclusive. Therefore, in order to provide the necessary control and administration function, such communications are used for supporting such networks. Most MANETs are based on IEEE 802.11 or WiFi medium access control (MAC) standard. Self configurability and easy deployment feature of MANET resulted in numerous applications in this modern era. Because of the distributed nature of these networks, ensuring security in such networks is a big challenge.

Due to considerations such as radio power limitation, channel utilization etc; a multi hop scenario occurs where the packets sent by the source host are relayed by several intermediate hosts before reaching the destination host. Many routing protocols, such as Ad hoc On-demand Distance Vector Routing (AODV) [1] and Dynamic Source Routing (DSR) [2], have been proposed for MANETs. These two protocols are on demand routing protocols, and they could improve the scalability of MANETs

II. RELATED WORKS

One of the earliest broadcast mechanisms is flooding, where every node in the network retransmits a message to its neighbours upon receiving it for the first time. Although flooding is extremely simple and easy to implement, it can be very costly and can lead to serious problem, named as broadcast storm problem, which is characterized by redundant packet retransmissions, network bandwidth contention and collision.

Ni et al. [3] 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 [3]. Thus, optimizing the broadcasting in route discovery is an effective solution to improve the routing performance.

Haas et al. [6] 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% 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 [5].

Kim et al. [4] 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 reachability.

M. Tamer Refaei et al [7] proposed reputation-based mechanism as a means of building trust among nodes. Here a node autonomously evaluates its neighbouring nodes based on completion of the requested service(s). This approach provides a distributed reputation evaluation scheme implemented autonomously at every node in an ad hoc network with the objective of identifying and isolating selfish neighbours. A reputation table is maintained by each node, where a reputation index is stored for each of the node's immediate neighbours. A node calculates reputation index of its neighbour based on successful delivery of packets forwarded through that neighbour. For each successfully delivered packet, each node along the route increases the reputation index of its next-hop neighbour that forwarded the packet and packet delivery failures result in a penalty applied to such neighbours by decreasing their reputation index.

III. NEIGHBOUR COVERAGE BASED PROBABILISTIC REBROADCAST BASED ON REPUTATION

A. On demand Route Discovery

On-demand routing protocols [1-2] construct a path to a given destination only when it is required. They do not maintain topological information about the whole network, and thus there is no periodic exchange of routing information. The focus of our study is on the route discovery part of the protocol. So we present a brief overview of the route discovery process in AODV in the remainder of this section.

When a source node **S** needs a route to some destination **D**, it broadcasts a RREQ packet to its immediate neighbours. Each neighbouring node rebroadcasts the received RREQ packet only once if it has no valid route to the destination. Each intermediate node that forwards the RREQ packet creates a reverse route pointing towards the source node **S**.

When the intended destination node **D** or an intermediate node with a valid route to the destination receives the RREQ packet, it replies by sending a route reply (RREP) packet. The RREP packet is unicast towards the source node **S** along the reverse path set-up by the forwarded RREQ packet. Each intermediate node that participates in forwarding the RREP packet creates a forward route pointing towards the destination **D**. The state created in each intermediate node along the path from **S** to **D** is a hop-by-hop state in which each node remembers only the next hop to destination nodes and not the entire route, as in DSR [2].
The routing overhead associated with the dissemination of routing control packets such as RREQ packets can be quite huge, especially when the network density is high and the network topology frequently changes. Traditional on-demand routing protocols [1-2] produce a large amount of routing control traffic by blindly flooding the entire network with RREQ packets during route discovery. Recently, the issue of reducing the routing overhead associated with the route discovery and maintenance processes in on-demand routing protocols has attracted increasing attention.

The neighbour coverage based probabilistic rebroadcast protocol combines both neighbour coverage and probabilistic methods. Neighbour knowledge based methods perform better than the area-based ones and the probability-based ones. We need a rebroadcast delay to determine the rebroadcast order to effectively exploit the neighbour coverage knowledge and then we can obtain a more accurate additional coverage ratio. In order to keep the network connectivity and to reduce the redundant retransmissions, we need a metric named connectivity factor to determine how many neighbours 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.

B. Reputation based Approach

Reputation is one node's opinion about another node. This reputation system can be used to make decisions about which nodes to include and which nodes to exclude from the network. The proposed approach is implemented over the existing on demand routing protocol Ad hoc On-demand Distance Vector Routing (AODV) [1]. Reputation value of node is used to classify a node as well behaving or misbehaving. Each node uses a monitoring mechanism like "watchdog" to monitor their neighbors. Monitoring the neighbors helps each node to calculate the reputation value of each of its neighbor. Reputation value is calculated using equation (3.1).Suppose there are 'N' nodes in the mobile ad-hoc network. Each node 'n_i' calculates the reputation $(R_{i,j})_t$ for each of its neighbor 'j' at time t.

For each node,

$$R_{(i,j)t} = \frac{\sum_{pkts=0}^{\infty} F_{pkts}}{\sum_{pkts=0}^{\infty} S_{pkts}}$$

Where $R_{(i,j)t}$ is the reputation value calculated by monitoring the neighbour 'j' directly at time 't' and $F_{pkts}$is the number of packets forwarded by node 'j' and S_{pkts} is the number of packets sent by node 'j'. This formula is used to calculate the reputation value of a node by directly monitoring the neighbouring node's past behaviour for some amount of time.

IV PROPOSED SYSTEM

The initial motivation of the protocol is neighbor coverage based probabilistic rebroadcast. 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, a proposal for a reputation based neighbour coverage-based probabilistic rebroadcast (NCPR) protocol is made. Combining the additional coverage ratio and the connectivity factor, we introduce a rebroadcast probability. A decision is made whether to rebroadcast the RREQ packet or not based on the reputation value, which is calculated as the ratio of the number of packets forwarded to the number of packets sent by each node. By using the reputation based approach, we can reduce the number of rebroadcasts of the RREQ packets to improve the routing performance.

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 and in order to keep the network connectivity and reduce the redundant retransmissions, we need a metric named connectivity factor to determine how many neighbours 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 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. The rebroadcast probability 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:
a. 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
b. connectivity factor, which reflects the relationship of network connectivity and the number of neighbours of a given node.

A. *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 about the nodes which have transmitted the packet to more neighbours, which is the key success for the proposed scheme. When a node ni receives an RREQ packet from its previous node s, node s can use the neighbour list in the RREQ packet to estimate how many its neighbours have not been covered by the RREQ packet . 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 exploit the neighbour coverage knowledge, it should be disseminated as quickly as possible. When node s sends an RREQ packet, all its neighbours ni, i = 1, 2... receive and process the RREQ packet.

Assume that node nk has the largest number of common neighbours with node s, node nk has the lowest delay. Once node nk rebroadcasts the RREQ packet, there are more nodes to receive the RREQ, because node nk has the largest number of common neighbours. Node nk rebroadcasts the RREQ packet depends on its rebroadcast probability. 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.

Algorithm describes the rebroadcast delay for the node ni

1. If a node receives RREQ from a previous node, use neighbour list table to see its uncovered neighbours.
2. If RREQ comes for the first time then find neighbour node knowledge
3. Else discard RREQ message
4. For every RREQ send by a node to its neighbor,
5. Rebroadcast RREQ based on Rebroadcast Probability which is find from the Algorithm for Rebroadcast probability.

B. *Rebroadcast Probability*

The scheme to calculate rebroadcast probability considers the information about the uncovered neighbours, connectivity metric and local node density to calculate the rebroadcast probability. The rebroadcast probability is composed of two parts:
a) 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
b) connectivity factor, which reflects the relationship of network connectivity and the number of neighbours of a given node.

The node which has a larger rebroadcast delay may listen to RREQ packets from the nodes which have lowered one. We do not need to adjust the rebroadcast delay because the rebroadcast delay is used to determine the order of disseminating neighbour coverage knowledge. When the timer of the rebroadcast delay of node ni expires, the node obtains the final uncovered neighbour set. The nodes belonging to the final uncovered neighbour 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 uncovered neighbour set is not changed, which is the initial uncovered neighbour set.
The final uncovered neighbour set is used to set the rebroadcast probability. The metric Ra 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.

Xue [7] 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 ni is Fc(ni).If the local node density is low, the parameter Fc increases the rebroadcast probability, and then increases the reliability of the NCPR in the sparse area. If the local node density is high, the parameter Fc could further decrease the rebroadcast probability, and then further increases the efficiency of NCPR in the dense area. Thus, the parameter Fc adds density adaptation to the rebroadcast probability.

The algorithm describes to set the Rebroadcast Probability

1. If a node receive duplicate RREQ from its neighbour node,
2. Node knows how many neighbours have been covered by previous RREQ.
3. Node adjusts its uncovered neighbour set according to neighbour list and set a reschedule timer for that node.
4. If timer expires, node obtains final uncovered neighbour set
5. For each uncovered neighbour set, calculate Number of nodes that are additional covered by rebroadcast(Fc (ni)) and Total number of neighbours of node (Node density).
6. If Fc (ni) is low, set Rebroadcast Probability as high else set Rebroadcast Probability as low.

C. Algorithm

1. If (ni receives a new RREQs from previous node) then
2. Calculate the uncovered neighbour set
3. Compute the rebroadcast delay
4. Set a Timer according to delay
5. end if
6. While ni receives a duplicate RREQj from nj before timer expires
7. do adjust the neighbour list and discard (RREQj)
8. end while
9. If timer expires, then
10. compute the rebroadcast probability
11. Generate a random number Rnd over the range [0,1]
12. If Rnd(0,1) < Pre(ni) then
13. calculate the reputation value.
14. if(reputation > 0.5) then
15. Broadcast the RREQ packet
16. else Drop RREQ

V. CONCLUSIONS

MOBILE ad hoc networks (MANETs) consist of a collection of mobile nodes that can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. Broadcasting is a fundamental and effective data dissemination mechanism in route discovery. But it causes the broadcast storm problem. To reduce the deleterious impact of flooding RREQ packets, a number of route discovery algorithms have been suggested over the past few years. One of the fundamental challenges of MANETs is the design of dynamic routing protocols with good performance and less overhead.

This paper proposed a reputation based probabilistic rebroadcast protocol based on neighbor coverage to reduce the routing overhead in MANETs.A new scheme to dynamically calculate the rebroadcast delay, which is used to determine the forwarding order and more effectively exploit the neighbor coverage knowledge is introduced. Reputation based approach was introduced to identify and to isolate the selfish nodes in the network and is based on AODV. Simulation results show that the proposed protocol generates less rebroadcast traffic than the flooding and some other optimized scheme in literatures. Because of less redundant rebroadcast, the proposed protocol mitigates the network collision and contention, so as to increase the packet delivery ratio and decrease the average end-to-end delay. The simulation results also show that the proposed protocol has good performance when the network is in high density or the traffic is in heavy load.

.

REFERENCES

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," *RFC 3561*, 2003.

[2] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR) for IPv4," *RFC 4728*, 2007.

[3] S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu. "The Broadcast Storm Problem in a Mobile Ad hoc Network," *Proc. of ACM/IEEE MobiCom'99, pp. 151-162*, 1999.

[4] J. Kim, Q, Zhang, and D. P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad hoc Networks," *Proc. of IEEE GLOBECOM'04*, 2004.

[5] J. D. Abdulai, M. Ould-Khaoua, and L. M. Mackenzie, "Improving Probabilistic Route Discovery in Mobile Ad Hoc Networks," *Proc. Of IEEE Conference on Local Computer Networks, pp. 739-746*, 2007.

[6] Z. Haas, J. Y. Halpern, and L. Li, "Gossip-based Ad hoc Routing," *Proc. IEEE INFOCOM'02, vol. 21, pp. 1707-1716*, 2002.

[7] M. Tamer Refaei, VivekSrivastava, LuizDaSilva, Mohamed Eltoweissy, " A Reputation-based Mechanism for Isolating Selfish Nodes in AdHoc Networks", Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05) , 2005

[8] Animesh Kr Trivedi1, Rishi Kapoor1, Rajan Arora1, Sudip Sanyal1 and SugataSanyal , " RISM – Reputation Based Intrusion Detection System for Mobile Adhoc Networks" Available from link profile.iiita.ac.in/aktrivedi_b03/rism.pdf.

[9]F. Xue and P.R. Kumar, “The Number of Neighbors Needed for Connectivity of Wireless Networks,” Wireless Networks, vol. 10, no. 2, pp. 169-181, 2004.

[10]. Ns-2. http:// www.isi.edu/nsnam /ns.