Performance Analysis of Acknowledgement based Vector Routing and Epidemic Techniques in infrastructure less Opportunistic Networks

Mrs. Dipti P Sonawane
Assistant Professor
Department of Computer Science
Engineering
GHRIEM, Jalgaon

Abstract—Opportunistic networks are one of the most increasing evolutions of MANETs. In opportunistic networks the existence of a simultaneous path is not assumed to transmit a message between a source and a destination. In opportunistic networks, path connecting to the mobile nodes never exits, mobile nodes transmit messages with each other when they get opportunity to transmit. Furthermore, nodes are not supposed to possess or acquire any information about the network topology. Routes are built dynamically, while messages are route between the source and the destination, and anyone node can be selected as opportunistic network and node which pass message to neighbor node, only if it is likely to bring the message nearer to the final destination. These features make opportunistic networks a challenging and promising field of research. In this paper we describe approach for routing in opportunistic networks, rendering old traditional routing protocols unable to deliver messages between hosts. Thus, there is a need for a new technique to route through such networks. We propose composite approach which combines concepts of Epidemic Routing and Probabilistic routing techniques together with acknowledgement approach for better delivery. Our results show that composite routing protocol is able to provide better message delivery probability and less message delay.

Index Terms—Epidemic Routing, Routing, Opportunistic networks, Probabilistic Routing.

I. INTRODUCTION

Wireless network infrastructures have been exploring and expanding at a rapid pace throughout the globe. However, wireless networks may still be unavailable in many areas such as poor regions, sensors in underwater or military operations. In order to provide networking support for situations where there are no directly connectivity paths, opportunistic network can be applied. Using an adhoc like fashion network is interconnected to each other is an opportunistic network which is one type of delay tolerant (MANET) is opportunistic network. Wireless networks’

Properties, such as having no connection of nodes, partitions of networks, user’s mobility and path between that users” instability, these properties are considered to be as exceptions in traditional network. This makes the design of MANET significantly more complex and difficult [1]. When a source node or other node wants to deliver data to destination node or another node but if there does not having a direct communication between them between them, packets can be transferred or given to most appropriate intermediate node or participating nodes which will result in finally delivering the packet from one position to another or from the source to the destination. Opportunistic networks [2] results to be a mobile devices carried by people, without any dependence on any already existing network topology. Opportunistic networks consideration of no connections, mobility, partitions, etc. as rules of opportunistic networks instead of the exceptions can be possible due to opportunistic network. In opportunistic network mobility is used as a kind of technique to provide interconnection between the no of nodes where there is no connection. Unlike a typical ad-hoc structure, however, opportunistic network assumes there is almost never a fully connected path between source to destination and the intermediate nodes may not encounter other nodes frequently or consistently[1],[7],[15]. In some cases, intermediate nodes may have to buffer the packets received for a long time. Due to the uncertainty of packet delivery success in opportunistic networks, numerous-routing protocols were proposed to maximize packet delivery rate. One of the most well known routing protocols for opportunistic networks is a protocol called PRoPHET [1], [3]. Since the chance of having a directly connected path from a source node to the destination node is rare or non-existent, identifying potential follow. Intermediate carriers for the packets to be transferred are essential. Forwarding data to intermediate carriers that rarely encounter the destination node will, in the worst case, fail to deliver the data. PRoPHET [1] uses a predictability value, which is calculated using the history of encounters between nodes to evaluate the packet forwarding preference. While PRoPHET has shown decent results [1], there is still room for improvements. Due to the FIFO queuing nature of PRoPHET [1], packets may be dropped consistently when packets are forwarded to a few concentrated nodes. Packets may also be lost due to node failures or incomplete transmissions [3], and another protocol is Epidemic routing [2], [4], [11] in which a node A “infects” every contact B with packets that it has that B doesn’t have. Missing packets are determined by exchanging summary vectors of nodes. Epidemic routing is unbeatable
from the point of view of successful delivery as long as the load does not stress the resources (bandwidth, storage).

The design of efficient routing protocols for opportunistic networks is generally a difficult task due to the absence of knowledge about the network topology. Routing performance depends on knowledge about the expected topology of the network. We present a novel composite approach for routing in opportunistic network. We propose the use of probabilistic routing approach [1], and Epidemic Routing approach [2] assuming non-random mobility of nodes to improve the delivery rate of messages while keeping usage of buffer and communication overhead to low level.

It represents the currently working environment and behavior of different users. It helps to identify best suitable forwarders based on context information stored in summary vector about the destination. We can classify the main routing approaches proposed in the literature based on the amount of context information of users stored in summary vector they exploit.

II. RELATED WORK

Vahdat and Becker present a routing protocol for intermittently connected networks named as Epidemic Routing [2]. This protocol relies on the theory of epidemic algorithms [4] by performing pair-wise information of messages between multiple nodes when they get in contact with each other to finally deliver messages to destination. Messages are buffered by Hosts even if currently there is no path to the destination available. An indexing of these messages known as summary vector is maintained by the nodes, and when two nodes meet they exchange their copy of summary vectors. After this exchange is one, each node can determine about other nodes that they have some message that was previously unseen to this node. In that case, the node sends request for messages to other node. This means unless buffer space is available, messages will sprayed like an epidemic of some disease within the network and nodes meet to “infect” each other. Each message contains a globally unique message ID to determine its previously seen status. Besides the standard and obvious fields of source and destination addresses, messages also contain a hop count fields. This field same as TTL field in IP packets and it determines the maximum number of hops to send a message, and can be used to limit the utilization of resource of the protocol. Messages having hop count as one will only be delivered to their final destination eventually.

The usage of resources of this scheme is managed by the hop count placed in the messages, and the buffer space available at the nodes. If these are sufficiently large enough, the message will finally be propagated throughout the entire network if the possibility exists. They however have shown that by selecting an appropriate maximum hop count, we can keep delivery rates high while the utilization of resource is lower in the scenarios used in their evaluation [2].

A communication model that is similar to Epidemic Routing is presented by Beaufour et al. [5], which focuses on data dissemination among sensor networks. The Pollen network proposed by Glance et al. [6] is also similar to Epidemic Routing.

Chen and Murphy proposed a protocol known as Disconnected Transitive Communication (DTC) [7]. It utilizes an application-tunable utility function for locating the current node in the cluster of currently connected nodes that it is best to forward the message to next node based on the needs of provided application. In each step, a node searches the cluster of currently connected nodes to find a node that is “closer” to the destination, where the closeness is generated by a utility function that can be optimized by the application to provide appropriate results.

Shen et al. proposed Interrogation-Based Relay Routing, a routing protocol for ad hoc space networks with Scientific Earth Observing (SEO) satellites [8], characterized with frequently changing topologies, and intermittent and sparse connectivity. The satellites interrogate with each other to learn more about current network topology and nodal capacity to generate intelligent routing decisions.

Work by Li and Rus [9] deal with a similar communication problem in disconnected networks. They proposed a solution in which nodes actively change their trajectories to create new connected paths to accommodate the data transmission. While this might work in military applications and in some of robotic sensor networks, in many scenarios it is not likely that nodes will move just to communicate with other nodes (if it is even possible to communicate the need for it).

Grossglauser and Tse looks at the utility to use the mobility of nodes to deliver messages to their destination with a slightly different point of view. One of major problem with ad hoc networks is that they scale badly due to interference of concurrent transmissions between nodes. Grossglauser and Tse show results by only doing local communications between neighbors and instead by relying on the movement of nodes to bring a message to its final destination, this problem can be mitigated [10].

III. PROBABILISTIC ROUTING

Though the random way-point mobility model can be used in evaluations of mobile ad hoc protocols, real users will not likely be moving around randomly, but rather moving in a predictable manner based on repeating their behavioral patterns such that if a node has visited a location several times before, means there is chance of that its visit to that location again. We would like to make use of these kind of observations and this information to improve our routing performance by doing enhanced probabilistic routing using History of Encounters and Transitivity [1].

To accomplish this, we establish a probabilistic metric called delivery predictability, \( P(b,a) \in [0,1] \), at every node \( b \) for every known destination \( a \). This indicates chances of this node delivering a message to destination. When two nodes meet each other, they exchange summary vectors which also contains the delivery predictability information stored at the each nodes. This information helps to update the internal delivery predictability vector as described below, and next the information in the summary vector helps to decide which messages should be requested from the other nodes based on the current forwarding strategy implemented.

A. Delivery predictability calculation [1]

The calculation of the delivery predictabilities divided in
three parts. The first one is to update the metric whenever a node is encountered in network, so that nodes that are often encountered will have high delivery predictability. For this calculation refer to “(1)”, where \( P_{\text{init}} \in [0, 1] \), is an initialization constant.

\[
P(a,b) = P(a,b)_{\text{old}} + (1 - P(a,b)_{\text{old}}) \times P_{\text{init}}.
\]

(1)

If a pair of nodes does not encounter each other in a while, they are considered less likely to be good forwarders of messages to each other, thus the delivery predictability values must age accordingly, after being reduced in the process which is calculated in following aging equation. Refer to “(2)”, where \( \gamma \in [0,1] \) is the considered as aging constant, and \( k \) is the number of time units that have elapsed since the last time the metric was aged. The time unit used can differ in some ways, and should be defined based on the current application and the expected delays in the targeted network.

\[
P(a,b) = P(a,b)_{\text{old}} \times \gamma k.
\]

(2)

The delivery predictability also contains transitive property, that is based on the some observations as if node B frequently encounters node A, and node C frequently encounters node B, then node C probably is a good node to forward messages destined for node A. Refer to “(3)”, it shows the result of transitivity affects the delivery predictability, where \( \beta \in [0, 1] \) is a scaling constant that decides how large impact the transitivity should be having on the delivery predictability.

\[
P(a,c) = P(a,c)_{\text{old}} + (1 - P(a,c)_{\text{old}}) \times \beta \times P(a,b) \times P(b,c).
\]

(3)

IV. EPIDEMIC ROUTING

Epidemic Routing [2], [4] provides final delivery of messages to destinations with minimum assumptions regarding the current topology and connectivity of the current working network. In fact, only periodic pair-wise connectivity would be required to ensure final message delivery to destination. Epidemic Routing provides the final message delivery to random destinations with minimum assumptions about the topology and approx. connectivity of the network. Final delivery of messages only depends on periodic pair-wise connectivity between all mobile devices. The Epidemic Routing approach is working on the theory of epidemic algorithms [6]. In this, each host maintains two buffers with itself, one for storing its originated messages and second for buffering of messages on behalf of other hosts. Each mobile device maintains summary vector that contains a very compact representation of currently stored messages in buffer.

The Epidemic Routing protocol works as follows. Epidemic protocol relies majorly upon the transitive distribution of all messages through ad hoc networks, with messages finally reaching their desired destination. Each host manages a buffer consisting of all messages that it has originated and the messages that it is buffering on behalf of other hosts. For better efficiency, a hash table is used to index this list of messages; it is keyed by a unique identifier associated with each message. Each host stores a bit vector known as the summary vector which indicates about the status of the entries in their local hash tables.

When two hosts come within communication range of one another, the host having smaller identifier initiates session with the host containing larger identifier. To avoid redundant connections in network, each host manages a cache of hosts. Anti-entropy is not re-initiated with other remote hosts that have already been contacted within a mentioned configurable time period. During anti-entropy, the two hosts does the exchanging of their summary vectors to identify which messages that are stored remotely have not been viewed by the local host. In return, each host then requests for copies of the messages that it has not yet viewed. In the design for the Epidemic Routing, it associates a unique a hop count, message identifier, and an optional ack request with each and every message. The message identifier is generated unique 32-bit number. This identifier is a combination of the locally-generated message ID and host’s ID (16 bits each). However, if some hosts in an ad hoc network are assigned the similar subnet mask, then the remaining bits of the IP address is used as the identifier. In this implementation, the hosts in the ad hoc network are assigned ID’s statically. In this the hop count field determines the maximum no. of epidemic exchanges subjected to a particular message. While the hop count is same as the TTL field in IP packets, messages with one hop count will only be delivered to their desired end destination. The larger values for hop count more quickly it will distribute a message through the network. This will eventually reduce average delivery time for message, but will also increase the total resource consumption during message delivery. Thus, high priority messages should be marked with a high hop count, and most messages can be marked with a close value to the expected number of hops for a provided network configuration to reduce consumption of resource [2], [4], [11], and [13].

V. PROPHET ROUTING

PROPHET [7], a Probabilistic Routing Protocol using History of Encounters and Transitivity makes use of current observations that real users mostly moving in a predictable fashion. If a user has visited a location several times before, then there is high probability of user to visit the same location again. PROPHET uses this information for improving performance of routing. To accomplish this in effective manner, PROPHET manages delivery predictability metric at each and every node. This metric represents message delivery probability of each host to the desired destination. PROPHET is similar to Epidemic Routing in some ways but it is enhanced with new concept of delivery predictability. Delivery predictably is the finding of most probable node to reach to the destination. When two nodes come near, they also exchange their delivery predictability information and summary vectors. This information is used by nodes to update the delivery predictability information of metric.

When a message is received at node, node verifies availability of destination. If destination is unavailable, node stores the message to itself and upon each encounters with another device or nodes, it takes decision to transfer a message or not. Message is transferred to the other node only if the other node
is considered with higher message delivery probability to the desired destination [7].

VI. VECTOR ROUTING APPROACH

Composite routing protocol is a novel approach for effective and efficient routing in opportunistic network. In this approach we try to combine both the Probabilistic Routing approach an Epidemic Routing. A node forwards the message to the any two neighbors having maximum delivery predictability.

Delivery predictability, \( P(a,b) \in [0,1] \), at every node a for each known destination b is ability of a node to deliver message to destination b node.

When two nodes encounter each other, they exchange their summary vectors which contains the delivery predictability information stored at each nodes. This information is used for updating the internal delivery predictability vector at nodes, and then the information in the summary vector is used to take decision about which messages to be requested from the other nodes as described below.

Each host manages a buffer consisting of messages that it has originated and all messages that it has buffered on behalf of other hosts. A hash table indexes this list of messages, it contains a key which is unique identifier associated with each message in table. Each host stores a bit vector called the summary vector which indicates the status of the entries store in their local hash tables. To avoid redundant connections among nodes, each host maintains a cache of previously encountered hosts. When two hosts meet by coming into communication range of one another, they exchange each other’s summary vectors to determine the messages that are stored remotely but have not been seen by the local host. In turn, each host will requests for copies of messages that it has not yet seen.

When message reaches to desired destination, acknowledgment is sent in the same manner to the sender node that sent the message.

For example, while transmitting the message the source node searches the nodes in its range, thereafter by exchanging delivery predictability information he finds MN1 and MN2 having higher delivery predictability than other nodes in range therefore source node forwards current message to nodes MN1 and MN2 as shown in fig. (a). The nodes who received the message from source node again follow the same process as source node executed but as shown in fig (b) MN2 is receiver of message from source as well as node MN1. MN1 and MN2 only exchanges their summary vectors. And by exchanging they know that they don’t have new messages to exchange so communication is stopped. In fig. (c) The node MN4 follows same procedure and message reaches to the desired destination.

A. Proposed System Algorithms

Step 1: Deploy ‘N’ number of nodes to generate wireless network
Step 2: Choose source node ‘S’ and destination node
Step 3: Create TCP/UDP connection among the nodes
Step 4: Declare default Energy value ‘E’ for All nodes in the network
Step 5: Declare trust value ‘T’ for All nodes present in the network
Step 6: Create Routing Table, one- hop neighbor for all Nodes deployed in current Wireless network
Step 7: Create Routing path

For Node (i=0, i<=n)

If { trust value = 0
assign the node to routing table Rt
energy value <1
assign the node to routing table Rt
}

Get Rt

Step 8: Start the packet delivery by using the router derived above
Step 9: Update the counter credit value for Nodes in Rt incrementing value by one
Step 10: Destination receives packet from source.

B. Performance Analysis

1. SIMULATION SETUP

We have performed simulations using the tool ns-2 to evaluate our proposed ideas. The simulation parameters that we have chosen are summarized in table I.
Table 1. Simulation Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>200ms</td>
</tr>
<tr>
<td>Monitoring Area</td>
<td>1500 X 500</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>30</td>
</tr>
<tr>
<td>Communication Range</td>
<td>30m</td>
</tr>
<tr>
<td>Length of Packets</td>
<td>100bytes</td>
</tr>
</tbody>
</table>

2. SIMULATION RESULTS

This part describes the Proposed systems Results and Graphs, The Result will be displayed on the with the help of Network Animator (NAM) in NS2-2.35, There are 15 wireless Movable node are available to simulates the proposed system. The Result Graph of proposed system is to be described with help of the NS2-2.35 graphs; The Graphs are nothing but the raw data or processed data which is to collected during the simulation of the Network Simulator.

VII. ADVANTAGES

- Increased message delivery rate than probabilistic or epidemic model.
- Considerable reduction in resource consumption than epidemic model.
- Black hole attack is almost removed since a message is sent to two different nodes having higher delivery predictability.

VIII. CONCLUSION

Thus the Proposed System Acknowledgement based Vector Routing based on Delivery Predictability and history of nodes for Infrastructure less Opportunistic Network. The technique
has been inspired from the geographical routing technique and uses history of movements to model the behavior of the nodes. Prediction is carried out to select the best next hop node. The Result shown in Proposed system are better than Existing system it means that it performs well in terms of the number of packets delivered up to the destination, less end to end delay and reduced in packet loss. Hence, the proposed system shows the improved result compared to the existing system.

IX. FUTURE WORK

In proposed work delivery predictability is calculated by using three metrics as- time span between their meetings, number of encounters between nodes and transitive property of delivery predictability.

It will be interesting to evaluate delivery predictability by using different metrics like detailed context information of nodes. In future, it is planned to introduce backup path in routing the packets from node to node and plan to send the encrypted data from source node to destination node.

REFERENCES


