ISSN No. 0976-5697

Volume 4, No. 9, July-August 2013

International Journal of Advanced Research in Computer Science

REVIEW ARICLE

Available Online at www.ijarcs.info

A Survey of Routing Protocols for Opportunistic Mobile Adhoc Networks

Er.Maggi Goyal*[1], Er.Manoj Chaudhary[2],Er.Abhishek Bharti[3]

[1]Student, [2]Assitant Professor, [3]Student, Computer Science, Yadavindra College,Talwandi Sabo,Punjab,India.

agg.maggi@gmail.com[1], ermanojchaudhary@gmail.com[2], abhiarch21.bharti@gmail.com[3]

Abstract- Opportunistic networks are the network in which the nodes are wirelessly connected and the nodes can be fixed or mobile. This network is usually based on asynchronous communication in which the packets are not delivered at the same rate. In Opportunistic Networks (OppNets), routing is one of the main challenges. This paper presents a survey of routing protocols for opportunistic mobile adhoc networks. The protocols can be AODV, Epidemic Routing, PROPHET, Spray and Wait. This paper gives the techniques for the routing of these algorithms with some problem solutions. The techniques are based upon different approaches like Dissemination-Based, Context-Based, Fixed Infrastructure and Mobile Infrastructure Based approaches. In this paper survey shows the comparative study of the algorithms and the techniques used for them.

Keywords: Opportunistic networks, AODV, Epidemic Routing, PROPHET, Spray and Wait.

I. INTRODUCTION

A. Opportunistic network:

An opportunistic network is a wirelessly connected node. Nodes may be either fixed or mobile. Communication range is not fixed. In which device make link to the user. Different nodes exchange data from source to destination [1].Opportunistic networks are usually asynchronous communications. No infrastructure is required. Nodes communicate directly with each other. They can be characterized by the following features:

(a). They are governed by operators through the provision of resources (e.g., spectrum available) and policies, as well as context/ profile information and knowledge, which is exploited for their creation/maintenance.

(b). They are extensions of the infrastructure that will include various devices and terminals potentially organized in an infrastructure-less mode, as well as elements of the infrastructure.

(c). They will exist temporarily, i.e. for the time frame necessary to support particular applications (requested in specific location and time). Applications can be related to the social networking and prosumer (derives from the combination of "producer" and "consumer") concepts as well as to the support of an enterprise (in a particular area and time interval) for developing and delivering products or digital services.

(d). At the lower layers, the operator designates the spectrum that will be used for the communication of the nodes of the opportunistic network (i.e. the spectrum derives through coordination with the infrastructure). In this respect, in principle, the bands will be licensed.

(e). The network layer capitalizes on context-, policy-, profile-, and knowledge-awareness to optimize routing and service/content delivery.

a. Find opportunity:

Network is able to find opportunity in direct communication range. A node needs to find neighbour node in its vicinity in order to start collaboration. Neighbour nodes act as spontaneous manner whenever they come in close.

b. Message exchange:

When two nodes successfully discovered each other both nodes share data in user awareness. A node can exchange data to its neighbour nodes within the direct range. Nodes pass data to its successfully discover neighbour nodes.

c. Information sprinkler:

An information sprinkler is a dedicated node which is not mobile. It is fixed in dedicated location in opportunistic network. One information sprinkler is connected to other information sprinkler through wired or wire fewer networks which have other nodes in its range.

d. Nodes:

Nodes are any network component which has the property of receiving and forwarding the message. Nodes may be mobile or fixed in dedicated location. Like a computer with blue tooth, a radar, a laptop, a wi –fi network, a mobile phone etc. when one source node have message and it want to sent to the particular destination node then source node find its all possible bound neighbor nodes and distribute the message that particular node that is closer to it with the destination node address. So hop node receiving the message and then repeat the above procedure until message not delivered to the correct location.

B. Routing Protocols:

The elimination of the need to build paths drastically simplifies the routing in opportunistic networks; however, challenges remain that are distinct from those of conventional network routing methods. A routing scheme in OppNets has to provide data with some reliability1 (ideally with full reliability) even when the network connectivity is intermittent or when an end-to-end path is temporally

nonexistent. The following are the different routing protocols in the opportunistic mobile adhoc networks .

a. ***AODV:*** AODV is Adhoc On Demand Distance Vector Routing. In Opportunistic Mobile adhoc network when that want to communicate with another node that is not in the range it finds the route thorough other nodes. As shown in fig 2 node 1 is not in the range with node 3 so it simply talks to node 3 through node 2.

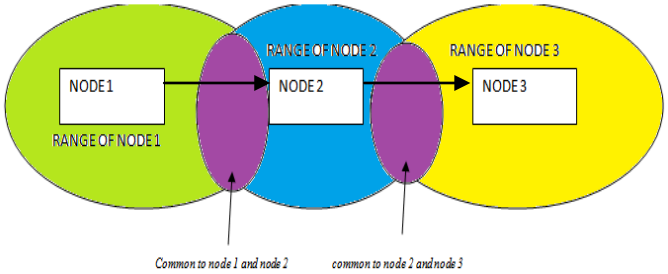

Figure 2 Forwarding of packet to node not in range

It works by using route request message and route reply messages if a node is not in range with the node that it want to talk to is send route request to its neighbours the route request contains source IP address and sequence no. , destination IP address and sequence number as well as life span of the route request (RREQ) if a neighbour of the source doesnot know a route to a destination it rebroadcast the route request . If a neighbour does knows a route to the destination it send route reply (RREP) back to the source[2].As shown in fig 3.

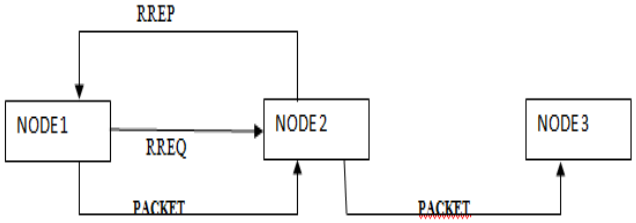

Figure 3 Architecture of AODV protocol

b. ***Epidemic Routing****:* Epidemic Routing for opportunistic networks is flooding-Based in nature in which every incoming packet is sent through every outgoing link. Epidemic Routing first proposed by Vahdat and Becker for forwarding data in an opportunistic network[5]. In Epidemic Routing, the nodes are continuously replicate and transmit messages to newly discovered contacts that do not already hold a copy of the message.

Each node receives a request packet and forwards the packet on its entire outgoing links except the one corresponding to the incoming link on which the packet arrives. Each request packet may reach the destination node along a different route at a different time [6]. The advantage of flooding-based routing is its simplicity in finding a route, in particular, a minimum delay ratio for a connection request because it doesn't require any global information about network topology, or any context information.

c. ***Prophet:*** PROPHET is a Probabilistic ROuting Protocol using History of Encounters and Transitivity. This protocol uses an algorithm that attempts to exploit the non-randomness of real-world encounters by maintaining a set of probabilities for successful delivery to known destinations in the DTN (delivery predictabilities) and replicating messages during opportunistic encounters only if the Mule that does not have the message appears to have a better chance of delivering it. The Probabilistic Routing scheme - PRoPHET calculates the delivery predictability from a node to a particular destination node based on the observed contact history, and forwards a message to its neighboring node if and only if that neighbor node has a higher delivery predictability value[3]. The context information used in PRoPHET is the frequency of meetings between nodes, as is also seen in the MV (Meeting and Visits) and MaxProp protocols[7]. A node uses MaxProp to schedule packet transmission to its peers and determines which packets should be deleted when buffer space is almost full. Packets are scheduled based on path likelihoods to peers according to historical data.

d. ***Spray And Wait Routing:*** Spray and Wait distributes only a small number of copies. Spray and Wait routing consists of the following two phases:

a) ***Spray Phase:*** for every message originating at a source node, L message copies are initially spread—forwarded by the source and possibly other nodes receiving a copy—to L distinct path.

b) ***wait phase:*** if the destination is not found in the spraying phase, each of the L nodes carrying a message copy performs"Direct Transmission"[4].

Spray and Wait have some advantages over flooding based routing protocols like under low load, Spray and Wait results in much fewer transmissions and comparable or smaller delays than flooding-based schemes And Under high load, it yields significantly better delays and fewer transmissions than flooding-based schemes It can be easily tuned on line to achieve given QoS requirements, even in unknown networks.

C. Oppnets Based Approaches:

The design of efficient routing strategies for opportunistic networks is generally a complicated task due to the absence of knowledge about the network. Routing performance improves when more knowledge about the expected topology of the network can be exploited.

a. Dissemination-based Approach:

Routing techniques based on Data Dissemination perform delivery of a message to destination by simply spreading it all over the network. The concept behind this routing approach is that, when there is no dedicated path to send message and the next hop is not defined then spread the message over the network it will reach the destination node by passing neighbour nodes in the network. High number of transmission may lead to traffic congestion.

b. Context-based Approach:

In context based we pass message to only those nodes which are known and have knowledge about direct contact with destination node. This approach helps to reduce message duplication as well as resource consumption of dissemination based approach. It will reduce delay and message loss.

c. Fixed Infrastructure Approach:

A fixed infrastructure consists of special fixed nodes, i.e., base stations, which are moved all over the network. A

source node wishing to deliver a message keeps it until it comes within reach of a base station, then forwards the message to the base station. Two variations of the protocol are possible. only node-to-base-station communications and both node-to-base-station and node-to-node communications[8].

II. RELATED WORK

The opportunistic networks (OppNets) are characterized as a most challenging evolution of Mobile Ad – Hoc Networks (MANET). OppNet provide possibility to exchange messages between mobile nodes (users) even in such a disconnected environment by opportunistically selection any nearby device to move messages closer to the final nodes. The routing protocols that we use in opportunistic network are very different form that we use in the wireless or wired communication the routing protocols in opportunistic networks has been given by various researchers. In year 2007 Rainer Baumann[2] gives a paper on a protocol called Ad-Hoc-on-Demand Distance Vector (AODV). AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbors and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop. When a link breaks a Count-To-Infinity could happen. AODV is an 'on demand routing protocol' with small delay.

That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used by Keshav AODV is distributed, hop-by-hop, deterministic, single path and state dependent. When number of nodes increasing occupancy of links increases too and it also burden of networks and limits the effective data flow.

In year 2007 Ram Ramanathan, Richard Hansen and Prithwish Basu[1] has given a routing algorithm PRioritized EPidemic (PREP) in this PREP prioritizes bundles based on costs to destination, source, and expiry time. Costs are derived from per-link "average availability" information that is disseminated in an epidemic manner. PREP maintains a gradient of replication density that decreases with increasing distance from the destination. Actually it is prurly based on flooding each source node send out the request packet and forward the packet on its entire outlinks. Each request packet may reach the destination along the different route at different time. It simply finds the route to the destination. Flooding causes a huge number of control packets which can result in network congestion very costly in terms of energy consumption. To overcome this one way is to use the hop counter in the header of each packet and decrement when reaches to zero and simply discard the packet. Then in the year 2008 another routing protocol comes in existence called Spray and Wait, Thrasyvoulos Spyropoulos, Konstantinos Psounis, CauligiS. Raghavendra[3] gives a paper on Spray and Wait in that paper Spray and Wait distributes only a small number of copies. Spray and Wait routing consists of the following two phases: **spray phase:** for every message originating at a source node, L message copies are initially spread—forwarded by the source and possibly other nodes receiving a copy—to L distinct path. **wait phase:** if the destination is not found in the spraying phase, each of the L nodes carrying a message copy performs"Direct Transmission".

Then in year 2012 Mamoun Hussein Mamoun, Wafaa Shaban[4] gives another algorithm for the routing in the opportunistic networks and publish a paper named Performance Comparison of Routing Protocols in Opportunistic Networks in this it gives a comparison of routing algorithm called Probability Routing Using History of Encounters and Transitivity (PROPHET) and Epidemic routing protocol . PROPHET is based on context information technique and Epidemic based on context oblivious. And finally conclude that Epidemic routing protocol gives a better results than PROPHET. PROPHET firstly detect the new neighbour execute PROPHET HELLO PROTOCOL to confirm then exchange information then periodically repeat complete information exchange. In this protocol break off and connection may happen at any stage.

III. COMPARITIVE STUDY

Author(s)	Year	Paper Name	Technique	Result
Ram Ramanathan, Richard Hansen and Prithwish Basu	2007	Prioritized Epidemic Routing for Opportunistic Networks	Epidemic routing (Context Oblivious)	Easily to route packet but create congestion and very costly
Rainer Baumann, baumann	2007	Ad hoc on Demand Distance Vector Routing Protocol	AODV(Reactive routing)	Easy to implement does not create congestion
Thrasyvoulos Spyropoulos, Konstantinos Psounis, CauligiS. Raghavendra	2008	An efficient routing scheme for intermittently connected mobile network	Spray and Wait (Multicast)	More power consumption and less security
Mamoun Hussein Mamoun, Wafaa Shaban	2012	Performance Comparison of Routing Protocols in Opportunistic Networks	PROPHET (context Based)	Less power consumption but communication break off can be happen at any stage

Zehua Wang, Yuanzhu Chen	2012	CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks	AODV	Less power consumption and cheap
Mamoun Hussein Mamoun, Saud Barrak	2013	Adaptive Priority Routing Protocol for DTN Networks	APRP (Fuzzy Based)	Less delivery rate and overflow is more

IV. CONCLUSION

In this paper comparative study of different routing protocol with different tehchnique is dissucsed. In this survey different protocols use in the opportunistic network have their own limitations as in Spray and Wait have less security and more power consumption. In Epidemic routing protocol , it congested the network and it is very costly too. And in Probability Routing Using History of Encounters and Transitivity (PROPHET) break off may happen at any stage. In the comparative study we conclude that Epidemic routing protocol gives the better result and the PROPHET gives the worst result to transfer the packet from source to the destination. And in Ad-Hoc-On-Demand-Distance-Vector(AODV) routing protocol it limits the data flow but can be use for the future work in opportunistic network. Because packets in the AODV protocol guaranteed reaches to its destination in a very secure manner. And it is less costly in terms of energy consumption.

V. REFERENCES

[1]. Mamoun Hussein Mamoun, Saud Barrak "Adaptive Priority Routing Protocol for DTN Networks" International Journal of Engineering and Technology Volume 3 No. 3, March, 2013.

[2]. Zehua Wang et al. "CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks" IEEE Journal on Selected Areas in Communications, VOL. 30, NO. 2, February 2012.

[3]. Mamoun Hussein Mamoun, Wafaa Shaban "Performance Comparison of Routing Protocols in Opportunistic Networks" International Journal of Engineering and Technology Volume 2 No. 6, June, 2012.

[4]. Thrasyvoulos Spyropoulos, Konstantinos Psounis, Cauligi S. Raghavendra "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case" IEEE/ACM Transactions on Networking, Vol. 16, No. 1, February 2008.

[5]. Chung-Ming Huang, Kun-chan Lan and Chang-Zhou Tsai "A Survey of Opportunistic Networks" IEEE Computer Society, 978-0-7695-3096-3/2008.

[6]. Ram Ramanathan , Richard Hansen "Prioritized Epidemic Routing for Opportunistic Networks" June11,2007, San Juan, Puerto Rico, USA.

[7]. Pelusi, L., Passarella, A. and Conti, M. (2006) "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks", IEEE Communications Magazine, Vol. 44, pp.134–141.

[8]. V. Karpijoki, "Security in Ad hoc Networks", Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland, 2000.