ProEp Protocol for Message Passing in Opportunistic Networks

Amit G Patil
M.Tech Scholar,
CIIT, Indore,
Madhya Pradesh, INDIA.

Megha Singh
Asst. Professor,
CIIT, Indore,
Madhya Pradesh, INDIA.

ABSTRACT
Opportunistic networks are one of the most interesting evolutions of MANETs. In opportunistic networks, route connecting to the mobile nodes never exits, mobile nodes communicate with each other when they got opportunity to communicate. Furthermore, nodes are not supposed to possess or acquire any knowledge about the network topology. Routes are built dynamically, while messages are route between the source and the destination, and any possible node can opportunistically be used as next hop, provided it is likely to bring the message closer to the final destination. These requirements make opportunistic networks a challenging and promising research field. In this report I describe hybrid approach for routing in opportunistic networks, rendering traditional routing protocols unable to deliver messages between hosts. Thus, there is a need for a way to route through such networks. We propose hybrid approach which combines Epidemic Routing and Probabilistic Routing approaches together, we named the protocol as **ProEp**. This protocol results in improved message delivery and low overhead on resources.

Keywords
PROPHET, Epidemic routing, Opportunistic Networks

1. INTRODUCTION
With the proliferation of a variety of wireless access technologies, seamless connectivity and anywhere, anytime computing are commonly touted as the paradigms for serving mobile users. Further, broadband wireless access is described as the panacea for the last-mile problem. While the vision of seamless connectivity and broadband wireless Internet access is attractive, it is far from reality. For various regulatory, technical and economical reasons, wireless access networks worldwide fail to fulfill the promise of continuous, high-bandwidth, and affordable service.

Cellular networks (e.g., GSM/UMTS) are the most common option for mobile wide-area network access. Their coverage continues to be variable and intermittent. In terms of performance, 2/2.5G networks provide low bandwidth access. While 3G promises high bandwidth access, it is expensive and its metered service is not viewed as a true option for extensive Internet access. The potential success of newer technologies using licensed spectrum such as IEEE 802.16 (WiMax) remains questionable.[2] The substantial investment made in 3G licenses and infrastructure is a deterrent for network operators to adopt a new technology for mobile broadband access. As a broadband solution to the last-mile problem in poor and developing countries and in rural and remote areas, WiMax and other licensed wireless access technologies face the chicken-and-egg problem of the simultaneous need for both a market and an infrastructure. Providing continuous broadband coverage in rural areas can be an expensive endeavor for network operators due to the sparse population density, e.g., challenging terrain, and lack of other relevant infrastructure such as reliable supply of electricity [2]. IEEE 802.11 (WiFi) has experienced widespread proliferation thanks to its operation in the unlicensed spectrum and cheap hardware. But coverage of WiFi hotspots is limited to few hundred meters.

In spite of efforts to extend the coverage of infrastructure wireless networks, for instance, using the multi-hop ad-hoc and mesh networking approach, intermittent connectivity prevails. Still, wireless access networks today are architect for providing continuous, synchronous access to users; to a great extent this can be attributed to the end-to-end communication paradigm prevalent in the Internet. Irrespective of the kind of network services a user is interested in, the end-user is expected to be physically present within the coverage of these infrastructure based access networks for any communication to take place. This, we believe, is a major hurdle for extending network access to a sizeable user population who cannot afford to be physically present within the coverage area of the nearest base station or hotspot and to mobile users who find it cumbersome keeping track of their intermittent network access as they move in and out of the sporadic coverage. While continuous, connectivity is essential for synchronous applications such as real-time video and voice conferencing, there are many asynchronous applications: cached Web access, electronic mail, multimedia messaging, news casting, file sharing, and blogging, to name a few that do not need continuous network access. But today's networks and protocols are not resilient to disruption of communication links, and are not designed to exploit intermittent availability of network resources. Communication opportunities in a network can arise in different forms. They can be:

1. Deterministic periodic connectivity, e.g., in an interplanetary network based on the movement patterns of planets and satellites, or connectivity that is a function of time synchronization among sensors.
2. Coordinated a group of users deciding to meet at a particular location at a certain time to share data.
3. Spontaneous when two or more devices meet by chance, e.g., two or more users with common interests meeting at an airport.

1.1 Wireless Ad Hoc Networks

A wireless ad-hoc network is a decentralized type of wireless network.[4] The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks

1.2 Types of Wireless Ad-Hoc Networks

1.2.1 MANET

A mobile ad-hoc network (MANET) is a self-configuring infra-structure less network of mobile devices connected by wireless links. ad hoc is Latin and means "for this purpose" [18].

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

1.2.2 VANET

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes [19].

1.2.3 OPPNET

The literal meaning of the term "opportunistic" is evident-the tendency of network devices to exploit available resources in the network as and when possible. In the context of communication networks, though, it represents many more subtle properties [21].

Opportunistic networks are intrinsically fault tolerant for they are not limited by the end to-end connectivity assumption. These networks are distributed and self-organizing in that the control and management is largely up to the individual devices or users (within the boundaries defined by the network operator's policies, if part of a commercial network). The communication in these networks is localized, i.e., decisions such as routing are made by devices based on locally available information. Opportunistic also means being able to take advantage of locally accessed global information, where devices implicitly convey global reach ability information strictly through local interaction. This type of network are useful in condition of disaster where network or communication line which we are currently using shuts down and people can help each other to communicate. Though there are some issues with reliability and security of opportunistic network as for reliability packet will be forward in the direction opposite to which destination node is wasting bandwidth. Security in opportunistic network is a biggest problem as packets will pass from many nodes between source and destination there is no guarantee that security will be preserved.

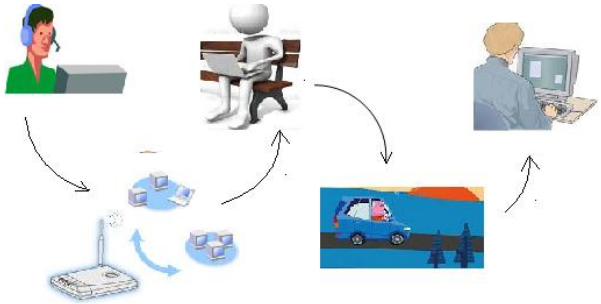

Figure 1: Example of Opportunistic Networking

For example, as is shown in Figure 1, the man at the desktop opportunistically transfers, via a Wi-Fi link to his collogue seated at the other office. First the message reach to the wireless hub then after it moves to boy seated on bench in a park with his laptop accessing the same wireless hub. Then this message is send to the men with his cars Bluetooth radio will carry the information closer to the destination. The men with car moves through the long distance, then uses its Bluetooth radio to forward the message to the final destination device while moving near by the office of the second men. As it is clearly shown in this example, a network connection between the two men never exists but, by opportunistically exploiting contacts among heterogeneous devices, the message is delivered hop-by-hop (hopefully) closer to the destination, and eventually to the destination itself.

Wireless network infrastructures have been expanding at a rapid pace throughout the world. However, wireless networks may still not be available in areas such as poor regions, underwater sensors, or military operations. In order to provide networking support for situations where there are no directly connectivity paths, opportunistic network can be applied. Opportunistic network is a type of delay tolerant, intermittently connected network using an ad-hoc like structure. When a node wants to deliver data to another node but there does not exist a direct connection between them, packets can be forwarded to intermediate participating nodes which aid in delivering the packet from the source to the destination. 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. 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 [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 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, there is still room for improvements. Due to the FIFO queuing nature of PRoPHET, 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 [5]. And another protocol is Epidemic routing [4] in which a node A ”infects” every contact B with packets that it has that B doesn't have. A summary vector is typically exchanged to determine the missing packets. Epidemic routing is unbeatable from the point of view of successful delivery as long as the load does not stress the resources (bandwidth, storage).

We present a novel hybrid approach for routing in opportunistic network. We propose the use of probabilistic routing [3], and Epidemic Routing [4] using an assumption of non-random mobility of nodes to improve the delivery rate of messages while keeping buffer usage and communication overhead at a low level.

2. RELATED WORK

Routing Techniques in opportunistic networks:

In opportunistic networks, network resources are constrained eg., node depends on nodes battery power for its working, nodes are subjected to low memory space; also performance of these networks is depends on bandwidth of network. Routing is difficult in opportunistic networks because of no topology defined and frequent disconnections in nodes.

According to the method used to forward the message in opportunistic network we categorize them as follows:

- Single-copy routing schemes.
- Multiple-copy routing schemes.

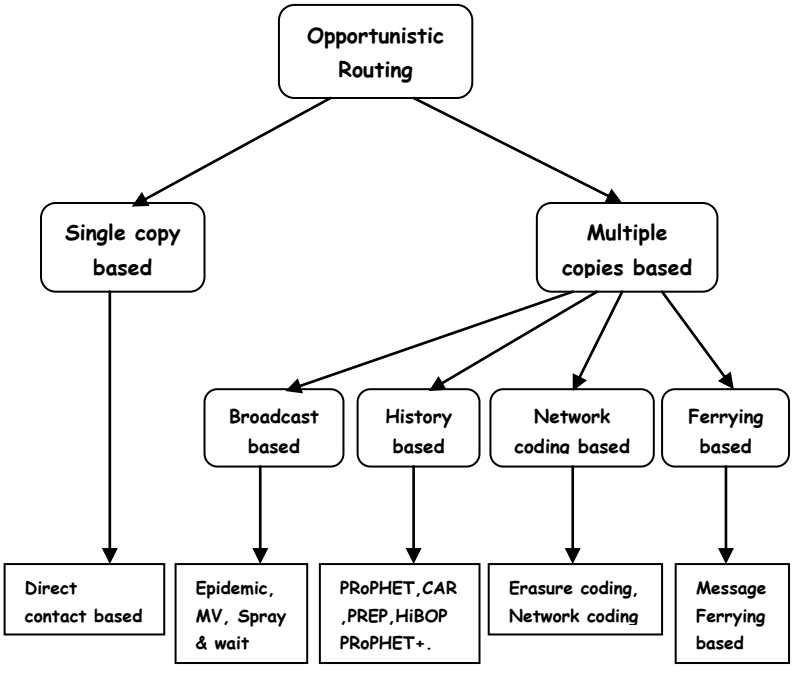

Figure 2: Classifiaction of Opportunistic Networking

Single-copy routing schemes

Single copy routing based algorithms do not duplicate messages in network, from sender to receiver transmission takes place only. Direct contact based algorithm are well known algorithm in single copy schemes [14].

Direct contact based algorithm

Using single-copy approaches the direct contact based algorithm was found the problem of efficient routing in intermittently connected mobile networks [14]. In this algorithm each node maintains the record of time elapsed since every other node was last communicated. Some kind of a utility function for each node (on a per-destination basis), gives the probability that the node will deliver the packet to the destination. With the help of these utility function we can gets the indirect location of the nodes. Here they defined such a utility function and propose a utility-based routing scheme, based on it and compare its performance, both analytically and using simulations, to that of a simple randomized routing algorithm. Also they derive and analyze an oracle-based optimal algorithm, and compare its performance to that of the on-line algorithms. T. Spyropoulos proposed a simple single-copy routing called direct transmission routing [14]. In this approach, after the source node generates a message, the message is hold by the source node until it reaches the destination node.

Multiple-copy routing schemes:

In multiple copy routing schemes messages are relayed in network, while transmission between sender and receiver. In this technique resource consumption is more. Some of well known protocols from this are described as follows.

Broadcast based algorithms:

In message Broadcasting Routing techniques message is reached to its destination by broadcasting the message by every intermediate nodes. This approach is used because, there is no knowledge of a possible path towards the destination nor of an appropriate next-hop node, should a message be sent everywhere. Broadcast-based techniques work well in highly mobile networks where contact opportunities, which are needed for data diffusion, are very common.

Following algorithms are based on broadcast based technique:

Epidemic routing:

Epidemic Routing relies on the theory of epidemic algorithms by doing pair-wise information of messages between nodes as they get contact with each other to eventually deliver messages to the destination. Nodes buffer messages when there is no available path to the destination. An index of these messages called a summary vector is kept by the nodes, and when two nodes meet they exchange them. So doing, each node can determine if the other node has some message that it did not see before and requests it. This means that, as long as there is some available buffer spaces, messages will spread epidemically as a disease, as nodes meet and ”infect” each other. Besides the obvious fields of source and destination addresses, messages also contain a hop count field. This field is similar to the TTL field in IP packets and determines the maximum number of hops a message can be sent, and can be used to limit the resource utilization of the protocol [4].

MV routing:

MV routing maintains a movement model of the participant's nodes and with the maintained information performs the routing of the messages [13]. The probability of a particular message being delivered by a given peer is calculated, and it makes the routing decisions. The MV routing protocol is a

further step beyond epidemic routing. Messages are exchanged during pair-wise contacts as in epidemic routing. However, the MV protocol introduces a more sophisticated method to select the messages to forward to an encountered node. Basically, the choice depends on the probability of encountered nodes to successfully deliver messages to their eventual destinations.

Spray and wait:

Spray and Wait routing schemes combines the single and multiple copy scheme [12]. It works in two phases, initially it starts spreading message copies as like epidemic routing (ie., broadcasting) and then after it stop spreading and starts direct transmission when it guarantees that enough copies have been spread that one of them will find the destination quickly. The major issue here is when to stop spreading. One of the solution is Binary Spray and Wait, in this source starting with suppose 'n' number of copies are starts spreading initially, any node say A has n>1 message copies, and communicates with the other node say B with no message copies, copies to B [n/2] and keeps [n/2] for itself, and finally when it remains only one copy, it starts direct transmission. In the low load, Spray and Wait gives fewer transmissions and smaller delays than flooding-based schemes, under high load, it results significantly better delays and fewer transmissions than flooding-based schemes.

History data based algorithms

History data based algorithms uses the history of nodes for taking forwarding decision. History of nodes contains information like context data, number of previous encounters, movement pattern.

This method includes following protocols

PROPHET:

In the Probabilistic Routing Protocol using History of Encounters and Transitivity, the selection of the best neighbor node is based on how frequently a node encounters another [3]. Prophet uses a probabilistic metric called delivery predictability that indicates how likely it is that A will meet B, and thus that will be able to deliver a message to B. When two nodes meet, they exchange their summary vectors, which contain their delivery predictability information. If two nodes do not meet for a while, the delivery predictability reduces. When the sender wants to send a message to the destination D, it will look for the neighbor node that has the highest amount of time encountering D, meaning that has the highest delivery predictability to D. This property is further transitive.

HiBoP Protocol :

HiBOP protocol is based on the concept of using context information for routing decision [20]. Basically forwarding is based on the concept of opportunity to reach a certain destination, measured in term of probability of carrying the message closer to the destination. Messages are forwarded only to nodes with higher probability of getting them closer to the destination.

PRoPHET:

PRoPHET+ routing scheme is designed to maximize successful data delivery rate and minimize transmission delay [5]. In this scheme a deliverability value is calculated for determining routing path for packets. Deliverability is calculated using a weighted function consisting of evaluations of nodes' buffer size, power, location, popularity, and the predictability value from PRoPHET. This minimizes drawbacks of PRoPHET,by using weighted function technique.

Prioritized Epidemic Routing for Opportunistic Networks:

Prioritized Epidemic (PREP) uses expiry time information of the bundles carried by nodes and topology awareness to decide which bundles to delete or hold back when nodes face a resource (buffer, bandwidth) crunch [6].

Context-Aware Routing (CAR):

In Context-Aware Routing (CAR) protocol asynchronous communication for message concepts provides by [8]. While delivering the message most of the times the receiver in opportunistic network is not often the same connected network, that's why the synchronous delivery of messages is really hard. CAR sends the message to the host that has highest probability, when synchronously delivery is not possible. The hosts act as a message carrier in this case. Probability is based on the evaluation and prediction of context information using Kalman filters. The process of prediction starts when there is an temporary disconnection and the process is continued until it is possible to guarantee certain accuracy.

Ferrying based algorithms

Message Ferrying uses a set of special mobile nodes called message ferries which provide communication services for nodes in the network [10]. As in the real life, message ferries move around the deployment area and collect and carry data between nodes. The non-randomness in the movement of nodes is the basic idea of this protocol. And with the help of this non-randomness they try to exploit such non-randomness to help deliver data. This approach is most of the times in the areas like battlefields, disaster relief, wide area sensing, non-interactive internet access and anonymous communication.

Network coding based algorithms

Erasure based coding:

Routing in Delay Tolerant Networks (DTN) is challenging because of two main reasons, one is the uncontrolled node mobility which generally results in disconnections in the network and second is poor information abot the network dynamics results into bad decision making.

Sushant Jain proposes an alternate method of improving delay performance [16]. In this approach the erasure code a message and distribute the produced code blocks over a big number of relays. Instead of sending the whole copy of the message over the relay, only part of code blocks is sent over the each relay. This approach is uses to controls the routing overhead.

Network coding based:

The algorithm is stateless, which do not required future and past encounters. Network coding based communication algorithm is similar to probabilistic routing but is based on network coding [17]. In network coding with some linear combinations of the previously received information, message is forwarded instead of simply forwarding packets. As compares to the opportunistic network forwarding techniques the network coding based protocol performs well in the extreme conditions such as a sparse mobile network with high packet drop rate and the nodes continuously goes into the sleeping mode to consume the power.

3. PROPOSED WORK

3.1 Problem Definition

In an opportunistic network, when nodes move away or turn off their power to conserve energy, links may be disrupted or shut down periodically. These events result in intermittent connectivity. When there is no path existing between the source and the destination, the network partition occurs. Therefore, nodes need to communicate with each other via opportunistic contacts through store-carry-forward operation. In this section, we consider two specific challenges in an opportunistic network: the contact opportunity and the node storage.

During the survey of opportunistic networks, we came across the problems faced by opportunistic networks. When the message is passed from sender to destination, the message is broadcasted as the sender doesn't know about the exact location of the destination node. During this broadcasting, the message packet travels through the network searching for the destination node. During this, many message packets are lost. This is one problem with opportunistic network.

When the sender node sends a message packet to destination node, it remains unsure about the delivery of the message packet to destination. There is no guarantee of the successful delivery of message packet to the destination node. This brings the unreliability in the opportunistic network broadcasting mechanism.

On broadcasting the message packet to the neighboring nodes, many message packets is uselessly forwarded hence it results into Broadcast Storm Problem. This is one more issue in the opportunistic networks.

In opportunistic networks, the message packets are carried from sender to destination by the intermediate nodes. This brings in the problem of security. As the intermediate nodes receive the message packet, they can have an easy access to the content of the packets. So security has always been an issue in opportunistic networks.

The privacy and security challenges for opportunistic networks can be listed as follows
A. Increasing trust and secure routing
B. Helper privacy and opportunistic network privacy
C. Protecting data privacy
D. Ensuring data integrity
E. Identifying most dangerous attacks and sketching solutions
F. Intrusion detection. Right margins should be justified, not ragged.

The nodes participating in the broadcasting in opportunistic networks have to face the problem of location privacy. The nodes communicating with each others will know the location of the nodes they are communicating with and the nodes on the other side will also be able to know about their location. This gives the problem of location privacy.

In our research, we have chosen the problem of reliability. During the process of broadcasting, we have tried to provide a method of reliable broadcasting so that the sender will be assured that the message will be successfully delivered to the destination node. We have also tried to reduce the problem of **Broadcasting Storm**. Probability based forwarding of packets has been used as the method to implement reliable broadcasting in opportunistic networks.

3.2 Goals and Objectives

For building an efficient opportunistic network, several goals need to be focused. Following are the goals which need to be accomplished during implementing proper opportunistic networks.

- *Obtaining reliability:-*

Reliability means providing assured delivery of message from sender to destination node. When the message is forwarded from nodes to nodes, during every such forwarding an acknowledgements should be provided to the sender node from receiving node. This will guarantee the sender node that the message packet it forwards reaches the estimated destination.

- *Reducing the delay:-*

Delay means the total time taken by a message packet to reach the destination from source. When the message packets are broadcasted in the opportunistic network, the nodes carrying the message packet should chose the next hop considering that it should be the best next hop. This will ensure that the message packet reaches the required destination in minimum time.

- *Obtaining Security:-*

Security, as we know is one of the biggest issue in opportunistic networks. Security basically includes message content privacy and location privacy of the nodes participating in the opportunistic networks. To build an efficient opportunistic network, we should be able to tackle these two security challenges. The goal is to achieve a secured broadcasting mechanism..

- *Preventing Packet Loss:-*

During broadcasting in opportunistic networks, every node broadcasts the received packet to its neighbors. During this, there comes a phase of route discovery. During this phase, several packets are lost. The goal is to reduce this loss and prevent the loss by selecting only those nodes that will guarantee that they will be able to deliver the message to the further nodes successfully.

3.3 Proposed System

We are going to develop hybrid architecture for reliable message passing in opportunistic network, rendering traditional routing protocols unable to deliver messages between hosts, which combines Epidemic Routing and Probabilistic Routing approaches together.

3.3.1 Hybrid approach (ProEp protocol)

ProEp protocol is a novel approach for routing in opportunistic network. In this approach we combine both the Epidemic Routing and Probabilistic Routing. A node forwards the message to the two neighbors which are 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 to deliver message to destination b.

When two nodes meet, they exchange summary vectors which in this case also contain the delivery predictability information stored at the nodes. This information is used to update internal delivery predictability vector and after then the information in the summary vector is used to decide which message to request from the other node. Each host maintains a buffer consisting of messages that it has originated as well as messages that it is buffering on behalf of other hosts. A hash table indexes this list of messages, keyed by a unique identifier associated with each message. Each host stores a bit vector called the summary vector that indicates which entries in their local hash tables are set. To avoid redundancy, each

host maintains a cache of previously communicated hosts. When two hosts come into communication range of one another, they exchange their summary vectors to determine which messages stored remotely have not been seen by the local host. In turn, each host then requests copies of messages that it has not yet seen.

4. CONCLUSION

Opportunistic network is an emerging system that is getting growing interest in networking research community. The opportunistic network places different research challenges on different layers of a protocol stack. In this report, I provide hybrid routing approach for opportunistic network, which is made with taking features of epidemic and probabilistic routing techniques, which results in improved message delivery and low overhead on resources.

5. REFERANCES

[1] S. Burleigh et al.,"Delay-tolerant networking: An approach to interplanetary internet", IEEE ,Communications Magazine, June, 2003.

[2] Leszek Lilien, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta, "Opportunistic Networks:The Concept And Research Challenges In Privacy And Security"

[3] Anders Lindgren, Avri Doria, Olov Schelen, "Probabilistic Routing in Intermittently Connected Networks "

[4] Amin Vahdat and David Becker, "Epidemic routing for partially connected ad hoc networks", Technical Report CS-200006, Duke University, April 2000..

[5] Ting-Kai Huang, Chia-Keng Lee, Ling-Jyh Chen, "PRoPHET+: An Adaptive PRoPHET- Based Routing Protocol for Opportunistic Network", IEEE Proceedings,2011.

[6] Ram Ramanathan and Richard Hansen and Prithwish Basu, "Prioritized Epidemic Routing for Opportunistic Networks", MobiOpp'07, June 11, 2007, San Juan, Puerto Rico, USA. Copyright 2007 ACM 978-1-59593-688-2/07/0006.

[7] Anders Lindgren and Avri Doria and Olov Schelen, "Poster: Probabilistic routing in intermittently connected networks", in Proceedings of The 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing , June 2003.

[8] Chung-Ming Huang and Kun-chan Lan and Chang-Zhou Tsai, "A Survey of Opportunistic Networks", 22nd International Conference on Advanced Information Networking and Applications - Workshops, 978-0-7695-3096-3/08 IEEE DOI 10.1109/WAINA.2008.292.

[9] Elizabeth M. Royer and Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications Magazine, vol. 6, no. 2, pp. 46-55, Apr. 1999.

[10] Wenrui Zhao and Mostafa Ammar and Ellen Zegura (2004), "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks"

[11] Vijay Erramilli and Mark Crovella, "Forwarding in Opportunistic Networks with Resource Constraints", (2004)

[12] Thrasyvoulos Spyropou- los and Konstantinos Psounis and Cauligi S. Raghavendra , "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks", (2005).

[13] Daddy Marasigan and Papa Rommel,"Mv routing and capacity building in disruption tolerant networks", In INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Proceedings IEEE, volume 1, pages 398-408 vol. 1, March 2005.

[14] T. Spyropoulos and K. Psounis and C. S. Raghavendra, "Single-copy routing in intermittently connected mobile networks In Sensor and Ad Hoc Communications and Networks", IEEE SECON 2004, 2004, pages 235-244.

[15] J. Sushant, K. Fall and R. Patra, "Routing in a delay tolerant network", (2004).

[16] Yong Wang and Sushant Jain and Margaret Martonosi and Kevin Fall, "Erasure coding based routing for opportunistic networks ", In WDTN '05: Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, pages 229-236, New York, NY, USA, August.

[17] Jorg Widmer and Jean-Yves Le Boudec, "Network coding for efficient communication in extreme networks", In WDTN '05: Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, pages 284-291, New York, NY, USA, 2005. ACM

[18] Julien Haillot, "Content-Based Communication in Disconnected Mobile Ad Hoc Networks"

[19] Kamini Rakesh Ku mar ,"VANET Parameters and Applications: A Review", (2010).

[20] Boldrini and Marco Conti and Iacopo Iacopini and Andrea Passarella, "History Based Routing Protocol for Opportunistic Networks", 2007.

[21] Upinder Kaur and Harleen kaur, "Routing techniques for Opportunistic Networks and Security Issues , (2009).

[22] Qun Li and Daniela Rus, "Communication in disconnected ad-hoc networks using message relay", Journal of Parallel and Distributed Computing, 2003.

[23] P. Marshall, "The disruption tolerant networking program",2005.http://www.darpa.mil/sto/solicitations/DTN/briefs.htm.

[24] A. Pentland and R. Fletcher and and A. Hasson. Daknet, "Rethinking connectivity in developing nations, IEEE Computer 37(1), 78-83, Jan 2004.

[25] Werner Vogels and Robbert van Renesse and Ken Birman, "The power of epidemics: Robust communication for large-scale distributed systems," in Proceedings of First Workshop on Hot Topics in Networks (HotNets-I), 28-29 October 2002, Princeton, New Jersey, USA, oct 2002.