Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Opportunistic Networks: An Evolution in Mobile Ad-Hoc Networks

J. Divyateja, R.Vijay Prakash
SR Engineering College, Warangal,
Telangana, India

Abstract: In MANET's opportunistic networks are great step as the nodes in this type of network can interact with each other even in absence of no route existing between them. Information about the topology of the network is not reveled to the node which will be forwarding the data which is necessary in for data transfer in traditional routing protocols. In opportunistic network while messages are sent then the routes are built dynamically. When data is transferred from source to destination hops are opportunistically created based on the closest one compared to the destination. In this type of network end to end path may exists or many not exists, so finding the path will be a tricky part. The main function when transferring the data is reliability and congestion controls are ineffective in opportunistic networks. Intermediate nodes take the responsibility of maintaining the data and start the transfer once the connectivity resumes. All these interesting features make opportunistic networks a challenging and research topic.

Keywords: MANETs, Intermittently connected networks, Opportunistic networks, Transfer reliability, Storage congestion control.

I. INTRODUCTION

Opportunistic network is an evolution of mobile ad-hoc networks (MANET), when researchers start bringing MANET research from theory to practice [3]. In contrast to MANET, opportunistic networks do not assume that there exists an end-to-end connectivity between source and destination nodes, which is usually an unrealistic assumption in MANET research. Optimization by reducing the number of copies of the same message has been studied, such as Spray and Wait routing where each message can only have a limited number of copies in the network. When mobile nodes are not connected to a fixed-infrastructure network or a docking station they operate in disruption tolerant mode. In this mode they utilize node to-node contact to come up as nodes move around, to seek content in a peer-to-peer manner. We consider an opportunistic network as a subclass of Delay-Tolerant Network where communication opportunities (contacts) are discontinuous, as a result end-to-end path between the source and the destination may never exist.

II. ICN OVERVIEW

As shown in figure.1 three networks are connected continuously to each other in which a satellite link is established between the two networks namely 1 and 2 and a vehicular network is established between networks 1 and 3.Here the satellite link is likely to be predictable and scheduled accordingly whereas on the other hand vehicle based links seems to be unpredictable so treated as opportunistic. When vehicle contacts are occurred due to short or long duration then ICN nodes have to take responsibility and manage data transfer among disconnected networks at that movement. As soon as when node comes to contact then it can transfer data for sending as well as receiving bundles (arbitrary sized data unit) that have time to live before the bundle expires. Also when node or link is not available the node can wait for some time and stores bundle or else sent to the neighboring node so that it can get better chance to reach destination.

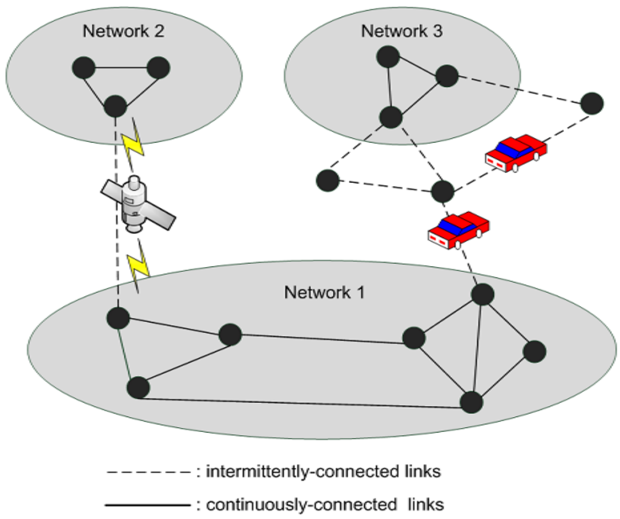

Figure 1: Intermittently connected networks

The communications that are were disconnected areas previously is likely to be perform by store forward method that is in between networks 1 and 2 or else in (SCF) mechanism, e.g. in the vehicular network between network 1 and 3. In SF, when there is no next hop known or no available link to the next known node that gets bundles that were stored at node buffer waits for next turn.

2.1. ICN Routing Strategies

Due to lack of updating in network topology data we get complications in ICNs as compared to MANETs. So we broadly divide in to three categories in the case of regularity in nodes those are as follows:

- on-demand contact,
- scheduled or predicted contact and
- opportunistic contact

As shown in Fig. 2 ,we divide networks in to either static or mobile based on node mobility and second one considered to be wireless sensor networks in which nodes can conserve energy based on radio connection when not available. So in turn links are always available when needed in case of MANETs so termed as on-demand contact. Similarly we can schedule or predicted node contacts but in some cases we can't predict we call it as opportunistic networks.

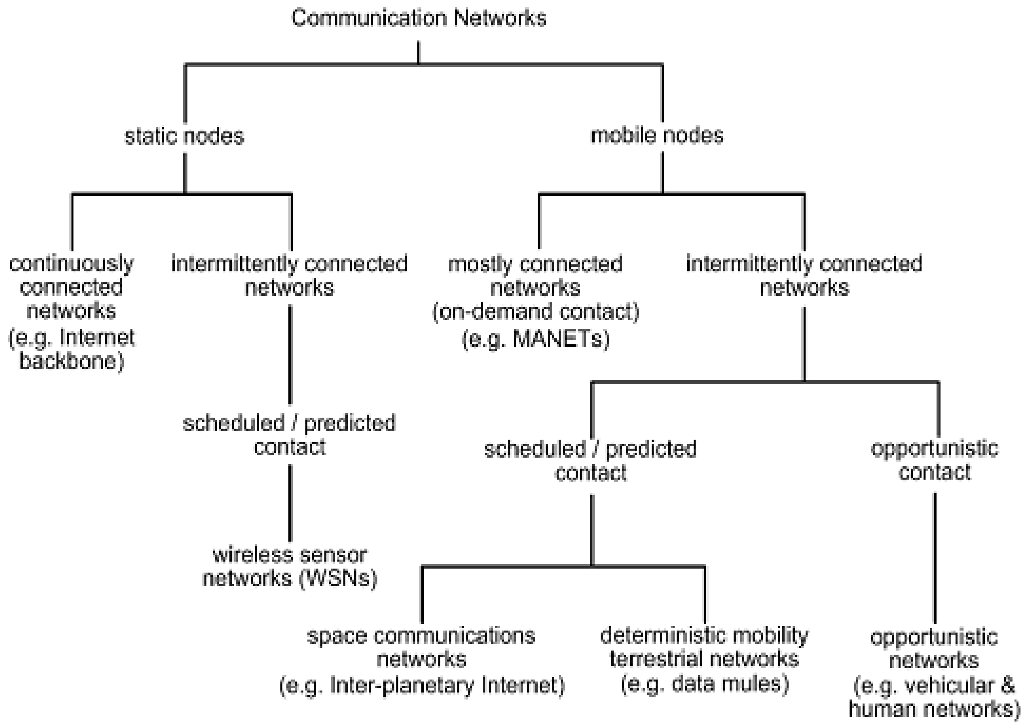

Fig. 2. Taxonomy of communication networks.

2.2. Poor Performance of TCP in ICNs

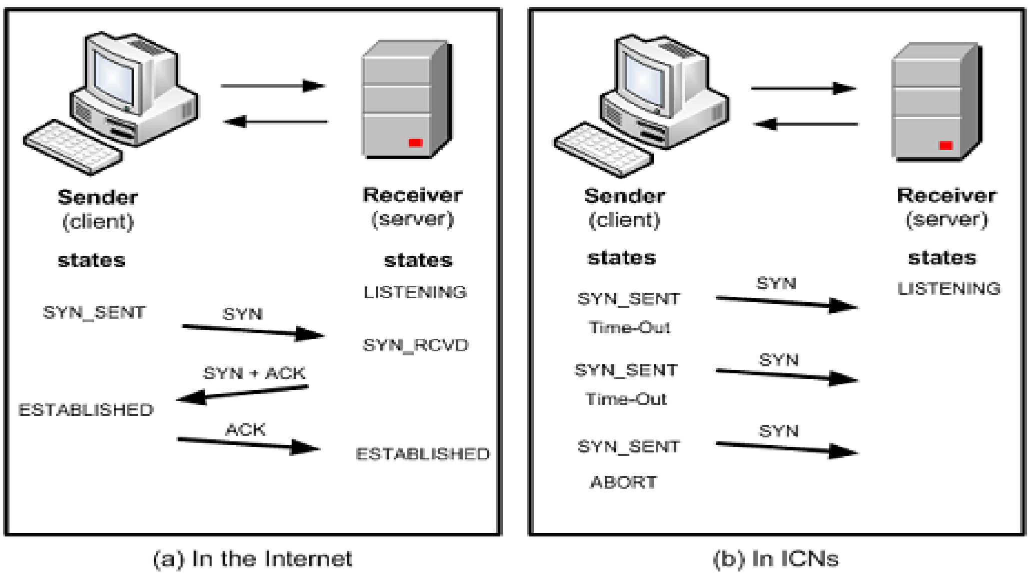

Fig. 3 TCP 3-way handshake.

Here TCP performs badly in ICNs due to long transfer delays in which foremost problem is -3-way handshake mechanism problem in which it doesn't works in case of high end to end delay latency. To do this we require 3 messages that can establish a TCP session between the sending party we call it as client and receiving party we call it as server as depicted in figure.3a.

As depicted in figure 3b due to high latency in the network TCP's retransmission timer gets expired finally makes TCP to stop to open the connection. Similarly second limitation is TCP's reliable data transfer so it can improvised by sending acknowledgement (Ack) to the source by the receiver when it gets data correctly

Due to variable network delays are high in case of ICNs the message round trip time couldn't be calculated and also retransmission time-out (RTO) values cannot be set easily so therefore source cannot detect lost message correctly and need to keep unacknowledged messages, for a long duration. In the same manner to maintain a good throughput, so that TCP has to use a big window size that is feasible for networks with reasonable delays

Finally, TCP had no chance of explicit knowledge of the congestion state in networks. On the other hand if source receives three duplicate Acks, or else TCP's retransmission timer expires, then it consider to be traffic congestion has occurred in turn reduces the sending rate to limit the network congestion. This kind of behaviour does seem to be in effectively in ICNs that have frequent link disruptions as well as long transfer delays: an acknowledgement received by the source that doesn't reflect the current condition of the network so therefore the source doesn't respond to congestion correctly.

III. T RANSFER RELIABILITY AND CONGESTION CONTROL IN OPPORTUNISTIC NETWORKS

Opportunistic networks have some characteristics that are distinct from ICNs in general and deep space networks in particular. In opportunistic networks, nodes usually move at random and link breaks due to node mobility are stochastic. In addition, the long transfer delay is due to the unpredictability of contact events and the limited contact period when nodes are in range, caused by long propagation delays.

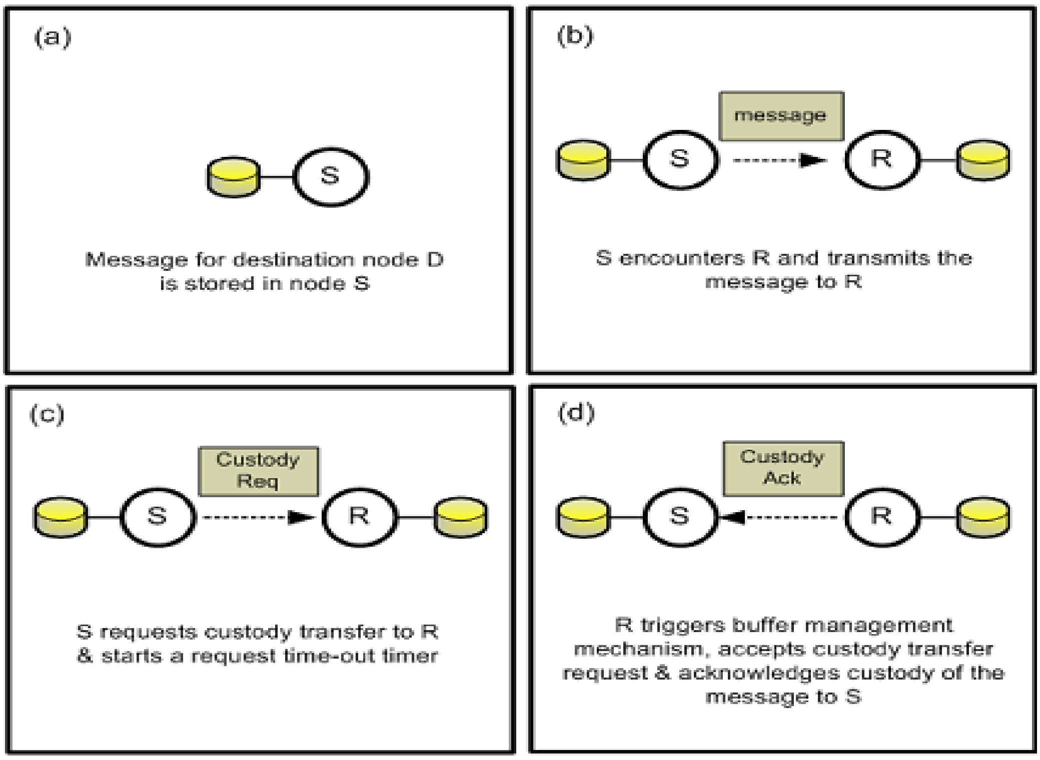

Fig. 4. Interaction of transfer reliability and congestion control strategies in Opportunistic networks.

We consider the simple custody transfer scenario shown in Fig. 4. A message destined for node D currently resides in the persistent storage of node S (Fig.4 (a)).

During its travel, node S encounters node R and, based on its routing protocol, determines that node R is a better relay of the message to node D. Node S therefore forwards the message to R (Fig. 4(b)). S then requests a custody transfer service for the message to R and starts a request time-out timer (Fig. 4(c)). Upon receiving the custody request, R triggers its buffer management mechanism (part of the storage congestion control function) to determine whether receiving the message is likely to lead to buffer congestion in future, and therefore decides whether to accept or reject the custody request. In the example shown, R accepts the request (Fig. 4(d)).

Based on the example in Fig. 4 we can summaries the requirements of the transfer reliability and congestion control strategies in opportunistic networks as follows:

- Transfer reliability should be implemented on a per-hop basis, for example using custody transfer.
- Congestion control should also be implemented on a perhop basis, based on locally available information and should be autonomous for every node.

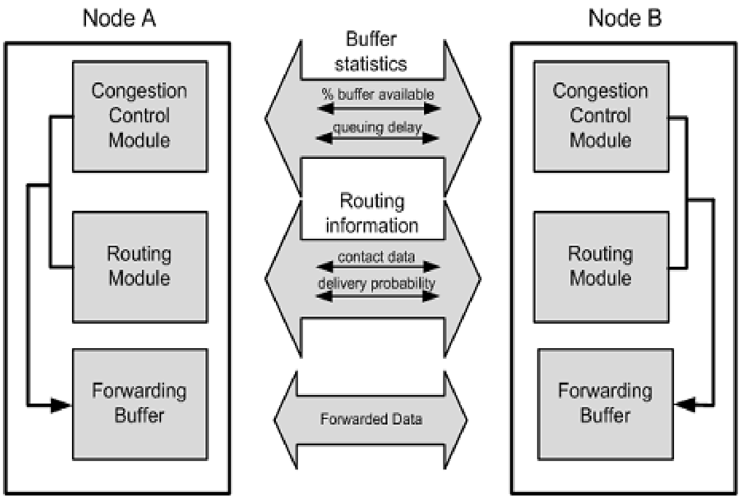

Fig. 5. Congestion-aware forwarding module in opportunistic network nodes

In Fig. 5, we depict a typical node's congestion-aware forwarding modules. The routing and congestion control modules work together to make forwarding decisions for messages in the buffer. A node will forward messages to a neighbour during contact if the neighbor meets the routing criteria and if the forwarded messages are unlikely to create congestion in the receiving neighbour's buffer in the future.

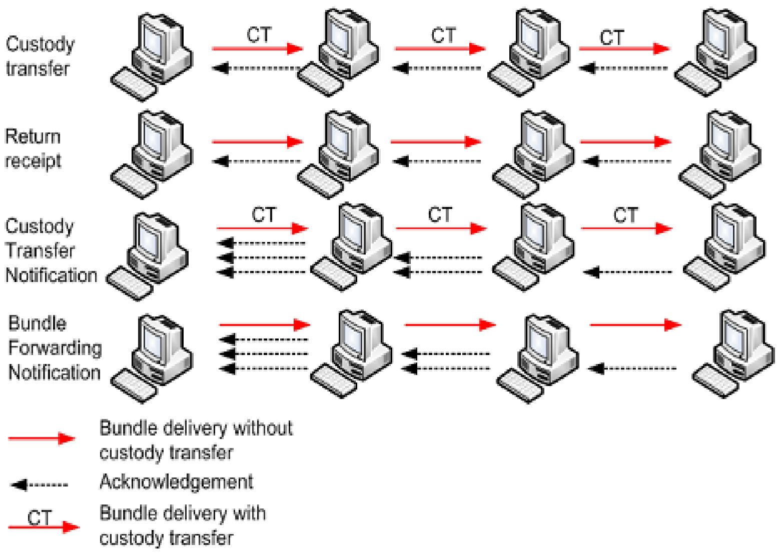

Fig. 6. ICN reliable message transfer services

Warthman [34] describes four classes of reliable message transfer service in ICNs, namely custody transfer (CT), return receipt (RR), CT notification and bundle forwarding notification (Fig. 6).

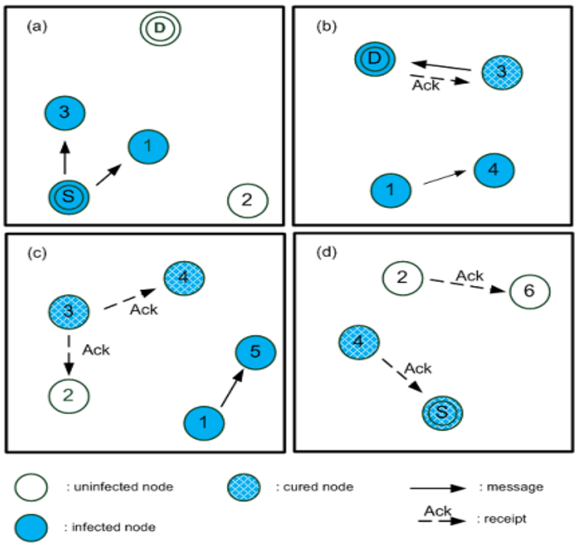

Fig. 7 Active-receipt reliability strategy.

3.1.Reliable Message Transfer

In this scheme (Fig. 7), nodes treat a receipt as a new message that needs to be forwarded to all other nodes at every contact. In Fig. 7(a) the source S passes the message to node 1 and 3; in Fig. 7(b) node 1 infects node 4 while node 3 delivers the message to the destination D and receives a receipt in return. On the way back to the source (Fig.7(c)), the receipt is passed to nodes 4 and 2, allowing the relay nodes to release the acknowledged message from their buffers (using the analogy of an epidemic, the "infected" nodes that have a copy of the message are "cured" by having the original message flushed).

IV. CONGESTION CONTROL

In this method Congestion makes a node to drop a message present in the buffer will makes to degrade the network's delivery ratio since there are no other available copies of the message present in the network and no mechanism can exists to intimate the source in a timely fashion so that it should retransmit the dropped message.

4.1. Storage Congestion Management - Economic Models

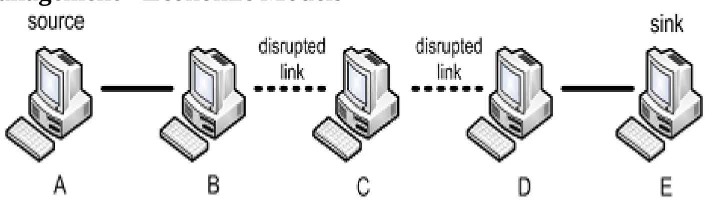

Fig. 8. Five-node line topology (Burleigh & Jennings)

In simulations, the authors used a linear five-node topology (Fig. 8) with the source sending messages at a constant transfer rate via the three intermediate (relay) nodes.

4.2. Storage Congestion Management - Traffic Distribution

This human movement behavior is triggered by individuals' social activity and is commonly described in social (relation) networks.

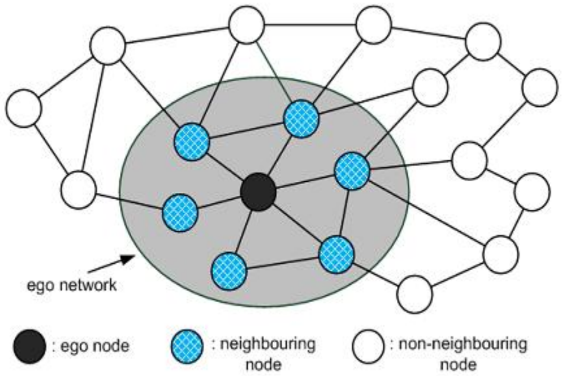

Fig. 9. An ego network

4.3. Congestion Avoidance

Token Based Congestion Control (TBCC) is a congestion avoidance proposal that attempts to match the volume of messages injected into a network with the total network capacity, i.e. the volume of messages the network can deliver to destinations in a bounded time.

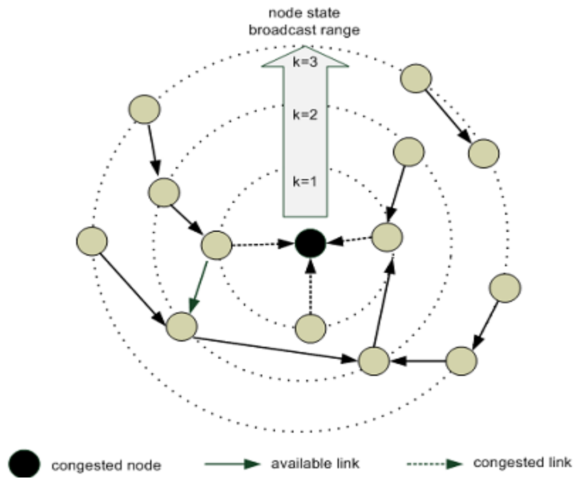

Fig. 10. Path avoidance among k-hop neighbouring nodes.

V. CONCLUSION

Strategies related to congestion and transfer need to be taken care while the messages are being transferred in a hop by hop basis manner and regularly used fixed networks function like packet dropping ,forwarding , congestions control are interrelated with each other. In this paper we provide an summary about congestions and transfer of data in opportunistic networks. Considering transfer reliability and congestion control proposals taking account of opportunistic networks' characteristics and identifying open research issues in transfer reliability and congestion control in opportunistic networks.

We hope the article enables readers to have a better understanding of the current state of the evolving research.

REFERENCES

[1] A. Lindgren and A. Doria, "Experiences from deploying a real life dtn system," In 2007 4th IEEE Consumer Communications and Networking Conference, pp. 217–221, 2007.

[2] "The zebranet wildlife tracker," http://www.princeton.edu/ mrm/zebranet.html.

[3] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Single-copy routing in intermittently connected mobile networks," In 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, pp. 235 –244, 2004. 1676

[4] P. Szczytowski, A. Khelil, A. Ali, N. Suri, "TOM: Topology Oriented Maintenance in Sparse Wireless Sensor Networks", Proc. 8th IEEE SECON, Salt Lake City, Utah, USA, June 2011.

[5] P. Juang, H. Oki, Y. Wang, "Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with Zebranet", Proc. ASPLOS, Oct. 2002.

[6] A.K. Pietilainen, C. Diot, "Social Pocket Switched Networks", Proc. 9^{th} INFOCOM Workshops, Rio de Janeiro, April 2009.

[7] P. Jacquet, P. Muhlethaler, T. Clausen, A.Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks",Proc. IEEE INMIC, Lahore, Pakistan, Dec. 2001.

[8] C.E. Perkins, E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop on Mobile Computing Systems and Application, New Orleans, Louisiana, USA, Feb. 1999.

[9] D. Johnson, Y. Hu, D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", IETF RFC 4728, 2007.

[10] G. Holland, N. Vaidya, "Analysis of TCP Performance over Mobile AdHoc Networks", Proc. ACM MOBICOM, Seattle, WA, USA, Aug. 1999

