IISRC International Industrial Scientific Research Corporation
International Conference on Industrial Scientific Research Engineering
www.worldconferences.org

Techniques to Ensure Reliable Data Transfer and Congestion Control in Wireless Networks

B. REVATHI[1], S.S. RAJA KUMARI[2]
[1]PG Scholar, Dept of CSE, John's College of Engineering & Technology, JNTUA, AP, India,
Email: bingi.revathi0@gmail.com.
[2]Assoc Prof, Dept of CSE, John's College of Engineering & Technology, JNTUA, AP, India,
Email: ssrajakumari2009@gmail.com.

Abstract: Opportunistic networks are a class of mobile ad hoc networks (MANETs) where contacts between mobile nodes occur unpredictably and where a complete end-to-end path between Source and destination rarely exists at one time. Two important functions, traditionally provided by the transport layer, are ensuring the reliability of data transmission between source and destination, and ensuring that the network does not become congested with traffic. However, modified versions of TCP that have been proposed to support these functions in MANETs are ineffective in opportunistic networks. Potential mechanisms for transfer reliability service are hop-by-hop custody transfer and end-to-end return receipt. The requirements for storage congestion control are identified and categorize based on the number of message copies distributed in the networks. The principal storage congestion control mechanisms for single-copy forwarding are storage congestion management and congestion avoidance mechanisms, for multiple-copy forwarding, replication management and drop policy.

Keywords: Mobile Ad hoc Networks (MANETS), Opportunistic Networks, Transfer Reliability, Storage Congestion Control.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are infrastructure less networks where nodes can move freely. One node can directly communicate with another if they are within radio communication range. A message traverses the network by being relayed from one node to another node until it reaches its destination (multi-hop communication). Since the nodes are moving, the network topology regularly changes and so finding a delivery path to a destination is a challenging task. Constructing end-to-end delivery paths and ensuring robust message delivery in the face of dynamic topology changes are challenges that have been addressed in MANETs. In some scenarios complete end-to-end paths rarely or never exist between sources and destinations within the MANET, due to high node mobility or low node density. As a consequence, the end-to-end transfer delays in these intermittently connected networks (ICNs). Within ICNs we can identify opportunistic networks, which are networks where contacts between mobile nodes occur unpredictably because the node's movement is effectively random, and where the duration of each node contact is also unpredictable. The challenges of developing efficient algorithms for opportunistic networks are different from those of classic ICNs.

II. TRANSFER RELIABILITY AND CONGESTION CONTROL IN OPPURTUNISTICS NETWORKS

Opportunistic networks have some characteristics that are distinct from ICNs. 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 within range, rather than being caused by long propagation delays. The requirements of an opportunistic network SCF delivery mechanism as follows

1. Hop-by-hop message relaying: an end-to-end path is divided into multiple hops and at every hop a node receives a message completely from its neighbor, stores it in memory, performs a routing table lookup and forwards the message to the next hop when contact occurs.

2. Storing messages for an extended period of time: due to the opportunistic contact, messages may have to be stored in a node's buffer for a long and unpredictable period of time. Buffer management is therefore particularly important. However, storage congestion control algorithms are difficult to design, since a node has no explicit knowledge of future node contacts or network topology.

3. Dealing with unpredictably moving nodes: since the network nodes move randomly, node contact is unpredictable and the contact duration may be limited, with large variations between individual contact events. An efficient forwarding strategy is therefore required to prioritize, select and forward messages that are to be transferred to a next hop node during the limited contact event.

A basic opportunistic network scenario is described and shown how the transfer reliability and congestion control functions may interact. Consider the simple custody transfer scenario shown in Fig. A message destined for node D currently resides in the persistent storage of node. 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. S then requests a custody transfer service for the message to R and starts a request time-out timer. 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. In order to optimize the overall delivery success ratio, node buffer management needs to consider several attributes of a message, such as message priority, message lifetime, message size, and the probability of message being further forwarded. Based on the example summarized requirement of the transfer reliability and congestion control strategies in opportunistic networks are 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 per hop basis, based on locally available information and should be autonomous for every node.

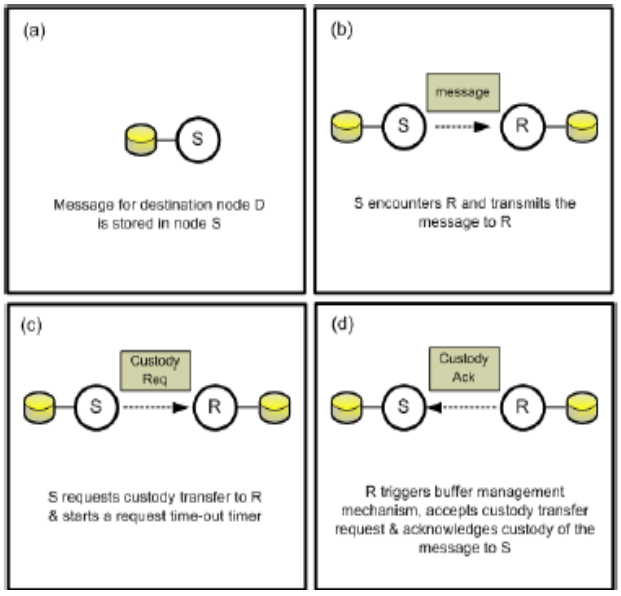

Fig1.

There are two forms of congestion in communication networks, namely link congestion and node storage congestion. A congested link occurs when two or more nodes that are within transmission range contend to transmit message using the same link or channel. However, congested links rarely occur in opportunistic networks. On the other hand, congested storage occurs when messages contend for the use of limited node storage space. Congestion control strategies in opportunistic networks are closely related to the number of message copies distributed throughout the network. Routing protocols may use a multiple copy strategy to increase the delivery ratio and/or to reduce end-to-end delivery latency. In this strategy, several copies of a message circulate in the network at any instant. Given the existence of redundant messages in the network it is likely that the provision of a custody service for messages is no longer needed, and in this case congestion control can be in the form of a message drop strategy. The end-to-end TCP mechanism ensures delivery, by requesting the source to retransmit the dropped messages.

In opportunistic networks, the long round trip time means that the end- to- end delivery mechanism is slow acting and hence dropped messages cannot be detected easily by the source. When an opportunistic network node has to drop messages during congestion, it needs to consider network delivery performance, for example by dropping those messages that have less impact on the end-to-end delivery. However, in the case of a single copy routing strategy, dropping messages during congestion may substantially decrease is overall delivery performance in the network. The congestion control strategy, or storage congestion management, should carefully select which messages are stored in a node so as to avoid future congestion. As an example, retaining messages that have longer remaining times to live (TTLs) is more risky and expensive for node buffer space than storing messages with small TTLs. TCP reduces its sending rate when it detects packet drops, as signaled by TCP's acknowledgment mechanism. However, as this end-to-end approach is inappropriate in opportunistic networks. Instead, congestion control should be performed on per hop basis, and a node should use locally available congestion information to manage message flows.

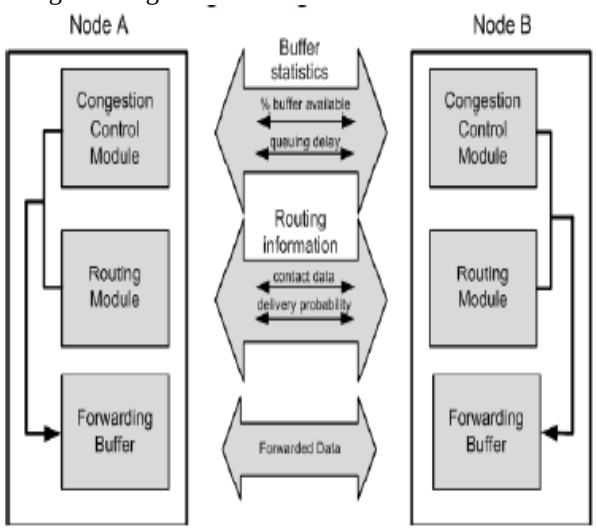

Fig2.

A typical node's congestion-aware forwarding module is shown. The routing and congestion control modules work

together to make forwarding decisions for messages in the buffer. During node contact, each module exchanges status data with its peer: the routing modules exchange routing information such as history contact data, delivery probability and node ranking, while the congestion control modules exchange node buffer statistics, for example buffer free space, queue growth rate, queuing delay and drop rate. A node will forward messages to a neighbor during contact if the neighbor meets the routing criteria and if the forwarded messages are unlikely to create congestion in the receiving neighbor's buffer in the future. In the multiple-copy forwarding case, the congestion control module can include a replication manager that controls the number of message copies distributed in the network based on the network's congestion state CT and RR are more applicable in opportunistic networks. This is because the other strategies consume significant mobile node energy and network bandwidth by sending many more Ack signals to upstream relays and the source.

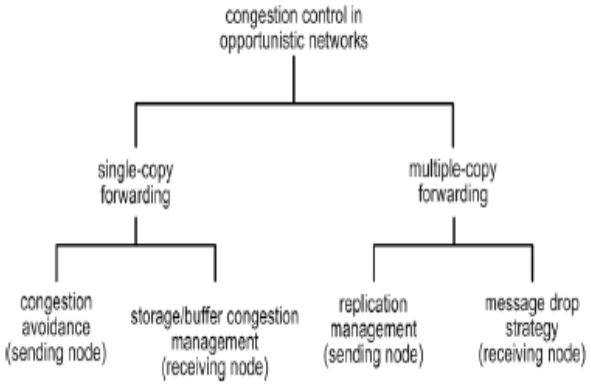

Fig3.

III. RELIABLE MESSAGE TRANSFER

There are four classes of reliable message transfer service in ICNs, namely custody transfer (CT), return receipt (RR), CT notification and bundle forwarding notification.

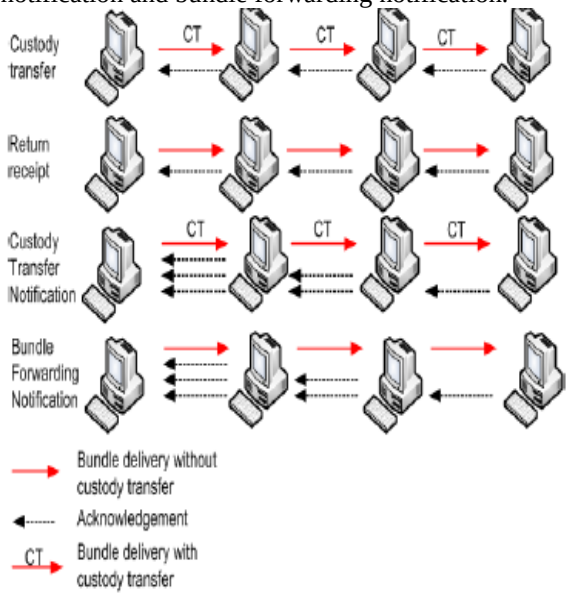

Fig4.

In CT, a custodian node takes responsibility for retransmission so the source can release its buffer quickly without waiting for an Ack to arrive from the destination. However, CT cannot provide a fully reliable data transfer service since if a custodian node fails it is unable to notify the source. On the other hand, in RR an end-to-end Ack is sent back to the source confirming that a message has been received by the destination. RR is therefore able to provide a fully end-to-end reliable service, but at the cost of using the source's storage space, which has to retain unacknowledged messages, potentially for a long time. Harras and Almeroth introduce four different end-to-end reliability approaches for opportunistic networks that use epidemic (oblivious) routing. These are hop-by-hop reliability, active receipt, passive receipt and network bridge receipt. In the hop-by-hop reliability strategy an acknowledgement is sent across the hop to confirm receipt of the message, as in Warthman's custody transfer scheme. Again, this does not ensure end-to-end reliability, but it has the advantage of minimizing the amount of time a message remains in the source buffer. The second scheme, active receipt, addresses end-to-end reliability by sending back an end-to-end acknowledgement (or receipt) from the destination to the source to acknowledge delivery of a message to the destination.

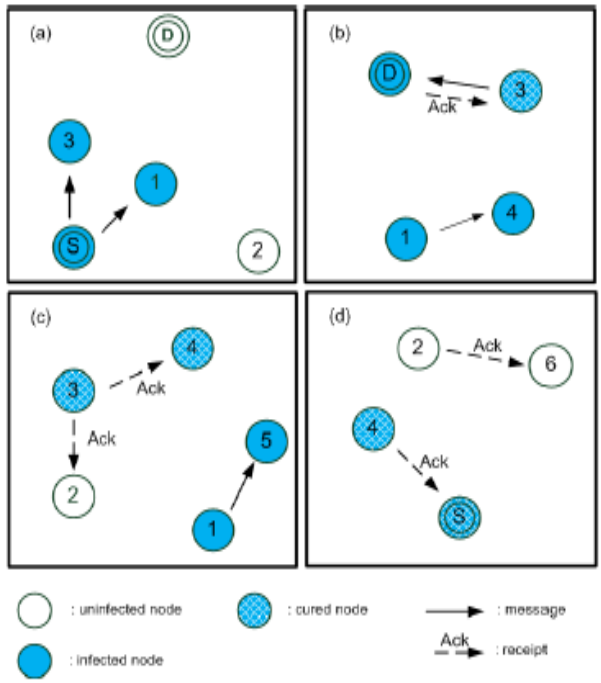

Fig5.

In this scheme nodes treat a receipt as a new message that needs to be forwarded to all other nodes at every contact. In this the source S passes the message to node 1 and 3; in Fig. 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 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). Even though the active receipt can offer end-to-end reliability, this is at a high cost since two messages, i.e. the original message and its receipt, are simultaneously

infecting nodes in the network. Node 2 also forwards the receipt to uninfected node 6).

The third of Harras and Almeroth's schemes, passive receipt, attempts to reduce the cost of active receipt. Here, a cured node does not actively send the receipt to all other nodes during contact; instead it forwards the receipt to an infected node only if the infected node tries to pass it the original message. By selectively forwarding the receipt, this scheme can reduce the total cost of forwarding receipts in the network. Finally, the fourth scheme, network-bridge receipt, was proposed to reduce the round trip time between two end nodes so that a receipt is quickly received by the source and hence the source can release the message promptly. This scheme assumes a parallel cellular network, which provides an alternative path to send a receipt directly to the source. This has the added complexity of bridging the opportunistic network and the cellular network. However, assuming the existence of a cellular network is contrary to the idea of the opportunistic network, since the latter typically operates in challenged environments with intermittent network connectivity. In these circumstances, it is inappropriate to assume nodes have access to infrastructure networks.

IV. CONGESTION CONTROL

In a single-copy forwarding strategy, every time a node successfully forwards a message to the next relay node or the destination, the forwarding node deletes the message in its storage. Thus, at any instant only one copy of the message exists in the network. Congestion that forces a node to drop a message in the buffer will significantly degrade the network's delivery ratio since there are no other copies of the message in the network and no mechanism exists to inform the source in a timely fashion that it should retransmit the dropped message. Hence, storage congestion management mechanisms are required at the receiving nodes and congestion avoidance mechanisms are required at the forwarding nodes. Together, these enable nodes to offer a safe and efficient message custody service. Storage management in opportunistic networks can be modeled as a financial or economic activity; a decision is made autonomously based only on local information since global information is often not available or is out of date because the networks are dynamic. In these economic models, a node storage (or buffer) space can be considered as a renewable resource since it can be reused by releasing messages in the storage.

Congestion occurrence in a custody node is a gradual procedure, and that early detection of congestion can be performed by assessing the node's state. They define three states, namely normal state (NS), congestion adjacent state (CAS) or congestion state (CS). The examination considers the rate at which node storage is used up. When the storage utilization exceeds a predefined level with most of the storage space used and the rate of increase of storage occupancy exceeds some threshold, the node is close to congestion and is defined as CAS. Then, if the storage utilization continues to increase and reaches another level with storage nearly exhausted and the rate of increase of the storage occupancy does not drop below the given threshold for a certain time interval, the node is congested and is marked as state CS. A multiple-copy forwarding strategy typically needs less knowledge of the underlying network than a single-copy strategy; indeed, epidemic routing requires no network topology information. Whilst message replication can be used as a forwarding mechanism to increase message delivery probability, it can easily overwhelm node storage and network capacity, and quickly deplete node energy. Consequently, a replication control strategy is ideally required. On the other hand, message redundancy means that a node can now drop messages from its buffer when congestion occurs without causing loss of the messages from the network, although excessive message drops will significantly reduce network delivery performance.

In the multiple-copy case, therefore, networks need message replication management and message drop policies to deal with node storage congestion. Message replication can improve the average delivery ratio in opportunistic networks, at the cost of worse storage congestion in relay nodes. The second aspect of storage management is that a non-custody node must drop messages as its buffer gets close to full. Consequently, a drop policy is necessary to determine which messages should be discarded so as to have low impact on overall delivery ratio. A drop strategy for opportunistic networks is a complex task since several factors need to be considered to minimize the impact of message deletion on delivery performance. We can categorize drop strategies based on the data required: Single-message statistics: a simple drop strategy that only needs the attributes of a message in the node buffer, such as its forwarding or arrival statistics, or message lifetime. Network-wide message statistics: a complex drop strategy that needs message attributes collected from the entire network, such as the number of copies of a message.

V. CONCLUSION

Transfer reliability and congestion control mechanisms have to be implemented in the network on a per-hop basis, and traditional fixed network functions, such as packet forwarding and dropping and congestion control, become more tightly coupled. The Main Contributions Are 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. This enables readers to have a better understanding of the current state of the evolving research.
The intention is to provide better insight into the importance of transfer reliability and congestion control functions in supporting the message delivery service, whether that be focused on high message delivery ratio or low delivery latency.

VI. REFERENCES

[1] Delay Tolerant Networking Research Group, available online:http://www.dtnrg.org.
[2] Y. Hu, V.O.K. Li, "Satellite-based Internet: a Tutorial", IEEE Commun.Mag., vol. 39, no. 3, pp. 154-162, March 2001.
[3] M. Marchese, M. Rosei, G. Morabito, "PETRA: Performance Enhancing Transport Architecture for Satellite Communications", IEEE J. Sel. Areas Commun., vol. 22, no. 2, pp. 320-332, Feb. 2004.
[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. 9th 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 Ad Hoc Networks", Proc. ACM MOBICOM, Seattle, WA, USA, Aug. 1999.

Author's Profile:

S.S.Rajakumari, She Have Total 10 Years of Teaching Experience Currently She Is Working As Associate Professor In St. John's College of Engineering And Technology. Completed M.Tech Under Jntu Anantapur, A.P, India.

B.Revathi, Completed B.Tech, In Information Technology In G.Pullaiah College Of Engineering & Technology, Kurnool India In 2011, Pursing M. Tech In Computer Science Engineering In St.John's College Of Engineering And Technology Affiliated To Jntu Anantapur, India, Total 2 Years of Teaching Exp.