Transfer Reliability and Congestion Control Strategies in Opportunistic Networks: A Survey

Bambang Soelistijanto and Michael P. Howarth

***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. In addition, opportunistic networks require different approaches to those adopted in the more common intermittently connected networks, e.g. deep space networks. In this article we capture the state of the art of proposals for transfer reliability and storage congestion control strategies in opportunistic networks. We discuss potential mechanisms for transfer reliability service, i.e. hop-by-hop custody transfer and end-to-end return receipt. We also identify the requirements for storage congestion control and categorise these issues based on the number of message copies distributed in the networks. For single-copy forwarding, storage congestion management and congestion avoidance mechanism are discussed. For multiple-copy forwarding, the principal storage congestion control mechanisms are replication management and drop policy. Finally, we identify open research issues in the field where future research could usefully be focused.**

***Index Terms*—MANETs, intermittently connected networks, opportunistic networks, transfer reliability, storage congestion control.**

I. Introduction

MOBILE ad hoc networks (MANETs) are infrastructureless networks where nodes can move freely. One node can directly communicate with another if they are within radio communication range. A node can simultaneously serve both as a source or destination of a message and as a relay for other messages. 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, and an abundance of routing and transport protocols have been proposed. In all these protocols, it is implicitly assumed that the network is continuously connected and that there exists at all times end-to-end paths between all source and destination pairs in the networks. However, 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. These networks may experience frequent partitioning, with the disconnections lasting for long periods. As a consequence, the end-to-end transfer delays in these *intermittently connected networks* (ICNs) are much greater than typical IP data transfer delays in conventional networks such as the Internet. In the literature, intermittently-connected networks are often referred to as *delay-* or *disruption tolerant networks* (DTN); however this term is more strictly associated with the Delay / Disruption Tolerant Networking architecture that is currently the subject of work within the IRTF DTN Research Group (DTNRG) [1].

Whilst research in ICN routing is now well established, research in ICN transfer reliability and congestion control is still in its early stages. So far, most of the work in these areas has been targeted at applications in deep space communications, for example the interplanetary Internet.

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 such as deep space networks.

This article reviews transfer reliability and congestion control strategies in opportunistic networks. We initially consider ICNs in Section II, and review the DTN architecture, ICN routing strategies and transport protocols for ICNs. We then proceed to opportunistic networks in Section III, where we consider how a network's characteristics affect its requirements for transfer reliability and congestion control. We then consider in detail proposals in the literature that address these subjects: in Section IV, we review strategies that have been proposed for message transfer reliability in opportunistic networks, and in Sections V and VI we review proposed strategies in congestion control for opportunistic networks. We categorise them based on the underlying forwarding strategy, i.e. single-copy (Section V) or multiple-copy (Section VI). Future research topics and challenges are discussed in Section VII. Finally, in Section VIII we conclude the article.

II. ICN Overview

ICNs occur in challenged network environments; examples include deep space communications where links have very long delays [2][3], sparse sensor networks where connectivity is frequently intermittent [4], animal wildlife monitoring

Manuscript received May 3, 2012; revised Dec. 12, 2012 and March 25, 2013.

The authors are with the Centre for Communication Systems Research, Department of Electronic Engineering, University of Surrey, Guildford, GU2 7XH, UK (e-mail: {b.soelistijanto, m.howarth}@surrey.ac.uk).

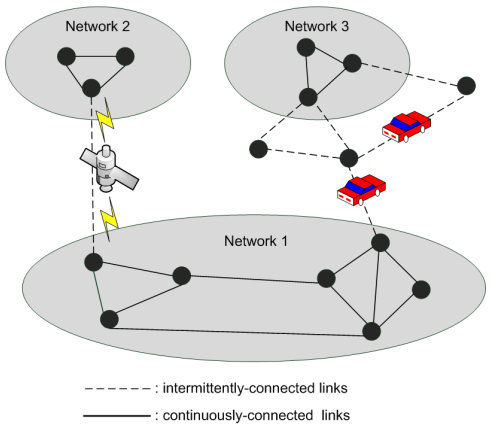

Fig. 1. Intermittently Connected Networks (ICNs).

networks where animal movements are unpredictable, e.g. Zebranet [5], and in human (social) networks where connectivity occurs opportunistically, e.g. pocket-switched networks [6]. In general, ICNs do not satisfy traditional networking assumptions, where end-to-end paths always exist, and the networks have low propagation delays or round-trip times, low bit error rates, and high bandwidth. As a result, communication protocols built for these conventional networks, e.g. the Internet and MANETs, are not able to handle data communication efficiently in ICNs. End-to-end communication using the TCP/IP protocol suite is ineffective against the impairments of ICNs. In the network layer, MANET routing protocols, such as OLSR [7], AODV [8] and DSR [9], will drop packets if the destination cannot be found. In the transport layer, TCP variants for MANETs, such as TCP-EFLN [10], A-TCP [11], TCP Snoop [12] and TCP-BuS [13], will also break down in ICNs: these protocols assume that the network is continuously connected, and they consider link disruptions, due to node mobility or link layer contention, as temporary and short-term events. TCP eventually fails in ICNs, since link disconnections occur frequently and the round trip delays are too long. Hence, new protocols and system architectures need to be developed for ICNs.

A. *Delay-Tolerant Networking (DTN) Architecture*

An example ICN scenario is illustrated in Fig. 1, where three networks, each of which is continuously connected, are linked by intermittent connections, namely a satellite link (between networks 1 and 2) and a vehicular network (between networks 1 and 3). The satellite link is scheduled and predictable, whereas the vehicle-based links are unpredictable and therefore opportunistic. The vehicle contacts, when they occur, might be of long or short duration. ICN nodes (or simply "nodes" in this article) are responsible for managing data transfer between the temporarily disconnected networks. As nodes come into contact, they can transfer data, for example sending and receiving bundles. A bundle is an arbitrary sized data unit and has a time-to-live before bundle expiration; in the literature as well as in this article the term "message" is also used to refer to a "bundle". When a peer node or a link or path is currently not available, a node waits, storing the bundle or

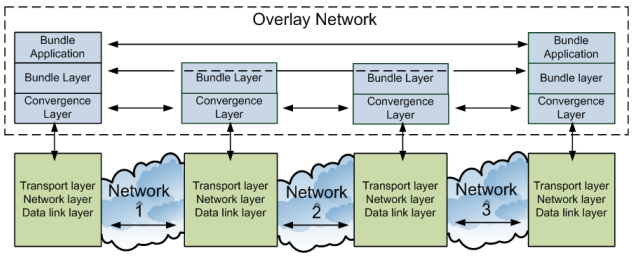

Fig. 2. DTN architecture (from the DTNRG).

forwarding it to another node that may have better a chance of delivering the bundle to its destination. Communications between disconnected areas can be performed by a *store-forward* (SF) mechanism, as in the satellite communications between network 1 and 2 or a *store-carry-forward* (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 known next hop, bundles are stored in a node buffer waiting for the next contact event. In SCF, physical message carriers, such as vehicles, humans or message ferries, are added to carry and forward messages between disconnected areas. For both mechanisms, the probability of node contact, the node contact duration and node resource capacity (e.g. storage and energy) are key attributes for effective data delivery in ICNs.

The architecture for delay and disruption tolerant networking (DTN) (Fig. 2) was developed by the Internet Research Task Force (IRTF) DTN Research Group (DTNRG) [14]. This architecture considers intermittently-connected networks that suffer from frequent partitions and which may consist of more than one protocol family. The basis of the DTN architecture lies in the Interplanetary Internet (IPN), which addresses the main issues of deep space communications, i.e. long delays and high packet losses. However, more generally the DTN architecture can be utilised in various operational environments that are subject to disruption and disconnection. As depicted in Fig. 2, DTNRG defines three layers for DTN communications that sit on top of network-specific layers such as the TCP/IP protocol stack, with these three layers forming an overlay network. The layers are the bundle application layer, bundle layer and convergence layer. An application uses DTN nodes to send and receive ADUs (application data units) by means of the bundle application layer. A bundle application protocol maintains end-to-end communication between the applications in the source and destination nodes. The convergence layer provides a direct mapping between the bundle layer and lower protocol layers, such as the transport layer (e.g. TCP or UDP) or link layer (e.g. Licklider Transmission protocol, LTP [15]). Finally, at the heart of the DTN architecture the bundle layer manages *hop-by-hop* message transfers from source to destination when link disruptions or high delays occur. The DTN architecture defines important data delivery tasks at the bundle layer, such as routing and forwarding, reliability and custody transfer, congestion and flow control, and security [14].

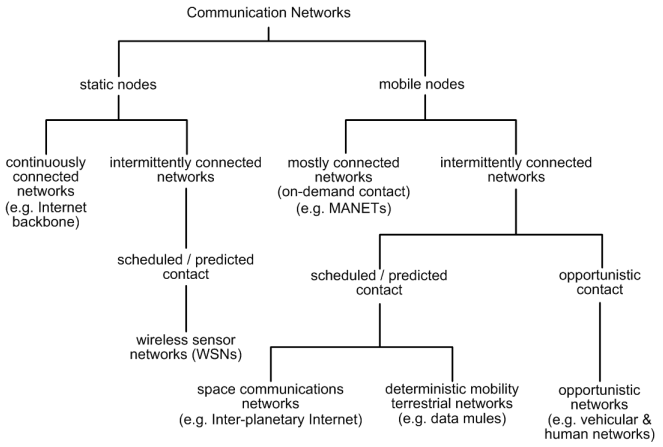

Fig. 3. Taxonomy of communication networks.

B. ICN Routing Strategies

Routing in ICNs is more complicated than in MANETs due to the lack of up-to-date network topology information. Here we briefly review ICN routing strategies since, as we shall see, the routing algorithms affect design decisions about transfer and congestion control mechanisms. ICN routing protocols typically use historical node contact data to predict future network topology. Three categories of regularity of node contacts can be defined, namely *on-demand contact*, *scheduled or predicted contact* and *opportunistic contact*. In Fig. 3, we use these categories in a taxonomy of communication networks. We first divide the networks, based on node mobility, into static and mobile nodes. Static node networks can be either continuously connected (such as the Internet backbone) or intermittently connected. The latter division includes wireless sensor networks (WSNs), whose nodes conserve energy by disabling their radio connection when not required. In the mobile node branch of the taxonomy, we again distinguish between networks where links between nodes generally exist and networks where node contact is intermittent. In MANETs, links are assumed to be always or usually available when needed; this is also known as *on-demand contact*. We use the regularity of node contact to further divide the intermittently connected mobile networks: we distinguish between networks where node contacts are predicted (e.g. the Interplanetary Internet (IPN)) or scheduled (for example, data mules [16]), and networks where node contacts are not generally predictable, such as vehicular networks and human networks. It is this latter category that is commonly called *opportunistic networks*.

In scheduled/predicted contact, future node contacts are known in advance. Two examples of this are a link between an earth station and a satellite where the satellite's view schedule is known in advance, and a link between wireless sensor devices and a data mule, which visits a sensor device at regular times to collect data. In these cases, message transmissions can be scheduled in advance so that optimal delivery performance can be achieved. Deterministic routing protocols, such as Space Time Routing [17], Tree Approach [18] and Modified Shortest Path [19], are able to achieve a high delivery ratio while minimising consumption of node resources, for instance by applying a *single-copy* forwarding strategy. In this strategy, at any instant only one copy of a message is circulating in the network.

In opportunistic meetings, a node knows nothing about future contacts or network topology. In this case a routing strategy can stochastically estimate future node contacts; it can also forward several copies to different nodes to increase delivery probability (a *multiple-copy* forwarding strategy). For example, in epidemic routing [20], a node floods copies of a message to all its neighbours within transmission range so that the copies are quickly distributed throughout the network. As this oblivious forwarding assumes unlimited node resources, it tends to deplete node resources rapidly which in turn significantly degrades the network performance. Alternatively, a routing strategy may use contact history or mobility patterns to calculate the probability of a node being able to deliver a message to the destination. A copy of the message is only forwarded to those nodes that satisfy given routing criteria (this is known as limited epidemic forwarding). A contact history based routing algorithm such as Prophet [21] or MaxProp [22] estimates a delivery predictability based on the previous contact times for each known destination, and estimates the ability of a node to deliver a message to its destination. As a third approach, a social-based routing algorithm, such as SimBet [23] or Bubble Rap [24], uses principles derived from the structure of social networks, and forwards copies of a message to nodes that have a greater volume of contact (a higher popularity or *centrality*) than the current node. For a more detailed discussion of ICN routing protocols, readers are referred to [25][26] and the references therein.

C. Poor Performance of TCP in ICNs

In the OSI reference model [27], flow/congestion control and transfer reliability functions are considered to be part of the transport layer. However, the Internet transport protocol, Transmission Control Protocol (TCP), performs poorly in the presence of the long transfer delays that occur in ICNs. The first problem is TCP's 3-way handshake mechanism, used to open a data transfer connection, which will fail due to the high end-to-end latency. Three messages are required to establish the TCP session between the sender (usually called the client) and the receiver (usually the server) (Fig. 4(a)). However, in ICNs (Fig. 4(b)) the network latency is high, causing TCP's retransmission timer to expire and eventually causing TCP to abort the attempt to open the connection.

The second problem concerns TCP's reliable data transfer. This is implemented by a receiver returning an acknowledgement (Ack) to the source when messages are correctly received. In ICNs that have highly variable network delays, the message round trip time (RTT) cannot be calculated easily or used to set retransmission time-out (RTO) values. The source is therefore unable to detect a lost message promptly; it also has to keep the outstanding unacknowledged messages, potentially for a long time. Also, in order to maintain a reasonable throughput, TCP has to use a large window size; this is feasible for networks with reasonable delays (of the order of seconds) but not if the delay is of the order of hours or days.

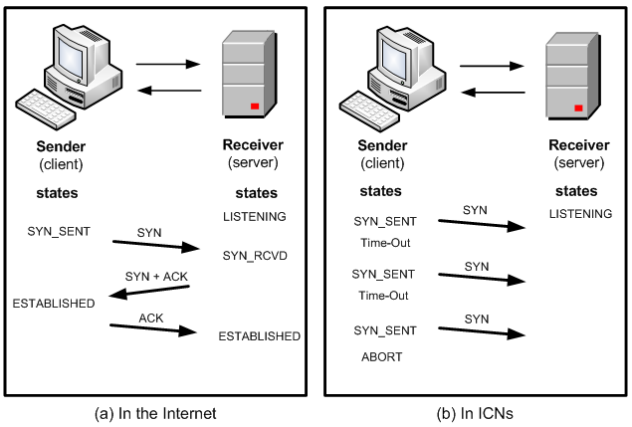

Fig. 4. TCP 3-way handshake.

Finally, TCP has no explicit knowledge of the congestion state in networks. Instead, it implicitly couples the end-to-end transfer reliability and congestion control mechanisms through its acknowledgments. If the source receives three duplicate Acks, or if TCP's retransmission timer expires, it assumes traffic congestion has occurred and it reduces the sending rate to limit the network congestion. This behaviour does not work effectively in ICNs, which have frequent link disruptions and long transfer delays: an acknowledgement received by the source does not reflect the recent condition of the network and hence the source cannot respond to congestion accurately.

Modified versions of TCP have been proposed for MANETs, for example TCP-EFLN [10], A-TCP [11] and TCP Snoop [12]. They are designed particularly to deal with wireless link disconnections due to node mobility or link layer contention, and assume that link disruptions are short-term events. During a link breakage, these TCP variants typically enter a standby state, freezing their parameters such as the congestion window and retransmission time-out values. When the link is re-established, TCP unfreezes the parameters and resumes the data transfer. In ICNs, however, where the link breaks may last for hours or days, the frozen TCP parameters are likely to be invalid for the resumed connections.

In TCP, congestion control relies on packet drop events which are signalled to the source through TCP's acknowledgement mechanism, providing end-to-end, closed-loop congestion control. In contrast, congestion control in ICNs cannot rely on end-to-end acknowledgements, and nodes have to use locally available information when determining the network's congestion level (i.e. distributed, open-loop congestion control). When we specifically consider opportunistic networks, their unpredictable contacts mean that the mechanisms used to implement transfer reliability and congestion control strategies differ from those of scheduled contact ICNs, such as deep space communication networks. The most important characteristics of deep space networks, such as the interplanetary Internet, are very long propagation delays, high link error rates, blackouts and bandwidth asymmetry [28]. Among these, the dominant factor that degrades TCP performance in deep-space communication is the extremely long propagation delay [29]. Several TCP-based transport protocols have been developed for space-based communication networks, such as SCPS-TP [30], TP-Planet [28], and Saratoga [31]. These protocols are mainly designed to overcome the problems of very long round trip time (RTT) and low channel efficiency due to the use of TCP's window-based mechanism. A comprehensive survey of protocols for reliable data transport in the deep-space Internet can be found in [32].

III. Transfer 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 within range, rather than being caused by long propagation delays. Grossglauser and Tse [33] argue that a node can exploit its mobility to physically carry messages between disconnected parts of the network (a store-carry-forward (SCF) delivery mechanism) to achieve eventual delivery and to increase overall network capacity. We thus see that in SCF networks the challenges and requirements in designing transfer reliability and congestion control differ from those in store-forward (SF) networks, such as deep space networks. We identify the requirements of an opportunistic network SCF delivery mechanism as follows:

- **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 neighbour, stores it in memory, performs a routing table lookup and forwards the message to the next hop when contact occurs.
- **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.
- **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 prioritise, select and forward messages that are to be transferred to a next hop node during the limited contact event.

We now describe a basic opportunistic network scenario and show how the transfer reliability and congestion control functions may interact. We consider the simple custody transfer scenario shown in Fig. 5. A message destined for node D currently resides in the persistent storage of node S (Fig. 5(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. 5(b)). S then requests a custody transfer

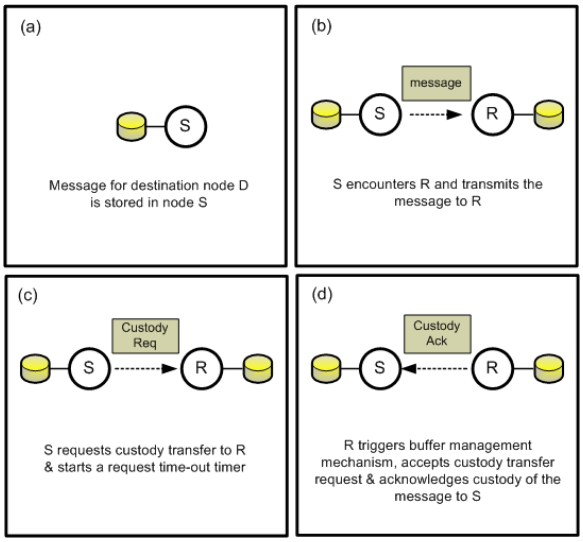

Fig. 5. Interaction of transfer reliability and congestion control strategies in opportunistic networks.

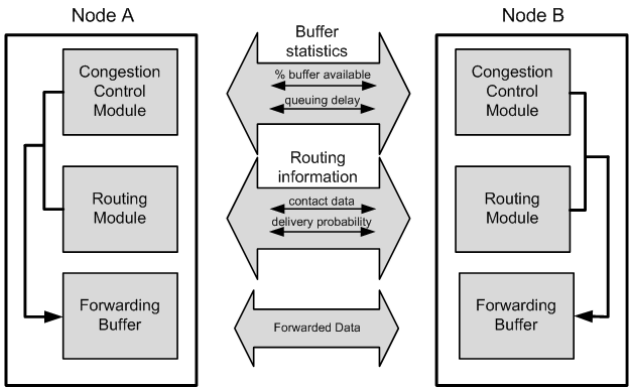

Fig. 6. Congestion-aware forwarding module in opportunistic network nodes [46].

service for the message to R and starts a request time-out timer (Fig. 5(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. 5(d)).

In order to optimise 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 in Fig. 5 we can summarise 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 *per-hop basis*, based on locally available information and should be *autonomous* for every node.

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. In the remainder of this article, we will use the term "congestion" to refer to the "storage or buffer congestion" that more frequently occurs in opportunistic networks, given the (mobile) nodes' limited storage capacity.

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*. In the fixed Internet, packet dropping is typically performed in the network's relay nodes, i.e. at IP routers. However, when an IP router drops messages during traffic congestion, it does not consider the overall delivery performance in the network. Instead, the end-to-end TCP mechanism ensures delivery, by requesting the source to retransmit the dropped messages. In opportunistic networks, as we noted above, 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 the 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 signalled by TCP's acknowledgment mechanism. However, as we have noted 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. In Fig. 6, 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. 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 neighbour during contact if the neighbour meets the routing criteria and if the forwarded messages are unlikely

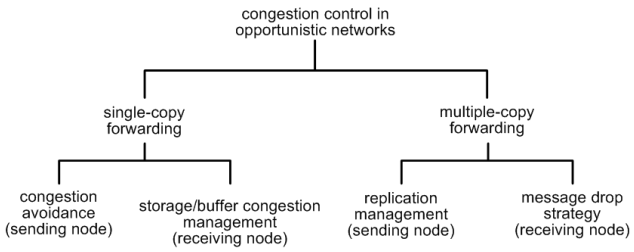

Fig. 7. Congestion control strategies for opportunistic networks.

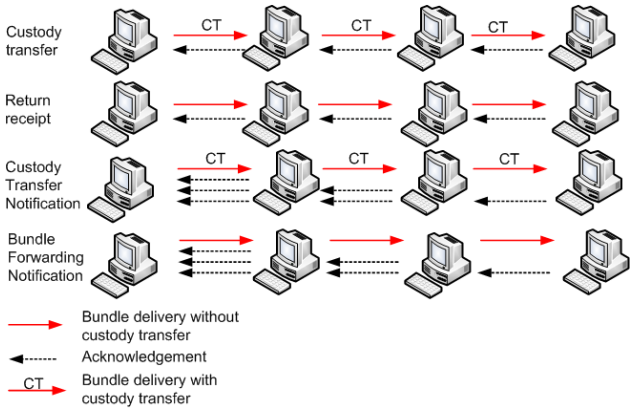

Fig. 8. ICN reliable message transfer services [34].

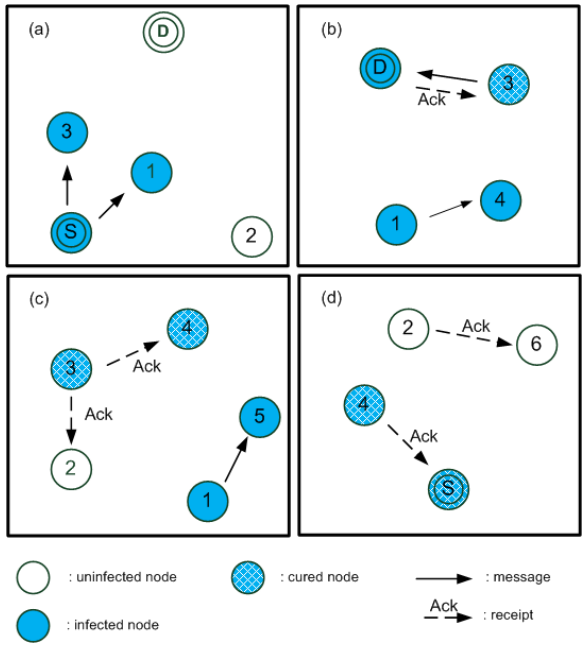

Fig. 9. Active-receipt reliability strategy.

to create congestion in the receiving neighbour'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.

To summarise our discussion of congestion control, Fig. 7 illustrates a taxonomy of strategies for opportunistic networks.

IV. Reliable Message Transfer

As we described in Section II.C, TCP is not able to provide efficient reliable end-to-end message transfer in ICNs. Other approaches have therefore been proposed. 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. 8). Of these, we consider that 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. 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 [35] 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 minimising 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. In this scheme (Fig. 9), nodes treat a receipt as a new message that needs to be forwarded to all other nodes at every contact. In Fig. 9(a) the source S passes the message to node 1 and 3; in Fig. 9(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. 9(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). 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 (in Fig. 9(d), 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.

V. Congestion Control (Single-Copy Case)

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. We now discuss storage congestion management and congestion avoidance approaches described in the literature. Existing storage congestion management proposals can be divided into two categories: those that use economic models to determine whether custody of a message should be transferred to a new node, and those that analyse network traffic levels to make this decision.

A. Storage Congestion Management - Economic Models

Mobile nodes in opportunistic networks usually have limited resource capacity, including in particular limited node storage. An individual node must therefore be careful when agreeing to accept a custody request for a message. Storage management in opportunistic networks can be modelled 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. We now briefly describe some of these economic models.

Fall *et al.* [36] argue that a decision to accept a message mimics a decision to purchase a perishable commodity. Here, the size of a message and the expected time to forward the message correspond to price and liquidity, respectively. The storage management algorithm should prefer a small, fast-released message, because this incurs a lower cost in term of storage space (low price) and a message that is forwarded quickly will free up storage space rapidly (or in financial terms, the message is highly liquid). Other factors, such as routing strategy, message priority, message lifetime and security, are also important considerations in the custody acceptance decision. To maximise the node resource utility and network delivery performance, a mathematical equilibrium theory, such as game theory [37], may also be applied.

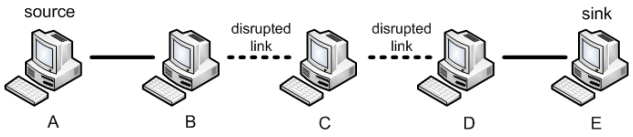

Fig. 10. Five-node line topology (Burleigh & Jennings) [38].

Burleigh and Jennings [38] proposed a custody acceptance decision algorithm based on a financial model. In the model, a sender pays a transport fee (which is a function of message size and requested quality of service) to get its message delivered, while relay nodes receive a commission for completing a single-hop delivery of a message. The relay's incentive is to accept the largest possible message and to forward it as quickly as possible. However, a large remaining lifetime is a disincentive for the relays to accept custody of a message, because the message may occupy buffer space for a long time. The congestion control algorithm in a receiving node uses the message's remaining lifetime and the node's queue growth rate as the main factors in deciding whether to accept a new message. A node will accept a new message if the message size is less than the free space of the node buffer and the potential risk of accepting the message is acceptable, where the risk is determined by considering both the projected buffer queue growth rate and the message's remaining lifetime. If the calculated risk of the message exceeds the mean risk of all messages currently in the buffer, the node will refuse to accept it.

In simulations, the authors used a linear five-node topology (Fig. 10) with the source sending messages at a constant transfer rate via the three intermediate (relay) nodes. By artificially imposing congestion, e.g. by randomly creating link disruptions over the multi-hop connections, the study showed that using local information to make decisions about custody transfer gave a high throughput. However, this static scenario may not properly represent message transfers in opportunistic networks where the network topology frequently changes due to node mobility. We believe that integrating the routing strategy with the congestion control algorithm would increase delivery performance in opportunistic networks. For instance, the risk of receiving a new message would depend not only on the message's size and its remaining lifetime, but also on the message destination. The more popular the message destination is, the lower the risk will be, as it is more probable that the message will be further forwarded within a short time, releasing storage space quickly.

Zhang and Liu [39] proposed dynamic opportunity cost as a mechanism for developing a storage congestion management strategy in intermittently connected networks. The algorithm applies the concepts of revenue management and dynamic programming to optimise the overall revenue by accepting

custody transfer of a message and forwarding the message under the assumption of minimally cooperative (non-rational) node behaviour. The algorithm aims to balance two conflicting demands, namely opportunity cost and benefit function, in order to maximise the benefit of accepting custody of a message. The opportunity cost is the value of the storage capacity that is consumed and therefore lost to a potentially higher benefit request as a result of consumption of the storage resource by the message. The benefit function, on the other hand, denotes the gain of forwarding a message to the next hop and can be defined in a number of ways, for example as a function of message size or message type. The dynamic resource management algorithm attempts to achieve the optimal benefit of accepting a custody request by maximising the difference between the benefit and the opportunity cost at any remaining storage capacity.

The authors' simulation results show that the dynamic resource management strategy can outperform a static-policy strategy (i.e. when the opportunity cost is set constant) in terms of load distribution and node utilisation. However, their simulation assumes the existence of an "oracle" that knows the entire network topology and which can distribute routing information to all nodes in the network. In practice, however, this assumption is unlikely to hold in an opportunistic network. As a result, determining opportunity cost and benefit function are nontrivial tasks since these functions include stochastic metrics; for example the opportunity cost should ideally take account of the time that the message spends in the node before being forwarded, and this queuing time depends on the message destination's popularity. Again, this suggests that congestion management would be improved by including routing information in the economic models.

B. Storage Congestion Management - Traffic Distribution

In one specific opportunistic network scenario, namely social (human-to-human) opportunistic networks, unfair traffic distribution among nodes has emerged as a key problem. Social opportunistic networks are intermittently connected networks that exploit human mobility to enable opportunistic contact between the devices carried by their users. This human movement behaviour is triggered by individuals' social activity and is commonly described in social (relation) networks. A discussion of social networks requires an understanding of a number of concepts, which we now briefly define:

- **Centrality**: a general measure of the importance of a node or individual in a social network. A more important node or individual has a higher centrality.
- **Degree centrality** of a node: the number of links or immediate neighbours the node has.
- **Betweeness centrality** of a node or link: the number of shortest paths between all pairs of nodes in the network that pass through the given node or link, divided by the total number of shortest paths in the network.
- **Ego network**: the part of a network that is composed of a node and its immediate neighbours (see Fig. 11). In an opportunistic network, "neighbours" means those nodes with which a node has recently been in contact.

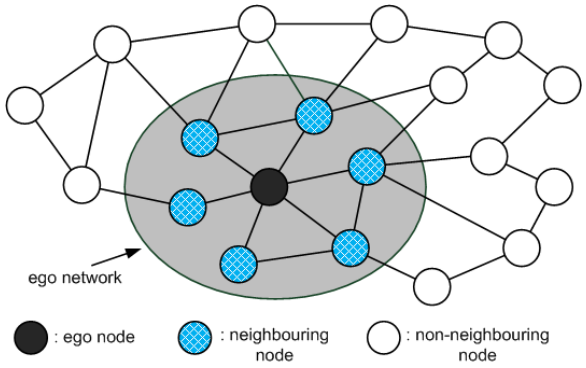

Fig. 11. An ego network.

- **Ego betweeness centrality**: the betweeness centrality of a node's ego network.

As an example, in Fig. 11, the shaded ego network comprises 7 nodes. Of the 21 (=7x6/2) shortest paths between these nodes, 18 pass through the black ego node and three paths do not. The black ego node therefore has an ego betweeness centrality of $18/21 \approx 0.86$.

Hossmann *et al.* [40] showed that social networks have a non-random structure, where a few nodes act as communication hubs in the network, carrying a high proportion of total network traffic. These hub nodes (i.e. the most important individuals, or those with the highest centrality) have many more relations with other nodes in the network and hence are much more popular in the society. Social-based routing protocols, such as SimBet [23] and Bubble Rap [24], which use structural properties of individuals in social networks as routing metrics, favour these hub nodes as better relays for message transfers. As a result, these nodes, which only constitute a small part of the network, will be heavily loaded with messages. For instance, for SimBet the top 10% of nodes perform 54% of all deliveries (to end destinations) and 85% of all handovers (to other relay nodes) [41]. For Bubble Rap, Fig. 12 clearly shows that unfair traffic distribution also exists in real social opportunistic networks, namely the Reality [42] and Cambridge [43] experimental human networks; in each network a small number of nodes are carrying a much higher level of traffic than all the other nodes. The unfair traffic distribution can quickly deplete the central hub nodes' resources, especially node storage, causing traffic congestion and eventually reducing the overall delivery ratio. It could be argued that unfair traffic distribution is a network load balancing issue that typically happens in the Internet. However, we agree with Khabbaz *et al.* [44] and Kathiravelu *et al.* [45] who both refer to it as a congestion problem, since the central nodes are the best forwarders and are therefore always receiving messages, resulting in storage congestion. Storage space can be managed by ensuring that sending nodes refrain from forwarding messages to congestion-prone nodes, such as central (or hub) nodes, and in the following we discuss some proposals described in the literature.

Congestion Aware Forwarding (CAFé) [46] aims to distribute load away from hub nodes. We illustrated the algorithm in outline form in Fig. 6: it consists of two main modules, i.e.

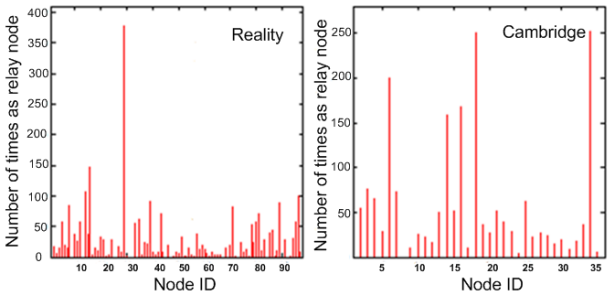

Fig. 12. Traffic distribution in social opportunistic networks [24].

routing and congestion control, that work together to make a single-hop forwarding decision for a message. In the routing module, CAFé applies the social-based routing algorithm, SimBet [23], using a social metric (ego betweeness centrality) to identify better relay nodes that can deliver messages to the destinations faster; a node with a high betweeness centrality lies on the shortest path between many nodes in the network, and is therefore more likely to be able to deliver a message to its destination rapidly. In an ideal network, the node betweeness centrality (based on the entire network) would be used to identify the better relay nodes; however, the calculation of node betweeness centrality requires complete network information, which is not normally available in an opportunistic network, and so both SimBet and CAFé calculate an approximation to the betweeness centrality using an ego network [47], which, as defined earlier, is the sub-network comprising the local or recent neighbours of the node in question (Fig. 11).

In CAFé's congestion control module, node buffer statistics (average buffer free space, average buffer queuing delay and buffer congestion rate) are used to estimate a node's ability both to retain a message (what the authors call node "retentiveness") and to receive and forward it later (node "receptiveness"). To improve congestion detection the algorithm also considers local congestion information supplied by neighbouring nodes. Ideally, a node's congestion control strategy requires congestion information from all nodes in the network, but again this is not normally available in opportunistic networks. Instead, CAFé uses congestion statistics based on its ego network to estimate the network's congestion level. The congestion control algorithm allows a node to forward its messages to a node that might for example have worse buffer congestion state than the current node, but which has a better chance of meeting the nodes that have a lower buffer congestion level.

Since CAFé uses buffer statistics collected from nodes in the ego-network to calculate the node's local congestion level, we see an opportunity to improve the algorithm, by considering the structural properties of the neighbouring nodes in the network. Since an ego network is the first-order neighbourhood of a node (the ego), it only considers direct neighbours, and disregards the neighbours of the ego's neighbours. In highly clustered networks such as social networks, a node (or individual) that has neighbouring nodes with high centralities tends itself to be more central as well [48], and therefore it is more likely to receive more traffic. By considering neighbours' centralities, a node can improve the CAFé local congestion calculation. Moreover, our work in [49] shows that the use of ego betweeness centrality as a routing metric results in poor traffic distribution in social opportunistic networks. Instead, a different local metric, degree centrality, can give a better traffic distribution than ego betweeness centrality.

Fair Route [41], like CAFé, is a proposal that addresses the unfair load distribution in social opportunistic networks. This forwarding strategy also relies on both routing and congestion control modules to make a forwarding decision during node contact. The routing module uses the perceived level of interaction with neighbour nodes to make routing decisions. This interaction level, or *tie strength*, represents the probability of a future contact between a pair of nodes. The tie strength increases with node contact events, but decreases exponentially over time. To achieve a balanced traffic distribution, node buffer statistics are also considered in the forwarding strategy. The congestion control module only considers the buffer queue length. The algorithm applies an *assortative* based queue control, where nodes will only accept a forwarding request from other nodes of equal or higher "status" (the term assortative is borrowed from sociology where people with similar social status tend to interact together, but disregard interactions with individuals of lower status). Here, node status is defined by the size of the node's queue length, with a longer queue length being a higher status. Thus, in Fair Route higher status nodes (nodes with longer buffer queue length) will be able to forward their messages faster, while lower status nodes will have to find alternative paths. As social opportunistic networks typically show a diversity of delivery paths between any two end nodes [50], the authors then claim that the assortative-based congestion control does not necessarily imply a reduction of overall throughput, and that it has a positive impact on traffic distribution fairness in the network.

Kathiravelu *et al.* introduced the Adaptive Routing protocol [51], which relies on a predictability metric that measures the degree of connectivity between a node and its neighbour. This favours more popular nodes (i.e. those having better connectivity) as relay nodes to increase the delivery likelihood of a message. However, since this strategy increases congestion in the most connected nodes, the authors later proposed their Congestion Aware Adaptive (CAA) algorithm [45] to address the Adaptive Routing algorithm's drawback. The CAA algorithm improves a "naive" congestion control approach in which a node simply advertises its buffer free space to other nodes. Instead, each node initially performs a self assessment of its connectivity to its neighbours (a routing task) and then calculates a safety margin for its buffer according to its popularity level (a congestion control task). The buffer safety margin rises and falls with the increase or decrease respectively of the node's popularity level. In addition, the CAA algorithm favours receiving messages destined for the more popular nodes to reduce queue waiting time, hence reducing the probability of buffer congestion. At each node contact, the nodes exchange their storage availability information, i.e. buffer free space and threshold, as well as a list of nodes with the highest delivery predictability. A sending

node is then allowed to forward a message to its contact node only if the message size satisfies the receiver's allowed buffer margin and the destination is in the receiver's list of nodes with high delivery probability. However, despite its simplicity we still see a potential drawback of the algorithm especially in large scale networks. Since, the algorithm requires every node to maintain a node predictability table, this table will grow linearly with the increasing number of nodes in the network, with a consequent scalability issue in large networks.

C. Congestion Avoidance

Hua *et al.* [52] argue that 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 utilisation 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 utilisation 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. During node contacts, the node state is broadcast to all neighbours during opportunistic contacts, notifying them of the node's congestion status. When a node enters CAS, the neighbours mark the link to the node as partially congested, meaning that any paths that include the link should be avoided unless no other link is available. On the other hand, when a node is congested and in CS, the neighbours cannot choose a link to the node irrespective of network condition. Thus, the path avoidance algorithm refrains from forwarding a message to a node that is close to congestion or is actually congested. We can see that the effectiveness of the algorithm relies on how far the node congestion information can be broadcast. Ideally, the farther the information is propagated, the better the algorithm performs since k-hop neighbouring nodes can redirect their traffic away from the congested node (Fig. 13). However, as the broadcasting of information will be delayed in intermittently-connected networks, neighbours further away from the congested node may receive out-of-date node state information, leading them to choose inappropriate paths to message destinations. The trade-off between information broadcast range and overall delivery performance plays an important role in the algorithm and needs to be further investigated.

Token Based Congestion Control (TBCC) [53] 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. The algorithm is similar to Token Ring/Bus in that a node must possess a token to transmit data, but differs in that it only needs a token to inject a *new* message into the network. The algorithm views the network as a black box and the cost for a node to inject a single message into the black box is a single token (assuming a constant message length). A token can be reclaimed when a message leaves the network, i.e. when a message arrives at the destination or when the message's lifetime expires. TBCC furthermore assumes all nodes in the network cooperate in forwarding messages and are entitled to share available tokens equally. Tokens are initially evenly distributed among nodes in the network. When a source node wants to forward a message to a relay node, it initially checks its own token availability, transmits the message if its token count is greater than zero, and decrements its token count after successfully transmitting the message. If the token count is zero, the source node can query the peer node, asking for an extra token. Message transmission between relay nodes does not incur any token reduction, since tokens are only used when a message is initially injected into the network by the source. The authors' experiments assumed a constant number of nodes and tokens, which represent the total network capacity, and showed that the algorithm was able to manage message delivery and minimise node storage congestion probability. Despite the algorithm's simplicity, we consider that in practice the assumption is unrealistic in open networks, e.g. social opportunistic networks, since mobile users can autonomously join and leave the network at any time. Calculating the network capacity that corresponds to the number of tokens provided in the network is a challenging task if the number of active nodes in the network varies with time.

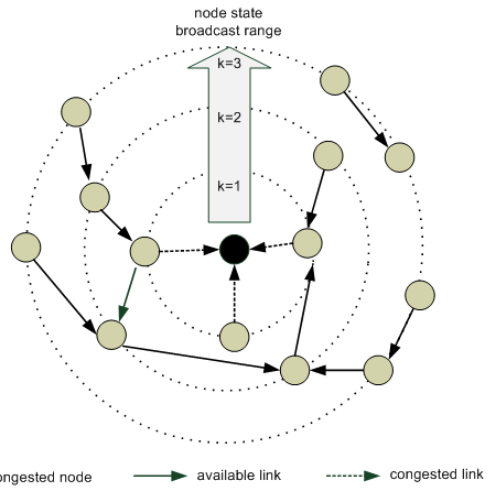

Fig. 13. Path avoidance among k-hop neighbouring nodes.

VI. Congestion Control (Multiple-Copy Case)

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, and in the following we discuss existing proposals for both of these.

A. Replication Management

It is known that message replication can improve the average delivery ratio in opportunistic networks, at the cost of worse storage congestion in relay nodes. Some routing protocols attempt to reduce congestion by capping message replication at a maximum level, for example Spray-Wait [54] and Encounter Based Routing [55]. However, due to the dynamic nature of opportunistic networks, it is difficult to determine the correct number of message copies to achieve optimum delivery performance. Other routing protocols limit message replication by setting a specific forwarding policy, for instance by evaluating node delivery probability based on contact history, as in Prophet [21] and MaxProp [22]. Nonetheless, in these protocols if a message in a node's buffer meets the replication criteria during a node contact, the protocol will continue to replicate the message regardless of the network congestion state. Dynamic replication control is therefore needed to adaptively adjust the message replication rate to the network congestion level.

Retiring Replicant [56] employs dynamic message replication to control the replication rate according to the network congestion level. An ideal congestion control scheme would monitor the entire network to learn the current network congestion level and feed this information back to all nodes in the network in a timely manner. Since this scheme is impractical in opportunistic networks, the authors of [56] developed a mathematical model of the spread of a single message throughout the network in order to find suitable local metrics that act as a proxy measure for the network-wide congestion level. Their mathematical model suggested that the ratio of either the message drop rate or the buffer occupancy rate to either the rate of receiving end-to-end acknowledgements or the rate of receiving messages from the neighbours should give a good indication of the network congestion level. In fact, the authors' simulation results showed that node buffer occupancy is generally high even at low congestion levels and that the spread of acknowledgements is unreliable and delayed in opportunistic networks. The authors therefore concluded that the best local metric that represented the network-wide congestion level was the ratio of message drop rate to the rate of receiving messages at a single node. During node contact, nodes exchange their current congestion information and independently calculate their estimates of the current local congestion level. Each node updates its local congestion estimate as it comes into contact with other nodes and adjusts its replication limit accordingly. The replication threshold increases gradually when the congestion level decreases, but is reduced multiplicatively when the congestion level increases, thus mimicking TCP's AIMD (additive increase multiplicative decrease) behaviour. However, we note that a message drop is not always due to storage congestion: the node inter-contact time can be very long in opportunistic networks, and messages are removed from the buffer when their lifetime expires, so the message drop rate might not accurately measure the node congestion level. It is therefore necessary to select the message lifetime carefully: a shorter lifetime will give a higher message drop rate even when the buffer is not congested, thus giving false information to the algorithm.

Another proposal that uses replication management is Round Robin Forward Scheduling (RRFS) [57]. Generally, a forwarding strategy follows the routing policy to determine the transmission order of messages queued in the buffer. Since the goal of most routing algorithms in opportunistic networks is to achieve a high delivery ratio, the algorithm will prioritise forwarding of messages based on criteria such as message delivery probability, message service class or message lifetime. The RRFS algorithm instead aims to avoid messages at the front of the queue being excessively replicated, by prioritising messages according to the number of message copies already distributed in the network. Each message keeps an estimate of the total number of copies in the network. This estimate is stored in the message header and is incremented whenever the message is replicated during node contact. For instance, suppose that a counter $n_{relay}(m)$ represents the estimated number of relay nodes that hold copies of message m. During node contact, if the messages in the buffer meet the routing criteria they are put in the node's forwarding queue. The algorithm sorts them in ascending order of $n_{relay}(.)$ and the replication and forwarding mechanism processes the messages in this order, i.e. starting with the message with the lowest value of $n_{relay}(.)$. This strategy effectively controls the number of copies of a message where there is limited contact time, and hence reduces network congestion.

CAFRep [58] is a multiple-copy variant of CAFé [46] that controls the number of copies of messages forwarded to relay nodes. As with CAFé, CAFRep also considers three types of metrics: node social-network metrics, node buffer statistics and ego network statistics. A CAFRep node calculates its total node utility ($TotUtil$) as the sum of its own metrics, thus capturing the node's own delivery capability. During node contact, a node compares its total utility with that of the contact peer to choose the next hop node as well as to decide the number of messages to be copied to the node. For example, suppose that node x is in contact with node y; then the number of (copy) messages that x will send to y, given that x has N messages in the buffer, is

$$Repl\_rate(x) = N\frac{TotUtil(y)}{TotUtil(x)+TotUtil(y)}$$

Since the total node utility varies with time, the replication rate adaptively changes with the available resources both of the current node and of the nodes in its ego network (Fig. 12), and CAFRep enables message replication at different rates in different nodes and parts of the network. CAFRep is therefore designed to reduce congestion probability in the more popular (hub) nodes that generally exist in social networks, by combining the routing metrics and the congestion control metrics. The algorithm's advantages, disadvantages and potential areas for improvement are therefore similar to those of CAFé.

B. Message Drop Strategy

Storage management needs to include a handling strategy when node storage fills up. In a multiple-copy network, messages are generally not removed from the current node's buffer once a copy has been forwarded to another node, so that the original message can be further replicated in future node contacts. Fig. 9 suggests that an end-to-end receipt can flush an acknowledged message from the buffer of the source and any relay nodes that transfer the acknowledgement. However, obsolete message copies may still reside in the buffers of nodes that do not receive the receipt. Thus, 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. Unfortunately, it was shown in [59] that the simple drop-tail policy commonly used in the Internet's routers performs poorly in opportunistic networks. A drop strategy for opportunistic networks is a complex task since several factors need to be considered to minimise the impact of message deletion on delivery performance. We can categorise 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.

We initially consider drop strategies that use single message statistics. Lindgren and Phanse [60] and Erramili and Crovella [61] studied some simple drop policies in opportunistic networks, such as FIFO (first in first out), MOFO (drop most forwarded first), MOPR (drop most favourable forwarded first), SHLI (drop shortest lifetime first) and LEPR (drop least probable first). They evaluated the policies' performance in terms of network delivery ratio and delivery delay. Similarly, Bjurefors *et al.* [62] conducted work on a data-centric opportunistic network architecture based on a publish/subscribe model, and investigated several drop strategies that can be classified as follows:

- **Degree of interest based**:
  1) LI (least-interested): drop the data object that the fewest number of neighbours are interested in. This strategy has two effects: (i) it reduces the diversity of content in the network; on the other hand (ii) it increases the overall delivery ratio of other objects since the overall interest matching increases.
  2) MI (most-interested): drop the data objects that most neighbours are interested in. Compared to the LI strategy, this will keep object diversity in the network high, but at the expense of a lower delivery ratio, since it will reduce the number of copies of the most popular objects.
- **Degree of replication based**:
  1) MAX (max-copies): drop a data object after a maximum number of copies have been made at a node.
  2) MF (most-forwarded): drop the data object with the highest number of replications.
  3) LF (least-forwarded): drop the data object with the lowest number of replications.

Drop strategies that consider network-wide message statistics have also been investigated. Yun *et al.* [63] proposed AFNER (Average Forwarding Number based on Epidemic Routing) as a drop strategy in opportunistic networks that use epidemic routing. The algorithm works when a node's storage is full and the node needs to accept another incoming message. The node randomly drops a message from those whose forwarding number is larger than the network's average forwarding number. The forwarding number of a message is defined as the number of copies that have been made of a message, and the average forwarding number is the mean forwarding number of all the messages currently in the network. The authors' simulation calculated the average forwarding number, but this cannot readily be done in a real opportunistic network. In practice, only local information is available for a node, although it does not appear to have been shown that the local metric is a good estimate of the global metric. The authors did not discuss how to calculate a local estimate of the global average forwarding number, and further work would be required to establish this.

Krifa *et al.* [59] developed a theoretical framework based on epidemic routing, and proposed two variants of an optimal buffer management drop policy strategy. The first variant, Global Knowledge Based Scheduling and Drop (GBSD), uses global network information to derive a message utility. The utility captures the marginal value of a given message copy with respect to a chosen optimisation metric. The authors consider two performance metrics, namely delivery ratio and average delay. Using the calculated message utility, two functions are performed in a node: forwarding scheduling and message dropping. In forwarding scheduling, a node replicates and forwards messages in decreasing order of their utilities, thus prioritising the messages when there is limited node contact time. For the message dropping, when a node exhausts the available storage space it first drops the message with the smallest utility. The calculation of the message utility in GBSD requires global information concerning the distribution of a message, such as the number of nodes that have seen the message, the number of copies of the message and the number of different messages, and hence it is impractical in a real implementation. The authors therefore consider a variant that employs a distributed (local) algorithm based on statistical learning from the network history to estimate current network global statistics. This algorithm, History Based Scheduling and Drop (HBSD), uses the same algorithm as GBSD to calculate message utility, but uses local estimators for global metrics. In HBSD, the global attributes of a message are estimated by using the average value of the attribute for all messages that have formerly resided in the node buffer. By substituting the estimators into GBSD's delivery ratio and delay message utility calculations, the new per-message utility can be used without any need for global metrics.

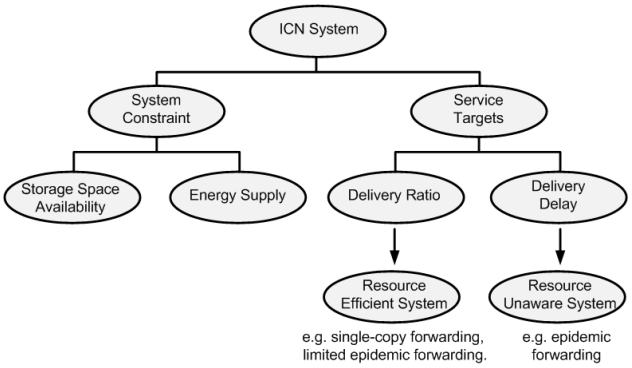

Fig. 14. ICN service targets and system constraints [65].

VII. Discussion and Future Research Issues

We have reviewed and discussed proposals for transfer reliability and storage congestion control in opportunistic networks in Section IV, V and VI, and we provide a summary of the congestion control strategies in Table I. This table includes the service target of each strategy, giving the principal delivery objective as either maximum delivery ratio or minimum delivery delay or both. The authors of some papers clearly state the service target of their proposal, whereas other authors use the delivery ratio and/or delivery delay as metric(s) to measure the proposal's performance in computer simulations or mathematical models.

Psaras *et al.* [64] contend that there are two ultimate goals, and therefore service targets, of ICN protocols, namely a high delivery ratio and a low delivery delay. Given that nodes in ICNs are generally battery-powered mobile devices, the service targets will be constrained by the nodes' resources, such as their energy supply and message storage space. Even though delivery delay may seem counterintuitive as a service target in ICNs, in fact some applications can tolerate different delivery delays. For instance, while email applications require 100% delivery ratio but can tolerate a high delay, "web-on-the-move" applications (e.g. in [65]) and telemetry data (e.g. in [66]) become useless if the data is not delivered in a timely fashion. Now, to achieve a high delivery ratio the system has to be energy efficient, and one way to achieve this is by limiting the number of message copies. Conversely, to achieve low delivery delay, the network has to accept a degree of risk by distributing message copies to a relatively large number of neighbouring nodes in the expectation that at least one of them will find the fastest path and reach the message's destination within the deadline. There are thus tradeoffs in the design of these protocols. These system constraints and service targets are illustrated in Fig. 14.

Given the unique characteristics of opportunistic networks, it is clear from the published literature that many research issues remain to be resolved. We now discuss some of these research issues in the areas of transfer reliability and congestion control for data delivery in opportunistic networks.

1) **Interaction of routing and congestion control in message forwarding**: routing is the process of collecting information about the network and determining the best paths to various destinations, whereas forwarding is the task of using a packet's destination address to select the best next-hop node [67]. In opportunistic networks, the distinction between routing and forwarding becomes even more explicit: as shown in Fig. 6, forwarding decisions now rely not only on routing decisions, but also on storage congestion control considerations. In their survey of ICN routing protocols, Cao and Sun [26] included congestion control as a routing technique in their taxonomy and considered congestion control utilities as routing metrics. In contrast, we consider that congestion control should be regarded as a complementary component of the overall routing strategy in opportunistic networks. Both components share the same challenge in opportunistic networks, namely incomplete network information, with each node only having local information available. As examples, in the routing component the authors of [23][24] investigated local routing metrics to identify the best relay nodes; in the congestion control component the authors of [56][64] examined local congestion metrics as a proxy for the global congestion level. Researchers need to consider how congestion can best be locally measured and then how it can most effectively be taken into account by the routing algorithms. A further question is how the two components are implemented: for example, is it better to bind together congestion control and routing in a single protocol; or should the two algorithms be decoupled so that any congestion control algorithm could interwork with any routing algorithm.

2) **Interaction of network conditions and message generation rate**: congestion occurs when there is a large number of messages in a node's buffer, and therefore congestion control is needed to manage a node's incoming traffic so that messages do not overwhelm the node's storage [38][39][46]. It has been shown [49] that when the message generation rate in a node exceeds the network's capacity to deliver messages over a certain interval time, the network state changes to one of congestion. Yet there is currently no mechanism in opportunistic networks to control the message generation rate at a node and thereby reduce network congestion. Such a mechanism would be an ICN / opportunistic network analogue of TCP's congestion avoidance mechanism used in conventional networks. This feedback mechanism could take account of two sources of information in an opportunistic network: (a) feedback to the source of network conditions encountered by transmitted messages (this is like TCP in conventional networks); and (b) the network conditions encountered by traffic that transits through the node (since an ad hoc network is one whose nodes constitute their own routing infrastructure). The problem is complicated in ICNs and opportunistic networks because of the long network delays, and the incomplete knowledge of network state.

3) **Impact of hub nodes on network performance**: Many opportunistic network protocols have been developed under the assumption that all nodes have a uniform probability of meeting all other nodes in the network (i.e. a uniform, random geographical node distribution), for example [53][54][57]. However, as we have seen, opportunistic networks often have highly connected hub nodes that play an important part in routing, and many algorithms [23][24] tend to route messages through these hub nodes because they provide low-delay paths. This therefore results in a highly uneven traffic distribution and increases congestion in parts of the network. A number of algorithms have been developed that distribute traffic away from these hub nodes, for example [41][46]. Further work is however needed on congestion control strategies that are more effective at directing traffic away from hub nodes while maintaining efficient message delivery.

4) **Improved local measures of node importance**: as described in [68], there are several metrics that can be used to assess node importance or popularity (centrality). Examples of these are degree centrality (the number of neighbours a node has), betweeness centrality (the number of shortest paths that pass through the node divided by the number of shortest paths in the network) and closeness centrality (the maximum number of hops required to reach any other node in the network). However, these metrics are all defined in terms of the full network-wide topology, and their accurate calculation is not possible in opportunistic networks, since message transfer delays mean that any individual node's view of the network topology is based on out-of-date information. Thus, localised versions of centrality have been used in the literature for protocol design [23][24][46]. But these local measures are not always good approximations to their global equivalents: for example, Everett *et al.* [47] note that theoretically there is no relation between the ego betweeness centrality and the complete network's betweeness centrality. The use of localised centrality measures as routing metrics (such as ego betweeness or node degree) can have a worse impact on traffic distribution than that of a global centrality metric [49]. Further work is therefore required to establish robust local metrics that act as good proxy measures of network-wide statistics. We therefore agree with Katsaros *et al.* [69] that there is a need for further studies to develop means for accurately calculating node centrality across the whole network topology using low-cost local estimation methods.

5) **Improved local measures of other network parameters**: ideally, efficient transfer reliability and congestion control algorithms require knowledge of network-wide metrics. However, due to the long network delays, this global information is not available in opportunistic networks. Instead, local values are used as proxies for network-wide statistics, such as the number of copies of any single message [57][59][63], the number of distinct messages in the network [59], the network congestion level [56] and the network capacity [53]. Further study is needed, either to improve the existing local metrics or to find new ones that can act as better proxies to accurately estimate, for example, the number of message copies (for use in transfer reliability) or network congestion status.

6) **Issues in transfer reliability**: Some issues in transfer reliability need to be addressed, as follows:
   - Improved algorithms for removing from the network copies of successfully delivered messages (i.e. resolving the problem illustrated in Fig. 9).
   - Message transfer approaches that provide reliability while using fewer acknowledgements, and which deliver acknowledgements back to the source faster than existing approaches.
   - Reporting mechanisms for notifying the source in single-copy forwarding following message drops due to custody node failures or buffer overflow.

VIII. Conclusion

The nature of opportunistic networks means that some conventional end-to-end transport functions have to be additionally supported within the network. In particular, 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. In this article we have provided an overview of the state of the art of proposals for transfer reliability and congestion control in opportunistic networks. We have described existing proposals for opportunistic network transfer reliability in Section IV. We have discussed congestion control approaches, based on the network's replication strategy, whether single-copy (Section V) or multiple-copy strategies (Section VI). The main contributions of this article 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.

We hope the article enables readers to have a better understanding of the current state of the evolving research. Unlike ICN routing, research in these areas is still in its early stages and there are many open issues that need to be addressed before the benefits of opportunistic networks can be fully realised. Finally, it is our intention that the article 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.

TABLE I
SUMMARY OF CONGESTION CONTROL STRATEGIES FOR OPPORTUNISTIC NETWORKS

Proposal	**Congestion control category**	**Congestion control method**	**Underlying routing algorithm**	**Forwarding strategy**	**Performance evaluation / service target**
Sole & Joint Custody Transfer [36]	Storage congestion management	Economic model	Not specified	Single-copy	Delivery ratio
Autonomous Congestion Control [38]	Storage congestion management	Economic model & rule based storage management	Not specified	Single-copy	Delivery ratio
Dynamic Opportunity Cost [39]	Storage congestion management	Revenue management & dynamic programming	Routing based oracle	Single-copy	Delivery ratio
Congestion Aware Forwarding Algorithm (CAFé) [46]	Storage congestion management	Node resource assessment & traffic distribution	SimBet	Single-copy	Delivery ratio
Fair Route [41]	Storage congestion management	Assortative-based queue control & traffic distribution	Social-aware routing	Single-copy	Delivery ratio
Congestion Aware Adaptive strategy [45]	Storage congestion management	Storage assessment & delivery predictability	Adaptive routing	Single-copy	Delivery ratio
Path Avoidance [52]	Congestion avoidance	Node resource assessment & traffic distribution	Not specified	Single-copy	Delivery delay & Delivery ratio
Token Based Congestion Control [53]	Congestion avoidance	Token control	Not specified	Single-copy	Delivery delay & Delivery ratio
Retiring Replicant Congestion Control [56]	Replication management	Dynamic message replication based on congestion level	Epidemic, Prophet, Spray & Wait	Multiple-copy	Delivery ratio
Round Robin Forward Scheduling [57]	Replication management	Replication counter control	Epidemic routing	Multiple-copy	Delivery delay
CAFRep [58]	Replication management	Dynamic message replication based on total node heuristic utility	SimBet	Multiple-copy	Delivery delay & Delivery ratio
Queuing Policies & Forwarding Strategies [60]	Message drop	Drop strategy based on single message statistics	Probabilistic routing (Prophet)	Multiple-copy	Delivery delay & Delivery ratio
Forwarding in Opportunistic Networks with Resource Constraint [61]	Message drop	Drop strategy based on single message statistics	Delegation forwarding routing	Multiple-copy	Delivery delay & Delivery ratio
Congestion Avoidance in Data Centric Opportunistic Networks [62]	Message drop	Drop strategy based on interest & degree of replication	Interest based forwarding	Multiple-copy	Delivery ratio
Average Forwarding Number based on Epidemic Routing (AFNER) [63]	Message drop	Drop priority based on average forwarding number	Epidemic routing	Multiple-copy	Delivery delay & Delivery ratio
History Based Scheduling & Drop (HBSD) [59]	Message drop	Drop strategy based on local estimator of network-wide message statistics	Epidemic routing	Multiple-copy	Delivery delay & Delivery ratio

ACKNOWLEDGEMENT

The authors are grateful to the anonymous reviewers for providing valuable feedback. Bambang Soelistijanto is supported by the Indonesian Directorate General of Higher Education.

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.

[11] J. Liu, S. Singh., "ATCP: TCP for Mobile Ad Hoc Networks", *IEEE J. Sel. Areas Commun.*, vol.19, no.7, pp.1300-1315, July 2001.

[12] Y. Song, Y. Suh, "Rate-Control Snoop: a Reliable Transport Protocol for Heterogeneous Networks with Wired and Wireless Links", *Proc. IEEE Wireless Communications and Networking*, New Orleans, Louisiana, USA, March 2003.

[13] D. Kim, C.K. Toh, Y. Choi, "TCP-BuS: Improving TCP Performance in Wireless Ad Hoc Networks", *Journal of Communication and Networks*, vol.3, no.2, pp. 1-12, June 2001.

[14] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, H. Weiss, "Delay-Tolerant Networking Architecture", RFC 4838, April 2007.

[15] Licklider Transmission Protocol, available online: http://irg.cs.ohiou.edu/ltp/.

[16] R.C. Shah, S. Roy, S. Jain, W. Brunette, "Data MULEs: Modeling a Three-Tier Architecture for Sparse Sensor Networks", *Technical Report IRS-TR-03-001*, Intel Research, Jan. 2003.

[17] S. Merugu, "Routing in Space and Time in Networks with Predictable Mobility", *Technical Report GIT-CC-04-7*, Georgia Institute of Technology, 2004.

[18] R. Handorean, "Accommodating Transient Connectivity in Ad Hoc and Mobile Settings", *Proc. Pervasive*, Vienna, Austria, April 2004.

[19] S. Jain, K. Fall, R. Patra "Routing in a Delay Tolerant Network", *Proc. SIGCOMM*, Portland, Oregon, USA, Aug. 2004.

[20] A. Vahdat, D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks", *Technical Report CS-200006*, Duke University, 2000.

[21] A. Lindgren, A. Doria, O. Schelen, "Probabilistic Routing in Intermittently Connected Networks", *ACM SIGMOBILE Mobile Computing and Communication Review*, vol.7, no. 3, pp. 19-20, July 2003.

[22] J. Burgess, B. Gallagher, D. Jensen, B.N. Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks", *Proc. IEEE INFOCOM*, Barcelona, Spain, April 2006.

[23] E. Daly, M. Haahr, "Social Network Analysis for Routing in Disconnected Delay Tolerant MANETs", *Proc. 8th ACM Intl. Sym. on Mobile Ad Hoc Networking and Computing*, Montreal, Canada, Sep. 2007.

[24] P. Hui, J. Crowcroft, E. Yoneki, "BUBBLE Rap: Social-based Forwarding in Delay Tolerant Networks", *Proc. 9th ACM Intl. Sym. on Mobile Ad Hoc Networking and Computing*, Hong Kong, China, May 2008.

[25] Z. Zhang, "Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges", *IEEE Commun. Surveys Tuts.*, vol. 8, no. 1, pp. 24-37, 2006.

[26] Y. Cao, Z. Sun, "Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges", *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 654-677, 2012.

[27] R. Braden, "Requirements for Internet Host-Communication Layers", RFC 1122, 1989.

[28] O.B. Akan, J. Fang, I.F. Akyildiz, "TP-Planet: A Reliable Transport Protocol for Interplanetary Internet", *IEEE J. Sel. Areas Commun.*, vol. 22, no. 2, pp. 348-361, Feb. 2004.

[29] O.B. Akan, J. Fang, I.F. Akyildiz, "Performance of TCP protocols in deep space communication networks", *IEEE Commun. Lett.*, vol. 6, no. 2, pp. 478-480, Nov. 2002.

[30] Space Communication Protocol Standards (SCPS), available online: http://www.scps.org/html/tcp_peps.html

[31] L. Wood, C. Smith, W.M. Eddy, W. Ivancic, C. Jackson, J. McKim, "Saratoga: A Scalable File Transfer Protocol", Internet-draft draft-wood-tsvwg-saratoga-12.txt, Dec. 2010.

[32] R. Wang, T. Taleb, A. Jamalipour, B. Sun, "Protocols for Reliable Data Transport in Space Internet", *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 21-32, 2009.

[33] M. Grossglauser, D.N.C. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Networks", *IEEE/ACM Trans. Networking*, vol. 10, no. 4, pp. 477-486, Aug. 2002.

[34] F. Warthman, "Delay Tolerant Networks (DTNs): A Tutorial", *DTNRG doc. ver. 1.1 3/5/03*, 2003.

[35] K.A. Harras, K.C. Almeroth, "Transport Layer Issues in Delay Tolerant Mobile Networks", *Proc. IFIP Networking*, Coimbra, Portugal, May 2006.

[36] K. Fall, W. Hong, S. Madden, "Custody Transfer for Reliable Delivery in Delay Tolerant Networks", *Technical Report IRB-TR-03-030*, Intel Research Berkeley, 2002.

[37] R.B. Myerson, "Game Theory: Analysis of Conflict", *Harvard University Press*, 1991.

[38] S. Burleigh, E. Jennings, "Autonomous Congestion Control in Delay Tolerant Networks", *Technical Report*, Jet Propulsion Lab., available online: http://hdl.handle.net/2014/40636.

[39] G. Zhang, Y. Liu, "Congestion Management in Delay Tolerant Networks", *Proc. 4th Annual International Conference on Wireless Internet*, Brussels, Belgium, 2008.

[40] T. Hossmann, T. Spyropolous, F. Legendre, "A Complex Network Analysis of Human Mobility", *Proc. IEEE Conf. on Computer Commun. Workshops*, Shanghai, China, 2011.

[41] J.M. Pujol, A.L. Toledo, P. Rodriguez, "Fair Routing in Delay Tolerant Networks", *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009.

[42] The Reality Mining project, available online: http://reality.media.mit.edu

[43] J. Leguay, A. Lindgren, J. Scott, T. Friedman, J. Crowcroft, "Opportunistic Content Distribution in an Urban Setting", *Proc. ACM SIGCOM Workshop on Challenged Networks (CHANTS-06)*, Pisa, Italy, Sept. 2006.

[44] M.J. Khabbaz, C.M. Assi, W.F. Fawaz, "Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges", *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 607-640, 2012.

[45] T. Kathiravelu, N. Ranasinghe, A. Pears, "An Enhanced Congestion Aware Adaptive Routing Protocol for Opportunistic Networks", *Proc. 6th Intl. Conf. on Industrial and Information Systems*, Sri Lanka, Aug. 2011.

[46] M. Radenkovic, A. Grundy, "Congestion Aware Forwarding in Delay Tolerant and Social Opportunistic Networks", *Proc. 8th Intl. Conf. on Wireless On-Demand Network Systems and Services*, Bardonecchia, Italy, 2011.

[47] M. Everett, S.P. Borgatti, "Ego Network Betweeness", *Social Networks* 27, pp. 31-38, 2005.

[48] F. Fabbri, R. Verdone, "A Sociability-Based Routing Scheme for Delay-Tolerant Networks", *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, article ID 251408, pp. 1-13.

[49] B. Soelistijanto, M. Howarth, "Traffic Distribution and Network Capacity Analysis in Social Opportunistic Networks", *Proc. IEEE WiMob12 Workshop on Selected Topics in Mobile and Wireless Computing*, Barcelona, Spain, Oct. 2012.

[50] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, J. Scott, "Pocket Switched Networks and Human Mobility in Conference Environments", *Proc. ACM Sigcomm WDTN05*, Philadelphia, Pennsylvania, USA, 2005.

[51] T. Kathiravelu, N. Ranasinghe, A. Pears, "Towards Designing a Routing Protocol for Opportunistic Network", *Proc. Intl. Conf. on Advances in ICT for Emerging Regions*, Colombo, Sri Lanka, Sep. 2010.

[52] D. Hua, X. Du, L. Cao, G. Xu, Y. Qian, "A DTN Congestion Avoidance Strategy based on Path Avoidance", *Proc. 2nd Intl. Conf. Future Computer and Commun.*, Wuhan, China, 2010.

[53] E. Coe, C. Raghavendra, "Token Based Congestion Control for DTNs", *Proc. Aerospace Conference 2010*, Big Sky, Montana, USA, 2010.

[54] T. Spyropolous, K. Psounis, C.S. Raghvendra, "Spray and Wait: an Efficient Routing Scheme for Intermittently Connected Networks", *Proc. ACM SIGCOMM Workshop on DTN*, Philadelphia, Pennsylvania, USA, Aug. 2005.

[55] S.C. Nelson, M. Bakht, R. Kravets, "Encounter-Based Routing in DTNs", *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009.

[56] N. Thompson, S.C. Nelson, M. Bakht, T. Abdelzaher, R. Kravets, "Retiring Replicants: Congestion Control for Intermittently-Connected Networks", *Proc. IEEE INFOCOM*, San Diego, California, USA 2010.

[57] Y.K. Ip, W.C. Lau, O.C. Yue, "Forwarding and Replication Strategies for DTN with Resource Constraints", *Proc. IEEE 6th Vehicular Technology Conference*, Dublin, Ireland, May 2007.

[58] M. Radenkovic, A. Grundy, "Framework for Utility Driven Congestion Control in Delay Tolerant Opportunistic Networks", *Proc. 7th IWCMC*, Istanbul, Turkey, 2011.

[59] A. Krifa, C. Barakat, T. Spyropolous, "An Optimal Joint Scheduling and Drop Policy for Delay Tolerant Networks", *Proc. WoWMoM*, New Port Beach, California, USA, 2008.

[60] A. Lindgren, K.S. Phanse, "Evaluation of Queuing Policies and Forwarding Strategies for Routing in Intermittently Connected Networks", *Proc. First Intl. Conf. Comsware*, New Delhi, India, 2006.

[61] V. Erramili, M. Crovella, "Forwarding in Opportunistic Network with Resource Constraints", *Proc. Intl. Conf, MobiCom*, San Francisco, California, USA, Sep. 2008.

[62] F. Bjurefors, P. Gunningberg, C. Rohner, "Congestion Avoidance in a Data-Centric Opportunistic Network", *Proc. ACM SIGCOMM Workshop on Informatics-Centric Networking*, Toronto, Ontario, Canada, Aug. 2011.

[63] L. Yun, C. Xinjian, L. Qilie, Y. Xiaohu, "A Novel Congestion Control Strategy in Delay Tolerant Networks", *Proc. 2nd ICFN*, Hainan, China, 2010.

[64] I. Psaras, L. Wood, R. Tafazolli, "Delay-/Disruption-Tolerant Networking State of the Art and Future Challenges", *Technical Report*, University of Surrey, UK, 2010.

[65] S. Toivonen, "Web on the Move, Landscapes of Mobile Social Media", *VTT Research Notes 2403*, available online: http://vtt.fi/inf/pdf/tiedotteet/2007/T2403.pdf.

[66] B. Townsend, J. Abawajy, T.H. Kim, "SMS-based Medical Diagnostic Telemetry Data Transmission Protocol for Medical Sensors", *Sensors 2011*, pp. 4231-4243, 2011.

[67] A. Zinin, "Cisco IP Routing: Packet Forwarding and Intra-Domain Routing Protocols", *Addison-Wesley*, 2002.

[68] S.P. Borgatti, "Centrality and Network Flow", *Social Networks 27*, pp. 55-71, 2005.

[69] D. Katsaros, N. Dimokas, L. Tassiulas, "Social Network Analysis Concepts in the Design of Wireless Ad Hoc Network Protocols", *IEEE Network*, vol. 24, no. 6, pp. 23-29, Dec. 2010.

Bambang Soelistijanto is currently studying for his PhD at the Centre for Communication Systems Research at the University of Surrey, UK. He received his bachelor's degree in Electrical Engineering from Gadjah Mada University, Indonesia in 1993 and his M.Sc. degree from the Faculty of Electrical Engineering, Mathematics and Computer Science of Delft University of Technology, the Netherlands in 2007. His main research interests include opportunistic networks, mobile social networks and transport protocols for mobile ad hoc networks.

Michael Howarth received his bachelor's degree in engineering science and a DPhil degree in electrical engineering, both from Oxford University, and his MSc in telecommunications from the University of Surrey. He has worked for several networking and IT consultancies and is currently a lecturer in the Centre for Communication Systems Research (CCSR) in the Department of Electronic Engineering at the University of Surrey. His research interests include traffic engineering, quality of service, security and privacy, applied in fixed Internet, wireless and satellite networks. He is a chartered electrical engineer and a member of the UK IET.