

An Evaluation of Routing Reliability in Non-Collaborative Opportunistic Networks*

Ling-Jyh Chen, Che-Liang Chiou, and Yi-Chao Chen

Institute of Information Science, Academia Sinica
{ccljj, clchiou, yichao}@iis.sinica.edu.tw

Abstract

An opportunistic network is a type of challenged network that has attracted a great deal of attention in recent years. While a number of schemes have been proposed to facilitate data dissemination in opportunistic networks, there is an implicit assumption that each participating peer behaves collaboratively. Consequently, these schemes may be vulnerable if there are uncooperative or malicious peers in the network. In this study, we identify five types of non-collaborative behavior, namely free rider, black hole, supernova, hypernova, and wormhole behavior, in opportunistic networks. We also evaluate the impacts of the five types of behavior on the data transmission performance of three widely used routing schemes. Using simulations as well as real-world traces of network mobility, we show that the data forwarding performance degrades significantly as the number of non-collaborative peers, except wormholes, increases. Moreover, we find that the three compared routing schemes can benefit from wormhole behavior, especially when the network connectivity is poor and the buffer size is limited.

1. Introduction

An opportunistic network is a type of challenged network that has the following characteristics: (1) network contacts (i.e., communication opportunities) are intermittent; (2) there is rarely an end-to-end path between the source and the destination; (3) disconnection and reconnection are common; and (4) link performance is highly variable or extreme. Emerging applications of opportunistic networks are wide ranging.

*This paper is based on research supported by the National Science Council of Taiwan under Grant No. NSC 97-2628-E-001-007-MY3 and NSC 97-2631-S-003-002.

For instance, it would be quite advantageous to be able to interconnect mobile search and rescue nodes in disaster areas (where communication infrastructures have been disabled by earthquakes, hurricanes, wildfires, or floods), allow message exchange in underdeveloped areas (remote towns and villages interconnected by wireless networks, but not guaranteed an always-on Internet connection), and permit scientific monitoring of wilderness areas (remote monitoring of various forms of wildlife).

Data transmission in an opportunistic network is challenging and completely different to routing in a conventional network. Ideally, a routing scheme for opportunistic networks should provide reliable data delivery, even when the network connectivity is intermittent or when an end-to-end path is temporally unavailable. Moreover, since ‘network contacts’ (i.e., communication opportunities) in an opportunistic network may appear arbitrarily without prior information, neither scheduled optimal routing (e.g., linear programming routing in delay tolerant networks of scheduled contacts [17]) nor mobile relay approaches [27, 28] can be applied.

Several data forwarding schemes have been proposed for opportunistic networks [6, 22, 24–26]. Generally, the schemes rely heavily on close collaboration among network participants. However, on the downside, the schemes may be unreliable if there are non-collaborative (either uncooperative or malicious) peers in the network. The objective of this study is to investigate the impact of non-collaborative behavior on the data transmission performance of opportunistic networks.

Specifically, the contribution of this work is two-fold. First, we identify five types of non-collaborative behavior in opportunistic networks, namely free rider, black hole, supernova, hypernova, and wormhole behavior. Second, using simulations as well as real-world traces of network mobility, we evaluate the impact of the five

types of non-collaborative behavior on the data transmission performance of three routing schemes (epidemic routing [24], P_{RO}PHET routing [22], and HEC-BI routing [11]), which are widely used in opportunistic networks. The results show that the performance of each scheme degrades significantly as the number of non-collaborative peers, except wormholes, increases. Interestingly, we find that the three compared routing schemes are robust against wormholes, and can even benefit from wormhole behavior when the network connectivity is poor and the network buffer is limited. Our results demonstrate the impacts of non-collaborative peers on data transmission in opportunistic networks, and also provide practical guidelines for the future deployment of such networks.

The remainder of the paper is organized as follows. Section 2 contains a review of related works. In Section 3, we define the five types of non-collaborative behavior in opportunistic networks. Section 4 presents a comprehensive set of simulation results for various opportunistic network scenarios; the results are also analyzed and explained in detail. We then summarize our conclusions in Section 5.

2. Background

Replication is the most popular design choice for opportunistic routing schemes. For instance, the *Epidemic Routing* scheme [24] sends identical copies of a message simultaneously over multiple paths to mitigate the effects of a single path failure; thus, it increases the possibility of successful message delivery. However, flooding a network with duplicate data tends to be very costly in terms of traffic overhead and energy consumption.

To address the problem of excess traffic overhead caused by flooding, Harras et al. proposed a *Controlled Flooding* scheme that reduces the flooding overhead while maintaining reliable message delivery [13]. To control flooding, the scheme uses three parameters: *willingness probability*, *Time-to-Live*, and *Kill Time*. Additionally, after a message has been delivered successfully, a *Passive Cure* is generated to “heal” network nodes that have been “infected” by the message. Controlled flooding substantially reduces the network overhead by preventing the excess traffic overhead problem, while maintaining reliable data delivery.

Node mobility also impacts on the effectiveness of opportunistic routing schemes. Previous studies have shown that if the network mobility differs from that of well-known random way-point mobility models (e.g., the Pursue Mobility Model [7] or the Reference Point Group Mobility Model [14]), the overhead carried by

epidemic- and/or flooding-based routing schemes can be reduced by considering node mobility. For instance, the *Probabilistic Routing* scheme [21] calculates the *delivery predictability* from a node to a particular destination node based on the observed contact history, and forwards a message to its neighboring node if and only if that node has a higher delivery predictability value. Leguay et al. [18] extended the scheme by taking the *mobility pattern* into account, i.e., a message is forwarded to a neighbor node if and only if that node has a mobility pattern similar to that of the destination node. The results reported in [18, 19] show that the extended *mobility pattern* scheme is more effective than previous schemes.

Another class of opportunistic network routing schemes is based on encoding techniques, which transform a message into a different format prior to transmission. For example, to reduce the number of transmissions required in a network, an integration of *network coding* and epidemic routing techniques was proposed in [26]. Meanwhile, [25] suggested combining *erasure coding* and the simple replication-based routing method to improve data delivery for cases with the *worst delay performance* in opportunistic networks.

Following the concept of erasure coding-based data forwarding [25], Y. Liao et al. proposed an Estimation-based Erasure-Coding routing scheme (EBEC) that adapts the delivery of erasure coded blocks by using the Average Contact Frequency (ACF) estimate [20]. In addition, [10] proposed a hybrid scheme, called HEC, which combines the strength of erasure coding and the advantages of *Aggressive Forwarding*. The HEC scheme has been further enhanced by employing techniques like sequential forwarding (i.e., HEC-SF) [11], probabilistic forwarding (i.e., HEC-PF) [9], full interleaving (i.e., HEC-FI) [11], and block-based interleaving (i.e., HEC-BI) [11].

3. Problem Definition

As mentioned in the previous section, the success of opportunistic network routing depends to a large extent on close collaboration among network participants; however, on the downside, data transmission may be impacted if there are non-collaborative peers in the network. We consider five types of non-collaborative behavior in opportunistic networks, namely free rider, black hole, supernova, hypernova, and wormhole behavior. Hereafter, for convenience, we use the names listed in the right-hand column of Table 1 to refer to collaborative peers and the respective non-collaborative peers. Next, we describe the five types of behavior in detail.

Peer type	Conventional Name(s)
Cooperative Peers	Calvin, Charles, Conan
Free rider	Frank
Black hole	Barry
Supernova	Sam
Hypernova	Howard
Wormhole	Wesley

Table 1. Conventional names for the compared network peers

3.1. Free Rider Behavior

Free rider is a type of selfish behavior [5] that has been studied extensively in the problem of peer-to-peer networking in recent years. In an opportunistic network, a free rider peer uses the network to help him forward data to other peers, but he refuses to serve as a relay for other participating peers. As a result, free riders require less memory and energy than collaborative peers, but the system has to bear the cost (in terms of the overall data transmission performance) due to the reduced level of collaboration.

For instance, under the PROPHET scheme, if *Calvin* encounters *Frank* and asks him to help relay a message to *Charles*, *Frank* will declare that he has never met *Charles* and respond with the delivery predictability $P_{(Frank, Charles)} = 0$. Similarly, under the epidemic routing scheme or the HEC-BI scheme, *Frank* simply pretends that *Calvin* cannot reach him, unless he needs *Calvin* to help relay messages initiated by him; thus, *Calvin* will not ask *Frank* to help relay the message.

3.2. Black Hole Behavior

Black hole is another type of uncooperative behavior [12], where the peer drops all of his/her relayed data without forwarding it to other peers. This may be intentional or due to a lack of capability, such as limited battery power or buffer size. Consequently, black holes cause data loss and may significantly degrade the transmission performance of opportunistic networks.

For instance, if *Calvin* encounters *Barry* and asks him to help relay a message to *Charles*, *Barry* will respond that he meets *Charles* frequently (i.e., under the PROPHET scheme, the delivery predictability $P_{(Barry, Charles)} \approx 1$) and he can relay the message. However, after *Barry* receives the message from *Calvin*, he drops it immediately without forwarding it to *Charles*, but *Calvin* is not aware of the situation. Note that, unlike free rider behavior, which is always deliberate, the behavior of black-hole peers is likely to be unintentional. In other words, they cannot avoid

dropping the relayed data due to their poor networking capability, such as limited battery power or insufficient storage capacity.

3.3. Supernova Behavior

In contrast to the behavior of free riders and black-hole peers, *supernova* behavior is a type of malicious attack that actively propagates random messages destined for other network peers; in other words, it is similar to email spamming, network worms, and denial of service attacks on the Internet. As a result, the malicious traffic consumes valuable network resources (such as network bandwidth, network buffer, and battery power), and interferes with the transmission of regular messages over the network.

For example, assume that *Sam* generates a number of random messages intended for *Charles*, and he asks *Calvin* to help relay them. Since *Calvin* is collaborative, he accepts the request and starts forwarding the messages to other peers. However, when *Charles* receives the messages, he ignores them because he is not interested in them. Consequently, a substantial amount of network resources are wasted, and the transmission of genuine messages is thus degraded.

3.4. Hypernova Behavior

Similar to supernova, *hypernova* is also a type of active malicious behavior. However, unlike supernova, which initiates messages destined for valid network peers, hypernova propagates random messages intended for a virtual peer that may or may not exist in the opportunistic network. As a result, the network tends to carry the propagated messages much longer than those initiated by supernova, since it has to keep them until they find their destination nodes or they are dropped due to network buffer overflow. Therefore, like supernova, hypernova behavior wastes network resources by transmitting malicious messages such that the transmission of genuine messages is degraded.

3.5. Wormhole Behavior

Wormhole behavior [15, 23] is also a potentially severe threat to data transmission in opportunistic networks. A network wormhole peer is composed of one black hole and one white hole. While black holes ‘absorb’ data from other peers, white holes ‘radiate’ data as much as they can into the network. As a result, the wormhole peer is very likely to be overloaded, and the system may be affected by the *single-point-of-failure*

problem. Moreover, since a wormhole is a tunnel connecting the black hole and the white hole, it can examine every piece of data that passes through the tunnel, which may create other problems, such as breaches of security, privacy, and anonymity.

For example, if *Calvin* encounters *Wesley* and asks whether he can help relay a message to *Charles*, *Wesley* will reply that he meets *Charles* frequently, and that he is willing to relay the message (i.e., like a black hole). Then, when *Wesley* encounters another peer in the network, say *Conan*, *Wesley* pretends that *Conan* is better able to forward the message (i.e., the delivery predictability $P_{(Wesley, Charles)} < P_{(Conan, Charles)}$ in the PRoPHET scheme); thus, he forwards the message to *Conan* (i.e., like a white hole).

4. Evaluation

In this section, we evaluate the reliability of three popular opportunistic network routing schemes, namely the epidemic routing scheme [22], the PRoPHET scheme [24], and the HEC-BI scheme [11]. We implemented the three schemes and performed simulations in DTNSIM [3], a Java-based opportunistic network simulator. All the results presented here are based on the average performance of 200 simulation runs for each network configuration.

In each simulation run, the source and the destination pair was randomly selected from all participating peers; and the source peer transmitted messages in the first 10% of the simulation time with a Poisson rate of 1,800 seconds/message. For simplicity, we assume that data transmission between peers is via Bluetooth 2.0 EDR [1] with a fixed rate of 2Mbps, and all messages are 1Mbyte. Moreover, the buffer size of each peer is fixed at 1GByte for the first two evaluations (i.e., free riders and blackholes) and 100MBytes for the others (i.e., supernova, hypernova, and wormholes)¹. For each type of non-collaborative behavior, we varied the percentage of non-collaborative peers in the network, and compared the delivery performance of the three routing schemes (i.e., the average percentage of messages received by the destination at the end of the simulation run). We present the evaluation scenarios in the Subsection 4.1, and discuss the results in Subsections 4.2 to 4.6.

¹We use a smaller buffer size in the evaluations of the supernova, hypernova, and wormhole scenarios because these three types of behavior require a tremendous amount of network buffer, and their data transmission performance is very sensitive to the size of buffer available on each network peer. Thus, we reduce the buffer size to trigger more buffer overflow events in the simulations.

Table 2. The properties of the iMote and UCSD network scenarios

Trace Name	iMote	UCSD
Device	iMote	PDA
Network Type	Bluetooth	WiFi
Duration (days)	3	77
Devices participating	274	273
Number of contacts	28,217	195,364
Avg # Contacts/pair/day	0.25148	0.06834

4.1. Evaluation Scenarios

We evaluated two network scenarios based on realistic wireless network traces, namely, the iMote [2] and UCSD [4] traces, which are publicly available for research purposes. They correspond to the opportunistic people networks of conference and campus scenarios respectively. Table 2 details the basic properties of the two network scenarios.

The iMote trace is a human mobility trace collected at the 2005 IEEE Infocom conference. It was aggregated from 41 Bluetooth-based iMote devices distributed to the student attendees for the duration of the 3-day conference. Each iMote device was pre-configured to periodically broadcast query packets to find other Bluetooth devices within range, and record the devices that responded to the queries. In addition to the distributed iMote devices, another 233 devices were recorded in the trace. They may have been other Bluetooth-enabled devices (e.g., PDAs, cell phones, or headsets) used during the conference. For simplicity, we assume there is a network contact between two Bluetooth devices if there are query-and-response interactions between them.

The UCSD network trace is client-based and records the availability of WiFi-based access points (APs) for each participating portable device (e.g., PDAs and laptops) on the UCSD campus. The trace covered a two and half-month period, and there were 273 participating devices. Similar to [8, 10, 16], we assume that two participating devices in ad hoc mode encounter a communication opportunity (i.e., a network contact) if they are associated with the same AP at the same time.

4.2. Evaluation I: Free Riders

In the first set of simulations, we evaluate the impact of free riders on data transmission in opportunistic networks. Figure 1 illustrates the delivery performance of the three routing schemes with various percentages of free riders. It is obvious that, in all test cases, the

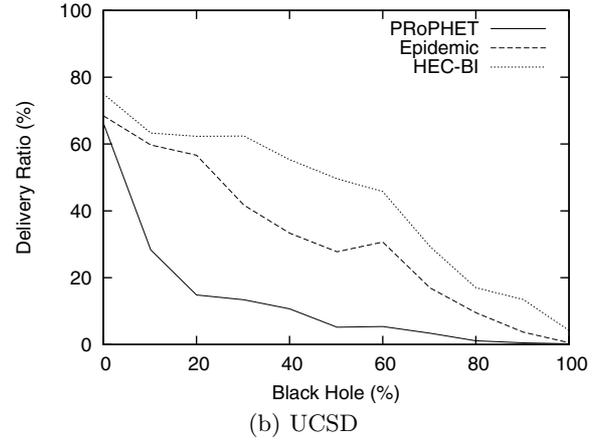
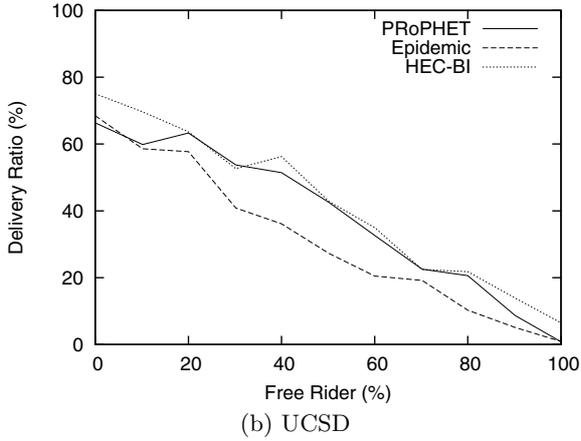
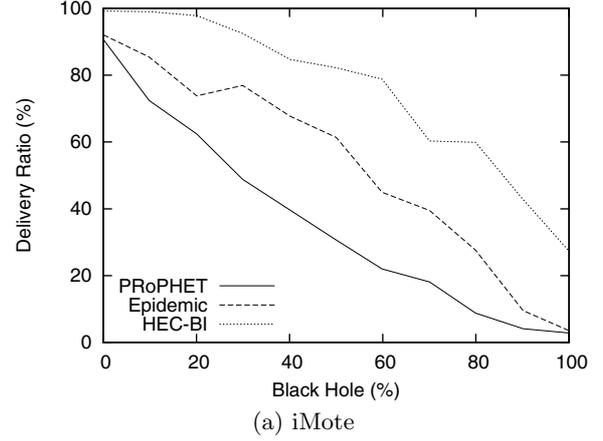
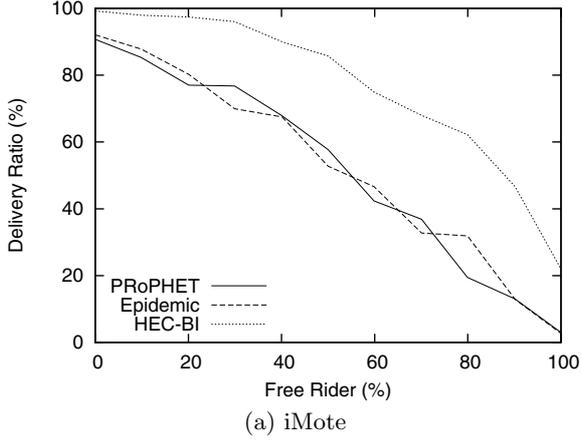


Figure 1. The delivery performance of the three routing schemes with various percentages of free riders.

Figure 2. The delivery performance of the three routing schemes with various percentages of black hole peers.

performance degrades as the percentage of free riders increases. The results indicate that *free riders are very harmful to data transmission in opportunistic networks*. Moreover, the results show that, in the iMote scenario, the delivery performance of the PProPHET and epidemic schemes are comparable, while the HEC-BI scheme achieves the best performance. By contrast, in the UCSD scenario, the performances of the HEC-BI and PProPHET schemes are comparable, while the epidemic scheme performs the poorest. The reason is that the HEC-BI and the epidemic schemes create a large amount of traffic overhead during data transmission due to erasure encoding and replication. Consequently, if the network connectivity is not very good, and/or the wireless bandwidth is limited, the two schemes require a larger number of ‘network contacts’ to forward relayed messages. As shown in Table 2, network contacts are much more frequent in the iMote scenario

than in the UCSD scenario; hence, the HEC-BI and the epidemic schemes can achieve a better delivery performance in the iMote scenario. In contrast, the performance of the PProPHET scheme is not so sensitive to the frequency of network contacts because it does not produce much traffic overhead.

4.3. Evaluation II: Black Hole Peers

Next, we evaluate the impact of black holes on the data transmission performance of opportunistic networks. Figure 2 shows the delivery performance of the three routing schemes with various percentages of black holes in the iMote and the UCSD scenarios. Similar to the simulations in the previous subsection, the delivery performance degrades as the percentage of black holes increases, which indicates that *black holes are very harmful to data transmission in opportunistic networks*. The results show that the HEC-BI scheme sig-

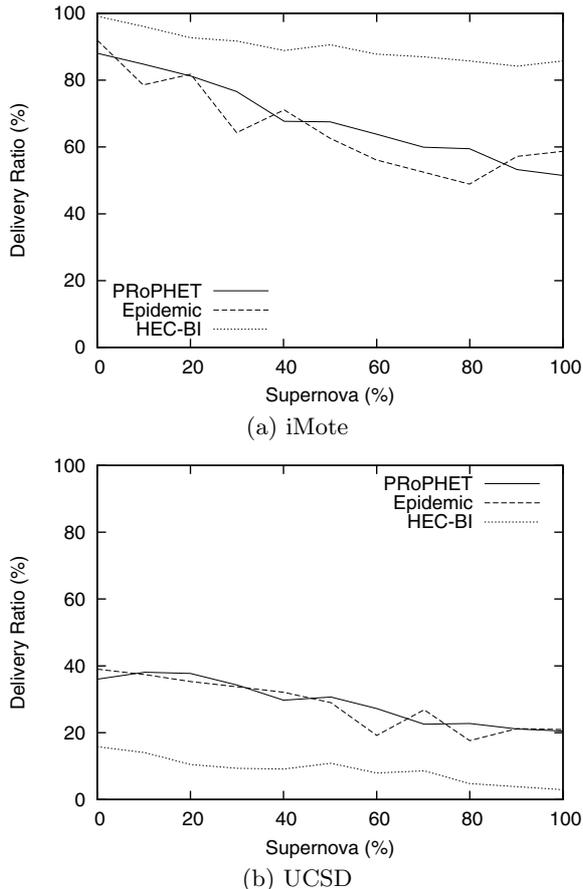


Figure 3. The delivery performance of the three routing schemes with various percentages of supernova peers.

nificantly outperforms the other schemes in both scenarios. The PRoPHET scheme yields the poorest performance in all test cases, since it assumes that all peers in the network are honest and collaborative. Thus, it has no idea about the existence of black holes, but it tends to utilize them to relay messages whenever possible (because the black holes always indicate that they can provide very reliable delivery). As a result, the routing reliability degrades as the number of black holes increases. On the other hand, the HEC-BI and the epidemic schemes are more resilient to black holes, because they select peers to relay messages in an FCFS-based manner (regardless of the peers' capability and willingness).

4.4. Evaluation III: Supernova Peers

Figure 3 shows the delivery performance of the three routing schemes with various percentages of supernova

peers in the iMote and UCSD scenarios. Similar to the results of the free rider and black hole scenarios, the delivery performance degrades as the percentage of supernova peers increases for all routing schemes. However, the degradation rates of the three routing schemes in the supernova scenario are much slower than those in the free rider and black hole scenarios. This indicates that the three schemes are more robust against supernova behavior than free rider and black hole behavior.

The results also show that while the HEC-BI scheme outperforms the other schemes in the iMote scenario, it only achieves about half of the delivery ratio of the other two schemes in the UCSD scenario. This is because, compared to the other schemes, HEC-BI is very sensitive to the available buffer size and network connectivity. Since the network connectivity of the UCSD scenario is very poor compared to that of the iMote scenario, the HEC-BI scheme requires much more network buffer to cache messages for transmission; however, according to our simulations, this is impossible due to the buffer size settings. Therefore, HEC-BI is at a disadvantage and yields a poor delivery performance.

4.5. Evaluation IV: Hypernova Peers

Next, we evaluate the three routing schemes with various percentages of hypernova peers. The results, shown in Figure 4, are very similar to the results for supernova in Figure 3. Thus, the effects of supernova and hypernova are similar, and they both have less impact on the data transmission performance than free riders and black holes. Moreover, when the network connectivity is poor, the HEC-BI scheme is not favored, unless every network peer has a sufficiently large buffer size.

4.6. Evaluation V: Wormhole Peers

Finally, we evaluate the three routing schemes with various percentages of wormhole peers. The simulation results are shown in Figure 4.

Surprisingly, the delivery performance does not degrade as the percentage of wormholes increases. For example, in the UCSD scenario, when the percentage of wormholes increases from 0% to 100%, the delivery ratio increases from 47.82% to 68.43% under the PRoPHET scheme, from 39.00% to 71.80% under the epidemic scheme, and from 15.80% to 78.20% under the HEC-BI scheme. The results indicate that the three schemes are robust against wormholes, and they can even benefit substantially from wormholes when the network connectivity is poor (i.e., in the UCSD

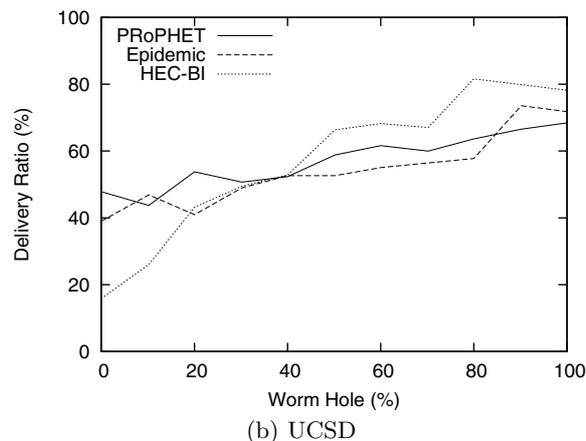
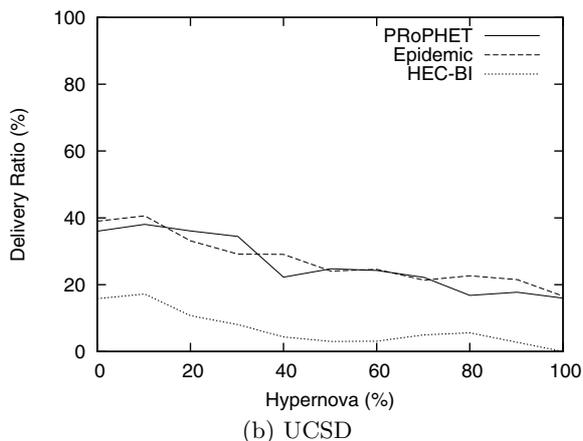
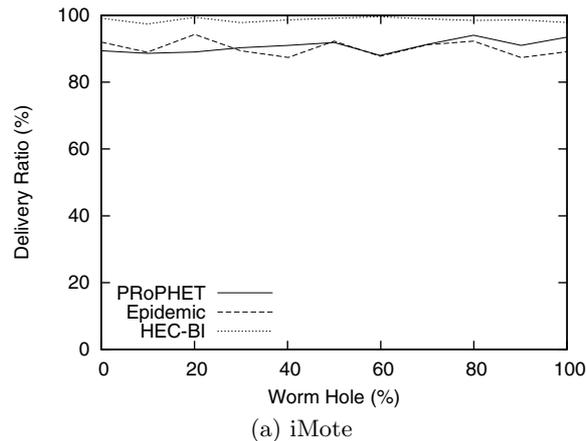
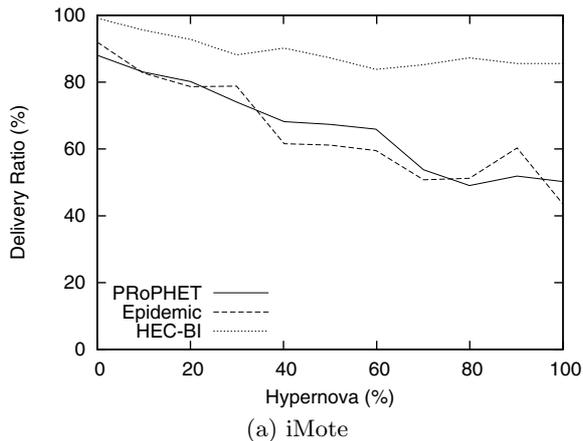


Figure 4. The delivery performance of the three routing schemes with various percentages of hypernova peers.

Figure 5. The delivery performance of the three routing schemes with various percentages of wormhole peers.

scenario). Even so, wormhole behavior should not be encouraged in opportunistic networks because it is likely to create other reliability and security problems, such as eavesdropping, message tampering, and identity spoofing.

5. Conclusion

In this paper, we study the routing reliability issue in opportunistic networks. We consider five types of non-collaborative behavior, namely free rider, black hole, supernova, hypernova, and wormhole behavior, and evaluate their impacts on three popular routing schemes: epidemic routing, PProPHET routing, and HEC-BI routing. Using simulations as well as realistic mobility traces, we show that the data transmission performance degrades significantly as free rider, black hole, supernova, or hypernova behavior increases. In

contrast, all three routing schemes are robust against wormhole behavior, and they can even benefit from it - especially when the network connectivity is poor. Work on enhancing routing reliability and detecting malicious behavior is ongoing, and we hope to report the results in the near future.

References

- [1] Bluetooth specifications core v2.0. <http://www.bluetooth.com>.
- [2] Crowdad project. <http://crowdad.cs.dartmouth.edu/>.
- [3] Delay tolerant network simulator. <http://www.dtnrg.org/code/dtnsim.tgz>.
- [4] UCSD wireless topology discovery project. <http://sysnet.ucsd.edu/wtd/>.

- [5] E. Adar and B. A. Huberman. Free riding on gnutella. http://www.firstmonday.org/issues/issue5_10/adar/, 2000.
- [6] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine. MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks. In *IEEE Infocom*, 2006.
- [7] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communication and Mobile Computing Journal*, 2(5):483–502, 2002.
- [8] A. Chaintreau, P. Hui, J. Crowcroft, C. D. and Richard Gass, and J. Scott. Impact of human mobility on the design of opportunistic forwarding algorithms. In *IEEE Infocom*, 2006.
- [9] L.-J. Chen, C.-L. Tseng, and C.-F. Chou. On using probabilistic forwarding to improve hec-based data forwarding for opportunistic networks. In *IFIP EUC*, 2007.
- [10] L.-J. Chen, C.-H. Yu, T. Sun, Y.-C. Chen, and Hao-huaChu. A hybrid routing approach for opportunistic networks. In *ACM SIGCOMM Workshop on Challenged Networks*, 2006.
- [11] L.-J. Chen, C.-H. Yu, C.-L. Tseng, H. hua Chu, and C.-F. Chou. A content-centric framework for effective data dissemination in opportunistic networks. *IEEE Journal of Selected Areas in Communications*, 26(5):761–772, June 2008.
- [12] H. Deng, W. Li, and D. P. Agrawal. Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40:70–75, October 2002.
- [13] K. A. Harras, K. C. Almeroth, and E. M. Belding-Royer. Delay tolerant mobile networks (dtmns): Controlled flooding in sparse mobilenetworks. In *IFIP Networking*, 2005.
- [14] X. Hong, M. Gerla, R. Bagrodia, and G. Pei. A group mobility model for ad hoc wireless networks. In *ACM MSWIM*, 1999.
- [15] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In *IEEE Infocom*, 2003.
- [16] P. Hui, A. Chaintreau, J. Scott, R. Gass, Jon-Crowcroft, and C. Diot. Pocket switched networks and human mobility in conference environments. In *ACM SIGCOMM Workshop on Delay Tolerant Networks*, 2005.
- [17] S. Jain, K. Fall, and R. Patra. Routing in a delay tolerant network. In *ACM SIGCOMM*, 2004.
- [18] J. Leguay, T. Friedman, and V. Conan. Dtn routing in a mobility pattern space. In *ACM SIGCOMM Workshop on Delay Tolerant Networks*, 2005.
- [19] J. Leguay, T. Friedman, and V. Conan. Evaluating mobility pattern space routing for dtms. In *IEEE Infocom*, 2006.
- [20] Y. Liao, K. Tan, Z. Zhang, and L. Gao. Estimation based erasure-coding routing in delay tolerant networks. In *International Wireless Communications and Mobile Computing Conference*, 2006.
- [21] A. Lindgren and A. Doria. Probabilistic routing protocol for intermittently connected networks. draft-lindgren-dtnrg-prophet-01.txt, IETF Internet draft, July 2005.
- [22] A. Lindgren, A. Doria, and O. Schelen. Probabilistic routing in intermittently connected networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(3):19–20, July 2003.
- [23] K. Sanzgiri, B. Dahill, B. N. Levine, and C. S. E. M. Belding-Royer. A secure routing protocol for ad hoc networks. In *IEEE ICNP*, 2002.
- [24] A. Vahdat and D. Becker. Epidemic routing for partially-connected ad hoc networks. Technical Report CS-2000-06, Duke University, 2000.
- [25] Y. Wang, S. Jain, M. Martonosi, and K. Fall. Erasure coding based routing for opportunistic networks. In *ACM SIGCOMM Workshop on Delay Tolerant Networks*, 2005.
- [26] J. Widmer and J.-Y. L. Boudec. Network coding for efficient communication in extreme networks. In *ACM SIGCOMM Workshop on Delay Tolerant Networks*, 2005.
- [27] W. Zhao, M. Ammar, and E. Zegura. A message ferrying approach for data delivery in sparse mobile ad hoc networks. In *ACM MobiHoc*, 2004.
- [28] W. Zhao, M. Ammar, and E. Zegura. Controlling the mobility of multiple data transport ferries in a delay-tolerantnetwork. In *IEEE Infocom*, 2005.