Poster Abstract: An Evaluation Study of Routing Reliability in Opportunistic Networks*

Che-Liang Chiou and Ling-Jyh Chen
Institute of Information Science, Academia Sinica
{clchiou, cclljj}@iis.sinica.edu.tw

ABSTRACT

An opportunistic network is a type of challenged network that has attracted increasing attention recently. While a number of schemes have been proposed to facilitate data forwarding in opportunistic networks, an implicit assumption is made in common that each participating peer is collaborative in the network. Consequently, these schemes become vulnerable when there exist uncooperative peers in the network. In this study, we evaluate two widely used routing schemes in opportunistic networks with three types of uncooperative behaviors, namely free riders, black holes, and wormholes. Using simulation as well as realistic network scenarios, we show that the data forwarding performance degrades significantly as the number of free riders increases. Moreover, we show that the epidemic scheme is more resilient against black holes than the PROPHET scheme, while both schemes are robust against wormholes.

Categories and Subject Descriptors

C.4 [**Performance of Systems**]: [Reliability, availability, and serviceability]

General Terms

Performance, Security

1. INTRODUCTION

An opportunistic network is a type of challenged network that satisfies the following conditions: (1) network contacts are intermittent, (2) an end-to-end path between the source and the destination rarely exists, (3) disconnection and reconnection is common, and (4) link performance is highly variable or extreme. Emerging applications of opportunistic networks are wide ranging, such as mobile search/rescue in disaster areas, message exchanges in underdeveloped areas, and scientific monitoring of wilderness areas.

Several data forwarding schemes have been proposed for opportunistic networks [5]. Yet, these schemes all rely on an implicit assumption that every network participant is collaborative and willing to help forward data in the network. However, on the downside, these data forwarding schemes are thus vulnerable (in terms of network reliability) if there are uncooperative peers in the network, such as free riders, black holes, and wormholes.

*This work was supported by the National Science Council of Taiwan under grant numbers NSC 96-2221-E-001-010.

MobiHoc'08, May 26–30, 2008, Hong Kong SAR, China.
ACM 978-1-60558-083-9/08/05.

cooperative node	Alice
free rider	Frank
black hole	Brad
wormhole	William

Table 1: Conventional names for malicious node

In this study, we investigate the routing reliability issue in opportunistic networks. Using two widely used opportunistic network routing schemes, namely epidemic routing [4] and PROPHET [3] schemes, we evaluate the impact of free riders, black holes, and wormholes on the data forwarding in opportunistic networks. The results show that the data forwarding performance degrades significantly as the number of free riders increases. Moreover, the results also show that the epidemic scheme is more resilient against black holes, while both schemes are robust against wormholes.

2. PROBLEM STATEMENT

In an opportunistic network, a message will be forwarded by several intermediate nodes before arriving its destination. The reliability of network routing depends on whether network nodes are cooperative in forwarding messages. Here we define three types of uncooperative node: free rider, black hole, and wormhole. For convenience, we use the names on the right column of Table 1 to represent the three corresponding uncooperative nodes in the followings.

1. **Free Rider**: Free riders are selfish peers who make use of the network to help them forward data to other peers in the network, but refuse to serve as relays for the others. For instance, when Alice encounters Frank, Frank will declare he has never encountered any other nodes, i.e., his delivery predictability $P_{(a,b)} = 0$ for all destinations b. Since Alice adopts PROPHET to route messages, she will not ask Frank to relay any messages. On the other hand, when the epidemic routing scheme is used, Alice will ask Frank to help relay data, but Frank simply drops all of them immediately.

2. **Black Hole**: Black holes make their best to absorbs messages and drop them immediately without forwarding to other peers. For instance, when Alice encounters Brad, Brad will declare he has very frequent contact with the destination nodes (i.e., the delivery predictability $P_{(a,b)} = 1$ for all destinations b). According to PROPHET, Alice will rely on Brad to forward messages. On the other hand, when the epidemic routing scheme is used, a black hole simply drops all messages like free riders.

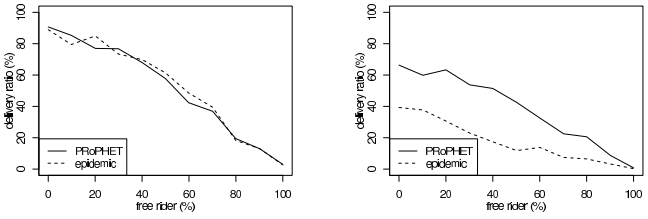
3. **Wormhole**: A wormhole is composed of one black hole and one white hole. While black holes 'absorb' data from other

peers, white holes 'radiate' data as much as they could to the network. For instance, William will act like a black hole in the way that he declares his delivery predictability $P_{(a,b)} = 1$ for all destinations b. However, instead of dropping data immediately, William forwards those absorbed data to other network peers as much as he can.

3. EVALUATION

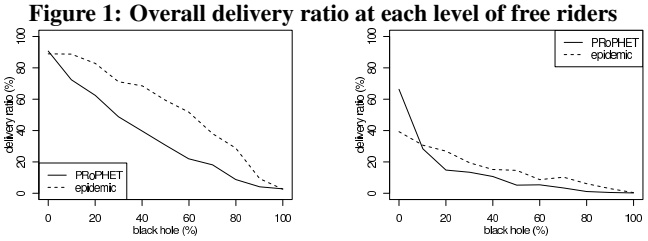
We implemented two data forwarding schemes, namely the epidemic routing scheme and the PROPHET scheme, in the DTNSIM simulator, and we evaluated the reliability issue using two opportunistic network scenarios based on realistic wireless network traces (i.e., the iMote [1] and UCSD [2] traces). We set bandwidth between any two contacted nodes to be 1 Mbyte/sec, and message size fixed to 3M bytes. For each type of uncooperative behavior, we have a control group in which all nodes are ordinary epidemic or PROPHET routers, and 10 experimental groups in which 1/10, 2/10, . . . , 10/10 of nodes, respectively, are randomly selected to be malicious nodes. For each network configuration, we calculate the delivery ratio by averaging the results of 100 simulation runs.

In the first set of simulation, we evaluate the impact of free riders on routing reliability in opportunistic networks. Figure 1 demonstrates the delivery ratio performance of the epidemic scheme and the PROPHET scheme with various percentage of free riders in the network. It is very obvious that the delivery ratio performance degrades as the percentage of free riders increases, i.e., free riders are harmful for data forwarding in opportunistic networks. Moreover, we also observe that the PROPHET scheme significantly outperforms the epidemic scheme in the UCSD scenario, while the performance of these two schemes are comparable in the iMote scenario. The reason is because the epidemic scheme creates much more traffic overhead than the PROPHET scheme, thereby resulting in packet losses of buffer overflow. However, since network connectivity is very rich in the iMote scenario, the epidemic scheme is able to achieve comparable performance as long as at least one of the replica is received by the destination node.



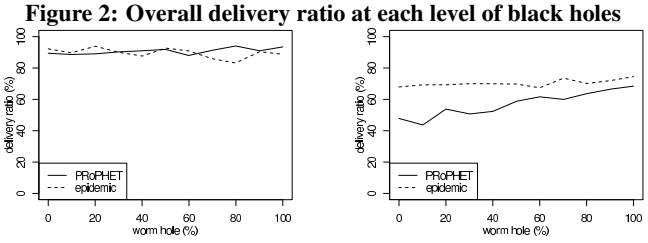
(a) iMote (b) UCSD

Figure 1: Overall delivery ratio at each level of free riders



(a) iMote (b) UCSD

Figure 2: Overall delivery ratio at each level of black holes



(a) iMote (b) UCSD

Figure 3: Overall delivery ratio at each level of wormholes

Next, we evaluate the impact of black holes on the routing reliability in opportunistic networks. Figure 2 shows the delivery ratio performance of the epidemic routing and PROPHET routing with various percentage of black holes in the iMote and the UCSD scenarios. Similar to the previous evaluation results, the delivery ratio performance degrades as the percentage of uncooperative nodes increases. However, we also observe that the epidemic scheme outperforms the PROPHET scheme when black holes are present in the network (i.e., $> 0\%$). The reason is because the PROPHET scheme assumes all peers are honest and collaborative. As a result, the PROPHET scheme tends to make use of the black holes, and therefore lose the reliability. On the other hand, the epidemic scheme is more resilient to black holes due to its flooding nature.

Finally, we evaluated the impact of wormholes on the routing reliability. Figure 3 shows the delivery ratio performance of the epidemic routing and PROPHET routing with various percentage of black holes in the iMote and the UCSD scenarios. The results show that the delivery ratio increases as the percentge of wormhole increases, especially in the UCSD scenario. More precisely, in the UCSD scenario, the delivery ratio increases from 47.82% to 68.43% when the percentge of wormholes increases from 0% to 100%. The epidemic scheme, on the other side, maintains the delivery ratio performance regardless of the percentage of wormholes in the network. However, it should also be mentioned that even though wormhole looks not harmful for the delivery ratio performance for both the epidemic and PROPHET schemes, they may cause other reliability and security issues since they tend to absorb all messages in the network.

4. CONCLUSION

In this paper, we study the routing reliability issue for opportunistic networks. We consider three types of uncooperative behaviors, namely free riders, black holes, and wormholes, and evaluate their impacts using two widely used routing schemes, namely epidemic routing and PROPHET routing. Using simulation as well as realistic mobility traces, we show that the data forwarding performance degrades significantly as the number of free riders increases. Moreover, we also show that the epidemic scheme is more resilient against black holes, while both schemes are resilient against wormholes. Work on enhancing reliability of DTN routing is still undergoing, and we plan to report the results in the near future.

5. REFERENCES

[1] Crawdad project. http://crawdad.cs.dartmouth.edu/.

[2] Ucsd wtd project. http://sysnet.ucsd.edu/wtd/.

[3] A. Lindgren, A. Doria, and O. Schelen. Probabilistic routing in intermittently connected networks. *Mobile Computing and Communications Review*, 7(3):19–20, July 2003.

[4] A. Vahdat and D. Becker. Epidemic routing for partially-connected ad hoc networks. Technical Report CS-2000-06, Duke University, 2000.

[5] Z. Zhang. Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: Overview and challenges. *IEEE Comm. Surveys and Tutorials*, 8(1):24–37, 2006.