Rate Limiting Against Mitigating Attacks

[1]P.Saranya II ME CSE [2] A.V.Shanthini II ME CSE

[3] Dr.S.Uma Prof and Head, PG Department of CSE, Hindusthan Institute of Technology, Coimbatore.

Abstract -- Most routing protocols in disruption tolerant networks use redundant transmissions to explore the diversities in routing paths in order to reduce data transmission delay. However mobile nodes in DTN usually have limited energy and may prefer fewer transmissions for longer lifetime. Hence, it is vital to carefully balance the tradeoff between data transmission delay and the amount of transmissions among mobile nodes. We consider the problem to route a batch of data packets in DTN. By making an analogy between the routing protocol and lower density erasure codes, we investigate the information-theoretical optimal number of transmission in delivering data. With extensive theoretical analysis and simulations, we show that network coding facilities a better tradeoff between resource usage and protocol performance, and that protocol offers unique advantages over replication-based protocols.

Index Terms : DTN, P- Claim, T – Claim, Flood Attack, Replica Attack, E – NCP

1 INTRODUCTION

Disruption tolerant networks (DTN), or opportunistic networks, represent a class of networks where connections among wireless nodes are not contemporaneous, but intermittent over time. Such networks usually have sparse node densities, with short communication ranges on each node. Connections among nodes may be disrupted due to node mobility, energy–conserving sleep schedules, or environmental interference. In such networks, an opportunistic link may be temporarily established when a pair of nodes “meet” – when they move into the communication ranges of each other. A possible data propagation path from the source to the destination, referred to as an opportunistic path, is composed of multiple opportunistic links, possibly established over different time instances. Clearly, more than one such opportunistic paths may exist.

In DTNs, a source may transmit data directly to its destination when they are connected by an opportunistic link. Although such a direct-transmission protocol consumes the minimum amount of network resources, it may incur an exceedingly long transmission delay. On the other extreme, epidemic routing has been proposed to flood data packets to all nodes in the network, essentially exploring all opportunistic paths from the source to the destination, and attaining the shortest data transmission delay. However, most mobile nodes in DTNs have limited energy and may prefer fewer transmissions than flooding to conserve energy, and to prolong network lifetime. For these reasons, probabilistic routing and spray-and-wait, are proposed to achieve tradeoffs between network resource consumption and protocol performance by focusing on routing a single packet in a network with unlimited bandwidth and node buffer capacity.

Motivated by the need to transmit a large amount of data such as a file in DTN, we consider the DTN routing problem under more realistic network settings, where limited transmission opportunities and rely buffers are insufficient to accommodate all data to be transmitted. We observe that there exists an analogy between DTN routing and erasure codes, as the amount of transmissions in DTNs is similar to the density of erasure codes. The existence and optimality of low density erasure codes indicates the existence of an information theoretical optimal number of data transmissions in DTNs.

Randomized network coding allows intermediate nodes to perform coding operations besides simple replication and forwarding. Using the paradigm of network coding in DTN routing, a node may transmit a coded packet as a random linear combination of existing data packets to another node when the opportunity arises. Intuitively, when replication is used to minimize transmission delay, a node should transmit a packet with the minimum number of replicas in the network, since it is the packet with the longest expected delay. Unfortunately, one does not have precise global knowledge of which packet has the minimum number of replicas in opportunistic networks. When network coding is used, however a node can transmit a coded packet as a combination of all packets in its buffer such that their information can be propagated simultaneously to the destination.

2 RELATED WORKS

The variety of routing protocols has been designed for disruption tolerant networks, based on different sets of assumptions. Some assume a prior knowledge on connectivity patterns, or the historical patterns can be used to predict future message delivery probabilities. Others assume control over node mobility. We propose a network coding based efficient routing protocol with neither a priori knowledge of network connectivity, nor control over node mobility.

Previous studies have proposed to use erasure coding to address network disruptions in DTNs, with no information of node mobility patterns, or with prior knowledge of network topologies. Unlike network coding, in such source based erasure coding approaches, different upstream nodes may transmit duplicates of coded data to the same node, and may unnecessarily consume additional bandwidth.

It has been shown that network coding can improve the throughput in wireless communication, by exploring the broadcast nature of the wireless medium. However, in disruption tolerant networks considered , a node seldom has more than one neighbors, and such wireless coding

IJSER

opportunities rarely occur. The protocol based on network coding can broadcast multiple messages among nodes with a shorter period of time, compared to that without network coding.

2.1 Network Model

We consider unicast communication from a source to a destination in a disruption tolerant network with N wireless nodes, moving within constrained area. The source has K packets to be transmitted to the destination. A transmission opportunity arises when a pair of nodes “meet”, they are within the communication range of each other. To facilitate the analysis without loss of generality, we assume that when nodes a and b meet, the transmission opportunity is only sufficient to completely transmit one data packet. With respect to the buffering capacities, while the source and the destination are able to accommodate all K packets, we assume that the buffer on each of the immediate relay nodes is only able to hold B packets.

We assume that the time between two consecutive transmission opportunities is exponentially distributed with a rate. In the Literature, the majority of previous work makes such an assumption, either explicitly or implicitly. Although measurement based studies have shown that such inter-meeting time may follow heavy tail distributions in some applications, more recent studies have shown that the exponential distributions is in fact more prevalent both in theory and in many practical system. With a similar preference for mathematical tractability, we assume that there does not exist background traffic beyond the unicast communication under consideration, and leave the more general case background traffic to our future work. We opt for more mathematically tractable models in our analysis, and believe insights obtained from our analysis.

2.2 Security Model

There are two types of nodes: misbehaving nodes and normal nodes. A misbehaving node drops the received packets even if it has available buffers,1 but it does not drop its own packets. It may also drop the control messages of our detection scheme. We assume a small number of misbehaving nodes may collude to avoid being detected, and they may synchronize their actions via out-band communication channels. A normal node may drop packets when its buffer overflows, but it follows our protocol. In some DTN applications, each packet has a certain lifetime, and then expired packets should be dropped whether or not there is buffer space. Such dropping can be identified if the expiration time of the packet is signed by the source. Such dropping is not misbehavior, and will not be considered in the following presentations.

We assume a public-key authentication service is available. For example, hierarchical identity-based cryptography has been shown to be practical in DTNs. In identity-based authentication, only the offline trusted private key generator can generate a public/private key pair, so a misbehaving node itself cannot forge node identifiers (e.g., to launch Sybil attacks). Generally speaking, a node’s private key is only known by itself; however, colluding nodes may know each other’s private key.

2.3 The Effect of Flood Attacks

To study the effect of flood attacks on DTN routing and motivate our work, we run simulations on the MIT Reality trace [17] (see more details about this trace in Section 7). We consider three general routing strategies in DTNs. 1) Single-copy routing after forwarding a packet out, a node deletes its own copy of the packet. Thus, each packet only has one copy in the network. 2) Multicopy routing the source node of a packet sprays a certain number of copies of the packet to other nodes and each copy is individually routed using the single-copy strategy. The maximum number of copies that each packet can have is fixed. 3) Propagation routing when a node finds it appropriate to forward a packet to another encountered node, it replicates that packet to the encountered node and keeps its own copy. There is no preset limit over the number of copies a packet can have. In our simulations, Propagation is used as representatives of the three routing strategies, respectively. In Propagation, a node replicates a packet to another encountered node if the latter has more frequent contacts with the destination of the packet.

Two metrics are used; the first metric is packet delivery ratio, which is defined as the fraction of packets delivered to their destinations out of all the unique packets generated. The second metric is the fraction of wasted transmissions. The higher fraction of wasted transmissions, the more network resources is wasted. We noticed that the effect of packet flood attacks on packet delivery ratio has been studied by Burgess et al. using a different trace. Their simulations show that packet flood attacks significantly reduce the packet delivery ratio of single-copy routing but do not affect propagation routing much. However, they do not study replica flood attacks and the effect of packet flood attacks on wasted transmissions.

3 OUR WORK

We demonstrate the advantage of E-NCP and validate our theoretical analysis by experiments. We have developed a discrete-event simulator with the implementation of network coding, the original epidemic routing based protocols, and our efficient protocols. To mitigate randomness in simulations, we show for each data point in all network.

The average number of rely transmissions and the transmission delay as functions of the maximal spray counter. We set the maximal spray counters for all source packets to be identical and vary the value from 1 to 36.

The amount of relay transmissions increases linearly as the maximal spray counter increases, matching perfectly with the analytically result of which is omitted in the figure for clarity. We investigate the impact of the relay buffer size from 1 to 20. We further set the number of pseudo source packets to 105 in E-NCP. All the other settings are the same as the previous experiments. This confirms our analysis in Sec. VI-B that the relay buffer sizes can be very small for E-NCP, On the othr hand, the transmission delay of E-RP increases dramatically when the relay buffer size is smaller than 10 as shown by both simulation result and the analytical lower bound.

3.1 Packet Forwarding Scheme Algorithm (Claim-carry-and-check)

To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. However, since the node may send its packets to any node it contacts at any time and place, no other node can monitor all of its sending activities. To address this challenge, our idea is to let the node itself count the number of unique packets that it, as a source, has sent out, and claim the up-to-date packet count (together with a little auxiliary information such as its ID and a timestamp) in each packet sent out. The node's rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L. If an attacker is flooding more packets than its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of attack. The claimed count must have been used before by the attacker in another claim, which is guaranteed by the pigeonhole principle, and these two claims are inconsistent. The nodes which have received packets from the attacker carry the claims included in those packets when they move around. When two of them contact, they check if there is any inconsistency between their collected claims. The attacker is detected when an inconsistency is found.

4 CONCLUSION

We demonstrate the analogy between DTN routing and erasure codes. Based on this insight, we explore the information-theoretical optimal scaling of data transmission, and propose an efficient network coding based protocol that significantly decreases the amount of resource used in transmitting a batch of data packets, while only increasing the data transmission delay slightly. We evaluate the proposed E-NCP protocol with extensive analysis and simulation. Our theoretical analysis results yield further insights into the difference between coding based and replication based protocols, and provides guidelines in tuning protocol parameters to attain the best tradeoff to accommodate a diverse set of application requirements.

REFERENCES

[1] S. Jain, K. Fall, and R. Patra, "Routing in a Delay Tolerant Network," in Proc.of ACM SIGCOMM, 2004.

[2] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc. IEEE INFOCOM, 2006, pp. 1–11.

[3] W. Gao and G. Cao, "User-centric data dissemination in disruption tolerant networks," in Proc. IEEE INFOCOM, 2011, pp. 3119–3127.

[4] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in Proc. ACM MobiHoc, 2007, pp. 32–40.

[5] V. Erramilli, A. Chaintreau,M. Crovella, and C. Diot, "Delegation forwarding," in Proc. ACM MobiHoc, 2008, pp. 251–260.

[6] N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," Pers. Ubiquitous Comput., vol. 10, no. 4, pp. 255–268, 2006.

[7] J. Burgess, G. D. Bissias, M. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in Proc. ACM MobiHoc, 2007, pp. 61–70.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp. 255–265.

[9] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: Self-organized network- layer security in mobile ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 261–273, 2006.

[10] S. Buchegger and Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in Proc. MobiHoc, 2002, pp. 226–236.

[11] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp. 27-34, 2003.

[12] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM, 2005.

[13] M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. MobiCom, pp. 243-257, 2005.

[14] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[15] S.J.T.U.Grid Computing Center, "Shanghai Taxi Trace Data," http://wirelesslab.sjtu.edu.cn/, 2012.

[16] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[17] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.

IJSER

IJSER

IJSER

IJSER