

An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-hoc Networks

Chao-Chin Chou, *Student Member, IEEE*, David S. L. Wei, *Member, IEEE*,
C.-C. Jay Kuo, *Fellow, IEEE*, and Kshirasagar Naik, *Member, IEEE*

Index Terms

peer-to-peer, P2P, anonymity, MANET.

I. INTRODUCTION

THE Peer-to-peer (P2P) network has drawn increasing attention nowadays, and has been widely deployed on the Internet for various purposes, including distributed data storages, file sharing networks, collaborative computing and Internet telephony. The P2P system is popular for its being scalable, fault-tolerant, and self-organized. Meanwhile, mobile ad-hoc networks (MANETs) have been proposed as an alternative to cellular networks for use in areas where fixed infrastructures such as base stations are unavailable. MANET resembles the P2P network in some ways. First, both systems lack fixed infrastructure and network topology. The P2P peers join and leave frequently and unpredictably, while MANET nodes move randomly. Second, both systems require no centralized coordinator for communication. Instead, they both require the cooperation of network nodes for communication. MANET is now emerging as a new paradigm of wireless communication for civilian applications. Nowadays, numerous portable devices such as laptops, PDAs and mobile phones are everywhere, and people use them for their professional and daily lives. The materialization of wireless technologies has changed the scenario of ad-hoc networking, its usage, its players, as well as its importance. Therefore, MANET appears to be an attractive platform for the P2P applications. In fact, P2P applications on Internet are gradually migrating to MANET [1][2][3][4]. Emerging P2P applications over MANET include (1) sharing multimedia files among mobile hand-held devices, (2) sharing traffic, weather and traveling information among moving vehicles, and (3) sharing real-time information among military units on the battlefield.

Providing peer privacy in the P2P network has always been an important topic, which poses even more challenges when facing a P2P system over MANET. First, the open environment in MANET makes its radio signals vulnerable to eavesdropping. Second, the multihop communication in MANET involves untrustworthy nodes in a private conversation. Third, MANET nodes are constrained by limited battery and computing power, which makes computation-intensive schemes such as the public-key cryptography too expensive to be adopted. Therefore, existing solutions for wireline Internet cannot be applied directly on MANET for P2P communication without considerable modifications.

We present the *MANET Anonymous Peer-to-peer Communication Protocol* (MAPCP), which serves as an efficient anonymous communication protocol for P2P applications over MANET. MAPCP is designed to be a flexible middleware between the P2P applications and MANET routing protocols. MAPCP employs a broadcast-based mechanism together with a probabilistic-based flooding control algorithm to establish anonymous paths between peers, which requires no hop-by-hop encryption/decryption, hence requires lower computational complexity and power consumption. MAPCP establishes multiple anonymous paths between communication peers within a single query phase, and is highly resilient to node mobility, failure, and malicious attacks. Furthermore, MAPCP provides schemes for communication peers to control the tradeoff between anonymity degree and bandwidth efficiency.

REFERENCES

- [1] G. T. Marco Conti, Enrico Gregori, "A cross-layer optimization of gnutella for mobile ad hoc networks," in *Proc. ACM MobiHoc'05*, 2005, pp. 343–354.
- [2] D. P. T. G. C. T. S. F. Z. S. Gerd Kortuem, Jay Schneider, "When peer-to-peer comes face-to-face: Collaborative peer-to-peer computing in mobile ad hoc networks," in *Proc. IEEE P2P'01*, 2001.
- [3] B. B. Gang Ding, "Peer-to-peer file-sharing over mobile ad hoc networks," in *Proc. IEEE PERCOMW'04*, 2004.
- [4] C.-C. S. Duran Ahmet, "Mobile ad hoc p2p file sharing," in *Proc. IEEE WCNC'04*, 2004, pp. 114–119.

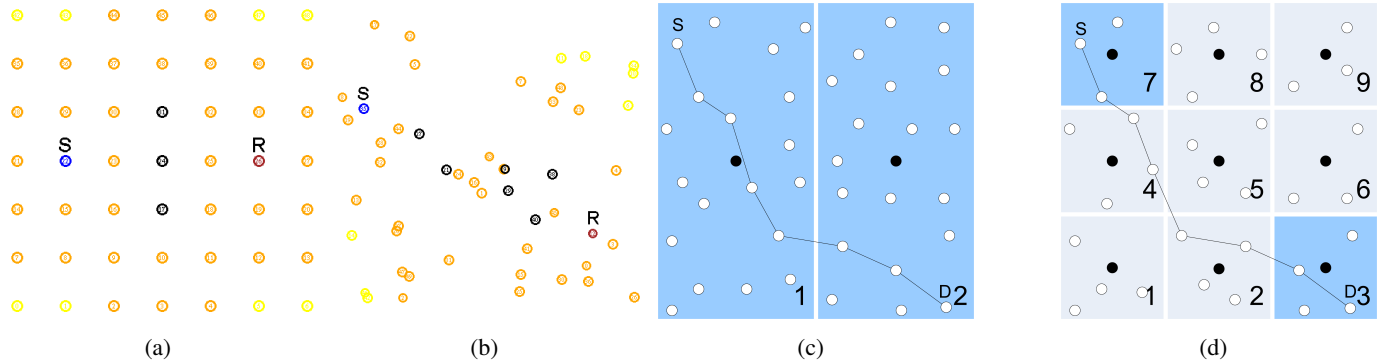


Fig. 1. Probability assignment results of flooding control in (a) a grid topology, and (b) a randomly generated topology in the 700m-by-700m network field. S is the sender, and R is the receiver. (c)(d) By traffic analysis such as timing analysis and payload matching, colluded attackers (represented by black nodes) can divide the network space into smaller cells and shrink the anonymity set into a specific cell.

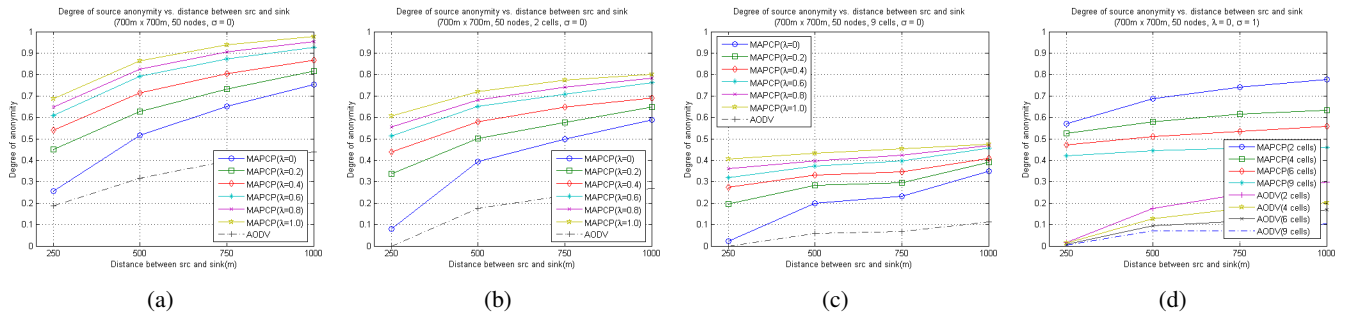


Fig. 2. Degree of anonymity in the 700m-by-700m field divided into (a) 1 cell, (b) 2 cells, and (c) 9 cells. (d) Degree of anonymity with a larger α value.

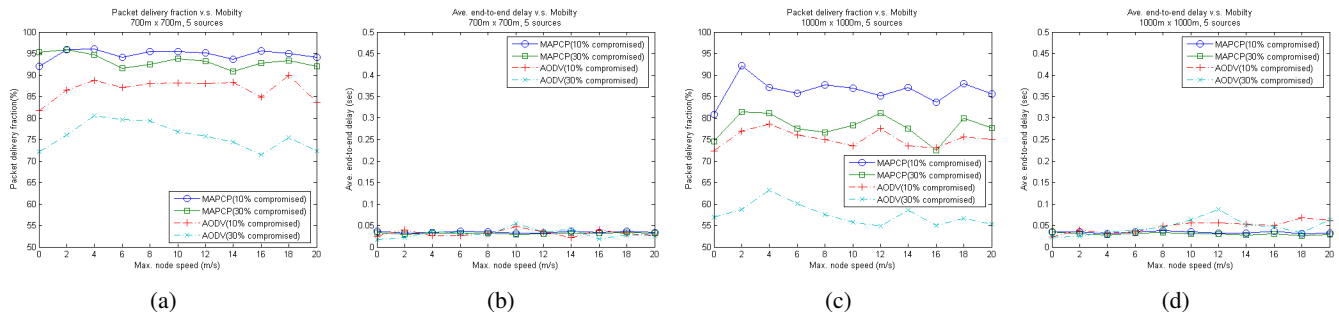


Fig. 3. Simulation results in the hostile environments. The packet delivery fraction and end-to-end delay in (a)(b) the 700m-by-700m field and (c)(d) the 1000m-by-1000m field.