Abstract

The emanate of extremely powerful mobile communication devices in recent times has elicit the development of many exploitative technologies that attempt at leveraging the ever increasing processing, storage and communicating capacities of these devices. One of the most developing areas of network is opportunistic network that provides communication even in disconnected mode. Nodes are mobile and can change their location and message or packet is forward through many intermediate nodes so identity of users is shown to all. Any intermediate can drop the data packets if the node is malicious and do not wishes to forward the data to a particular destination id. A few privacy preventing algorithms are proposed to maintain it. In this research an algorithm is proposed to maintain the privacy of user if user wants it. Stable node provides a new virtual ID to a user who wishes to communicate without disclosing his privacy. This research ensures the privacy of the data with the use of concept of cluster estimation. In this research the public private cryptography technique is used for data encryption and decryption. Algorithm is implemented on NS2 (Network Simulator 2. 35).
- A. Pentland, R. Fletcher, and A. A. Hasson, A road to universal broadband


**Index Terms**

Computer Science

Security

**Keywords**