

Ostra: Leveraging trust to thwart unwanted communication

Alan Mislove^{†‡}

Ansley Post^{†‡}

Krishna Gummadi[†]

Peter Druschel[†]

[†]Max Planck Institute for Software Systems

[‡]Rice University

SOSP 2007 Work in Progress Session

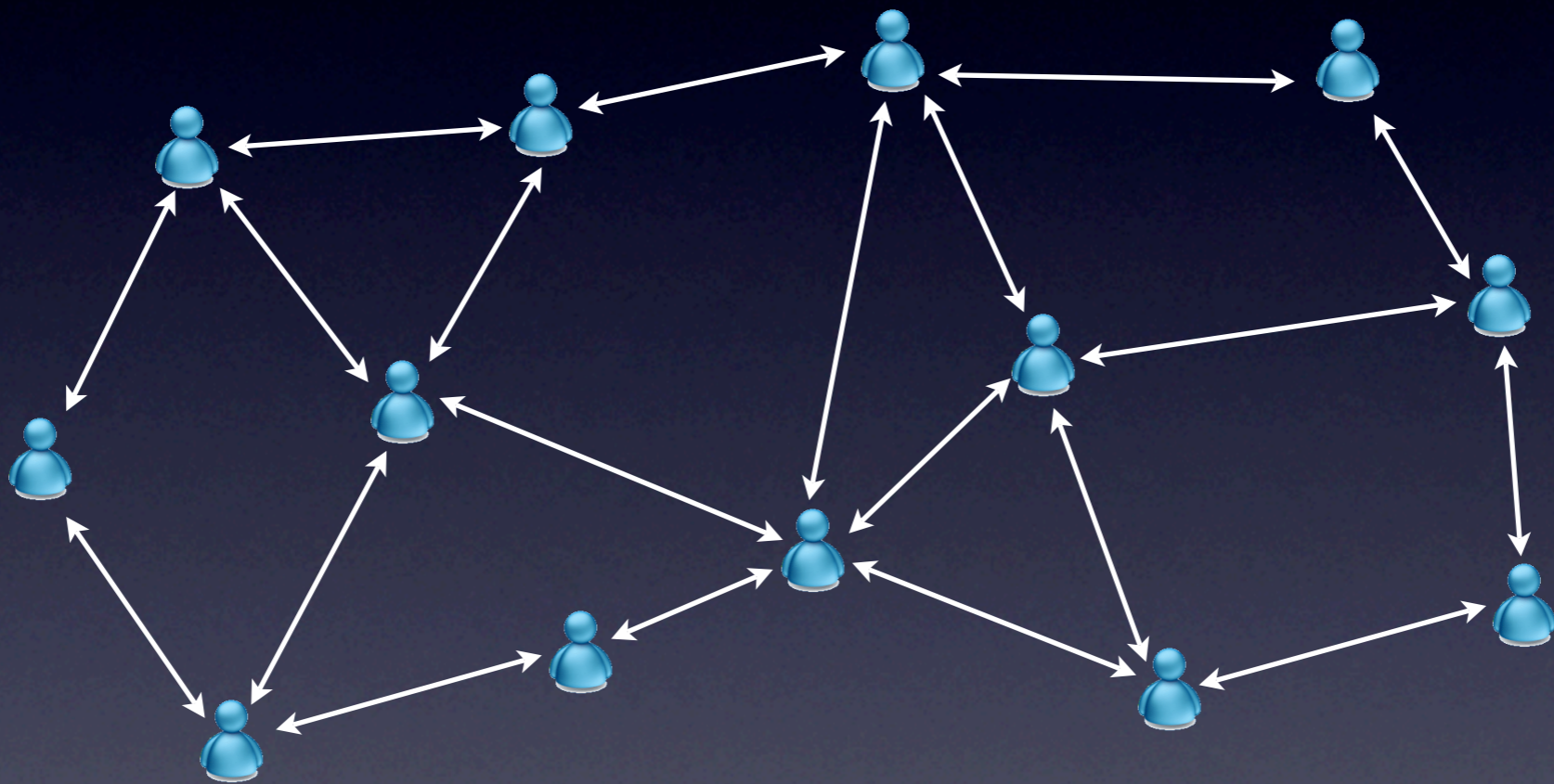
Unwanted communication

- Unwanted communication is a known problem
 - Spam in email
- Spreading to popular emerging systems
 - Example: Mislabeled videos plaguing YouTube
- Usual defenses don't work
 - Content filtering on video content?

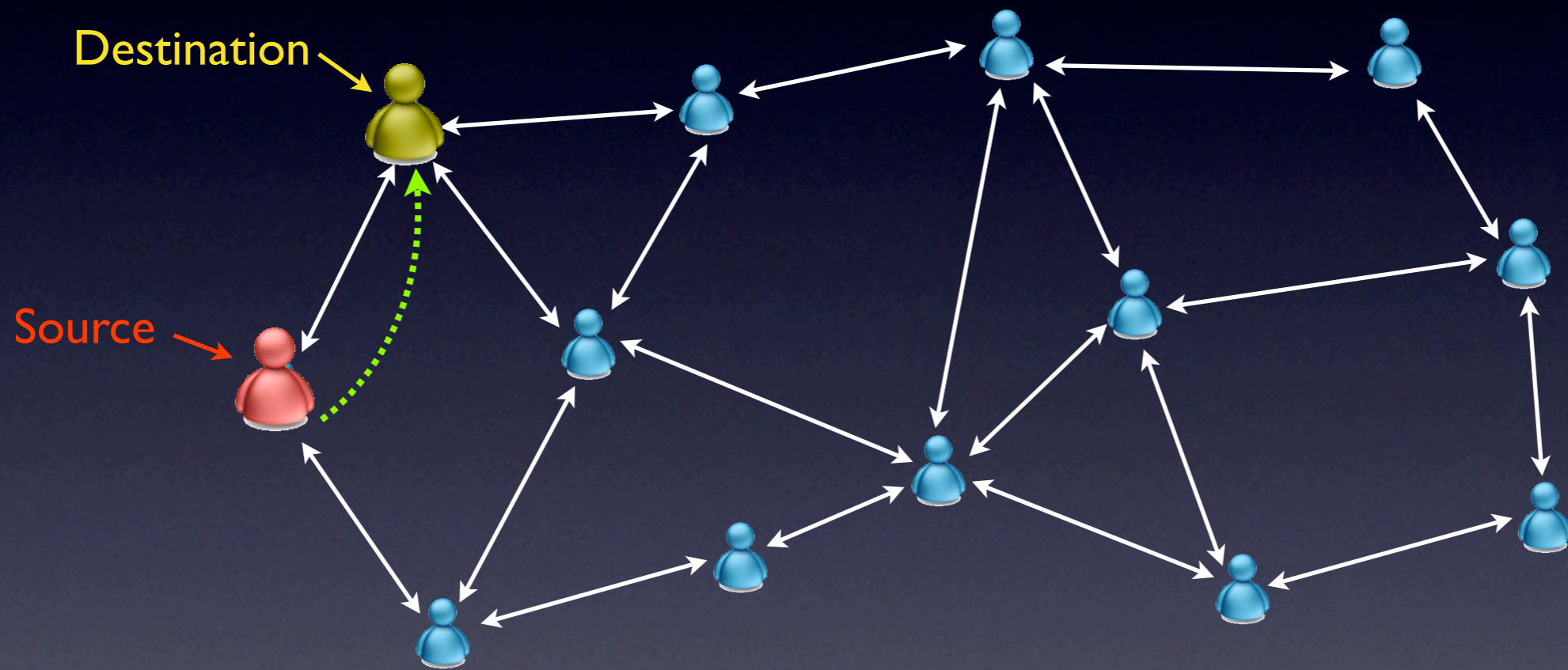
Ostra: A new approach



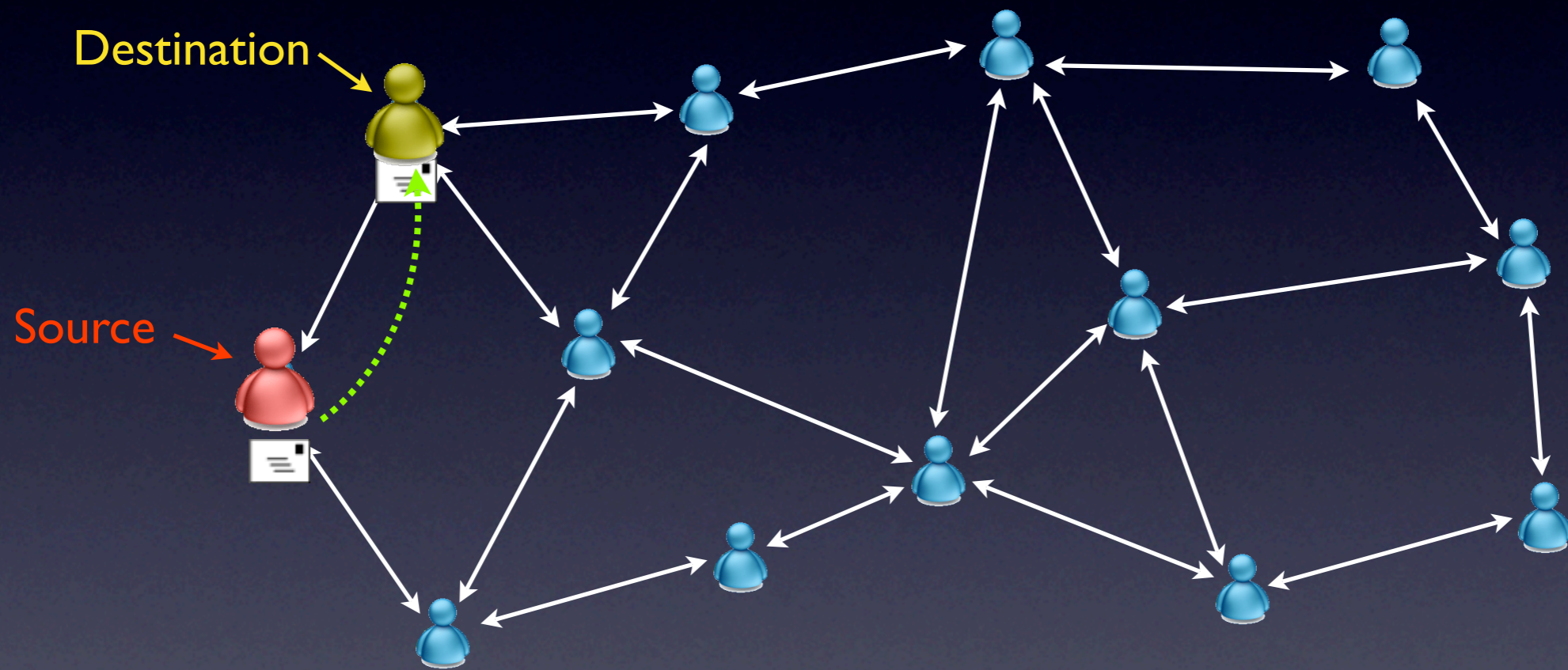
Ostra: A new approach



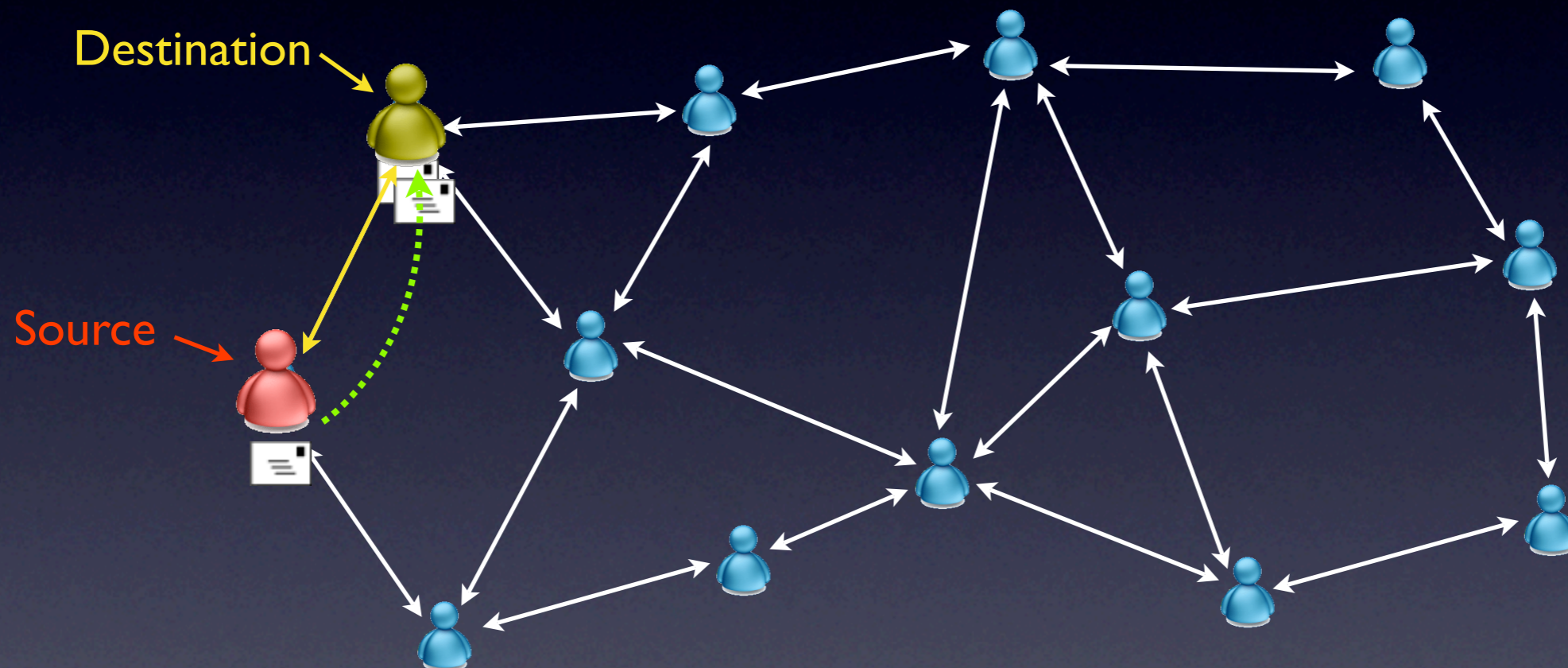
Ostra: A new approach



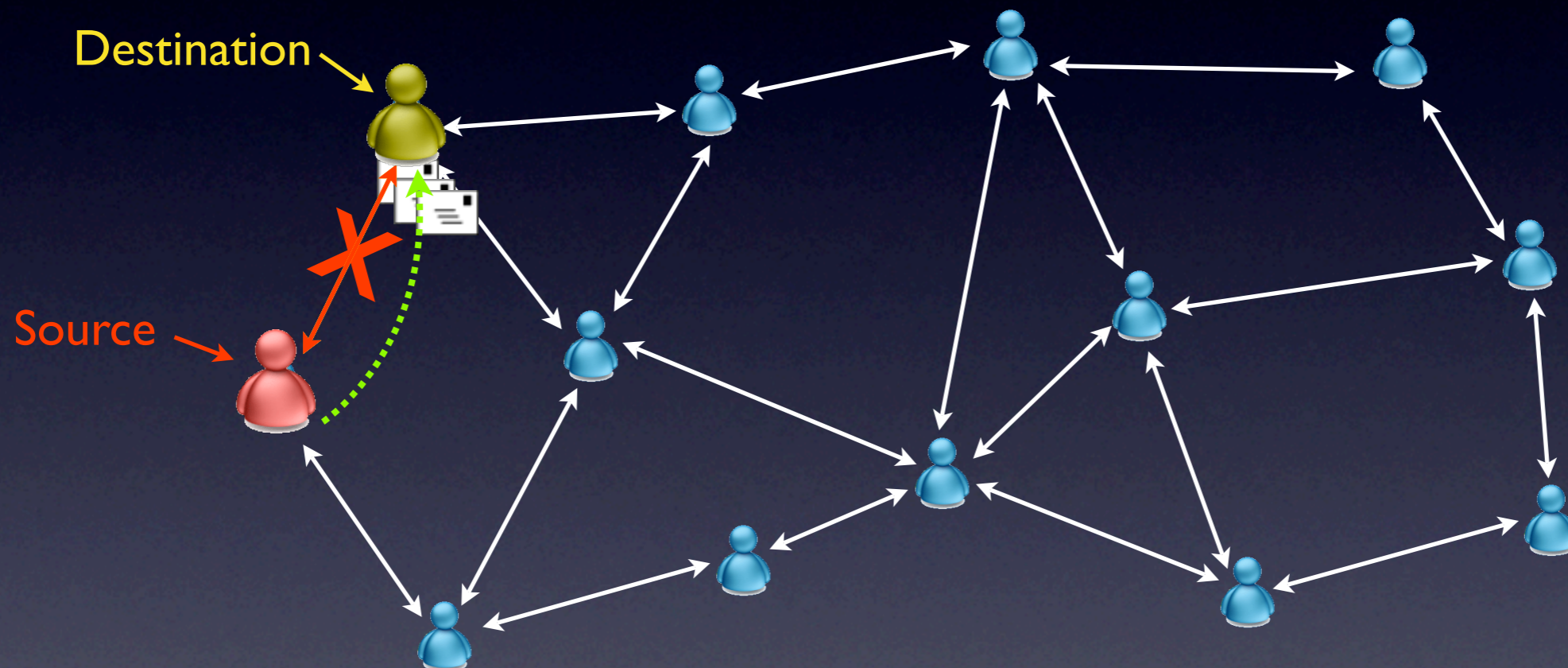
Ostra: A new approach



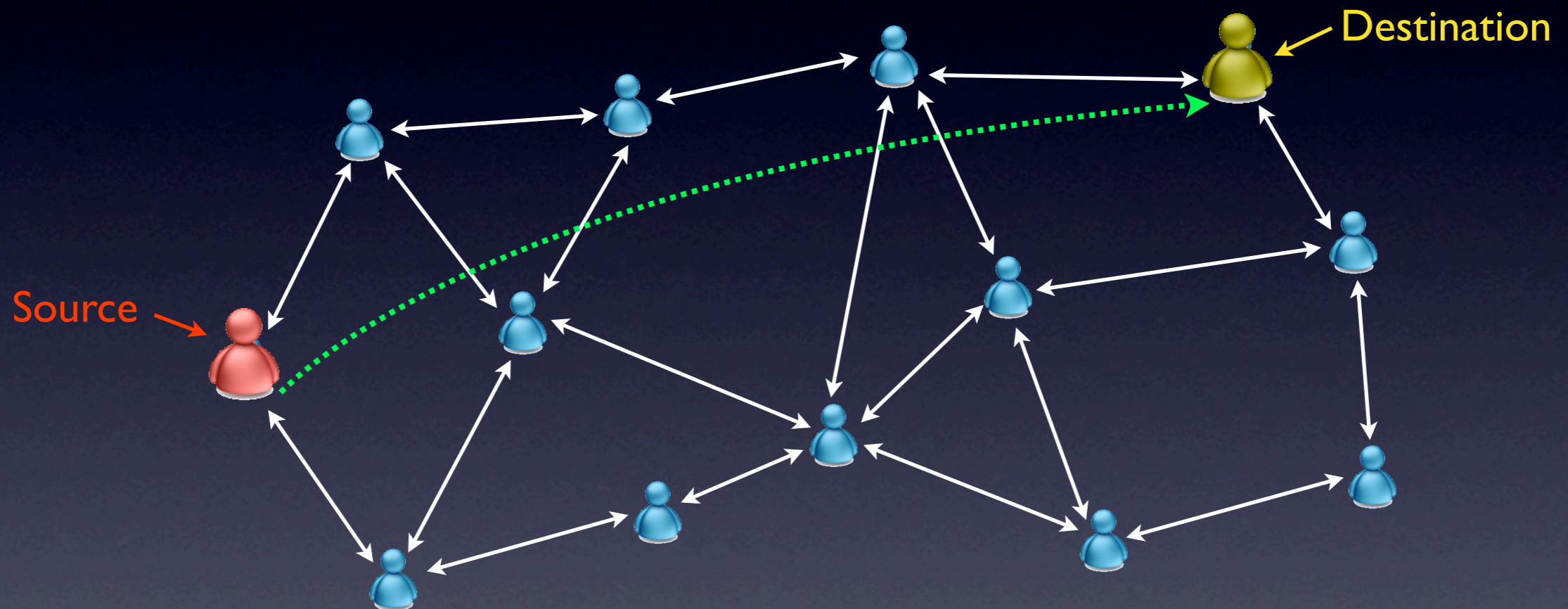
Ostra: A new approach



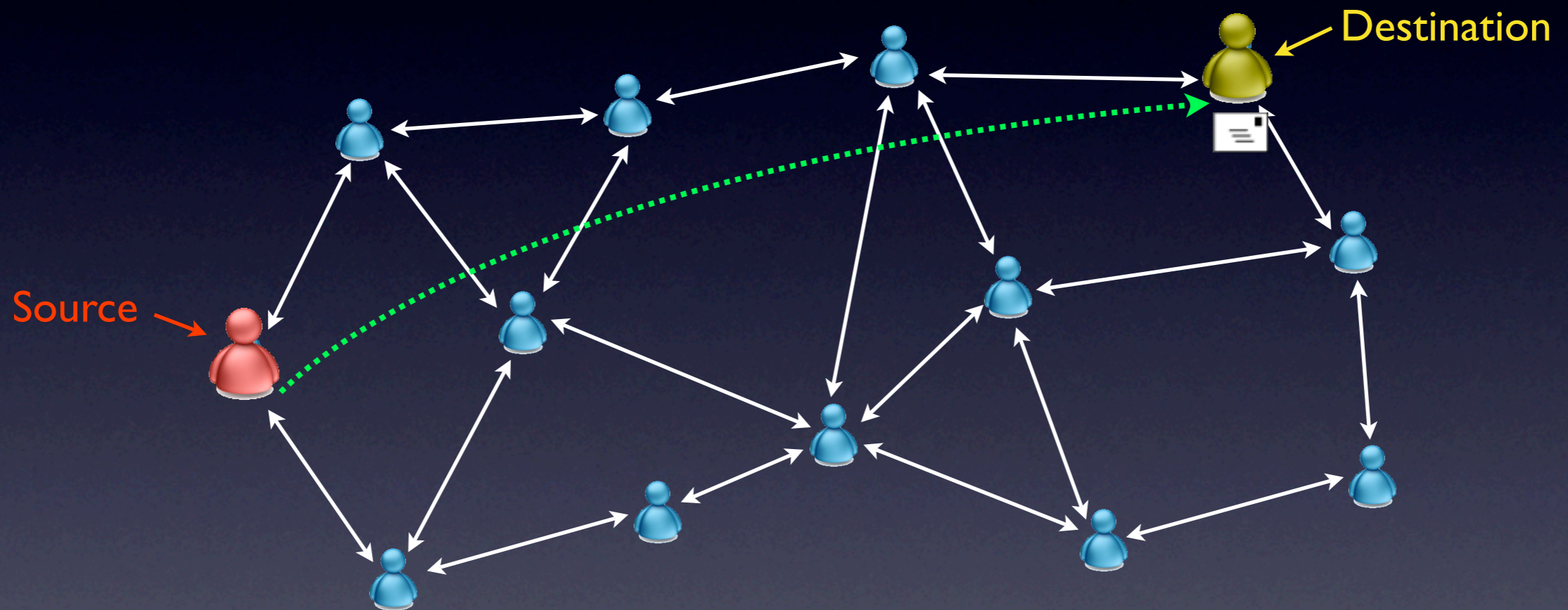
Ostra: A new approach



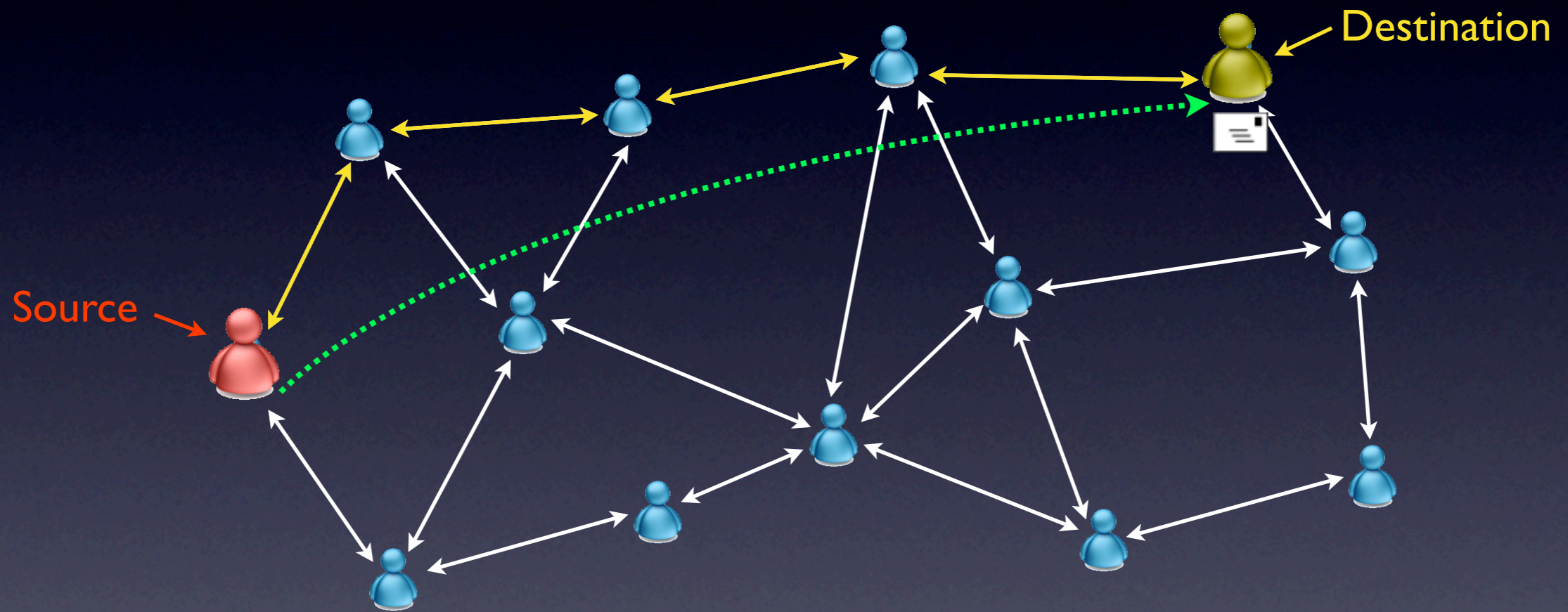
Ostra: A new approach



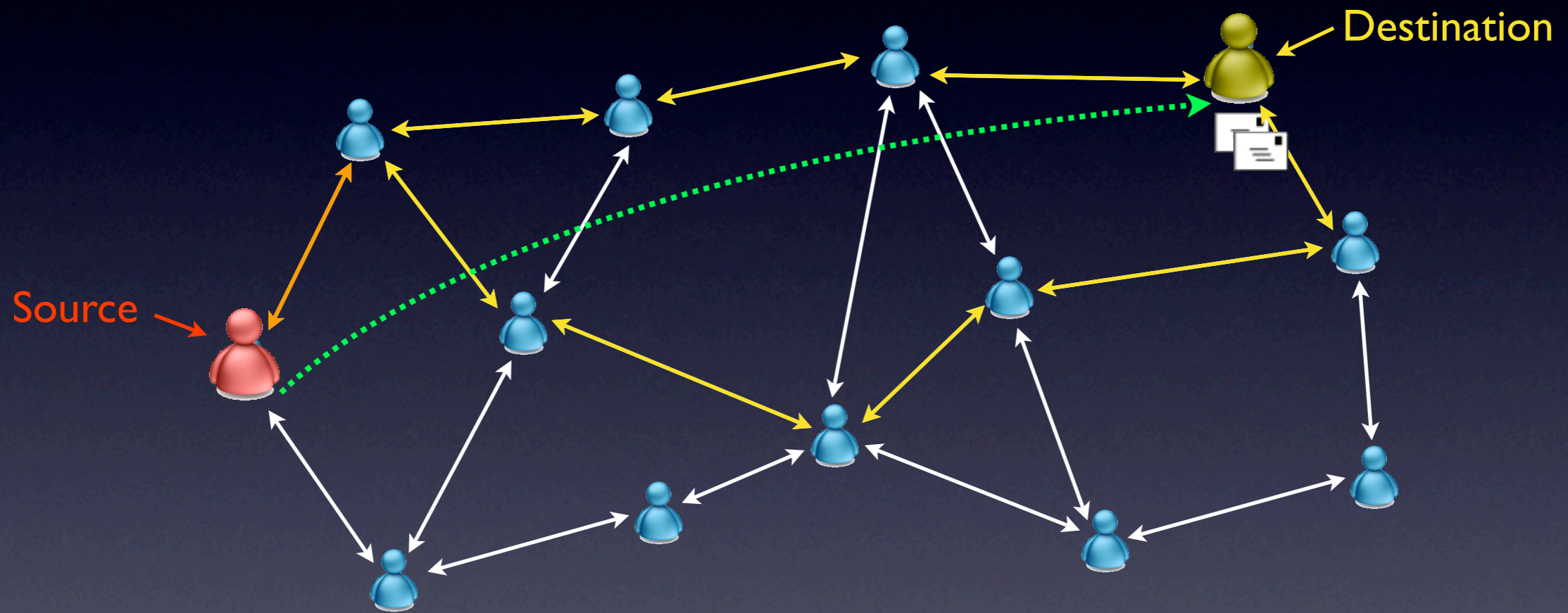
Ostra: A new approach



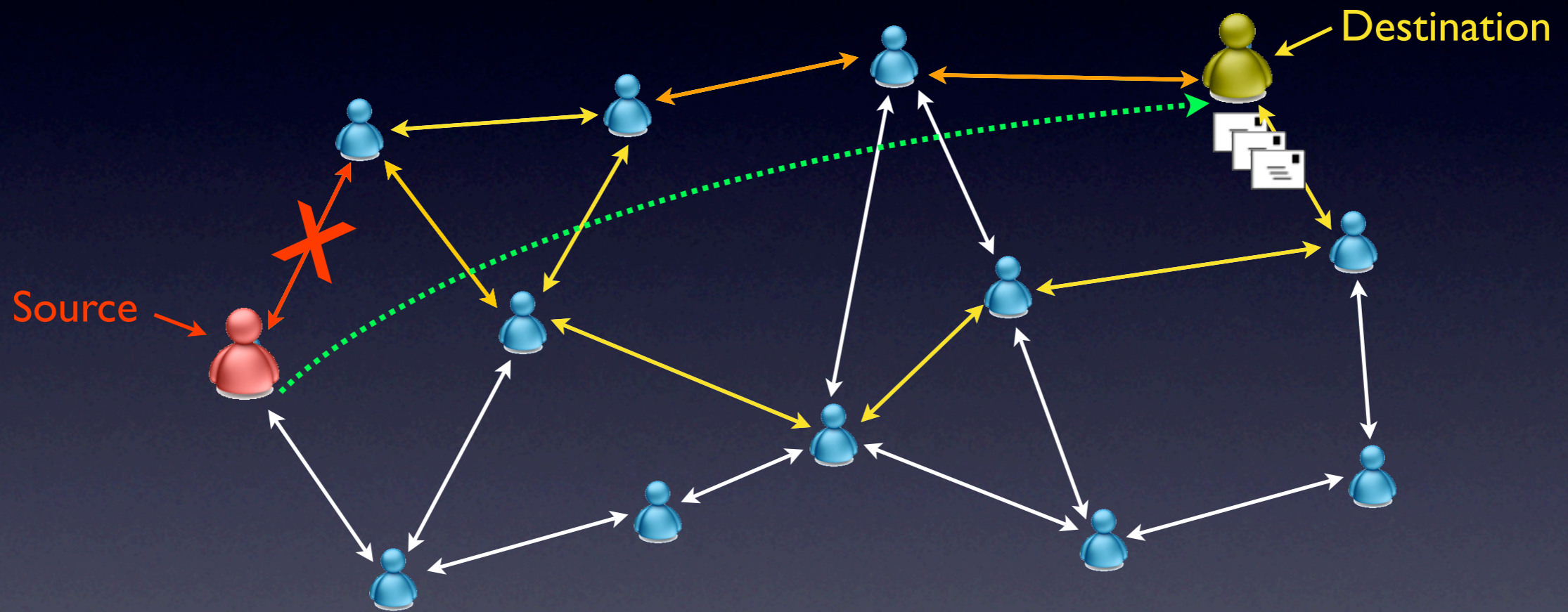
Ostra: A new approach



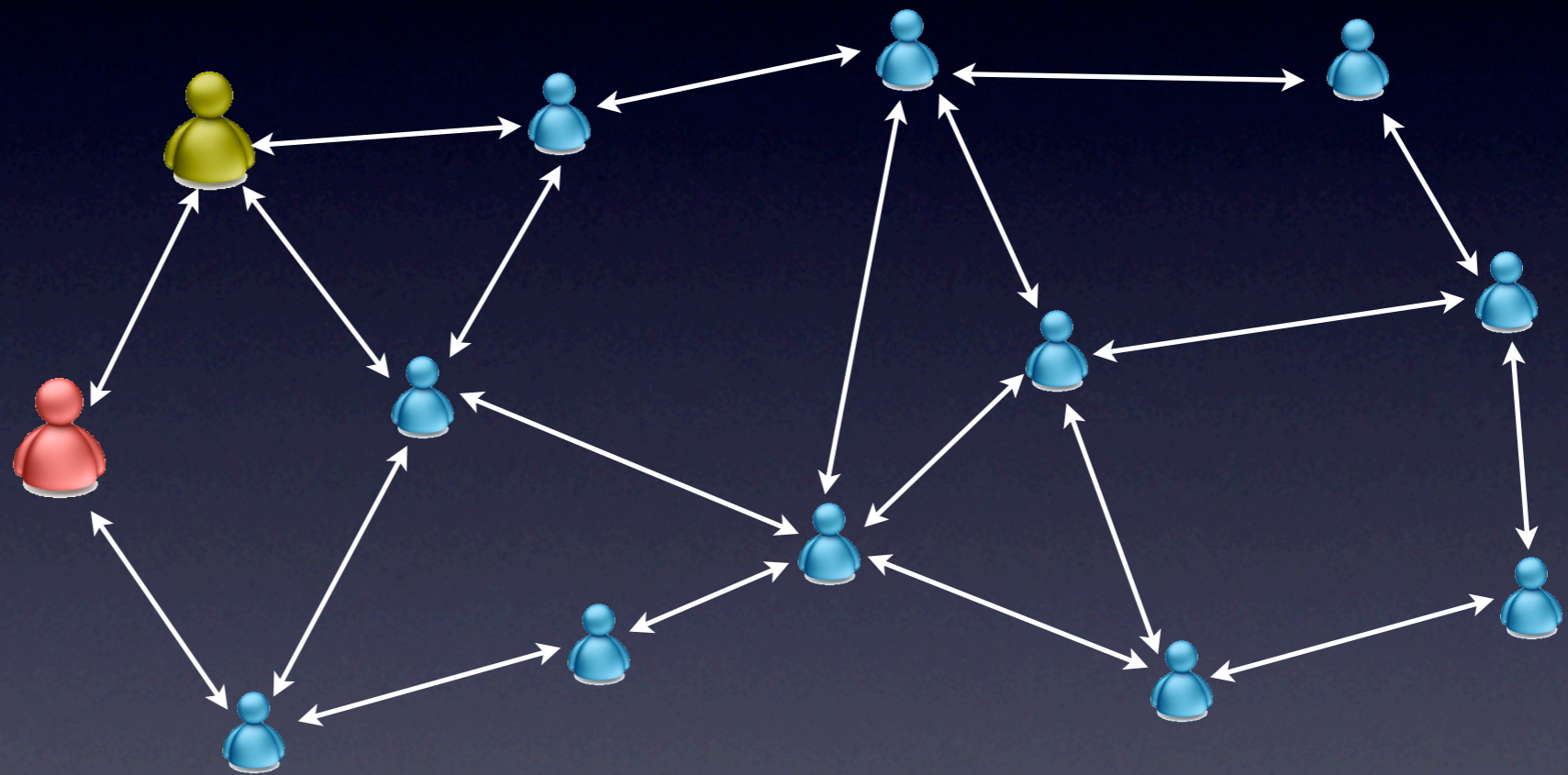
Ostra: A new approach



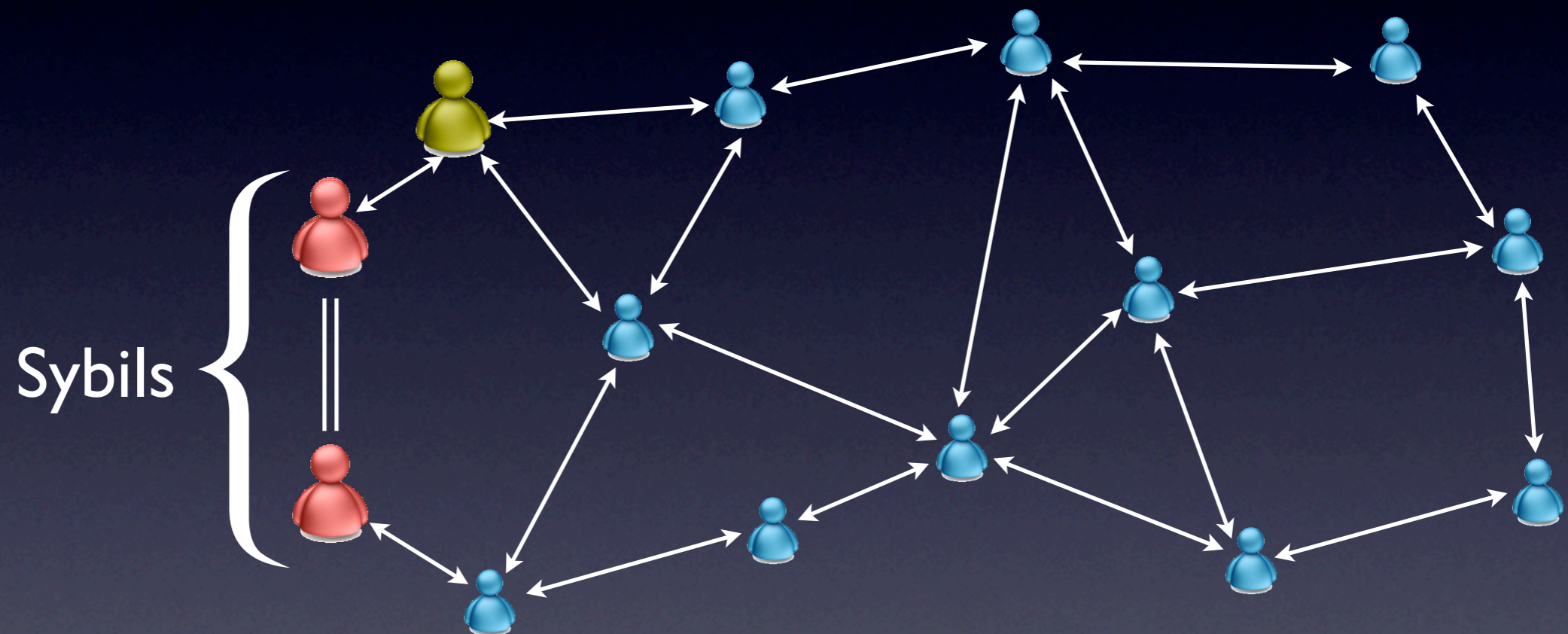
Ostra: A new approach



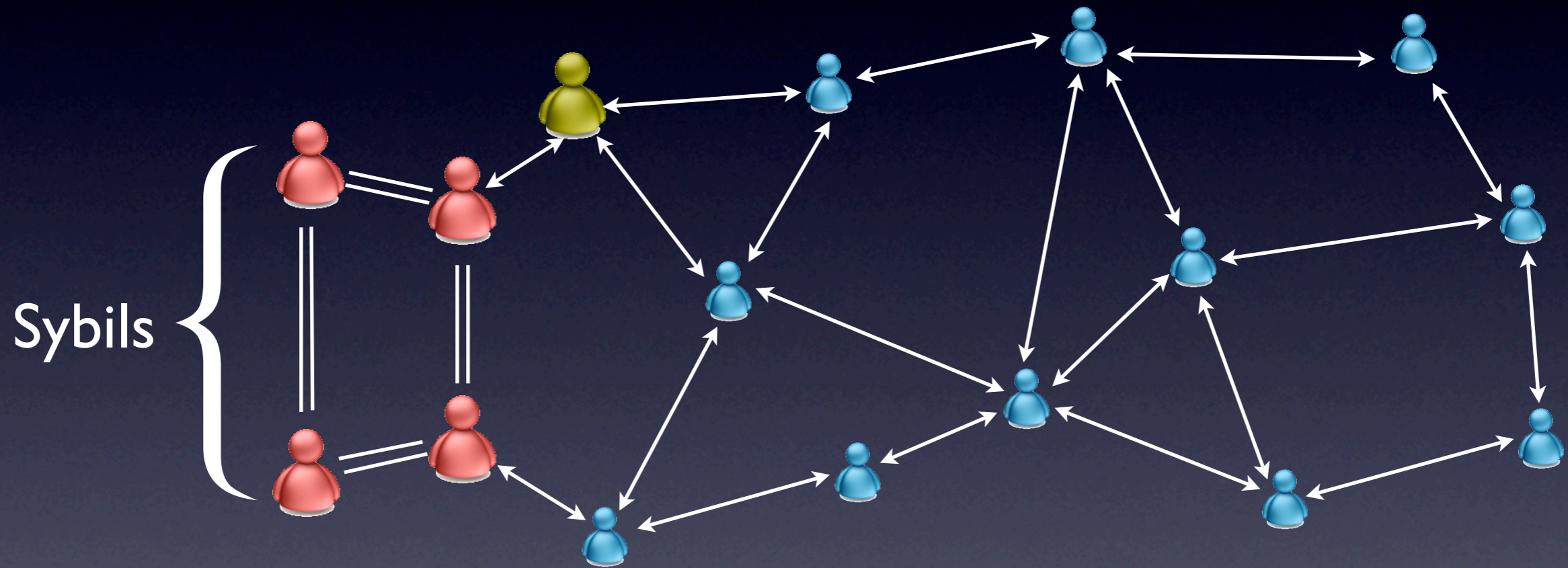
No requirement of strong identities



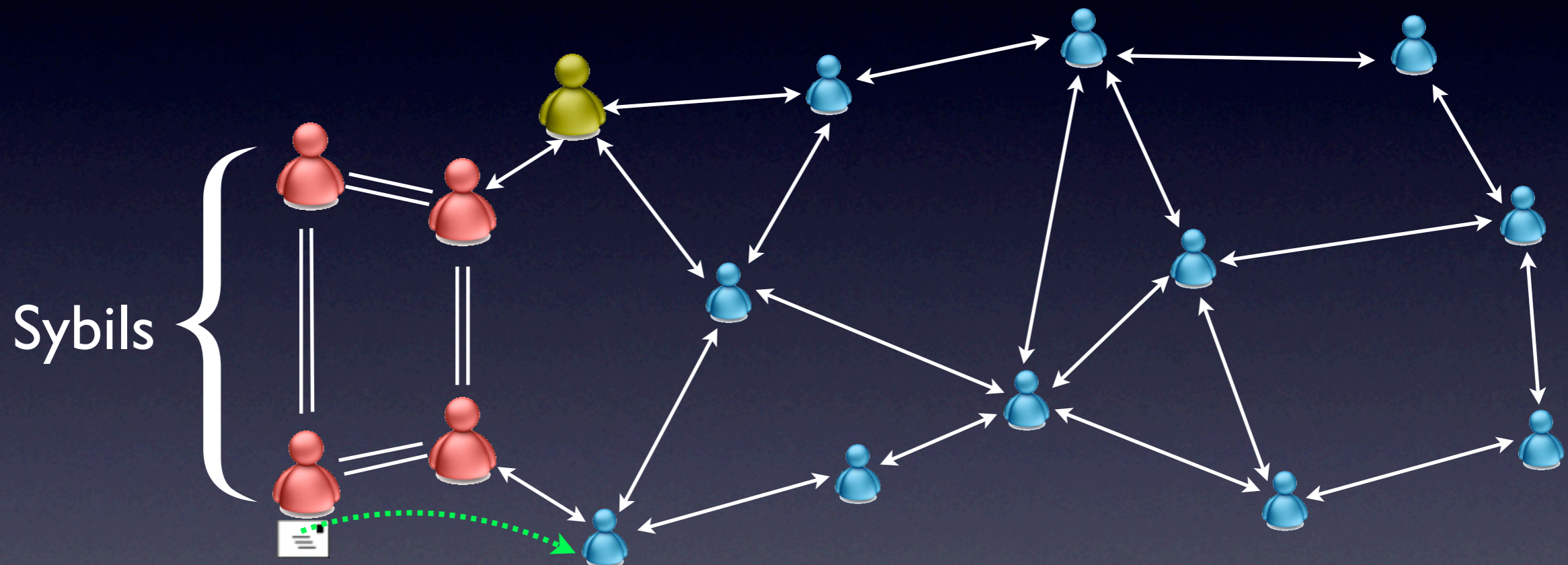
No requirement of strong identities



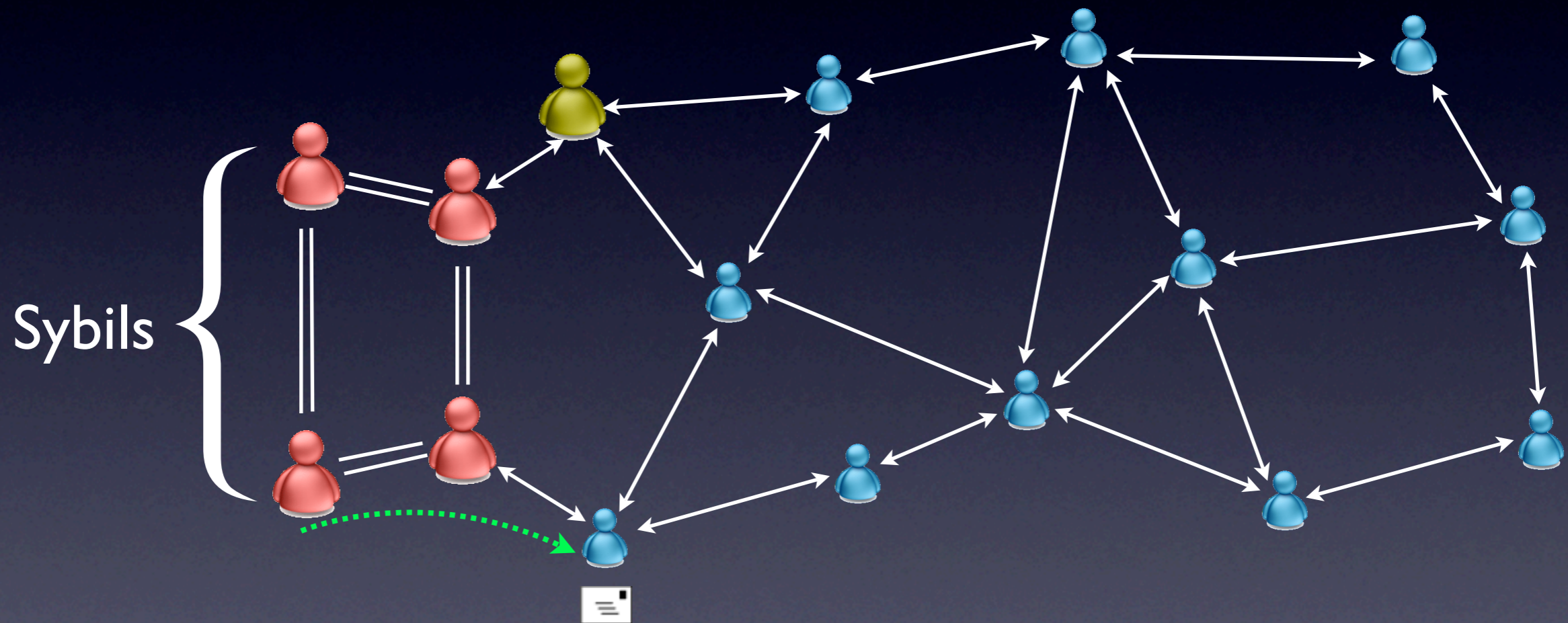
No requirement of strong identities



No requirement of strong identities



No requirement of strong identities



Ostra: Leveraging trust

- We present Ostra, a **new approach**
 - Prevents unwanted communication in an existing system
 - Examples: Email, Skype, IM, YouTube
- Ostra uses the **relationships which exist between users**
 - Often already present (i.e. social networks)
- Ostra has desirable properties
 - Does not require global user identities
 - Does not rely on automatic content classification
 - Respects recipient's notion of wanted/unwanted communication

Thanks!
