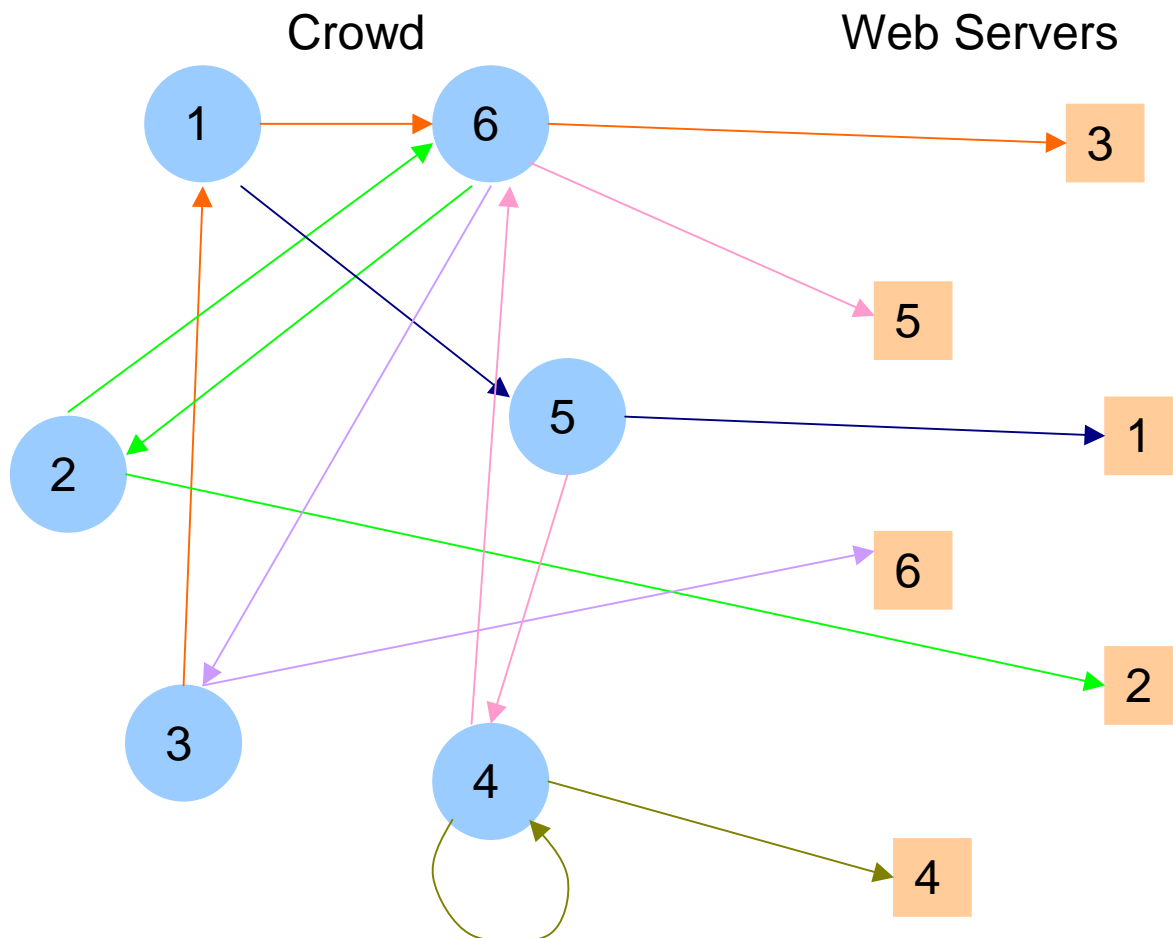


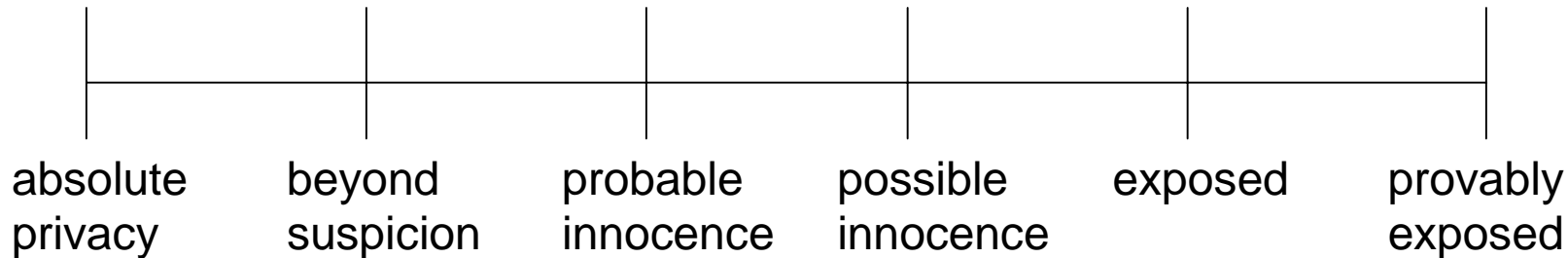
6. Crowds for anonymous Web-Transactions [Reiter/Rubin 1998]

1. user first joins a "crowd" of other users, where he is represented by a "jondo" process on his local machine
 2. user configures his browser to employ the local jondo as a proxy for all new services
 3. user's request is passed to a random member of the crowd
 4. that member can either submit the request directly to the web server or forward it to another randomly (with $p_f > 1/2$) chosen user.
- request is eventually submitted by a random member



Communication between jondos is encrypted by keys shared between jondos

Degrees of Anonymity:



- **Beyond suspicion:** sender appears no more likely to be the originator of a sent message than any other potential sender in the system
- **Probable innocence:** sender appears no more likely to be the originator than not to be the originator
- **Possible innocence:** there is a nontrivial probability that the real sender is someone else

Anonymity properties provided by Crowds:

Attacker	Sender anonymity	Receiver anonymity
local eavesdropper	Exposed	P(beyond suspicion) $\rightarrow 1$ $n \rightarrow \infty$
c collaborating members, $n < \lceil pf / (pf - 1/2) \rceil * (c+1)$	probable innocence, P(absolute privacy) $\rightarrow 1$ $n \rightarrow \infty$	P(absolute privacy) $\rightarrow 1$ $n \rightarrow \infty$
end servers	beyond suspicion	N/A

Limitations:

- Web server's log may record submitting jondo's IP address as the request originator's address
- Request contents are exposed to jondos on the path
- Anonymising service can be circumvented by Java Applets, Active X controls
- Performance overhead (increased retrieval time, network traffic and load on jondo machines)
- No defend against DoS-attacks by malicious crowd members

Comparison to Mixes:

Crowds:

sender anonymity

no protection against global eavesdropper

better performance

Mixes:

unlinkability of sender and receiver

protection against global eavesdropper

n public key encryptions, n private key decryptions (n = number of Mixes on the path)