Part I
PS 3 discussion of SPINS paper

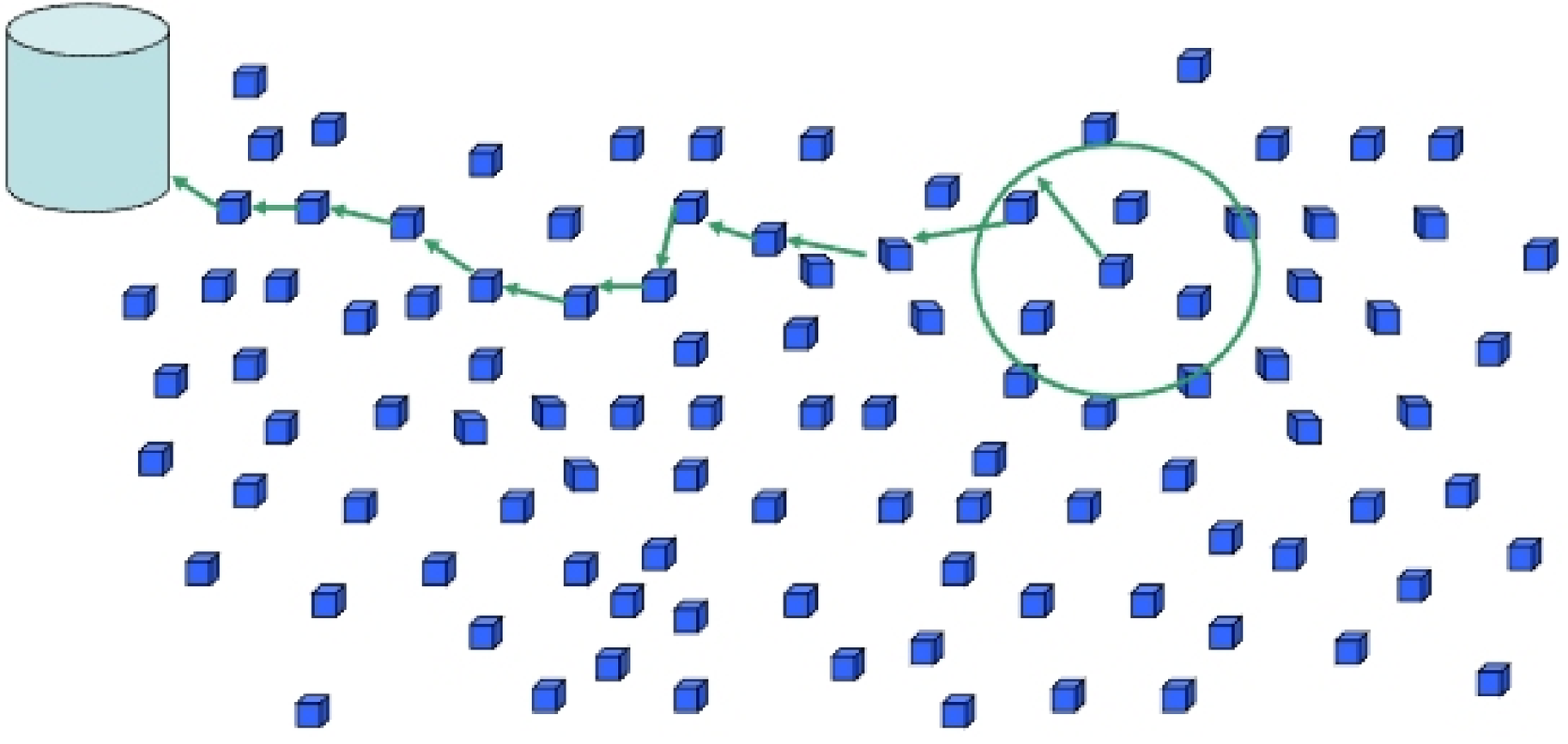
CS 588

February 22, 2005

nate@cs.virginia.edu

Scenario

High-power base station



Thousands of small, low-powered devices with sensors and actuators, communicating wirelessly

Message Authentication Code (MAC)

- Essentially a one-way hash function with a key, *k*
- Used for message *integrity* and *authentication*
  - If *m* is altered to *m'* then MAC(*m*) ≠ MAC(*m'*)
  - Only those that know *k* can create correct MAC