IOWA STATE UNIVERSITY

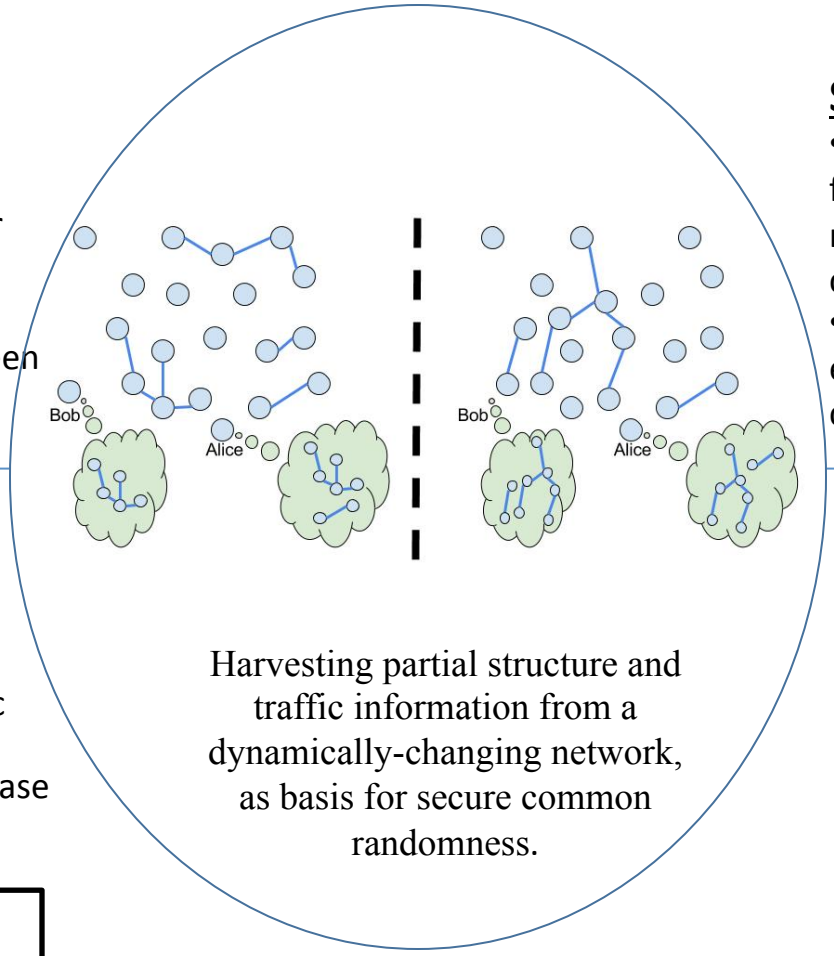
Security in Dynamic Environments: Harvesting Network Randomness and Diversity

Challenge:

- Quantify a general network's inner potential for supporting various forms of security by achieving secret common randomness between pairs or groups of nodes.

Solution:

- Investigate bounds by modeling as finite-length correlated HMMs.
- Identify protocol-specific sources of randomness
- Apply standard three-phase approach to secret key generation.



Scientific Impact:

- Introduces a mathematical framework for quantifying a network's potential for secure common randomness
- Practical protocols for key establishment from harvested common randomness.

Broader Impact:

- Broad applications to ad-hoc networks, for both military and consumer electronics.
- Will enable secure communication in the absence of a trusted security infrastructure.
- Directly impacts three graduate courses.

CCF 1320351
Iowa State University
George T Amariucai, gamari@iastate.edu