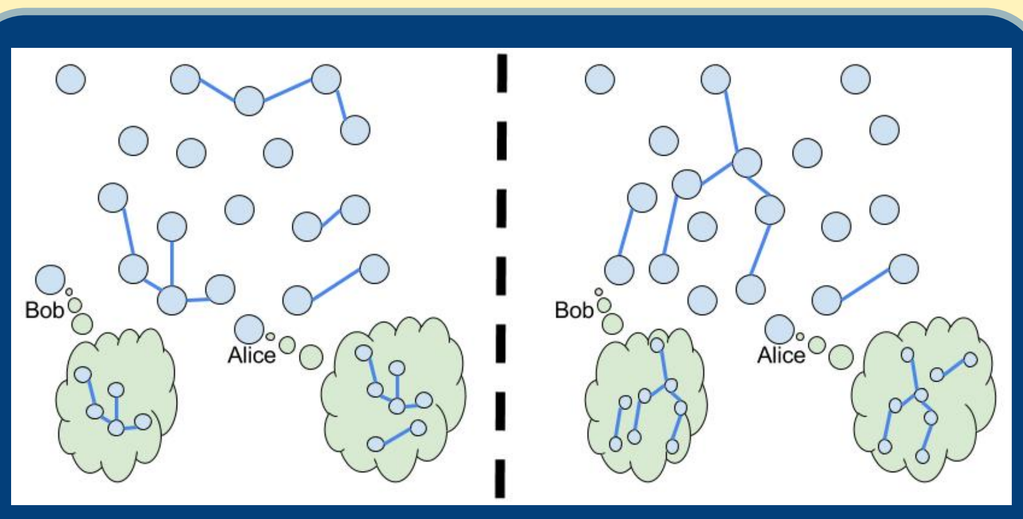
# Security in Dynamic Environments: Harvesting Network Randomness and Diversity

PIs: Shuangqing Wei (Louisiana State University),
George T. Amariucai (Iowa State University), and Jing Deng (University of North Carolina at Greensboro)

The project aims at quantifying a general network's inner potential for supporting various forms of security by achieving secret common randomness between pairs or groups of its nodes.

Statistical and computational secrecy measures are being considered against a general passive adversary.




Harvesting partial structure and traffic information from a dynamically-changing network, as basis for secure common randomness

Secure common randomness is achieved through:
- Culture building
- Crowd shielding

Broad range of protocols, covering:
- Multipath diversity
- Network tomography
- Secure network coding
- Anonymous routing
- Information dissemination (spread of epidemics, virality, etc.).

## Technical Challenges

- Designing secure protocols for key-establishment based on network randomness;
- Optimizing various compromises relating to network infrastructure:
  - sparse networks allow better confidentiality, but richly-connected networks provide more diversity
  - quasi-static networks allow better information reconciliation, but dynamic networks provide more (common) randomness;
- Characterizing mathematically a general network's potential for secure common randomness

# Approach

## Identifying Sources of Network Randomness

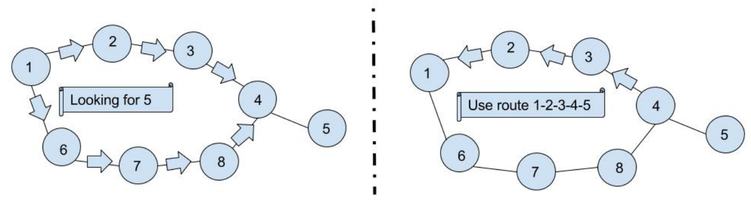
• Sources of randomness depend on the specific networking protocols, and may consist of:
- End-to-end or local delays;
- Local traffic loads;
- Local network connectivity (in dynamic networks);
- Local transmission patterns;
- Short-term employed routes (in dynamic networks).

## Standard Three-Phase Approach to Secret Establishment

• Advantage Distillation – protocol dependent
•Information Reconciliation – focus on practical, heuristic algorithms
•Privacy Amplification – roughly the attacker's conditional min-entropy on the probability distribution of the secret.
In practice, secrecy outage is often unavoidable, and needs to be parametrized.

## Common randomness from routing metadata

DSR-based routing in an ad-hoc network



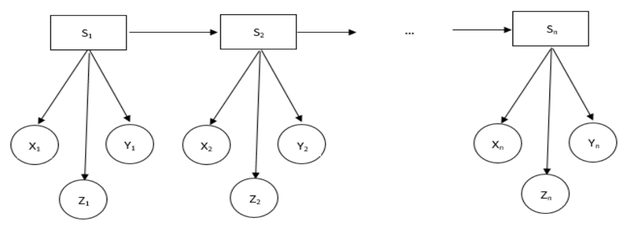

DSR-based routing in an ad-hoc network:
- All nodes maintain route tables for previously-estabished routes
- Each route has a unique route identifier (RID).
- Two nodes establish a secret by extracting randomness from the routes they have in common − information reconciliation done by exchanging RIDs.
- Key size roughly equal to adversary's min entropy on conditional probability distribution of a route.
- Some routes may be eavesdropped, so a security parameter characterizes probability of secrecy outage.

## More complex sources of common randomness

- Time-varying network connectivity − network varies as a Markov chain.
- Transmission-schedule-dependent network observation (observed only when some nodes communicate).
- Position-dependent network observation.
- Observations are subgraphs of network's instantaneous connectivity graph, augmented with rates, delays, etc.

## Current directions: theoretical limits of a model's potential for secure common randomness

Finite-length, correlated Hidden Markov Models (HMMs)




Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

IOWA STATE UNIVERSITY