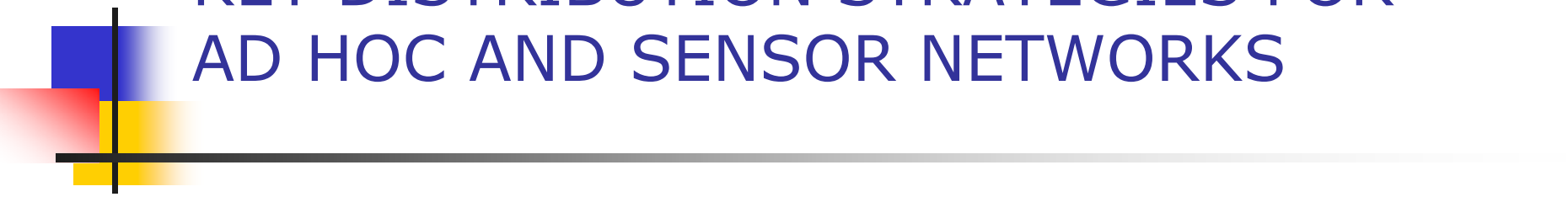
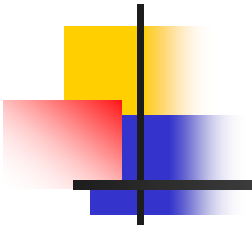


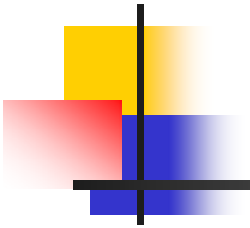
KEY DISTRIBUTION STRATEGIES FOR AD HOC AND SENSOR NETWORKS

Patrick Traynor
Department of Computer Science and Engineering
The Pennsylvania State University
Advisor: Dr. Tom La Porta



Approaches to Cryptography

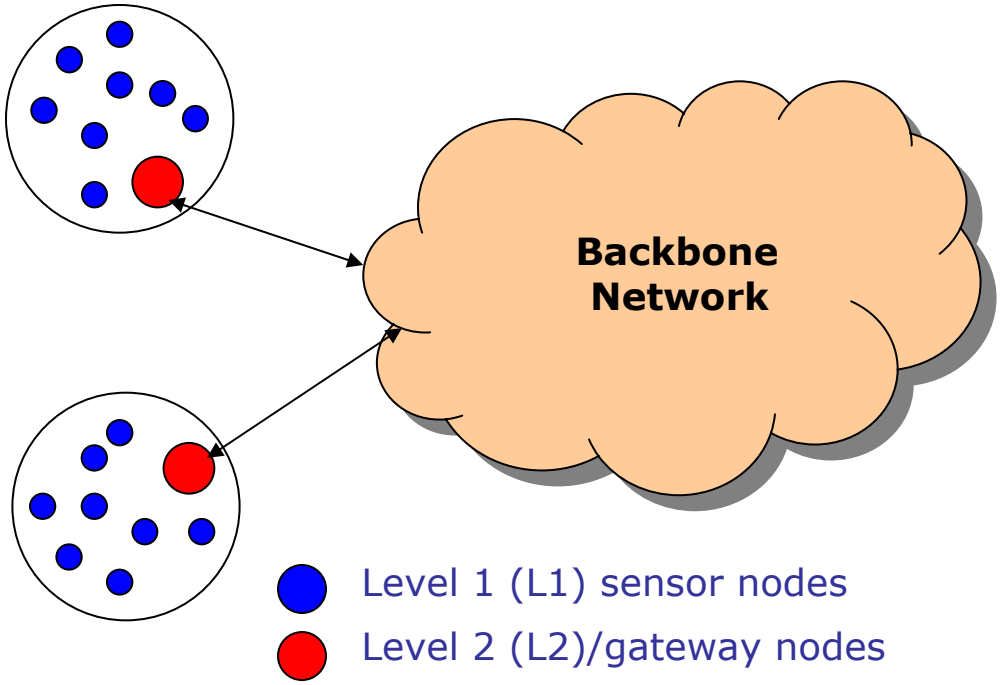
- Asymmetric (e.g. RSA):
  - Computationally VERY expensive!
  - The presence of a Key Distribution Center (KDC) can not be ensured in a remote, wireless environment.
  - Sensor nodes lack enough memory to hold all of the variables necessary for 1024-bit RSA encryption
  - Another approach must be taken!



Approaches to Cryptography

- Symmetric (e.g. DES, AES):
  - Using a single key compromises the entire network if a single node is captured.
  - Another traditional approach requires n-1 keys per node to ensure communication between all nodes-> $O(n^2)$
  - Pre-distributing specific keys can reduce the difficulty in key exchange, but the potential overhead can be huge!
  - Is it possible to distribute enough random keys in each node to ensure communication?

Robust Network Model



Traditional flat topologies only work in best- case scenarios

Equations

P(Balanced Key Conn)

$$p' = 1 - \frac{((P-k)!)^2}{P!(P-2k)!}$$

P(Unbalanced Key Conn)

$$p' = 1 - \frac{(P-k)!(P-m)}{P!(P-m-k)!}!$$

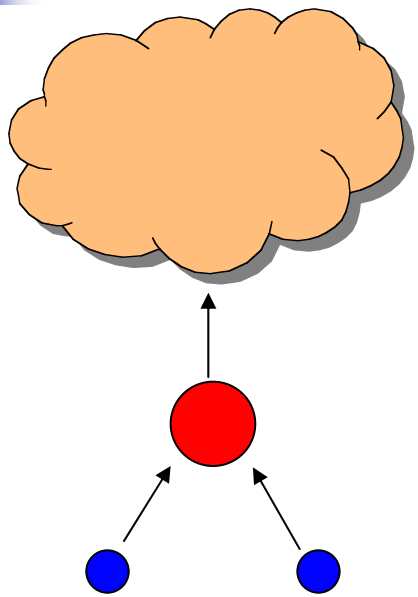
P(L1->L1)

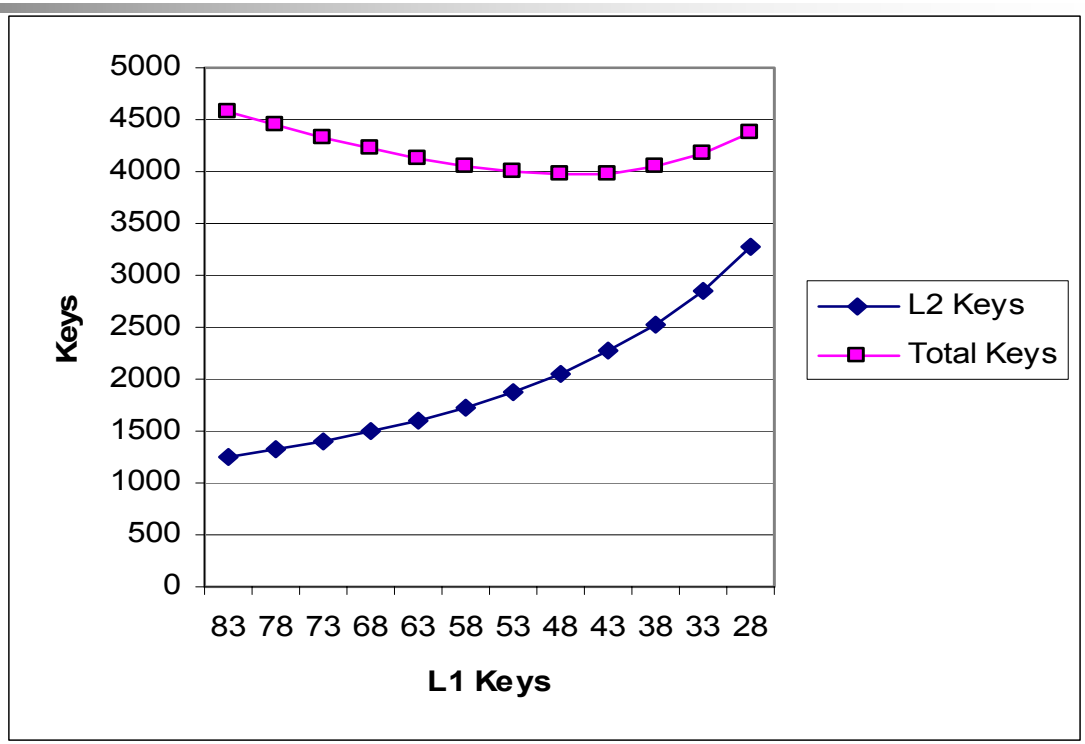
$$P(S) = 1 - \prod_{h=0}^{n-2} (1 - L1^{h+1})^R$$

P(L1->L2->L1)

$$P(A) = 1 - \prod_{h=0}^{n-2} (1 - (L1^h)(L2))^R$$

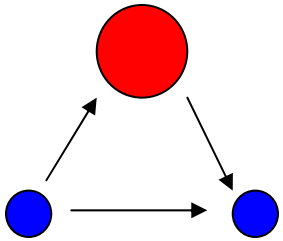
Backhaul Case

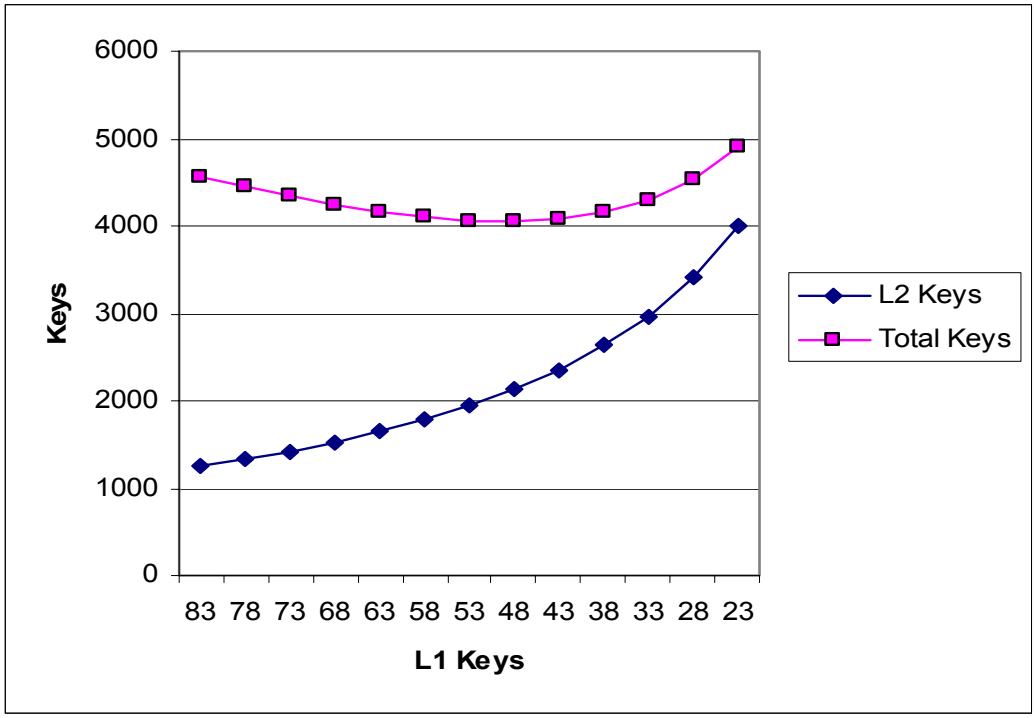




Balanced Case: 328 keys/node
Total: 13,120 keys
Unbalanced Case: 20-80 keys/node

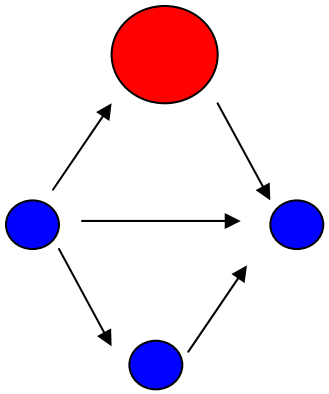
Local P2P, Limited Trust

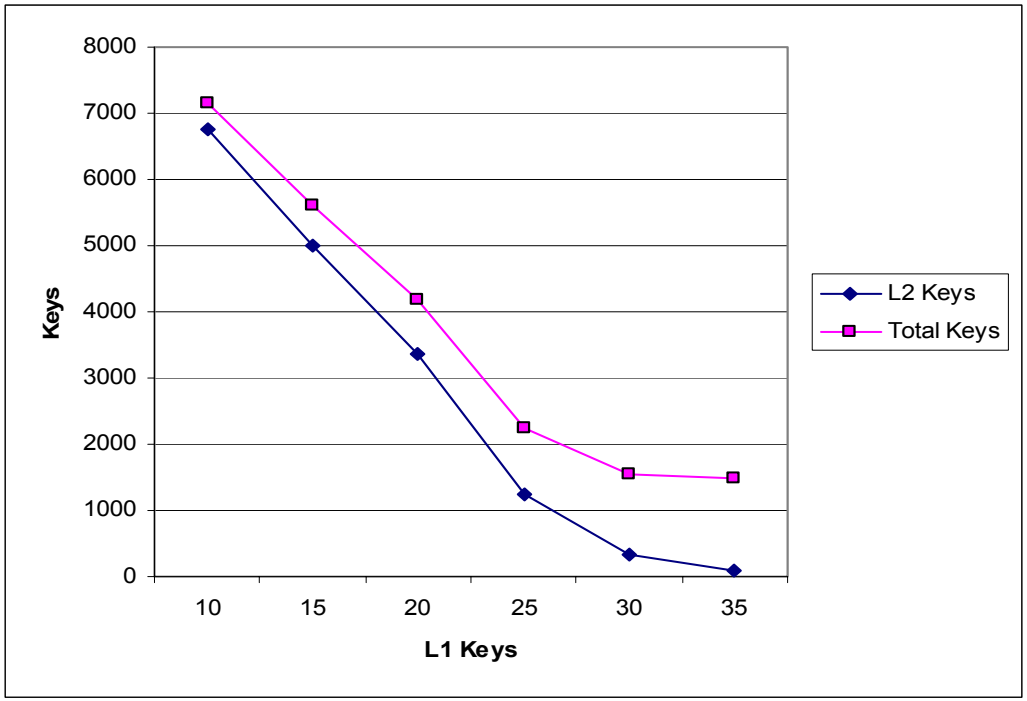




Balanced Case: 328 keys/node
Total: 13,120 keys
Unbalanced Case: 20-80 keys/node

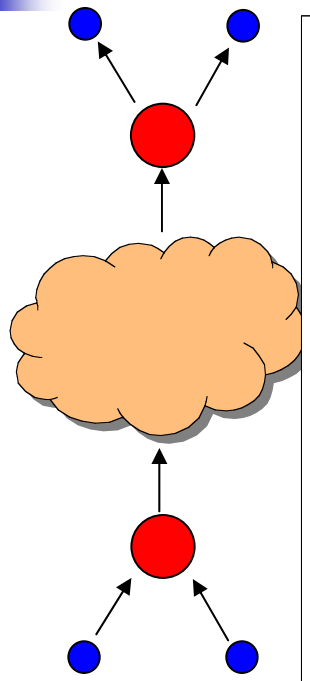
Local P2P, Liberal Trust

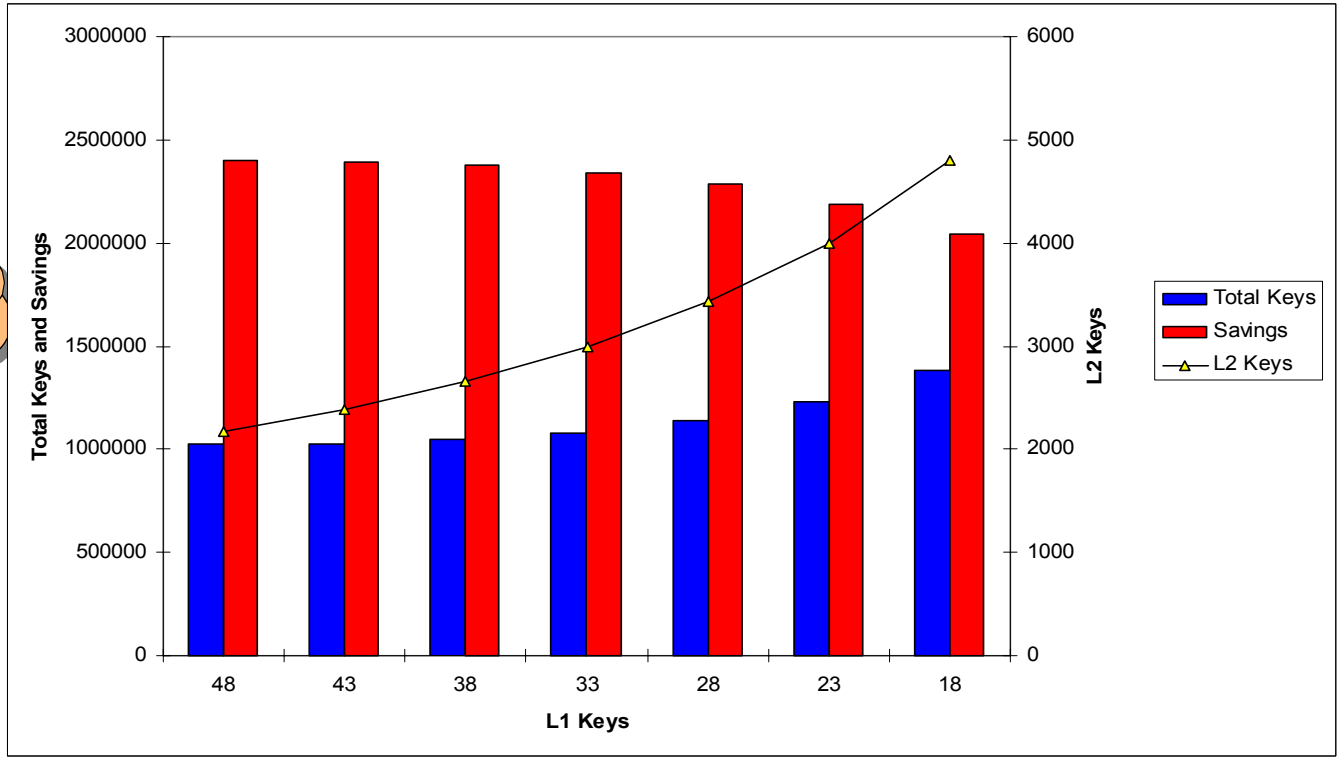




Balanced Case: 40 keys/node
Total: 1,600 keys
Unbalanced Case: 10-35 keys/node

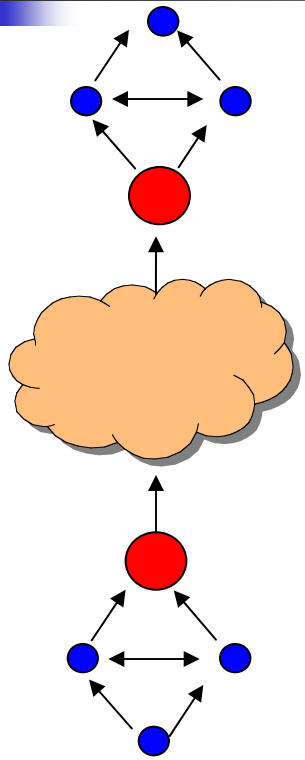
Non-Local P2P, Limited Trust

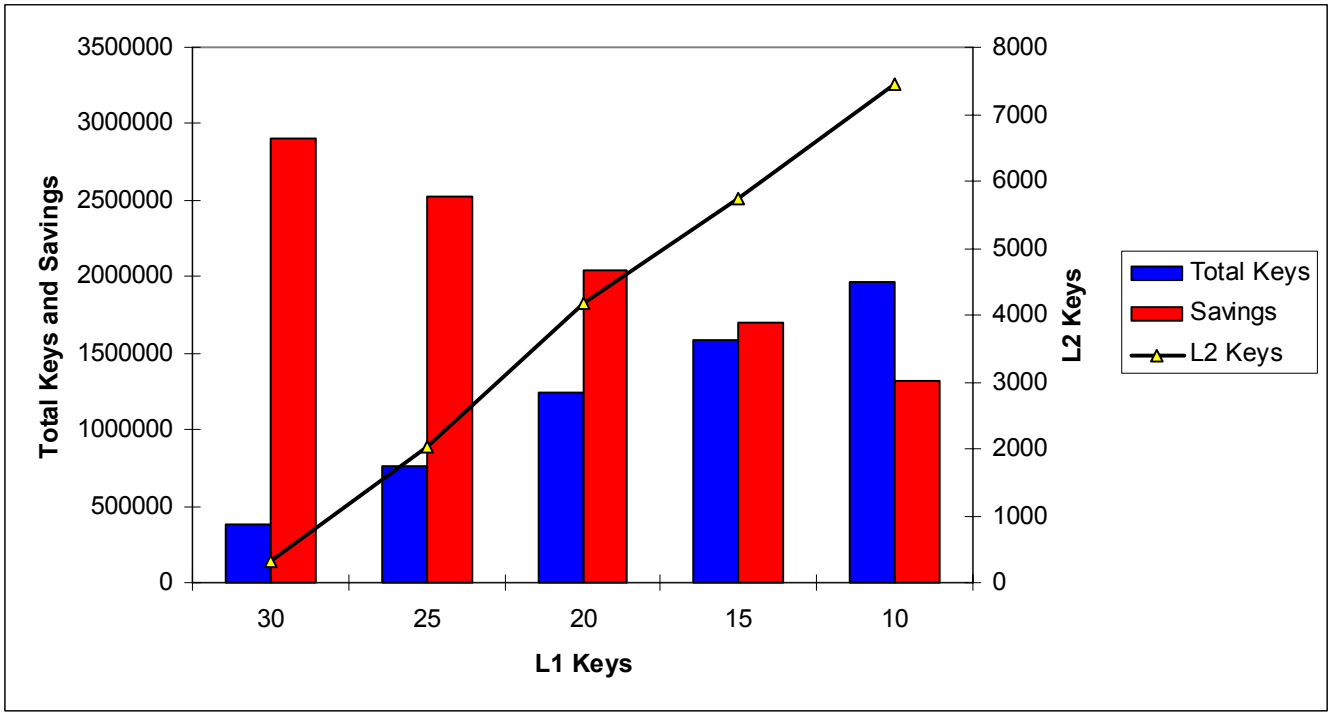




Balanced Case: 342 keys/node
Total: 3,420,000 keys
Unbalanced Case: 18-48 keys/node

Non-Local P2P, Liberal Trust





Balanced Case: 342 keys/node
Total: 3,280,000 keys
Unbalanced Case: 10-30 keys/node