SET: Clone Detection in Sensor Networks

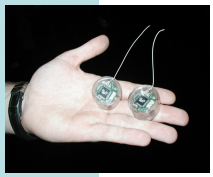
Heesook Choi, Sencun Zhu, Thomas F. La Porta
NSRC, Computer Science & Engineering Department
Contact: hchoi@cse.psu.edu

Sensors may be deployed in hostile environments. If an adversary captures a node, they may be able to access the private information within the node. The adversary then can **clone** these sensors and deploy them in the network to launch a variety of attacks. In this paper, we propose a new scheme, called ***SET***, to detect such cloning attacks. Exclusive subsets are reliably constructed, and the intersection and union of these subsets are calculated to detect the existence of node duplication.

Motivations

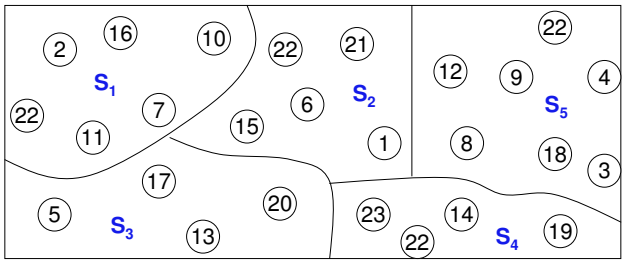
❑ **What makes it easy to clone sensors?**

- Unattended deployment and management
- Easy to capture physically
- Available general sensors (Cheap)
- Not equipped with tamper-resistant hardware



All CLONES are under the control of an adversary

SET Model



** S_i : a set of nodes in a sub-area i*

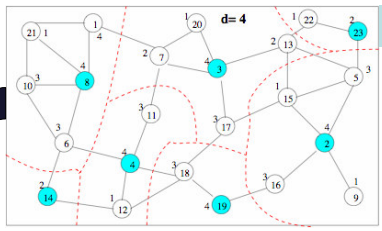
$S_1 \cap S_2 \cap S_3 \cap S_4 \cap S_5 = \varnothing$?

❑ Construct a set of random subsets
- BS broadcasts a seed
- exclusive subsets based on MIS

❑ Construct multiple sub-trees

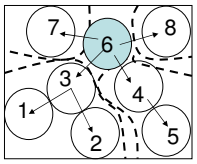
❑ Compute the union and intersection of subsets

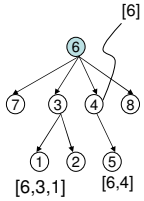
Construction of subsets and sub-trees



Construct EXCLUSIVE subsets (ESMIS)

- ❑ Each node computes $H_1 = H(seed, ID_i)$ for itself and neighbors in transmission range
- ❑ A node having maximum H_1 becomes SLDR
- ❑Other nodes, but SLDRs, are ruled by a SLDR
- ❑ A set of SLDRs is a Maximal Independent Set (MIS)



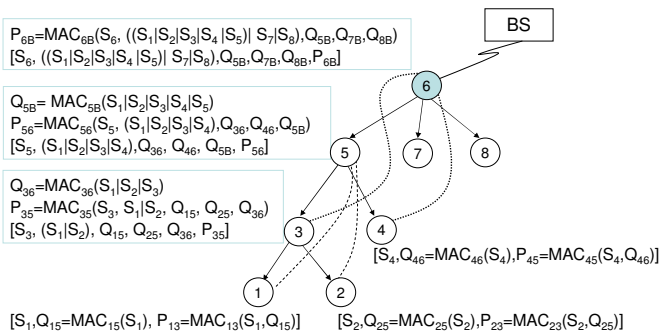


Construct multiple sub-trees

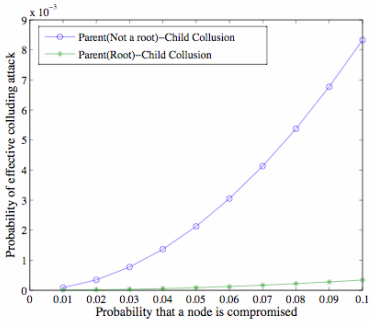
- ❑ Each node also computes $H_2 = H(seed)$
- ❑ A SLDR which has at least one member in $[H_2, H_2+B]$ becomes a root
- ❑ B is a parameter to control the number of sub-tress in the network
- ❑ Each sub-tree covers an exclusive area (a subset of nodes, without overlapping)
- ❑ Set union and intersection are computed in each sub-tress
- ❑ Each root sends the set result to the BS

Interleaved set computation

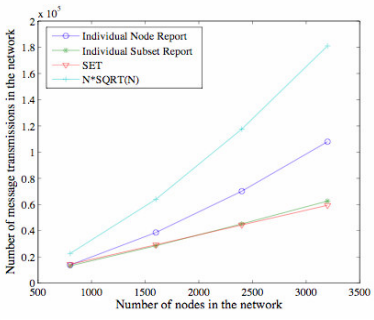
Set computation in a sub-tree is not reliable !



Security & Overhead



Effectiveness of Adversary



Message Transmission Overhead

Schemes	Communication Cost
Broadcast	O(N2)
Randomized Multicast	O(N2)
Line-Selected Multicast	O(N√N)
Individual Node Report	O(N√N)
Individual Subset Report	O((N/2)√N)
SET	O(N)

Communication Cost Comparison

Sponsored by NSF