LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks

Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao and Tom La Porta

The Problem

- Researchers have modeled sensor networks as homogeneous systems with either full or no access to infrastructure.
- Security solutions, especially in key management, have been built upon the same assumptions.
- If we designed security around the way real networks are built, more secure and efficient systems would result.

Real Scenarios

- A sensor network is air-deployed along a disputed border before friendly forces move into the area.
- The network should securely establish itself in isolation so that it can conduct its mission.
- When up-linked friendly forces arrive, the network should be able to take advantage of these new connections and the security guarantees they provide.
- None of the work done in the field thus far considers this changing nature of backbone connectivity and its effects on security.

Network Characteristics

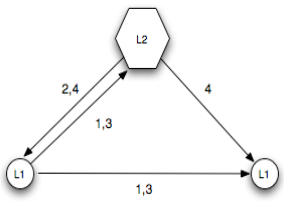
- Networks may consist of a heterogeneous mix of nodes: Level 1 (L1) or sensing nodes, Level 2 (L2) or gateway nodes and Key Distribution Centers (KDC).
- The hierarchy of resources and ability is: L1→L2→KDC.
- Nodes with more resources store more keys. We call this an "unbalanced key distribution".
- For a two level hierarchy, we have demonstrated that P[connectivity] between two nodes is:

$$P[Conn] = 1 - \frac{(P-k)!(P-m)!}{P!(P-m-k)!}$$

$$p(i) = \frac{\binom{P}{i}\binom{P-i}{(m-i)+(k-i)}\binom{(m-i)+(k-i)}{m-i}}{\binom{P}{m}\binom{P}{k}}$$

Network Models

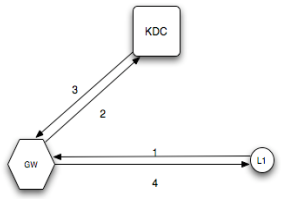
LION



Standalone Keying Model

- Network securely operates in isolation.
- True authentication of neighbors is difficult.
- This method may require a large number of transmissions, which are expensive.

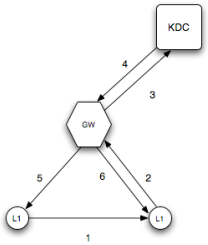
TIGER



Infrastructure-Base Model

- Uses a secure KDC in a backbone network to assist in key management.
- Security is dependant on the connection to KDC.
- Lower messaging overhead than LION.

LIGER

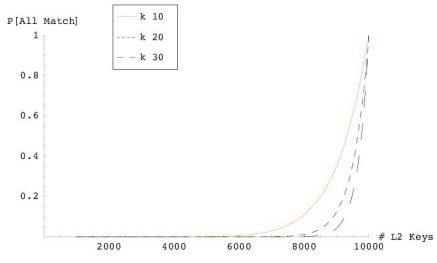


Hybrid Model

- Uses a KDC if available to authenticate nodes; otherwise, loosely authenticates nodes at L2/GW.
- Enforces least privilege by requiring both parties to participate in requests to the KDC.

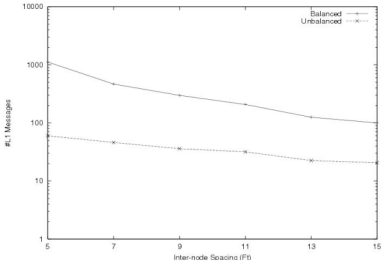
Results

Robustness



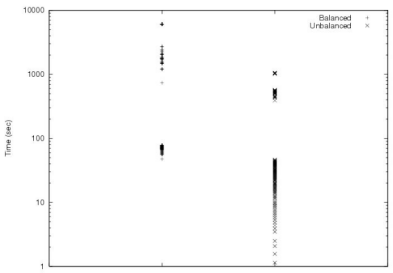
- An adversary would have to capture 63% of the entire key pool in the network to have a 1% chance of impersonating another node.

Efficiency



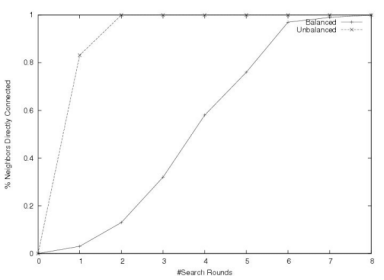
- Network initialization can be achieved in an average of 58.968 transmissons/node instead of 1199.180 transmissions/node.

Initialization



- Using our unbalanced keying method, a network of 200 nodes initializes in 274.667 seconds instead of 1865.170 for a balanced distribution

Connectivity



- Nodes using the unbalanced scheme establish keys with 90% of their neighbors in fewer rounds than those using the balanced method.

Conclusions

- Realistic modeling of networks allows us to construct more secure systems.
- The unbalanced method of key management implemented in this work makes network initialization occur more quickly.
- Less damage is incurred with node compromise using our keying scheme. An administrator can therefore focus their resources on protecting the more powerful nodes in the system
- Because fewer messages are needed for a system using the unbalanced method.

Sponsored by: The Pittsburgh Digital Greenhouse/Technology Collaborative and 3eTI