Security and Privacy Support for Data-centric Sensor Networks

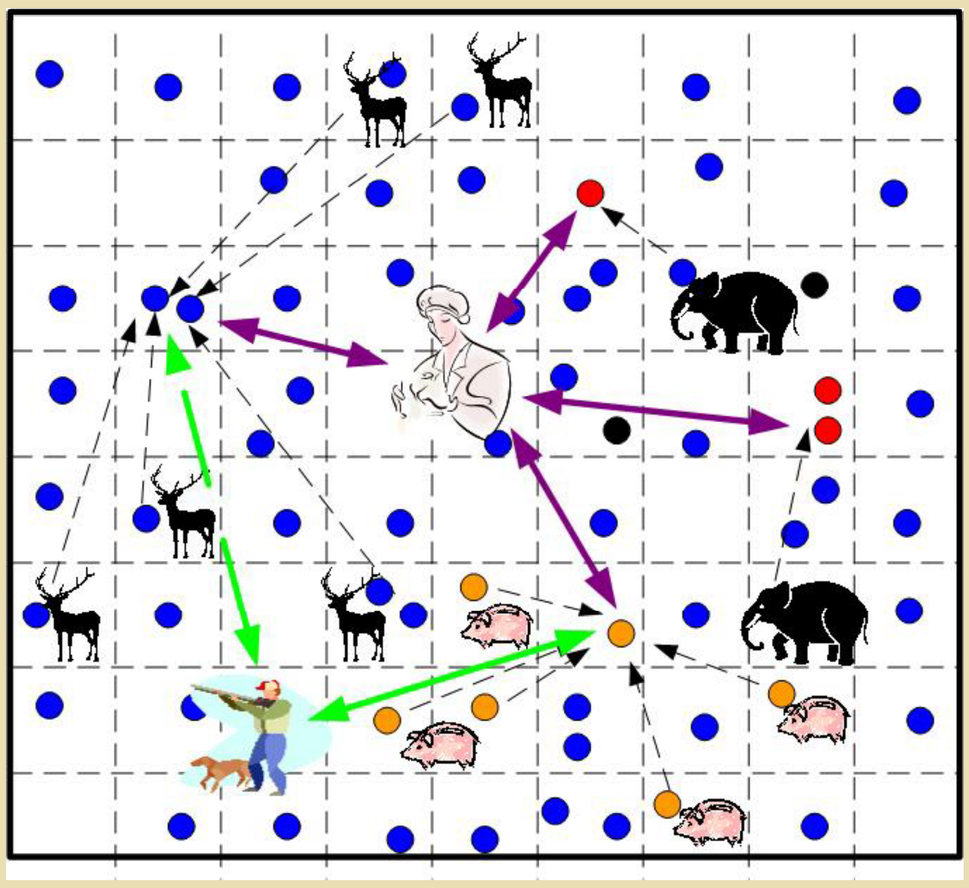
PIs: Sencun Zhu and Guohong Cao, Computer Science & Engineering, PSU

Project Description

In a data-centric sensor network, sensing data are named based on attributes such as event type and sensing data with the same name are stored in the same location, queries for data of a particular name can be sent directly to the nodes storing these data rather than flooding the query throughout the network. However, saving data in the network also creates high security and privacy problems. For example, an attacker may find out/compromise/destroy the storage nodes for the events of his interest or trace back to the data sources.

Example:

In a wild animal habitat, the detected location of each type of animal is forwarded and stored in one location. The zoologist should be able to query and access all the locations, whereas a hunt is only authorized to access the locations of certain animals (e.g., dears and boars) for hunting, not that of elephants.



Attack Model:

- local passive attack – local eavesdropping, no node compromise
- global passive attack – global eavesdropping, no compromise
- compromise-based active attack – with node compromises

We propose one approach for each attack model.

Approach and Impact

Approaches

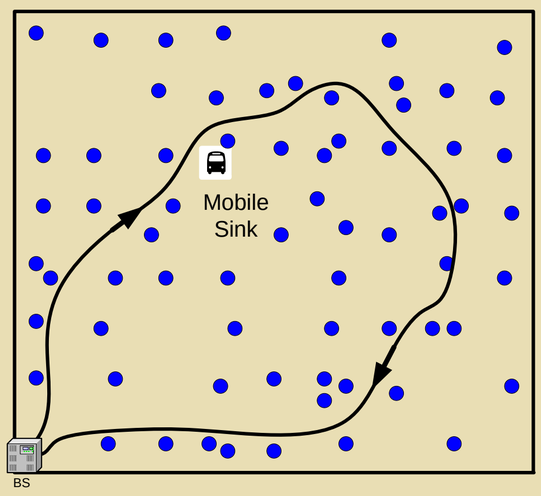
- Principle of least privilege to restrict the access rights of mobile users
- Anonymization techniques for source location privacy and source-destination mapping
- Optimal mechanism for filtering dummy traffic

Research Impact

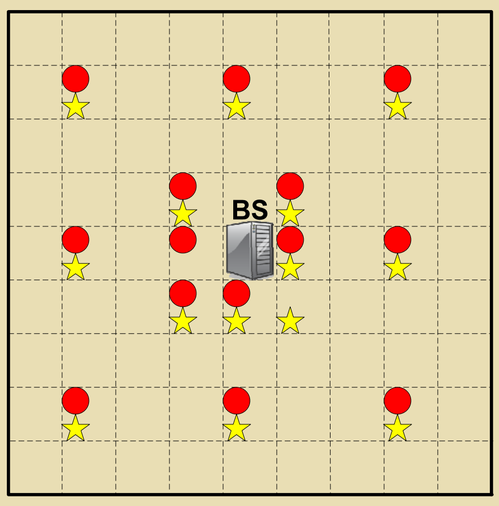
- preventing eavesdropping and traffic analysis
- resilience to node/user compromises
- proposing the notation of *statistically strong source anonymity*

Technical Details

- Based on the principal of least privilege, we design several security restriction schemes which only grant the user the least privilege required to accomplish their tasks.
- To preserve the privacy of source-destination location mapping, we provide private data-location mapping based on various types of cryptographic keys.
- To provide event source location privacy under global passive attack, we introduce dummy traffic such that the traffic patterns of sensor nodes that detect real events are statistically indistinguishable from when no real events occur, while minimizing the transmission latency for real events. Further, dummy traffic is proactively filtered and dropped before they reach the destinations.



A mobile sink is granted the least privilege based on its projected trajectory and time of task



Optimal placement of proxies for filtering dummy traffic

Publications:

M. Shao, S. Zhu, W. Zhang, G. Cao, pDCS: Security and Privacy Support for Data-Centric Sensor Networks, *IEEE INFOCOM 2007,* to appear.

H. Song, W. Zhang, S. Zhu, and G. Cao. Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks. To appear in *ACM Transaction on Sensor Networks, 2008*.

Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks, *ACM WiSec 2008*.

M. Shao, Y. Yang, S. Zhu, and G. Cao. Towards Statistically Strong Source Anonymity for Sensor Networks. IEEE *INFOCOM 2008*.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

Mobile Computing and Networking Laboratory