SCONCE
Secure Computing and Networking Center

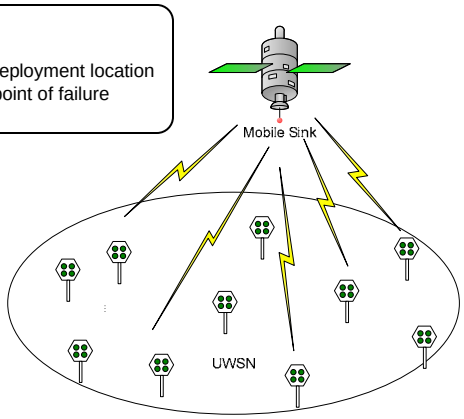
Self-Defense in Unattended Wireless Sensor Networks (UWSNs)

Di Ma, Claudio Soriente and Gene Tsudik

Computer Science Department
UCIrvine

How to cope with mobile adversary in Unattended Wireless Sensor Networks?

UWSNs:
- Remote/inaccessible deployment location
- Avoidance of central point of failure



UWSN Characteristics:
- Sink visits periodically
- Sensors accumulate data and waits for the next sink visit

UWSN Examples:
1. Monitoring nuclear activity in a rogue country
2. Underground WSN monitoring troop movements or border crossings
3. Anti-poaching WSN in a national park monitoring firearm discharge

New Adversary Model – Mobile Adversary

Traditional WSN Adversary Model:
1. **Fixed compromise power:** set max. number of nodes compromised overall
2. Solutions focus on detection
3. On-line sink can mitigate attacks

New Adversary Model:
1. **Mobility:** compromises different set of sensors at each time interval → given enough time can subvert the entire WSN
2. Sink is off-line: real-time detection does not help
   -- adversary can reach its goal and leave without being detected)
3. Different from cryptographic mobile adversary model
   -- No global secrets
   -- Meager resources (power, storage, …)

Adversarial Flavors

Adversaries defined by goal/operation/visibility

Goal:
1. Search-and-replace
2. Search-and-erase
3. Curious
4. Polluter
5. Eraser

Operation:
1. Reactive
2. Proactive

Visibility:
1. Stealthy
2. Visible

Goal

Visibility	Search-and-erase	Search-and-replace	Curious	Polluter	Eraser
Stealthy	Proactive Reactive	Proactive Reactive	Proactive	N/A	N/A
Visible	Proactive Reactive	N/A	N/A	Proactive	Proactive

Mitigating Sensor Compromise

Data category:
(a) Data collected before compromise
   -- Need **forward security**
(b) Data collected during compromise
(c) Data collected after compromise
   -- Need **backward security**

Can we protect data in category (a) and (b)?

Periodical secret update:
1.One-way function
   -- No backward security
2. True Random Number Generator (TRNG)
3. Secure hardware or online TTP

NOTE: 2 and 3 not realistic in UWSNs

Cooperative Self-Healing

Basic Idea: let each sensor serve as a source of secure randomness for others

Secret update: based on a sensor's prior secret and all randomness received.

Observation: a sensor whose randomness is compromised can regain security if it obtains at least one "infusion" of secure randomness from a peer sensor whose randomness is not compromised

Deterministic secret update schemes (secrets used as encryption keys):
   -- DISH (SSS'08)
   -- POSH (SRDS'08)

Conclusion

1. UWSNs confronted with mobile adversaries → need new security solutions.
2. Forward and backward security are crucial for mitigating mobile adversary threat.
3. Sensor cooperation is an effective way to achieve forward and backward security

Future Work

1. Addressing other adversarial types
2. Formal treatment of mobile adversary.

10th International Symposium on Stabilization, safety and security of Distributed Systems, Detroit, MI