How to Withstand a Mobile Adversary in Unattended Sensor Networks

Gene Tsudik
SCONCE – Secure Computing and Networking Center
UC Irvine
http://sconce.ics.uci.edu

Joint work with:

Roberto Di Pietro
Università di Roma 3

Claudio Soriente
University of California, Irvine

Luigi Mancini
Università di Roma "La Sapienza"

Angelo Spognardi
Università di Roma "La Sapienza"

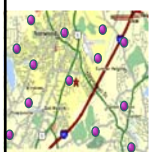
Di Ma
University of California, Irvine

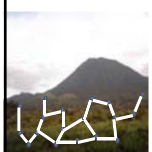
Roadmap

- Introduction
  - A certain kind of WSN
  - New adversarial model (with many flavors)
- Naïve defense strategies
- Cryptography to the rescue
- Related Work
- Conclusions + challenges

2

A “Typical” Wireless Sensor Network



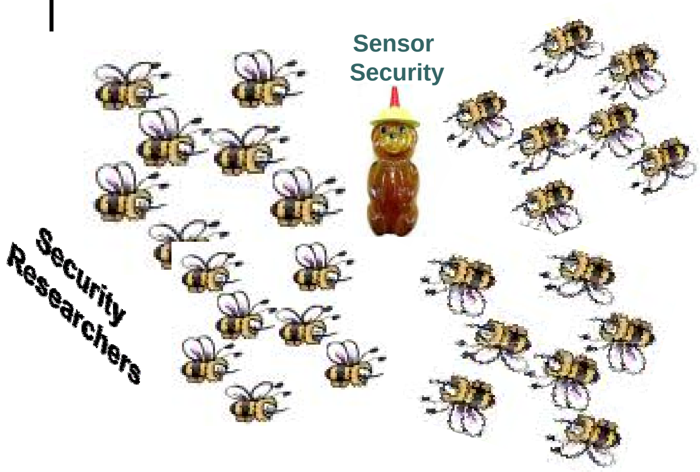


Many real, alleged and imagined applications

- Networking
  - Sensor-to-sink communication (opt. sink-to-sensors)
- Collection method
  - Periodic collection
    or
  - Event driven
    or
  - Query based = on-demand
- Online Sink
  - Real-time off-loading of data

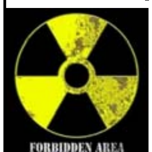
3

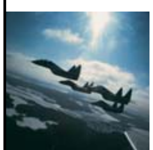
Lots of Prior Work on Sensor Security



4

Unattended Wireless Sensor Network (UWSN)

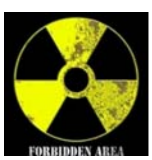


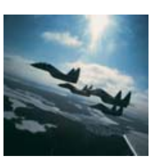


- Nodes operate in hostile environment
  - Initial deployment might be ad-hoc
- No ever-present sink
  - Itinerant, visits UWSN periodically
- Periodic data sensing (on-demand – N/A, event-driven -- ?)
  - Nodes might retain data for a long time
  - Data might be valuable
- Nodes are mostly left on their own
  - Adversary roams around with impunity
  - Adversary has **lots of time**
- **Challenge: Data Survival in UWSNs**

5

Examples





- WSN deployed in a recalcitrant country to monitor any potential nuclear activity
- Underground WSN monitoring sound and vibration produced by troop movements or border crossings
- Anti-poaching WSN in a national park tracking/recording firearm discharge locations

6

UWSN Mobile Adversary

Adv defined by: goal / operation / visibility

Goal:
- Search-and-erase
- Search-and-replace
- Curious
- Polluter
- Eraser

Operation:
- Reactive
- Proactive

Visibility:
- Stealthy
- Visible

Focus:
- General
- Targeted

7

UWSN Mobile Adversary

Adv 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 Reactive	Proactive Reactive

8

New kind of Adversary (Adv)

- Well-informed
  - Knows network topology and network defense strategy
- Erratic (seemingly)
  - Unpredictable and possibly untraceable movements
- Mobile
  - Migrates between sets of nodes between sink visits
- Data-centric
  - No interference with sensing or network operation
- Powerful (but not omnipotent)
  - Compromises up to a certain # of nodes

9

Assumptions

- Scheduled (per round) data sensing/collection
  - Max ***v*** rounds between sink visits
  - Assumption: Adv's round = UWSN round
- Adv compromises at most ***k*** (out of ***n***) nodes per round
  - Compromised nodes not necessarily contiguous
  - Reads all storage
  - Listens to all incoming and outgoing communication
- Adv knows which data to target and when it was sensed
  - Receives external signal at collection time
    - Target node identity + collection round
    - Possibly, also target value
- UWSN knows nothing…
  - Equal protection for all data

10

BTW

Does all this sound familiar?

Cryptographic Mobile Adversary

Proactive Cryptography

- Ostrovsky &Yung: How to Withstand Mobile Virus Attacks, PODC 1991
- Proactive Cryptography: Decryption and Signatures (e.g., RSA, DSA, Schnorr)

Agenda

- Introduction
  - A different kind of WSN
  - New adversarial model (with many flavors)
- Search-and-Erase Adv: Naïve defense strategies
- Cryptography to the rescue
- Related Work
- Conclusions + challenges

Stealthy Search-and-Erase Adv

IEEE Percom'08, this week in Hong Kong ☺

13

What we want: whack-a-mole

14

What if sensors have no crypto capability?

- Cheap sensors
  - No crypto
  - Can only (attempt to) hide data location
- Data Migration strategies
  - Do Nothing
  - Move Once
  - Keep Moving
- Adv Goal: Search-and-erase
  - Looks for target data in compromised sensors
- Adv strategy:
  - Lazy
  - Frantic
  - Smart

15

Survival vs. Attack Strategies

	Attack Strategy		
Survival Strategy	LAZY	FRANTIC	SMART
DO NOTHING	✗	✓	✗
MOVE ONCE	✗	✓	✗
KEEP MOVING	✓	✓	✓

16

Do Nothing

- Data kept at originating sensor
  - Trivial
- Adversary wins in one round
  - Round 0
    - Learns originating sensor
  - Round 1
    - Compromises it
    - Deletes target data

17

Move Once

- Data off-loaded to a random recipient node
  - Kept there for all subsequent rounds (until sink visit)
- Adversary wins in at most $\left\lceil \frac{n}{k} \right\rceil$ rounds
  - Round 0
    - Learns originating node (data is not there anymore)
  - Round i
    - Move to next set of previously uncompromised nodes
  - At most $\left\lceil \frac{n}{k} \right\rceil$ rounds to find and erase

18

Keep Moving

```
Algorithm 1: KEEP-MOVING
      /* start round 0 */
      all nodes sense their values
      each node exchanges data with others
0     A learns s̄_0 and x
      /* end round 0 */
      SET z=min(v, n/k)
      SET found=FALSE
      for ((r ← 1 to z) and (not found)) do
          /* start round r */
1         select C_r  /* new set of nodes to compromise */
2         compromise C_r and release C_{r-1}
3         if (x found on some s_i ∈ C_r) then
3.1           delete x
3.2           SET found=TRUE
          all nodes sense their values
          each node exchanges data with others
4         if (x received by some s_i ∈ C_r) then
4.1           delete x
4.2           SET found=TRUE
          /* end round r */
```

Adv learns target data at round 0

Adv looks for target data in the new set of compromised nodes

Nodes exchange messages

Adv looks for target data in the messages received by corrupted nodes

- Adv has two chances per round
  - Before data exchange
  - After data exchange

Keep Moving – Lazy

- Exploit the fact that data is constantly moving among sensors
- Two chances at round 1; one chance each new round
- Prob. data survives v rounds

$$P_L(v) = P_1 \cdot P_2^{\,v-1}$$

$$P_1 = \frac{k}{n} + \left(1 - \frac{k}{n}\right)\frac{k}{n} = \left(1 - \frac{k}{n}\right)^2$$

$$P_2 = 1 - \frac{k}{n}$$

Keep Moving – Frantic

- Select a new random k-set to compromise at each round
- Two chances per round
- Probability that data survives v rounds:

$$P_F(v) = P_1 \cdot P_2^{v-1} \cdot P_3^{v-1}$$

$$P_1 = \frac{k}{n} + \left(1 - \frac{k}{n}\right)\frac{k}{n} = \left(1 - \frac{k}{n}\right)^2$$

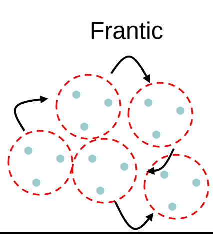
$$P_2 = 1 - \frac{k}{n}$$

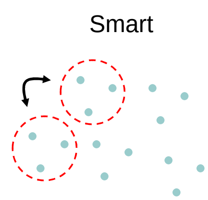
$$P_3 = 1 - \frac{k}{n-k}$$

21

Keep Moving – Smart

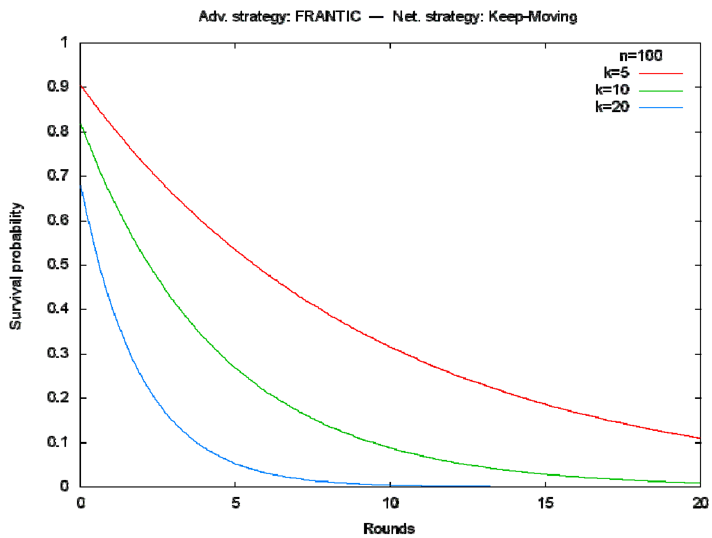
- Moves between two fixed (non-overlapping) set of nodes
  - No matter what adversarial strategy, data recipient node is always chosen according to an uniform distribution
  - Same survival probability!





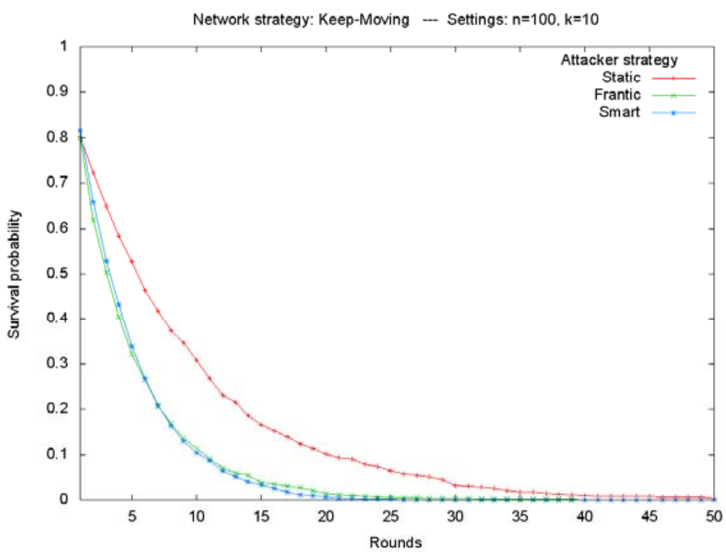
22

Results



23

Keep Moving – Smart



24

Overhead 1

scheme	msg × round (r)	msg tot	Queue	msg rec
Move-Once	n	$v \cdot n$	$Pr[\exists s_i \text{ s.t. } L_i^r \geq r+\sqrt{nr}] \leq e^{-r/2+\ln n}$	$O(\ln n)$
Keep-Moving	$r \cdot n$	$(r^2/2)n$	$Pr[\exists s_i \text{ s.t. } L_i^r \geq 2er] \leq 2^{-r+\ln n}$	$Pr[\exists s_i \text{ s.t. } M_i^r \geq 2er] \leq 2^{-r+\ln n}$

- Prob. # stored messages do not exceeds a given value ℓ
- L^i_r = # msg stored on s_i at round r $\rightarrow$ $E[L_i^r] = r$
- From the method of bounded differences, given $\ell > r + \sqrt{rn}$

$$Pr[L_1^r \geq \ell \cup \ldots \cup L_n^r \geq \ell] \leq nPr[L_1^r \geq \ell] \leq e^{-r/2+\ln n}$$

Overhead 2

scheme	msg × round (r)	msg tot	Queue	msg rec
Move-Once	n	$v \cdot n$	$Pr[\exists s_i \text{ s.t. } L_i^r \geq r+\sqrt{nr}] \leq e^{-r/2+\ln n}$	$O(\ln n)$
Keep-Moving	$r \cdot n$	$(r^2/2)n$	$Pr[\exists s_i \text{ s.t. } L_i^r \geq 2er] \leq 2^{-r+\ln n}$	$Pr[\exists s_i \text{ s.t. } M_i^r \geq 2er] \leq 2^{-r+\ln n}$

- Prob. # stored messages do not exceeds a given value ℓ
- L^i_r = # msg stored on s_i at round r $\rightarrow$ $E[L_i^r] = r$
- From the method of bounded differences, given $\ell > r + \sqrt{rn}$

$$Pr[L_1^r \geq \ell \cup \ldots \cup L_n^r \geq \ell] \leq nPr[L_1^r \geq \ell] \leq e^{-r/2+\ln n}$$

- Variables L^i_r are independent $\rightarrow$ Chernoff bound $\rightarrow$ $Pr[L_1^r \geq \ell] \leq 2^{-r}$ for $\ell > 2er$
- M^i_r = # msg received by s_i at round r

$$Pr[M_1^r \geq \ell \cup \ldots M_n^r \geq \ell] \leq nPr[M_1^r \geq \ell] \leq 2^{-r+\log_2 n}$$

Replication

- Each sensor produces R copies of its reading
  - Information survives as long as one copy survives
- $X_{i,j}$ = 1 if replica i survives up to round j

$$Pr[X_{1,j}=1]=P_1\cdot P_2^{j-1}\cdot P_3^{j-1}$$

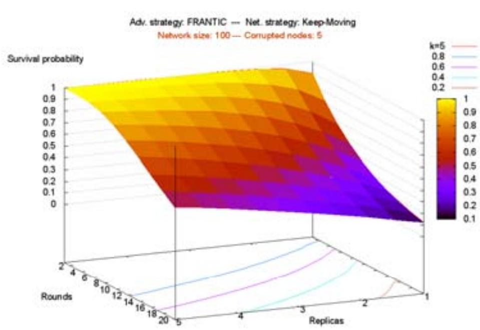
$$\overline{P_R^v}=Pr[X_{1,v}=0\wedge\ldots\wedge X_{R,v}=0]=Pr[X_{1,v}=0]^R=$$
$$=(1-Pr[X_{1,v}=1])^R=(1-P_1\cdot P_2^{v-1}\cdot P_3^{v-1})^R$$

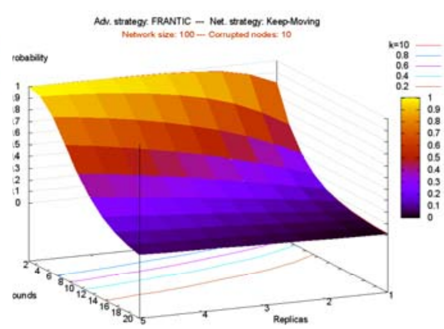
- Prob. that information survives:

$$P_R^v=1-\overline{P_R^v}=1-(1-P_1\cdot P_2^{v-1}\cdot P_3^{v-1})^R$$

27

Results





Replication of sensed data
- Increases survival probability
- Requires more storage and power
- Given enough rounds, **Adv always wins**

28

Encryption

- Goal: hide data contents and origin from the adversary
- Adv can not decrypt
- Adv can not identify data to erase
- Public Key vs. Symmetric key
- Randomized Encryption
  - Random values involved in the encryption process
  - Given two ciphertexts encrypted under the same key, it is infeasible to determine whether two corresponding plaintexts are the same

29

Public Key Encryption

- Each node knows sink's public key PK_S
- d_i^r -- data sensed by s_i at round r stored as

$$E_i^r = E(PK_S, r, s_i, etc.)$$

- Adv can only try brute-force guessing the plaintext
  - If random data involved in encryption, ciphertext guessing becomes infeasible (i.e., randomized encryption)

30

Symmetric Encryption

- Each s_i shares k_i^0 with the sink
- d_i^r -- data sensed by s_i at round r stored as:

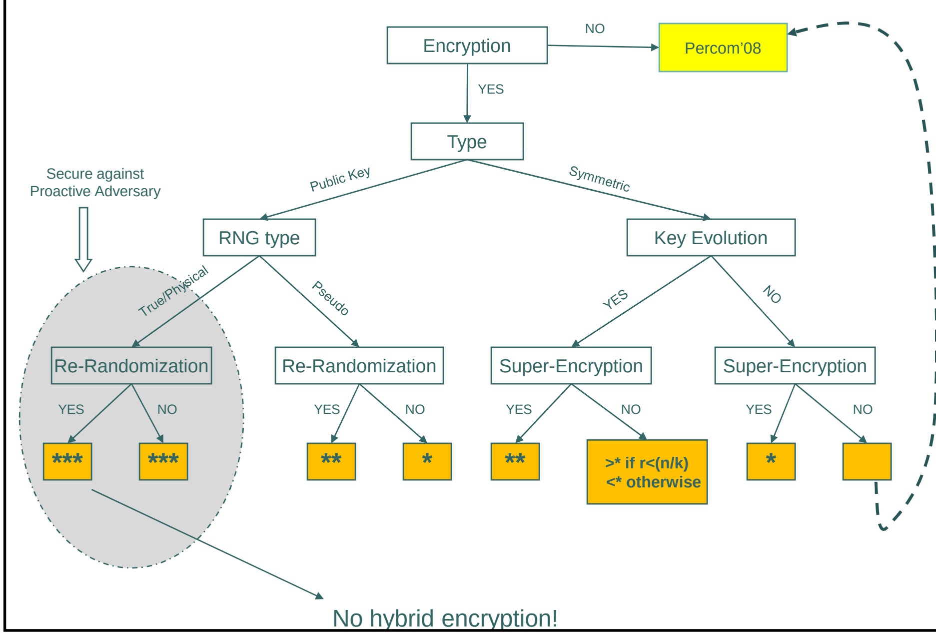
$$E_r^i = E(k_r^i, d_r^i, r, etc.)$$

- Forward security
  - per round key evolution:

$$k_{r+1}^i = OWF(k_r^i)$$

31
- Adv can not compute previous keys

"Crypto Decision Tree"



Near-Term Challenges

- How to recover from compromise without PK + TRNG
- What happens if Adv eavesdrops on migrating data?
- Effects of Adv positioning within UWSN topology (to maximize eavesdropping ability)

Related Work

- Mobile Ad Hoc Networks
  - Data availability in partitioned MANETs
    - [Hara, et al. 2006, Giannuzzi, et al. 2005]
  - Multi-path routing to improve confidentiality and availability
    - [Papadimitratos, et al. 2006, Berman, et al. 2005]
- Sensor Networks
  - Data coding to increase data recovery in presence of disasters
    - [Kamra, et al. 2006]

Conclusion + Future Directions

- Contributions:
  - New kind of network - UWSN
  - New mobile UWSN adversary
  - Simple approaches for data survival simply don't work!
- Lots of interesting problems
- Ongoing and Future work:
  - Explore the design space of cryptographic techniques
    - Encryption
    - Authentication
  - New adversarial models and flavors
    - What if Adv interferes with networking and/or sensing?

35

The End…

- Questions?
- Comments?
- Complaints?

36