

Securing Internet Coordinate Embedding Systems

Mohamed Ali Kaafar, INRIA, Fr

Laurent Mathy, Lancaster University, U.K

Chadi Barakat, INRIA, Fr

Kavé Salamatian, LIP6, Fr

Thierry Turletti & Walid Dabbous, INRIA, Fr



Introduction

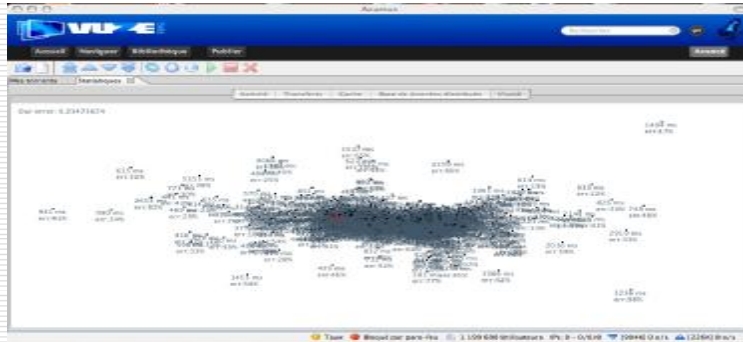
- ICS (Internet Coordinates Systems):
 - n Embed RTTs into geometric spaces

Decentralized Approaches

-Landmark-based Approaches (e.g. NPS)

-P2P Approaches (e.g. Vivaldi)

ICS: Applications



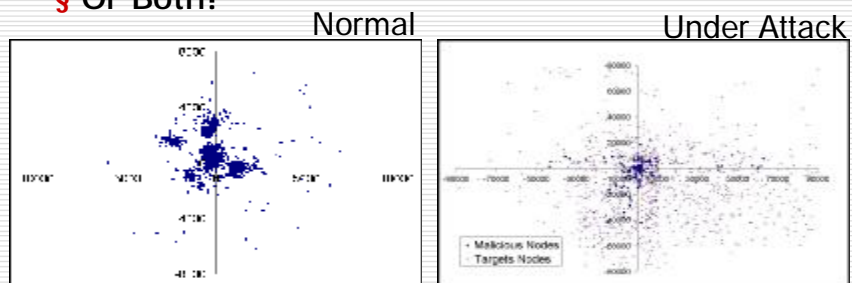
- ⊖ Accurate, ⊖ Scalable, ⊖ robust
 - ⊕ Long convergence time
- Deployed as an "Always-On and Large scale Service"

8/28/2007

3

Insider Attacks

- § Passively: not cooperating, falsifying coordinates
- § Actively: delaying probes
- § Or Both!



➔ Securing ICS is crucial for their deployment

8/28/2007

4

Rationale

- ICS are dynamics
 - n Coordinates keep changing

- Model of Normal behavior
 - n Need a "Clean" system

 - n Allow Abnormal behavior Detection
 - Comparing Model Predictions with observations (claims)

8/28/2007

5

Clean System? The Surveyors infrastructure

- Small Subset Trusted of nodes
 - n EXCLUSIVELY positioned using mutual measurements
 - No malicious Activity
 - n Involved in the ICS
 - USED by other nodes for positioning in the usual way

- Idea: Local behavior of a Surveyor is similar to that of other nearby nodes

8/28/2007

6

Nodes Behavior Model

- Measured Relative Error

$$D_n = \frac{|predicted - measured|}{measured}$$

- Model

$$D_n = \Delta_n + U_n$$

$$\Delta_{n+1} = b\Delta_n + W_n$$

Measurements errors,
Coordinates errors

RTTs fluctuations,
Modeling uncertainty

n Many sources contribute to errors

- Assumption: U_n and W_n follow Gaussian Distribution

- Empirically Validated

8/28/2007

7

Kalman Filter

- Separating nominal signal from noisy measurement

- Predicts the relative error $\hat{\Delta}_{n|n-1}$

- Characterizes the innovation process

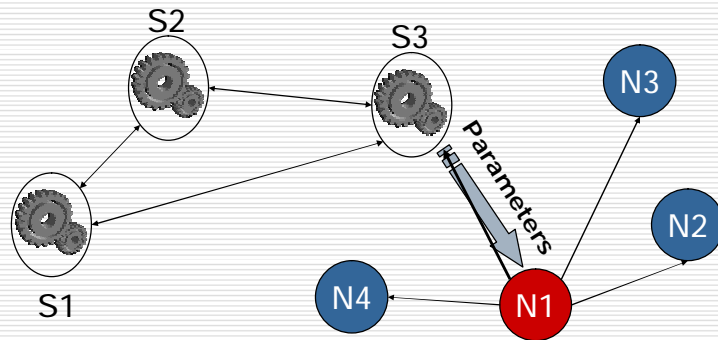
$$\eta_i = D_i - \hat{\Delta}_{i|i-1}$$

Abnormality = Significant Deviation
of the values of η_i

8/28/2007

8

Strategy



Step 1) Build a Normal Model with parameters to run parameter

8/28/2007

9

Abnormal Behavior Detection

- *Simple Hypothesis Testing*
 - n H_0 : the node has a Normal behavior
- FIND the threshold value t_n such that

$$P(|D_n - \hat{\Delta}_{n|n-1}| \geq t_n | H_0) = \alpha$$

α "significance-level"

8/28/2007

10

Abnormal Behavior Detection(2)

- If Observed deviation exceeds t_n :
 - n hypothesis is rejected
 - node is flagged as abnormal (potentially suspicious),
 - embedding step is aborted, and
 - measured relative error is discarded

8/28/2007

11

Validation

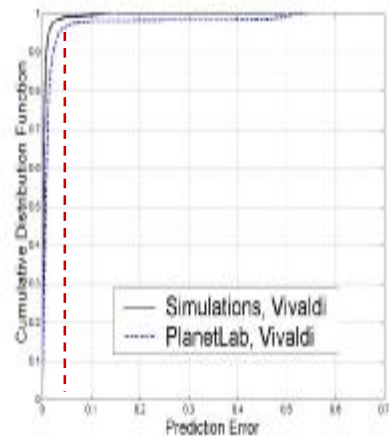
- Simulations
 - n King dataset
- PlanetLab
 - n 280 nodes
- Vivaldi and NPS
 - n Similar Results

8/28/2007

12

Validation (2): Model Accuracy

- Self-calibration of the Kalman filter
 - n at every node
 - n in a clean System



8/28/2007

13

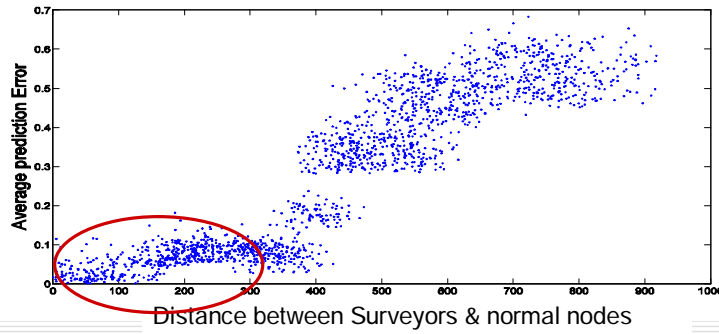
Representativeness of Surveyors

- Number of Surveyors Needed ?
- Randomly-chosen surveyors: 8% of population
 - n This is a conservative **upper bound**
- 1% with a simple K-means deployment
- Optimal is still open research issue

8/28/2007

14

Which Surveyor is representative?



§ Closer is better

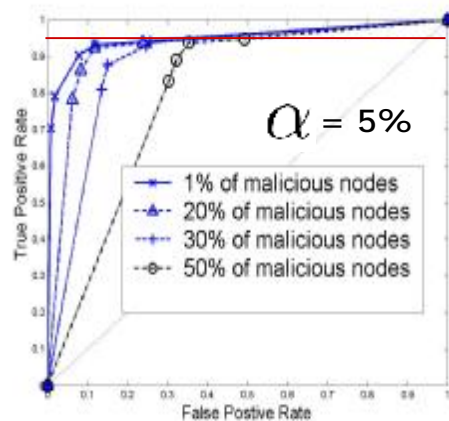
§ Close enough is good enough: **No need** for THE closest.

8/28/2007

15

Evaluation

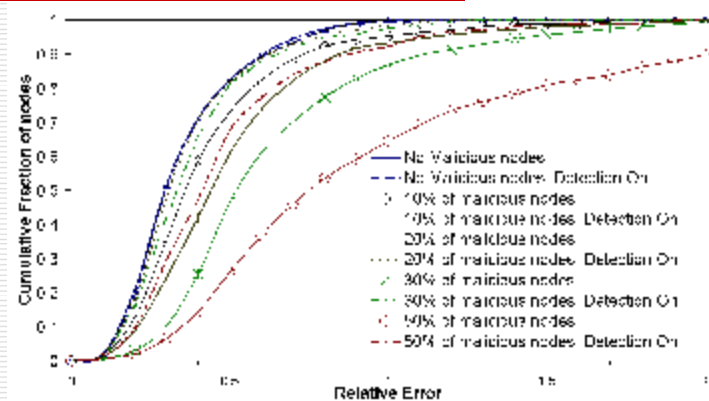
- ROC Curves
- Tradeoff FPR/TPR
- Higher Curves are better!
- Detection: Excellent up to 20% of malicious nodes
- Still performs well, under heavy attack, up to 30% of malicious Nodes



8/28/2007

16

Embedding System Performance



○ Practically immune to the attack $\alpha=5\%$

8/28/2007

17

Conclusions

- General Detection Method
 - n Decentralized
 - n Independent from the dimensions and the embedding protocol
- Very efficient although
 - n No trust propagation among normal nodes
- A "business"-driven strategic deployment could improve representativeness, and ? (why not) Security.

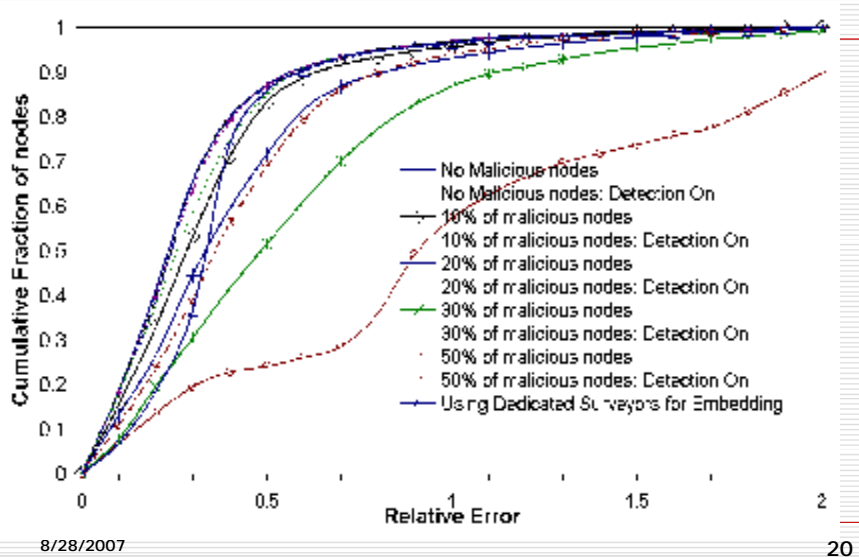
8/28/2007

18

Thanks!

Questions?

Using Surveyors for positioning other nodes



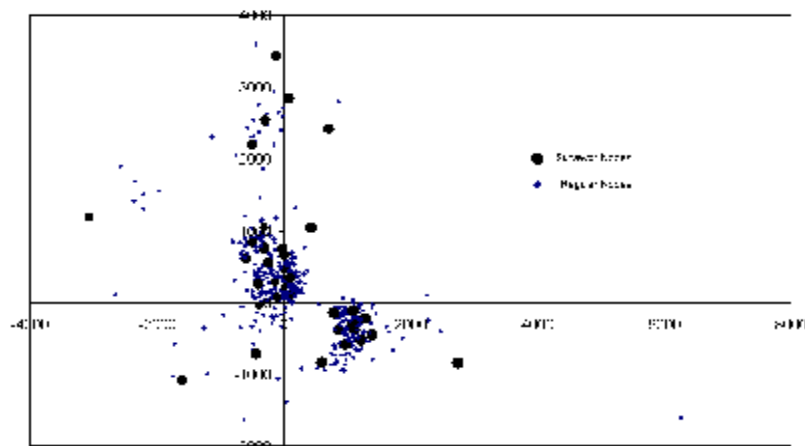
Future Works

- Don't Forget
 - n Still need to Secure the distance estimate phase
 - n Blatantly lie about coordinates when requested
 - n Certified Coordinates

8/28/2007

21

Surveyor nodes



8/28/2007

22

Kalman Filter equations

- 2 Steps: Prediction and Update

- Prediction Step: $\hat{\Delta}_{i|i-1} = \beta \hat{\Delta}_{i-1|i-1} + w$

■ Its a posteriori error variance is:

$$P_{i|i-1} = \beta^2 P_{i-1|i-1} + v_W.$$

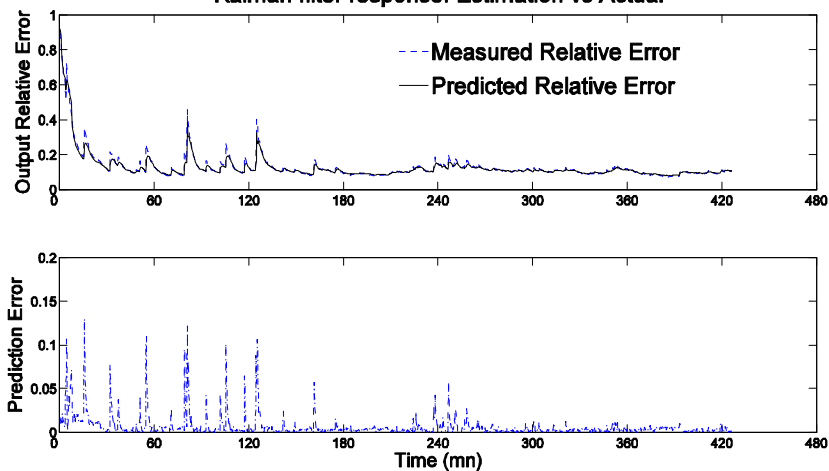
- Update Step, integrates the observed D_i :

$$\hat{\Delta}_{i|i} = \hat{\Delta}_{i|i-1} + K_i (D_i - \hat{\Delta}_{i|i-1})$$

$$K_i = \frac{P_{i|i-1}}{P_{i|i-1} + v_U} \quad P_{i|i} = \frac{v_U}{P_{i|i-1} + v_U} P_{i|i-1}$$

The vast majority of estimations are excellent

Kalman filter response: Estimation vs Actual



MALICIOUS BEHAVIOR DETECTION

- H_0 : The hypothesis that the peer node has a normal behavior (honest)

- PB: FIND the threshold value t_n such that

$$P(|D_n - \hat{\Delta}_{n|n-1}| \geq t_n \mid H_0) = \alpha$$

- We can demonstrate that:

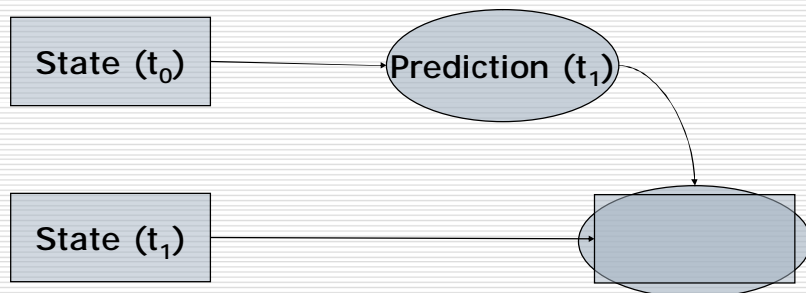
$$t_n = \sqrt{v_{\eta,n}} Q^{-1}(\alpha/2) \text{ where } Q(x) = 1 - \Phi(x)$$

$\Phi(x)$ CDF of $N(0,1)$, and α "significance-level"

8/28/2007

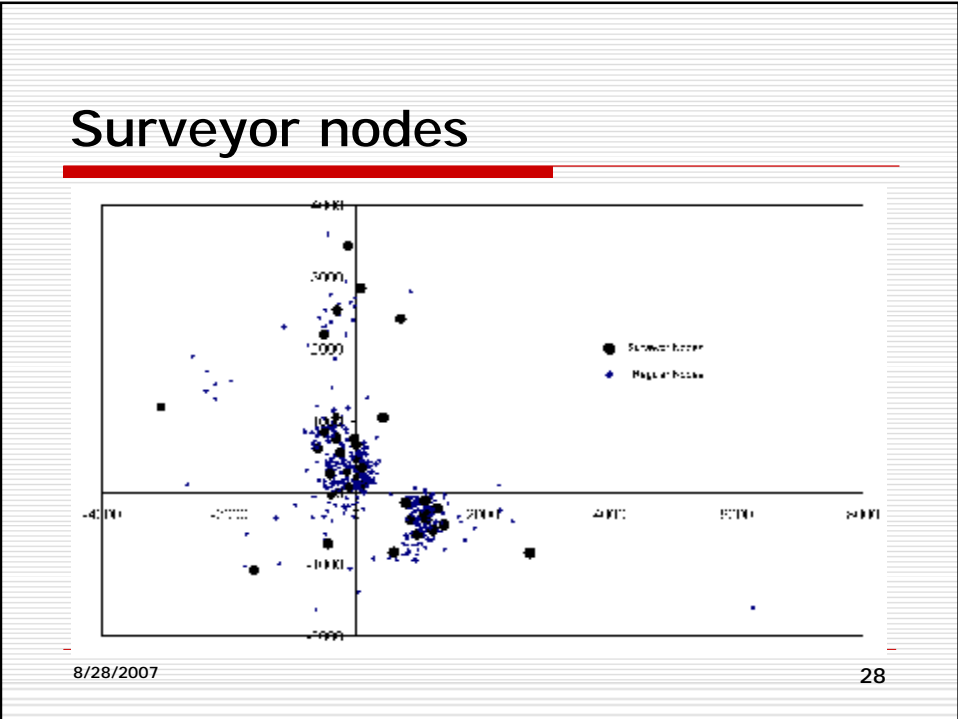
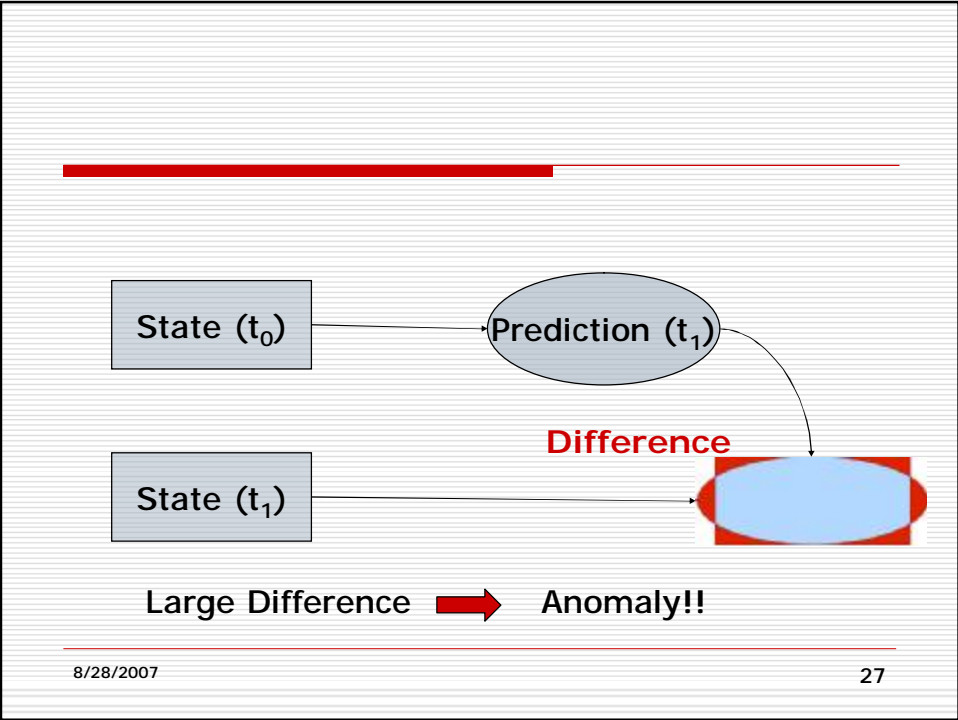
25

deviation Concept



8/28/2007

26



Strategy

Surveyors

- Inter-Surveyors measurements
- Calibrate Filters using Clean measurements
- Provide nodes with filter parameters

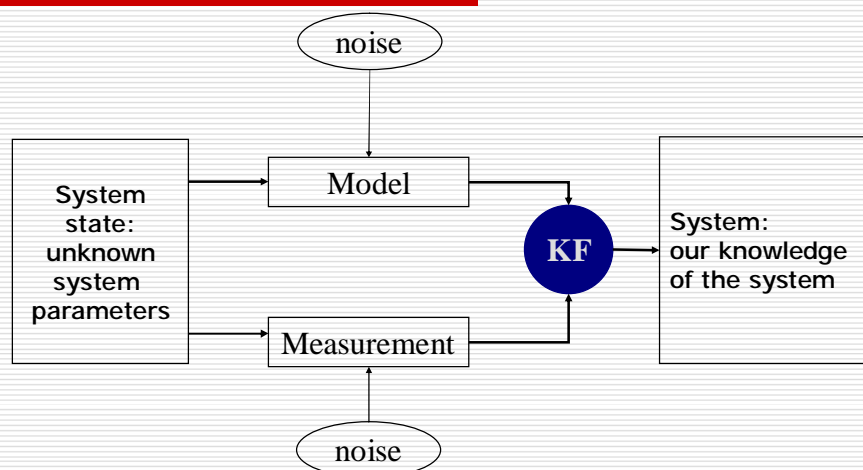
Nodes

- Select the closest Surveyor
- Run their filter with the provided parameters
- Filter-out abnormality

8/28/2007

29

Kalman Filter – KF



8/28/2007

30

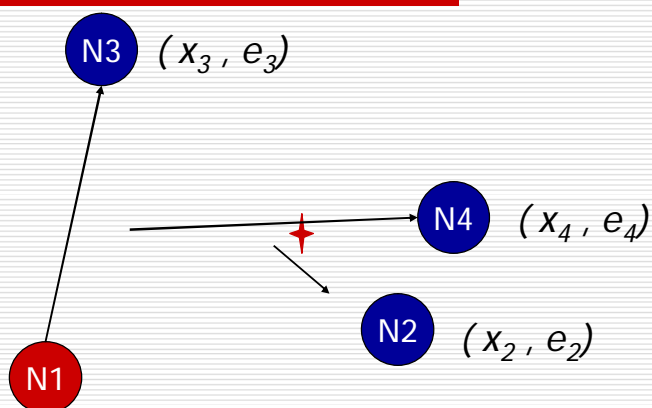
Attacks exploiting cooperation

- Means
 - n Passively: not cooperating, falsifying coordinates
 - n Actively: delaying probes
- Attacks
 - n Disorder (DoS)
 - n Isolation
 - n Repulsion (Free Riding)
 - n Collusion

8/28/2007

31

Vivaldi: Main Algorithm

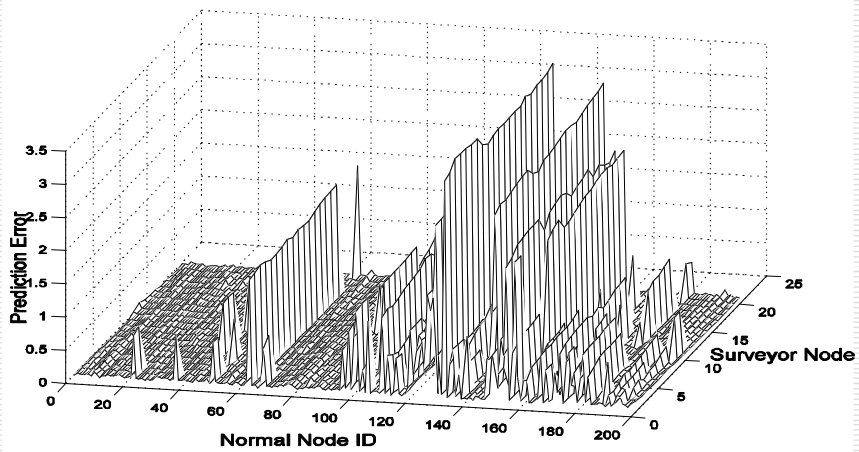


$$x_i = x_i + \delta \cdot (\text{rtt} - \|x_i - x_j\|) \cdot u(x_i - x_j)$$

8/28/2007

32

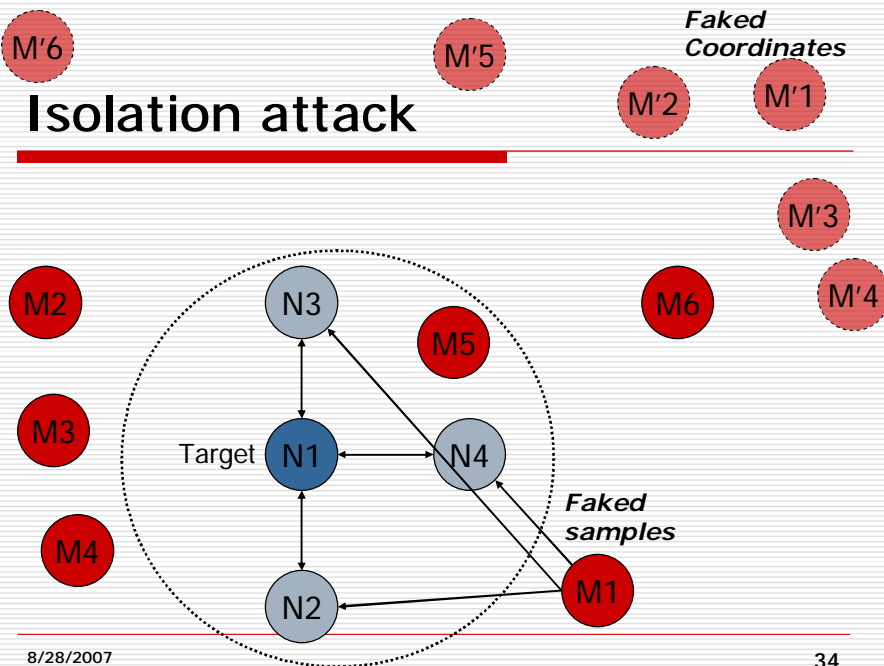
Which Surveyor?



8/28/2007

33

Isolation attack



8/28/2007

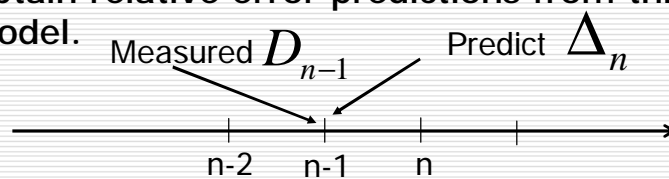
34

Linear state space model

$$\Delta_{n+1} = b\Delta_n + W_n$$

$$D_n = \Delta_n + U_n$$

- Obtain relative error predictions from this model.



8/28/2007

35

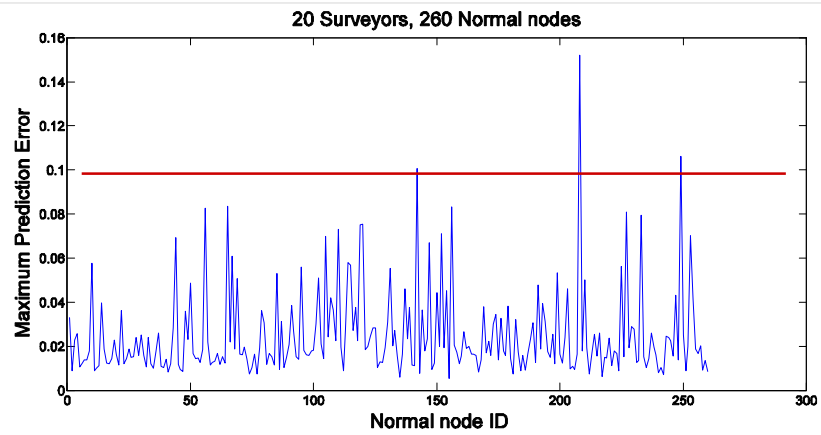
EM (Expectation Maximization) Method

- <http://www.gatsby.ucl.ac.uk/~zoubin/software.html>

8/28/2007

36

Using the closest surveyor's parameters



8/28/2007

37