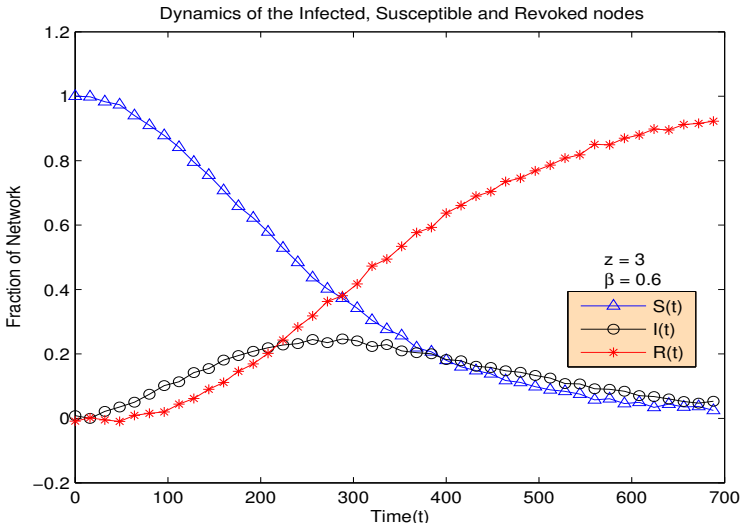
Simulation Study

- Objective is to capture the time dynamics of the spread of compromise
- Observe the duration and nature of the gradual recovery process with time
- Observe the effects of various parameters of network
  - Average node degree of key sharing network
  - Average infection rate
  - Average duration of infectivity

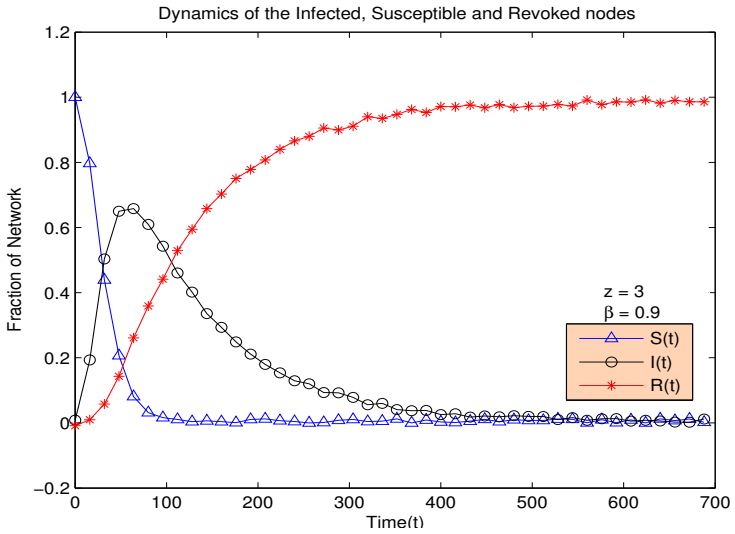
Simulation Results

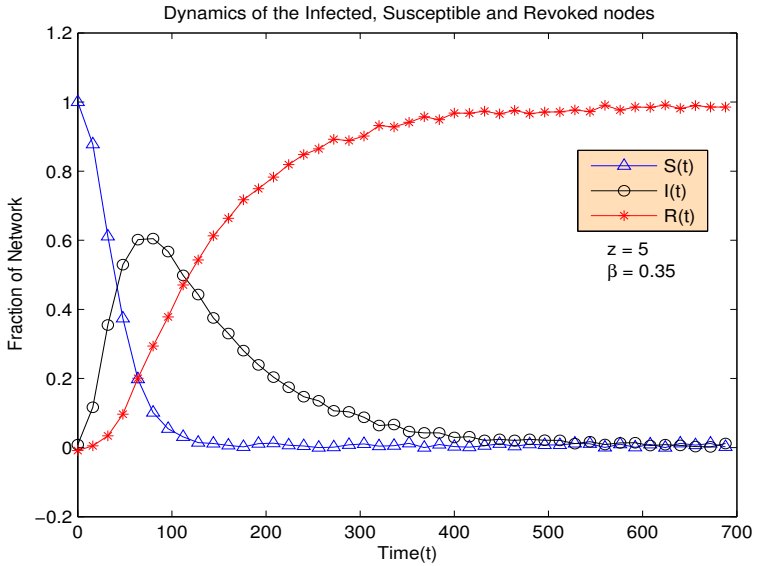
Under both scenarios – no node recovery and node recovery

$\tau = 30$

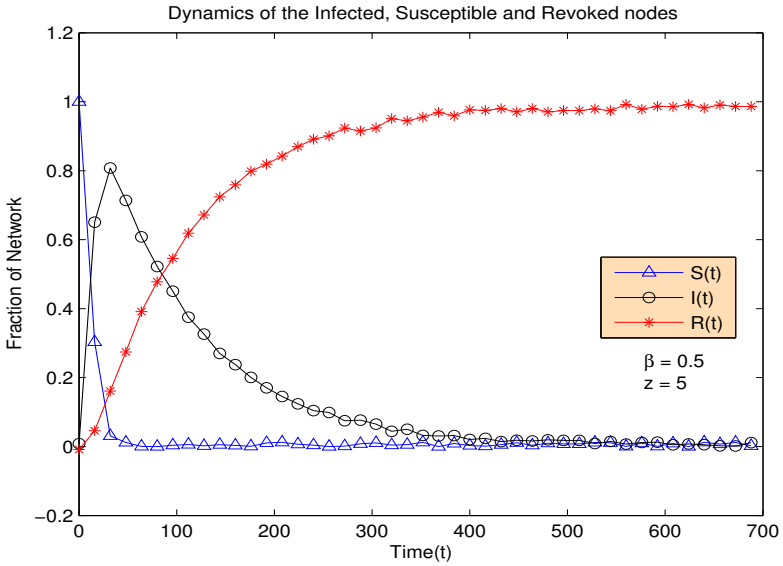


$\tau = 10$





$\tau = 10$



$\tau = 10$

Outline

- Introduction to Wireless Sensor Networks (WSNs)
- Security Challenges and Need for Multi-level Approach
- Node Compromise Modeling
- Trust / Model for Secure Data Aggregation
- Revoking Compromised Nodes
- Conclusion

Goals of a Trusted System

- Intrusion detection and protection against DoS attacks
- Secure data aggregation and routing capabilities
- Ensure information accuracy and confidentiality
- Reduce risk by real-time monitoring and response
- Achieve robustness in the presence of *insider attacks*

Attack: False data injection by compromised nodes

Our Motivations

- In WSNs, data are noisy (uncertain) and unreliable
- Redundancy from highly dense deployed sensors may provide “side information” for data fusion
  - e.g., How to exploit redundancy for abnormality detectection?
- Precise fusion is difficult with multiple questionable data
  - How to represent uncertainty in the aggregation result?
    e.g., Is there any measure to interpret the ignorance in fusion?
  - How to quantify uncertainty when fusion results are propagated?
    e.g., How to evaluate a hierarchical, bottom-up fusion result?

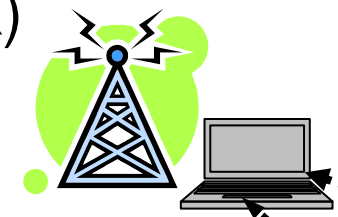
Developing Belief / Trust Model

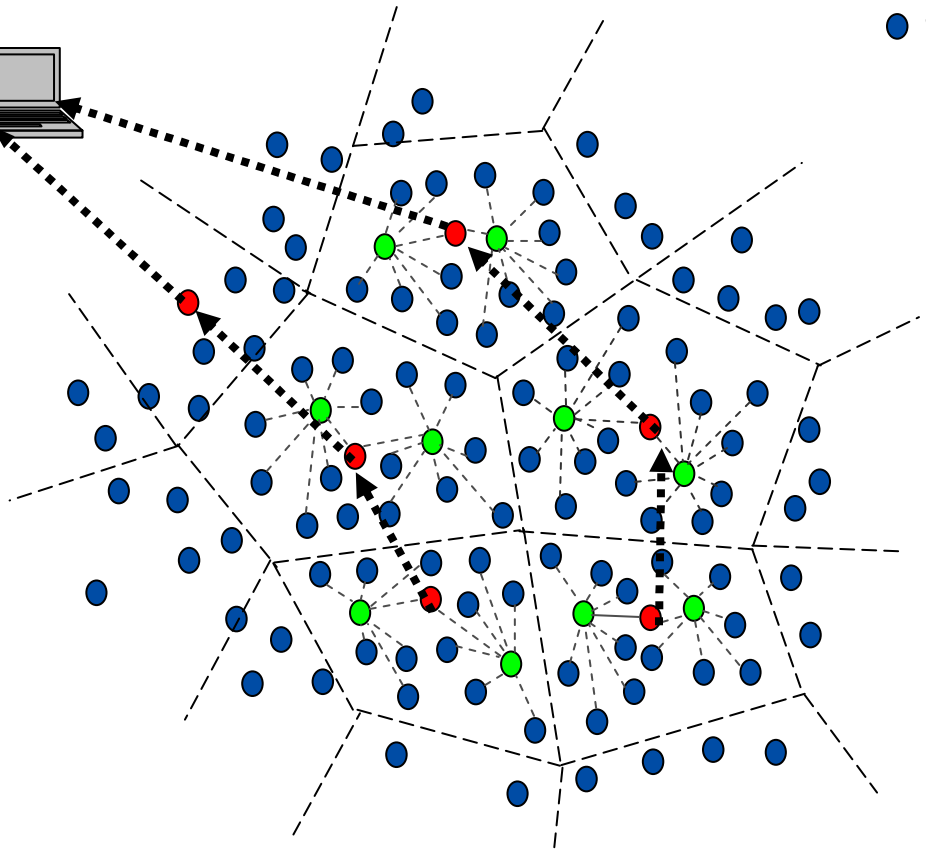
- Premise: False data injection from compromised nodes
  - Cryptographic techniques ineffective
- Objectives: Trust model to identify and purge false data. Reduce uncertainty in information aggregation.
- Solution:
  - Information theoretic (relative entropy) measure to quantify reputation / opinion of data, leading to higher confidence
    - Belief, disbelief, uncertainty, relative atomicity
  - Josang's belief model to define and manage trust propagation through intermediate nodes along the route
  - Identify malicious nodes by learning and outlier classification – purge false data to achieve secure aggregation

[W. Zhang, S. Das and Y. Liu, "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks, *IEEE SECON*, Oct 2006.]

Sensor Network Model

Base Station
(Sink)





- cluster head
- aggregator
- sensor nods (cluster member)

Network Model

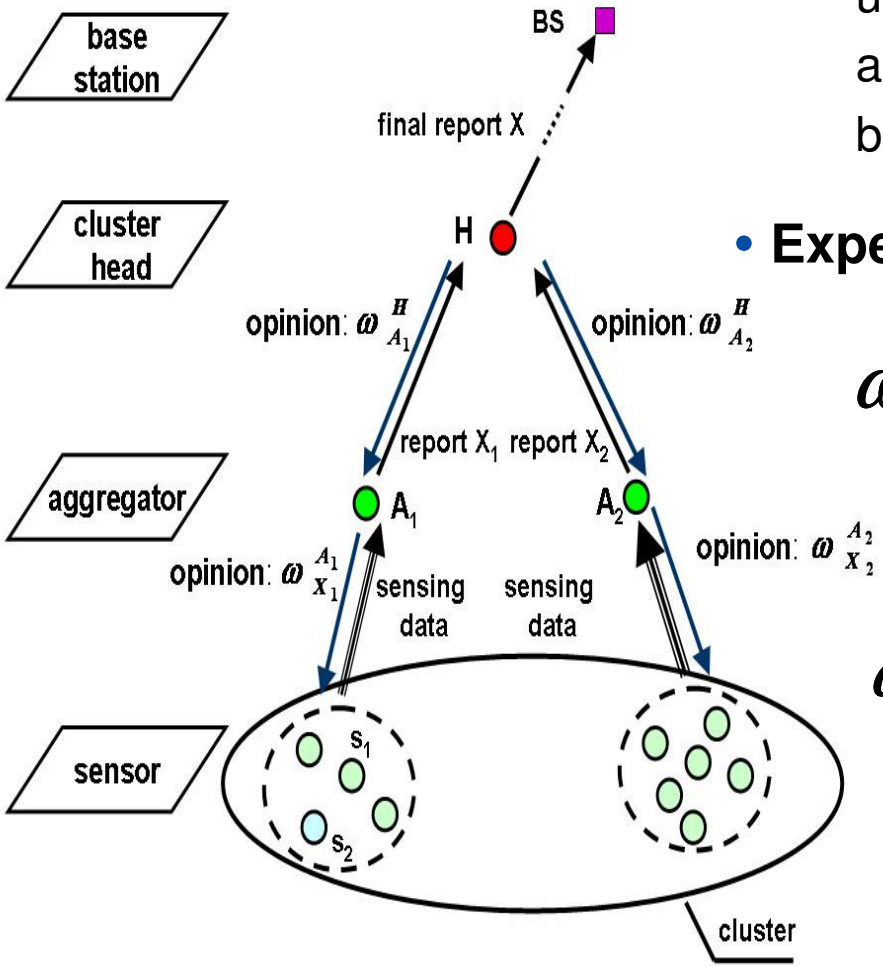
- **Network organized into clusters**
  - Base station, cluster heads, aggregators, sensor nodes
- **Sensor node (cluster member)**
  - Bidirectional communication capability
  - Aware of its one-hop neighbors
  - Message authentication code (MAC) via pair-wise key with each neighbor
- **Aggregator (A)**
  - Sampling, aggregating
- **Cluster Head (H)**
  - Gateway outside the cluster
- **In each cluster, sensor nodes including aggregators and cluster head monitor the environment similarly**

Threat Model

- **Compromised by physical capture or malicious code**
- **Attacker gains full control of compromised nodes (secret keys)**
- **Compromised nodes inject false data to disrupt normal network operations**
- **Compromised nodes**
  - Sensors, aggregators, cluster heads
  - Same capability as legitimate nodes

Josang's Belief Model

- **Opinion: $\omega = (b, d, u, a)$, $b + d + u = 1$**
  - b: belief
  - d: disbelief
  - u: uncertain
  - a: relative atomicity
  - b, d, u, a $\in$ [0,1]



- **Expected Opinion: $O = E(\omega) = b + au$**

ω_A^H **: Cluster head's opinion about aggregator**

$$\omega_{A_1}^{H} = (0.95, 0.03, 0.02, 0.5)$$

$$O_{A_1}^{H} = 0.95 + 0.5 * 0.02 = 0.96$$

ω_X^A **: Aggregator's opinion about its report X**

$$\omega_X^{A1} = (0.688, 0, 0.312, 0.9)$$

$$O_X^{A1} = 0.688 + 0.9 * 0.312 = 0.969$$

Belief Propagation: Subjective Logic

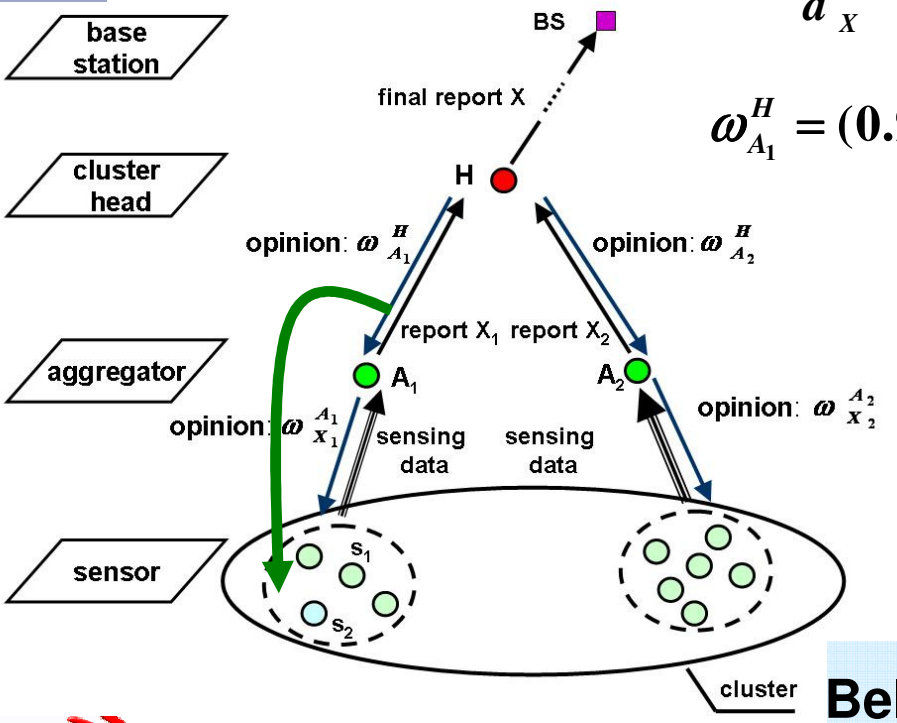
- **Belief discounting (recommendation)**

  Cluster head's opinion about X as a result of aggregator's opinion:

$$\omega_X^{H:A} = \omega_A^H \otimes \omega_X^A = (b_X^{H:A}, d_X^{H:A}, u_X^{H:A}, a_X^{H:A})$$

$$b_X^{H:A} = b_A^H * b_X^A \qquad u_X^{H:A} = d_A^H + u_A^H + b_A^H u_X^A$$

$$d_X^{H:A} = d_A^H * d_X^A \qquad a_X^{H:A} = a_X^A$$



$$\omega_{A_1}^H = (0.95, 0.03, 0.02, 0.5); \omega_X^{A_1} = (0.688, 0, 0.312, 0.9)$$

$$b_X^{H:A_1} = 0.95 * 0.688 = 0.654$$

$$d_X^{H:A_1} = 0$$

$$u_X^{H:A_1} = 0.03 + 0.02 + 0.95 * 0.312 = 0.364$$

$$a_X^{H:A_1} = 0.9$$

$$\omega_X^{H:A_1} = (0.654, 0, 0.364, 0.9)$$

Belief decreases, uncertainty increases

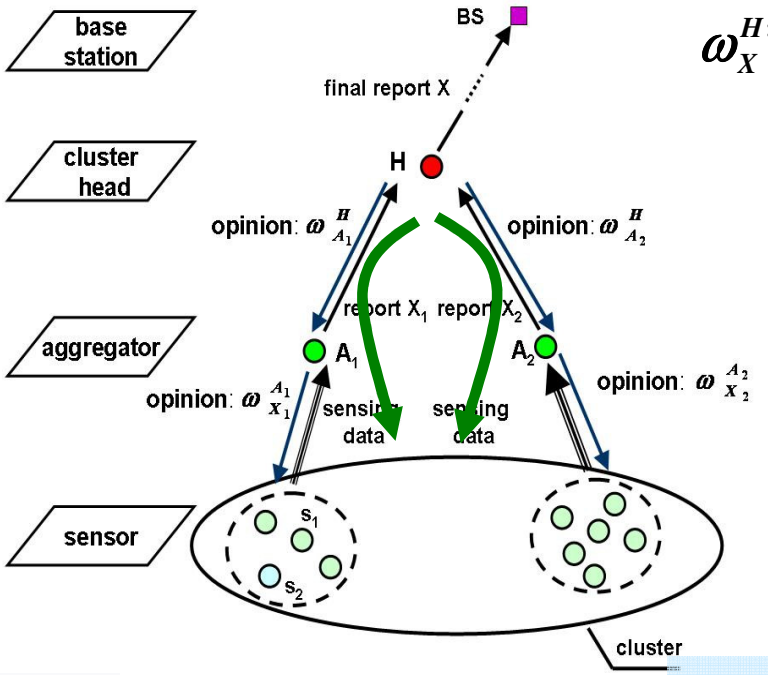
Belief Consensus

Cluster head's opinion about X via A_1: $\omega_X^{H:A_1} = (b_X^{H:A_1}, d_X^{H:A_1}, u_X^{H:A_1}, a_X^{H:A_1})$

Cluster head's opinion about X via A_2: $\omega_X^{H:A_2} = (b_X^{H:A_2}, d_X^{H:A_2}, u_X^{H:A_2}, a_X^{H:A_2})$

Cluster head's consensus opinion about X:

$$\omega_X^{H:A_1,H:A_2} = \omega_X^{H:A_1} \oplus \omega_X^{H:A_2} = (b_X^{H:A_1,H:A_2}, d_X^{H:A_1,H:A_2}, u_X^{H:A_1,H:A_2}, a_X^{H:A_1,H:A_2})$$



$$\omega_X^{H:A_1} = (0.654, 0, 0.346, 0.9); \omega_X^{H:A_2} = (0.368, 0, 0.632, 0.7)$$

$$b_X^{H:A_1,H:A_2} = \frac{0.654*0.632+0.368*0.346}{0.346+0.632-0.346*0.632} = 0.712$$

$$d_X^{H:A_1,H:A_2} = 0$$

$$u_X^{H:A_1,H:A_2} = \frac{0.346*0.632}{0.346+0.632-0.346*0.632} = 0.288$$

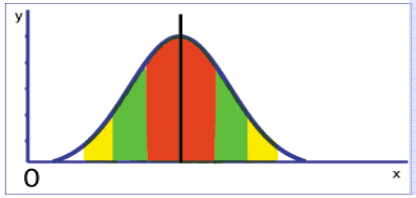
$$a_X^{H:A_1,H:A_2} = \frac{0.7*0.346+0.9*0.63-(0.7+0.9)*0.35*0.63}{0.35+0.63-2*0.35*0.63} = 0.85$$

$$\omega_X^{H:A_1,H:A_2} = (0.712,\ 0,\ 0.288,\ 0.85)$$

More evidences, belief in the result increases

Aggregator: Reputation computation for each sensor node

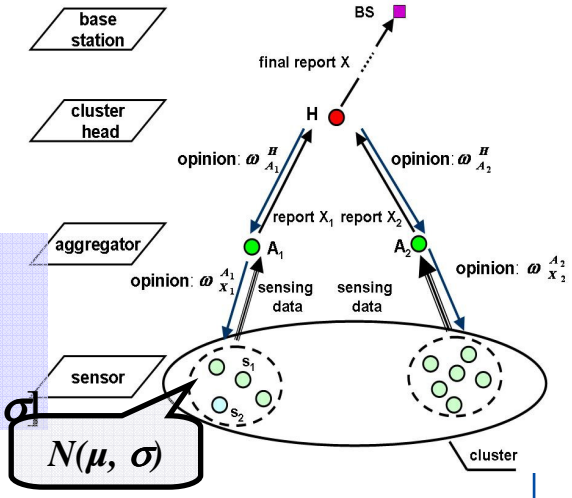
- **Outlier exclusion: Too far from median => outlier**
- **High density => Normal distribution *N(μ, σ)***



Red: 68% of data within [μ- σ, μ+σ]

Green: 95% of data within [μ- 2σ, μ+2σ]

Yellow: 99.7% of data within [μ- 3σ, μ+3σ]



- **Each sampling independent**
  - Ideal node frequency: in long run, $\mathbf{Pr}(p_i \mid x_i \in [\bar{x} - \sigma, \bar{x} + \sigma]) = 0.68$
  - Actual node frequency: $\mathbf{Pr}(q_i \mid x_i \in [\bar{x} - \sigma, \bar{x} + \sigma])$, learn from observation
  - Measure difference in ideal and actual frequencies: **Kullback Leibler distance**

$$D(p \parallel q) = \sum p(x) \log \frac{p(x)}{q(x)};$$

p(x), q(x) prob. mass function for ideal/actual node freq.
D(.) also called relative entropy measure

- **Reputation:** $r = \frac{1}{1 + \sqrt{D}}$

The shorter distance, more trustworthy, higher reputation

Sensor Node's Reputation: Example

- Two sensors, s_1 and s_2
  - Time t_1: $f_{s_1}^{t_1} = 0.65$, $f_{s_2}^{t_1} = 0.63$

$$D(f_{s_1}^{t_1} \,\|\, f_{ideal}^{t_1}) = (1-0.65) * \log \frac{(1-0.65)}{(1-0.68)} + 0.65 * \log \frac{0.65}{0.68} = 0.0029$$

$$r(s_1^{t_1}) = \frac{1}{1+\sqrt{0.0029}} = 0.949$$

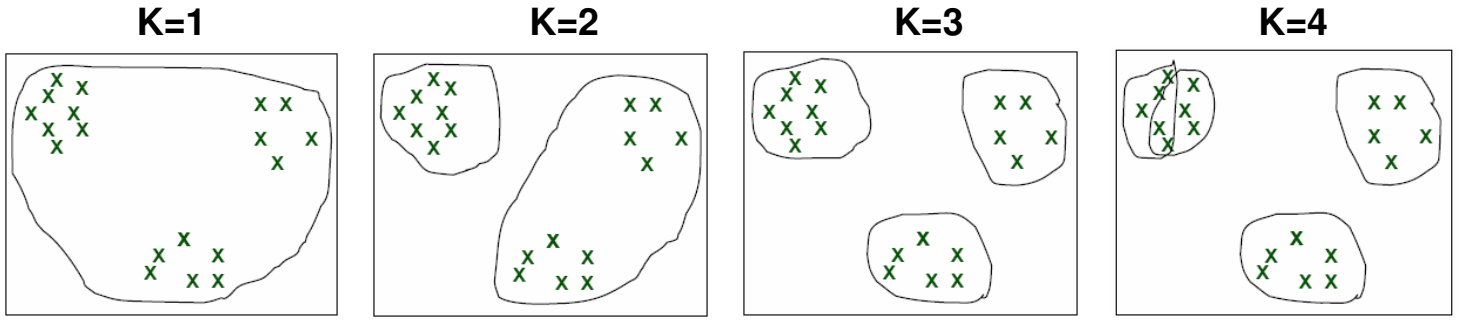
  - Time t_2: $f_{s_1}^{t_2} = 0.68$, $f_{s_2}^{t_2} = 0.30$

Time	Sensor node	Actual freq.	Ideal freq.	KL-distance	Reputation
t_1	s_1	0.65	0.68	0.0029	0.949
	s_2	0.63	0.68	0.0081	0.918
t_2	s_1	0.68	0.68	0	1
	s_2	0.30	0.68	0.436	0.602

Reputation changes with time based on behavior

Aggregator: Reputation Classification

- **Classify reputation to identify malicious nodes**
  - **Traditional system: threshold based classification**
  - **Online unsupervised learning, K-mean algorithm**
  - **No prior K available, how to dynamically decide K?**



Determining K

Ex:

Time	Sensor node	Reputation
t_1	s_1	0.949
	s_2	0.918
t_2	s_1	1
	s_2	0.602

1 group

2 group3

Aggregator: Opinion Formulation

- **Degree of trust in aggregation result**

$$\omega_X^A = (b_X^A, d_X^A, u_X^A, a_X^A)$$

- **Trustworthy**

  Nodes whose data close to mean

- **Uncertain**

  Nodes whose data not close to mean

  Uncertain nodes' reputation

  - how much contribution to expected opinion?

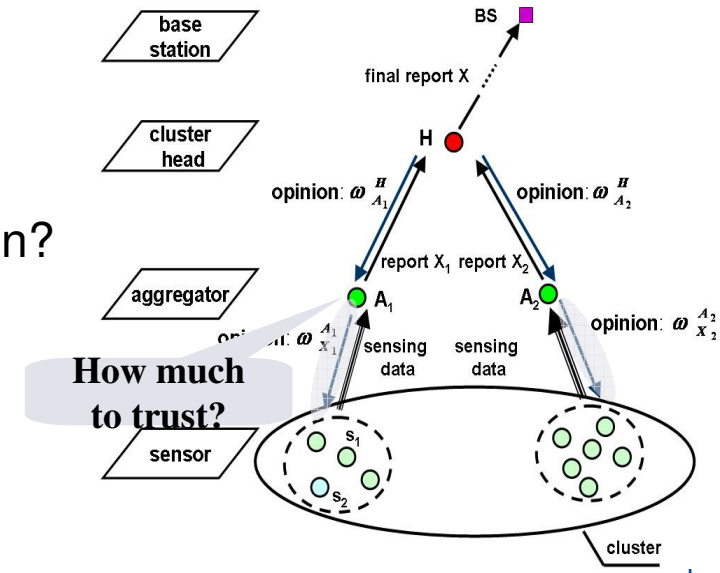
- **Formulation**

  belief: percentage in ($\bar{x} \pm \sigma$)

  disbelief: 0 (after excluding outlier)

  uncertain: percentage out of above range

  relative atomicity: reputation of nodes fall out the range



Cluster Head Operations

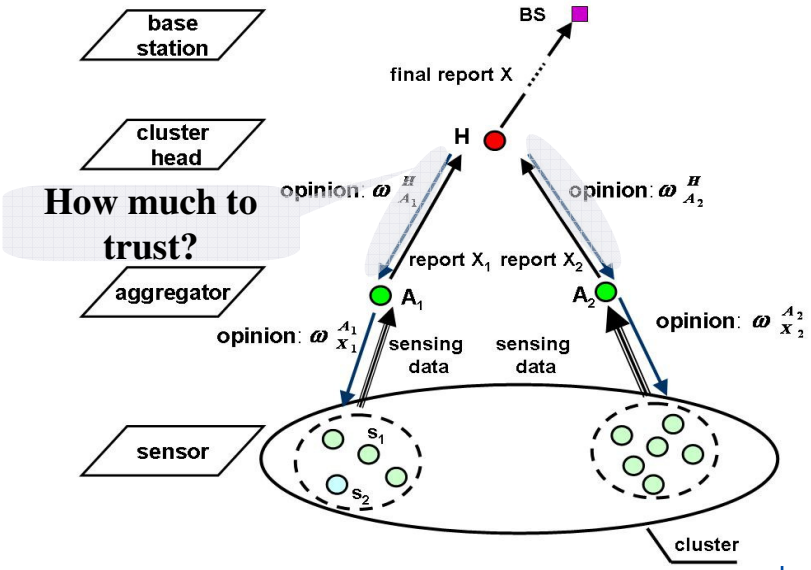
- **Opinion about aggregator:** $\omega_A^H = (b_A^H, d_A^H, u_A^H, a_A^H)$
  - Check consistency: its own data and all aggregators' reports
  - Match majority: honest
  - Otherwise: dishonest
  - binary event (honest/dishonest)
  - Opinion formulation

$$b_A^H = \frac{k_A^H}{k_A^H + l_A^H + 2}; d_A^H = \frac{l_A^H}{k_A^H + l_A^H + 2}$$

$$u_A^H = \frac{2}{k_A^H + l_A^H + 2}; a_A^H = 0.5$$

k_A^H: **Number of honest events**

l_A^H: **Number of dishonest events**



Cluster Head (Cont.)

- **Discount aggregator's belief:** $\omega_x^{H:A} = \omega_A^H \otimes \omega_x^A$

- **Final result and belief consensus (two aggregators)**
  - Result: $X_{final} = \omega_1 * X_1 + \omega_2 * X_{2;}$

$$\omega_i = E(\omega_X^{H:A_i}) / (E(\omega_X^{H:A_1} + \omega_X^{H:A_2})$$

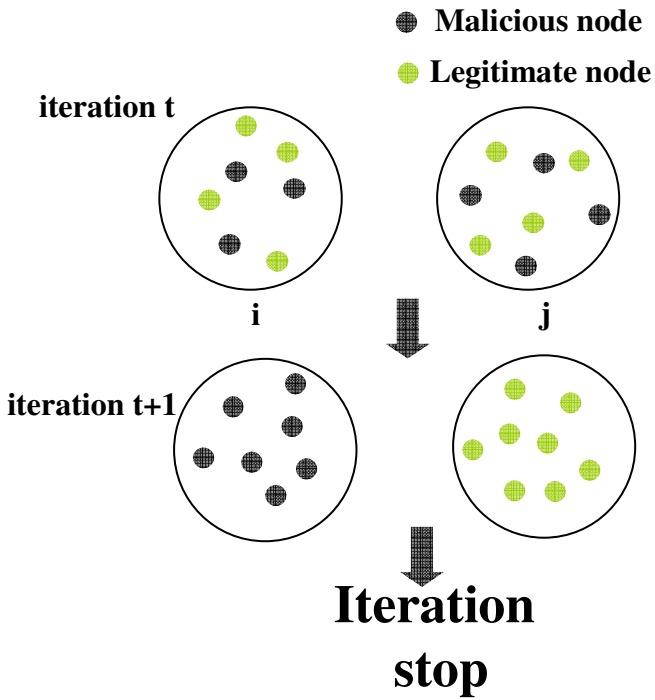
  - Belief consensus:

$$\omega_X^{H:A_1,H:A_2} = \omega_X^{H:A_1} \oplus \omega_X^{H:A_2}$$

Performance Analysis

- **Theorem: lower bound of K-mean based classification algorithm to distinguish malicious from good:**

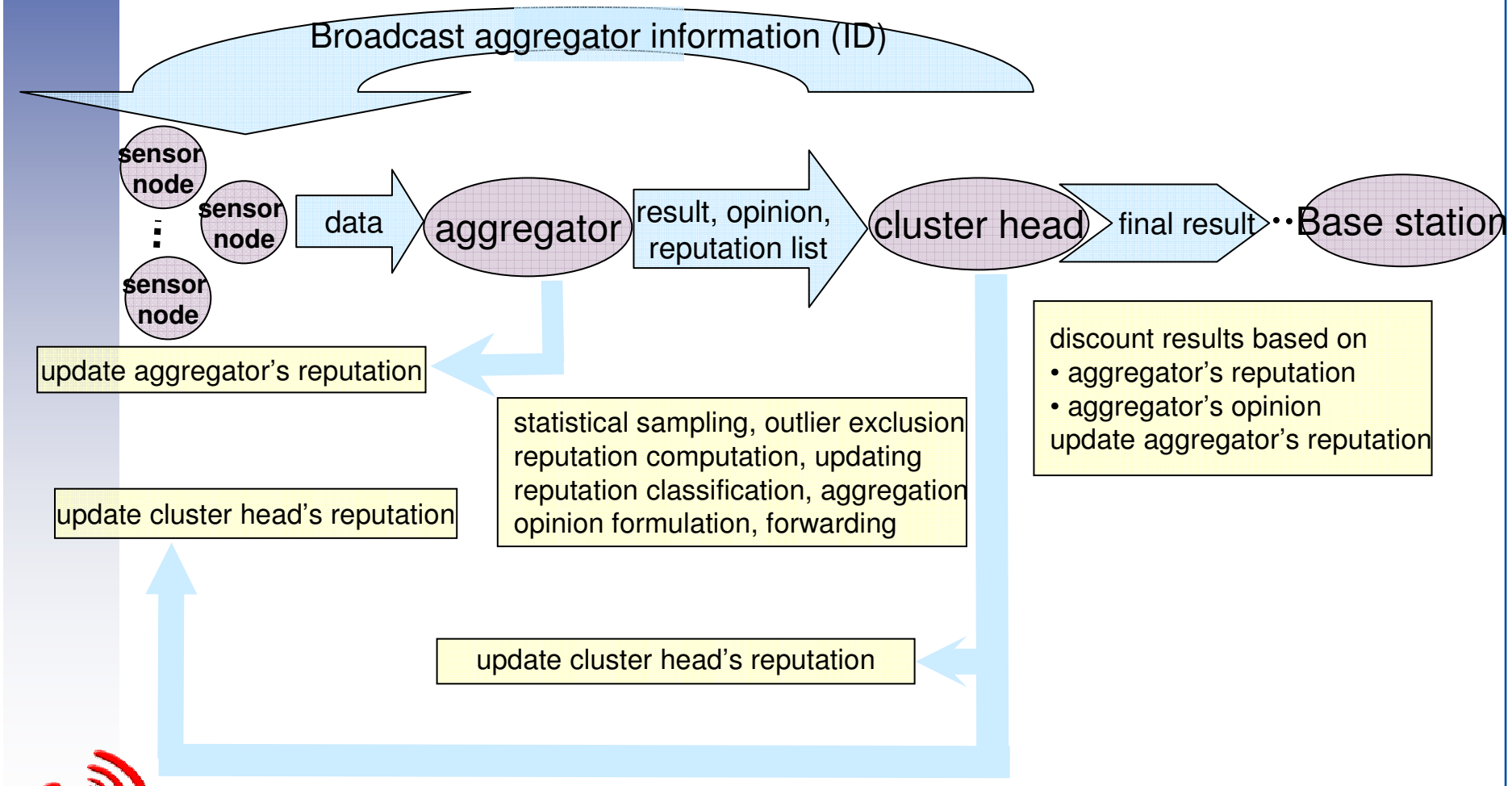
$$r_{g_{\min}} - r_{b_{\max}} > \frac{\Delta}{|G_i - G_j|}$$



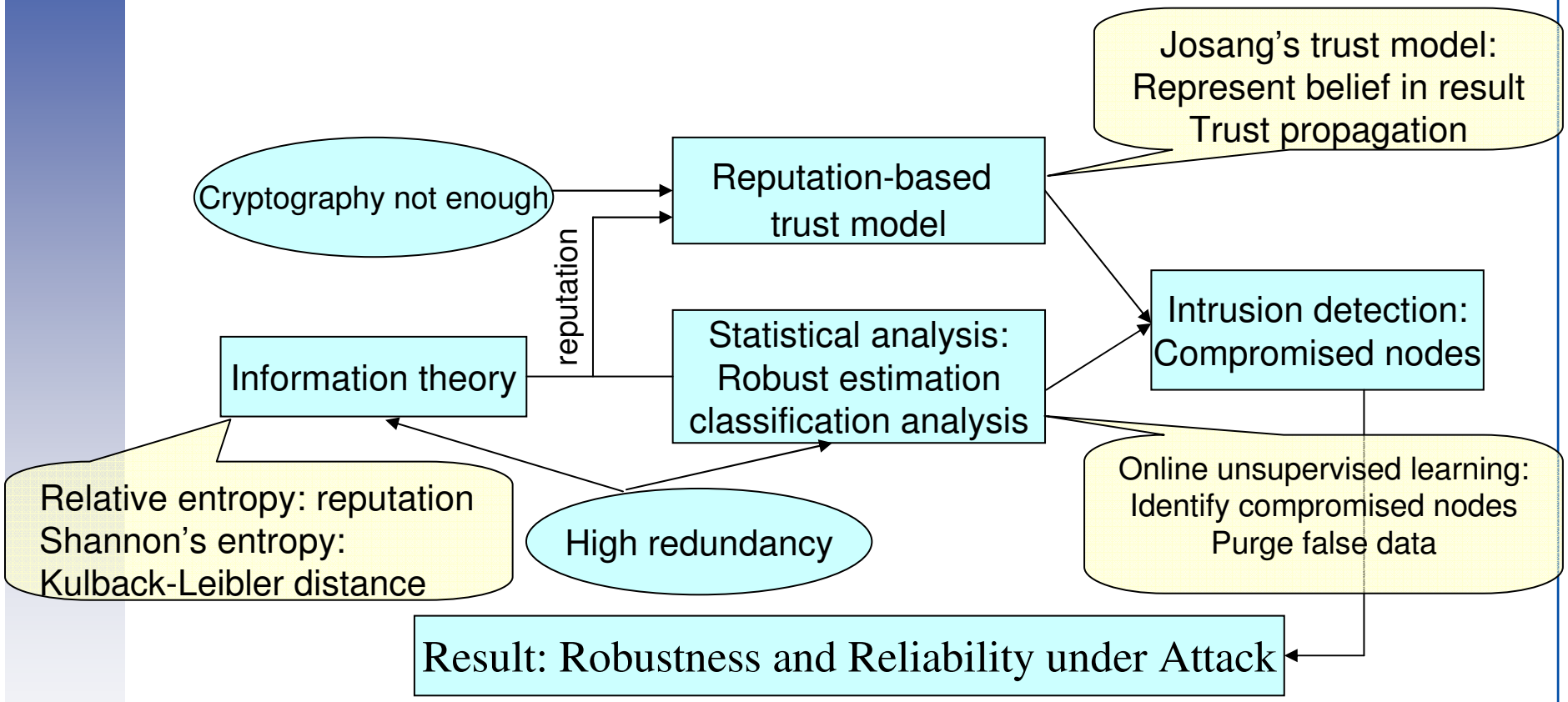
r_{gmin}: online minimal reputation for legitimate nodes;
r_{bmax},: online maximal reputation for malicious nodes;
Δ: threshold of difference in reputation;
G_i and G_j: percentage of good nodes in group G_i and G_j

Classification based on deference between reputation instead of absolute reputation value

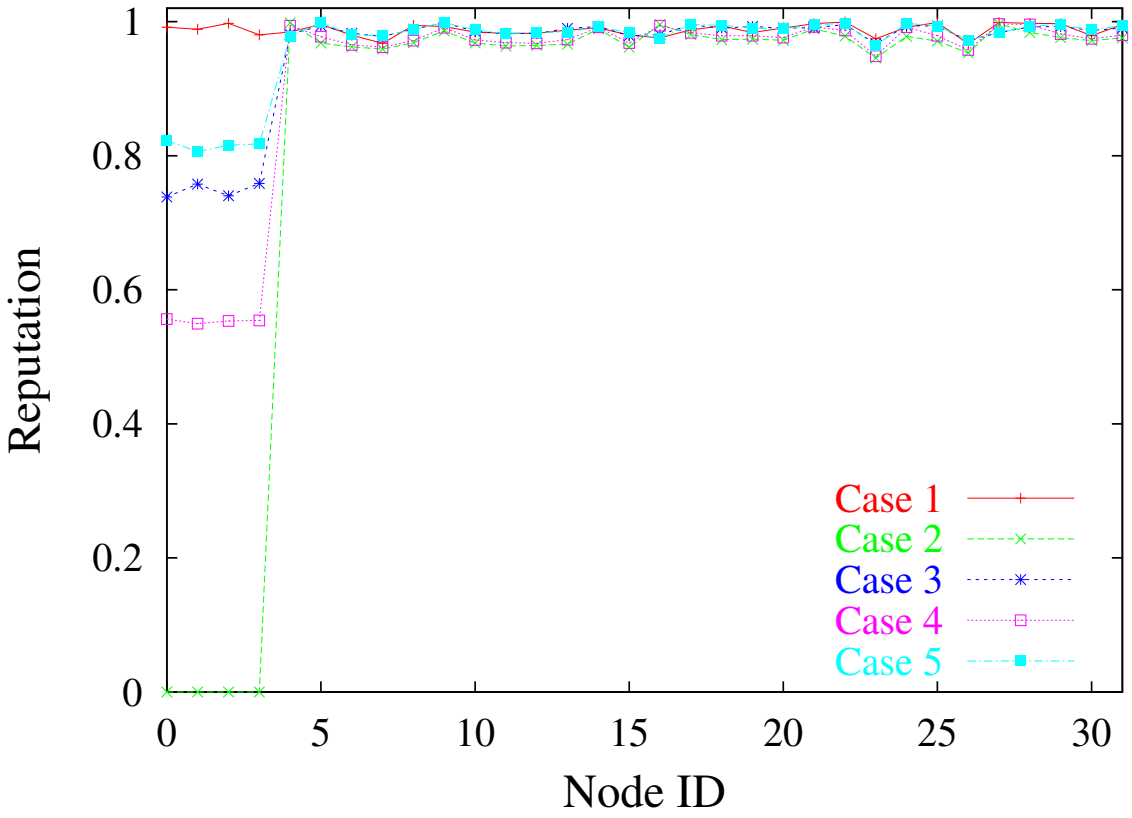
Trust Based Framework



Design Paradigm



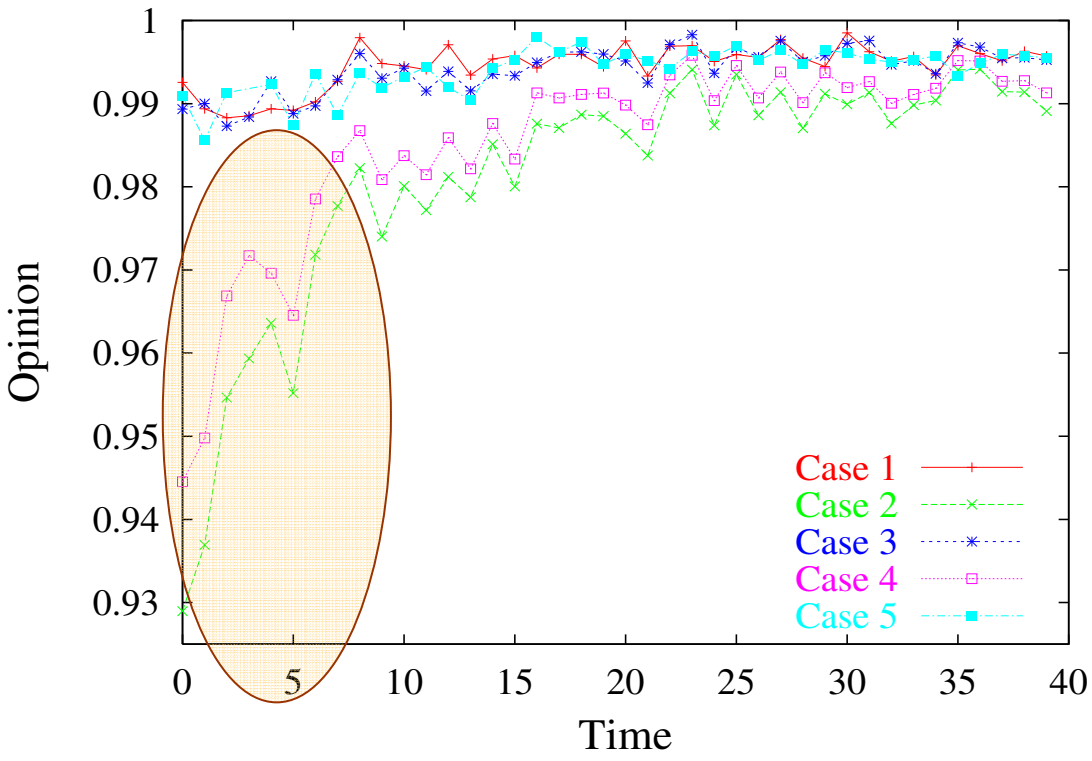
Simulation Results: Reputation



Case No.	Misbehaving time (%)	False data type
1	0	N/A
2	100	Obvious
3	100	Tricky
4	66	Obvious
5	66	Tricky

- No malicious nodes, all nodes' reputation close to 1
- Reputation of malicious nodes significantly lower than legitimate ones
- Reputation of malicious nodes proportional to amount of true data they send

Simulation Result: Opinion



Test case

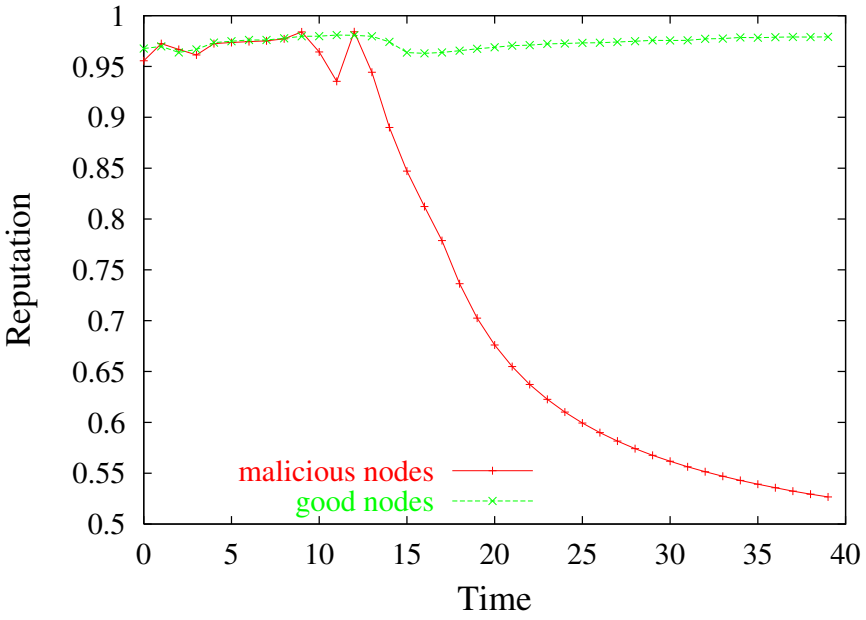
Case No.	Misbehaving time (%)	False data type
1	0	N/A
2	100	Obvious
3	100	Tricky
4	66	Obvious
5	66	Tricky

- False data sneaking into aggregation (Cases 2, 4) may affect result ➔ "pollute" legitimate node's reputation
- Low opinion or polluted reputation ➔ result from low reputation nodes
- Detection/blocking malicious nodes ➔ opinion / confidence increases
- Opinion correctly represents the belief in the result

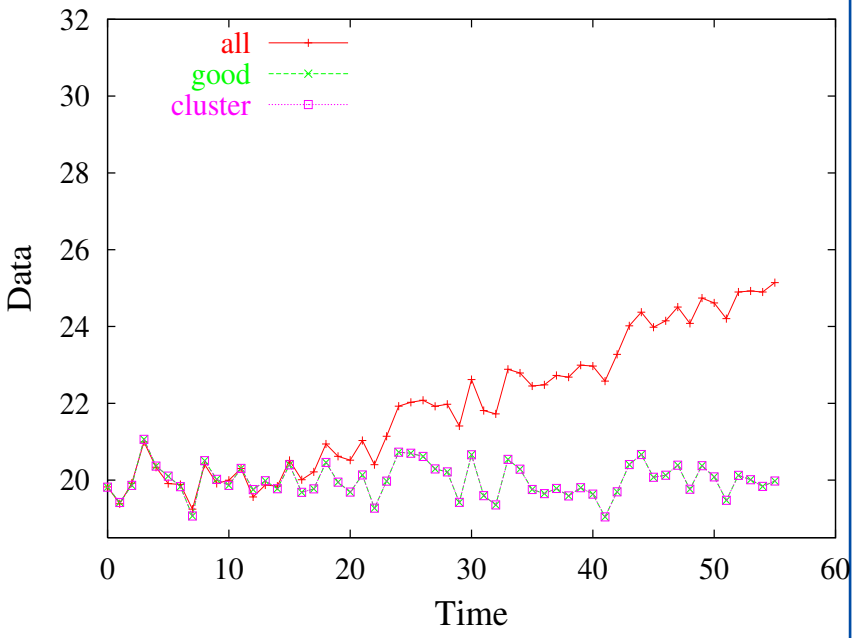
Cooperative Malicious Nodes (10%)

Scenario: Malicious nodes behave "good" at first 1/3 experiment, then they all send same data each time

Evolution of Reputation



Aggregation Result

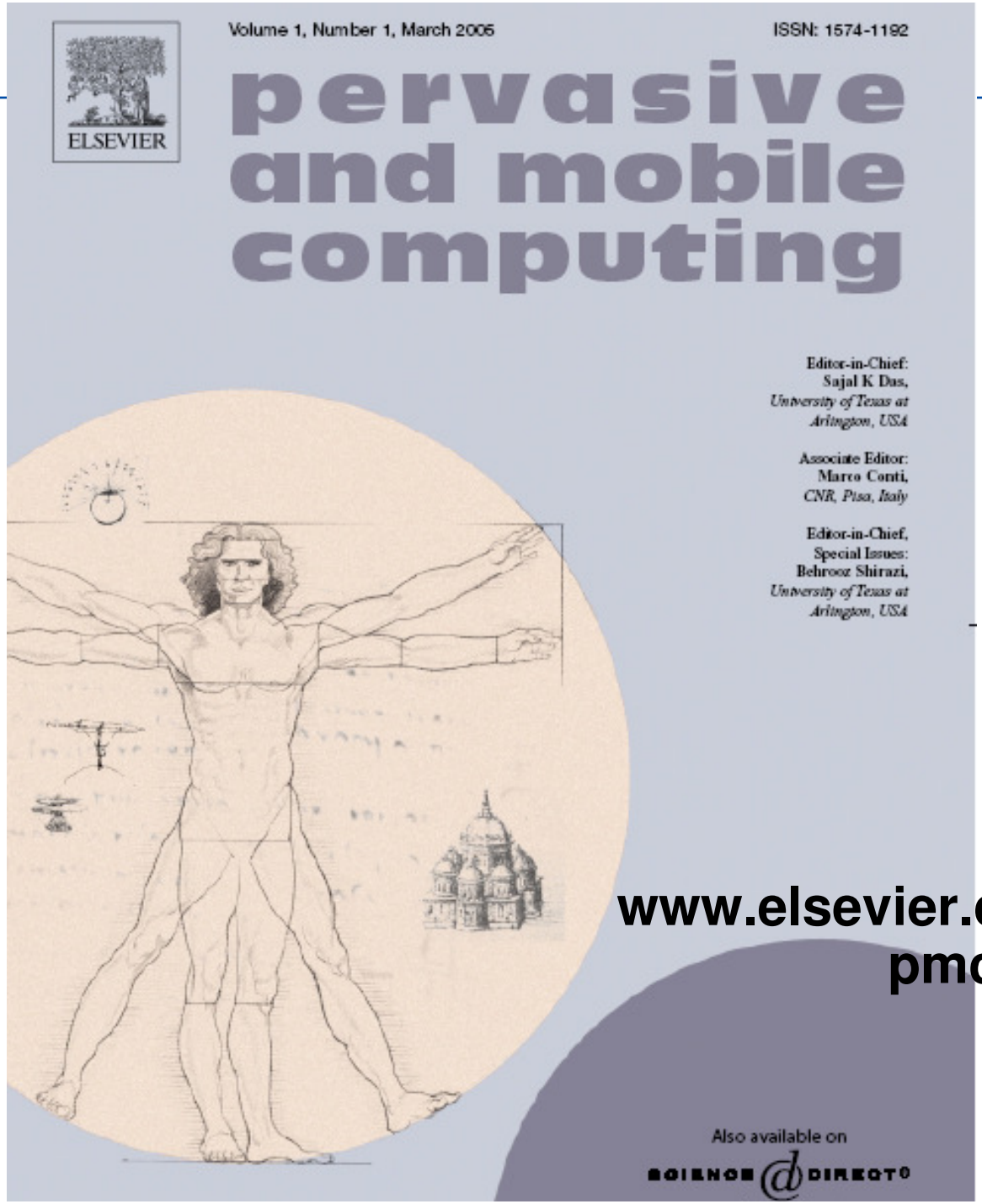


Malicious nodes can be identified as long as they misbehave.

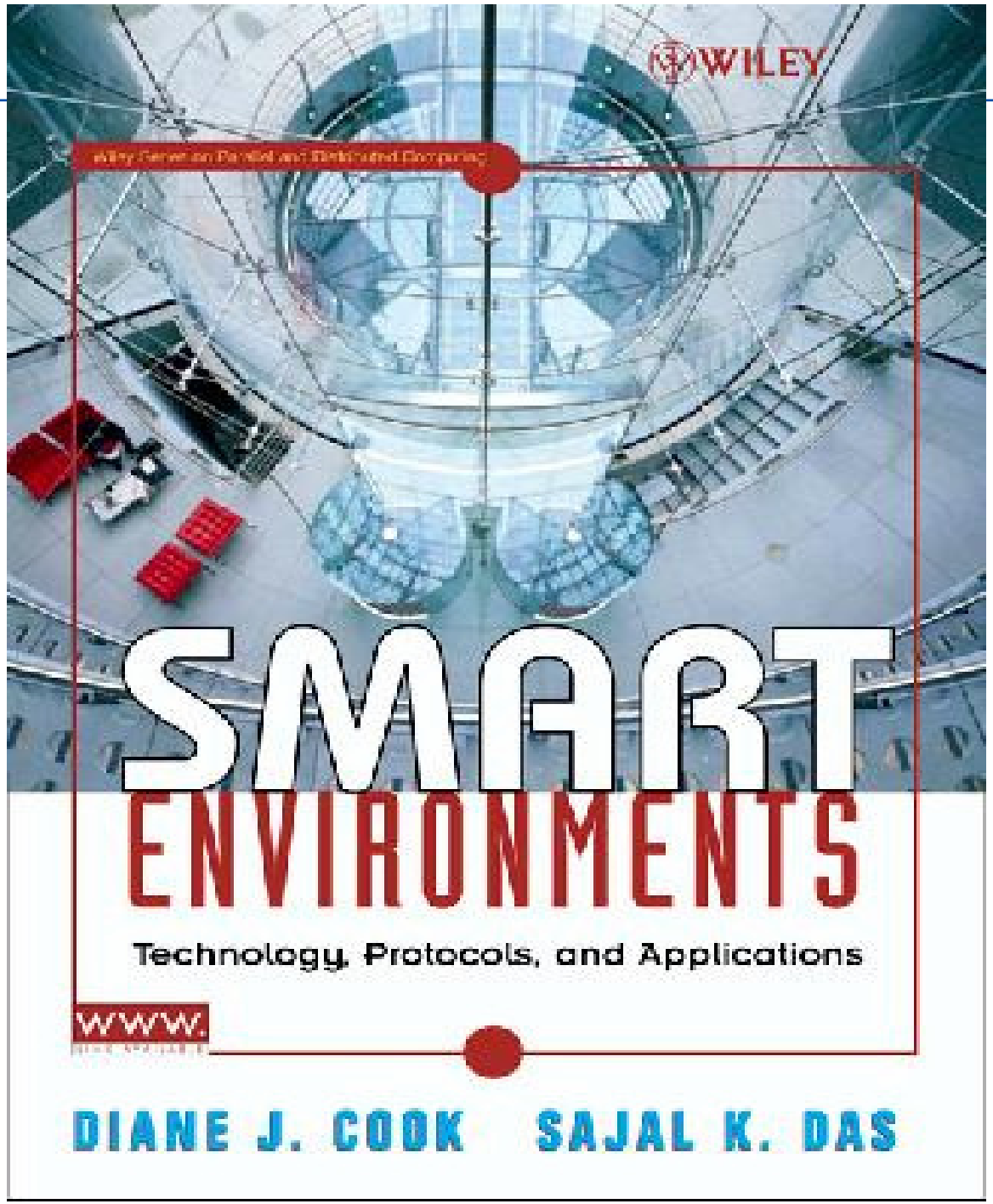
Aggregation result robust to cooperative malicious nodes of different fractions

Conclusion

- Integrated multi-level security framework in wireless sensor networks.
- Epidemic theory modeling to control spread of infected nodes and outbreak.
- Information theory-based reputation to detect intrusion of malicious nodes.
- Belief / trust model to ensure secure information aggregation by effectively filtering false data.
- Distributed key sharing and collaboration to revoke reveals secrets.
- Digital watermarking technique to self-correct compromised data.


ELSEVIER
Volume 1, Number 1, March 2006
ISSN: 1574-1192
pervasive and mobile computing
Editor-in-Chief:
Sajal K Das,
University of Texas at Arlington, USA
Associate Editor:
Marco Conti,
CNR, Pisa, Italy
Editor-in-Chief,
Special Issues:
Behrooz Shirazi,
University of Texas at Arlington, USA
www.elsevier.com/locate/pmc
Also available on
SCIENCE DIRECT®

S. K. Das

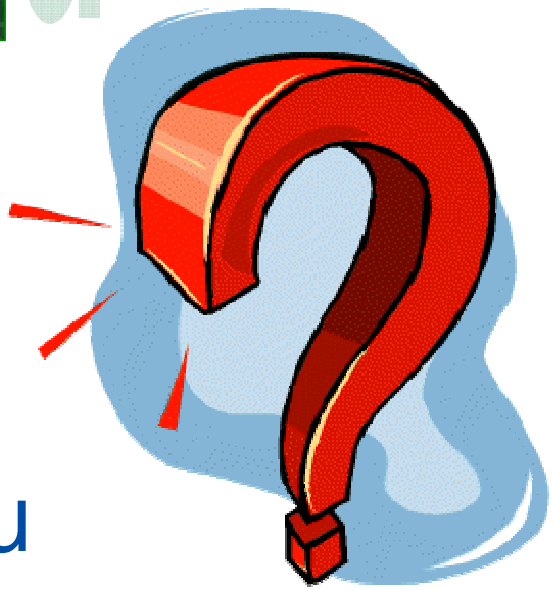

WILEY
SMART
ENVIRONMENTS
Technology, Protocols, and Applications
WWW.
DIANE J. COOK
SAJAL K. DAS

"A *teacher* can never truly teach unless he is still learning himself. A lamp can never light another lamp unless it continues to burn its own flame. The teacher who has come to the end of his subject, who has no living traffic with his knowledge but merely repeats his lesson to his students, can only load their minds, he cannot quicken them".

Rabindranath Tagore

(Indian Poet, Nobel Laureate,1913)

Thank You



http://crewman.uta.edu

S. K. Das