A Framework for Multi-Level Security in Wireless Sensor Networks

Sajal K. Das

Center for Research in Wireless Mobility & Networking (CReWMaN)

Department of Computer Science and Engineering

The University of Texas at Arlington, USA

E-mail: das@cse.uta.edu http://crewman.uta.edu

Acknowledgements

National Science Foundation, Texas Advanced Research Program

Outline

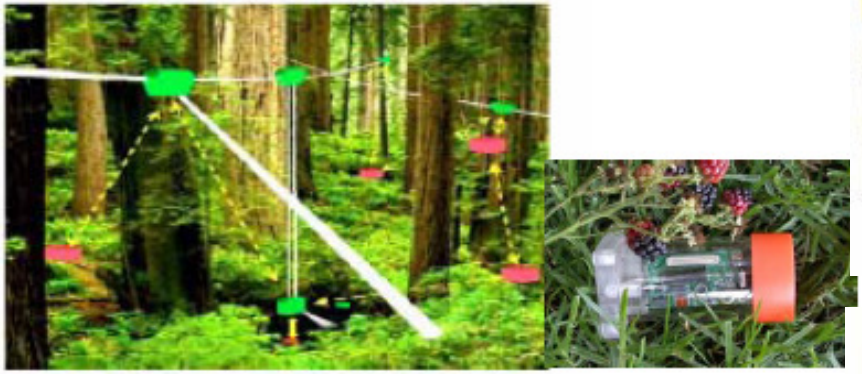
"Education is the manifestation of the perfection already in man."

- Swami Vivekananda

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

WSN Applications

- **Monitoring and Control**
  - Habitat
  - Environment
  - Ecosystem
  - Agricultural
  - Structural
  - Traffic
  - Manufacturing
  - Health



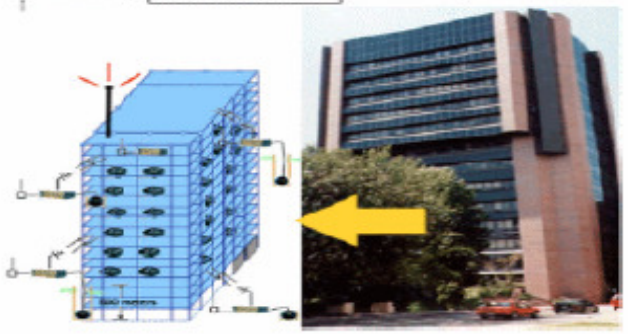
Ecosystems, Biocomplexity

Sensor Augmented Fire Response

ElderCare

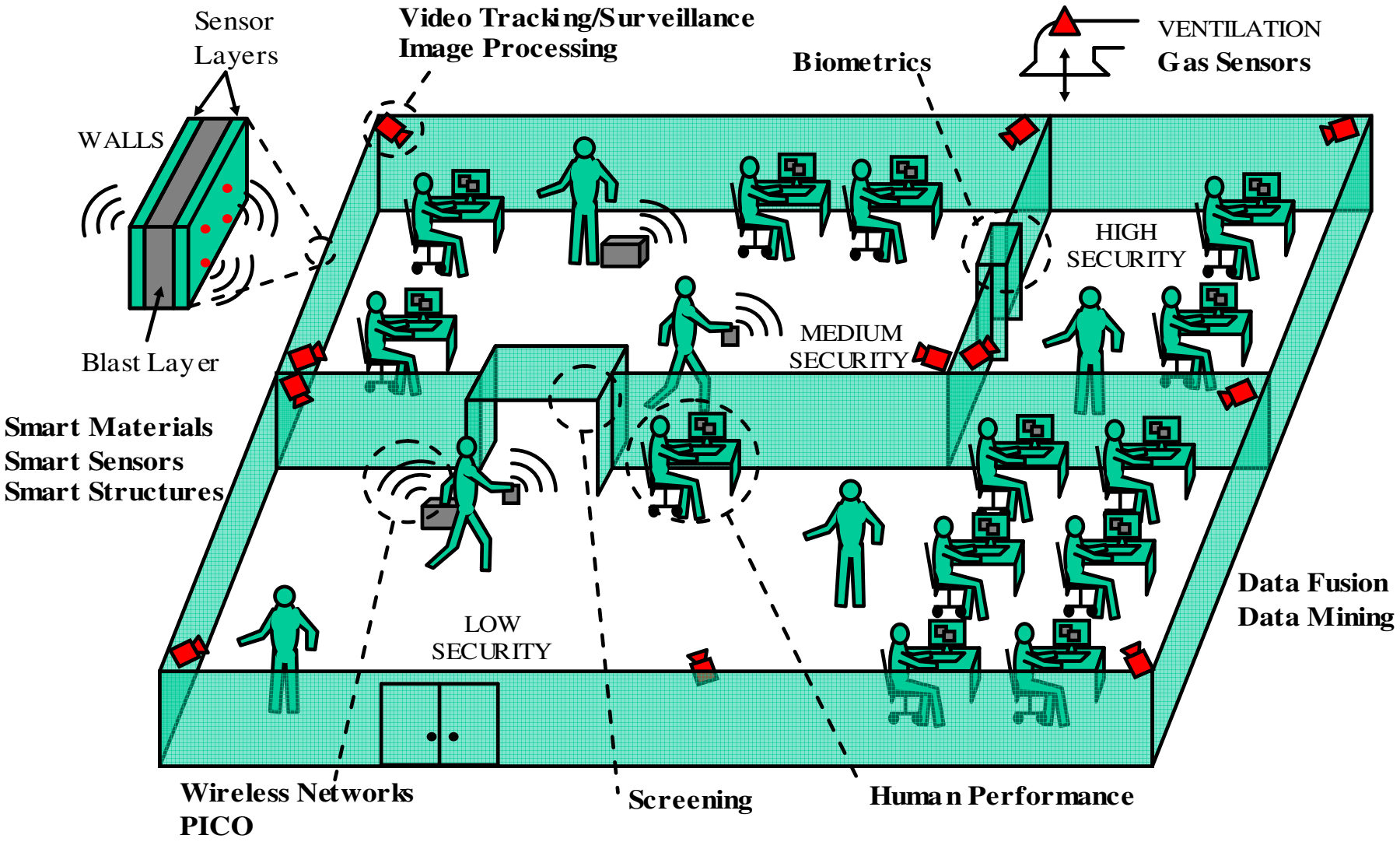
Manufacturing

Seismic Structure Response

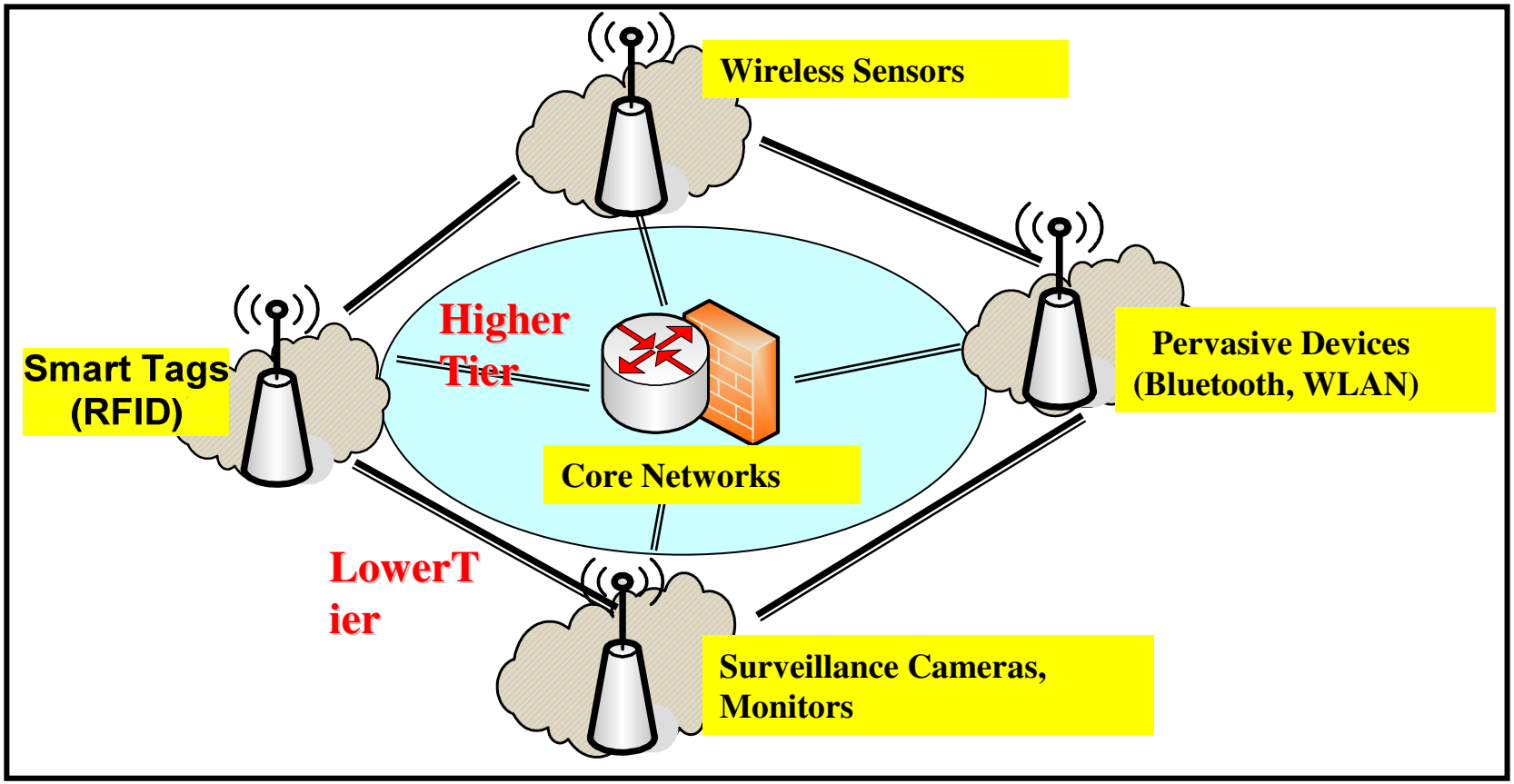


- **Security and Surveillance**
  - Border and Perimeter Control
  - Target Tracking
  - Intrusion Detection

Pervasively Secure Infrastructures

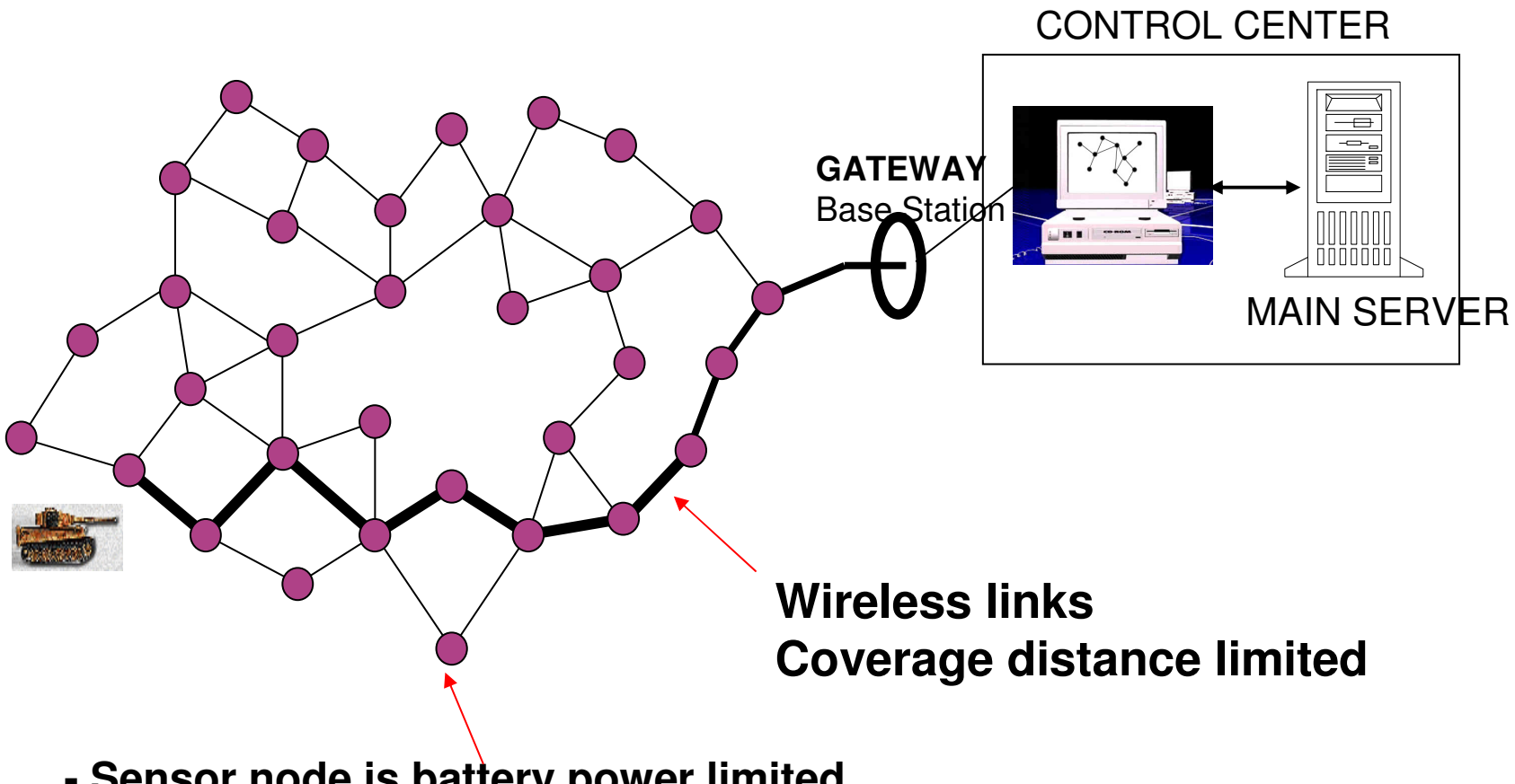


Two-Tier Architecture of PSI



- Lower tier (front-end): pervasive network of smart sensors and embedded devices monitoring security missions all the time
- Higher tier (back-end): mines collected data, discovers knowledge and patterns, makes intelligent decisions to provide security services

WSN Architecture



- Sensor node is battery power limited
- Can route adjacent sensor's data
- Low duty cycle (active and sleep modes)
- Aggregation done at intermediate nodes from source to sink

Characteristics of WSNs

- Task (application)-specific information gathering platform. Immediate reporting on critical changes of phenomenon → event driven.
- High density deployment and highly limited resources (battery, CPU, memory, sensing range, communication bandwidth).
- Frequent topology changes due to node mobility and failures. No knowledge of global topology. Generally, ad hoc deployment.
- Distributed collaboration for information gathering, processing and decision making.

Characteristics of WSNs (Cont'd)

- In-network processing (data fusion/aggregation, compression), exploit spatial / temporal redundancy to reduce communication.
- Broadcast based data dissemination – *many-to-one*, *one-to-many*, *push* (interest sensed by sensors) and *pull* (on demand).
- Data centric operations (e.g., routing) instead of address centric.

Outline

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

Security Challenges in WSNs

- Limited resources → Limited defense capability

  - Public key too costly to authenticate packets with digital signatures and disclose key with each packet

  - Storing one-way chain of keys along message route requires more memory and computation for en-route nodes

- Uncertain, unattended / hostile environment
  - Faulty prone nature vs. compromises
- No centralized control
- In-network processing → Loss of integrity, confidentiality
- Multiple-attacking angles

→ Single level defense mechanism highly vulnerable

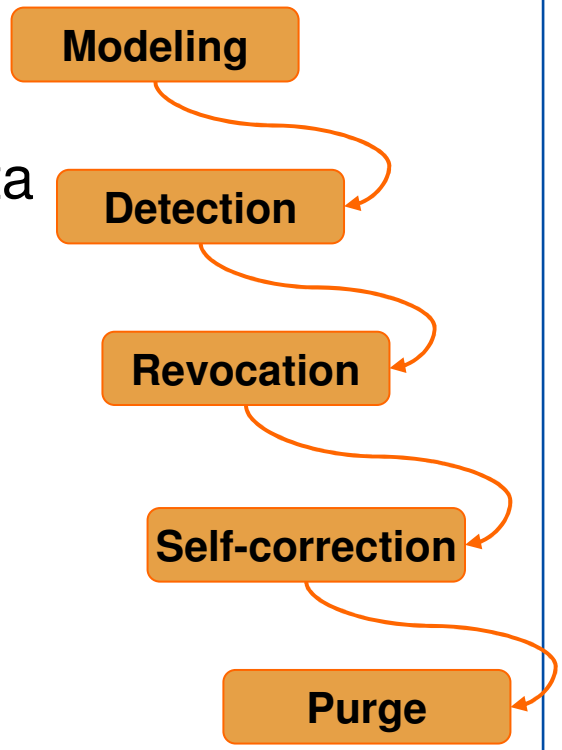
  - Cryptographic technique is not the panacea

Threats to WSNs

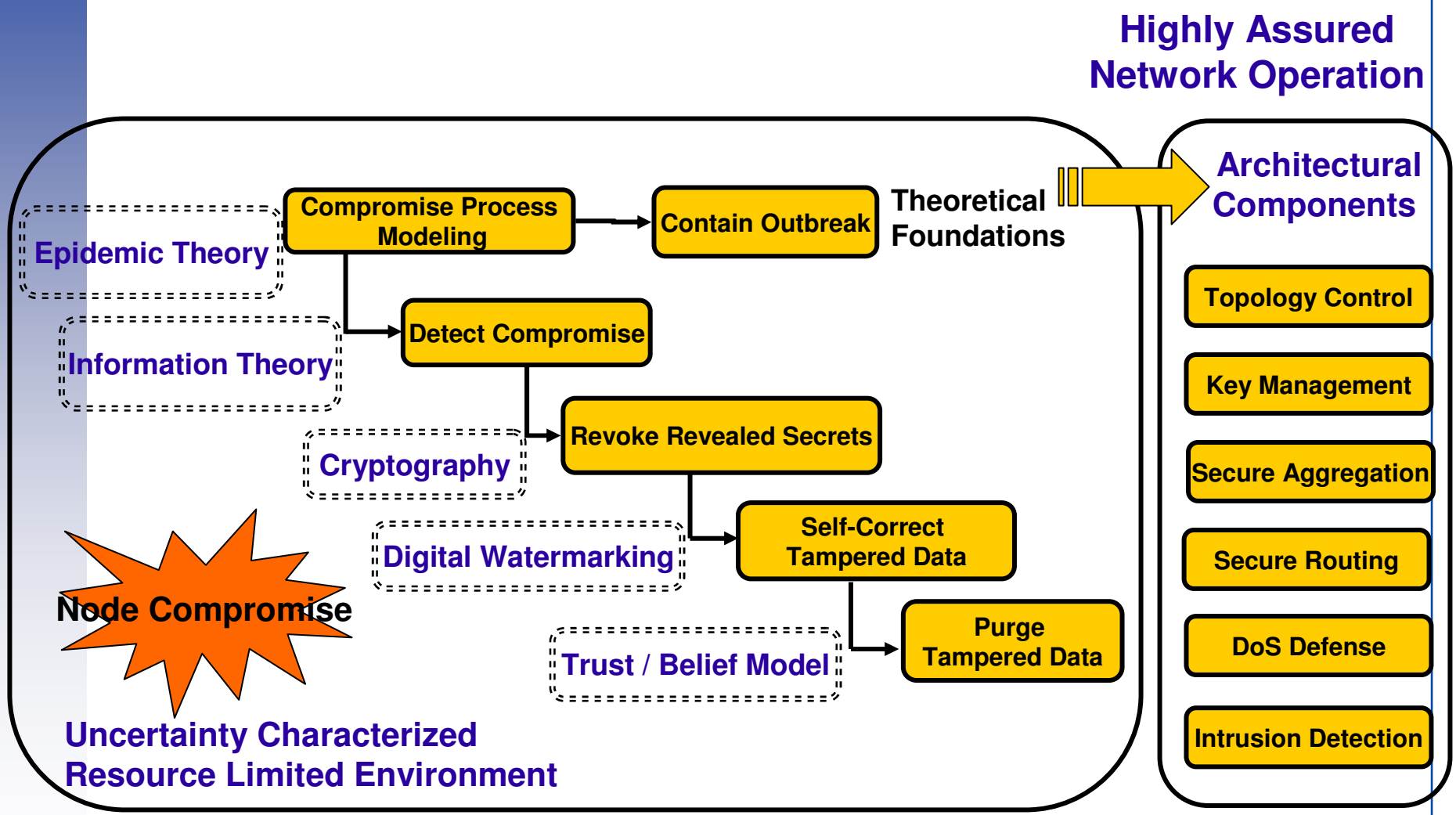
- **Node Compromises and Intrusions**
  - Physical capture
  - Sophisticated analysis: differential timing / energy analysis
- **Revealed Secrets**
  - Cryptographic keys, codes, commands, etc.
- **Enemy's Puppeteers**
  - Trojans in the network with full trust

Need for Multi-level Solution

- **Attack at multiple possible levels to be defended**
  - Model the propagation of node compromises
    - E.g., trojan virus spreading
  - Detect compromised nodes & forged data
    - E.g., abnormal reports
  - Revoke revealed secrets
    - E.g., broadcast confidentiality
  - Self-correct and purge false data
    - E.g., average temperature calculation



Multi-Level, Integrative Architecture



Uniqueness

- Full spectrum, multi-level, integrative approach
  - Defend against the whole process of compromise
  - Model, detect, revoke, correct, and purge node compromises and adversary attacks
- Rich and powerful theoretical foundations
  - Epidemic theory, information theory, cryptography, trust / belief model, game theory, etc.
  - Each uniquely exploited for defense against specific attacks
  - Joint, complementary defense results
- Direct translation to robust WSN architecture design
  - Secure routing, secure aggregation, key management, intrusion detection, etc.
  - Plug and play, reusable suite of security modules

Outline

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

Modeling Compromises: Epidemic Defense

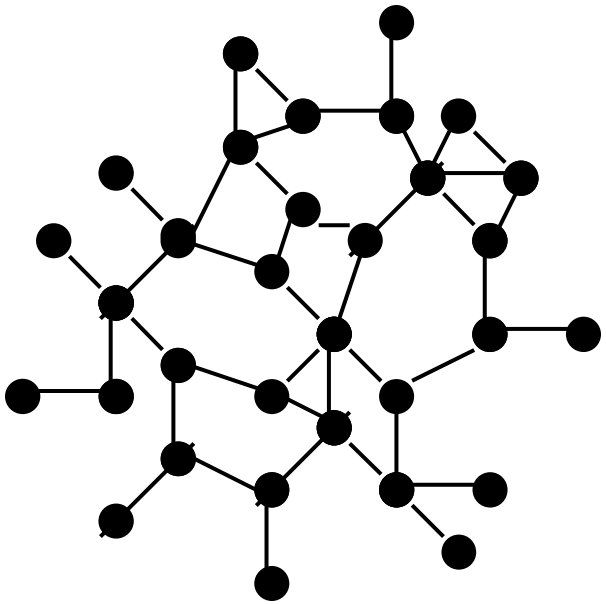
- Premise: Node compromises
  - Capture node deployment, key distribution, topology
  - Outbreak possible unless controlled

- Objectives:
  - Construct a model and analyze the spread of node compromises in WSNs based on Epidemic Theory
  - Characterize outbreak transition point of compromise process
  - Study the impact of infectivity duration of a compromised node on the process
  - Capture the time dynamics of the spread
  - Identify critical parameters to prevent outbreaks

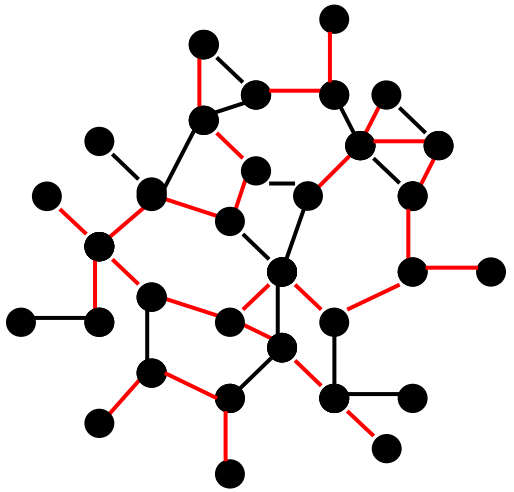
[P. De, Y. Liu, and S. Das, "Modeling Node Compromise Spreading in wireless Sensor Networks using Epidemic Theory," *IEEE WoWMoM*, June 2006.]

System Model

- Random Pair-wise Key Pre-distribution
  - A set of keys randomly chosen from a key pool



Physical Topology



Virtual Key-Sharing Topology

System Model

- Epidemic Models
  - Susceptible-Infected-Susceptible (SIS) Model
  - Susceptible-Infected-Recovered (SIR) Model
  - Homogeneously mixed population
    - Differential equation based formulation for the infection process
  - Heterogeneously mixed population

- Spread of node compromise

  - the number of contacts is determined by degree distribution of the key sharing network

- Static WSN is not fully mixed → random graph approach

Sensor Network Topology Model

- $\rho = \frac{N}{R^2}$ denotes the node density of the network

  - N: total number of nodes, R: sensing radius

- p = probability of link existence at the physical level

$$p = \frac{r^2 \rho}{N}$$

  – r is the average communication range between nodes

- Probability that l nodes are within communication range is given by

$$p(l) = \binom{N}{l} p^l (1-p)^{N-l}$$

Sensor Topology Model

- q = prob. of sharing pair-wise key between neighboring nodes
- Probability of sharing at least one key with exactly k neighbors given l nodes within its range is given by:

$$p(k|l) = \binom{l}{k} q^k (1-q)^{l-k}$$

- Probability of having k neighbors sharing at least one key is:

$$p(k) = \sum_{l=k}^{\infty} p(l)\, p(k|l)$$

$$p(k) = \sum_{l=k}^{\infty} \binom{N}{l} p^l (1-p)^{N-l} \binom{l}{k} q^k (1-q)^{l-k}$$

Epidemic Analysis

- When nodes do not recover, *transmissibility* (T) is expressed only in terms of the *infection probability*, \beta
- Node recovery is captured by expressing transmissibility as a function of average *duration of infectivity*, τ

$$1-T=\lim_{\delta t\to 0}(1-\beta\delta t)^{\tau/\delta t} \qquad T=1-e^{\beta\tau}$$

- Average cluster size as epidemic attains outbreak proportions

$$s=1+\frac{TG_0'(1)}{1-TG_1'(1)}$$

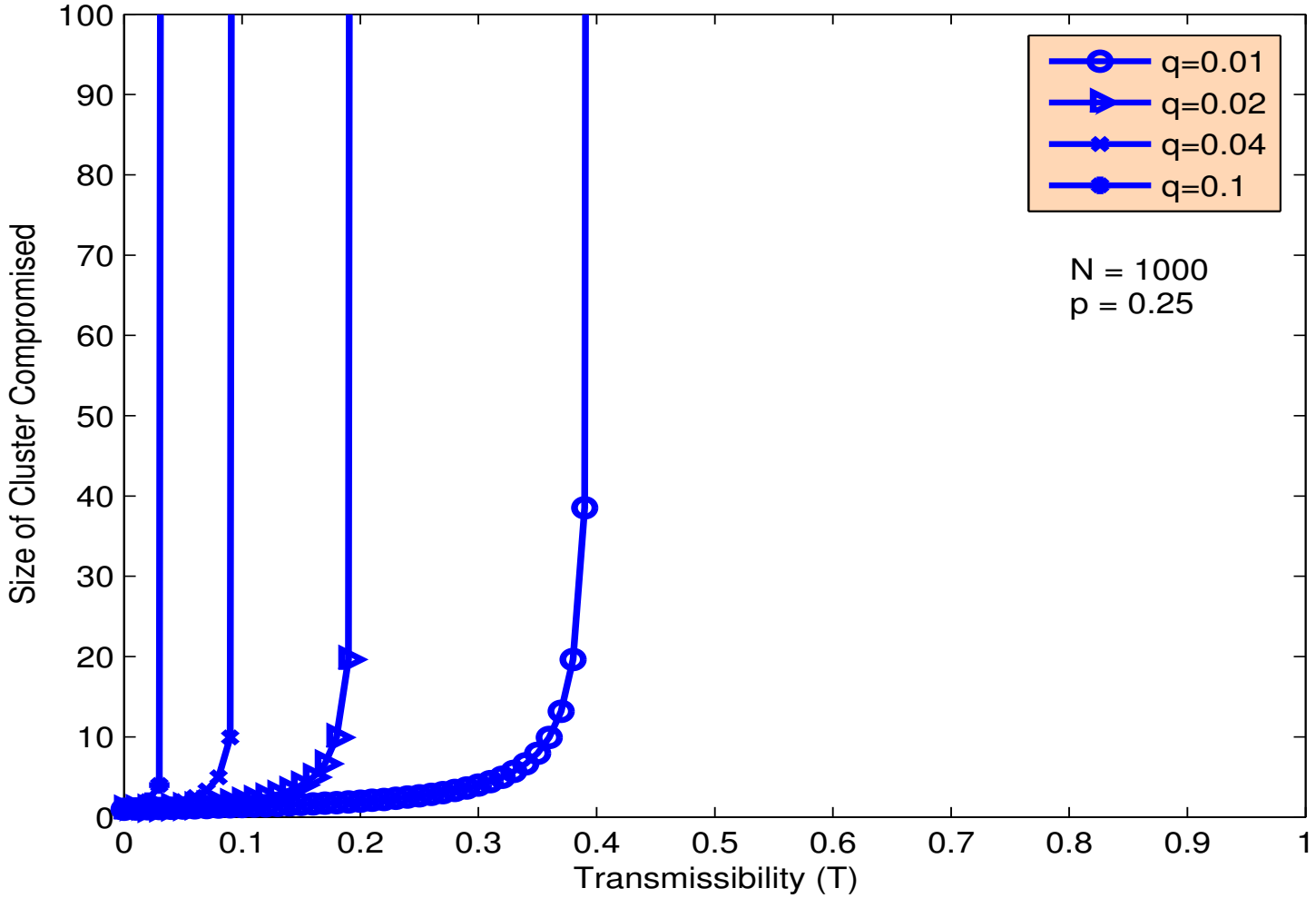
- Average Epidemic size after outbreak results

$$S=1-G_0(u)$$

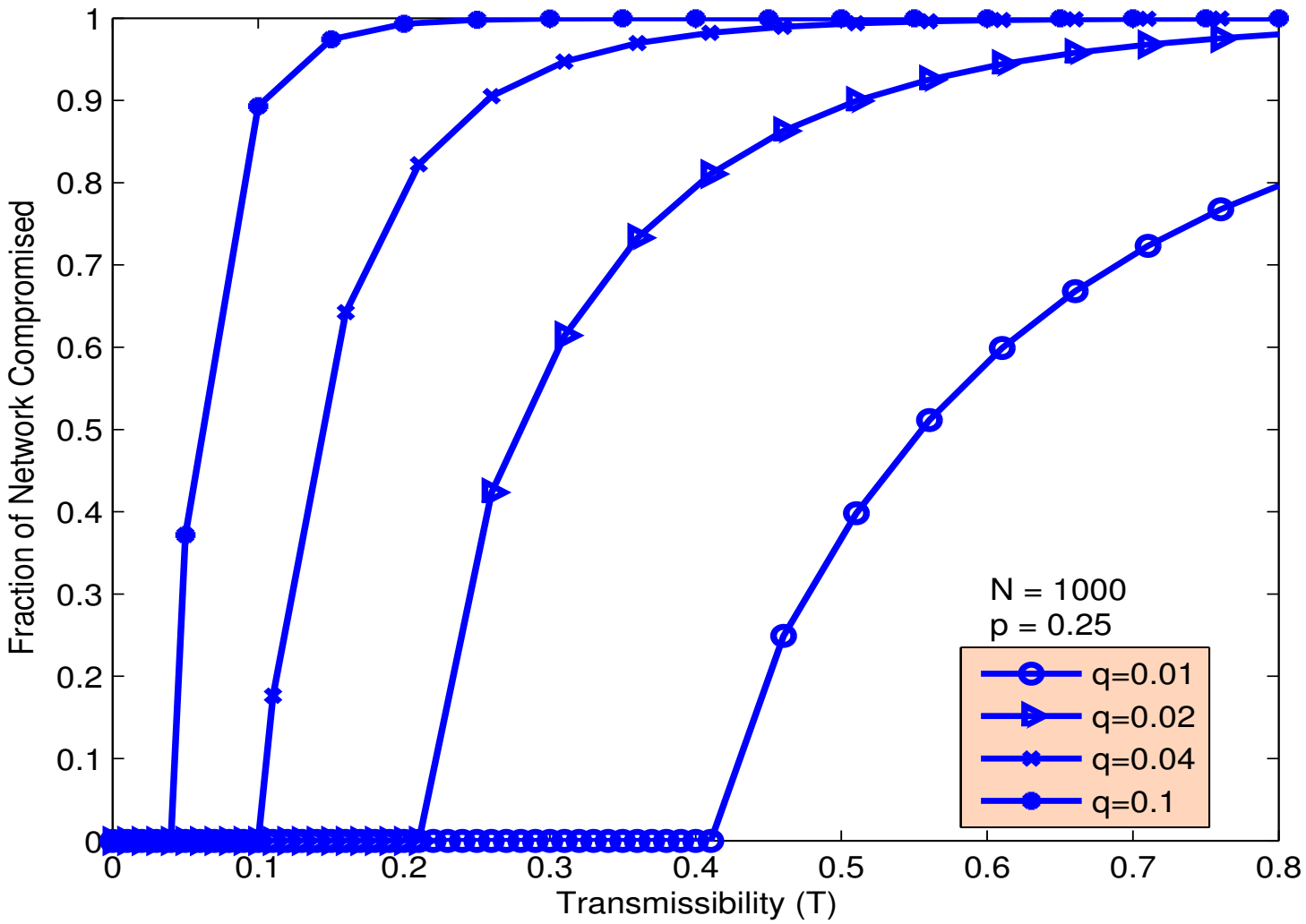
$$u=G_1(u)$$

Non-epidemic cluster size with infection probability

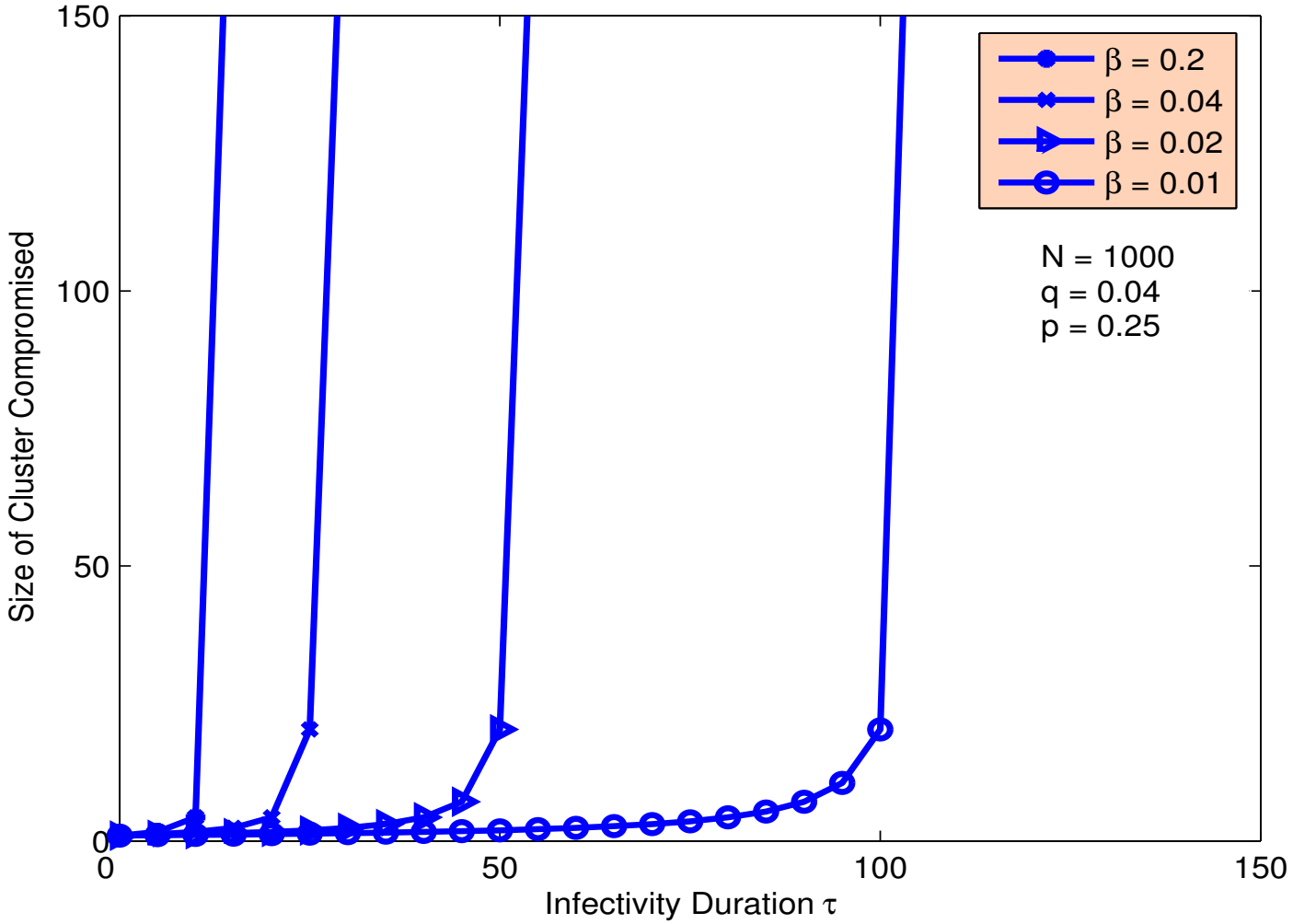
- q = prob. of sharing pair-wise key between neighboring nodes
- p = probability of link existence at the physical level



Epidemic Size with infection probability



Non-epidemic cluster size with infectivity duration



Epidemic Size with infectivity duration