

BANBAD: Bayesian-Network-Based Anomaly Detection for MANETs

Chaoli Cai¹, Ajay Gupta¹ and Leszek Lilien^{1,2}

¹WiSe Lab, Western Michigan University ²Affiliated with CERIAS

1. Outline

- Motivation (2)
- The BANBAD Algorithm (3)
- Bayesian Network (4)
- Application Models
 - The Chain Application Model (5)
 - The DAG Application Model (6)
- Training & Testing Processes (7)
- Simulation Results (8)
- Future Work (9)

2. Motivation

- Characteristics of MANETs
 - Arbitrary node movement
 - Lack of centralized control
 - Lack of fixed network topology
- Prevention
 - Encryption, authentication, etc.
 - Prevention alone can only reduce intrusions rather than eliminate them
 - Hence, *detection* is needed.
- Detection
 - Misuse detection – known attacks
 - Anomaly detection – unknown attacks
 - Hence, *anomaly* detection is needed.

3. The BANBAD Algorithm

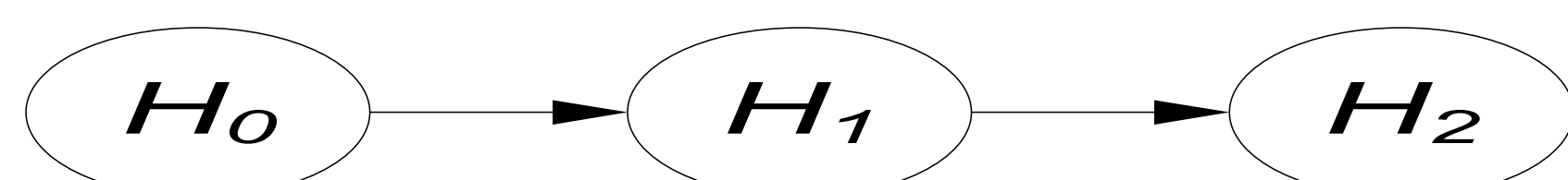
- Define a Bayesian Network to detect anomalies in
 - Power Consumption
 - Displacement
 - Local Computation
 - Communication
 - Velocity
- Incorporate various features using chain / tree model
- Set up acceptable ranges for features
- Goal is to reduce the false alarm rate and increase the detection rate

4. Bayesian Network (BN)

- Used extensively for modeling knowledge in medicine, engineering, text analysis, decision support systems, etc.

- BN is a directed acyclic graph

- Nodes represent variables (features)
- Arcs represent statistical dependence relationships among the variables, and local probability distributions for each variable

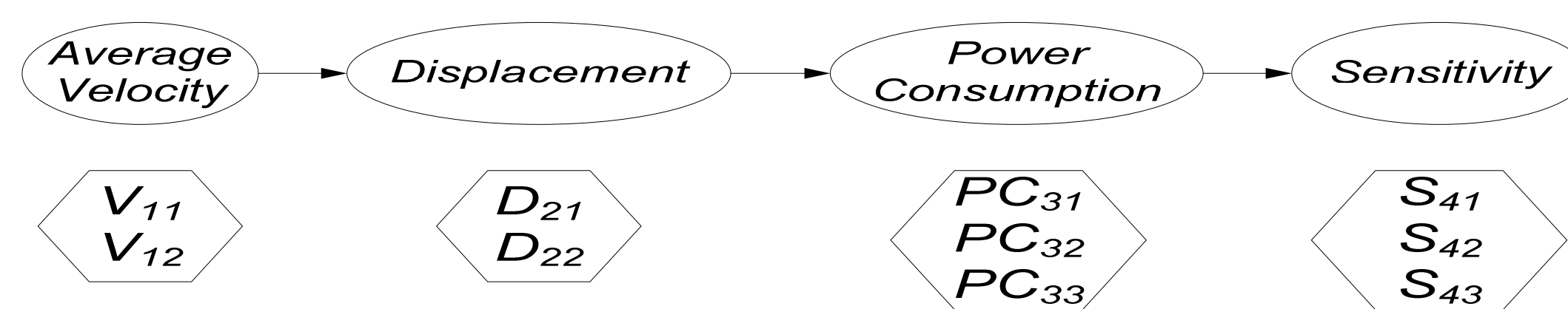


- Bi-directional Belief Propagation

- In belief propagation algorithms, each node transmits a π message to its children and a λ message to its parents
- Calculate belief for each variable as
 - $\text{Bel}(H_i) = \alpha \pi(H_i) \lambda(H_i)$
 - $\pi(H_i) = \pi(H_0) \cdot M(H_i | H_0)$ — the prior probability
 - $\lambda(H_i) = M(H_2 | H_i) \cdot \lambda(H_2)$ — the likelihood evidence
- Some notations
 - $f(x) \cdot g(x)$ — the dot product of two vectors
 - $f(x) \blacksquare g(x)$ — the congruent multiplication of two vectors
 - α — a constant used to normalize a vector so that its elements sum to 1.0
 - $\text{Bel}(H_i) = P(H_i | e)$ — the posterior probability
 - e — evidence
- A significant deviation between the prior and the posterior probabilities within any range of features of a node indicates an anomaly

5. The Chain Application Model

- Special case of DAG



- Chain Model contains 4 features along with their corresponding ranges
- Detect anomaly in displacement

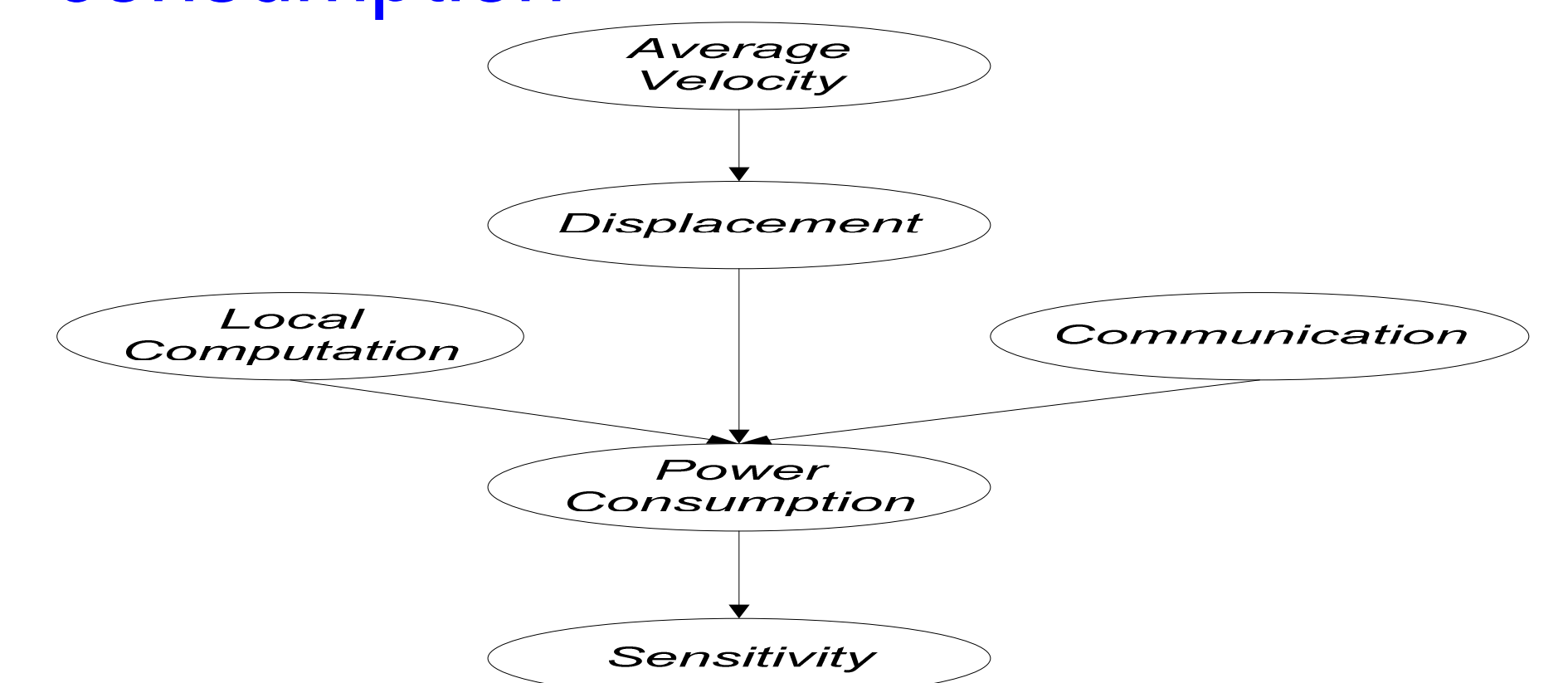
- Conditional probability representation

$$M(D|V) = \begin{bmatrix} P(D_{21} | V_{11}) & P(D_{22} | V_{11}) \\ P(D_{21} | V_{12}) & P(D_{22} | V_{12}) \end{bmatrix}$$

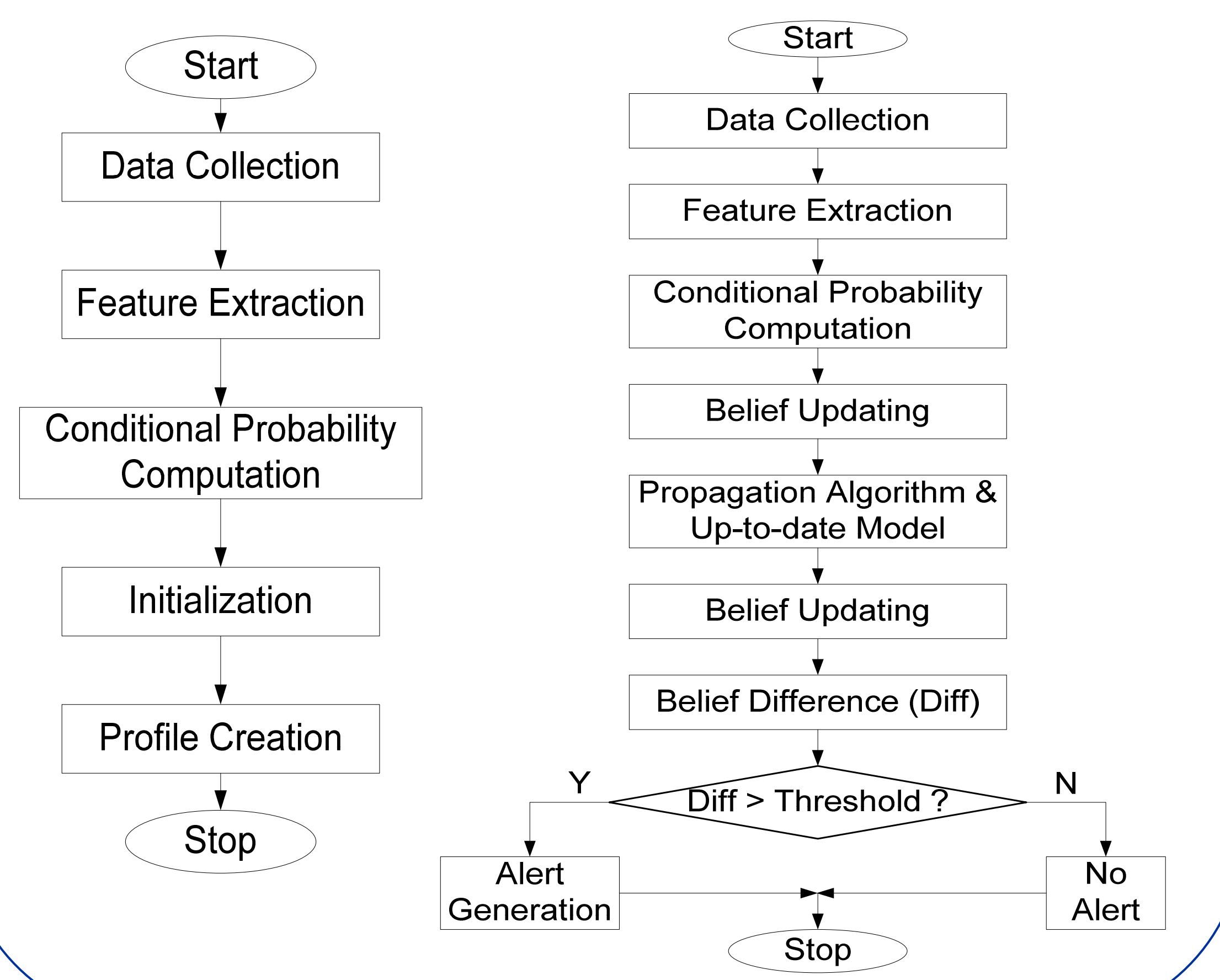
- $P(D_{21} | V_{11})$ — the conditional probability of range D_{21} given range V_{11}
- $M(D|V)$ — the conditional probability distribution of feature D given feature V

6. The DAG Application Model

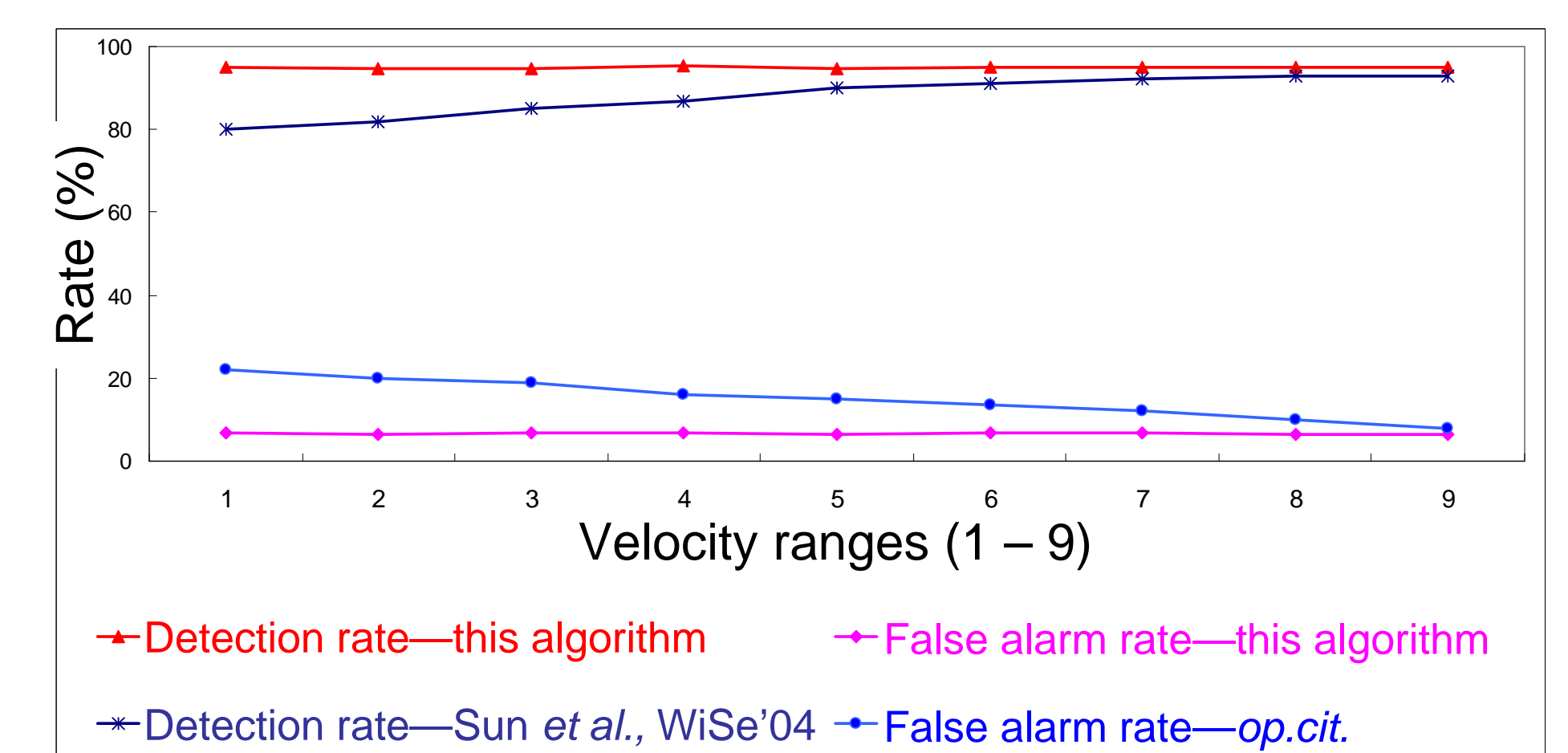
- More realistic and powerful
- Detect anomalies not only for displacement but for local computation and communication, based on the evidence of power consumption



7. Training & Testing Processes



8. Simulation Results



9. Future Work

- Data mining (prepares data for BANBAD)
 - Construct DAG from raw data set efficiently
- Multimodal / Multisensor fusion (to process results of BANBAD)
 - Represent anomaly by audio, video, image, etc. / Distribution issues