

## Attacks and Defense on Virtual Coordinate Based Routing in Wireless Sensor Networks

Jing Dong, Kurt Ackermann, Brett Bavar, Cristina Nita-Rotaru  
Department of Computer Science, Purdue University

### Abstract

Recent developments in wireless sensor networks bring about the need for point-to-point routing. Virtual Coordinate System (VCS) based routing presents an alternative to the traditional routing protocols with the following attractive properties:

- Proactive route discovery
- Requires only local interaction
- Requires only local state information

However, little work has been done to protect VCS-based routing. In this poster, we demonstrate several dangerous attacks against VCS-based routing and propose defense techniques.

### Virtual Coordinate based Routing

VCS-based routing typically follows a common design:

- **Coordinate Establishment**
  - A set of *reference nodes* are determined by pre-assignment or election
  - The reference nodes flood *coordinate messages*
  - The coordinates of each node are a vector of hop counts to each of the reference nodes and are derived from the hop count field in the coordinate messages
- **Coordinate Lookup**
  - One or more coordinate servers maintain the coordinates of all the nodes and answer coordinate queries
- **Greedy Forwarding**
  - Each node forwards the message to the neighbor closest to the destination

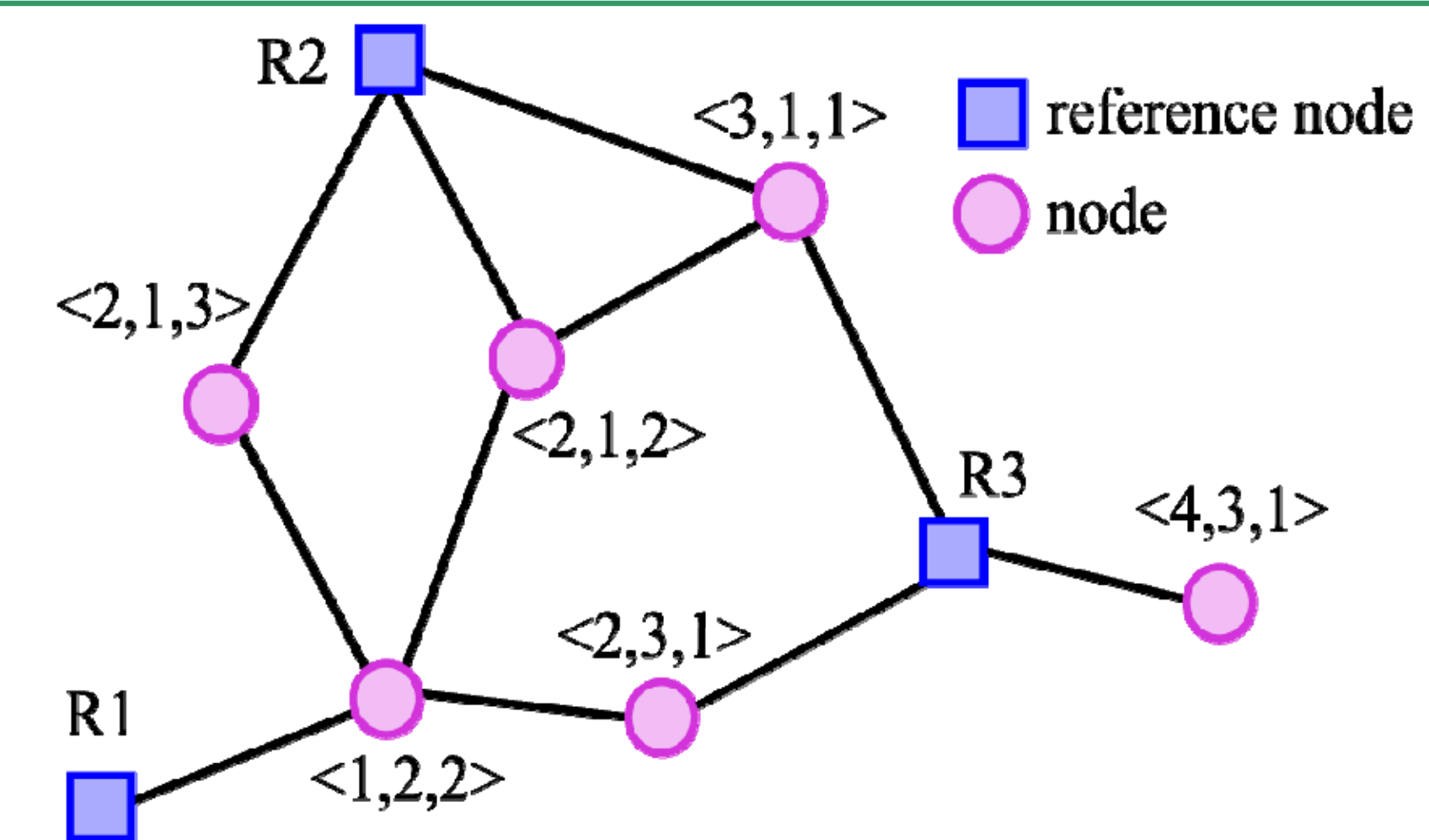
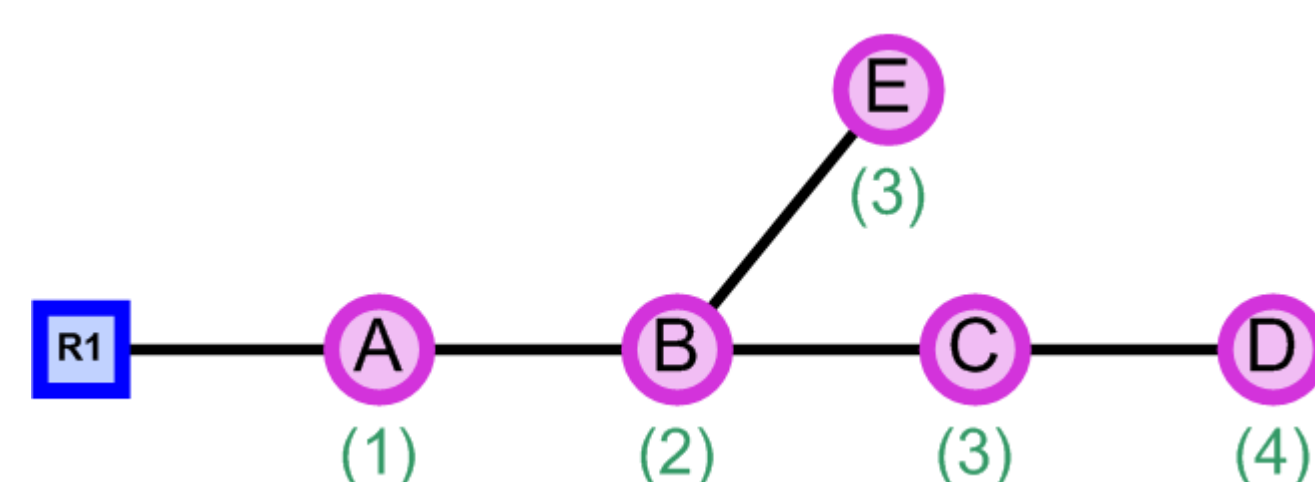


Figure 1  
Example of virtual coordinates in a small network

### Attacks on Virtual Coordinate Systems

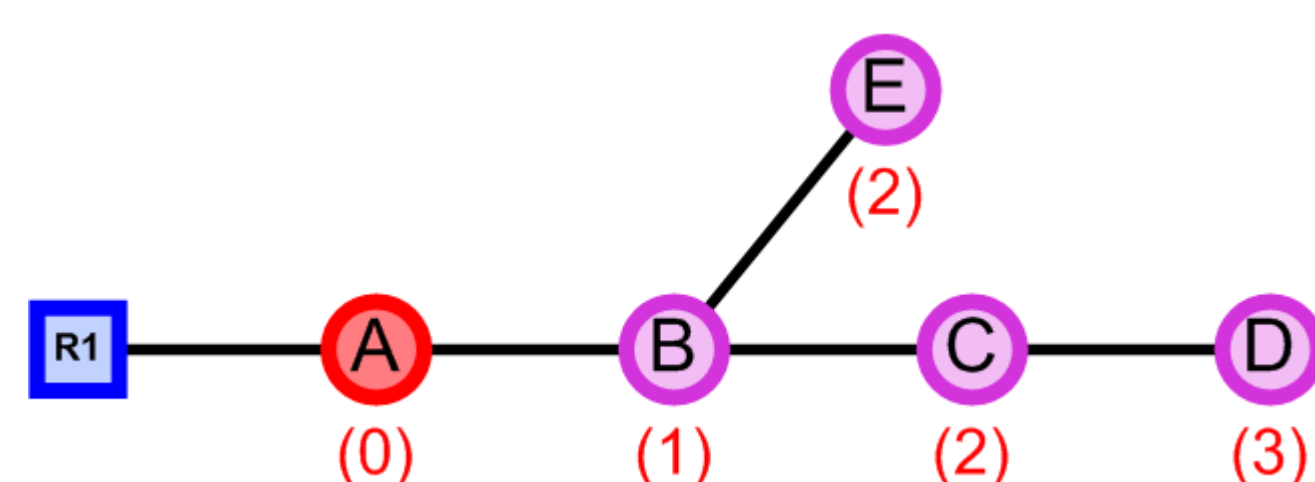
Attacks are epidemic!

#### Normal Coordinates



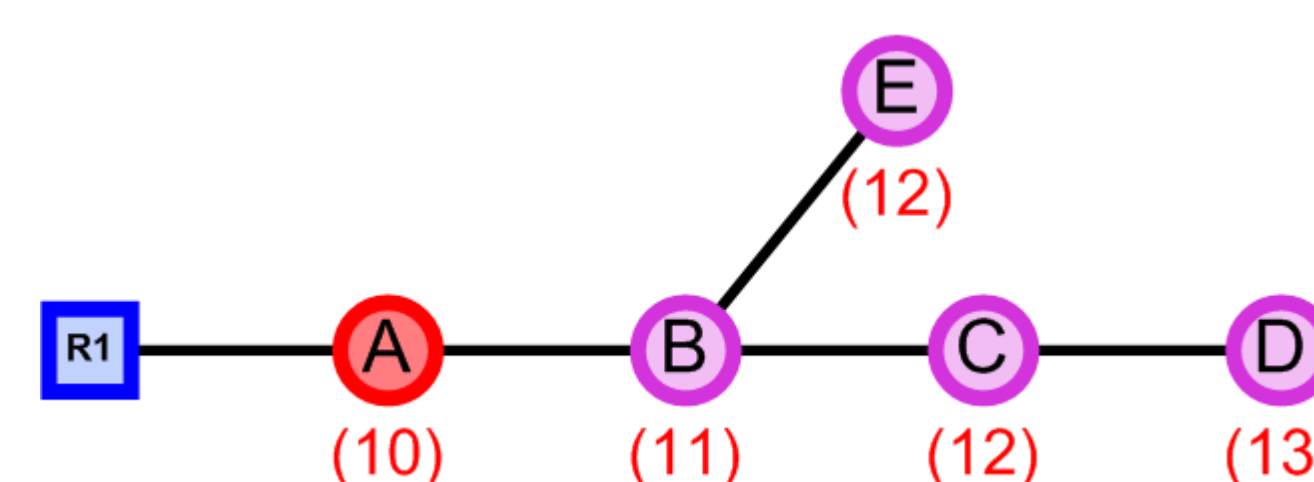
Coordinates of nodes without under attack

#### Coordinate Deflation Attack



Attacker A claims coordinate 0, causing node B,C,D, E to obtain incorrect small coordinates

#### Coordinate Inflation Attack



Attacker A claims coordinate 10, causing node B,C,D, E to obtain incorrect large coordinate

#### Coordinate Oscillation Attack

Attacker nodes alternate between large and small coordinate announcements or announce random coordinates to cause coordinate instability in nearby nodes

#### Coordinate Pollution Attack

Attacker nodes compromise coordinate servers or spoof coordinate replies to cause incorrect destination coordinates in messages

### Defense Mechanisms and Experimental Results

#### Detect Coordinate Deflation with Statistical Tests

- The epidemic effect of deflation attacks causes a large change in the distribution of coordinates in the network.
- We use Wilcoxon signed rank statistical test to detect the coordinate distribution change and hence the presence of attacks

#### Prevent Coordinate Deflation with One-way Hash Chain

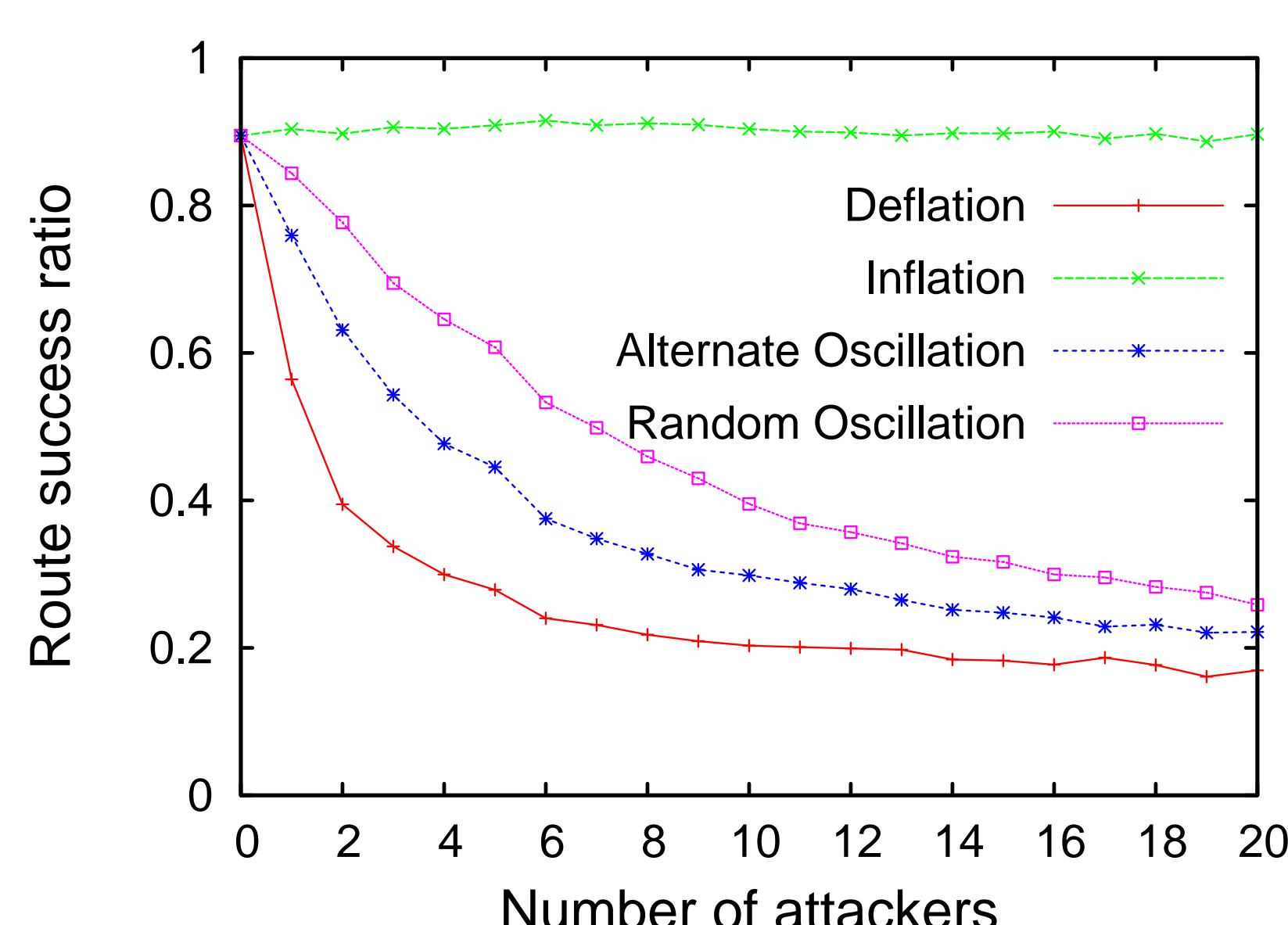
- Hop count is authenticated each hop with one way hash chain, so that intermediate nodes cannot announce coordinate messages with arbitrary small coordinates.

#### Stabilize Coordinates with PID Controller Technique

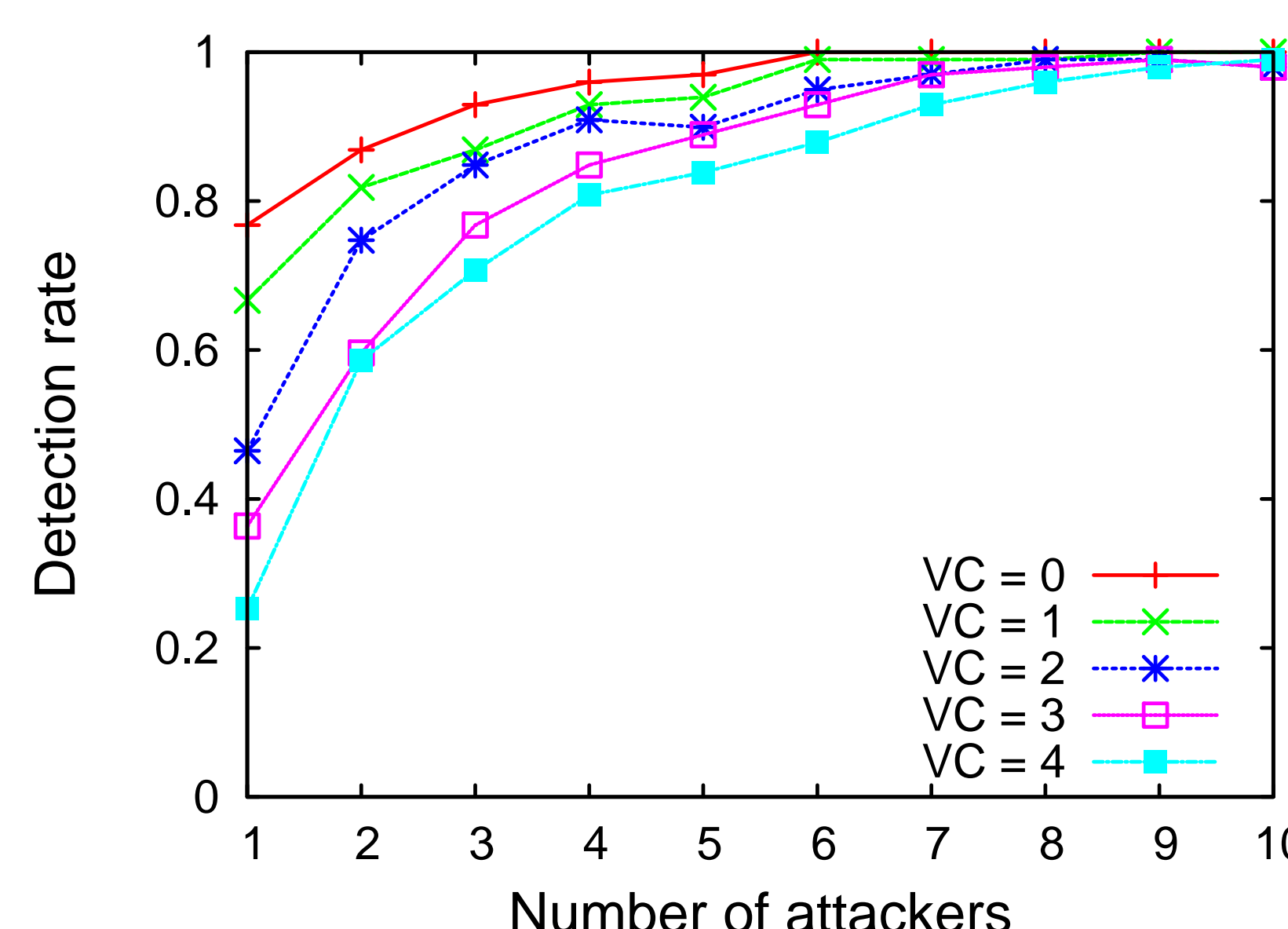
- Evaluate node coordinate stability with the technique of Proportional-Integral-Derivative (PID) controller
- Each node selects neighbors with stable coordinates as its parent for deriving its own coordinate
- Neighbors of the attacker will not select the attacker as their parent, thus attackers will be isolated

### Experimental Results

- Attacks impact routing significantly



- Statistical test detects attack with high accuracy



- Stabilization technique effectively mitigates oscillation attacks

