Detection of False Data Injection Attacks in Power Systems Using a Secured-Sensors and Graph-Based Method

G. Morgenstern[1]**,** L. Dabush[1], J. Kim[2], J. Anderson[3], G. Zussman[3], T. Rottenburg[1]

[1] Ben-Gurion University of the Negev, Beer-Sheva, Israel
[2] Kentech, Naju-si, South Korea
[3] Columbia University, New York, USA

Power System State Estimation

Power Measurements →

Located in the substations and transmission lines

Power System State Estimation

Performed in the control center

Estimated Voltages →

Located in the substations

Transmitting measurements via cyber communication is prone to cyber attacks

False Data Injection Attacks

Tampering with Power Measurements → Errors in System State Estimation → Erroneous System Operations → Adversary Gain

System Blackout

Economical Gain

A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly

At a time when the world faces a dangerous escalation in cyber warfare, a series of assaults on petrochemical companies in Saudi Arabia – possibly backed by nation states – has caused alarm

Nicole Perlroth, Clifford Krauss • Tuesday 20 March 2018 14:14 • Comments

Computers crashed at sites including Sadara Chemical Company, a joint venture between the oil and chemical giants Saudi Aramco and Dow Chemical *(Sadara)*

TECHNOLOGY NEWS JANUARY 18, 2017 / 1:06 PM / UPDATED 7 YEARS AGO

Ukraine's power outage was a cyber attack: Ukrenergo

By Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes 3 MIN READ

KIEV/MILAN (Reuters) - A power blackout in Ukraine's capital Kiev last month wa caused by a cyber attack and investigators are trying to trace other potentially infected computers and establish the source of the breach, utility Ukrenergo told Reuters on Wednesday.

Defense Against False Data Injections

Option 1: Attack prevention

Requires additional resources

Option 2: Attack detection

Relies on intrinsic system and attack properties

Outline

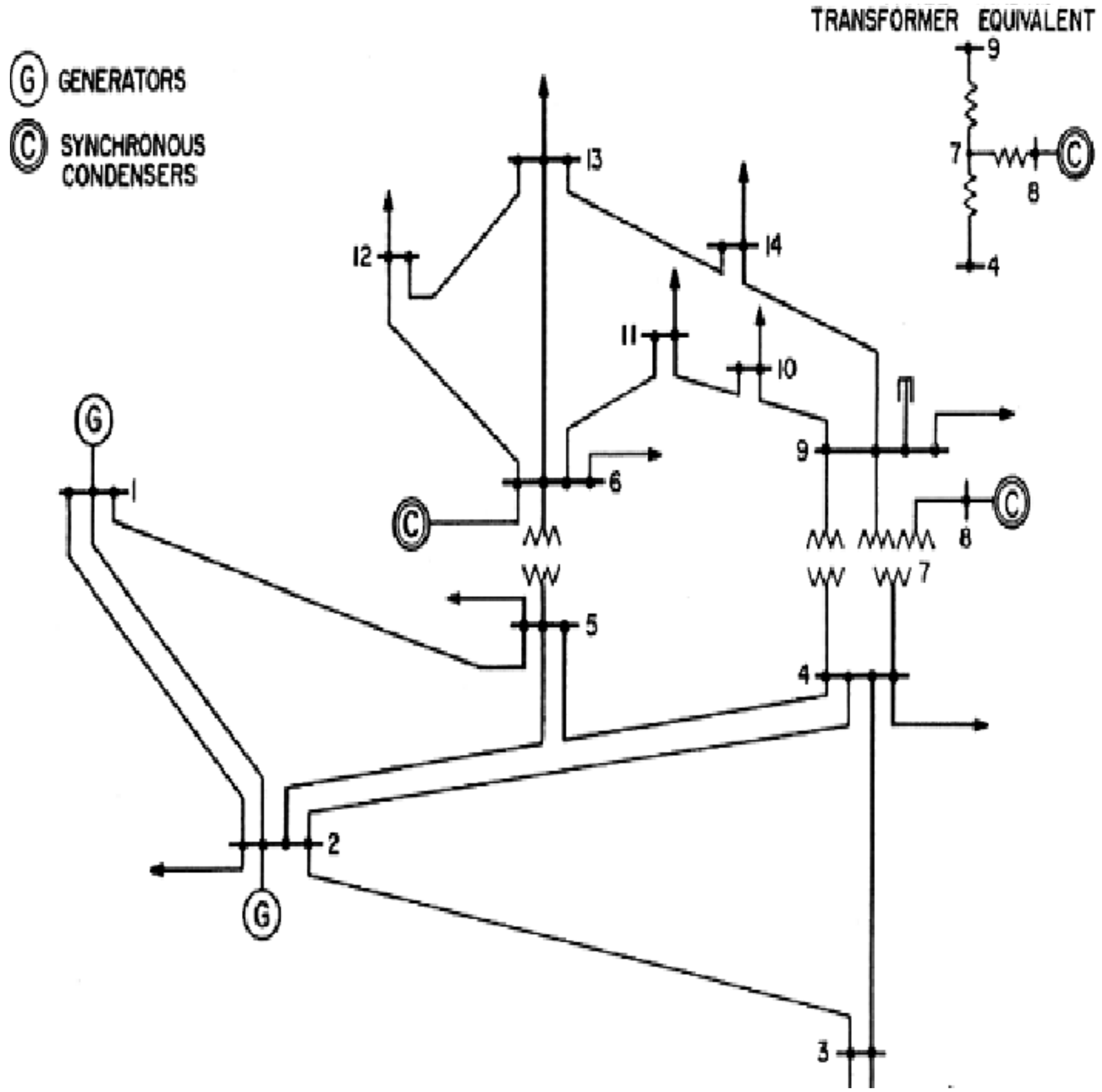
- Introduction
- **Background**
- Theory: Secured Sensors and Graph Smoothness Based Detection for False Data Injection Attacks
- Theory: Modification for Distributed Optimization
- Theory: Modification to Graph Low Pass Signals
- Performance Evaluation

Power System Represented as an Undirected Graph

Substations (generators/loads)

Transmission lines

Susceptance over the lines

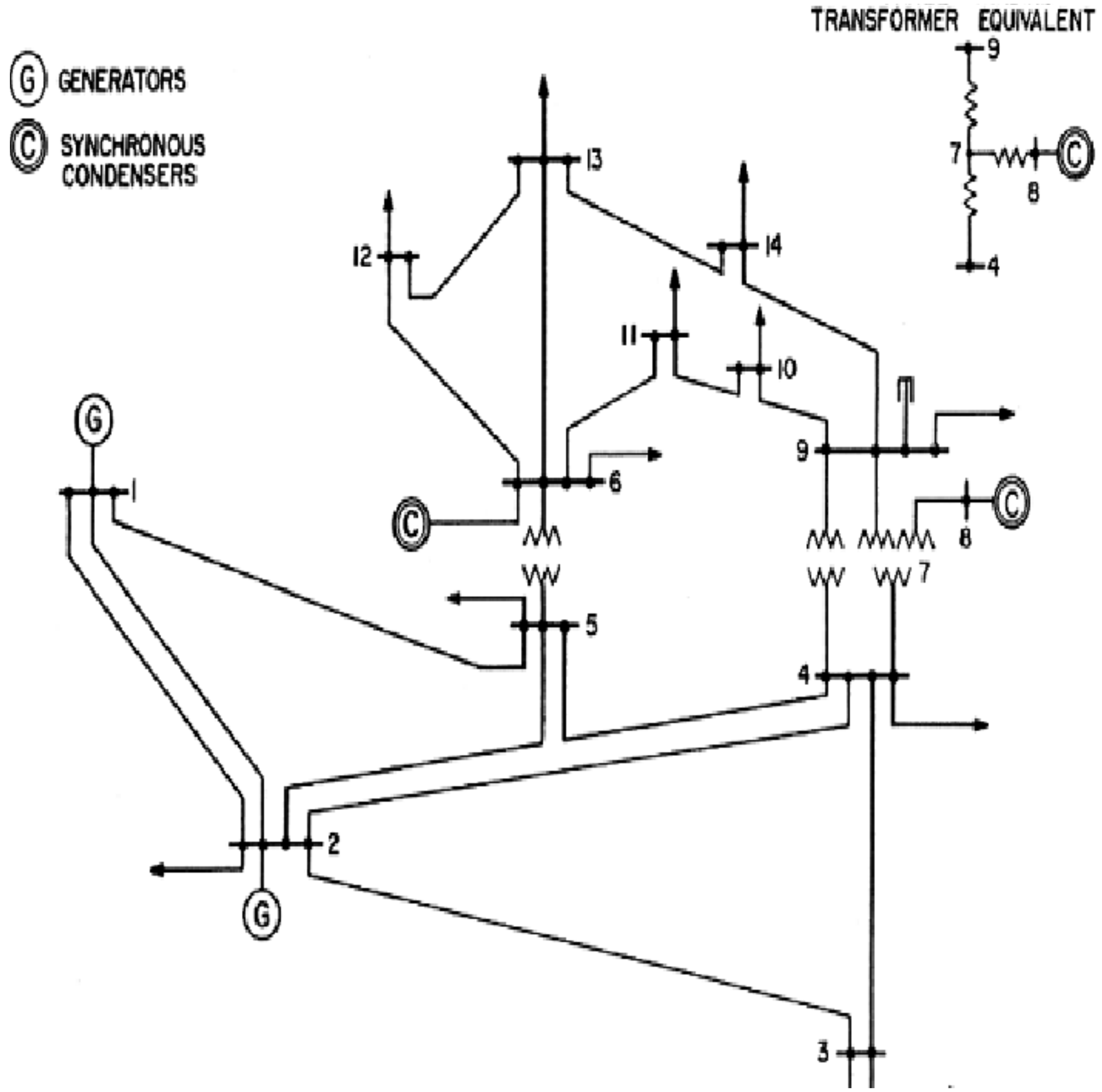


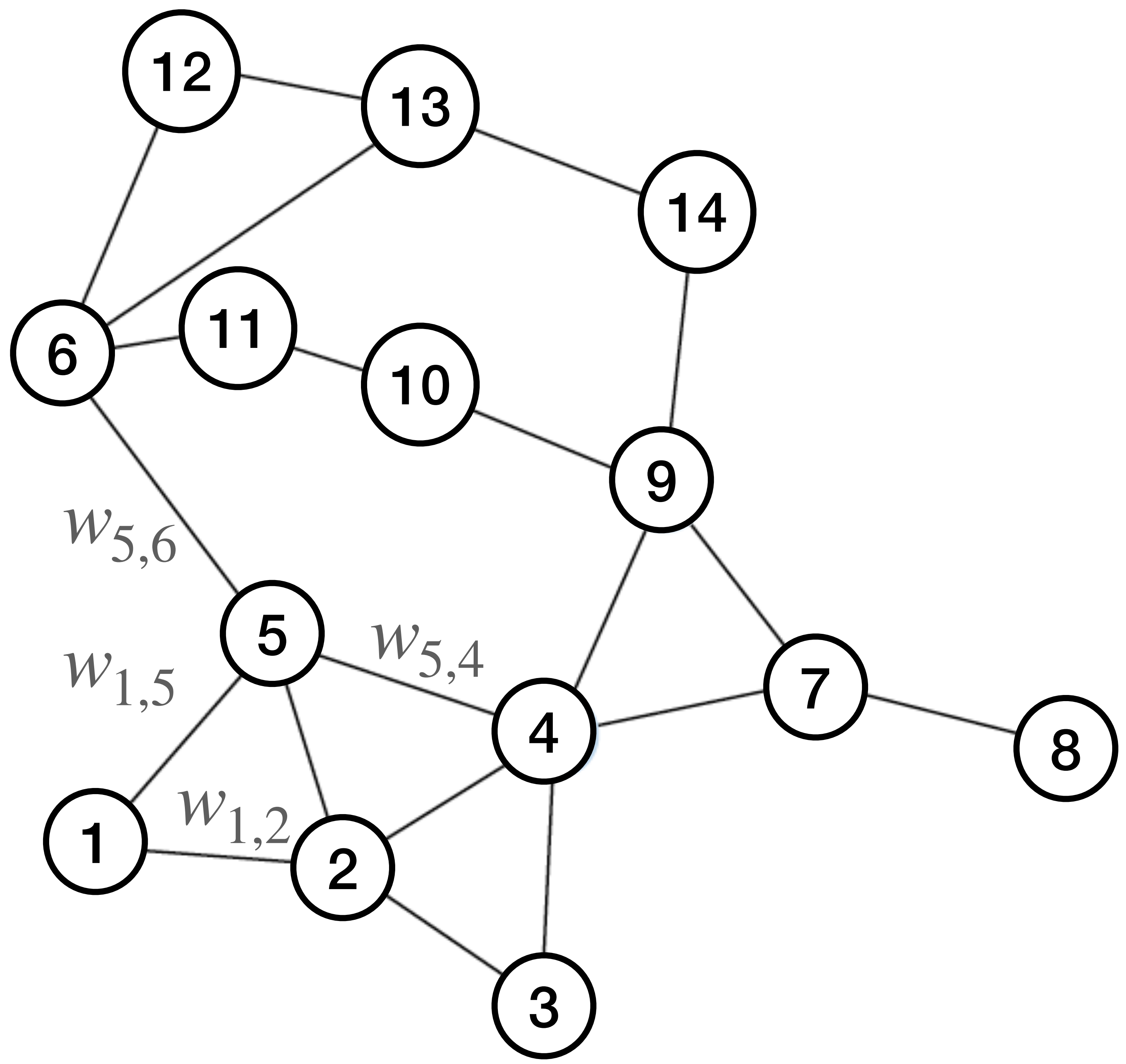
Power System Represented as an Undirected Graph

Substations (generators/loads) → vertices

Transmission lines → edges

Susceptance over the lines→ edge weights





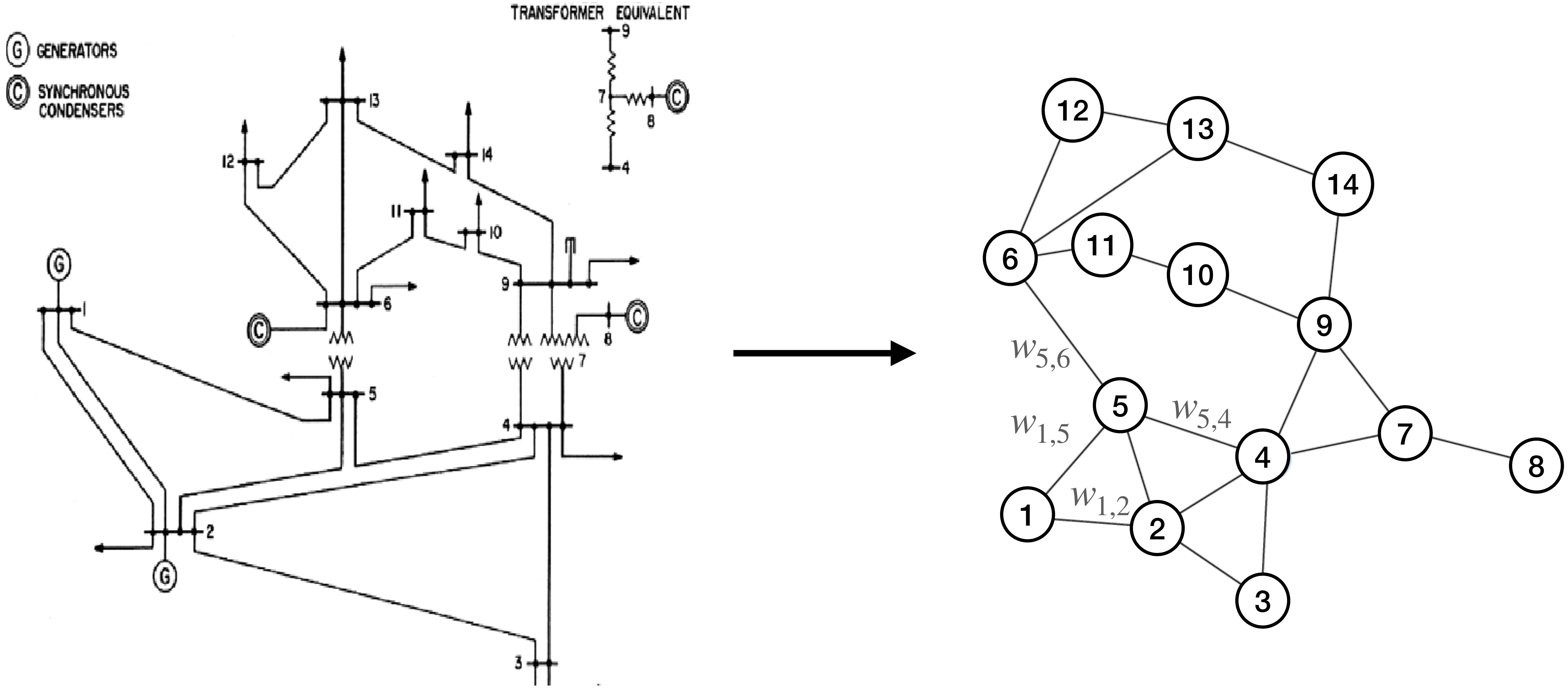
Power System Represented as an Undirected Graph

Substations (generators/loads) → vertices

Transmission lines → edges

(generators/loads) ⟷ (Sources/Sinks)

Susceptance over the lines→ edge weights



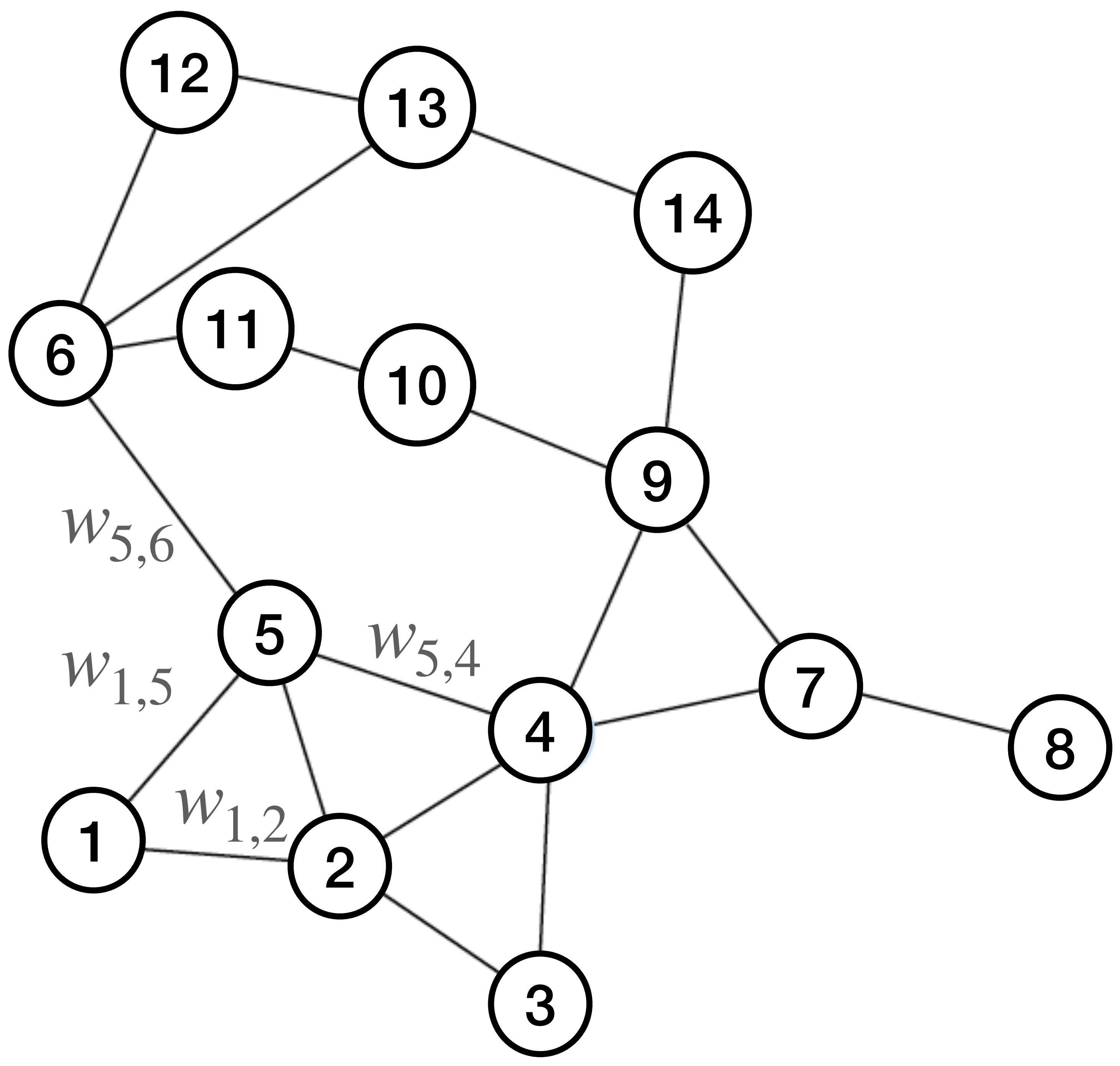
Direct Current Power Flow Model

Vertex measurement: (active power injection)

$$z_v = \sum_{u \in \mathcal{N}_v} w_{v,u}(\theta_v - \theta_u)$$

Edge measurement: (active power flow)

$$z_{(u,v)} = w_{v,u}(\theta_v - \theta_u)$$



$\mathcal{N}_v$: neighbor vertices of vertex v

$w_{u,v}$: weight over edge (u, v)

θ_v: state value over vertex v (voltage phase)

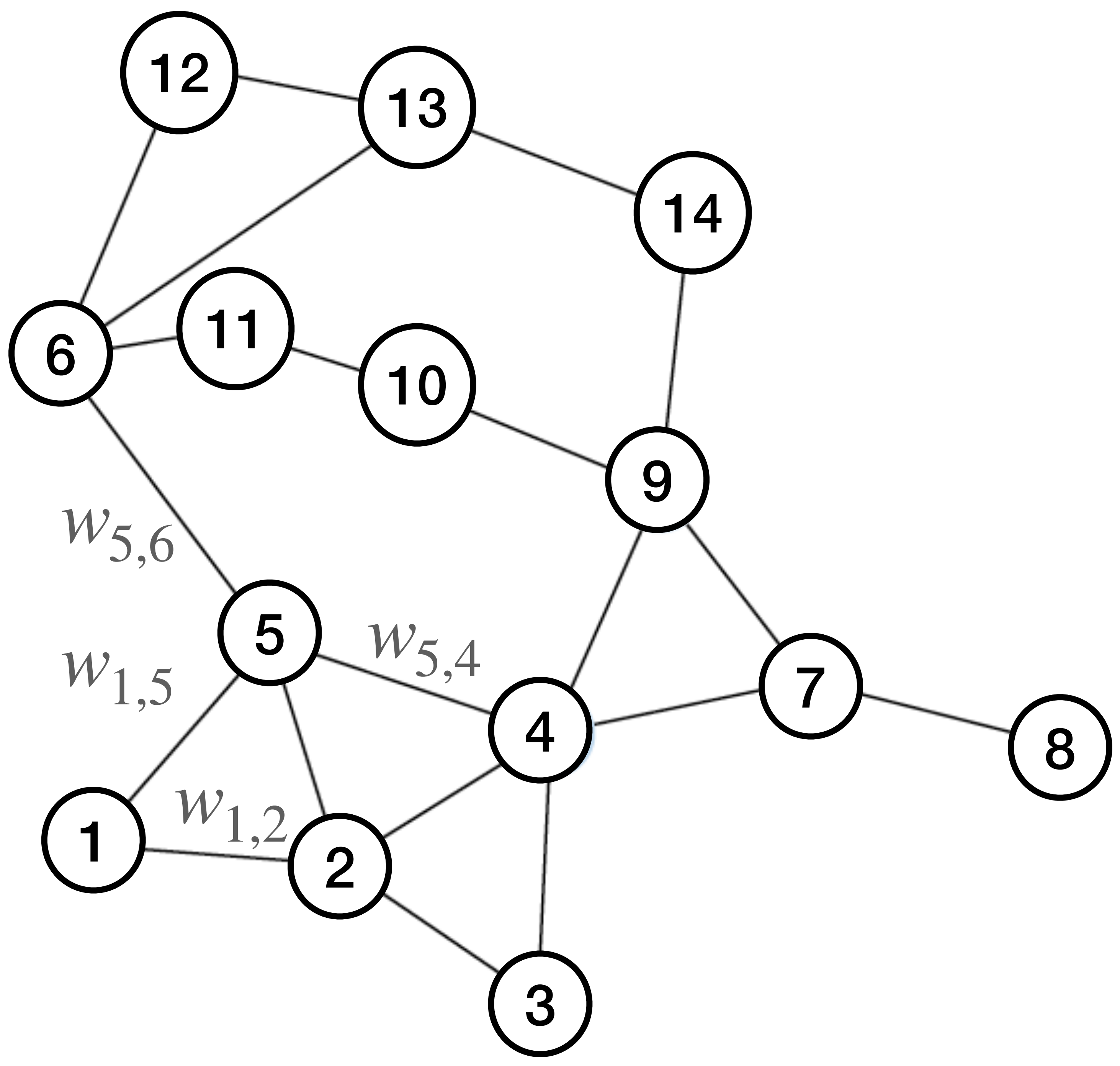
Direct Current Power Flow Model

Vertex measurement: (active power injection)

$$z_v = \sum_{u \in \mathcal{N}_v} w_{v,u}(\theta_v - \theta_u)$$

Edge measurement: (active power flow)

$$z_{(u,v)} = w_{v,u}(\theta_v - \theta_u)$$



$\mathcal{N}_v$: neighbor vertices of vertex v

$w_{u,v}$: weight over edge (u, v)

θ_v: state value over vertex v (voltage phase)

Linear Model

$$\boldsymbol{z} = \boldsymbol{H\theta} + \boldsymbol{noise}$$

$\boldsymbol{H}$ - represents the system topology

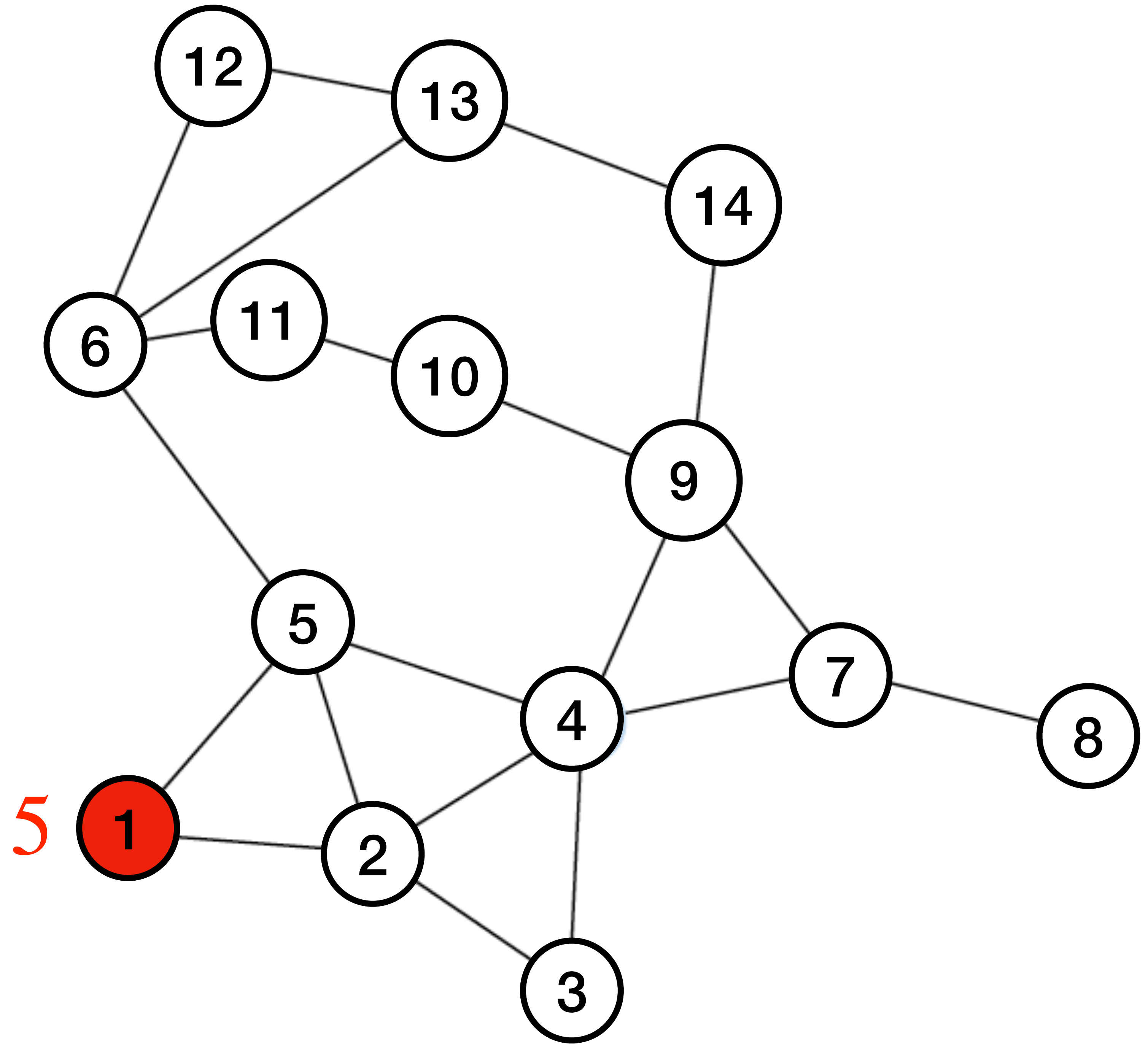
False Data Injection Attack Models

$$z = \boldsymbol{H\theta} + \boldsymbol{a} + noise$$

False Data Injection Attack Models

$$z = \boldsymbol{H\theta} + \boldsymbol{a} + noise$$

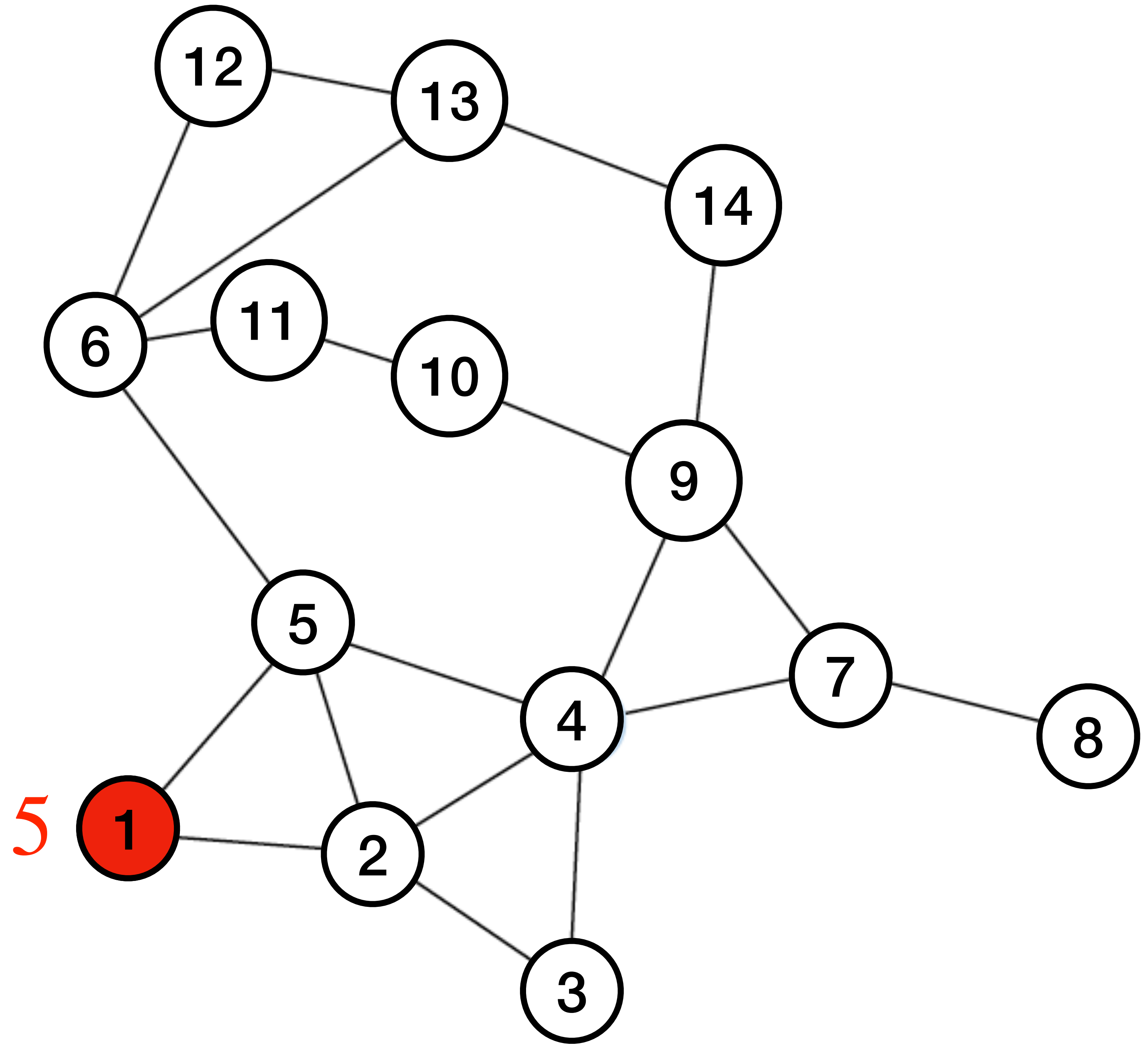
Regular: $\boldsymbol{a}$



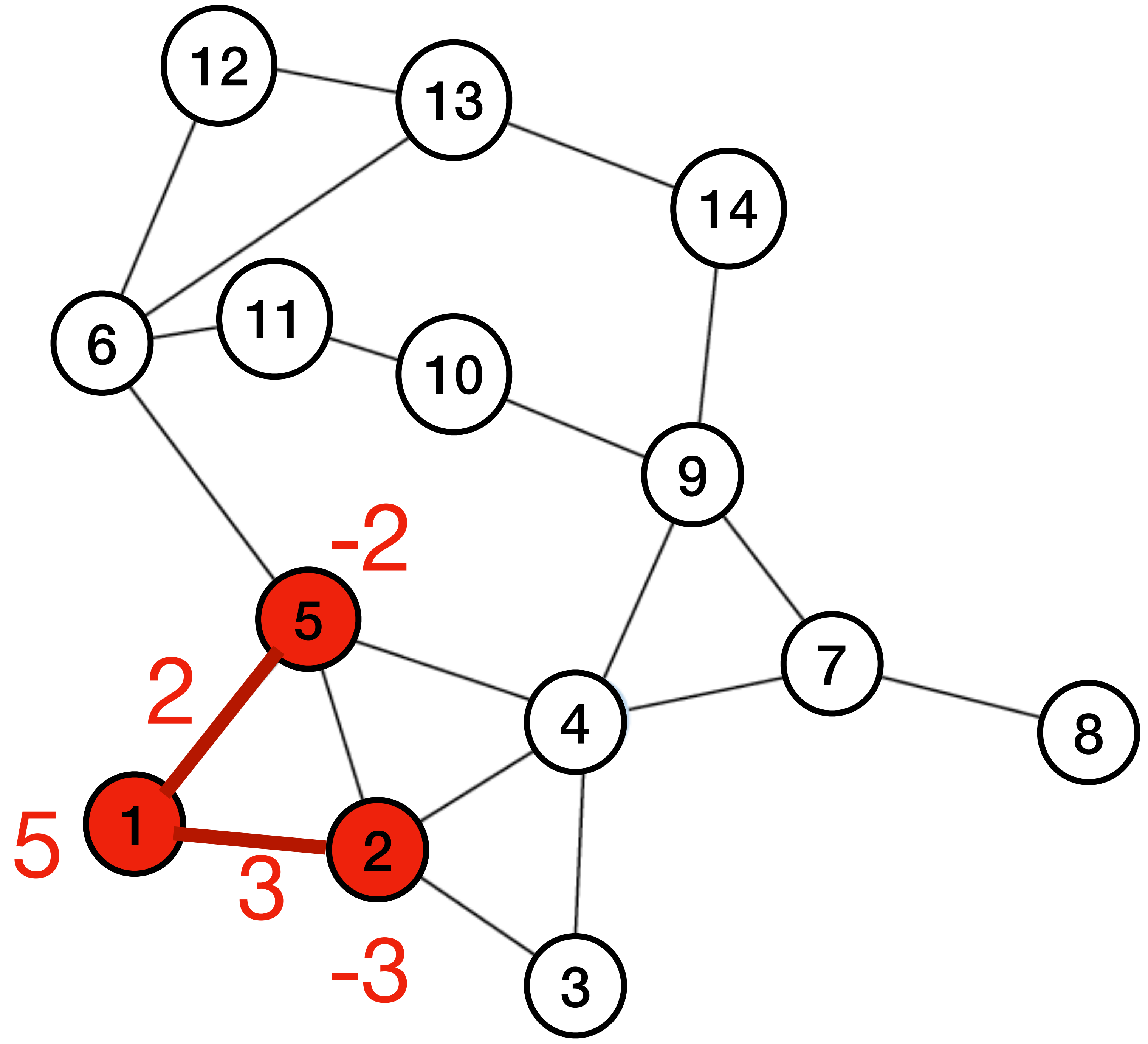
False Data Injection Attack Models

$$z = H\theta + a + noise$$

Regular: a

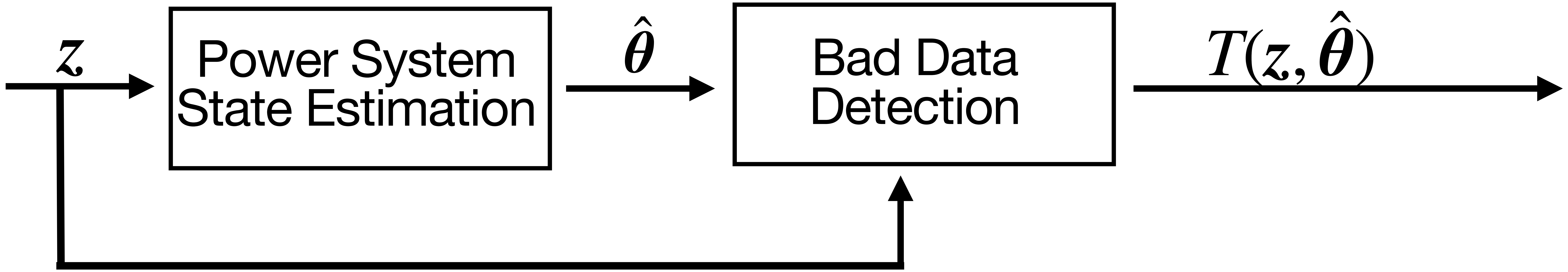


Unobservable: $a = Hc$



Traditional Bad Data Detection

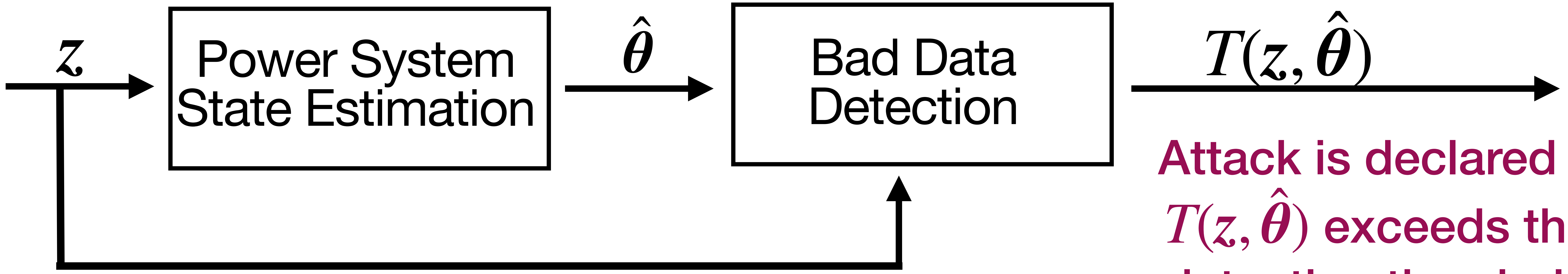
$$z = \boldsymbol{H\theta} + \boldsymbol{a} + noise$$



* The noise is assumed i.i.d with a standard normal distribution

Traditional Bad Data Detection

$$z = H\theta + a + noise$$

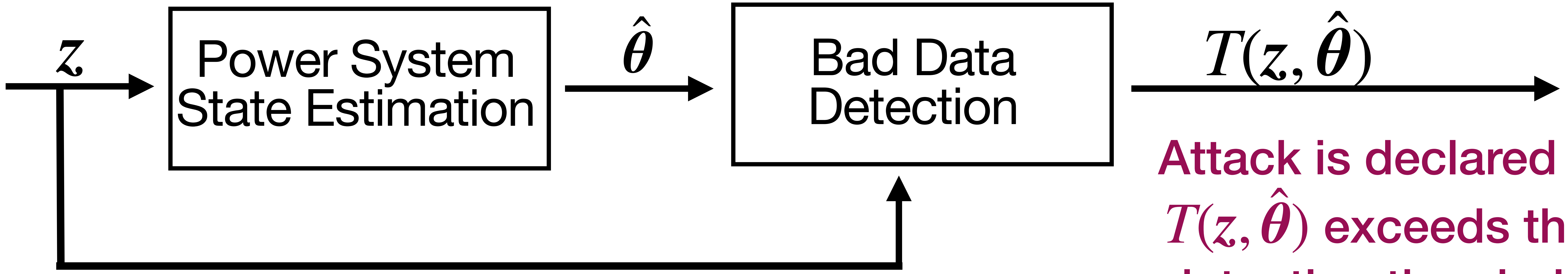


Attack is declared If $T(z, \hat{\theta})$ exceeds the detection threshold

* The noise is assumed i.i.d with a standard normal distribution

Traditional Bad Data Detection

$$z = \boldsymbol{H\theta} + \boldsymbol{a} + noise$$



Attack is declared If $T(z, \hat{\boldsymbol{\theta}})$ exceeds the detection threshold

$$T(z, \boldsymbol{\theta}) = ||z - \boldsymbol{H\theta}||_2^2$$

$$\hat{\boldsymbol{\theta}} = \min_{\boldsymbol{\theta}} \; T(z, \boldsymbol{\theta}) = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T z$$

* The noise is assumed i.i.d with a standard normal distribution

Traditional Bad Data Detection

Fail to detect unobservable false data injection attacks ($\boldsymbol{a} = \boldsymbol{Hc}$)

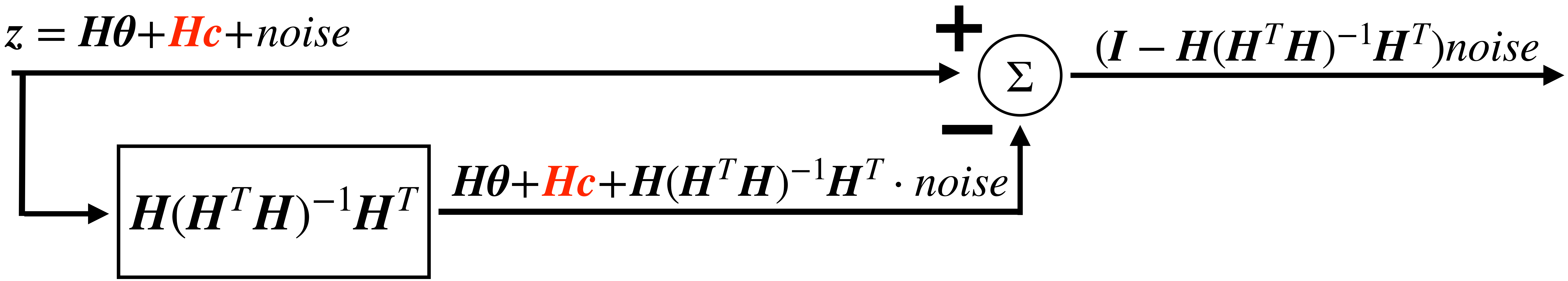
$$
\begin{aligned}
T(z, \hat{\boldsymbol{\theta}}) &= ||z - \boldsymbol{H}\hat{\boldsymbol{\theta}}||_2^2 \\
&= ||z - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{z}||_2^2
\end{aligned}
$$

Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, *14*(1), 1-33.

Traditional Bad Data Detection

Fail to detect unobservable false data injection attacks ($a = Hc$)

$$
\begin{aligned}
T(z, \hat{\theta}) &= ||z - H\hat{\theta}||_2^2 \\
&= ||z - H(H^T H)^{-1} H^T z||_2^2
\end{aligned}
$$



Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, *14*(1), 1-33.

Outline

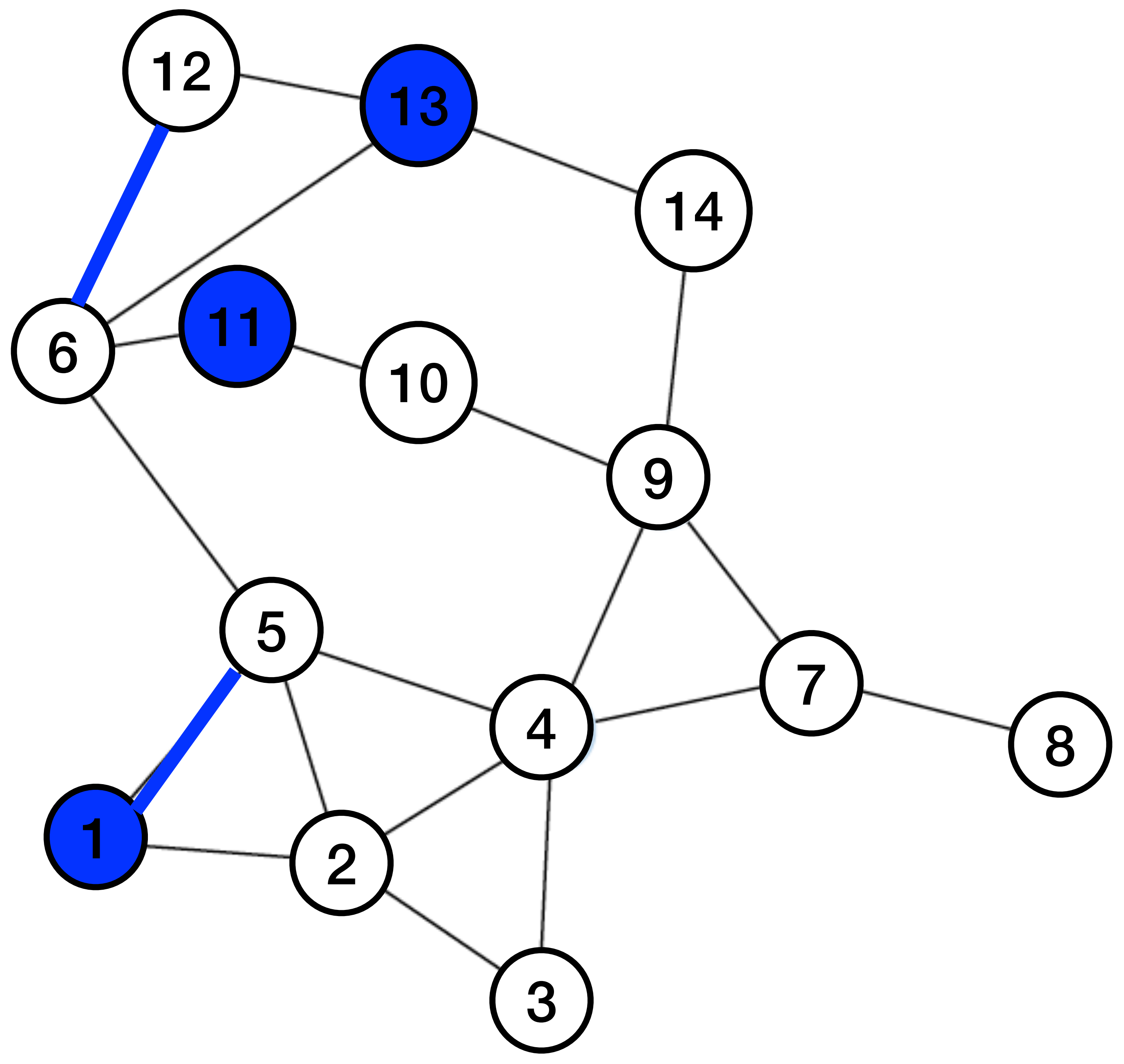
- Introduction
- Background
- **Theory: Secured Sensors and Graph Smoothness Based Detection for False Data Injection Attacks**
- Theory: Modification for Distributed Optimization
- Theory: Generalization From Smooth Graph Signals to Low-Pass Graph Signals
- Performance Evaluation

Secured Sensors

$\boldsymbol{a}_{\mathcal{S}} = \mathbf{0}$

Secured sensors are assumed to be immuned from an attack

Additional resources are used to protect these sensors: guards, electric fences, ….



$\mathcal{S} = \{1,11,13,(1,5),(6,12)\}$

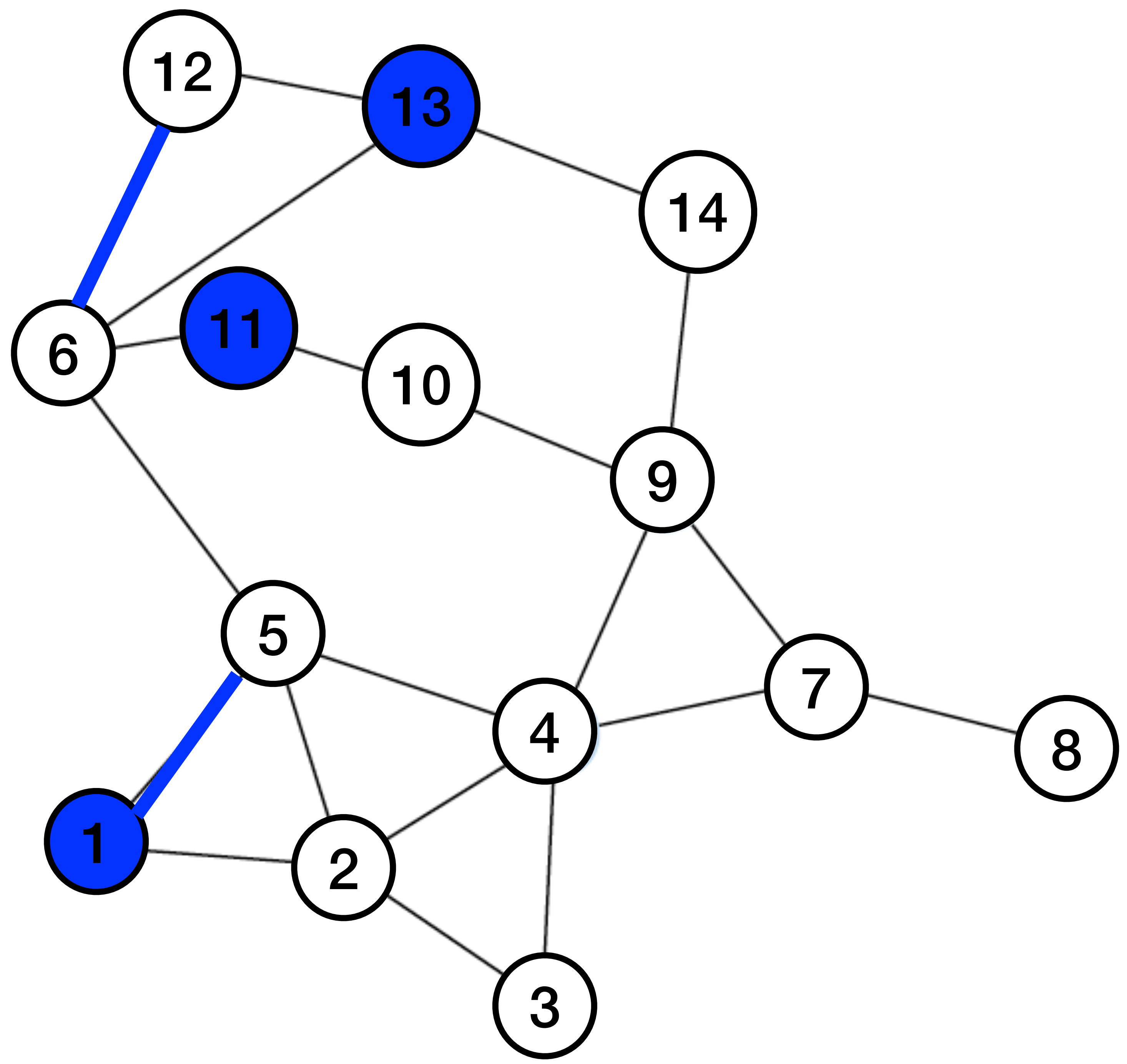
Secured Sensors

$\boldsymbol{a}_{\mathcal{S}} = \mathbf{0}$

Secured sensors are assumed to be immuned from an attack

Additional resources are used to protect these sensors: guards, electric fences, ….

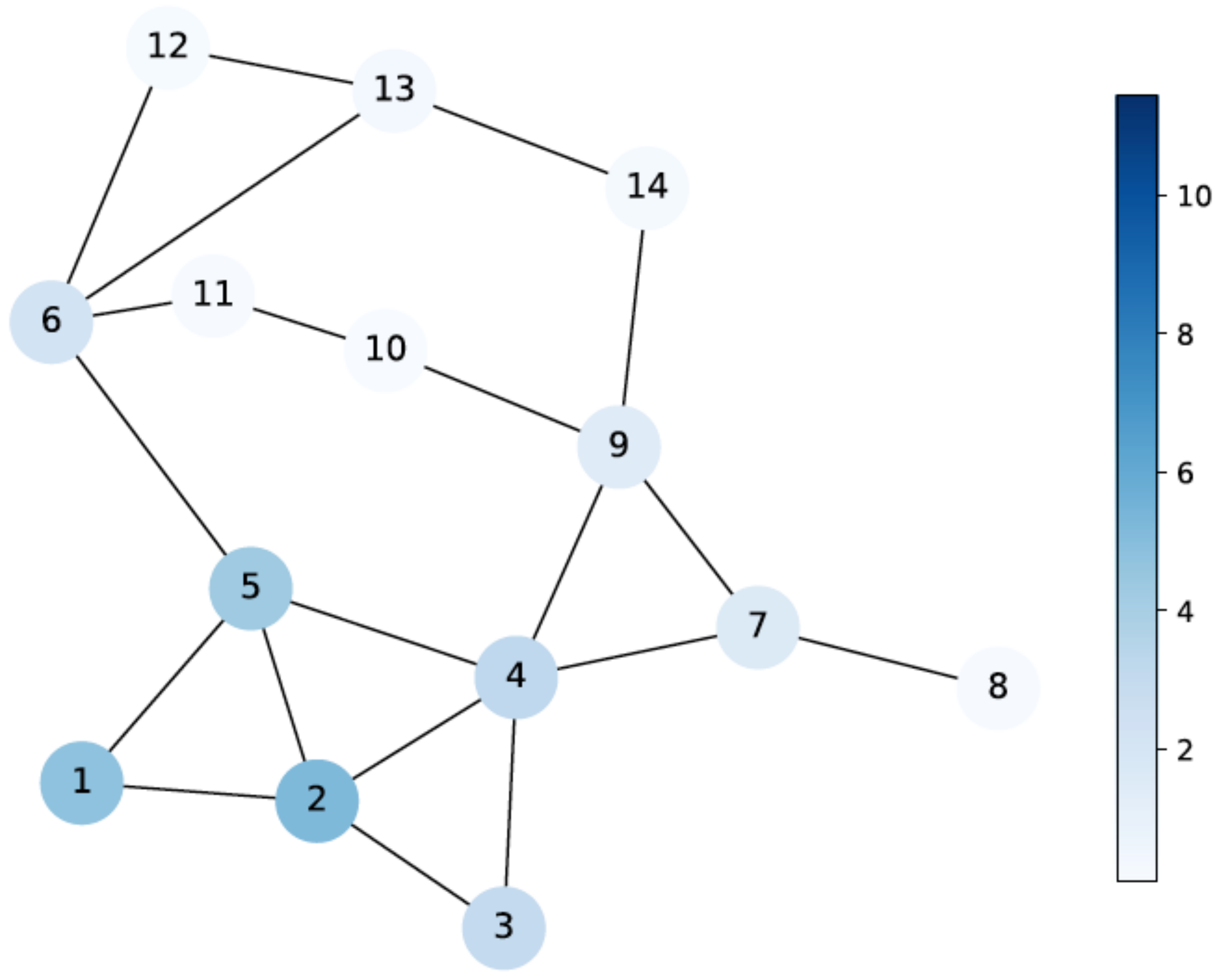
Design Flexibility
$\boldsymbol{a}_{\mathcal{S}} = \mathbf{0} \rightarrow \lvert\lvert \boldsymbol{a}_{\mathcal{S}} \rvert\rvert_2^2 \leq \epsilon_1$



$\mathcal{S} = \{1,11,13,(1,5),(6,12)\}$

Power System States are Smooth Graph Signals

The difference between the signal state values in neighbor vertices is assumed small



State Signal

Each vertex is assigned with a value represented by its color

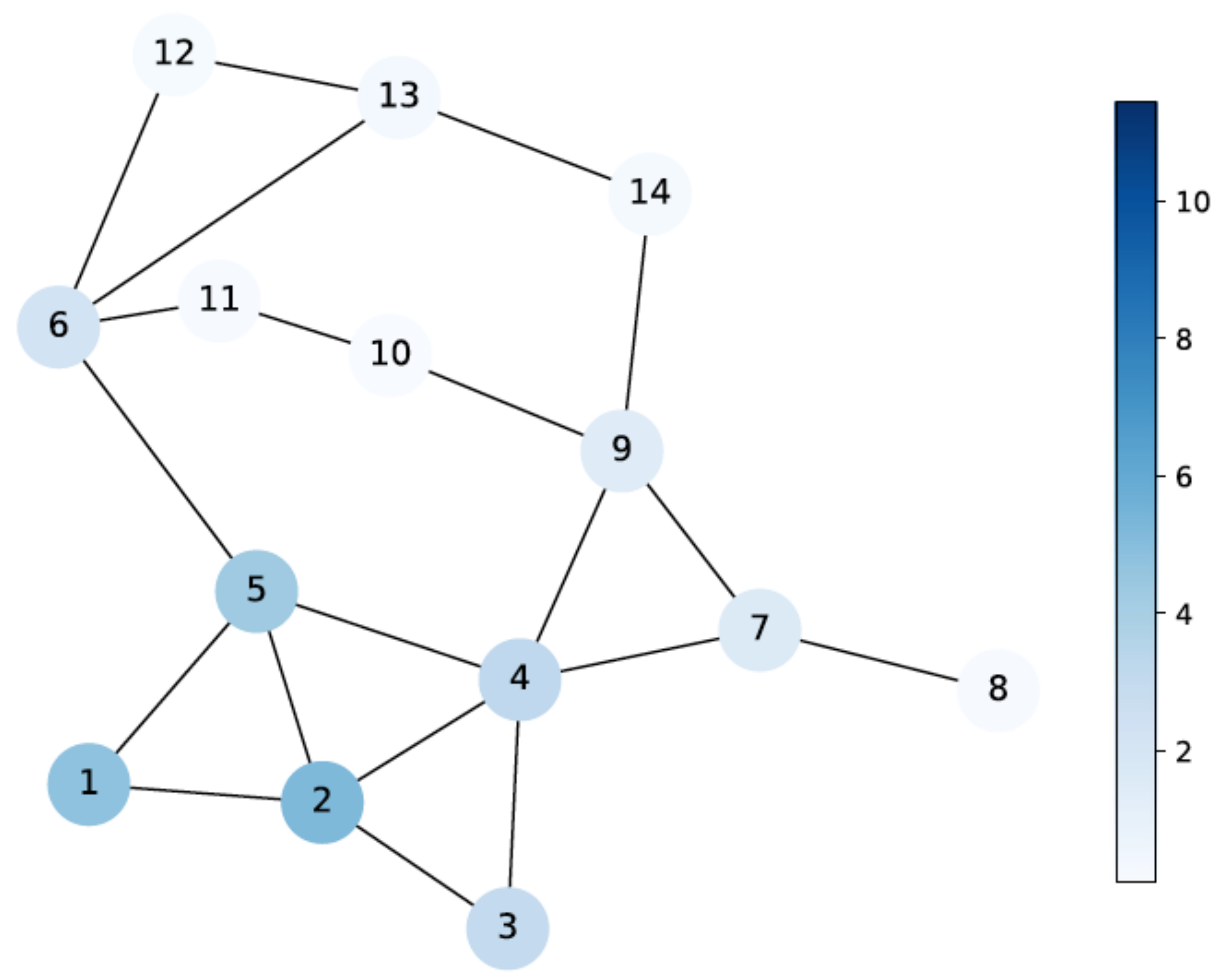
Dabush, Lital, Ariel Kroizer, and Tirza Routtenberg. "State estimation in partially observable power systems via graph signal processing tools." *Sensors* 23.3 (2023): 1387.

Power System States are Smooth Graph Signals

The difference between the signal state values in neighbor vertices is assumed small

↓

Hence, the signal variation over the graph is smooth



State Signal

Each vertex is assigned with a value represented by its color

Dabush, Lital, Ariel Kroizer, and Tirza Routtenberg. "State estimation in partially observable power systems via graph signal processing tools." *Sensors* 23.3 (2023): 1387.

Power System States are Smooth Graph Signals

The difference between the signal state values in neighbor vertices is assumed small

↓

Hence, the signal variation over the graph is smooth

↓

It has a bounded graph Total Variation

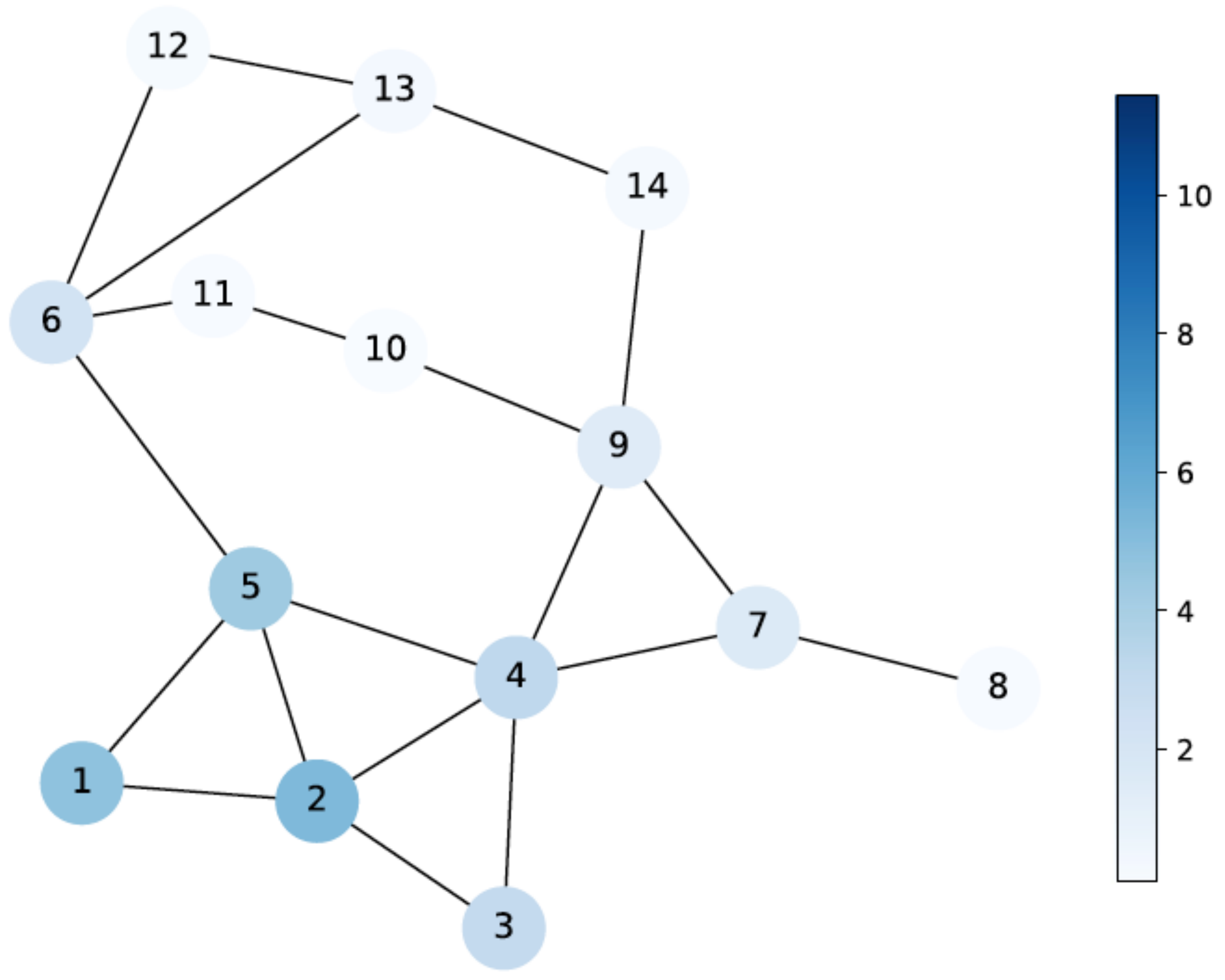
$$\sum_{v \in \mathcal{V}} \sum_{u \in \mathcal{N}_v} w_{v,u}(\theta_u - \theta_v)^2 \leq \epsilon_2$$

Sum over system vertices

Sum over vertex v neighbors

Edge weight

Signal variation between vertex v and vertex u



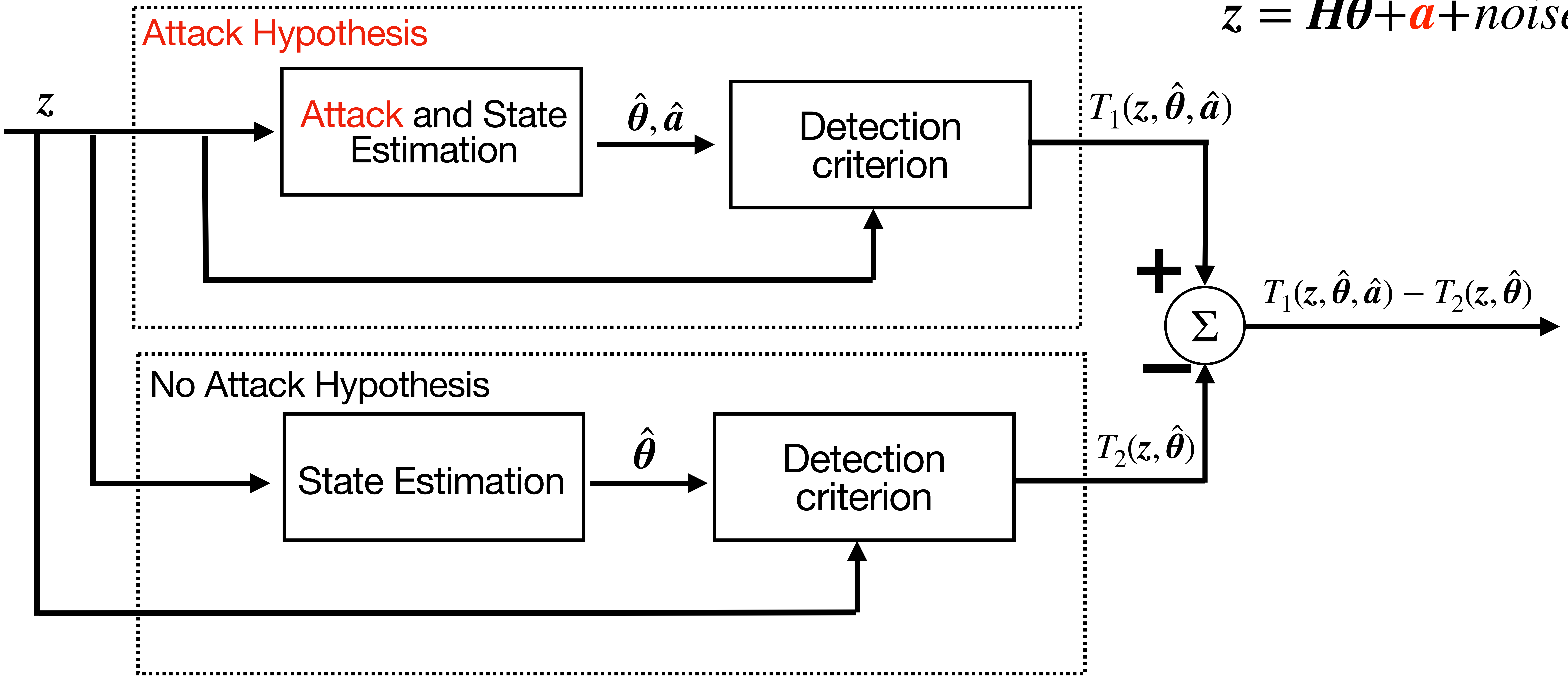
State Signal

Each vertex is assigned with a value represented by its color

Dabush, Lital, Ariel Kroizer, and Tirza Routtenberg. "State estimation in partially observable power systems via graph signal processing tools." *Sensors* 23.3 (2023): 1387.

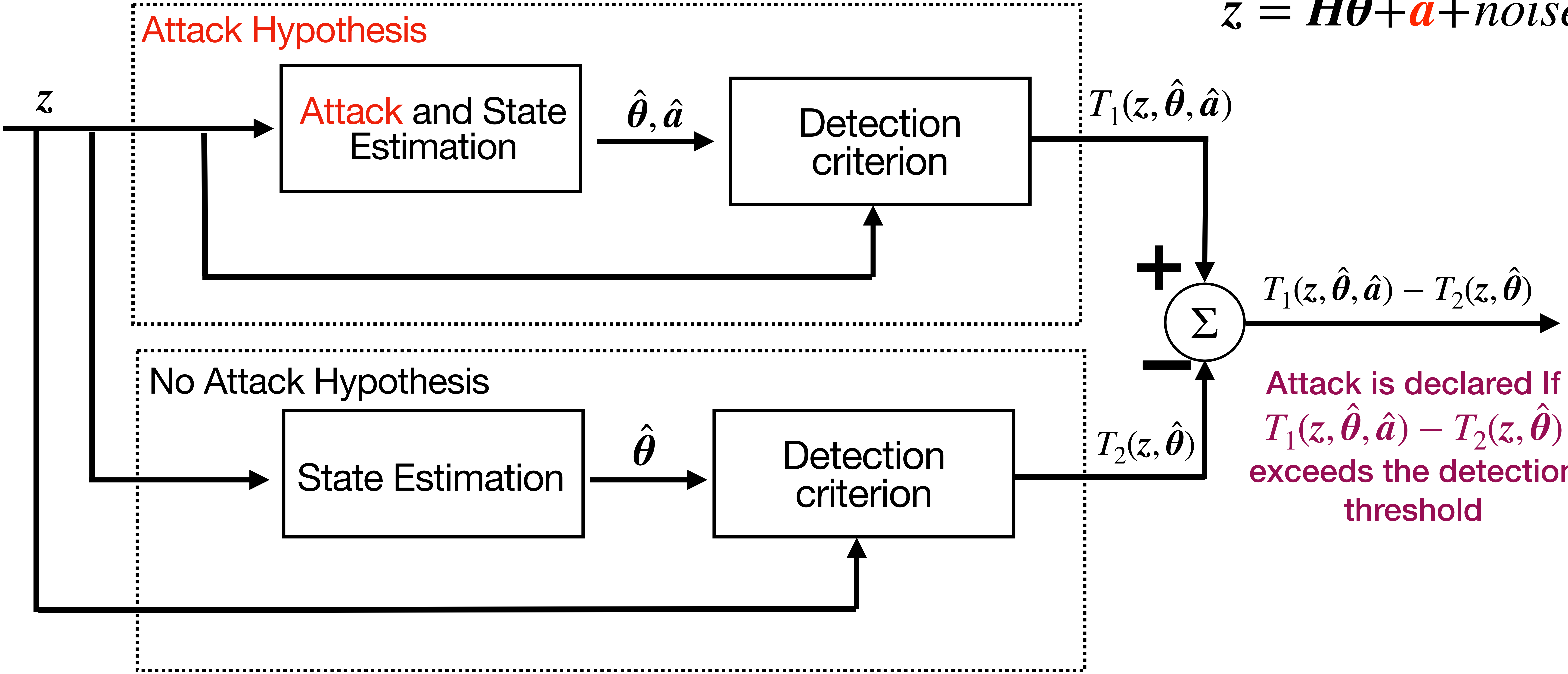
Secured Sensors and Graph Based Detection

$$z = \boldsymbol{H\theta} + \boldsymbol{a} + noise$$



Secured Sensors and Graph Based Detection

$$z = \boldsymbol{H\theta} + \boldsymbol{a} + noise$$



Attack is declared If $T_1(z, \hat{\boldsymbol{\theta}}, \hat{\boldsymbol{a}}) - T_2(z, \hat{\boldsymbol{\theta}})$ exceeds the detection threshold

Secured Sensors and Graph Based Detection

Attack Hypothesis

$$T_1(z, \boldsymbol{\theta}, \boldsymbol{a}) = ||z - \boldsymbol{H\theta} - \boldsymbol{a}||_2^2 - \mu_1 ||\boldsymbol{a}_{\mathcal{S}}||_2^2 - \mu_2 \sum_{v \in \mathcal{V}} \sum_{u \in \mathcal{N}_v} w_{v,u}(\theta_u - \theta_v)^2$$

$$\hat{\boldsymbol{\theta}} = \min_{\boldsymbol{\theta}, \boldsymbol{a}} \; T_1(z, \boldsymbol{\theta}, \boldsymbol{a})$$

No Attack Hypothesis

$$T_2(z, \boldsymbol{\theta}) = ||z - \boldsymbol{H\theta}||_2^2 - \mu_2 \sum_{v \in \mathcal{V}} \sum_{u \in \mathcal{N}_v} \omega_{v,u}(\theta_u - \theta_v)^2$$

$$\hat{\boldsymbol{\theta}} = \min_{\boldsymbol{\theta}} \; T_2(z, \boldsymbol{\theta})$$

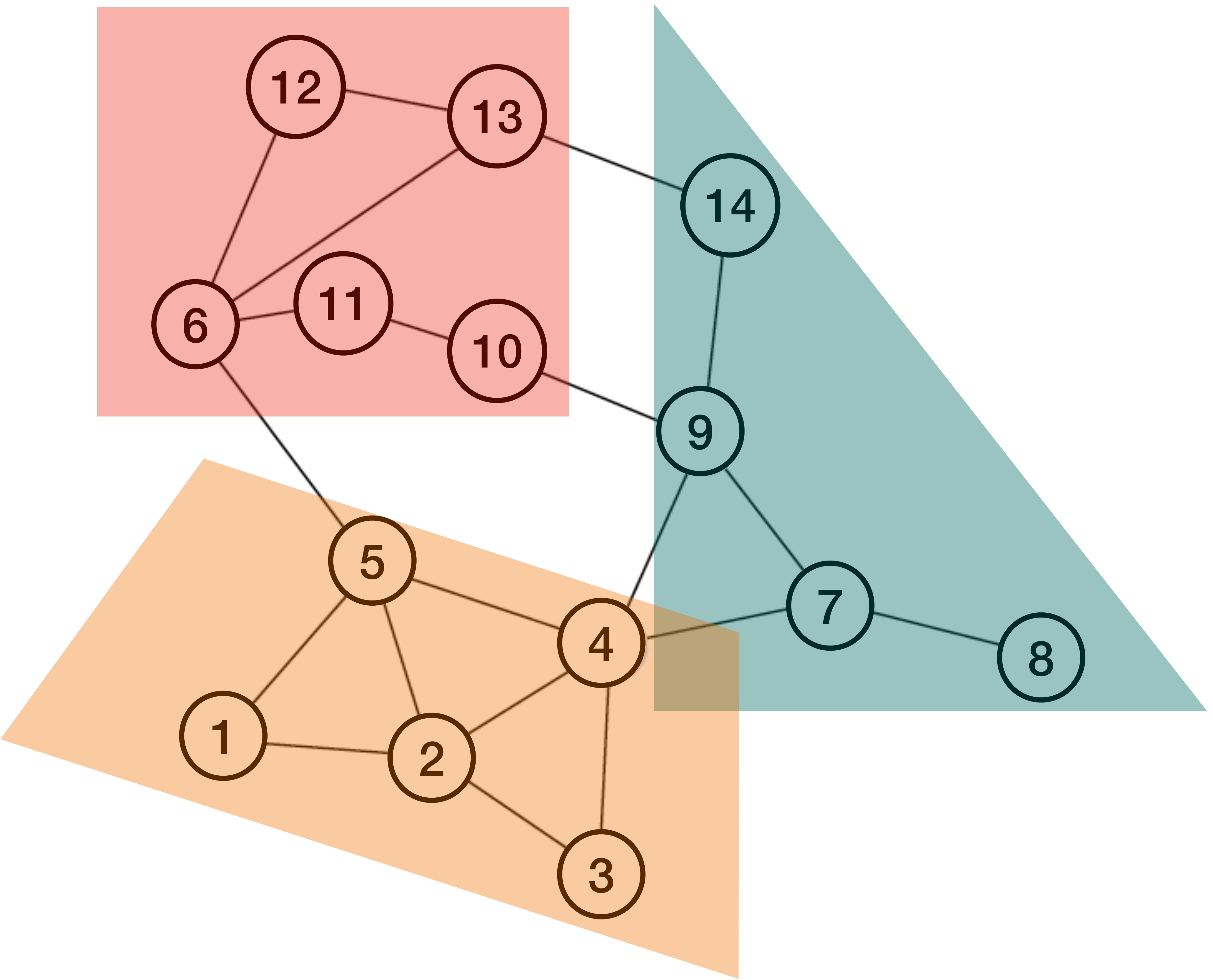
* The noise is assumed i.i.d with a standard normal distribution

Outline

- Introduction
- Background
- Theory: Secured Sensors and Graph Smoothness Based Detection for False Data Injection Attacks
- **Theory: Modification for Distributed Optimization**
- Theory: Generalization From Smooth Graph Signals to Low-Pass Graph Signals
- Performance Evaluation

Modification to Distributed Optimization

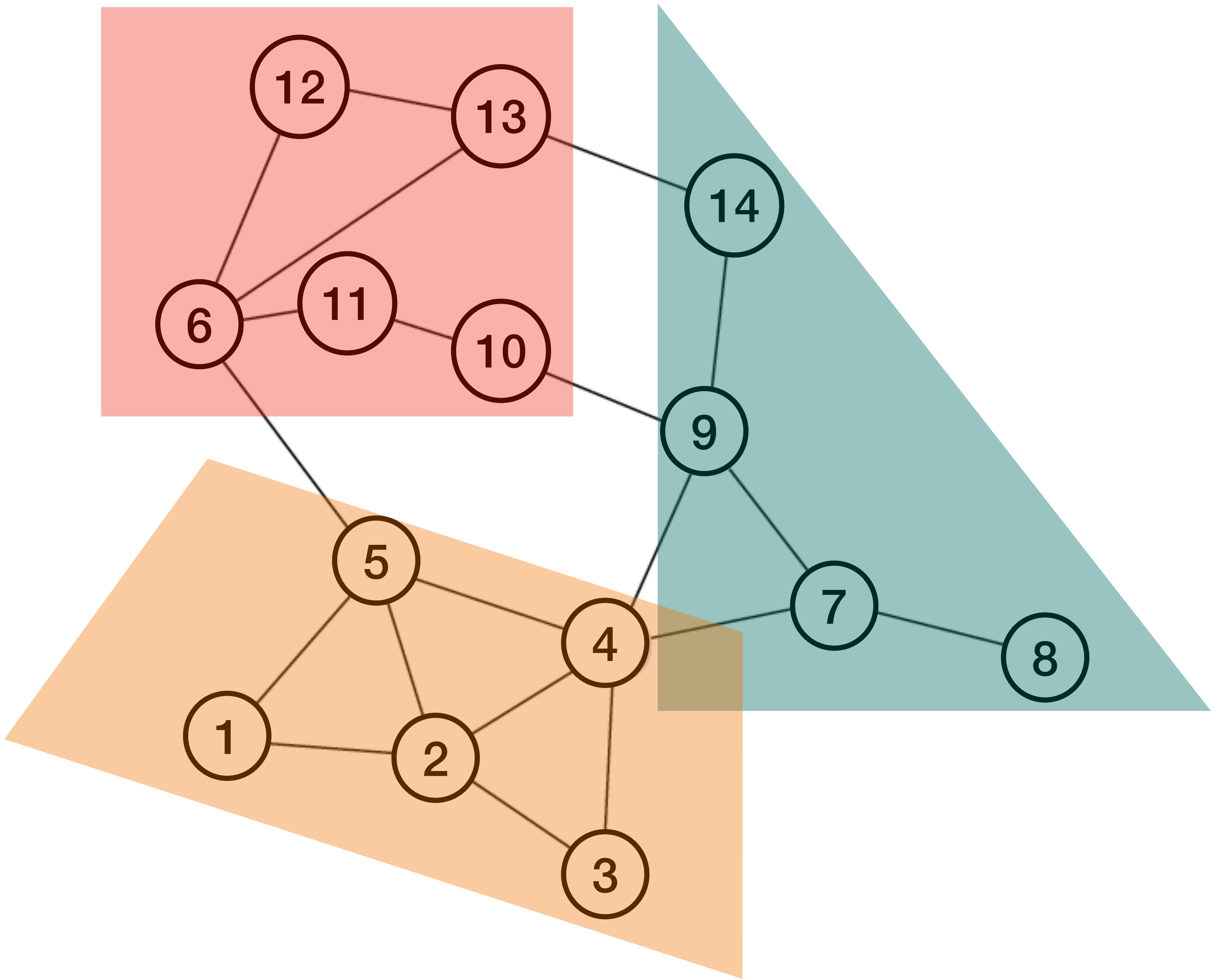
$$\boldsymbol{z}_l = \boldsymbol{H}_l\boldsymbol{\theta}_l + \boldsymbol{a}_l + noise, \quad l = 1,2,\ldots$$



Modification to Distributed Optimization

$$\boldsymbol{z}_l = \boldsymbol{H}_l\boldsymbol{\theta}_l + \boldsymbol{a}_l + noise, \quad l = 1,2,\ldots$$

- The measurements in each area are contained in the area
  e.g. vertex measurement in the orange area are: 1,2,3,4,5

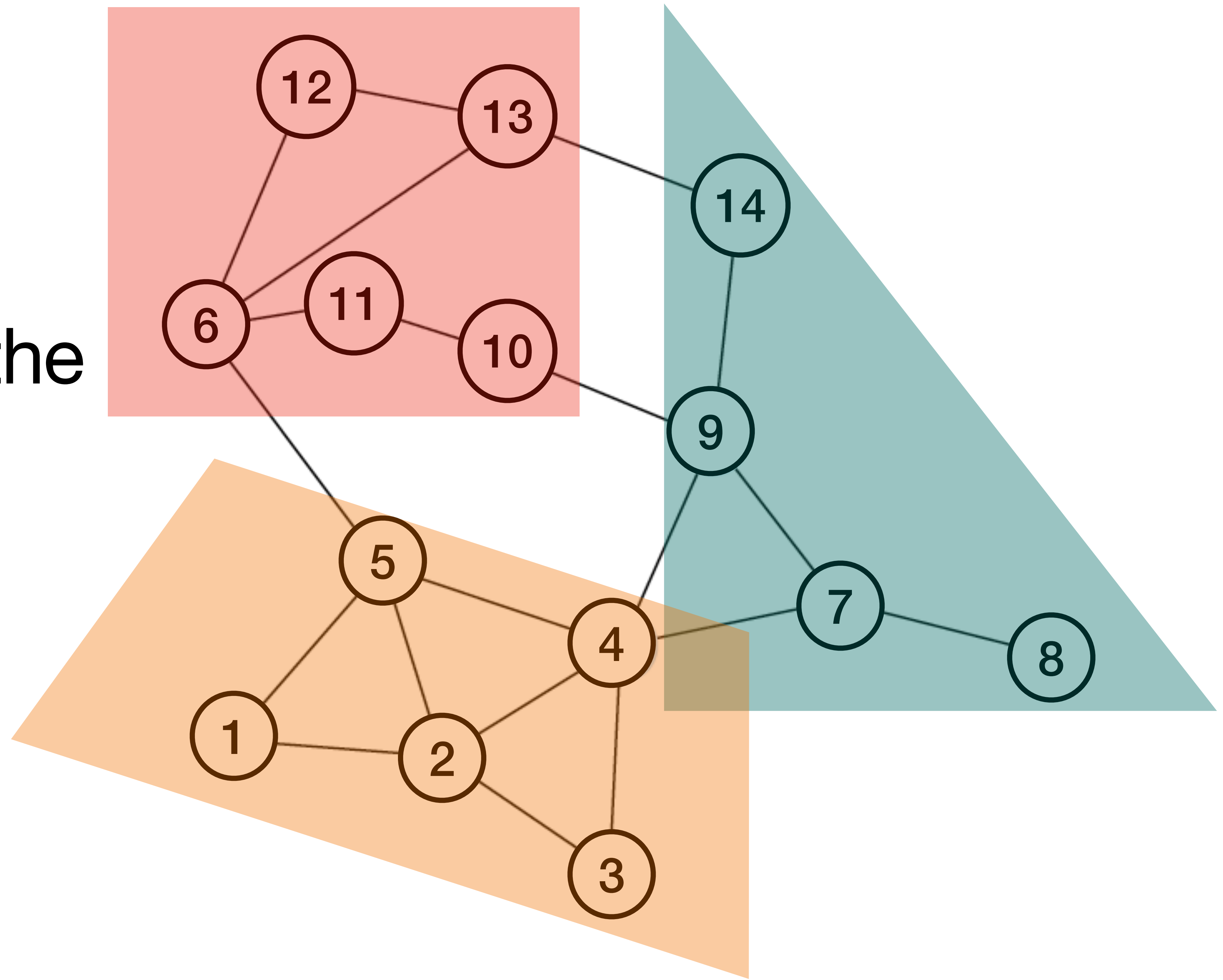


Modification to Distributed Optimization

$$\boldsymbol{z}_l = \boldsymbol{H}_l\boldsymbol{\theta}_l + \boldsymbol{a}_l + noise, \quad l = 1,2,\ldots$$

- The measurements in each area are contained in the area
  e.g. vertex measurement in the orange area are: 1,2,3,4,5

- The state variables in each area are the ones contained in the area and their first order neighbors.
  e.g. state variables in the orange area are: 1,2,3,4,5,6,7,9

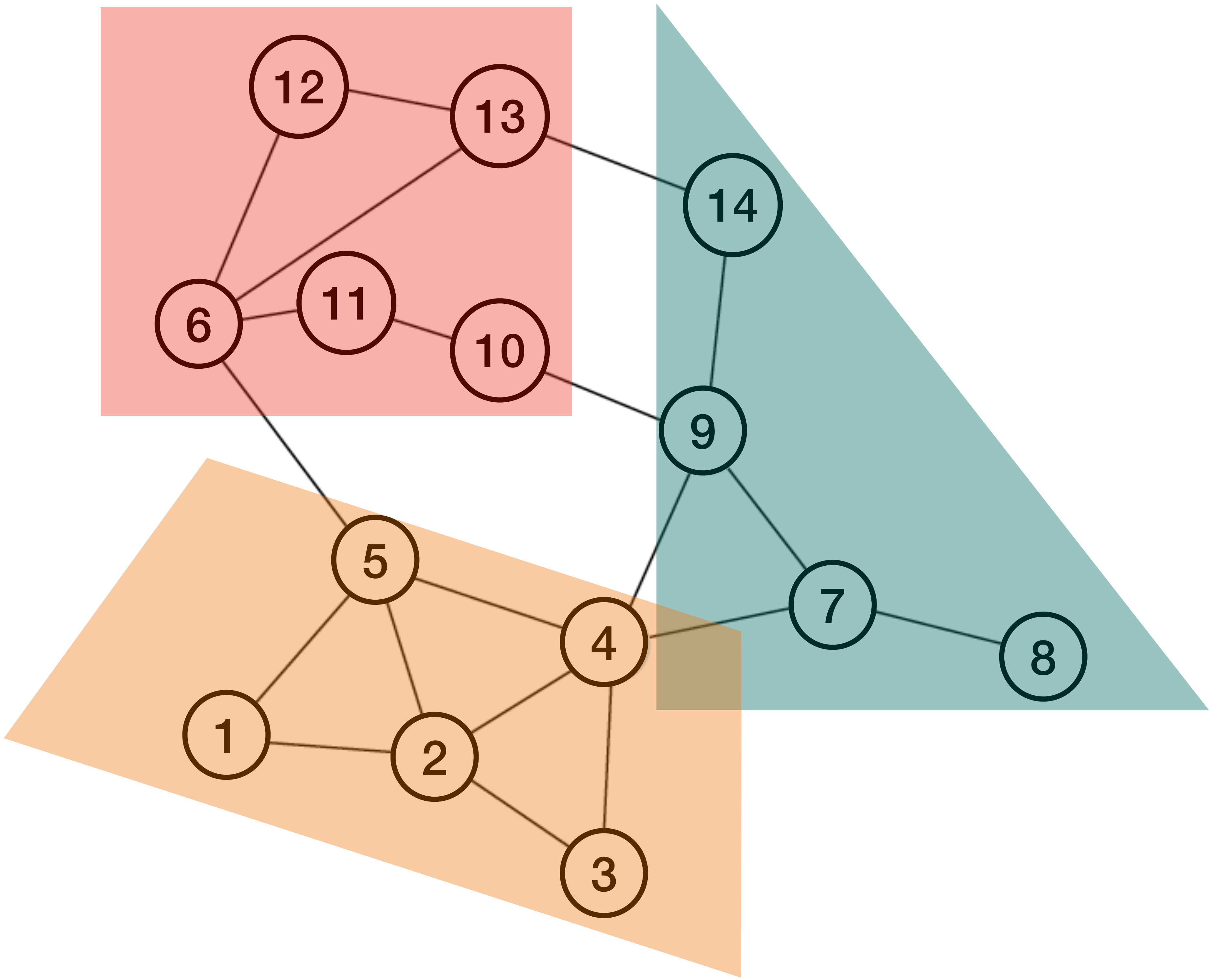


There is an overlap between state variables in neighbor areas

Modification to Distributed Optimization

$$z_l = H_l \theta_l + a_l + noise, \quad l = 1,2,\ldots$$

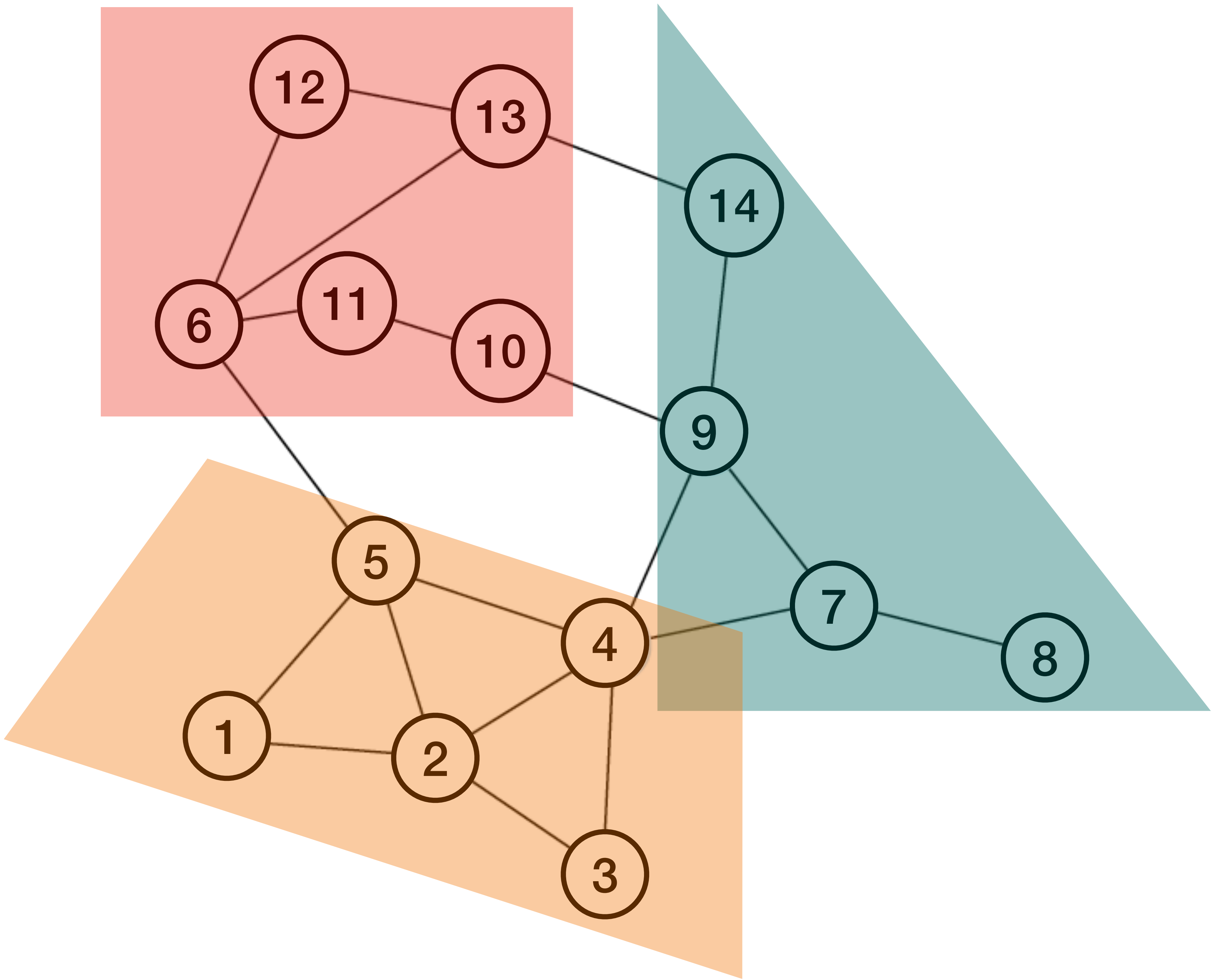
- State estimation and attack detection is performed in each area separately



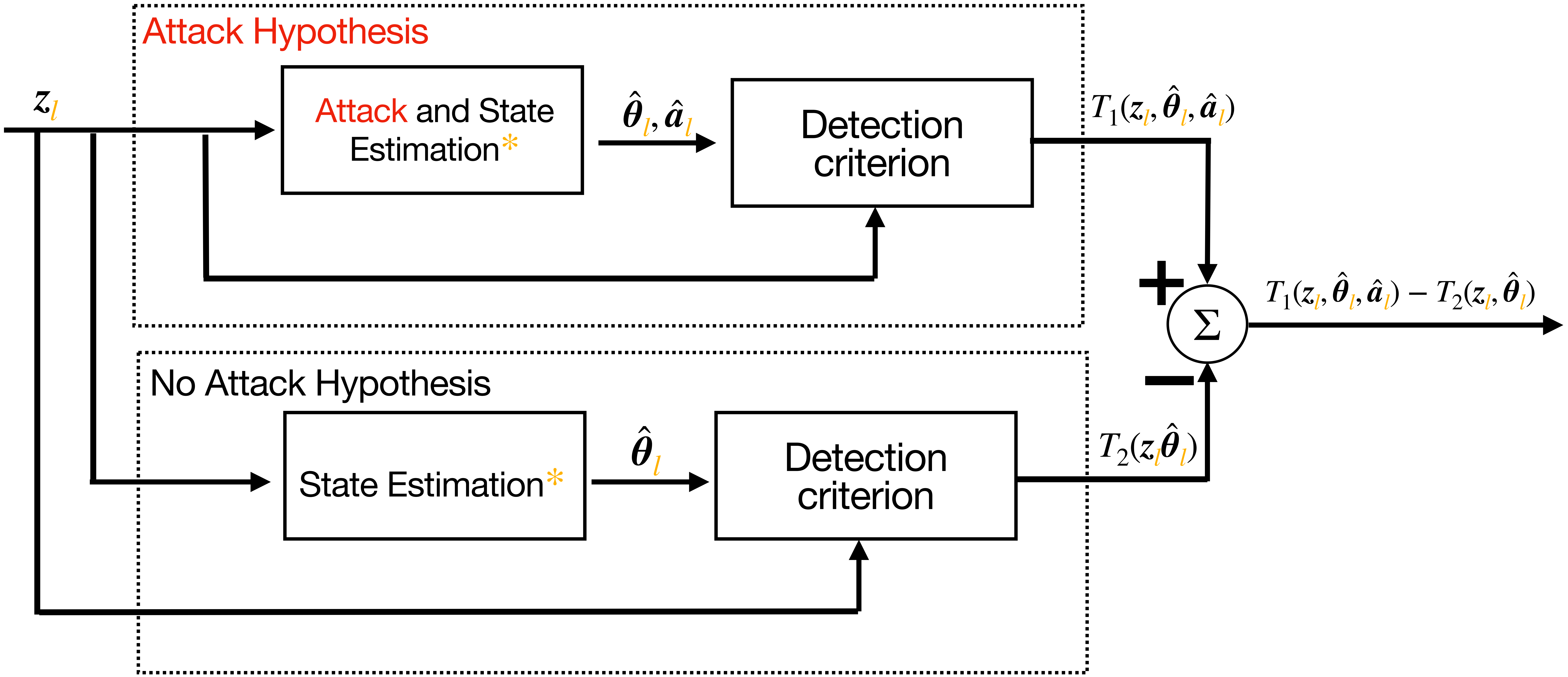
Modification to Distributed Optimization

$$\boldsymbol{z}_l = \boldsymbol{H}_l \boldsymbol{\theta}_l + \boldsymbol{a}_l + noise, \quad l = 1,2,\ldots$$

- State estimation and attack detection is performed in each area separately
- Estimation (states and attack) is performed in each area iteratively
- In each iteration, the control centers in neighbor areas share information on their state variables

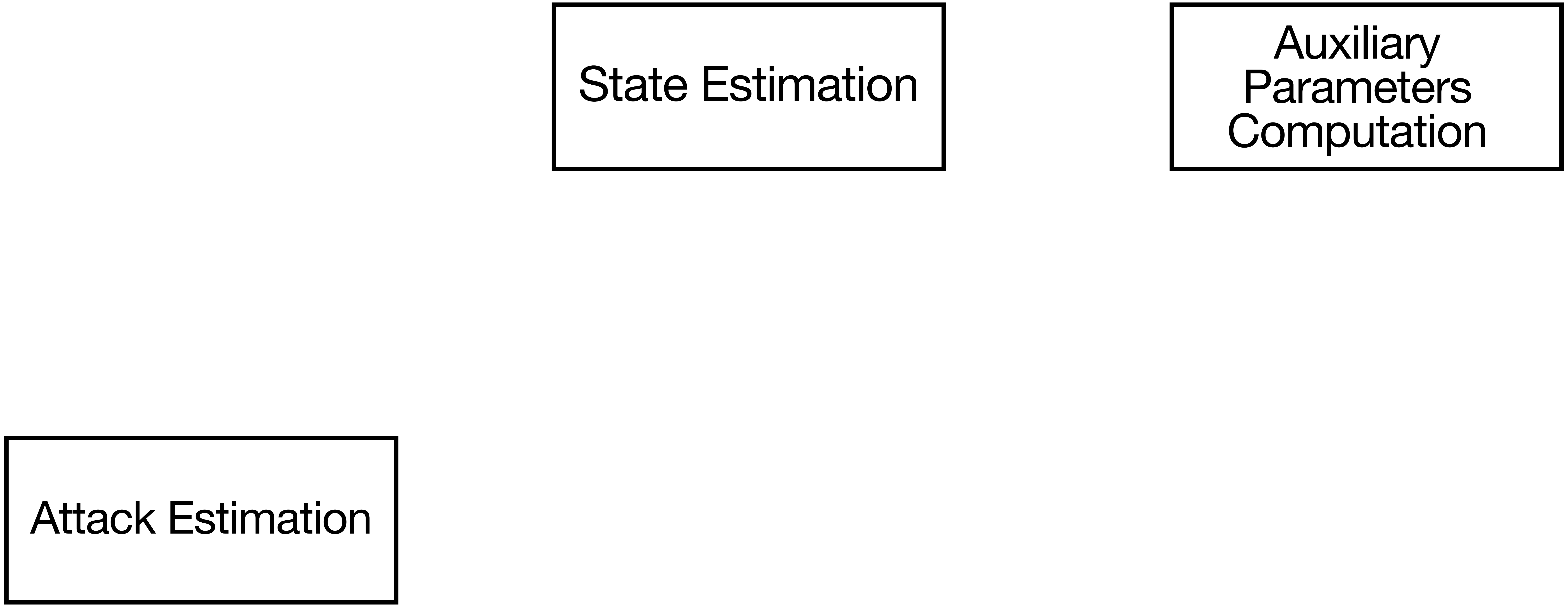


Secured Sensors and Graph Based Detection



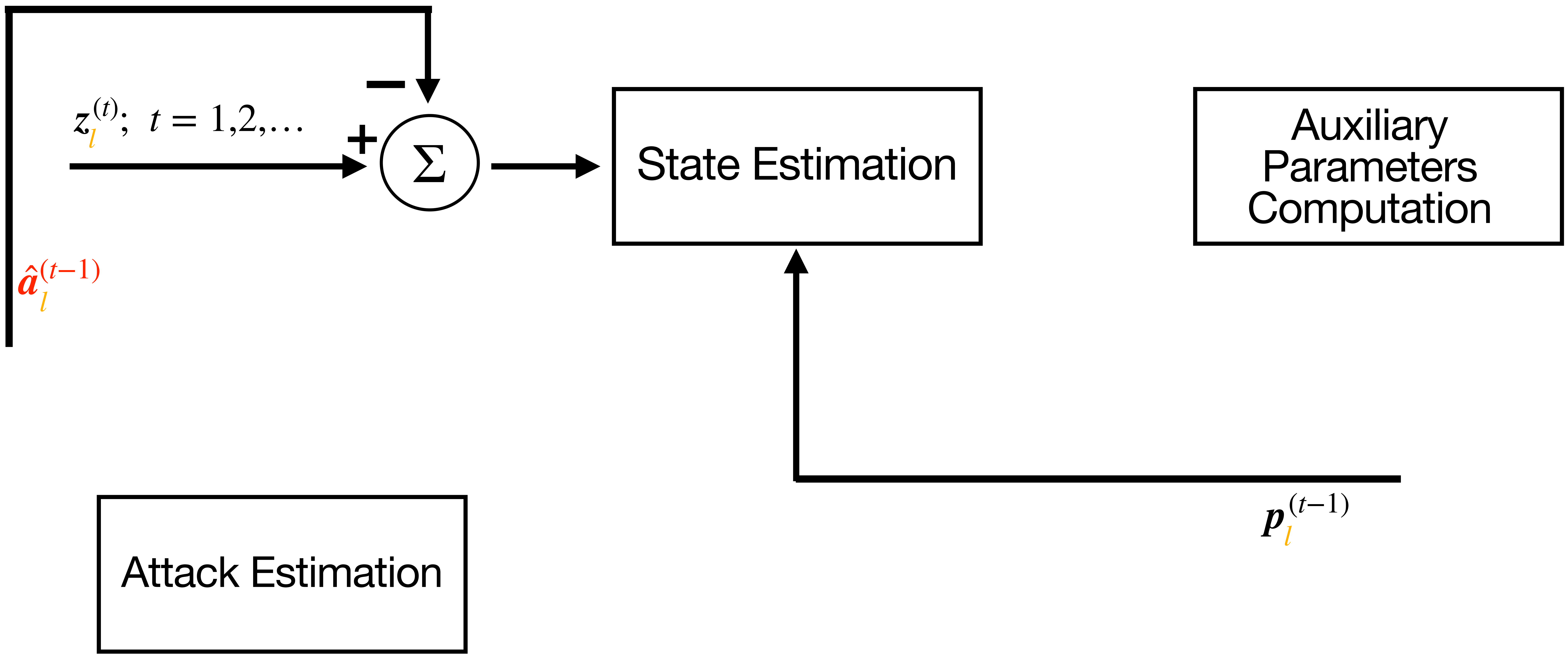
Secured Sensors and Graph Based Detection

Attack and State Estimation



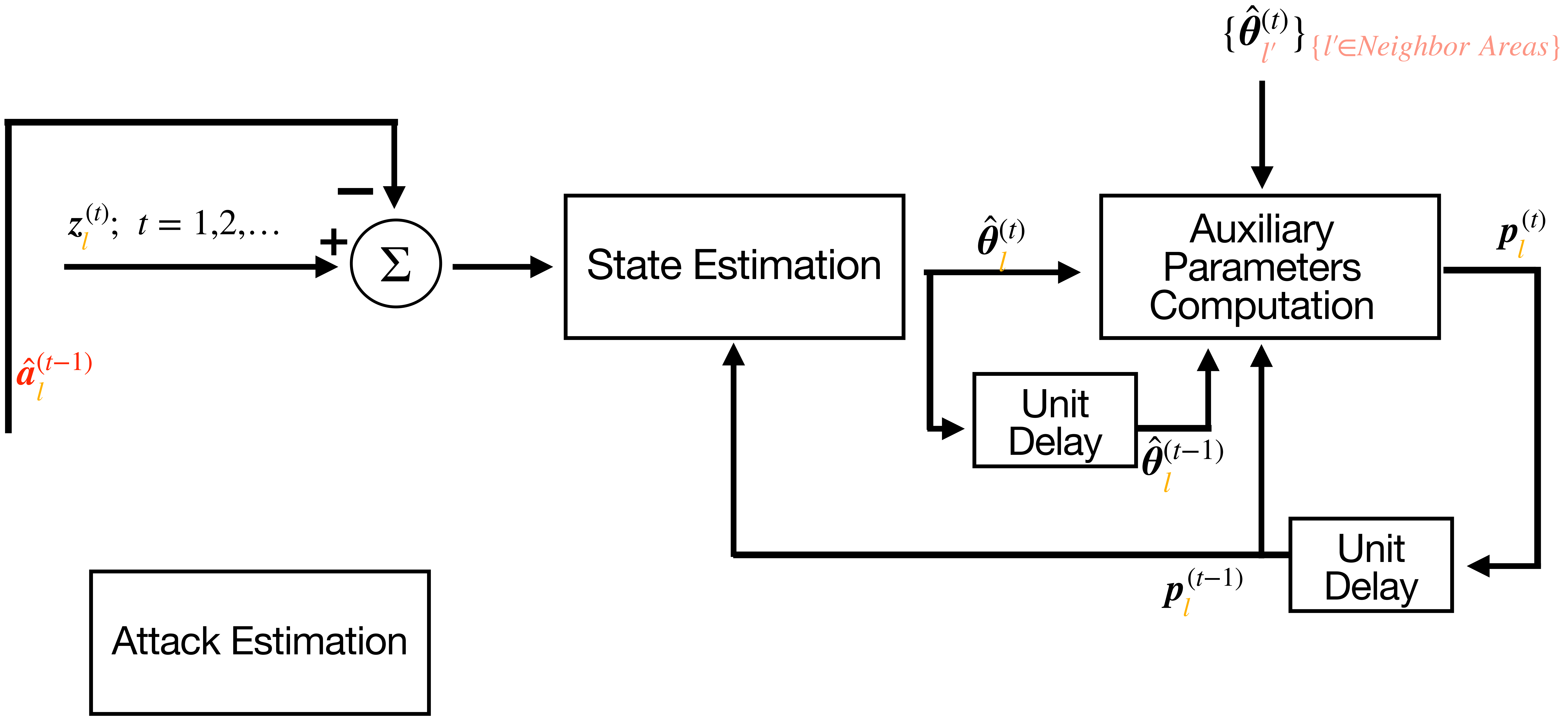
* Explained for the Attack hypothesis

Attack and State Estimation



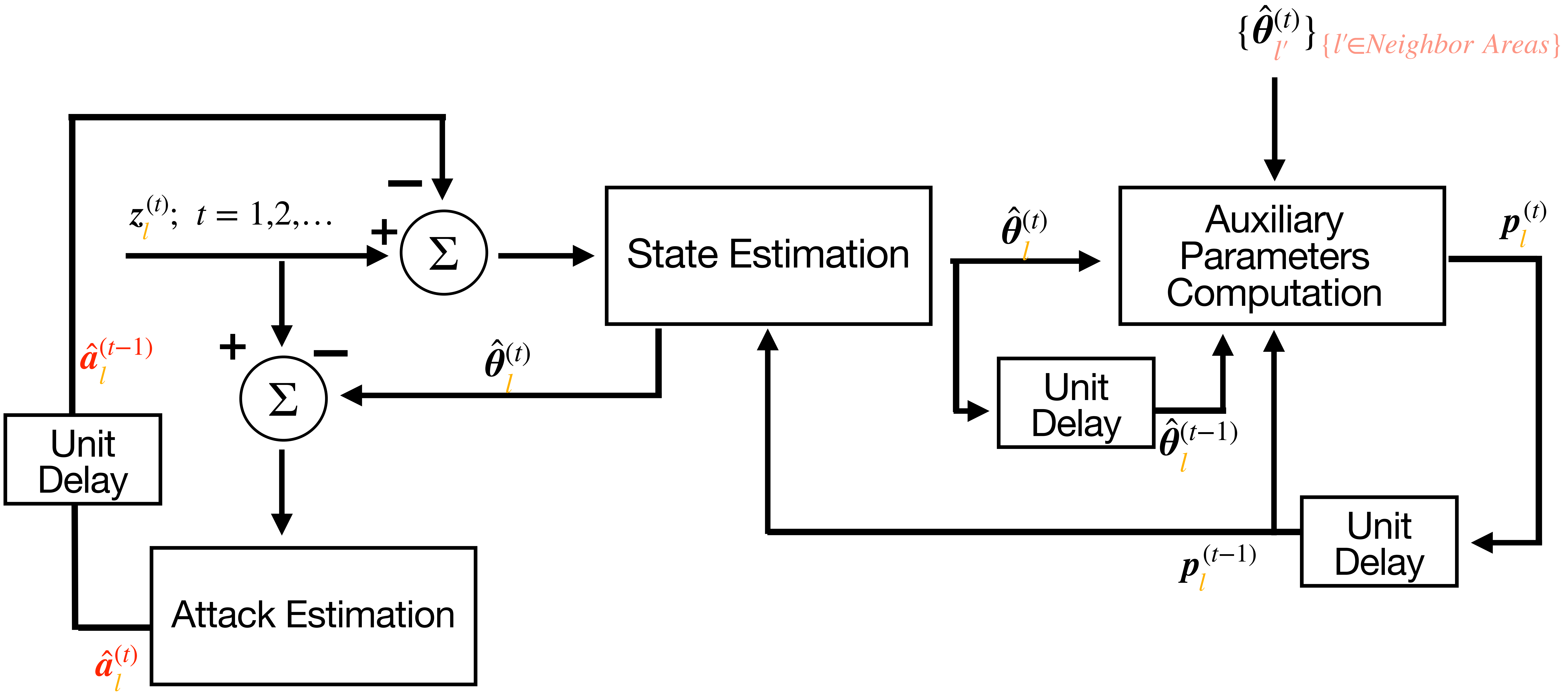
* Explained for the Attack hypothesis

Attack and State Estimation



* Explained for the Attack hypothesis

Attack and State Estimation



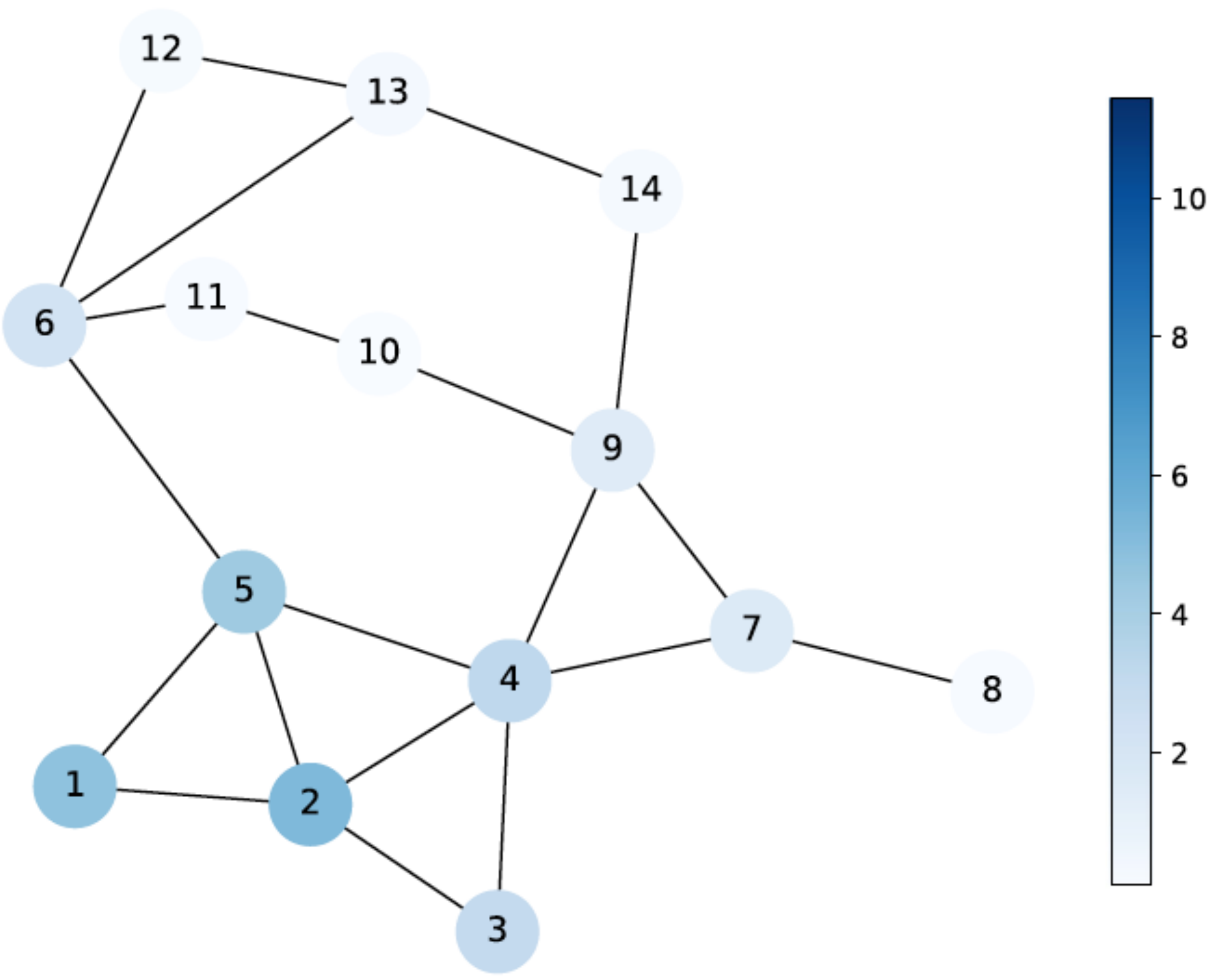
* Explained for the Attack hypothesis

Outline

- Introduction
- Background
- Theory: Secured Sensors and Graph Smoothness based Detection for False Data Injection Attacks
- Theory: Modification for Distributed Optimization
- **Theory: Generalization From Smooth Graph Signals to Low-Pass Graph Signals**
- Performance Evaluation

Power System States are Low Pass Graph Signals

The difference between the signal state values in neighbor vertices is assumed small



State Signal

Each vertex is assigned with a value represented by its color

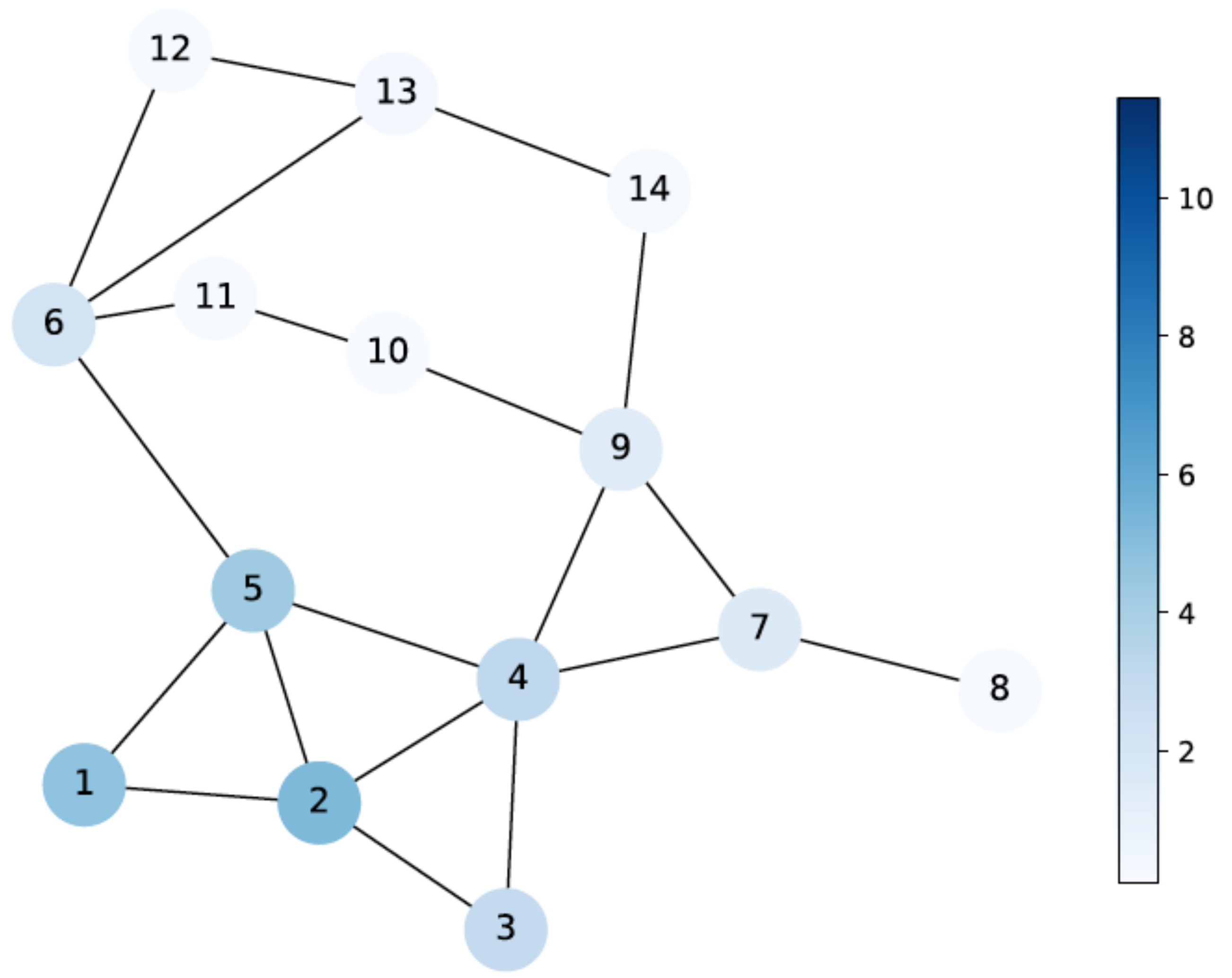
Drayer, Elisabeth, and Tirza Routtenberg. "Detection of false data injection attacks in smart grids based on graph signal processing." *IEEE Systems Journal* 14.2 (2019): 1886-1896.

Power System States are Low Pass Graph Signals

The difference between the signal state values in neighbor vertices is assumed small

↓

Hence, the signal variation over the graph is smooth



State Signal

Each vertex is assigned with a value represented by its color

Drayer, Elisabeth, and Tirza Routtenberg. "Detection of false data injection attacks in smart grids based on graph signal processing." *IEEE Systems Journal* 14.2 (2019): 1886-1896.

Power System States are Low Pass Graph Signals

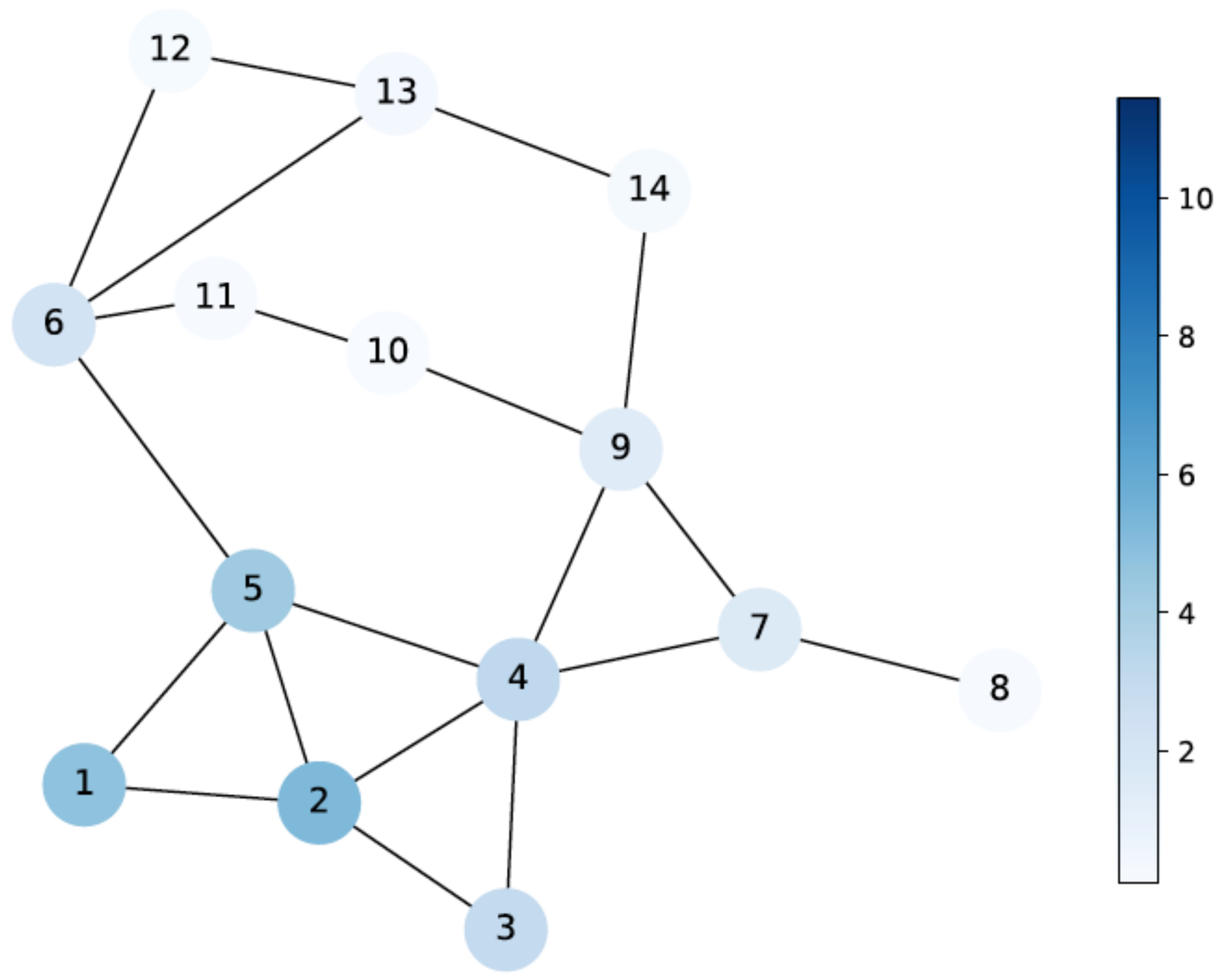
The difference between the signal state values in neighbor vertices is assumed small

↓

Hence, the signal variation over the graph is smooth

↓

The signals are assumed to be low pass graph signals

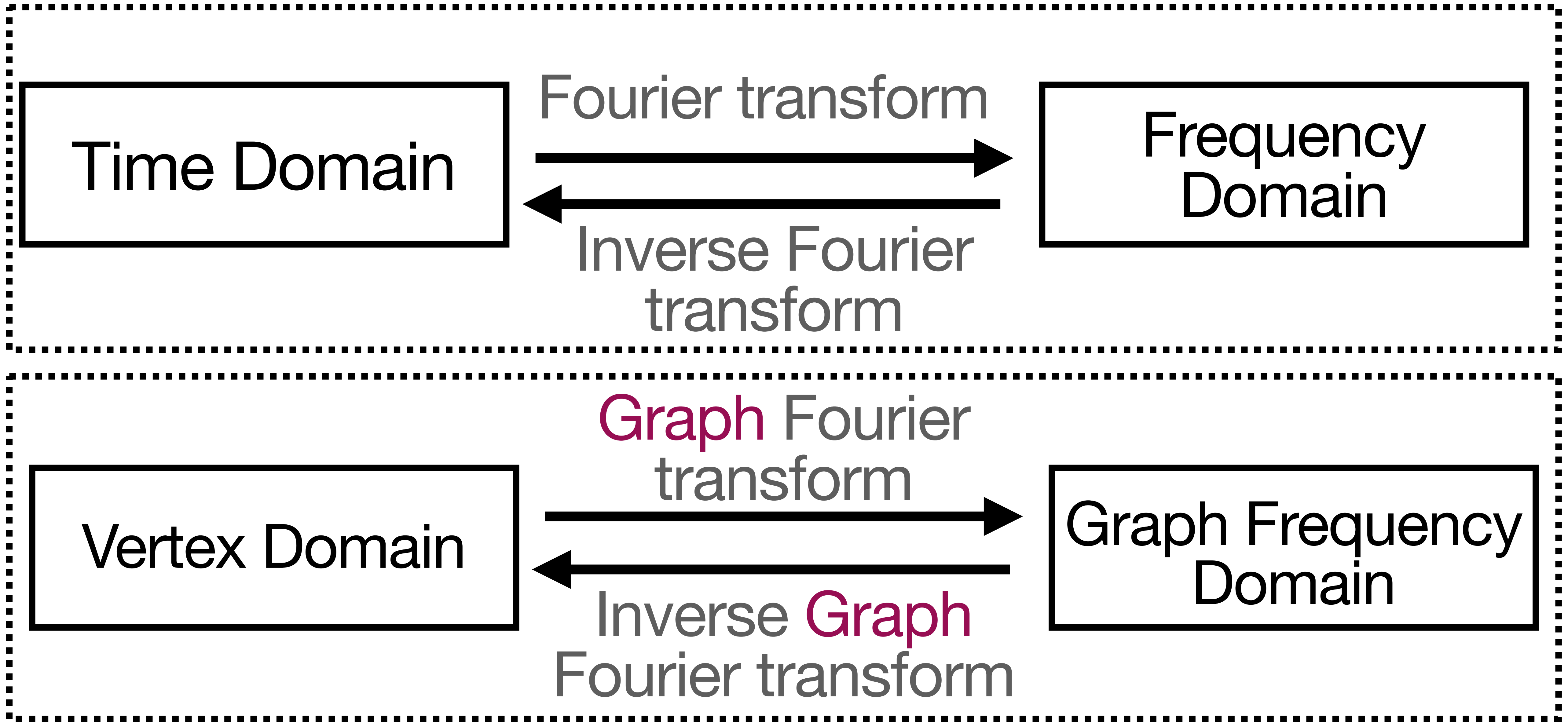


State Signal

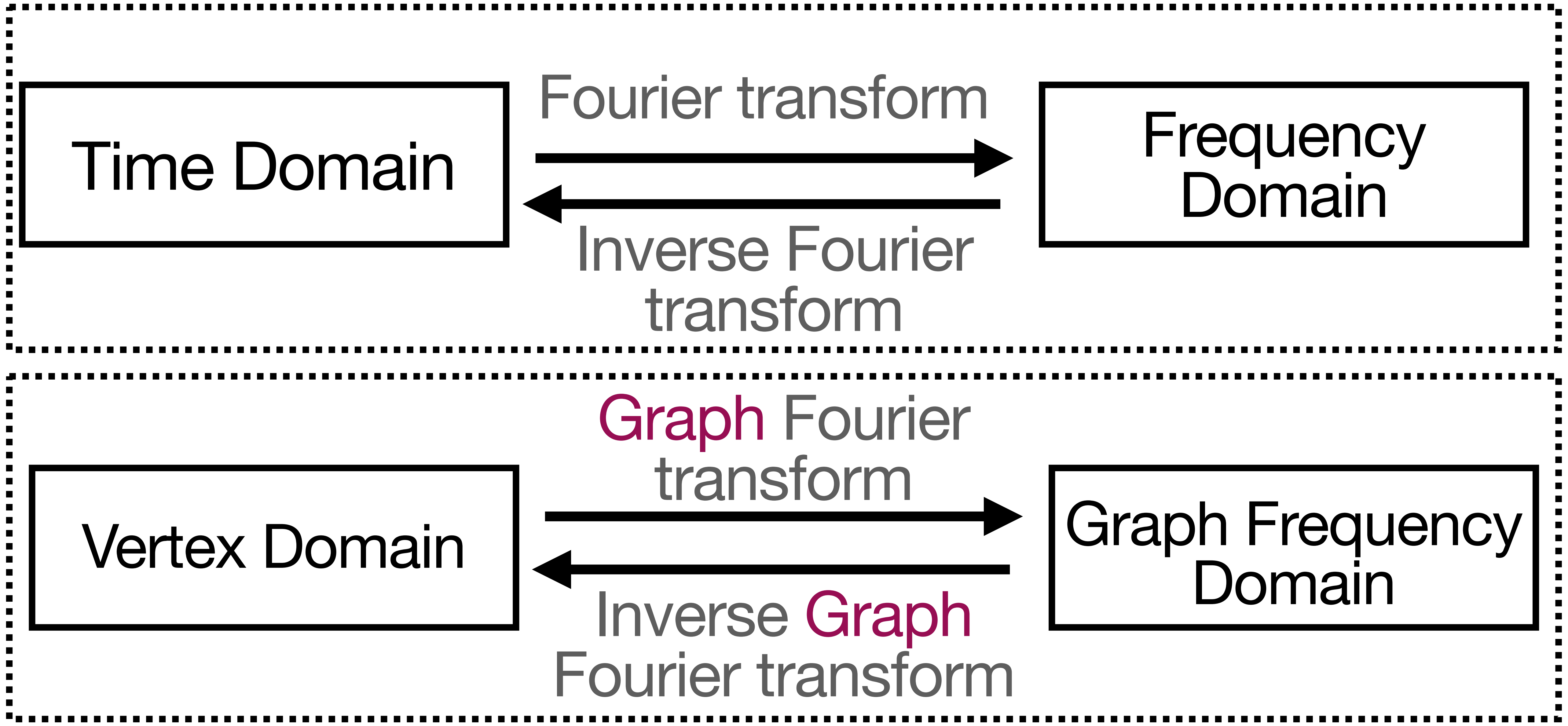
Each vertex is assigned with a value represented by its color

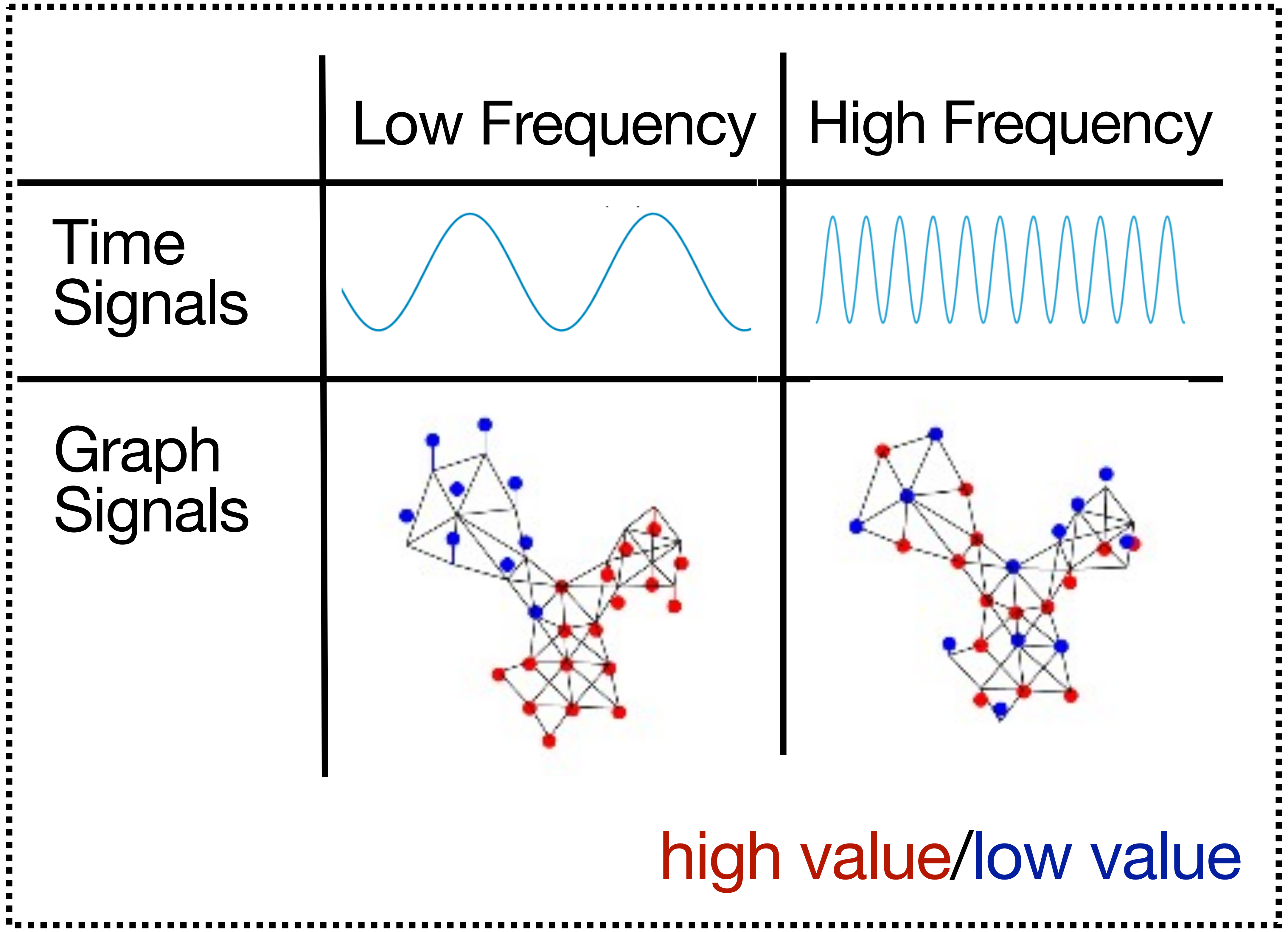
Drayer, Elisabeth, and Tirza Routtenberg. "Detection of false data injection attacks in smart grids based on graph signal processing." *IEEE Systems Journal* 14.2 (2019): 1886-1896.

Power System States are Low Pass Graph Signals



Power System States are Low Pass Graph Signals





Power System States are Low Pass Graph Signals

Low graph total variation

$$\sum_{v \in \mathcal{V}} \sum_{u \in \mathcal{N}_v} w_{v,u}(\theta_u - \theta_v)^2 \leq \epsilon_2$$

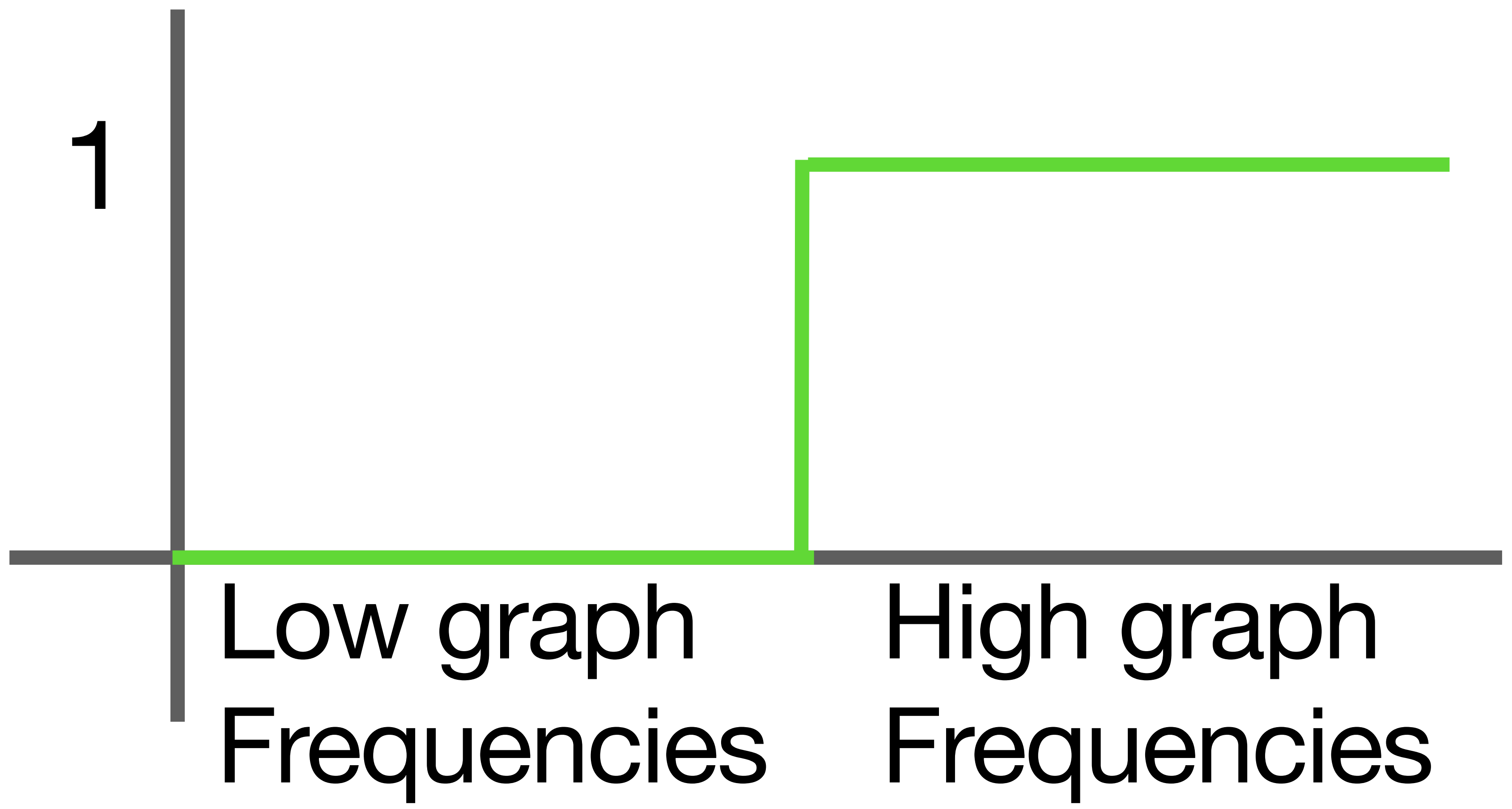
→

Low energy in high graph frequencies

$$||\boldsymbol{F\theta}||_2^2 \leq \epsilon_2$$

$\boldsymbol{F}$ - graph high pass filter

Ideal Graph High Pass Filter ($\boldsymbol{F}$)



Power System States are Low Pass Graph Signals

Low graph total variation

$$\sum_{v \in \mathscr{V}} \sum_{u \in \mathscr{N}_v} w_{v,u}(\theta_u - \theta_v)^2 \leq \epsilon_2$$

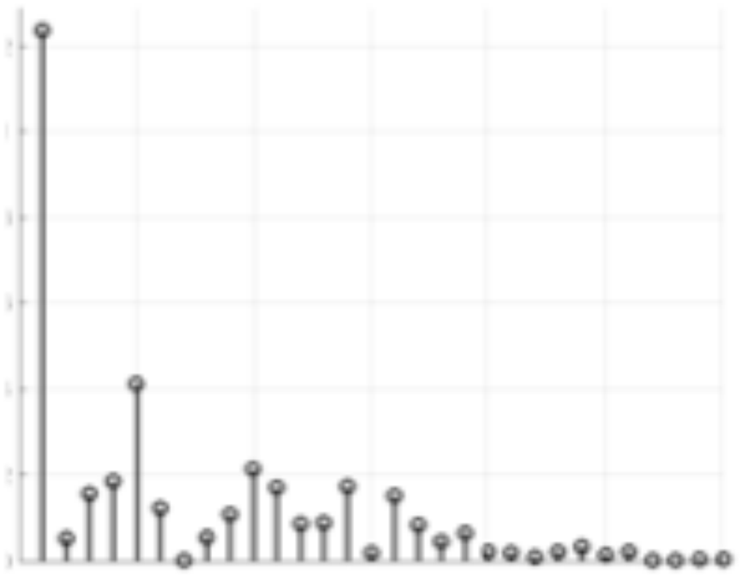
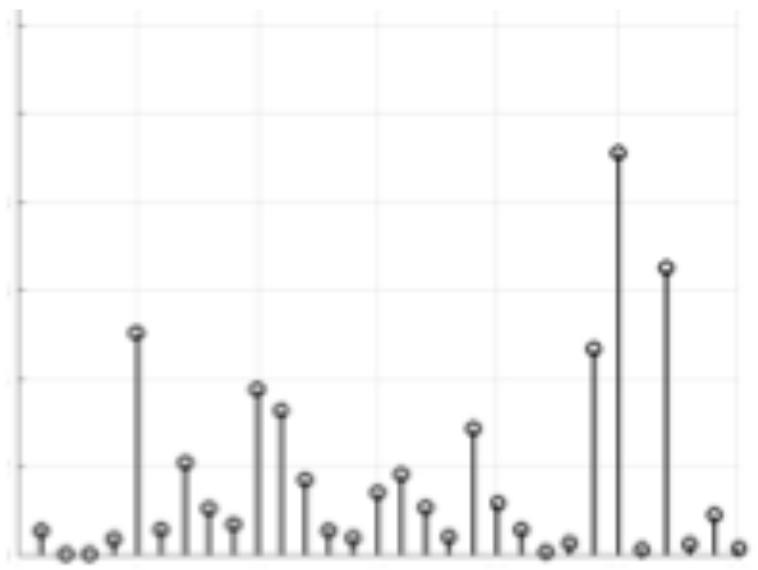
→

Low energy in high graph frequencies

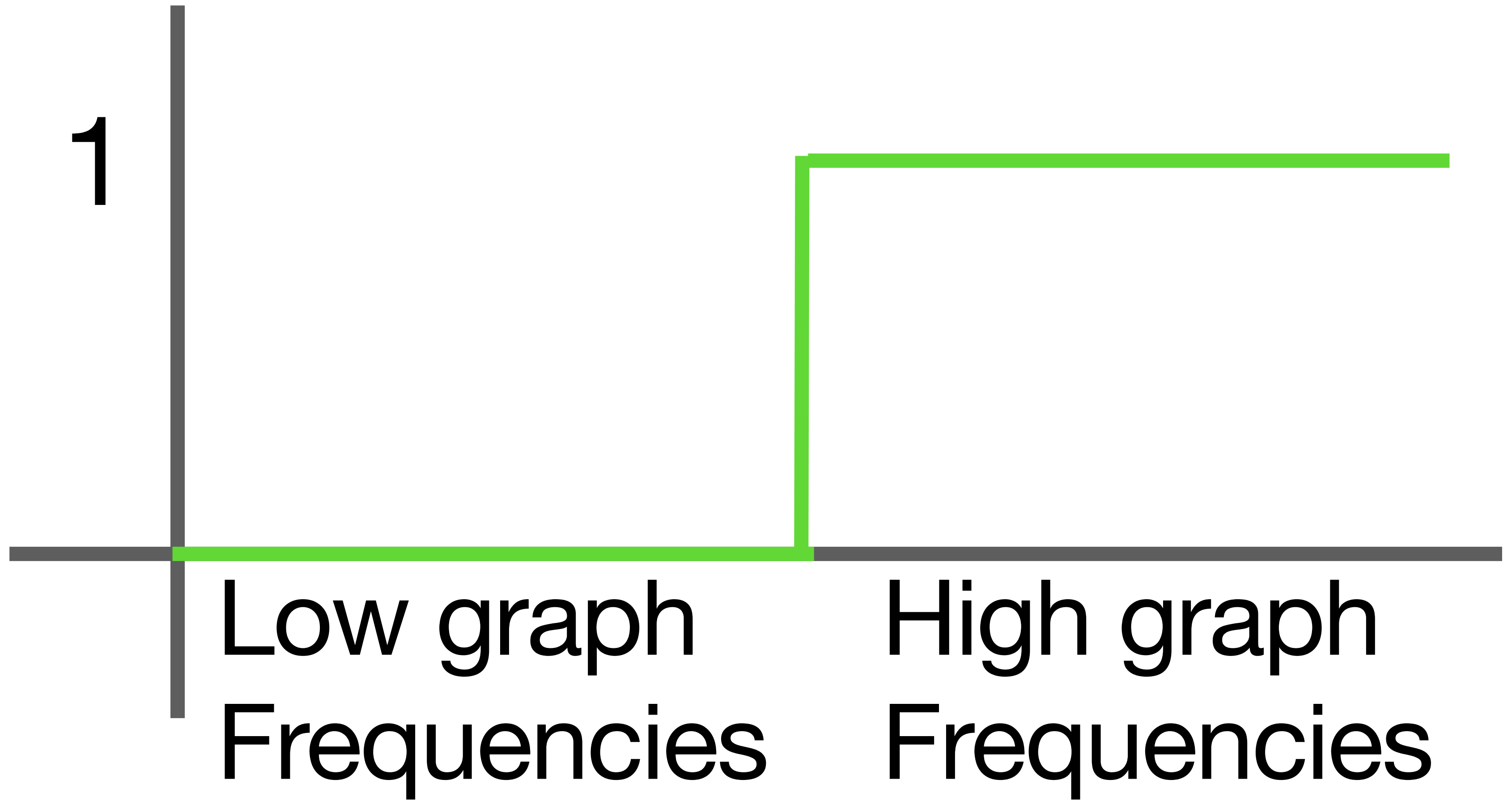
$$||\boldsymbol{F\theta}||_2^2 \leq \epsilon_2$$

$\boldsymbol{F}$ - graph high pass filter

Example

state signal (low pass)	attack signal
 Graph frequency domain (absolute value)	 Graph frequency domain (absolute value)

Ideal Graph High Pass Filter ($\boldsymbol{F}$)



Outline

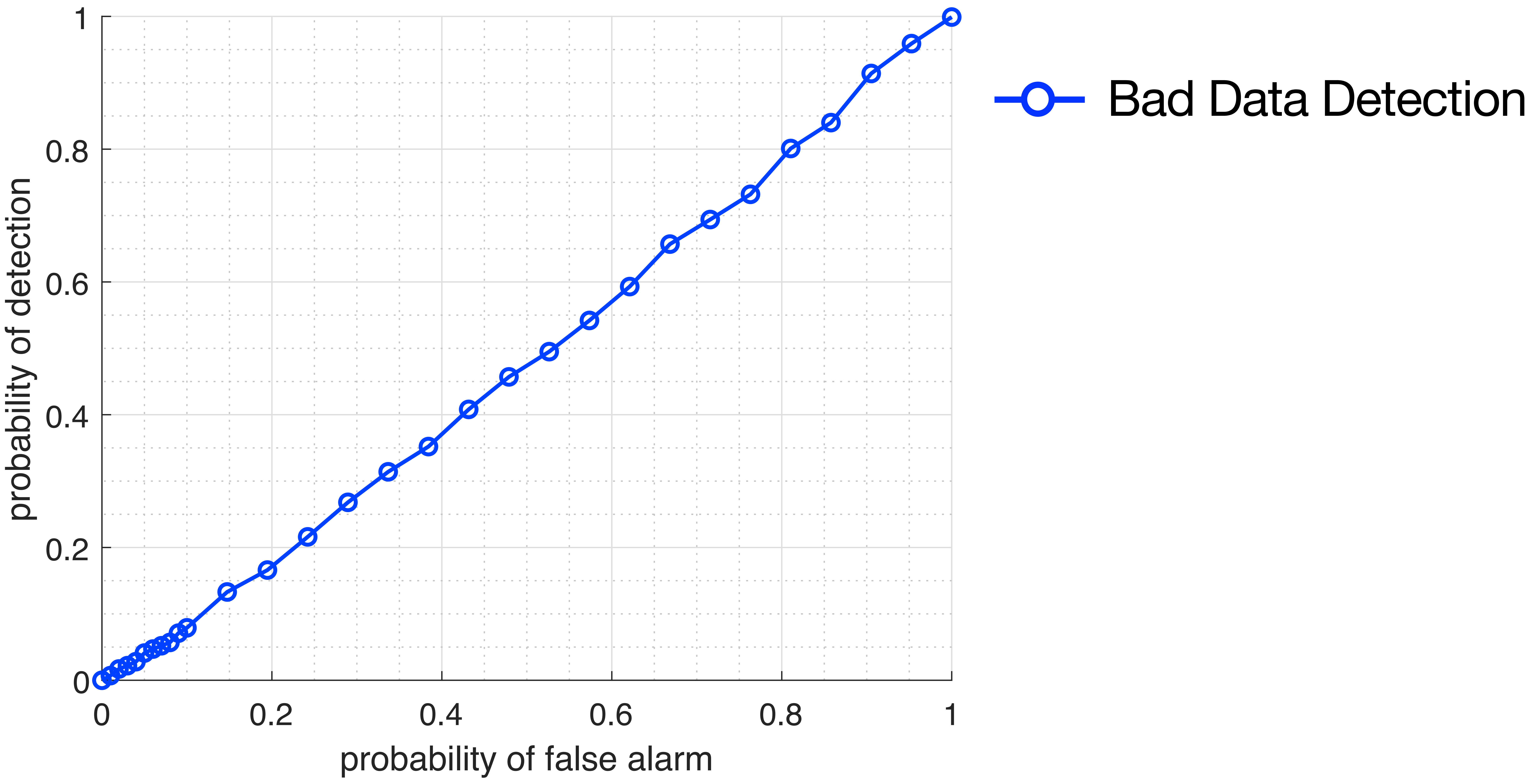
- Introduction
- Background
- Theory: Secured Sensors and Graph Smoothness Based Detection for False Data Injection Attacks
- Theory: Modification for Distributed Optimization
- Theory: Generalization From Smooth Graph Signals to Low-Pass Graph Signals
- **Performance Evaluation**

Performance Evaluation

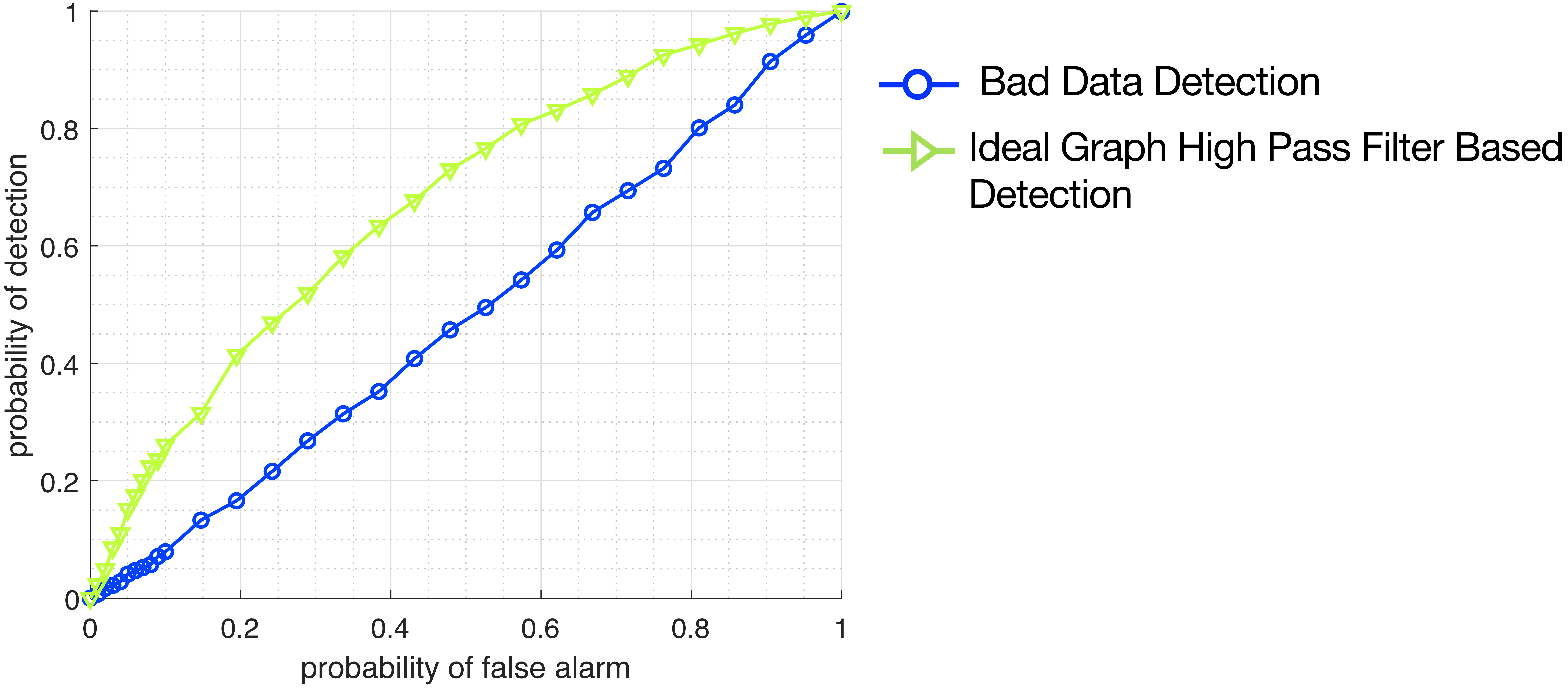
Set up

- IEEE-57 power system test case
- Attack on a single node (33)
- 36% of the measurements are secured
  - Ensuring the state variables in the generator substations cannot be manipulated

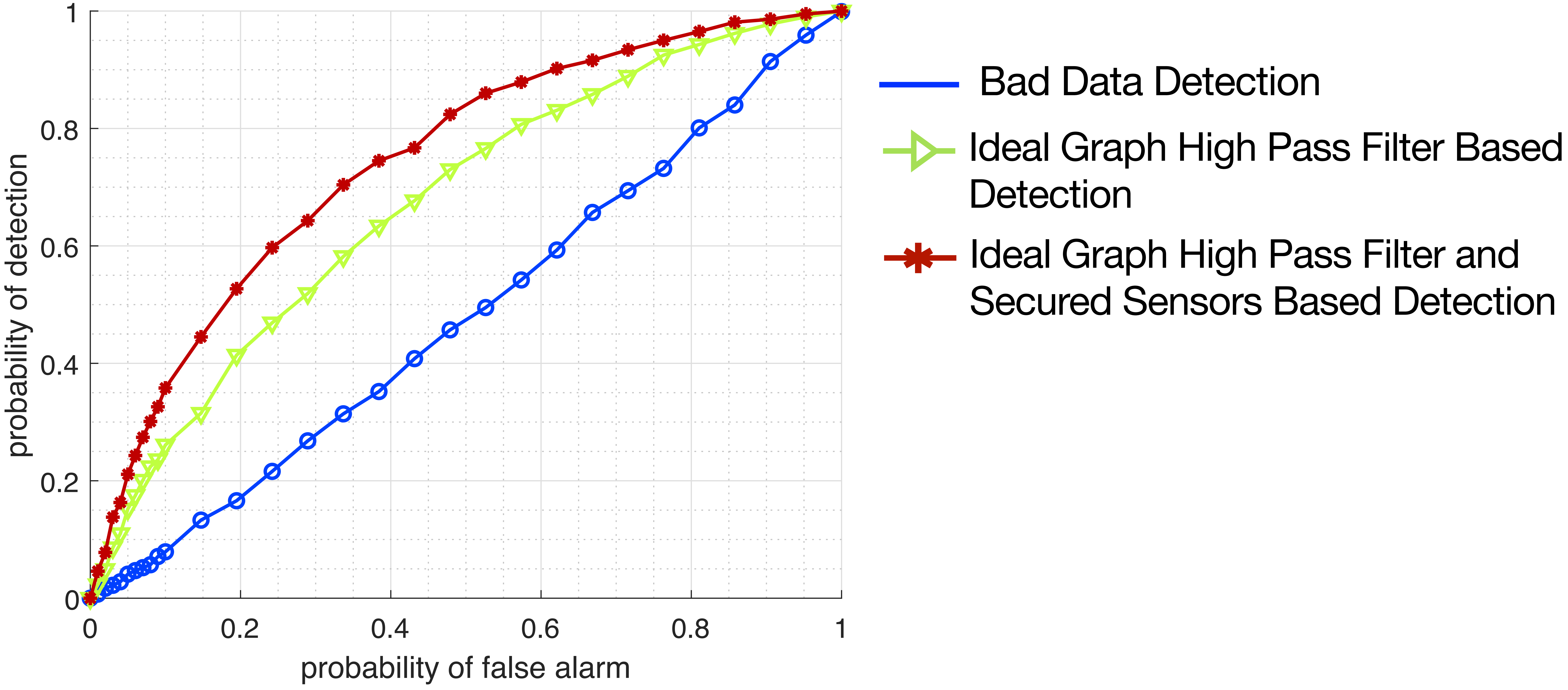
Receiver Operating Characteristics (ROC)



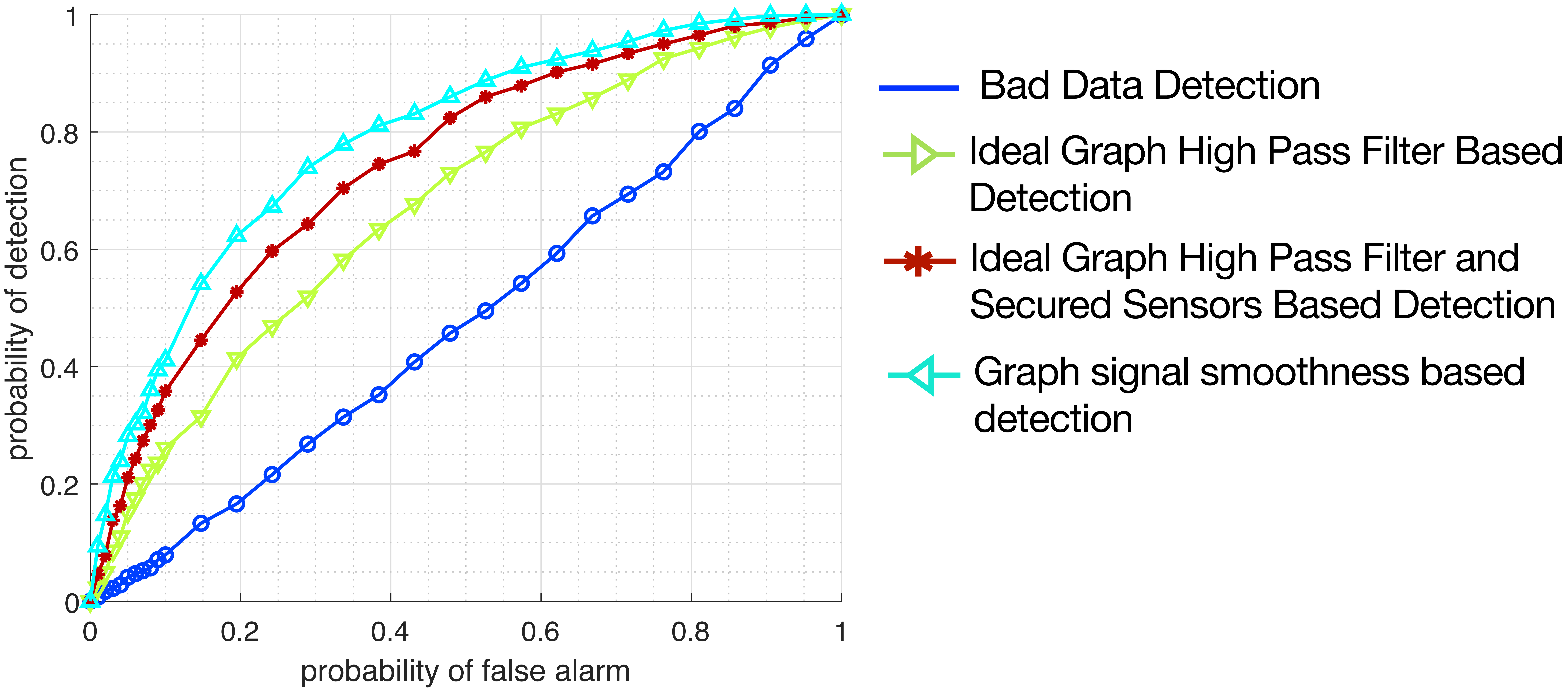
Receiver Operating Characteristics (ROC)



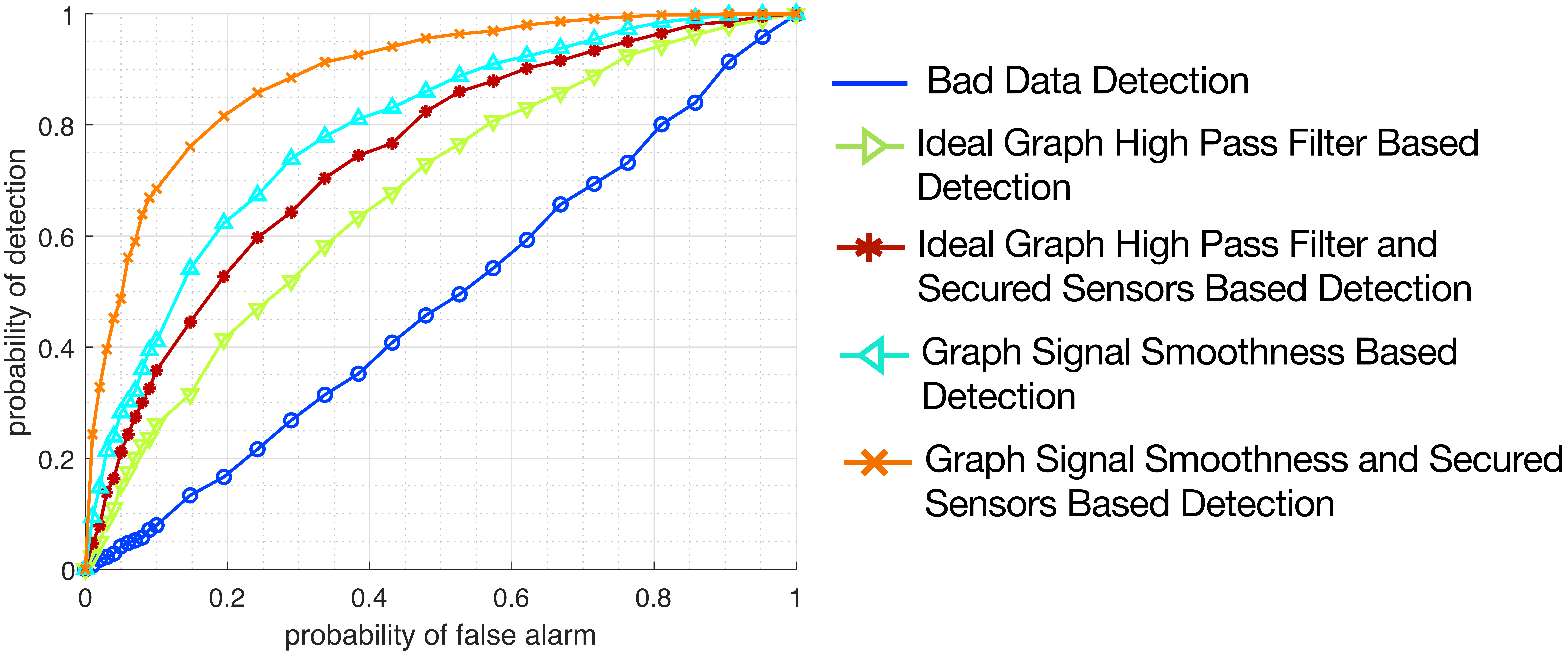
Receiver Operating Characteristics (ROC)



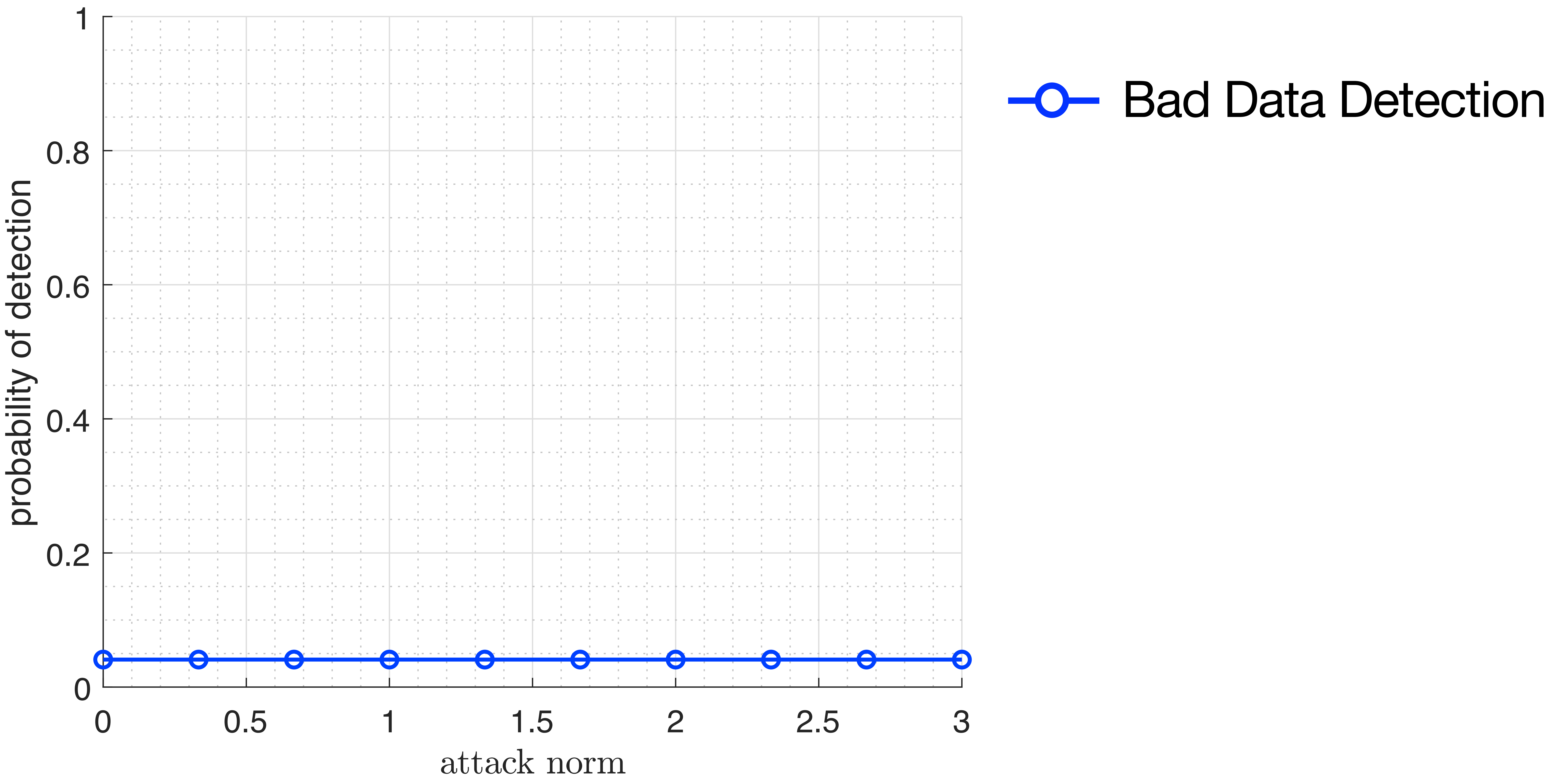
Receiver Operating Characteristics (ROC)



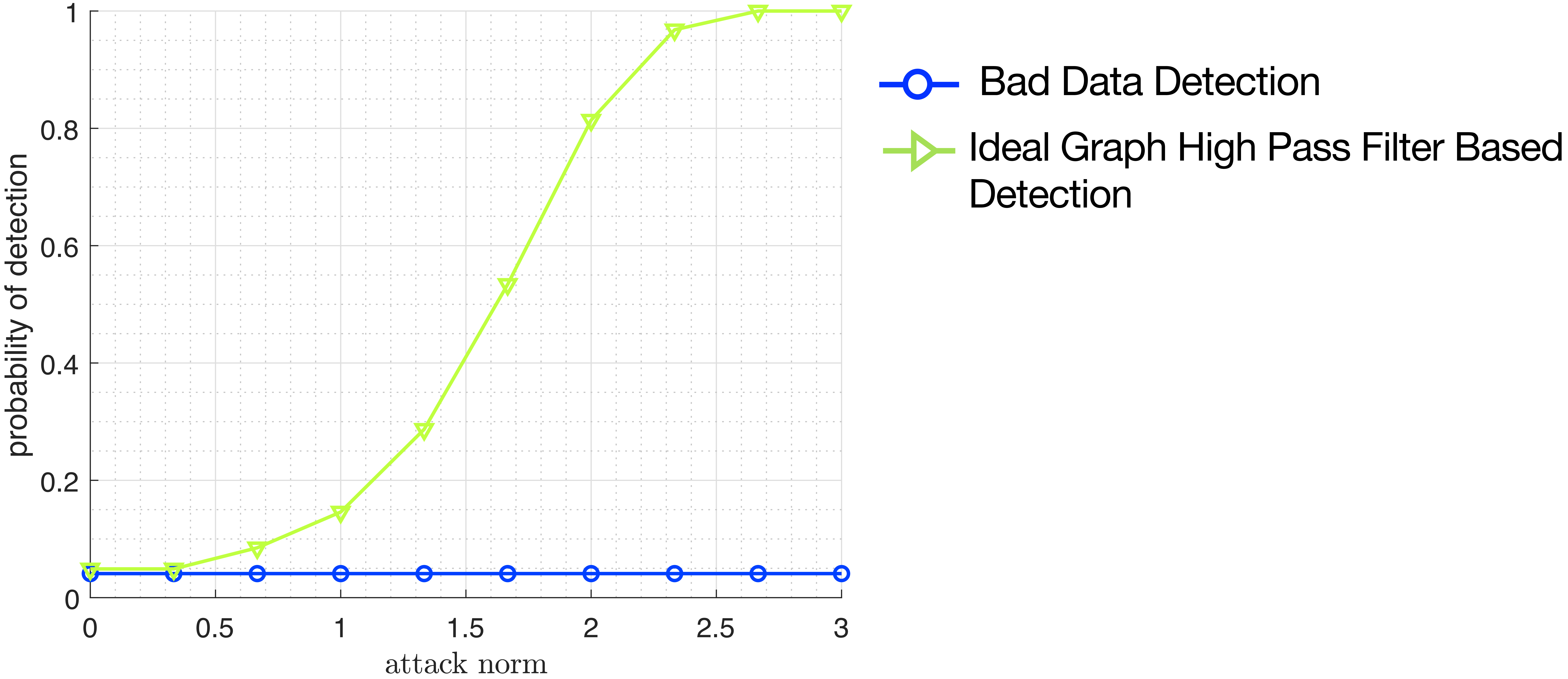
Receiver Operating Characteristics (ROC)



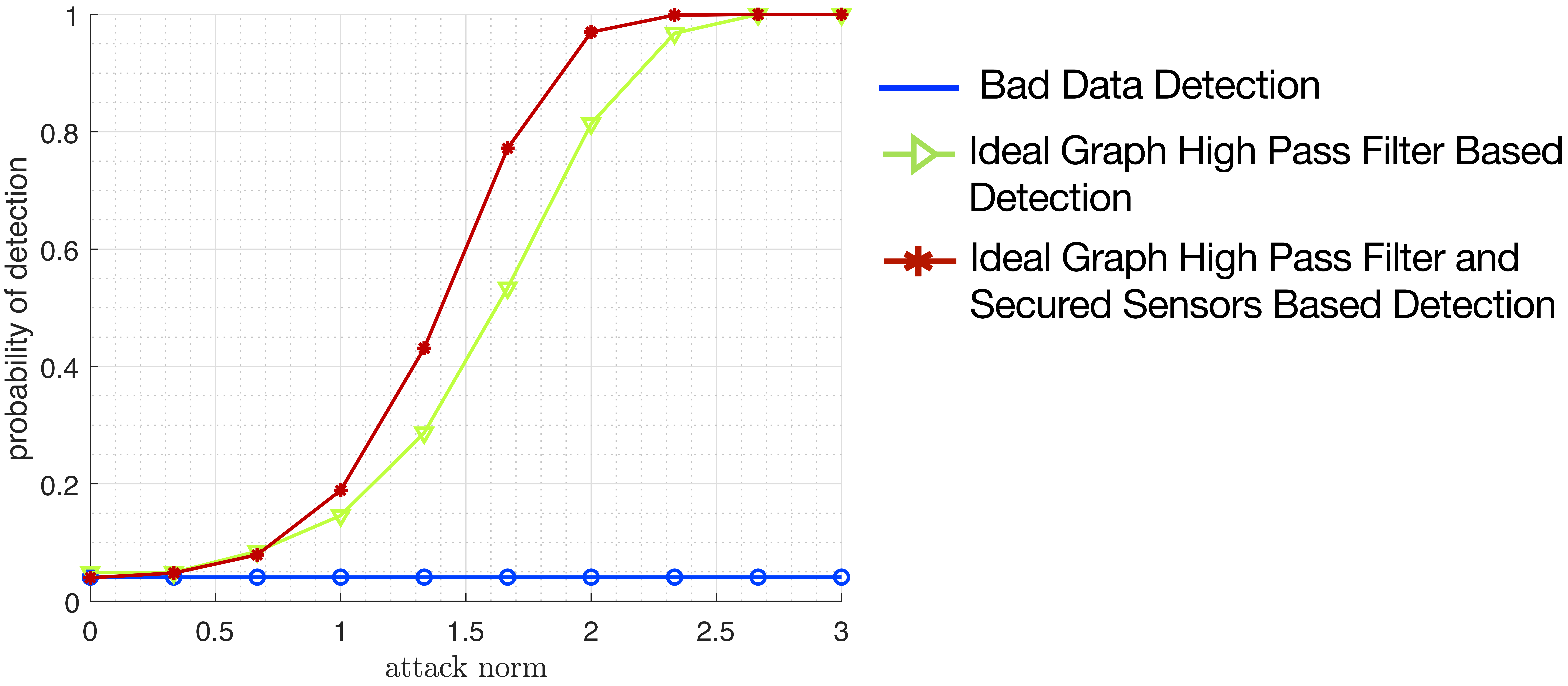
Probability of Detection Verse Attack Norm



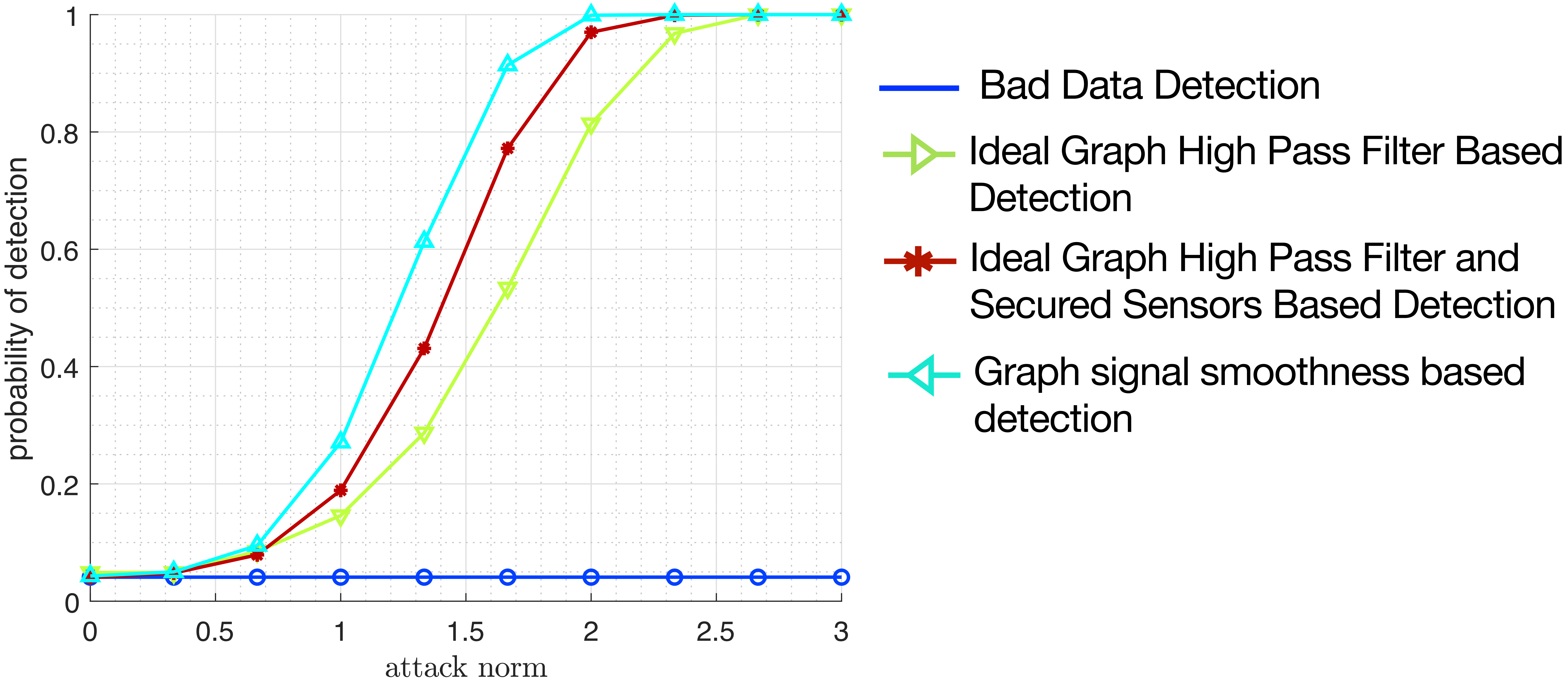
Probability of Detection Verse Attack Norm



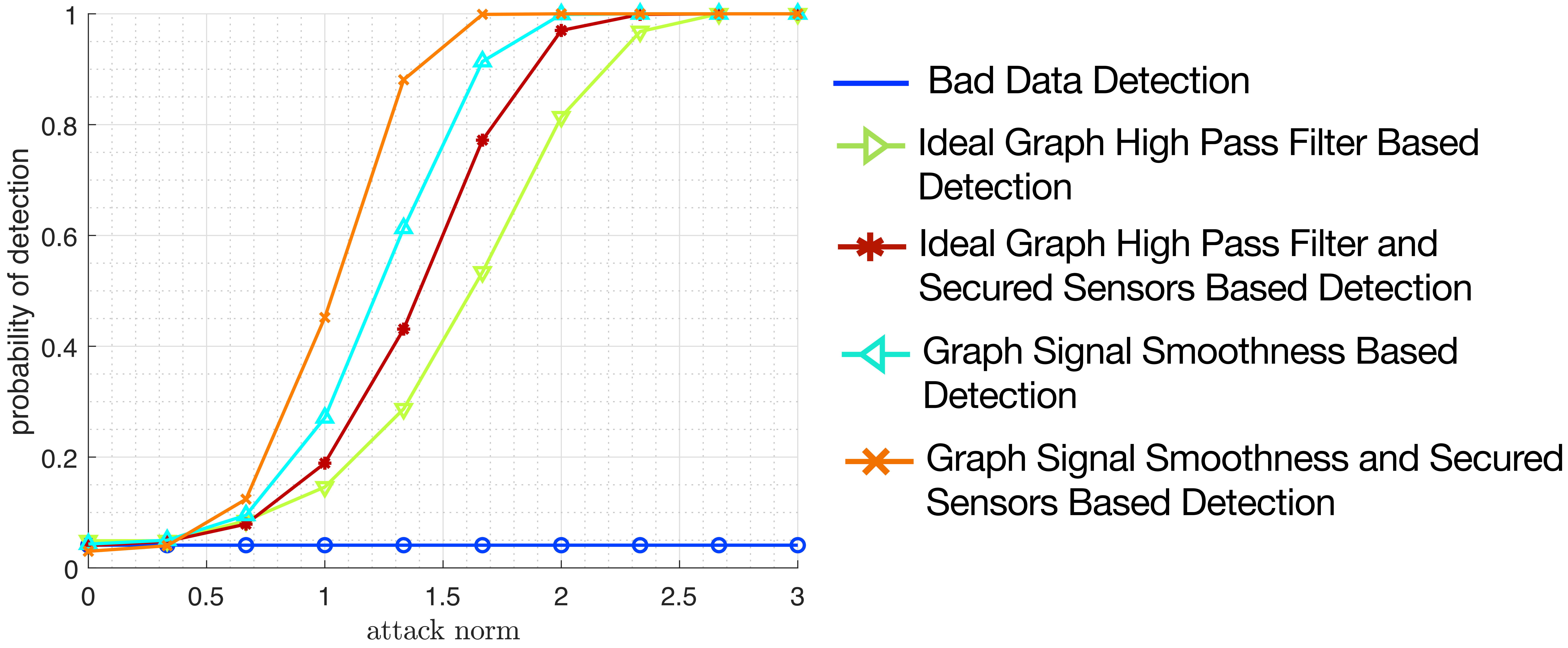
Probability of Detection Verse Attack Norm



Probability of Detection Verse Attack Norm



Probability of Detection Verse Attack Norm



Summary

- Introduced two regularization factors for power system state estimation under false data injection attacks
    1. Graph-based regularization on the system states
    2. Secured sensors-based regularization on the attack
- Provided a detection method against false data injection attacks
- Provided a modification of the detection method to distributed optimization

Israel Ministry of Science, Technology and Space
NGI
Ministry of National infrastructure, Energy and Water Resources
www.energy.gov.il
NSF
NRF National Research Foundation of Korea
School of Sustainability and Climate Change
U.S. DEPARTMENT OF ENERGY

Gal Morgenstern
galmo@post.bgu.ac.il

IEEE-57 Power System Test Case