Meng-zhou GAO, Dong-qin FENG, 2018. Stochastic stability analysis of networked control systems with random cryptographic protection under random zero-measurement attacks. *Frontiers of Information Technology & Electronic Engineering*, 19(9):1098-1111.
https://doi.org/10.1631/FITEE.1700334

Stochastic stability analysis of networked control systems with random cryptographic protection under random zero-measurement attacks

Key words: Networked control systems; Security; Cyber attacks; Stochastic stability; Cryptographic protection

Corresponding author: Dong-qin Feng
E-mail: dongqinfeng@zju.edu.cn

Motivations

1. Cyber attacks can be understood as intermittent or random implementations because of the dependence of the network circumstances and attackers' limited resources.

2. To protect the integrity and confidentiality, cryptographic protection can be applied to refuse stealthy attacks.

3. Cryptographic protection requires extra computational overhead, time, and energy consumption, which often makes security objectives conflict with real-time dynamic performance.

4. Therefore, random attacks are considered and random cryptographic protection is used to decrease the number of implementations and reduce implementation costs.

Main idea

1. In random cryptographic protection, communicated measurements are stochastically protected at every sampling instant.

2. For unencrypted signals, zero-measurement attacks are randomly launched, which are designed by changing all sampled measurement signals into zeros to spoof NCS with no need for external inputs.

3. According to stochastic stability analysis, the proper probability of random cryptographic protection for maintaining stability of NCS under random zero-measurement attacks of certain attack probabilities can be determined.

Main idea

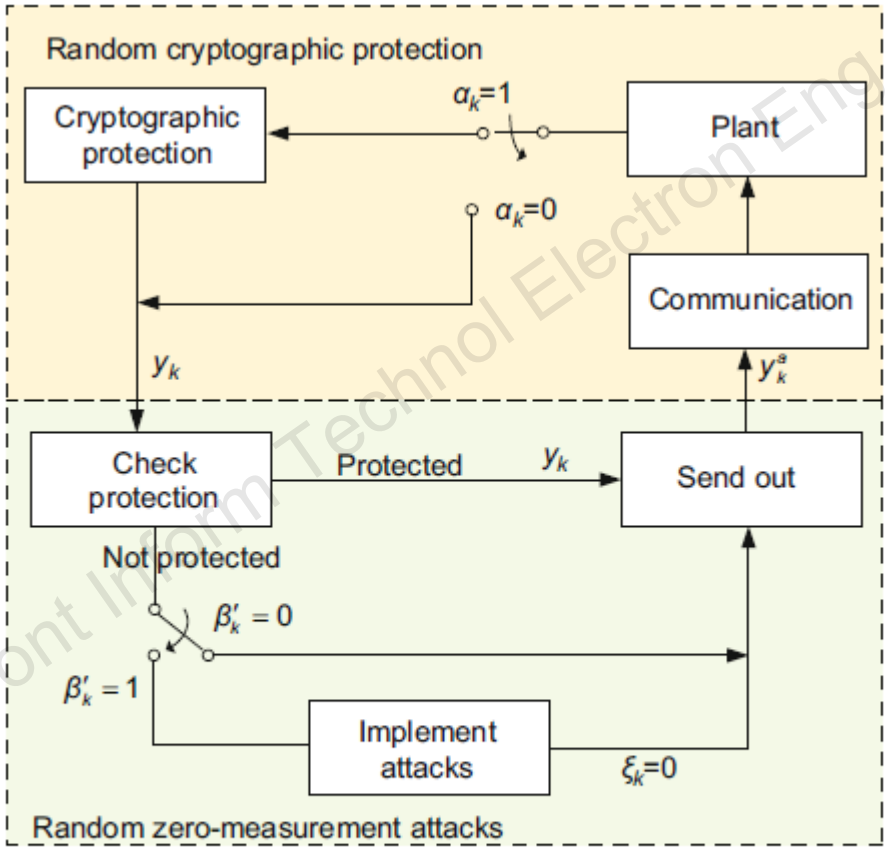

Fig. 1 The networked control system model under random zero-measurement attacks and random cryptographic protection

Methods

1. The random cryptographic protection and random zero-measurement attacks are implemented following two correlated Bernoulli stochastic variables.

2. For the system with random cryptographic protection under random zero-measurement attacks, the definition of stochastic stability is provided following Xu et al. (2004).

3. Sufficient conditions for the stochastic stability analysis were proposed and mathematically demonstrated by an LMI method.

Major results

1. Random zero-measurement attacks can destroy the stability of the system.

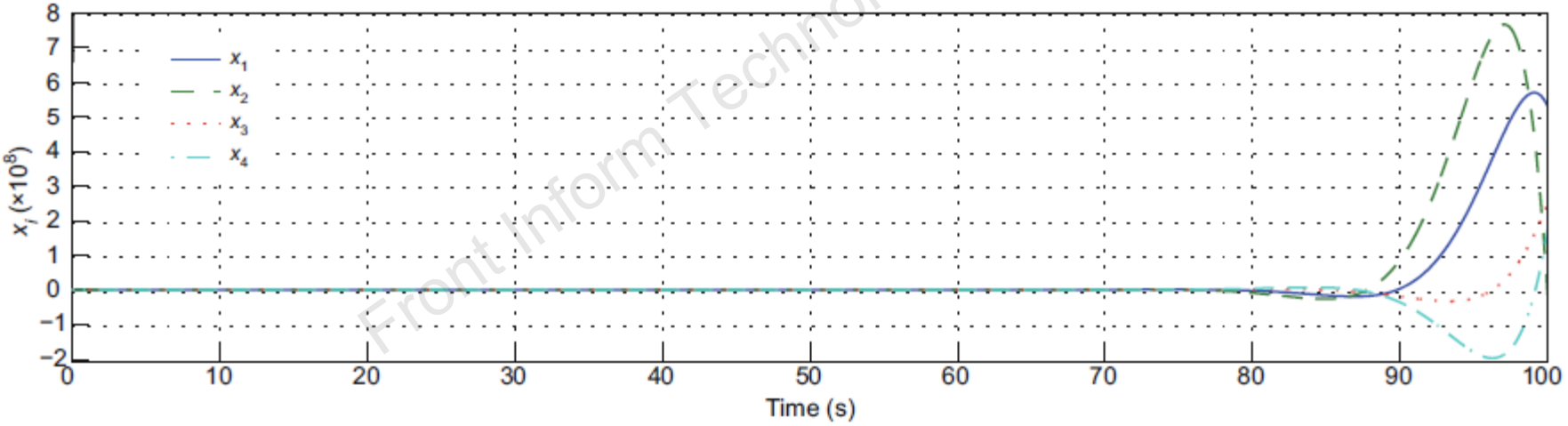

Fig. 3 Trajectories of system states without random cryptographic protection under random zero-measurement attacks of probability $\bar{\beta} = 1$

Major results

2. Random cryptographic protection can help the system maintain stochastic stability under random zero-measurement attacks.

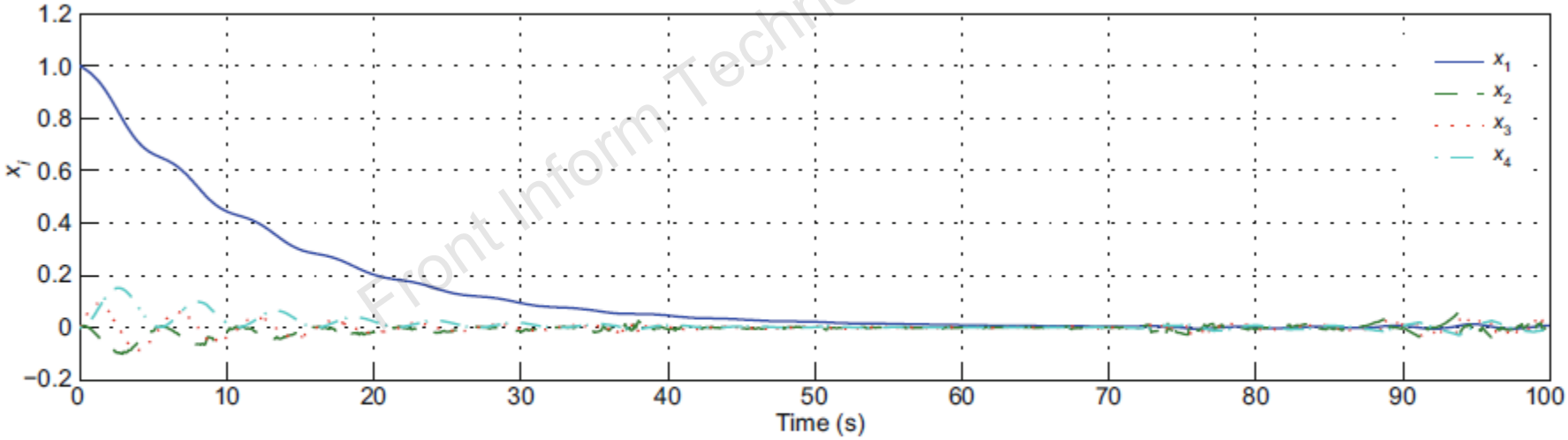

Fig. 4 Trajectories of system states with random cryptographic protection of probability $\bar{\alpha} = 0.279$ under random zero-measurement attacks of probability $\bar{\beta} = 1$

Major results

3. The random protection has some robustness in the presence of measurement noise.

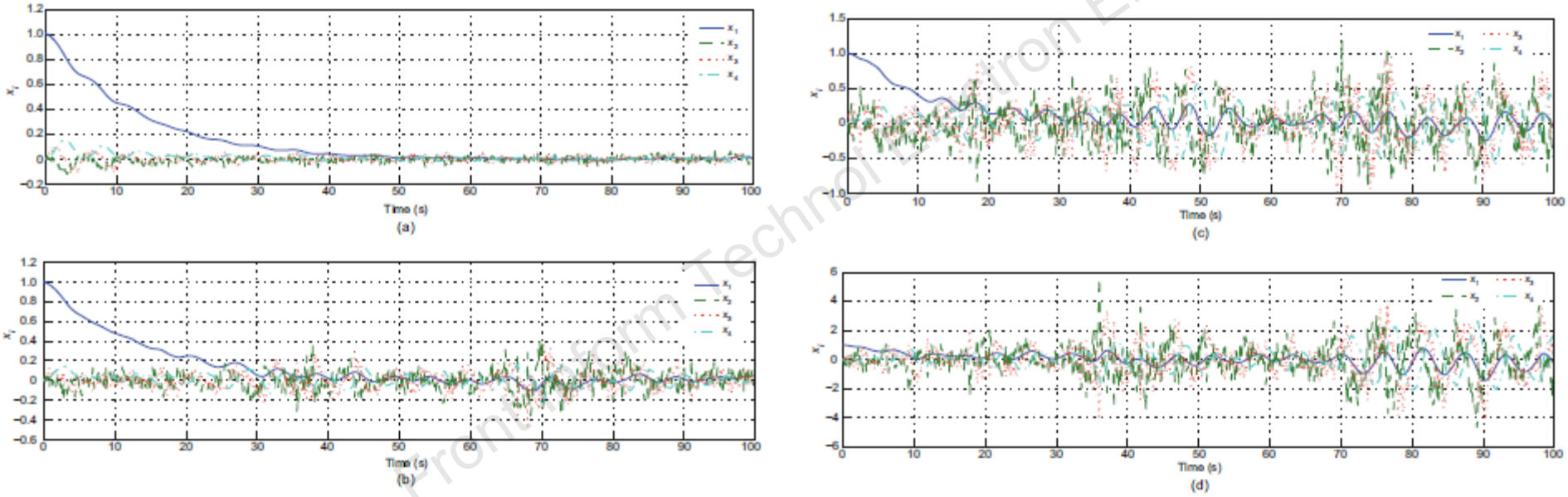

Fig. 5 Robustness of random cryptographic protection when measurement noises are $\omega \sim \mathcal{N}(0, 0.001)$ (a), $\omega \sim \mathcal{N}(0, 0.01)$ (b), $\omega \sim \mathcal{N}(0, 0.1)$ (c), and $\omega \sim \mathcal{N}(0, 1)$ (d)

Major results

4. The performance of random cryptographic protection for stability maintenance under different delays is studied based on simulations.

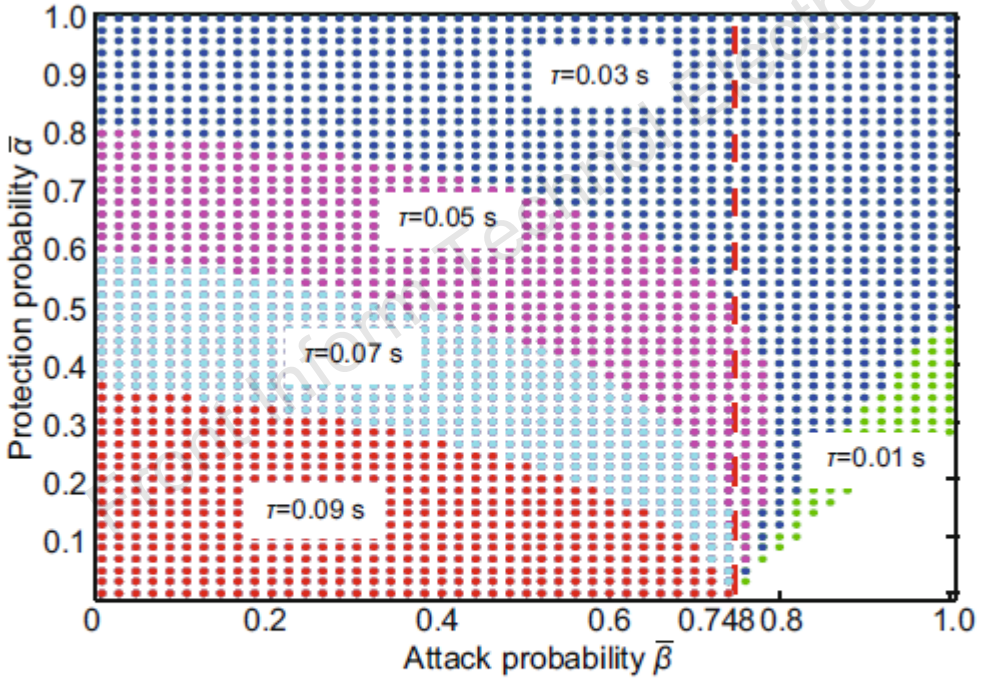

Fig. 6 Stability analysis of the networked control system with random zero-measurement attacks and random cryptographic protection for various protection delays τ

Major results

5. The performance of random cryptographic protection for stability maintenance under different sampling periods is studied based on simulations.

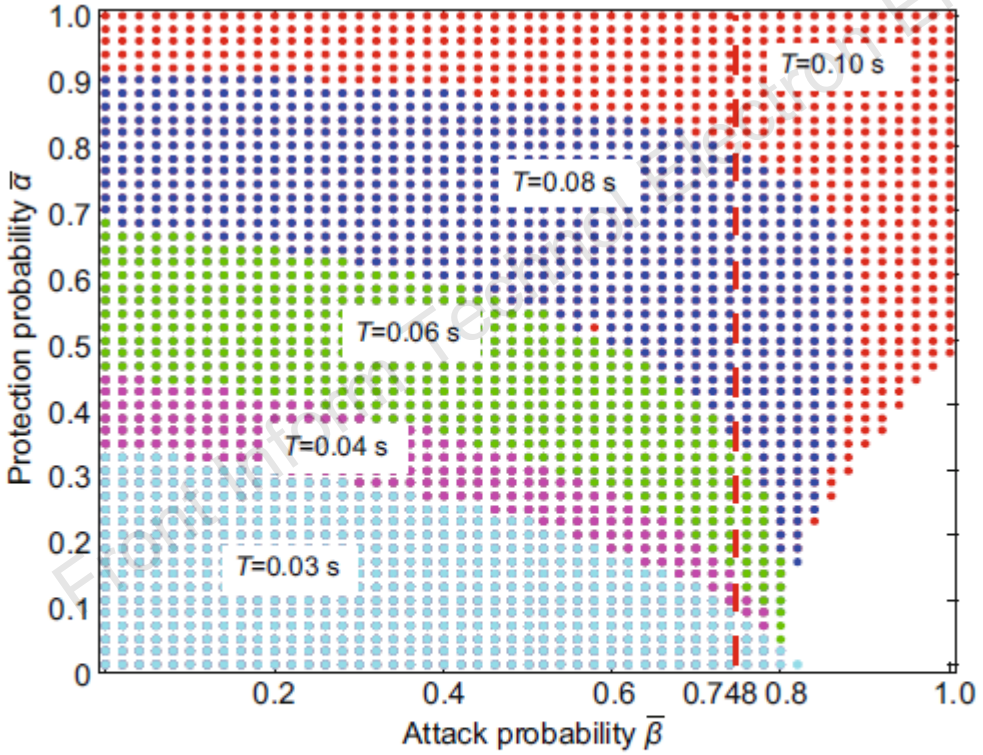

Fig. 7 Stability analysis of the networked control system with random zero-measurement attacks and random cryptographic protection for various sampling periods T

Conclusions

1. Random cryptographic protection can maintain the stability of NCS under random zero-measurement attacks.

2. The proper probability of random cryptographic protection can be determined by solving LMI based on the proposed theorem.

3. The simulation results proved the robustness of the proposed method against measurement noise.

4. The simulation results showed that the system sampling period and cryptographic delay have some effects on the stability analysis.