# Article information:

Resilient LFC design of power system with delay and DoS attacks | IEEE Conference Publication | IEEE Xplore  
<https://ieeexplore.ieee.org/document/9550460>

# Article summary:

1. The study focuses on resilient Load frequency control (LFC) design of a single area power system with communication delay and DoS attacks.

2. A switched delay system is established to describe the frequency dynamic of power system under DoS attack, and a resilient criterion of exponential stability is given by employing Lyapunov functional and switched system theory.

3. Resilient output feedback control gain is designed by linear matrix inequalities (LMIs), and numerical simulations are carried out to verify the theory.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article discusses the resilient Load frequency control (LFC) design of a single area power system with communication delay and DoS attacks. The study highlights the vulnerability of power systems to network attacks and proposes a resilient control method to counteract these attacks. The article provides a detailed analysis of the LFC system under nonperiodic DoS attacks, and a switched delay system is established to describe the frequency dynamic of the power system.

The article presents several contributions, including proposing a secure design method for additional control in LFC systems, designing static output feedback control law, and analyzing the resilience of LFC systems under DoS attacks. However, there are some potential biases in the article that need to be considered.

One-sided reporting is evident in this article as it only focuses on the resilience of LFC systems under DoS attacks. It does not consider other types of cyber-attacks that could affect power systems. This narrow focus may lead readers to believe that DoS attacks are the only threat to power systems.

The article also lacks evidence for some claims made. For instance, it assumes that energy-limited DoS attack interrupting addition control channel is constrained by its frequency and duration without providing any supporting evidence or data.

Furthermore, unexplored counterarguments are missing from this article. For example, it does not discuss potential drawbacks or limitations of using additional control inputs as compensation for delay-dependent stability in LFC systems.

Promotional content is also present in this article as it promotes the proposed method without discussing possible risks or limitations associated with its implementation. Additionally, there is partiality in presenting both sides equally as only one approach is discussed without considering alternative methods for countering cyber-attacks on power systems.

In conclusion, while this article provides valuable insights into resilient LFC design under DoS attacks, it has some potential biases and limitations that need to be considered when interpreting its findings.

# Topics for further research:

* Cybersecurity threats to power systems beyond DoS attacks
* Limitations of using additional control inputs for delay-dependent stability in power systems
* Risks associated with implementing resilient control methods in power systems
* Alternative approaches for countering cyber-attacks on power systems
* Impact of communication delay on power system stability
* Frequency dynamics of power systems under nonperiodic attacks

# Report location:

<https://www.fullpicture.app/item/f90d7471082da4383bea4c845d5f920d>