

## Accepted Manuscript

Successive Direct Load Altering Attack in Smart Grid

Peng Xun, Pei-dong Zhu, Sabita Maharjan, Peng-shuai Cui

PII: S0167-4048(18)30255-4  
DOI: [10.1016/j.cose.2018.03.009](https://doi.org/10.1016/j.cose.2018.03.009)  
Reference: COSE 1315

To appear in: *Computers & Security*

Received date: 23 November 2017  
Revised date: 7 February 2018  
Accepted date: 20 March 2018

Please cite this article as: Peng Xun, Pei-dong Zhu, Sabita Maharjan, Peng-shuai Cui, Successive Direct Load Altering Attack in Smart Grid, *Computers & Security* (2018), doi: [10.1016/j.cose.2018.03.009](https://doi.org/10.1016/j.cose.2018.03.009)



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

## Successive Direct Load Altering Attack in Smart Grid

Peng Xun<sup>a</sup>, Pei-dong Zhu<sup>a,b</sup>, Sabita Maharjan<sup>c</sup>, Peng-shuai Cui<sup>a</sup>

<sup>a</sup> College of Computer, National University of Defense Technology, Changsha, China

<sup>b</sup> College of Math and Computer Science, Changsha University, Changsha, China

<sup>c</sup> Department of Informatics, University of Oslo, Oslo, Norway

---

### Abstract

In smart grid, a malicious entity can launch a direct load altering attack by injecting false commands into aggregators responsible for direct load control. It may remotely manipulate load, causing deviation in the operating frequency, and consequently lead to disruption in the system. In this paper, we mainly focus on the successive direct load altering attack, with which the attacker can continuously manipulate aggregators to achieve the larger impact. In addition to resulting in a larger impact, it is difficult for the controllers to detect such attacks as the attackers can inject false data to contaminate feedback data from aggregators to controllers. We present an attack model, and our analysis in this paper is from an attacker's perspective. Our model and analysis can serve as an important component also in the future for designing the counter strategies to such attacks. We propose a new frequency response model, which shows changes of the frequency undergoing a successive direct load altering attack. Attackers can utilize this model to analyze the impact of an attack sequence. Considering that attack sequences with different false commands can result in different levels of impact, we develop a three-step optimization method to analyze and find the optimal attack sequence. Our simulation results validate the feasibility and effectiveness of the successive direct load altering attacks.

*Keywords:* False Command Injection, False Data Injection, Successive Attack, Cyber-Physical System, Security

---

متن کامل مقاله

دریافت فوری ←

**ISI**Articles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات