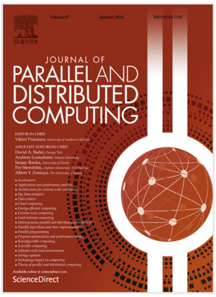

Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system

Beibei Li, Rongxing Lu, Wei Wang, Kim-Kwang Raymond Choo

PII: S0743-7315(16)30188-5
DOI: http://dx.doi.org/10.1016/j.jpdc.2016.12.012
Reference: YJPDC 3585

To appear in: *J. Parallel Distrib. Comput.*

Received date: 2 September 2016
Revised date: 10 November 2016
Accepted date: 4 December 2016

Please cite this article as: B. Li, R. Lu, W. Wang, K.-K.R. Choo, Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system, *J. Parallel Distrib. Comput.* (2016), http://dx.doi.org/10.1016/j.jpdc.2016.12.012

Distributed Host-based Collaborative Detection for False Data Injection Attacks in Smart Grid Cyber-Physical System

Beibei Li[a], Rongxing Lu[b,*], Wei Wang[a], Kim-Kwang Raymond Choo[c,d]

[a]*School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798*
[b]*Faculty of Computer Science, University of New Brunswick, Fredericton, Canada E3B 5A3*
[c]*Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA*
[d]*School of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, SA 5001, Australia*

Abstract

False data injection (FDI) attacks are a crucial security threat to smart grid cyber-physical system (CPS), and could result in cataclysmic consequences to the entire power system. However, due to the high dependence on open information networking, countering FDI attacks is challenging in smart grid CPS. Most existing solutions are based on state estimation (SE) at the highly centralized control center; thus, computationally expensive. In addition, these solutions generally do not provide a high level of security assurance, as evidenced by recent work that smart FDI attackers with knowledge of system configurations can easily circumvent conventional SE-based false data detection mechanisms. In this paper, in order to address these challenges, a novel distributed host-based collaborative detection method is proposed. Specifically, in our approach, we use a conjunctive rule based majority voting algorithm to collaboratively detect false measurement data inserted by compromised phasor measurement units

[*]Corresponding author.
Email addresses: bli012@e.ntu.edu.sg (Beibei Li), rlu1@unb.ca (Rongxing Lu), wei001@e.ntu.edu.sg (Wei Wang), raymond.choo@fulbrightmail.org (Kim-Kwang Raymond Choo)