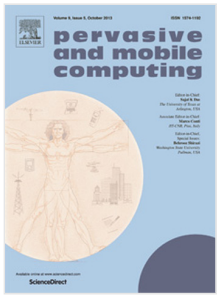
Accepted Manuscript



A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities

Jingxuan Wang, Lucas C.K. Hui, S.M. Yiu, Eric Ke Wang, Junbin Fang

PII: S1574-1192(17)30187-6
DOI: http://dx.doi.org/10.1016/j.pmcj.2017.04.005
Reference: PMCJ 829

To appear in: *Pervasive and Mobile Computing*

Received date: 19 September 2016
Revised date: 24 January 2017
Accepted date: 17 April 2017

Please cite this article as: J. Wang, L.C.K. Hui, S.M. Yiu, E.K. Wang, J. Fang, A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities, *Pervasive and Mobile Computing* (2017), http://dx.doi.org/10.1016/j.pmcj.2017.04.005

A Survey on Cyber Attacks against Nonlinear State Estimation in Power Systems of Ubiquitous Cities

Jingxuan Wang[a], Lucas C.K. Hui[a], S.M. Yiu[a,*], Eric Ke Wang[b], Junbin Fang[c]

[a] *Department of Computer Science, The University of Hong Kong, Hong Kong, China*
[b] *Harbin Institute of Technology Shenzhen Graduate School, China*
[c] *Dept. of Optoelectronic Engineering, Jinan University, China*

Abstract

It is well-known that critical infrastructures would be targets for cyber attacks. In this paper, we focus on the power systems (i.e. smart grids) in ubiquitous cities, where every meter is linked to an information network through wireless networking. In a smart grid system, information from smart meters would be used to perform a state estimation in real time to maintain the stability of the system. A wrong estimation may lead to diastrous consequences (e.g. suspension of electricity supply or a big financial loss). Unfortunately, quite a number of recent results showed that attacks on this estimation process are feasible by manipulating readings of only a few meters. In this paper, we focus on *nonlinear* state estimation which is a more realistic model and widely employed in a real power grid environment. We category cyber attacks against nonlinear state estimation, and review the mechanisms behind. State-of-the-art security measures to detect these attacks are discussed via sensor protection. Hope that the community would be able to come up with a secure system architecture for ubiquitous cities.

1. Introduction

A Ubiquitous City (U-city) is a highly integrated city, which manages ubiquitous information technologies (i.e. computation in communication networks) in urban areas via amounts of physicals (i.e. sensors). The power system is a fundamental component in U-city, with sensors (i.e. smart meters) as the physical entities and the SCADA (Supervisory Control And Data Acquisition) control system as the computational unit. Primarily, a smart grid is envisioned to be the power systems of U-city infrastructure in the future and has been employed in many countries already. A smart grid can adjust its power flows of electricity in real time, even when an electrical transmission path is interrupted, to meet the requirements from both power suppliers and customers. Smart

*Corresponding author
Email addresses: jxwang@cs.hku.hk (Jingxuan Wang), hui@cs.hku.hk (Lucas C.K. Hui), smyiu@cs.hku.hk (S.M. Yiu), wkhit@hitsz.edu.cn (Eric Ke Wang), junbinfang@gmail.com (Junbin Fang)

[1] A preliminary version of this paper appeared in ACISP'16 [1].