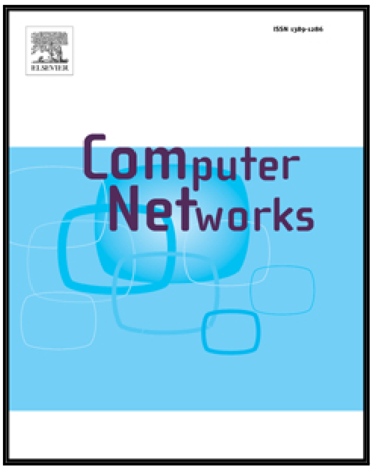
Accepted Manuscript



Virtual Incident Response Functions in Control Systems

Andrés F. Murillo Piedrahita, Vikram Gaur, Jairo Giraldo,
Alvaro A. Cardenas, Sandra Julieta Rueda

PII:	S1389-1286(18)30043-4
DOI:	10.1016/j.comnet.2018.01.040
Reference:	COMPNW 6388
To appear in:	*Computer Networks*
Received date:	1 August 2017
Revised date:	9 December 2017
Accepted date:	18 January 2018

Please cite this article as: Andrés F. Murillo Piedrahita, Vikram Gaur, Jairo Giraldo, Alvaro A. Cardenas, Sandra Julieta Rueda, Virtual Incident Response Functions in Control Systems, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.01.040

Virtual Incident Response Functions in Control Systems

Andrés F. Murillo Piedrahita[a,b], Vikram Gaur[b], Jairo Giraldo[b], Alvaro A. Cardenas[b], Sandra Julieta Rueda[a]

[a]*Department of Computer Science, Universidad de Los Andes, Colombia*
[b]*Department of Computer Science, University of Texas at Dallas, USA*

Abstract

In the past decade the security of industrial control systems has emerged as a research priority in order to safeguard our critical infrastructures. A large number of research efforts have focused on intrusion detection in industrial networks, however, few of them discuss what to do after an intrusion has been detected. Because the safety of most of these control systems is time-sensitive, we need new research on *automatic* incident response. In this article we show how software-defined networks, and network-function virtualization can facilitate automatic incident response to a variety of attacks against industrial networks. We also prototype an incident response solution that detects and responds automatically to sensor attacks and controller attacks. Our work shows the promise that cloud-enabled software-defined networks and virtual infrastructures hold as a way to provide novel defense-in-depth solutions for industrial systems.

1. Introduction

Industrial Control Systems (ICS) are responsible for operating various safety-critical infrastructures, such as power grids, water management, oil systems, and manufacturing. Recent events, like the blackout caused by the cyber-attack against the power-grid in Ukraine [1] show the dire need for improving the security of ICS.

Cybersecurity is a process consisting on (1) *protecting*, (2) *detecting*, and (3) *responding* to attacks [2]. Most of the literature on ICS security has focused on *preventing* and *detecting* attacks [3]; however, *responding* to attacks has received much less attention [3, 4]. In particular, most of the research papers focusing on intrusion detection for control systems do not discuss what to do after an attack has been detected [5].

In this paper we address this gap in the literature by designing intrusion response mechanisms that keep the control system operating safely while sustaining attacks. To design and implement our intrusion response architecture we use Software-Defined Networking (SDN), and cloud-based virtual infrastructures. While the use of SDN for protecting power systems has been considered before [6], previous work has focused on proactive defenses, and not as a *response* to detected attacks. Similarly while cloud-based intrusion detection sys-