Theoretical Computer Science 609 (2016) 606–619

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

# Optimal packet scan against malicious attacks in smart grids ☆

Subhankar Mishra [a], Thang N. Dinh [c], My T. Thai [b,a,*], Jungtaek Seo [d], Incheol Shin [e]

[a] Dept. of Comp. and Info. Sci. and Eng., University of Florida, Gainesville, 32611, USA
[b] Division of Algorithms and Technologies for Networks Analysis, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
[c] Dept. of Comp. Sci., Virginia Comm. University, Richmond, VA 23284, USA
[d] The Attached Institute of ETRI, Republic of Korea
[e] Info. Security Dept., Mokpo National University, Muan, Republic of Korea

ARTICLE INFO

*Article history:*
Received 1 November 2014
Received in revised form 26 May 2015
Accepted 28 July 2015
Available online 31 July 2015

*Keywords:*
Malicious attacks detection
Smart Grids
Approximation algorithms

ABSTRACT

With the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. Along with the salient features of the Smart Grid, cyber security emerges to be a critical issue because millions of electronic devices are inter-connected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a widespread infrastructure. In this paper, we discuss the packet based attacks and study the Optimal Inspection Points (OIP) problem, which asks us to find a subset of nodes in a given network to perform the Deep Packet Inspection so as to maximize the number of scanned packets while satisfying the delay constraints. This problem finds many applications for malicious attack detection, especially for those cases where each single packet or the network traffic is required to be inspected. Accordingly, we prove OIP is NP-complete and provide an FPTAS in the case of single path routing. For the multiple path routings, we design an FPTAS when the routing graph takes a form of series-parallel graphs, which is commonly used to model electric networks. We also discuss the multi-scan scenario and design PIVOT algorithm to tackle the problem and evaluate the algorithms through experiments.



## 1. Introduction

Smart Grids allow the energy industry to improve its reliability, availability, and efficiency with the technology of two-way communication between utility and its customers [1–4]. The Smart Grid consists of controls, computers, automation, and new technologies and equipment working together, but unlike Internet, the technologies will make electrical grid to respond digitally to our dynamic electric demand. Although in the approach to become “smarter”, more and more inter-connections are incorporated to the expanding grid which may become gateways for intrusions, error-caused disruptions,

☆ The first two authors contribute equally to this work.

* Corresponding author at: Dept. of Comp. and Info. Sci. and Eng., University of Florida, Gainesville, 32611, USA.
*E-mail addresses:* mishra@cise.ufl.com (S. Mishra), tndinh@vcu.edu (T.N. Dinh), thaitramy@tdt.edu.vn (M.T. Thai), mythai@cise.ufl.com (M.T. Thai), seojt@ensec.re.kr (J. Seo), ishin@mokpo.ac.kr (I. Shin).

http://dx.doi.org/10.1016/j.tcs.2015.07.054
0304-3975/

malicious attacks, and other threats. There are many new classes of cyber attacks that have been emerging in the last decade [5–8]. Adversaries through potential network intrusion [9] might end up with serious damages in the Smart Grid, including the leakage of private customer information and cascading failures which consequently lead to massive blackouts and destruction of infrastructures.

In theory, a utility smart grid could be totally independent of the Internet, but in practice it often makes sense to use existing infrastructure, that is Internet Protocol (IP). So instead of sealing the network from the Internet, the main focus has been on running secured services over the Internet; therefore, it inherits all the benefits of the Internet world. Unfortunately, it also carries the same vulnerability of the Internet i.e. cyber attacks, which can attack all three security objectives of Smart Grids, namely availability, integrity, and confidentiality [10]. For example, the denial-of-service (DoS) attacks target the availability with attempt to delay, block or corrupt the communication system in the Smart Grid. In another case, attackers can deliberately and illegally modify or disrupt data exchange to attack integrity of the Smart Grid. Attacks aiming confidentiality try to acquire unauthorized information from network resources in the Smart Grid.

In order to achieve both security and QoS (Quality of Service) requirements in the Smart Grid, we need more comprehensive security mechanisms. The possible countermeasures for the Smart Grid are of two types i.e. Networking and Cryptographic countermeasures [11]. Cryptographic measures include symmetric key cryptography and asymmetric key cryptography. The former needs more computational resources such as AES (Advanced Encryption Standard) and DES(Data Encryption Standard). The later needs secure exchange of keys such as RSA. There are many works on the cryptographic security in [7,8,12]. Although cryptographic approaches are primary countermeasures to deal with integrity and confidentiality attacks, they are very much less effective in detecting malicious attacks that can lead to network traffic dynamics by the use of malicious packets or malfunction by modifying the control data packets, thereby requiring the networking countermeasure. This method includes the signal and packet-based detection. The signal-based detection relies on the physical or MAC layer to measure signal strength (RSSI) to detect malicious attacks. The packet-based detection are applied to scan through each packet and discover the existence of potential attacks.

The packet-based detection, which uses the Deep Packet Inspection (DPI) method is promising in defending the malicious attacks which aim to alter packet contents. However, inspecting every single packet is time-consuming, thereby significantly increasing the delays in throughputs. Furthermore, Smart Grid communication protocol IEC 61850 relies on time critical messages which must arrive at the central monitoring node on time. Control messages not satisfying time constraints are discarded, which includes the risk of dropping important control messages leading to serious physical and/or financial damage, therefore inspection cannot be performed at all points and on all packets.

Based on the above motivation, we introduce and study a new optimization problem, namely *Optimal Inspection Points* (OIP). Given a network represented by a graph $G = (V, E)$, the goal is to find a subset $D \subseteq V$ which represents the set of inspection points, such that the number of scanned packets at the center node is maximized without violating the latency constraint. Clearly this problem helps to inspect the packets as much as possible to search for malicious ones while ensuring all packets arrive on time.

The routing schemes in different networks together with the strict latency constraints make this problem challenging and interesting. The time constraint in IEC 61850 [13–16], for example, could be as low as 3 ms for the critical fault isolation and protection control messages [11]. Also the number of the scanned packets, which in turn increases the probability of catching a malicious packet, has to be as high as possible. Therefore, it would be nice if we can devise a Fully Polynomial Time Algorithm Scheme (FPTAS) for the OIP. Indeed, we have developed such a solution for the single path routing scenario. As for the multiple path routing, we devised another FPTAS to OIP where the routing graph has a form of series-parallel graphs.

The remainder of this paper is organized as follows. Section 2 presents the network model and our problem definition. The complexity and FPTAS are discussed in Section 3 and 4 respectively. We introduce our FPTAS for multiple path routing in series-parallel graphs in Section 5 and provide more discussion with different scanning scenarios in Section 6. Section 7 evaluates our approach by conducting several experiments and finally, Section 8 concludes our paper.

## 2. Model and problem definitions

A smart grid is modeled as a directed graph $G = (V, E)$ where the vertices in $V = \{r\} \cup O \cup S$ represent the set of nodes in the grid and $E$ represents the set of communication links among the nodes (Fig. 1).

The set of vertices $V$ includes the following:

- The center node $r$ which represents the Supervisory Control And Data Acquisition (SCADA) center. All the state estimations and corresponding actions based on the message received from $S$ are done by $r$.
- $S$ is the set of the nodes that can act as a source of malicious packets and hence can be under the control of attackers. These nodes are the Intelligent Electronic Devices (IEDs) or the Remote Terminal Units (RTUs). IEDs or RTUs receive data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level.
- $O = V \setminus \{S \cup r\}$ is the set of intermediate nodes where DPI can be performed. If a node in O does not have DPI scanner, then equivalently the capacity of the scanner at that node is 0.