Chapter 14
Dynamic Trust Elective Geo Routing to Secure Smart Grid Communication Networks

Ming Xiang
Auckland University of Technology, New Zealand
William Liu
Auckland University of Technology, New Zealand
Quan Bai
Auckland University of Technology, New Zealand
Adnan Al-Anbuky
Auckland University of Technology, New Zealand

ABSTRACT

Smart Grid is believed to be the next generation of electrical power system. It integrate the existing electrical power infrastructure with Information Communication Technology (ICT) to achieve two way communication and become smart. A high level of network availability is therefore required to guarantee two-way flows of electricity and information among smart electrical units. The wireless mesh network infrastructure can provide redundant routes for the Smart Grid communications so as to ensure the network availability. However, the wireless connection is vulnerable to cyber-attacks. In this paper, we propose a Fuzzy-Based Energy Aware Trusted Geo-Routing (FEATGR), which can decide the optimal end-to-end path between any source and destination by effectively leveraging the energy consumption, location and trust metrics. The extensive simulation studies have confirmed that FEATGR is capable to achieve the stable and secured routing performance so as to guarantee the high level of network availability for wireless Smart Grid communications.

1. INTRODUCTION

Intricate webs of interlinked critical infrastructure such as telecommunication and Internet, electricity and transportation networks are essential for the minimal functioning of contemporary societies and economies. Advances in information and communications technology (ICT) underpin the increasing interactions among these human-engineered networks. For example, the emerging higher expectations
on the electrical power distribution and consumer systems are increasing every day, such as lower power price, more efficient and flexible usage, better power quality, smarter and interactive management, and also less carbon footprint impact on the environments, etc. (Yan et al., 2012; Baumeister, 2010; Yan et al., 2013, Zhang et al., 2011). The new Smart Grid paradigm is promising and regarded as the next generation electrical power network trend, which promises to meet the increasing requirements and satisfaction by our societies. It couples the power distribution network and communication networks as one smarter system, and they can perform two-way interactive information and control flows (Yan et al., 2012), so as to make intelligent decisions and optimization on electricity usages according to the state of the electrical power system and customer’s dynamical needs (Baumeister, T., 2010). The National Institute of Standards and Technology (NIST) has defined Smart Grid standard in seven domains, which are market, customer, service provider, bulk generation, distribution, operation, and transmission in (“IEEE Smart Grid Domains & Sub-domains”, 2015). Smart Grid communication network underpins and connects these seven domains together with two-way information data transmission so as to enable the power grid become smarter, intelligent, and also energy efficiency with optimal energy resource management.

Comparing with the traditional power grid, Smart Grid is the integration of information technology and power grid. As the communication network becomes more and more crucial in Smart Grid, a high level on reliability and robustness on network connectivity is required to support these interactive electrical services and applications. The wireless mesh network (WMN) is a promising infrastructure solution for Smart Grid which provides the reliable connection as a redundant routes provision, low cost, scalability, and flexibility. The WMN can provide high-speed and reliable wireless transmission, as well as the mesh-like network topology enables the redundant communication path options to be selected. Therefore the WMN can conduct fault-tolerant and self-healing operations during the network failures (e.g. node down or link cut occurs). It can adapt itself dynamically in an open error-prone wireless environment (Geelen et al., 2012; Jung et al., 2011; Athreya and Tague, 2012; Gharavi and Hu, 2011). On the other hand, each node in WMN is self-organised and connected with wireless network like Wi-Fi, ZigBee, etc. All these features of WMN make the network entities and their information flows easily accessed or attacked by the malicious parties. The security issues of the network are crucial in WMN. As the computing resources are limited in nodes in WMN, the traditional security mechanisms such as encryption need to be well considered to apply on the nodes. Moreover, as WMN is distributed network which the traditional trust infrastructure such as PKI is no longer suitable. The traditional security mechanisms are considered as hard security to defend and protect data integrity from malicious parties, but it might not be enough to protect the network from legitimate node misbehavior and selfish behavior (Yu et al., 2010). Trust is considered as a soft security mechanism to detect and avoid such soft security threats. Distributed trust-management is a popular trust solution for this nowadays.

To address the security issues in WMN under Smart Grid environment, we proposed the fuzzy logic approach trust-based routing algorithm. This is Fuzzy-based Energy Aware Trust Geo Routing (FEATGR). We have compared the FEATGR algorithm with previous proposed Dynamic Trust Elective Geo Routing (DTEGR) (Xiang, Bai, and Liu, 2012) algorithm in our extensive simulation studies and tried to find out which one is performing better by minimizing the damage cause by malicious attacks, such as packet loss number.

The rest of chapter is organized as follows. An introduction of Smart Grid infrastructure and its threats are given in section 2. Section 3 review the trust modelling in computer network routing. The FEATGR algorithm is proposed in section 4, and in section 5, the extensive simulation studies are given. Finally, the chapter is concluded in section 6.