Chapter 20
Quantum-Resistant Authentication for Smart Grid: The Case for Using Merkle Trees

Melesio Muñoz-Calderón
https://orcid.org/0000-0003-1105-5157
Cupertino Electric Inc., USA

Melody Moh
https://orcid.org/0000-0002-8313-6645
San Jose State University, USA

ABSTRACT

We are currently at the beginning of a great technological transformation of our electrical power grids. These new grids will be "smart" as a result of improved communication and control systems but will also have new vulnerabilities. A smart grid will be better able to incorporate new forms of energy generations as well as be self-healing and more reliable. This chapter investigates a threat to wireless communication networks from a fully realized quantum computer and provides a means to avoid this problem in smart grid domains. This chapter examines the security, complexities and performance of device authentication in wireless mesh networks (WMN) using public-key encryption and then using Merkle trees. As a result, the authors argue for the use of Merkle trees as opposed to public-key encryption for authentication of devices in WMN used in smart grid applications.

ORGANIZATION BACKGROUND

Cupertino Electric Inc. is a private company founded in 1954 and headquartered in San José, CA. It provides electrical engineering and construction services.

San José State University (SJSU) was founded in 1857 as a normal school and has matured into a metropolitan university in the Silicon Valley. It is one of 23 campuses in the California State University system, offering more than 145 areas of study with an additional 108 concentrations.

DOI: 10.4018/978-1-6684-5250-9.ch020

INTRODUCTION

Today our modern world is not so far removed from a "simpler time" when rapid transportation was by horse, water was hauled by hand and refrigeration was a sort of science fiction. Some of us will never forget the stories told by our elders of the first time they witnessed the magic of electricity. Since those times technology has advanced quickly. Presently, as a result of political turmoil, cyber-attacks and natural disasters we see how important electric power has become to our modern societies. Electricity keeps transportation systems moving in an orderly manner. It keeps water flowing. It keeps medicines and food refrigerated. In short electric power is now fundamental to our world.

The electrical power grid forms the functional foundation of our modern societies. Born in the Victorian Era the grid has served humanity well, but as our societies continue to evolve, demands are increasing, and requirements are being put on the grid that were not there a hundred years ago. In short, this infrastructure is hitting a limit and needs to be modernized. It is expected that by 2050 worldwide consumption of electricity will triple (Kowalenko, 2010). Furthermore, power grids are still susceptible to large-scale outages that can affect millions of people (U.S.-Canada Power System Outage Task Force, 2004). These are some of the motivations for the creation of an "advanced decentralized, digital, infrastructure with two-way capabilities for communicating information, controlling equipment and distributing energy" (National Institute of Standards and Technology (NIST, 2010). This infrastructure will be better able to incorporate new forms of energy generation, as well as be self-healing and more robust. Each device in a smart grid will likely have its own IP address and will use protocols like TCP/IP for communication. Thus, they will be vulnerable to similar security threats that face present day communication networks (Yan, Qian, Sharif, Tipper, 2012); however, the stakes will be much higher. That is to say, in the information technology industry the highest priority is the confidentiality, integrity and availability of information. In the electrical power industry, the highest priority is human safety. For the smart grid cyber security measures must not get in the way of safe and reliable power system operations (NIST, 2010).

Problem Statement

In Northern California the last several years have brought the limitations of our current power grid into a clearer focus. The autumn season, once a pleasant time of less coastal fog and warmer temperatures, now appear to be drier, longer and hotter than in previous times (Deedler, 1996). In parts of California this is now being referred to as "fire season" (Sahagun, 2019). It is the combination of several factors, dried out fuels from hotter summers, a later start to the rainy season and high winds that combine to create acutely dangerous fire conditions. Electrical power lines can produce arcs and sparks when they fall, this is a basic fact of electrical power distribution. Currently, to mitigate some of the dangers of fire, utility providers are shutting down power to some of their customers during weather events. This is a disruptive, and possibly clumsy approach, but not unreasonable considering the limits of our current grid. A valid argument could be made that with real time information, self-healing automation, and the ability for fine grain controls, a smart grid could be an important tool in combating the effects of fire season in California and elsewhere.

How we extract, use and distribute energy is at the heart of some of the most important issues of our day. Renewable energy sources offer a lot of promise but are often limited by the existing electrical infrastructure. "Falling costs and growing public support for renewable power generation will require