Byzantine Fault Tolerant Monitoring and Control for Electric Power Grid

E

Wenbing Zhao
Department of Electrical and Computer Engineering, Cleveland State University, USA

INTRODUCTION

The data communication infrastructure for electric power grid is in urgent need of transformation to modern computer networking technologies for a number of reasons:

- The recent deregulation would allow many independent parties to enter the utility industry by offering alternative channels for electric power generation, distribution, and trade. This inevitably demands timely, reliable and secure information exchanges among these parties (Bose, 2005).
- The current data communication infrastructure lacks the support for large-scale real-time coordination among different electric power grid health monitoring and control systems, which could have prevented the 2003 massive blackout incident in North America (Birman et al., 2005).
- The use of modern computer networking technology could also revolutionize the everyday electric power grid operations, as shown by the huge benefits of substation automation and the use of Phasor Measurement Units (PMUs) for electric power grid health monitoring (Melliopoulos, 2007).

However, the openness and the ease of information sharing and cooperation brought by the data communication infrastructure transformation also increased the likelihood of cyber attacks on the electric power grid, as demonstrated recently by an experiment conducted by the US Department of Energy's Idaho Lab (CNN, 2007). To address such vulnerability, intrusion detection and intrusion tolerance techniques must be used to enhance the current and future data communication infrastructure for the electric power grid. Byzantine fault tolerance is a fundamental technique to achieve the objective (Castro & Liskov, 2002; Lamport, Shostak, & Pease, 1982).

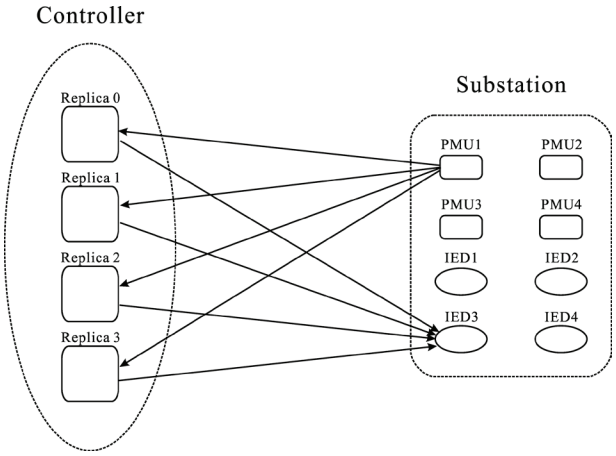
In this article, we focus our discussions on the security and reliability of electric power grid health monitoring and control. We elaborate in detail the need for Byzantine fault tolerance and the challenges of applying Byzantine fault tolerance into this problem domain. In particular, we investigate experimentally the feasibility of using such sophisticated technology to meet potentially very stringent real-time requirement for the health monitoring and control of electric power grid, while ensuring high degree of reliability and security of the system.

BACKGROUND

A Byzantine faulty process may behave arbitrarily. In particular, it may disseminate conflicting information to different components of a system, which constitutes a serious threat to the integrity of a system (Lamport, Shostak, & Pease, 1982). Because a Byzantine faulty process may also choose not to send a message, or refuse to respond to requests, it can exhibit crash fault behavior as well. Consider the scenario that multiple PMUs periodically report their measurement results to a controller for electric power grid health monitoring. When it detects an abnormally, the controller may wish to issue specific control instructions to the actuating devices, such as Intelligent Electronic Devices (IEDs) (Hossenlopp, 2007) located at the same substation as those PMUs to alleviate the problem. Due to the critical role played by the controller, it must be replicated to ensure high availability. Otherwise, the controller would

DOI: 10.4018/978-1-4666-5888-2.ch261

Figure 1. The interaction of substation devices (PUMs and IEDs) and the controller replicas



become a single-point of failure. The main components and their interactions are illustrated in Figure 1.

However, the controller replicas, the PMUs, and the IEDs, might be compromised under cyber attacks. Consider the following two scenarios:

- A Byzantine faulty PMU could potentially send inconsistent data to different controller replicas. Without proper coordination among the controller replicas, the state of the replicas might diverge in the former case, which would lead to inconsistent decisions among the replicas.
- A compromised controller replica could send conflicting commands to different IEDs. Without a sound mechanism at each IED, a malicious command might be executed in the latter case, which could lead to the destruction of a generator or a transmission line, as reported by CNN (2007).

Byzantine fault tolerance (BFT) refers to the capability of a system to tolerate Byzantine faults (Lamport, Shostak, & Pease, 1982). If BFT is used, the cyber attacks illustrated above could be defeated provided that the number of compromised controller replicas, f, is below a threshold, and the number of non-faulty PMUs and IEDs are sufficient for the normal operation of the substation. For the client-server system shown in Figure 1, BFT can be achieved by using $3f + 1$ replicas to tolerate up to f faulty replicas and by ensuring all non-faulty replicas to execute the same set of requests in the same order. The latter means that the server replicas must reach an agreement on the set of requests and their relative ordering despite the presence of Byzantine faulty replicas and clients. Such an agreement is often referred to as a Byzantine agreement (Lamport, Shostak, & Pease, 1982). The Byzantine agreement among the replicas ensures that a faulty client (i.e., a PMU) cannot cause the divergence of the state of non-faulty controller replicas. Furthermore, a Byzantine agreement must be reached among all non-faulty replicas on each command issued by the controller for reasons to be explained in the next section. Before an IED can accept the command, it must wait until it has collected at least $f + 1$ matching command from different replicas.

We should note that Byzantine fault tolerance has been a hot research area in many other areas, such as Web services (Merideth et al., 2005; Zhao, 2009) and data storage systems (Rhea et al., 2003). Even though the works are in a different context, many insights are useful for BFT controls in electric power grid applications. In particular, the mechanisms designed to cope with the interaction of a replicated object and the unreplicated external entities reported in (Merideth et al., 2005) have been partially incorporated in this work.

BYZANTINE FAULT TOLERANT MONITORING AND CONTROL MECHANISMS

In this work, we choose to use PBFT, a well-known Byzantine agreement algorithm developed by Castro and Liskov (2002). The PBFT algorithm is designed to