International Journal of Information Security
https://doi.org/10.1007/s10207-021-00561-8

REGULAR CONTRIBUTION

Insider attack mitigation in a smart metering infrastructure using reputation score and blockchain technology

Jaya Singh[1] · Ayush Sinha[1] · Priyanka Goli[1] · Venkatesan Subramanian[1] · Sandeep Kumar Shukla[2] · Om Prakash Vyas[1]

Abstract

The increasing use of smart metering infrastructure invites security threats through trusted insiders in spite of the devices' authentication phase. Trusted insiders equipped with high privilege are also become vulnerable to being attacked. In the presence of these malicious or compromised insiders, it becomes difficult to achieve an efficient, transparent, reliable, and cost-effective smart grid. Addressing the issues arising from an insider attack, we explore post-authentication attacks and present a reputation score-based model using blockchain technology. The reputation of a device is computed based on the neighbor's opinion. The opinions and incentives are stored on a blockchain to ensure integrity, availability, and decentralization. We analyze the latency of the proposed model by modifying the open-source Go Ethereum and security effectiveness through a reputation simulator. In addition to this, storage, communication, resource usage overhead, and security requirements are also analyzed to prove the efficiency of the proposed model for the lightweight smart metering infrastructure.

Keywords Smart grid · Smart metering · Blockchain · Reputation · Insider attack

1 Introduction

The emergence of Smart grid (SG) infrastructure advances the connectivity, communication, and automation of different verticals and zones of the power network. Though simultaneously it increases the security issues, that benefits the outside and the inside attacker. To address and solve these security and privacy-related issues, the researchers have introduced various lightweight authentication and key agreement protocols. These work provide a robust communication frameworks to support secure information transactions among trusted components while managing their privacy and also control the outside attackers though insider attack scenario remains unaddressed. In recent years, many comprehensive research have surfaced regarding authentication and key agreement for securing the communication from outsider attacks in smart grid systems, but very few research has been carried out to handle the post-authentication attacks in smart metering infrastructure.

The post-authentication attackers are always the inside devices, which are successfully verified during the authentication phase and later started behaving maliciously. This practice goes unidentified or hard to recognize and deal with it. These insiders are more dangerous and powerful than outside attackers in the smart grid environment since those devices are adequately familiar with the system's current security technique and structure. Broadly there are two types of inside threat agents: intended and unintended; intended threat agents can be a traitor or a masquerader [1,2]. A traitor is defined as the insider who exists in the system with legal access. At the same time, masquerader does not have legit-

✉ Jaya Singh
jayasinghoct20@gmail.com

Ayush Sinha
sinhamnnit@gmail.com

Priyanka Goli
priyankasuresh816@gmail.com

Venkatesan Subramanian
venkat@iiita.ac.in

Sandeep Kumar Shukla
sandeeps@cse.iitk.ac.in

Om Prakash Vyas
opvyas@iiita.ac.in

[1] Department of Information Technology, Indian Institute of Information Technology, Allahabad, Prayagraj, India

[2] Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, Kanpur, India

Published online: 21 September 2021