

Detection of False Reading Attack on Smart Energy Meter

Dr. Satish Turkane¹, Kunal Popalghat², Tushar Turkane³, Vaishnavi Gunjal⁴

Department of Electronics and Telecommunication Engineering
Pravara Rural Engineering College, Loni, Maharashtra, India

Abstract: *Smart net metering systems face significant challenges related to accurate electricity measurement, safety concerns, and the threat of external tampering. False-reading attacks, which manipulate recorded usage data, undermine billing accuracy and system integrity. Safety issues, including temperature variations and gas leaks, pose risks to users and the system. External tampering, such as data manipulation or physical damage, threatens security and accurate readings. To address these challenges, a comprehensive solution is proposed to improve measurement accuracy, enhance safety measures, and establish robust security protocols. The aim is to create secure and efficient smart grid net metering systems that benefit consumers, utility providers, and the energy ecosystem as a whole. The modernization of energy distribution systems through the implementation of smart grid technologies has led to the development of advanced smart net metering systems. These systems play a crucial role in monitoring and managing electricity consumption and generation. However, as these systems rely on data communication and digital technologies, they become susceptible to various cyber threats, including false reading attacks, which can have significant financial and operational consequences for both utility companies and consumers. This project aims to address the issue of false reading attacks in smart net metering systems by proposing a detection mechanism to safeguard the integrity of the data*

Keywords: Net Metering, Electricity Measurement, False- Reading Attacks, Safety Concerns, External Tampering, Billing Accuracy, Energy Distribution, Security Protocols, System Integrity

REFERENCES

- [1]. L. J. Lepolesa, S. Achari, and L. Cheng, "Electricity theft detection in smart grids based on deep neural network," IEEE Access, vol. 10, pp. 39638–39655, 2022.
- [2]. M. M. Badr, M. I. Ibrahim, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmay, "Detection of false-reading attacks in smart grid net metering system," IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1386–1401, 2021.
- [3]. A. Takiddin, M. Ismail, M. Nabil, M. M. Mahmoud, and E. Serpedin, "Detecting electricity theft cyber-attacks in AMI networks using deep vector embeddings," IEEE Systems Journal, vol. 15, no. 3, pp. 4189–4198, 2020.
- [4]. A.T.ElToukhy1,M.M.Badr,M.Mahmoud,G.Srivasta va, M.M. Fouda M.Alsabaan, "Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids"
- [5]. M. I. Ibrahim, M. Nabil, M. M. Fouda, M. M. Mahmoud, W. Alasmay, and F. Alsolami, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks," IEEE Internet of things journal, vol. 8, no. 2, pp. 1243–1258, 2020

AUTHORS

- Kunal popalghat, BE Electronics & Telecommunication, Pravara Rural Engineering College, kunalpopalghat95@gmail.com
- Tushar Turkane, BE Electronics & Telecommunication, Pravara Rural Engineering College, t.s.turkane@gmail.com
- Vaishnavi Gunjal, BE Electronics & Telecommunication, Pravara Rural Engineering College, vaishnavigunjal96@gmail.com