UNIVERSITÉ Concordia UNIVERSITY

Concordia Institute for Information System Engineering (CIISE)

Summary On

Advanced Metering Infrastructure (AMI) System Security

INSE 6640 – Smart Grids and Control System Security

Group Members

Vishal - (40294677), Bala Krishna Yadav Kunati- (40292128), Jaykit Kukadiya – (40261905), Raghu Pavan Annam – (40303699) - Virenkumar Virani – (40279337)

TERM – FALL 2024

Submitted to:

Professor M. Ghafouri

This paper reviews AMI-a major technology in modern energy management systems to enable two-way communications between utility providers and end-users-in terms of design, architecture, communication technologies, and associated security issues, and integration with Home Area Networks. The paper also compares various communication technologies like WiMAX, Zigbee, Wireless Mesh Networks, and cellular networks based on their special features and security vulnerabilities about DDoS-attacks and possible data losses. These may be recommended by integrating Intrusion Detection Systems and Public Key Infrastructure for the higher degree of assurance in security. The importance of continuous risk assessment and strong security control mention therein, ensures efficiency and resiliency in smart grid scenarios with AMI.

The electrical power sector has been undergoing major transformation due to technological advances, increasing use of renewable sources of generation, and a focus on sustainability. Conventional systems are giving way to intelligent networks that integrate decentralized generation units with advanced communication systems. In an intelligent network, two-way flow of information is possible, allowing for real-time monitoring and optimization of generation. Thus, consumers can better monitor their consumption and participate in demand-response programs, and utilities can better manage load distribution.

The architecture of the AMI is segmented into four domains: customer, distribution, transmission, and operation. Each such domain employs different communication technologies suitable for its range and data transfer limits.

1. Customer Domain: These are intelligent meters installed at customer premises, communicating through various home devices over Zigbee, PLC, Bluetooth, or WiFi. These meters measure energy usage, and the data is sent to the utility providers.

2. Distribution Domain: It collects data available locally in smart meters and sends the information to the main relay server via a neighbourhood area network. Communication technologies: WiFi, Cellular, and PLC.

3. Transmission Domain: Provides connectivity between the data aggregation access point and the AMI head end through a wide-area network by using WiMAX, cell networks, satellite communications, and optical fibers.

4. Operation Domain: This is used to manage and store data on the head end side of AMI, MDMS, and the Utility Center. This communicates with smart meters over their collected data and issuance of commands.

AMI systems face several security challenges, including:

Physical Attacks: Smart meters are tamperproof; however, unauthorized modification, if done, might result in fraudulent billing and tampering with data.

Protocol Weaknesses: Weak implementation of communication protocols, where the use of insecure encryption on Zigbee, opens the door for malicious attacks. Even old networks like 2G and 3G are still major security concerns.

Legacy Infrastructure: Outdated components that cannot satisfy new standards of security are the ones which will be exploited.

Data Privacy and Integrity: The AMI system transmits sensitive information that can be accessed by unauthorized parties; the consequences are financial loss and loss of confidence.

Proposed security framework to deal with these security concerns that cover:

1. PKI-based Authentication Using Digital Certificate: A digital certificate installed in each device for mutual authentication authenticates the communication of the Smart Meter with the Central management system.

2. Intrusion Detection Systems: Monitor network traffic and device behaviors for both internal and external threats. IDS systems apply machine learning and behavior analytics in the detection of advanced threats.

3. Protection of information access by applying the principles of safe communication channels and encryption techniques, including symmetric ones like AES, asymmetric ones like RSA and ECC, and TLS.

4. Protection against some very common types of attack: the flow will include traffic filtration, rate limiting, DDoS mitigation services, whitelisting of devices, and physical security against denial-of-service/distributed denial-of-service attacks, spoofing, and man-in-the-middle attack.

The risk assessment framework identifies vulnerabilities including data manipulation and communication breakdowns in Smart Metering and Smart Grid: countermeasures with regard to smart encryption techniques, intrusion detection systems to detect anomalies; PKI with regard to Smart device authentication; challenges: due to the lack of expertise on information security and intrinsic complexity of emerging technologies.

The integration of the AMI with HAN will facilitate the interaction of energy meters installed at consumer premises with utility-operated control centers. This network setup allows the monitoring of appliance functionality and control, along with demand-side management. At the same time, however, it opens up the need for secure communication channels and raises several issues on network security and user privacy.

The proposed framework is resilient against spoofing, Sybil attacks, and DoS attacks by way of PKI-based authentication and IDS. The simulation results prove high packet delivery ratios with negligible delays, hence promoting secure and efficient communications. Further implementation in AI-empowered threat detection, development of secure routing protocols, and cognizance of advanced cryptography techniques shall be carried out.

The security framework proposed for the AMI system covers the most relevant security issues and provides a tangible basis for future security studies on Smart Grids. The AMI systems will be dependable

and resilient only through continuous risk assessments and stringent security controls. The integration of the PKI-based authentications and IDS within the framework enhances security to ensure that AMI is efficient and robust in smart grid scenarios.