School of Electrical Engineering & Computer Science
UNIVERSITY OF NORTH DAKOTA

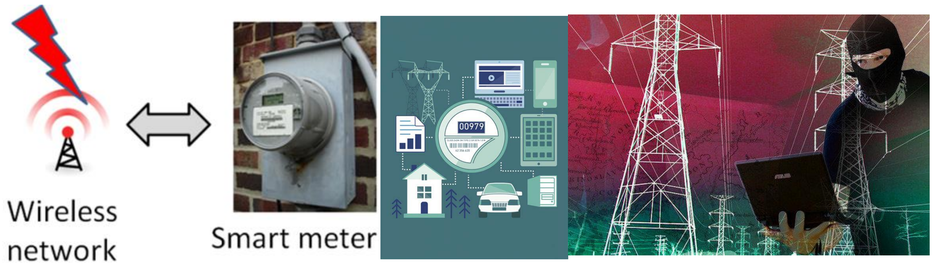
Smart Grid Metering Infrastructures: Threats and Solutions

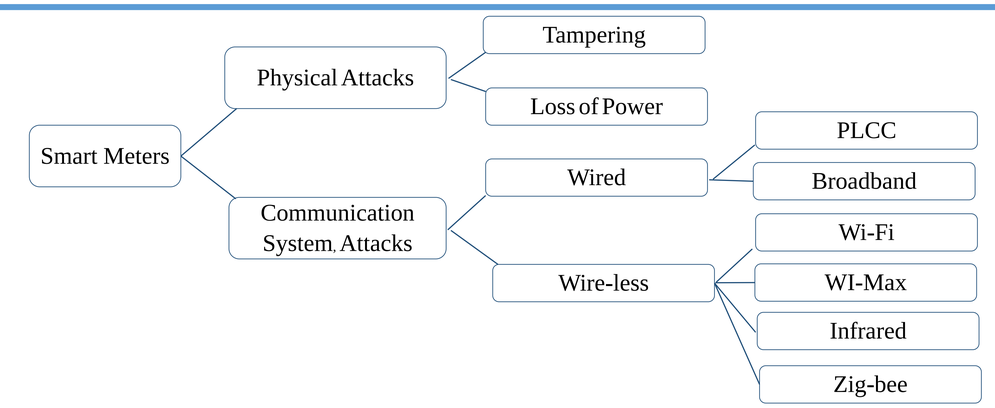
Rasel Mahmud, Ranganath Vallakati, Anupam Mukherjee, Prakash Ranganathan, Arash Nejadpak

DECS

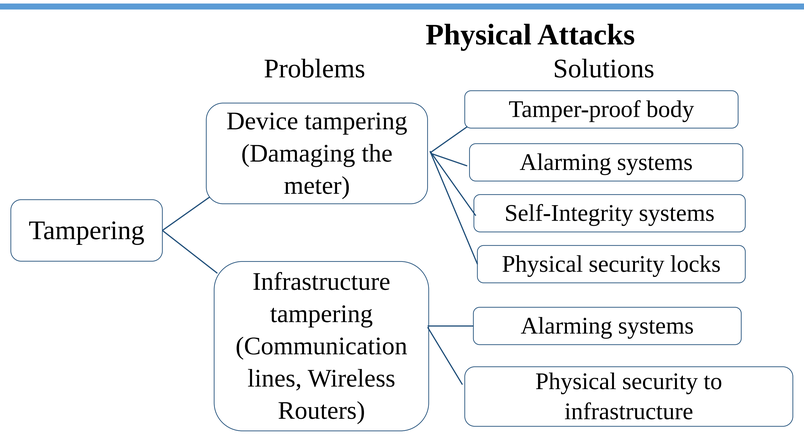
Introduction

A true smart grid infrastructure should detect all existing and predict future threats through intrusion detection methods. Smart grids are susceptible to various physical and cyber-attack as a result of communication, control and computation vulnerabilities employed in the grid. Smart Meters (SM) are significant components in Smart Grids (SG) that measure, gather and transmit information of the energy consumption at the distributed house-holds. This work provides a comprehensive study on types of threats and solutions on smart grid communication and metering infrastructures. Recommended remedial actions are also identified.





Classification of attacks on Smart Metering System



Classification of different types of physical attacks

Communication System Attacks

➢ *Attacks on SMs through Power Line Carrier Communication (PLCC):*

- Any attacker with portable equipment such as current transformer can extract information tapping high frequency waves.
- The other drawback in PLCC is that the information transmitted from SM is not encrypted.

Available solutions:

- Cryptography: All the SM manufacturers should implement privacy and integrity controls to protect SM data which needs to confidential.

➢ *Attacks on SMs through Optical Fiber Communication (OFC):*

- In-band Jamming is the technique of using a high power transmitter to kill the signal on an OFC cable.
- Out-of-band Jamming is another kind of technique which exploits crosstalk in optical components.

Available solutions:

- Power Detection and Intrusion Detection Systems

Vulnerabilities And Solutions To Types Of Wireless Communications Technologies

Technology	Advantage	Vulnerabilities	Available Solutions
Wi-Fi	Open Standard, High throughput Strong Home market penetration Low cost Relatively secure communication	Traffic Analysis, Passive and active eavesdropping, Man-in-the-middle attack, session hijacking, and replay attacks.	Two way authentication, encryption.
ZigBee	high reliability, self-configuration and self-healing, Low power consumption, low cost	Jamming, Message capturing and tampering, Exhaustion	A utility gateway device between HAN and SM, authentication, encryption
Mobile Communications and Femtocells	Consistent coverage in office or home, less power consumption	Network and service availability disruption, Fraud and service theft, Privacy and confidentiality disruption	Two way authentication, encryption
WiMAX	High data rate (1 Gbps for stationary users), Low latency, Advanced Quality of Service (QoS), Sophisticated security	Ranging Attack (DoS attack, downgrading attack, water torture attack), Power Saving Attack, man-in-the-middle attack, Replay theft of service attack, Traffic analysis techniques	Encryption, Intrusion detection schemes, access control to specific applications
Long Term Evolution (LTE)	Less Interference , Resource efficient	Attacks on the air interface, Attacks on the e- NB, Attacks against the core network	Two way authentication, encryption, introduction of mobile virtual network operator (MVNO).

Conclusions

➢ The conventional security mechanisms for hardware, cyber space, and communication network are not adequate enough for SMs as they have additional set of constraints, such as limited memory and processing power, heterogeneous network architecture and physical exposure of the smart meters.

➢ To effectively thwart attacks on SM, security solutions for SM should be designed considering the constraints associated with SMs and power system as these SMs are part broader smart grid infrastructure.