Attack countermeasure strategies in power grid system

How to prevent stealth attack on power grid control system?
To prevent a stealth attack on a power grid control system,it is essential to have appropriate security management in addition to using security strategies. This includes security policies,strategies,and programs based on accurate threat and risk analysis.

How to protect a smart grid from cyberattacks?
This approach is crucial in protecting the smart grid from cyberattacks by facilitating self-healing mechanisms,such as the reconnection of Phasor Measurement Units (PMUs) and the restoration of system observability . In Fig. 13,we can observe the self-healing process of a smart grid,where it undergoes several steps.

How do we deter deliberate attacks on the power grid?
The analysis focuses on two strategies for deterring deliberate attacks on the power grid: denial and cost imposition. For deterrence by denial,the report focuses on "outside-the-fence" interventions--ways in which DoD can engage with entities or infrastructure not owned by DoD.

Are smart grid systems vulnerable to trespassing?
Critical vulnerabilities have been identified,as discussed in Refs. [33,34]. Physical security emerges as a primary vulnerability. Unlike conventional power systems,the smart grid network includes numerous components located outside the utility's premises,exposing them to physical trespassing risks.

How can smart grids mitigate DoS attacks?
To address the challenge of mitigating Denial of Service (DoS) attacks in smart grids,a multifaceted approach integrating various techniquesis essential,as highlighted in Ref. . Specifically,no single solution exists for DoS mitigation,necessitating the integration of multiple techniques.

How do attackers manipulate meter measurements?
Attackers can manipulate meter measurements in a smart power grid by either locally compromising meters or falsifying data packets that are sent to the control centre by exploiting the plaintext transmission protocol. Altering the control centre database is another method used by attackers.

Smart Grid (SG) technology utilizes advanced network communication and monitoring technologies to manage and regulate electricity generation and transport. However, this increased reliance on technology and connectivity also introduces new vulnerabilities, making SG communication networks susceptible to large-scale attacks. While previous surveys have ...

References [22], [23], and [24] provide detailed modeling, analysis, and countermeasures to power system

load redistribution (LR) attacks. References [25] and [26] establish a market-level defense ...

Understanding the ways to detect and deal with cyber threats in SGs will increase the resilience of power systems. In this paper, conceptual models of SG vulnerabilities are presented to ...

Excluding production-related grids such as Transmission, Distribution, and Micro, the smart grid"s power system comprises three basic grids. A shorter self-healing time in the ...

The smart grid has become a cyber-physical system and the more cyber it becomes, the more prone it is to cyber-attacks. One of the most important cyber-attacks in smart grids is false data ...

Liu X, Li Z, Li Z (2016) Optimal protection strategy against false data injection attacks in power systems. IEEE Trans Smart Grid 8(4):1802-1810. Article Google Scholar Liu C, Wu J, Long C et al (2018) Reactance perturbation for detecting and identifying fdi attacks in power system state estimation.

Smart power grid (SG) is a complex cyber-physical system incorporating the physical power system, and the computing, sensing technology, and communication systems. A smart grid manages the flow of electricity as well as information over its ...

This paper investigates CCPAs in smart grid and shows that an adversary can carefully synthesize a false data injection attack vector based on phasor measurement unit (PMU) measurements to neutralize the impact of physical attack vector, such that CCPAs could circumvent bad data detection without being detected. Smart grid, as one of the most critical ...

attacks in power system operations, respectively. References [22], [23], and [24] provide detailed modeling, analysis, and countermeasures to power system load redistribution (LR) at-tacks.References[25]and[26]establishamarket-leveldefense and analysis against power system false data injection attacks (FDIAs).

3 days ago· Cyber-attacks on power systems can have devastating effects, disrupting essential services and causing significant economic losses [].As power systems become increasingly ...

Smart grid, as one of the most critical infrastructures, is vulnerable to a wide variety of cyber and/or physical attacks. Recently, a new category of threats to smart grid, named coordinated cyber-physical attacks (CCPAs), are emerging. A key feature of CCPAs is to leverage cyber attacks to mask physical attacks which can cause power outages and potentially trigger ...

As a classic cyber-physical system, smart grids often suffer from various types of attacks, one of which the most threatening attacks is coordinated cyber-physical attack (CCPA). In order to improve the robustness of the smart grids against CCPA, we predict and simulate various possible attack scenarios, and propose three

attack strategies, such as optimal attack strategy ...

IET Cyber-Systems and Robotics; IET Electric Power Applications ... This paper provides a comprehensive and systematic review of the critical attack threats and defence strategies in the smart grid. We start this survey with an overview of the smart grid security from the CP perspective, and then focuses on prominent CP attack schemes with ...

In power grid applications, the false data injection attack is a well-known example of this. In FDIA, the power grid state-estimation systems are targeted in order to distort real energy supply and demand figures, which may ...

DOI: 10.1016/j.jisa.2020.102518 Corpus ID: 222006113; Survey of false data injection in smart power grid: Attacks, countermeasures and challenges @article{Aoufi2020SurveyOF, title={Survey of false data injection in smart power grid: Attacks, countermeasures and challenges}, author={Souhila Aoufi and Abdelouahid Derhab and Mohamed Guerroumi}, journal={J. Inf. Secur.

The SG is an electrical network, which can smartly combine the action of all the components that are connected to the system. In SG, power flow is bidirectional, which means utility to consumer and consumer to the utility if a surplus is available at the consumer''s end [].According to the National Institute of Standards and Technology (NIST), SG is described as ...

According to vulnerability reports from the US ICS-CERT [1] and Kaspersky ICS-CERT [2], the energy sector has reported the greatest number of vulnerabilities among all network infrastructures. Fig. 1 shows the number of vulnerabilities of various Industrial Control System (ICS) elements between 2010 and 2019 [1], [2].Accordingly, 178, 110, and 283 cyberattack ...

A Review of False Data Injection Attacks Against Modern Power Systems. IEEE Trans Smart Grid 2017;8(4):1630-8. Electricity Information Sharing and Analysis Center(E-ISAC). Analysis of the Cyber Attack on the Ukrainian Power Grid Table of Contents. 2016; Krebs B. FBI: Smart Meter Hacks Likely to Spread. 2012.

Once access to a machine in the office network has been gained, the attacker can passively listen for user credentials and search for, e.g., a VPN tunnel to the PCN. Lateral movement from the office network is one of the most dangerous attack vectors for power system operators. An attack would, however, be limited to a single network. 3.1.2.

Kim et al. [45] investigate constructing FDI attacks on the power grid based on linearized measurement models, and propose strategic countermeasures against such attacks, by either immunizing a ...

In power grid applications, the false data injection attack is a well-known example of this. In FDIA, the power

grid state-estimation systems are targeted in order to distort real energy supply and demand figures, which may cause blackouts, physical damage, or even the loss of human lives . FDIA attacks may also effectively become a denial-of ...

1.1 Adversary Models. Adversary model in general is composed of attack strategy and the adversary resources, that is the model (system) knowledge, disclosure, and disruption resources as discussed in [].Moreover, many well-known attack schemes can be conveniently categorized based on the adversary resources as depicted in Fig. 1.Model knowledge is the ...

The smart grid is one of the core technologies that enable sustainable economic and social developments. In recent years, various cyber attacks have targeted smart grid systems, which have led to ...

This paper proposes an attack strategy, maximum attacking strategy using spoofing and jamming (MASS-SJ), which utilizes an optimal power distribution to maximize the adversarial effects. As an emerging fast-growing technology, smart grid networks (SGNs) have been dramatically accepted by the current power supply industry for achieving high performance ...

The implementation of CCPAs in smart grid and the effectiveness of countermeasures are demonstrated by using an illustrative 4-bus power system and the IEEE 9-bus, 14-bus, 30- bus, 118-bus, and ...