Funded by the European Union NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | RAISE

Design and testing of solutions for quality of services and protection from cyberattacks in industrial-type networks with Machine Learning based approaches

Keywords: Cybersecurity, Industrial Control System, Monitoring, Machine Learning

Obiettivo del progetto

Il prototipo proposto, che sfrutta strumenti/funzionalità basati su AI/ML, propone strategie innovative di rilevamento delle anomalie, basate sull'osservazione del comportamento fisico del processo industriale monitorato. Gli algoritmi basati su AI/ML estraggono alcune misure dei parametri fisici del sistema e le elaborano con un'architettura di rete neurale per costruire un classificatore che prenda decisioni automatiche sul comportamento del sistema e rilevi guasti e potenziali attacchi informatici (ad esempio, Man-in-the-middle, spoofing, ecc.).

Breve descrizione del problema che la tecnologia risolve

Le reti di tipo industriale rappresentano la spina dorsale tecnologica di molte infrastrutture critiche, in quanto comprendono tutti i componenti funzionali che consentono un corretto monitoraggio e controllo di strutture e asset, come nel caso dei sistemi di alimentazione/energia, in particolare quelli che utilizzano fonti rinnovabili (FER) in continua diffusione, grazie agli aspetti legati alla sostenibilità e all'indipendenza energetica. Un'adozione così diffusa, rende potenzialmente le FER un obiettivo lucrativo per gli attacchi informatici soggette a costante minacce, a causa delle potenziali conseguenze catastrofiche quali: perdita di produzione di energia (e relativi ricavi), danni permanenti agli asset e alle infrastrutture, fuga di informazioni commerciali e danni alla reputazione, non conformità normativa e multe, e infine (per le infrastrutture critiche interconnesse/dipendenti) rischi per la salute, la sicurezza e l'ambiente.
Le soluzioni che migliorano la resilienza del sistema elettrico e delle FER incluse rappresentano un vantaggio strategico per la sicurezza economica e sociale.

Vantaggi

Nel campo dei processi industriali (e in particolare nei sistemi energetici), le strategie di rilevamento delle anomalie si basano sulla stima dinamica dello stato, composta dall'utilizzo di equazioni che descrivono il sistema fisico, e sul confronto tra il comportamento previsto e le misure reali. Seppur efficiente, tale approccio presenta alcuni svantaggi quali la conoscenza dell'esatto comportamento del sistema, cioè dei parametri esatti delle equazioni e la difficoltà di scrivere un'equazione che tenga conto di tipi eterogenei di parametri, che possono essere superate con l'approccio di Machine Learning (ML). In caso di studio di comportamenti fisici scorretti durante un cyberattacco diventa obbligatorio applicare un algoritmo in grado di "apprendere" un comportamento considerato normale e classificare nuovi esempi.
L'approccio proposto, definito come rilevamento di anomalie, o di "novelty", o di "outlier", supporta una strategia globale per il rilevamento tempestivo di condizioni di lavoro insolite: ad esempio una condizione di lavoro fisica indesiderata del processo, una deviazione del

processo da una condizione di lavoro nota definita normale, o come un'osservazione impossibile dello stato del processo a causa di un'incoerenza delle misurazioni.

Settori di potenziale applicazione della tecnologia sviluppata
Settore degli Operatori di Servizi Essenziali (OSE), con focus su reti di produzione di energia elettrica ed energie rinnovabili.

Potenziali utenti
Qualunque tipo di Industria

Prodotto finale
Prototipo di algoritmo di rilevamento delle anomalie.

Referenze
Risultati preliminari sono già stati pubblicati dal gruppo di ricerca; nel dettaglio:

- G. Gaggero, et al. “From Microgrids to Virtual Power Plants: a Cybersecurity Perspective”, CRC Press
- Gaggero, G. B., et al. "Industrial Control System-Anomaly Detection Dataset (ICS-ADD) for Cyber-Physical Security Monitoring in Smart Industry Environments." IEEE Access (2024).
- Gaggero, G. B., et al. "Should We Include Cyberdefense Functionalities in Electrical Power System Protections?: A Proposed Approach." *IEEE Industrial Electronics Magazine* (2024).

Indicazioni su possibili valorizzazioni

In valutazione il deposito di domanda di brevetto.

Collaborazioni con industrie.

Responsabili scientifici

Prof. Mario Marchese mario.marchese@unige.it

Prof.ssa Paola Girdinio paola.girdinio@unige.it

Prof. Giovanni Gaggero giovanni.gaggero@unige.it

Sito web

https://www.scnl.dist.unige.it/

Contatti/informazioni

Servizio per il trasferimento tecnologico e delle conoscenze
Settore valorizzazione della ricerca, trasferimento tecnologico e rapporti con le imprese
trasferimentotecnologico@unige.it
tel. 010 2095922