RdS
RICERCA DI SISTEMA

ENEA
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

Ricerca di Sistema elettrico

Datalake per sviluppo e test di algoritmi di anomaly detection nel contesto delle cybersecurity nelle reti elettriche (LA3.11)

S. De Vito

RdS_PTR 22-24_PR 2.1_LA3.11_091

DATALAKE PER SVILUPPO E TEST DI ALGORITMI DI ANOMALY DETECTION NEL CONTESTO DELLE CYBERSECURITY NELLE RETI ELETTRICHE

Autori Saverio De Vito, Ph.D (ENEA)

09/2023

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dell'Ambiente e della Sicurezza Energetica - ENEA
Piano Triennale di Realizzazione 2022-2024

Obiettivo: *Decarbonizzazione/Digitalizzazione ed evoluzione delle reti*
Linea di attività: *3.11*
Responsabile del Progetto: Maria Valenti, ENEA
Responsabile Linea di Attività: Saverio De Vito, ENEA
Mese inizio previsto: 06/2022
Mese inizio effettivo: 06/2022
Mese fine previsto: 06/2023
Mese fine effettivo: 06/2023

Indice

1 Risultati attesi

Realizzazione di un datalake per il test di algoritmi di anomaly detection nel contesto delle cybersecurity nelle reti elettriche (LA3.11)

2 Risultati ottenuti

Selezione di dataset per il test di algoritmi di anomaly detection nel contesto delle cybersecurity nelle reti elettriche (LA3.11). Realizzazione di una repository con dati localmente scaricati a beneficio delle attività di sviluppo degli algoritmi di anomaly detection per la detezione di cyberattacchi con particolare riferimetno alle attività di model selection e validazione.

3 Prodotti attesi

Repository contenente dati locali da dataset utilizzabili per sviluppo e validazione di algoritmi di anomaly detection per la detezione di cyberattacchi in contesti assimilabili alle microgrid.

4 Prodotti sviluppati

Repository contenente dati locali da dataset utilizzabili per sviluppo e validazione di algoritmi di anomaly detection per la detezione di cyberattacchi in contesti assimilabili alle microgrid.

5 Analisi degli scostamenti su attività e risultati

Non ci sono scostamenti significativi rispetto a quanto preventivato.

6 Sintesi delle attività svolte

E’ stata condotta un attività di studio e selezione della letteratura relativa ad algoritmi per la detezione di cyberattacchi in architetture microgrid o assimilabili con l’ intento di individuare un sottoinsieme di dataset utilizzabili per lo sviluppo la validazione e, infine, il test si algoritmi innovativi. I dataset selezionati essendo stati utilizzati almeno in parte per la validazione di algoritmi in letteratura permetteranno di costituire una base dati (datalake) con capacità di fornire risultati comparativi rispetto a quanto appunto presente in letteratura.

7 Dettaglio delle attività svolte

La selezione operata ha dato luogo ad un elenco di dataset e alla produzione di una breve descrizione per gli scopi specifici delle attività di riferimento. Le descrizioni contengono i parametri significativi per la scelta da effettuarsi in fase di validazione per ognuno degli algoritmi sviluppati.

Alcuni di questi dataset sono riferiti a scenari assimilabili in termini architetturali oppure in termini di problematiche descritte con particolare riferimento a quelli tra loro che contengono registrazioni di comunicazioni su protocolli standard. Le tracce registrate contengono infatti anomalie nella struttura delle comunicazioni piuttosto che nel contenuto originatesi dagli effetti diretti o indiretti degli attacchi reali o simualti che siano. Altri sono riferiti a sistemi complessi con problematiche similari alle microgrid in termini di effetti o di vulnerabilità e pure individuando sistemi cyberfisici sostanzialmente differenti sono stati utilizzati in letteratura per il test di algoritmi di anomaly detection nel settore della cybersecurity soprattutto in termini di false data injection e change detection.

Di seguito l' elenco e la descrizione dei dataset individuati:

C-MAPSS

Il dataset C-MAPSS della NASA è un set di dati simulato di un motore turbofan commerciale. Il dataset è stato creato utilizzando il simulatore C-MAPSS, che è un modello di sistema ad alto livello progettato per simulare il degrado dell'engine in condizioni nominali e in presenza di malfunzionamenti.
Il dataset C-MAPSS è composto da dati di 30 parametri, tra cui:

- Parametri di volo: altitudine, velocità, temperatura ambiente, etc.
- Parametri di salute dell'engine: temperatura dei gas di scarico, pressione dei cuscinetti, etc.
- Misurazioni di temperatura e pressione

I dati sono campionati a una frequenza di 1 Hz e coprono un totale di 7 condizioni di volo, per un volo di circa 90 minuti.
Il dataset è stato rilasciato dalla NASA nel 2008 ed è stato utilizzato da diversi ricercatori per sviluppare algoritmi di intelligenza artificiale per il monitoraggio e la diagnosi dei guasti dei motori turbofan.
Il dataset è disponibile per il download gratuito dal portale dati aperto della NASA.
Ecco alcuni esempi di come il dataset C-MAPSS può essere utilizzato:

- Per sviluppare algoritmi di intelligenza artificiale per il monitoraggio del degrado dell'engine
- Per valutare l'efficacia dei sistemi di manutenzione predittiva
- Per migliorare la progettazione dei motori turbofan

Nel nostro caso specifico esso può essere utilizzato come base dati nella quale iniettare anomalie per il test di algoritmi di anomaly detection da attacchi FDI.
Il dataset è inoltre orientato alla simulazione di motori turbofan commerciali. Strutturalmente, è composto da quattro sotto-dataset, ciascuno con dati di addestramento e dati di test. I dati di test includono dati di funzionamento fino al guasto di diversi motori dello stesso tipo.
Ogni riga nei dati di test rappresenta un'ora di funzionamento. I dati di una riga includono tra l' altro:

- L'ID del motore
- Il numero del ciclo operativo corrente
- Tre impostazioni operative
- 21 valori dei sensori

I dati delle serie temporali terminano quando viene rilevato un guasto.
In definitiva pur essendo sviluppato in un contesto specifico di manutenzione aeronautica può essere usato anche in termini di anomaly detection in contesti cyberfisici come in problematiche di sicurezza. In questo caso le anomalie da cyberattacco di tipo FDI sono "simulate" dalle anomalie dovute a malfunzionamenti del

sistema. Un recente esempio di questo utilizzo si trova nel lavoro Mode et al., "**Impact of False Data Injection Attacks on Deep Learning enabled Predictive Analytics",** 2020, IEEE/IFIP Network Operations and Management Symposium (NOMS).

Web page:
https://www.nasa.gov/intelligent-systems-division/discovery-and-systems-health/pcoe/pcoe-data-set-repository
Direct Download Link:
https://phm-datasets.s3.amazonaws.com/NASA/6.+Turbofan+Engine+Degradation+Simulation+Data+Set.zip

CSE-CIC-IDS2018

ll dataset CSE-CIC-IDS2018 è un set di dati di intrusion detection in reti creato da ricercatori del Canadian Institute of Cybersecurity (CIC) e del Communications Security Establishment (CSE). Il dataset include sette diversi scenari di attacco, simulati su un'infrastruttura di rete complessa che comprende 50 macchine di attacco e 420 macchine vittima. I dati del dataset includono il traffico di rete catturato e i log di sistema di ciascuna macchina, insieme a 80 metriche estratte dal traffico catturato utilizzando CICFlowMeter-V3. Il dataset è stato creato utilizzando un approccio sistematico basato sulla nozione di profili. I profili sono descrizioni astratte di eventi e comportamenti osservati sulla rete. I profili possono essere utilizzati per generare dataset di intrusion detection diversificati e completi, che coprono una porzione del dominio di valutazione. Inoltre, essi possono essere utilizzati da agenti o operatori umani per generare eventi sulla rete. Grazie alla natura astratta dei profili generati, possono essere applicati a una vasta gamma di protocolli di rete con topologie diverse. I profili possono essere utilizzati insieme per generare un dataset per esigenze specifiche. Il dataset CSE-CIC-IDS2018 include due classi distinte di profili:

- B-profili: Incapsulano i comportamenti degli utenti utilizzando varie tecniche di apprendimento automatico e analisi statistica. Le features incapsulate sono essenzialmente distribuzioni delle dimensioni dei pacchetti di un protocollo, numero di pacchetti per flusso, determinati schemi nel payload, dimensioni del payload e distribuzione del tempo di richiesta di un protocollo.

- M-profili: Tentano di descrivere uno scenario di attacco in modo non ambiguo. Nel caso più semplice, gli umani possono interpretare questi profili e successivamente eseguirli. Idealmente, nello scenario identificato, verrebbero invece impiegati agenti autonomi insieme a compilatori per interpretare ed eseguire questi scenari.

Gli scenari di attacco inclusi nel dataset CSE-CIC-IDS2018 possono essere ricondotti essenzialmente alle seguenti descrizioni:

- Infiltrazione della rete dall'interno, nella pratica si parte con l' invio di un file dannoso tramite e-mail alla vittima e sfruttamento di una vulnerabilità dell'applicazione. A seguito dell' exploitation, verrà eseguito un backdoor sul computer della vittima e quindi si utilizzerà il suo computer per scansionare la rete interna alla ricerca di altre caselle vulnerabili e sfruttarle se possibile.

- Negazione del servizio HTTP: Utilizzo di metodi basati su Slowloris e LOIC come strumenti principali, al fine di rendere i server Web della rete target completamente inaccessibili utilizzando una singola macchina di attacco. Slowloris inizia stabilendo una connessione TCP completa con il server remoto. Lo strumento mantiene la connessione aperta inviando richieste HTTP valide e

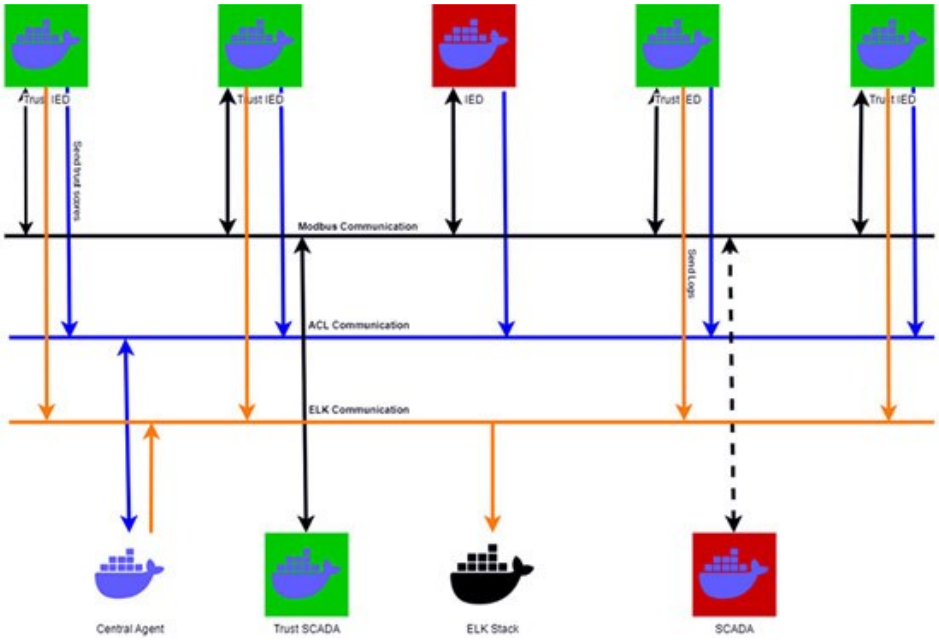
incomplete al server a intervalli regolari per impedire la chiusura dei socket. Poiché qualsiasi server Web ha una capacità finita di servire connessioni, sarà solo una questione di tempo prima che tutti i socket siano utilizzati e non sia possibile effettuare altre connessioni.

Web page:
https://www.nasa.gov/intelligent-systems-division/discovery-and-systems-health/pcoe/pcoe-data-set-repository
Direct Download Instructions page:
https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv/

CIC Modbus Dataset 2023

CIC Modbus Dataset (https://www.unb.ca/cic/datasets/modbus-2023.html) contiene acquisizioni di rete (pcap) e registri di attacchi da una rete di sottostazioni di potenza simulata. Il dataset è classificato in due gruppi: un dataset di attacchi e un dataset benigno.
Il dataset di attacchi include acquisizioni di traffico di rete che simulano vari tipi di attacchi al protocollo Modbus in un ambiente di sottostazione. Gli attacchi sono ricognizione, query flooding, invio di payload, ritardo della risposta, modifica dei parametri di lunghezza, iniezione di dati falsi, accatastamento di frame Modbus, scrittura brute force e riproduzione baseline. Questi attacchi si basano su alcune tecniche del framework MITRE ICS ATT&CK.
D'altra parte, il dataset benigno è costituito da acquisizioni di traffico di rete normali che rappresentano comunicazioni Modbus legittime all'interno della rete della sottostazione.
Lo scopo di questo dataset è facilitare la ricerca, l'analisi e lo sviluppo di sistemi di rilevamento delle intrusioni, algoritmi di rilevamento delle anomalie e altri meccanismi di sicurezza per le reti di sottostazioni che utilizzano il protocollo Modbus.

Complessivamente il CIC Modbus Dataset è stato generato attraverso segmenti di cattura ottenuti con Wireshark su un testbed simulato. La simulazione è costruita basandoti su ambienti Docker che vengono creati per rappresentare degli IED. Un numero limitato di component invece gioca il ruolo di HMI di SCADA.
La logica è implementata attraverso script python. Gli IED cambiano I valori di Voltaggio in maniera casual nel tempo oppure a seguito in una richiesta da parte di un componente HMI. Lo SCADA Segue invece normali regole di controllo con chiusure ed aperture regulate da condizioni di over o under voltage.
I containers eseguono sia il codice di controllo (scripts) sia i codici di detezione (Jar files) and scripts. E' possibile anche configurare la sola esecuzione della dinamica di controllo rendendo di fatto l' IED in oggetto un sistema inerentemente insicuro. Di converso gli IED o le HMI SCADA che eseguono anche il codice di detezione possono essere considerati oggetti sicuri. I componenti di detezione inviano gli eventi di rilevazione eventuali ad un sistema di raccolta centralizzato.



Industrial Control System (ICS) Cyber Attack Dataset 1 Power System Datasets

Il set di dati sugli attacchi ai sistemi di potenza ICS-CAD-1 (https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets#h.p_ID_32) è una raccolta di dati che descrive 37 scenari di eventi del sistema di alimentazione. Gli scenari sono divisi in tre categorie: eventi naturali, eventi nulli ed eventi di attacco.
Gli eventi naturali sono eventi che si verificano naturalmente nel sistema di potenza, come un cortocircuito. Gli eventi nulli sono eventi che non hanno alcun impatto sul sistema di alimentazione. Gli eventi di attacco sono eventi che sono stati creati da un attaccante per danneggiare il sistema di alimentazione.
Come accennato, il dataset è stato generato utilizzando un modello di simulazione che rappresenta un sistema di alimentazione a due linee con quattro interruttori. Il modello include i seguenti componenti:

- Due generatori di energia
- Quattro dispositivi elettronici intelligenti (IED) che controllano gli interruttori
- Due linee di trasmissione

Le features del dataset includono le seguenti informazioni:

- La posizione del cortocircuito (per gli eventi di guasto da cortocircuito)
- Lo stato degli interruttori (per tutti gli scenari)
- I parametri del sistema di potenza (per gli eventi di attacco)

Il set di dati è disponibile in due formati: ARFF (WEKA) e CSV.
Il dataset ICS-CAD-1 può essere utilizzato per sviluppare e valutare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per i sistemi di alimentazione. Può anche essere utilizzato per comprendere meglio i diversi tipi di attacchi che possono essere lanciati contro i sistemi di alimentazione.
Riepilogando, i tipi di scenari inclusi nel set di dati sono i seguenti:
Guasto da cortocircuito: si tratta di un cortocircuito su una linea elettrica che può verificarsi in vari punti lungo la linea. La posizione è indicata dall'intervallo percentuale sulla lunghezza della linea.

Manutenzione linee: uno o più relè vengono disattivati su una linea specifica per eseguire la manutenzione di quella linea.
Iniezione di comandi di switch remoto (attacco): si tratta di un attacco che invia un comando a un relè che provoca l'apertura di un interruttore. Può essere eseguito solo dopo che un aggressore ha penetrato le difese esterne.
Modifica dell'impostazione del relè (attacco): i relè sono configurati con uno schema di protezione di distanza e l'aggressore modifica l'impostazione per disabilitare la funzione del relè, in modo che il relè non scatti per un guasto valido o un comando valido.
Iniezione di dati (attacco): in questo caso si imita un guasto valido modificando i valori dei parametri del sistema di alimentazione, come la tensione e la corrente.
Ovviamente, quest' ultimo caso rappresenta il caso d' uso più interessante per i nostri scopi.

Web page:
https://www.unb.ca/cic/datasets/modbus-2023.html
Direct Download Instructions page:
https://www.unb.ca/cic/datasets/modbus-2023.html

HAI Security Dataset

L'insieme di dati HAL-based augmented ICS (HAI) security dataset è un set di dati di dati operativi ICS da situazioni normali e anormali per 38 attacchi. È stato sviluppato per la ricerca sulla rilevazione delle anomalie nei sistemi cibernetici-fisici (CPS).
Il set di dati è stato raccolto da un banco di prova ICS realistico aumentato con un simulatore HIL (hardware-in-the-loop) che emula la generazione di energia da turbina a vapore e la generazione di energia idroelettrica a pompaggio.
Il banco di prova HAI è infatti composto da componenti fisici quali una caldaia, una turbina, un componente di trattamento dell'acqua, e appunto, un simulatore HIL. I tre processi del mondo reale, ovvero la caldaia, la turbina e i processi di trattamento delle acque, sono controllati da tre diversi controllori ad-hoc.
Ne esistono diverse versioni infatti, il dataset HAI è stato rilasciato in diverse versioni, a partire dalla versione 20.07 nel luglio 2020. La versione più recente, HAI 23.05, è stata rilasciata nel 2022.
Le versioni successive hanno apportato miglioramenti alla qualità dei dati e alla copertura delle minacce.
Il datset HAI è un'importante risorsa per la ricerca sulla rilevazione delle anomalie nei CPS. È stato utilizzato in numerose competizioni di rilevamento delle minacce e ha contribuito a migliorare la precisione dei metodi di rilevamento delle anomalie.

Web page:
https://www.unb.ca/cic/datasets/modbus-2023.html
Direct Download Instructions page:
https://www.kaggle.com/datasets/icsdataset/hai-security-dataset

The Numenta Anomaly Benchmark (NAB)

NAB è un toolset usato diverse volte in pubblicazioni scientifiche creato appunto per rappresetnare un benchmark per valutare gli algoritmi per la rilevazione di anomalie in applicazioni di streaming e real-time. La sua base dati è composta da oltre 50 file di dati temporali etichettati provenienti da fonti reali e artificiali ed un meccanismo di punteggio innovativo progettato per applicazioni real-time. Questa base dati contiene diversi dataset da misure reali tra cui:
realAWSCloudwatch:

Contiene metriche da servers AWS collezionate da AmazonCloudwatch service. (CPU Utilization, Network Bytes In, and Disk Read Bytes)
rogue_agent_key_hold: Contiene I tempi di ritenuta dei tasti della tastiera per diversi utenti di computers. Il cambio dell' utente rappresenta un anomalia rilevabile.
rogue_agent_key_updown: Timing the key strokes for several users of a computer, where the anomalies represent a change in the user.
realTraffic:
Dati reali di occupazione velocità e tempo di transito da una città dello stato del Minnesota.
Questi sottoinsiemi dati possono essere utilizzati per i test preliminari degli algoritmi individuati.

Web page:
https://www.kaggle.com/datasets/boltzmannbrain/nab
Direct Download Instructions page:
https://github.com/numenta/NAB/tree/master/data/realAWSCloudwatch

Aposemat IoT-23

Il dataset IoT-23 contiene 20 acquisizioni di malware eseguite su dispositivi IoT e 3 acquisizioni di traffico di dispositivi IoT benigni. È stato pubblicato nel 2020 e contiene traffico di rete IoT catturato dal 2018 al 2019.
Il dataset è diviso in 23 scenari, di cui 20 sono di malware e 3 sono benigni. Gli scenari di malware sono stati creati eseguendo campioni specifici di malware su Raspberry Pi. Gli scenari benigni sono stati creati catturando il traffico di rete di tre dispositivi IoT reali: una lampada LED intelligente Philips HUE, un assistente personale intelligente domestico Amazon Echo e una serratura intelligente Somfy.
Sia gli scenari di malware che quelli benigni sono stati eseguiti in un ambiente di rete controllato con connessione Internet senza restrizioni.
L'obiettivo del dataset IoT-23 è fornire ai ricercatori un ampio dataset di traffico di rete IoT reale e etichettato. Questo dataset può essere utilizzato per sviluppare algoritmi di machine learning per rilevare e prevenire le minacce alla sicurezza degli IoT.
Web page:
https://www.stratosphereips.org/blog/2020/1/22/aposemat-iot-23-a-labeled-dataset-with-malicious-and-benign-iot-network-traffic
Direct Download page:
https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/iot_23_datasets_full.tar.gz

RIFERIMENTI BIBLIOGRAFICI

(Beg et al., 2017) O.A.. Beg; T.T. Johnson; A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids", IEEE Trans.Industrial Informatics, vol. 13, no. 5, pp. 2693-2703, 2017

(Cui et al., 2021) H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi and H. M. A. Aljahdali, "Cyber Attack Detection Process in Sensor of DC Micro-Grids Under Electric Vehicle Based on Hilbert–Huang Transform and Deep Learning," in IEEE Sensors Journal, vol. 21, no. 14, pp. 15885-15894, 15 July15, 2021, doi: 10.1109/JSEN.2020.3027778.

(Choi et al., 2023) Choi, J., Roshanzadeh, B., Martínez-Ramón, M., Bidram, A.: An unsupervised cyberattack detection scheme for AC microgrids using Gaussian process regression and one-class support vector machine anomaly detection. IET Renew. Power Gener. 17, 2113–2123 (2023). https://doi.org/10.1049/rpg2.12753

(Durairaj et al, 2022) Danalakshmi Durairaj, Thiruppathy Kesavan Venkatasamy, Abolfazl Mehbodniya, Syed Umar & Tanweer Alam (22 Jan 2022): Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network, Energy Sources, Part A: Recovery, Utilization, and Environmental Effects

(De Dutta and Prasad, 2020) S. De Dutta and R. Prasad, "Cybersecurity for Microgrid," 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), Okayama, Japan, 2020, pp. 1-5, doi: 10.1109/WPMC50192.2020.9309494.

(Dehghani et al., 2021) Dehghani, M.; Niknam, T.; Ghiasi, M.; Bayati, N.; Savaghebi, M. Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach. Electronics 2021, 10, 1914. [CrossRef]

(Durairaj et al., 2022) Durairaj, D.; Venkatasamy, T.K.; Mehbodniya, A.; Umar, S.; Alam, T. Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network. Energy Sources Part A Recover. Util. Environ. Eff. 2022, 44, 1–23.

(Duan et al., 2017) J. Duan; W. Zeng ; M.Y. Chow, "Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack", IEEE Trans. Smart Grid, vol. 9, no. 4, pp. 3543 – 3552, 2018.][Q. Yang, D. Li ; W. Yu ; Y. Liu ; D. An ; X. Yang ; J. Lin, "Toward Data Integrity Attacks Against Optimal Power Flow in Smart Grid", IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1726 – 1738, 2017

(Gallo et al., 2018) Gallo, A.J.; Turan, M.S.; Boem, F.; Ferrari-Trecate, G.; Parisini, T. Distributed watermarking for secure control of microgrids under replay attacks. IFAC-PapersOnLine 2018, 51, 182–187. [CrossRef]

(Jamil et al., 2021) Jamil, N.; Qassim, Q.S.; Bohani, F.A.; Mansor, M.; Ramachandaramurthy, V.K. Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. Appl. Sci. 2021, 11, 9812. https://doi.org/10.3390/app11219812

(Khaledian et al., 2021) Khaledian et al.: Real time synchrophasor data anomaly detection and classification using isolation forest, kmeans and LoOP, IEEE Transactions on Smart Grid, 2021, doi:10.1109/tsg.2020.3046602

(Kavousi-Fard et al., 2021) A. Kavousi-Fard, W. Su and T. Jin, "A Machine-Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids," in IEEE Transactions on Industrial Informatics, vol. 17, no. 1, pp. 650-658, Jan. 2021, doi: 10.1109/TII.2020.2964704.

(Kuruvila, A.P. et al., 2021) Kuruvila, A.P.; Zografopoulos, I.; Basu, K.; Konstantinou, C. Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids. Int. J. Electr. Power Energy Syst. 2021, 132, 107150.

(Liu et al., 2021) Liu, S.; Siano, P.; Wang, X. Intrusion-detector-dependent frequency regulation for microgrids

(Ma et al., 2020) Ma, M.; Lahmadi, A.; Chrisment, I. Detecting a Stealthy Attack in Distributed Control for Microgrids using Machine Learning Algorithms. In Proceedings of the 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), Tampere, Finland,10–12 June 2020; IEEE: Piscataway, NJ, USA, 2020; Volume 1, pp. 143–148.

(Marino et al., 2019) D. L. Marino et al., "Cyber and Physical Anomaly Detection in Smart-Grids," 2019 Resilience Week (RWS), San Antonio, TX, USA, 2019, pp. 187-193, doi: 10.1109/RWS47064.2019.8972003.

(Nejabatkhah et al., 2021) Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. Energies 2021, 14, 27. https://doi.org/10.3390/en14010027

(Panthi et al., 2020) M. Panthi, "Anomaly Detection in Smart Grids using Machine Learning Techniques," 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 2020, pp. 220-222, doi: 10.1109/ICPC2T48082.2020.9071434.

(Sadi et al., 2022) Sadi, M.A.H.; Zhao, D.; Hong, T.; Ali, M.H. Time Sequence Machine Learning-Based Data Intrusion Detection for Smart Voltage Source Converter-Enabled Power Grid. IEEE Syst. J. 2022 , 16. [CrossRef]

(Takiddin et al., 2022) A. Takiddin, S. Rath, M. Ismail and S. Sahoo, "Data-Driven Detection of Stealth Cyber-Attacks in DC Microgrids," in IEEE Systems Journal, vol. 16, no. 4, pp. 6097-6106, Dec. 2022, doi: 10.1109/JSYST.2022.3183140.

(Tang et al., 2018) Tang, Z.; Lin, Y.; Vosoogh, M.; Parsa, N.; Baziar, A.; Khan, B. Securing microgrid optimal energy management using deep generative model. IEEE Access 2021, 9, 63377–63387., Gallo, A.J.; Turan, M.S.; Boem, F.; Ferrari-Trecate, G.; Parisini, T. Distributed watermarking for secure control of microgrids under replay attacks. IFAC-PapersOnLine 2018, 51, 182–187.

(Toker et al., 2022) O. Toker and M. R. Khalghani, "Cyber Anomaly Detection Design for Microgrids using an Artificial Intelligent-Based Method," 2022 North American Power Symposium (NAPS), Salt Lake City, UT, USA, 2022, pp. 1-5, doi: 10.1109/NAPS56150.2022.10012203.

(Xi et al., 2020) Xi, W.; He, S.; Chen, R.; Xu, Y.; Li, W.; Zhou, G.; Yu, W.; He, H.; Huang, Z.; Yu, Y.; et al. Research on attack detection method of microgrid central controller based on convolutional neural network. In Journal of Physics: Conference Series; IOP Publishing: Bristol, UK, 2020; Volume 1646, p. 012076.

8 Contributo delle eventuali consulenze alle attività sopra descritte

N/A

9 Pubblicazioni scientifiche

Elenco delle pubblicazioni scientifiche eventualmente risultanti dall'attività svolta

N/A

10 Eventi di disseminazione

Lista degli eventi di disseminazione eventualmente scaturiti dall'attività svolta

N/A