Document type
Article

Source type
Journal

ISSN
02676192

DOI
10.32604/CSSE.2021.014384

Publisher
Tech Science Press

CODEN
CSSEE

Original language
English

View less

Computer Systems Science and Engineering • Open Access • Volume 37, Issue 1, Pages 33 - 46 • February 2021

Anomaly detection in ICS datasets with machine learning algorithms

Mubarak S.[a], Habaebi M.H.[a], Islam M.R.[a], Rahman F.D.A., Tahir M.[b]

Save all to author list

[a] International Islamic University Malaysia, Jalan Gombak, 53100, Malaysia

[b] Sunway University, Selangor, 47500, Malaysia

Abstract

An Intrusion Detection System (IDS) provides a front-line defense mechanism for the Industrial Control System (ICS) dedicated to keeping the process operations running continuously for 24 hours in a day and 7 days in a week. A well-known ICS is the Supervisory Control and Data Acquisition (SCADA) system. It supervises the physical process from sensor data and performs remote monitoring control and diagnostic functions in critical infrastructures. The ICS cyber threats are growing at an alarming rate on industrial automation applications. Detection techniques with machine learning algorithms on public datasets, suitable for intrusion detection of cyber-attacks in SCADA systems, as the first line of defense, have been detailed. The machine learning algorithms have been performed with labeled output for prediction classification. The activity traffic between ICS components is analyzed and packet inspection of the dataset is performed for the ICS network. The features of flow-based network traffic are extracted for behavior analysis with port-wise profiling based on the data baseline, and anomaly detection classification and prediction using machine learning algorithms are performed.

Author keywords

Anomaly detection; Industrial control system; Intrusion detection system; Machine learning; SCADA

Engineering controlled terms

Anomaly detection; Computer crime; Intrusion detection; Machine learning; Network security; SCADA systems

Engineering uncontrolled terms

Diagnostic functions; Flow-based network traffic; Industrial automation applications; Industrial control systems; Intrusion Detection Systems; Process operation; Remote monitoring; Supervisory control and dataacquisition systems (SCADA)

Engineering main heading

Learning algorithms

Topic cluster

SCADA System; Supervisory Control; Intrusion Detection

Prominence percentile

99.07629

Funding sponsor	Funding number	Acronym
International Islamic University Malaysia	P-RIGS18-003-0003	IIUM

See opportunities by IIUM

Funding text

Funding Statement: This work was conducted at the IoT and wireless communication protocols laboratory, International Islamic University Malaysia and is partially sponsored by the Publication-Research initiative grant scheme no. P-RIGS18-003-0003.

References (20)

View in search results format >

All

Export Print E-mail Save to PDF Create bibliography

1 (2013) *Security for industrial automation and control systems, Part 3-3: System Security Requirements and Security Levels*. Cited 27 times.
ISA

2 McMillen, D.
(2016) *Security attacks on industrial control systems*
[Online]. Available
https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

3 Van, L.
(2015) *Sequential detection and isolation of cyber-physical attacks on SCADA systems*
Ph.D. Thesis. University of Technology of Troyes

4 Keshk, M., Moustafa, N., Sitnikova, E., Creech, G.
Privacy preservation intrusion detection technique for SCADA systems (Open Access)

(2017) *2017 Military Communications and Information Systems Conference, MilCIS 2017 - Proceedings*, 2017-December, pp. 1-6. Cited 18 times.
ISBN: 978-150904003-2
doi: 10.1109/MilCIS.2017.8190422

View at Publisher

5 Maglaras, L. A., Jiang, J.
(2018) *Intrusion detection in SCADA systems using machine learning techniques*
Ph.D. Thesis. University of Huddersfield, UK

6 Qassim, Q., Ahmad, A.R., Ismail, R., Abu Bakar, A., Abdul Rahim, F., Mokhtar, M.Z., Ramli, R., (...), Mahdi, M.N.

An Anomaly Detection Technique for Deception Attacks in Industrial Control Systems

(2019) *Proceedings - 5th IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2019, 5th IEEE International Conference on High Performance and Smart Computing, HPSC 2019 and 4th IEEE International Conference on Intelligent Data and Security, IDS 2019*, art. no. 8819478, pp. 267-272.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/mostRecentIssue.jsp?punumber=8809626
ISBN: 978-172810006-7
doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00057

View at Publisher

7 Lopez Perez, R., Adamsky, F., Soua, R., Engel, T.

Machine Learning for Reliable Network Attack Detection in SCADA Systems (Open Access)

(2018) *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, art. no. 8455962, pp. 633-638. Cited 12 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/mostRecentIssue.jsp?punumber=8454845
ISBN: 978-153864387-7
doi: 10.1109/TrustCom/BigDataSE.2018.00094

View at Publisher

8 Solomon, I., Jatain, A., Shalini, B.
Neural network-based intrusion detection: State of the art
(2019) *India: International Conf. on Sustainable Computing in Science, Technology and Management (SUSCOM-2019)*
Amity University Rajasthan

9 Foley, J., Moradpoor, N., Ochenyi, H.

Employing a Machine Learning Approach to Detect Combined Internet of Things Attacks against Two Objective Functions Using a Novel Dataset (Open Access)

(2020) *Security and Communication Networks*, 2020, art. no. 2804291. Cited 3 times.
https://www.hindawi.com/journals/scn/
doi: 10.1155/2020/2804291

View at Publisher

10 Almalawi, A., Yu, X., Tari, Z., Fahad, A., Khalil, I.

An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems

(2014) *Computers and Security*, 46, pp. 94-110. Cited 68 times.
doi: 10.1016/j.cose.2014.07.005

View at Publisher

11 Sheykhkanloo, N.M., Hall, A.

Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset

(2020) *International Journal of Cyber Warfare and Terrorism*, 10 (2), pp. 1-26. Cited 3 times.
www.igi-global.com/journal/international-journal-cyber-warfare-terrorism/1167
doi: 10.4018/IJCWT.2020040101

View at Publisher

12 Teixeira, M.A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., Samaka, M.
SCADA system testbed for cybersecurity research using machine learning approach (Open Access)

(2018) *Future Internet*, 10 (8), art. no. 76. Cited 21 times.
http://www.mdpi.com/1999-5903/10/8/76/pdf
doi: 10.3390/fi10080076

View at Publisher

13 Robles-Durazno, A., Moradpoor, N., McWhinnie, J., Russell, G.
A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system

(2018) *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, art. no. 8560683. Cited 11 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/mostRecentIssue.jsp?punumber=8537418
ISBN: 978-153864683-0
doi: 10.1109/CyberSecPODS.2018.8560683

View at Publisher

14 Turnipseed, I.
(2015) *A new SCADA dataset for intrusion detection research*. Cited 15 times.
Ph.D. Thesis. Mississippi State University, USA

15 Polyakov, A.
Machine learning for cybersecurity 101, Dzone
(2018) . Cited 2 times.
AI Zone, [Online]. Available
https://dzone.com/articles/machine-learning-for-cybersecurity-101

16 Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S.
Deep Learning Approach for Intelligent Intrusion Detection System (Open Access)

(2019) *IEEE Access*, 7, art. no. 6287639, pp. 41525-41550. Cited 202 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/RecentIssue.jsp?punumber=6287639
doi: 10.1109/ACCESS.2019.2895334

View at Publisher

17 Singh, P.
(2018) *Machine learning with PySpark*. Cited 7 times.
Apress, Springer Nature Publishing Co., NY, USA

18 Almehmadi, A.
SCADA networks anomaly-based intrusion detection system
(2018) *SIN'18: Proceedings of the 11th Int. Conf. on Security of Information and Networks*, pp. 1-4. Cited 3 times.
Cardiff, UK

19 Malaiya, R.K., Kwon, D., Suh, S.C., Kim, H., Kim, I., Kim, J.

An Empirical Evaluation of Deep Learning for Network Anomaly Detection (Open Access)

(2019) *IEEE Access*, 7, art. no. 8846674, pp. 140806-140817. Cited 9 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/RecentIssue.jsp?punumber=6287639
doi: 10.1109/ACCESS.2019.2943249

View at Publisher

20 Duque Anton, S., Ahrens, L., Fraunholz, D., Schotten, H.D.

Time is of the essence: Machine learning-based intrusion detection in industrial time series data (Open Access)

(2019) *IEEE International Conference on Data Mining Workshops, ICDMW*, 2018-November, art. no. 8637462, pp. 1-6. Cited 8 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/conhome.jsp?punumber=1001620
ISBN: 978-153869288-2
doi: 10.1109/ICDMW.2018.00008

View at Publisher

Habaebi, M.H.; International Islamic University Malaysia, Jalan Gombak, Malaysia; email:habaebi@iium.edu.my

Back to results | 1 of 1

Top of page