Scopus

Documents

Balla, A.[a] , Habaebi, M.H.[a] , Elsheikh, E.A.A.[b] , Islam, M.R.[a] , Suliman, F.E.M.[b] , Mubarak, S.[a]

Enhanced CNN-LSTM Deep Learning for SCADA IDS Featuring Hurst Parameter Self-Similarity
(2024) *IEEE Access*, 12, pp. 6100-6116. Cited 4 times.

DOI: 10.1109/ACCESS.2024.3350978

[a] International Islamic University Malaysia, Department of Electrical and Computer Engineering, Kuala Lumpur, 53100, Malaysia
[b] King Khalid University, College of Engineering, Department of Electrical Engineering, Abha, 61421, Saudi Arabia

Abstract
Supervisory Control and Data Acquisition (SCADA) systems are crucial for modern industrial processes and securing them against increasing cyber threats is a significant challenge. This study presents an advanced method for bolstering SCADA security by employing a modified hybrid deep learning model. A key innovation in this work is integrating the Self-similarity Hurst parameter into the dataset alongside a CNN-LSTM model, significantly boosting the Intrusion Detection System's (IDS) capabilities. The Hurst parameter, which quantifies the self-similarity in a dataset, is instrumental in detecting anomalies. Our in-depth analysis of the CICIDS2017 dataset sheds light on contemporary attack patterns and network traffic behaviors. The CNN-LSTM architecture was substantially altered by adding multiple convolutional layers with progressively increasing filters, batch normalization for stable training, and dropout layers for regularization. Principal Component Analysis (PCA) was applied for dimensionality reduction, thereby optimizing the dataset. Test results demonstrate the superior performance of the model incorporating the Hurst parameter, achieving 95.21% accuracy and 82.59% recall, significantly surpassing the standard model. The inclusion of the Hurst parameter marks a substantial advancement in identifying emerging threats, while architectural improvements to the CNN-LSTM model led to more robust and accurate intrusion detection in industrial control settings. © 2013 IEEE.

Author Keywords
binary classification; Deep learning; Hurst parameter; intrusion detection system; self-similarity; supervisory control and data acquisition

Index Keywords
Classification (of information), Computer crime, Convolution, Long short-term memory, Network security, Principal component analysis, SCADA systems; Anomaly detection, Binary classification, Convolutional neural network, Deep learning, Hurst parameter, Intrusion Detection Systems, Intrusion-Detection, Security, Self-similarities, Supervisory control and data acquisition; Intrusion detection

References

- Wali, A.
(2022) *Analysis of Security Challenges in Cloud-based Scada Systems: A Survey*, Tech. Rep., Jul.

- Aghenta, L.O., Iqbal, M.T.
Low-cost, open source IoT-based SCADA system design using Thinger.IO and ESP32 thing
(2019) *Electronics*, 8 (8), p. 822.
Jul.

- Rabie, O., Balachandran, P., Khojah, M., Selvarajan, S.
A proficient ZESO-DRKFC model for smart grid SCADA security
(2022) *Electronics*, 11 (24), p. 4144.
Dec.

- Bhavsar, M., Roy, K., Kelly, J., Olusola, O.
Anomaly-based intrusion detection system for IoT application
(2023) *Discover Internet Things*, 3 (1), p. 5.
May

- Laghrissi, F., Douzi, S., Douzi, K., Hssina, B.
Intrusion detection systems using long short-Term memory (LSTM)
(2021) *J. Big Data*, 8 (1), p. 65.
Dec.

- Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A.
Toward generating a new intrusion detection dataset and intrusion traffic characterization
(2018) *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, pp. 108-116.

- Shurman, M., Khrais, R., Yateem, A.
DoS and DDoS attack detection using deep learning and IDS
(2020) *Int. Arab J. Inf. Technol.*, 17 (4), pp. 655-661.
Jul.

- Kim, A., Park, M., Lee, D.H.
AI-IDS: Application of deep learning to real-Time web intrusion detection
(2020) *Ieee Access*, 8, pp. 70245-70261.

- Ethala, S., Kumarappan, A.
A hybrid spider monkey and hierarchical particle swarm optimization approach for intrusion detection on Internet of Things
(2022) *Sensors*, 22 (21), p. 8566.
Nov.

- Altunay, H.C., Albayrak, Z.
A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks
(2023) *Eng. Sci. Technol., Int. J.*, 38.
Feb., Art. no. 101322

- Babiker, A.B., Habaebi, M.H., Mubarak, S., Islam, M.R.
A detailed analysis of public industrial control system datasets
(2023) *Int. J. Secur. Netw.*, 18 (4), pp. 245-263.

- Miele, E.S., Bonacina, F., Corsini, A.
Deep anomaly detection in horizontal axis wind turbines using graph convolutional autoencoders for multivariate time series
(2022) *Energy Ai*, 8.
May, Art. no. 100145

- Hnamte, V., Hussain, J.
Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach
(2023) *Telematics Informat. Rep.*, 11.
Sep., Art. no. 100077

- Yu, S.J., Koh, P., Kwon, H., Kim, D.S., Kim, H.K.
Hurst parameter based anomaly detection for intrusion detection system
(2016) *Proc. Ieee Int. Conf. Comput. Inf. Technol. (CIT).*, pp. 234-240.
Dec.

- Fernandes, D.A.B., Neto, M., Soares, L.F.B., Freire, M.M., Inacio, P.R.M.
On the self-similarity of traffic generated by network traffic simulators
(2015) *Modeling and Simulation of Computer Networks and Systems.*, pp. 285-311.
U.K.: Elsevier

- Kwak, B.I., Han, M.L., Kim, H.K.
Cosine similarity based anomaly detection methodology for the CAN bus
(2021) *Exp. Syst. Appl.*, 166.
Mar., Art. no. 114066

- Alsaeedi, A.H., Alfoudi, A., Manickam, S., Nuiaa, R.R., Dohan, M.I.
  Dynamic evolving Cauchy possibilistic clustering based on the selfsimilarity principle (DECS) for enhancing intrusion detection system
  (2022) *Int. J. Intell. Eng. Syst.*, 15 (5), pp. 252-260.

- Kotenko, I., Saenko, I., Lauta, O., Kribel, A.
  An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity
  (2020) *Energies*, 13 (19), p. 5031.
  Sep.

- Deka, R.K., Bhattacharyya, D.K.
  Self-similarity based DDoS attack detection using Hurst parameter
  (2016) *Secur. Commun. Netw.*, 9 (17), pp. 4468-4481.
  Nov.

- Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., Pieniak, D., Su, J.
  A software deep packet inspection system for network traffic analysis and anomaly detection
  (2020) *Sensors*, 20 (6), p. 1637.
  Mar.

- Balla, A., Habaebi, M.H., Elsheikh, E.A.A., Islam, M.R., Suliman, F.M.
  The effect of dataset imbalance on the performance of SCADA intrusion detection systems
  (2023) *Sensors*, 23 (2), p. 758.
  Jan.

- Mondal, M.A., Rehena, Z.
  Road traffic outlier detection technique based on linear regression
  (2020) *Proc. Comput. Sci.*, 171, pp. 2547-2555.
  Jan.

- Reddy, G.T., Reddy, M.P.K., Lakshmanna, K., Kaluri, R., Rajput, D.S., Srivastava, G., Baker, T.
  Analysis of dimensionality reduction techniques on big data
  (2020) *Ieee Access*, 8, pp. 54776-54788.

- Tang, D., Feng, Y., Zhang, S., Qin, Z.
  FR-RED: Fractal residual based real-Time detection of the LDoS attack
  (2021) *Ieee Trans. Rel.*, 70 (3), pp. 1143-1157.
  Sep.

- Ramli, K., Hayati, N., Ihsanto, E., Gunawan, T.S., Halbouni, A.H.
  Development of intrusion detection system using residual feedforward neural network algorithm
  (2021) *Proc. 4th Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI).*, pp. 539-543.
  Dec.

- Alzubaidi, L., Zhang, J., Humaidi, A.J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Farhan, L.
  Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions
  (2021) *J. Big Data*, 8 (1), pp. 1-74.
  Mar.

- Powers, D.M.
  Evaluation: From precision, recall and F-factor to ROC, informedness, markedness & correlation

(2008) *J. Mach. Learn. Technol.*,
[Online]

- Wang, Z., Xie, W., Wang, B., Tao, J., Wang, E.
A survey on recent advanced research of CPS security
(2021) *Appl. Sci.*, 11 (9), p. 3751.
Apr.

- Halbouni, A., Gunawan, T.S., Habaebi, M.H., Halbouni, M., Kartiwi, M., Ahmad, R.
CNN-LSTM: Hybrid deep neural network for network intrusion detection system
(2022) *Ieee Access*, 10, pp. 99837-99849.

- Singh, V.K., Ebrahem, H., Govindarasu, M.
Security evaluation of two intrusion detection systems in smart grid SCADA environment
(2018) *Proc. North Amer. Power Symp. (NAPS)*, pp. 1-6.
Fargo, ND, USA, Sep.

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

Publisher: Institute of Electrical and Electronics Engineers Inc.

ISSN: 21693536
Language of Original Document: English
Abbreviated Source Title: IEEE Access
2-s2.0-85182354176
Document Type: Article
Publication Stage: Final
Source: Scopus