

## 4 documents have cited:

VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model

Almahadin G., Aoudni Y., Shabaz M., Agrawal A.V., Yasmin G., Alomari E.S., Al-Khafaji H.M.R., (...), Maaliw R.R.

(2024) IEEE Transactions on Consumer Electronics, 70 (1) , pp. 4548-4555.

Search within results...



### Refine results

Limit to Exclude

#### Open Access

- ☐ All Open Access (3) >
- ☐ Gold (1) >
- ☐ Hybrid Gold (1) >
- ☐ Bronze (1) >

Learn more

#### Year

- ☐ 2024 (4) >

#### Author name

- ☐ Behera, P.K. (1) >
- ☐ Chakraborty, C. (1) >
- ☐ Dansana, D. (1) >
- ☐ Huang, C. (1) >
- ☐ Jamali, A. (1) >
- ☐ Lasisi, A. (1) >
- ☐ Naja, N. (1) >
- ☐ Naveed, Q.N. (1) >
- ☐ Nguyen, A.T. (1) >
- ☐ Nissar, N. (1) >

View less

View all

#### Subject area

- ☐ Engineering (3) >
- ☐ Computer Science (2) >
- ☐ Materials Science (1) >

#### Document type

- ☐ Article (3) >
- ☐ Editorial (1) >

#### Source title

### Analyze search results

Hide all abstracts Sort on: [Date \(newest\)](#)

☐ All [Export](#) [Download](#) [Citation overview](#) [View cited by](#) [Save to list](#) [...](#) [🖨](#) [✉](#) [📄](#)

	Document title	Authors	Year	Source	Cited by
<input type="checkbox"/> 1	Guest Editorial of the Special section on Customers Centric Communication and Networked Control for Intelligent Cyber-Physical Transportation Systems <i>Open Access</i>	Chakraborty, C., Nguyen, A.-T., Huang, C., Song, H.H.	2024	IEEE Transactions on Consumer Electronics 70(1), pp. 1702-1705	0

[View at Publisher](#) [Related documents](#)

[No abstract available]

<input type="checkbox"/> 2	Securing VANETs: Multi-Objective Intrusion Detection With Variational Autoencoders	Nissar, N., Naja, N., Jamali, A.	2024	IEEE Transactions on Consumer Electronics 70(1), pp. 3867-3874	0
----------------------------	--	----------------------------------	------	--	---

[View abstract](#) [View at Publisher](#) [Related documents](#)

<input type="checkbox"/> 3	A Multi-Scale Temporal Feature Extraction Approach for Network Traffic Anomaly Detection <i>Open Access</i>	Zhang, Y.	2024	International Journal of Information Security and Privacy 18(1)	0
----------------------------	--	-----------	------	---	---

[Hide abstract](#) [View at Publisher](#) [Related documents](#)

With the rapid advancement of network technology and the expanding scale of the Internet, network traffic data has grown exponentially, leading to increasingly prominent issues in network security. Many researchers are developing new network traffic anomaly detection models, but these models are difficult to effectively capture the multi-scale temporal characteristics of network traffic data and learn the correlation and importance among various feature dimensions. To this end, we propose a multi-scale temporal feature network (MSTFN-AM) based on an attention mechanism. MSTFN-AM integrates original data with temporal information through the temporal position encoding module and extracts multi-scale temporal features through the temporal feature extraction module. The temporal self-attention module can effectively identify dependencies and correlations between different time points. Ultimately, experiments conducted on two public datasets demonstrate that the MSTFN-AM model outperforms all baseline models in prediction performance.

<input type="checkbox"/> 4	BSMACRN: Design of an Efficient Blockchain-Based Security Model for Improving Attack-Resilience of Cognitive Radio Ad-hoc Networks <i>Open Access</i>	Dansana, D., Behera, P.K., Patro, S.G.K., (...), Lasisi, A., Wodajo, A.W.	2024	IEEE Access 12, pp. 10047-10058	2
----------------------------	--	---	------	---------------------------------	---

[View abstract](#) [View at Publisher](#) [Related documents](#)

Display: [20](#) results per page

1

[Top of page](#)

International Journal of Information Security and Privacy • Open Access • Volume 18, Issue 1 • 2024

Document type  
Article • Hybrid Gold Open Access


Source type  
Journal

ISSN  
19301650

DOI  
10.4018/IJISP.354884

[View more](#) 

# A Multi-Scale Temporal Feature Extraction Approach for Network Traffic Anomaly Detection

Zhang, Yaping 

 Save all to author list

<sup>a</sup> School of Computer and Information Engineering, Wuhan Railway Vocational College of Technology  
Hubei Province, Wuhan, China

Full text options  Export 

## Abstract

### Author keywords

### Indexed keywords

SciVal Topics

## Metrics

## Abstract

With the rapid advancement of network technology and the expanding scale of the Internet, network traffic data has grown exponentially, leading to increasingly prominent issues in network security. Many researchers are developing new network traffic anomaly detection models, but these models are difficult to effectively capture the multi-scale temporal characteristics of network traffic data and learn the correlation and importance among various feature dimensions. To this end, we propose a multi-scale temporal feature network (MSTFN-AM) based on an attention mechanism. MSTFN-AM integrates original data with temporal information through the temporal position encoding module and extracts multi-scale temporal features through the temporal feature extraction module. The temporal self-attention module can effectively identify dependencies and correlations between different time points. Ultimately, experiments conducted on two public datasets demonstrate that the MSTFN-AM model outperforms all baseline models in prediction performance. © 2024 IGI Global. All rights reserved.

### Author keywords

Anomaly Detection; Multi-Scale Temporal Features; Temporal Position Coding; Temporal Self-Attention

### Indexed keywords

SciVal Topics ⓘ

## Metrics

## References (38)

[View in search results format >](#)

☐ All
 ☐ Export
 ☐ Print
 ☐ E-mail
 ☐ Save to PDF
 ☐ Create bibliography

- 1 Abdulganiyu, O.H., Tchakoucht, T.A., Saheed, Y.K.  
Towards an efficient model for network intrusion detection system (IDS):  
systematic literature review

(2024) *Wireless Networks*, 30 (1), pp. 453–482. Cited 9 times.

<https://www.springer.com/journal/11276>

doi: 10.1007/s11276-023-03495-2

[View at Publisher](#)

Cited by 0 documents

Inform me when this document is cited  
in Scopus:

[Set citation alert >](#)

## Related documents

## Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning

Salvakkam, D.B. , Saravanan, V. , Jain, P.K.

(2023) Cognitive Computation

## Machine Learning and Deep Learning Methods for Cybersecurity

Xin, Y. , Kong, L. , Liu, Z.

(2018) IEEE Access

Cyber Security with AI—Part I

Chander, B. , Kumaravelan, G.  
(2021) *Lecture Notes in Networks and Systems*

[View all related documents based on references](#)

Find more related documents in Scopus  
based on:

Author &gt; Keywords &gt;

- 
- 2 Al-Mazrawe, A., Al-Musawi, B.  
**Anomaly Detection in Cloud Network: A Review**  
  
(2024) *BIO Web of Conferences*, 97, art. no. 00019.  
<https://www.bio-conferences.org/>  
doi: 10.1051/bioconf/20249700019  
  
[View at Publisher](#)
- 
- 3 Alkadi, O., Moustafa, N., Turnbull, B., Choo, K.-K.R.  
**A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks**  
  
(2021) *IEEE Internet of Things Journal*, 8 (12), art. no. 9098927, pp. 9463-9472. Cited 259 times.  
<http://ieeexplore.ieee.org/servlet/opac?punumber=6488907>  
doi: 10.1109/JIOT.2020.2996590  
  
[View at Publisher](#)
- 
- 4 Almahadin, G., Aoudni, Y., Shabaz, M., Agrawal, A.V., Yasmin, G., Alomari, E.S., Al-Khafaji, H.M.R., (...), Maaliw, R.R.  
**VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model**  
  
(2024) *IEEE Transactions on Consumer Electronics*, 70 (1), pp. 4548-4555. Cited 4 times.  
<https://ieeexplore.ieee.org/servlet/opac?punumber=30>  
doi: 10.1109/TCE.2023.3326384  
  
[View at Publisher](#)
- 
- 5 Baccari, S., Hadded, M., Ghazzai, H., Touati, H., Elhadeif, M.  
**Anomaly Detection in Connected and Autonomous Vehicles: A Survey, Analysis, and Research Challenges**  
  
(2024) *IEEE Access*, 12, pp. 19250-19276. Cited 7 times.  
<http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639>  
doi: 10.1109/ACCESS.2024.3361829  
  
[View at Publisher](#)
- 
- 6 Bazuhair, W., Lee, W.  
**Detecting Malign Encrypted Network Traffic Using Perlin Noise and Convolutional Neural Network (Open Access)**  
  
(2019) *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, art. no. 9031116, pp. 200-206. Cited 21 times.  
<http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9017208>  
ISBN: 978-172813783-4  
doi: 10.1109/CCWC47524.2020.9031116  
  
[View at Publisher](#)
- 
- 7 Chandrasekhar, A.M., Raghuveer, K.  
**Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset**  
  
(2014) *International Conference on Communication and Signal Processing, ICCSP 2014 - Proceedings*, art. no. 6949927, pp. 672-676. Cited 26 times.  
ISBN: 978-147993358-7  
doi: 10.1109/ICCSP.2014.6949927  
  
[View at Publisher](#)
- 
- 8 Diallo, B., Hu, J., Li, T., Khan, G.A., Liang, X., Wang, H.  
**Auto-attention mechanism for multi-view deep embedding clustering**  
  
(2023) *Pattern Recognition*, 143, art. no. 109764. Cited 20 times.  
[www.elsevier.com/inca/publications/store/3/2/8/](http://www.elsevier.com/inca/publications/store/3/2/8/)