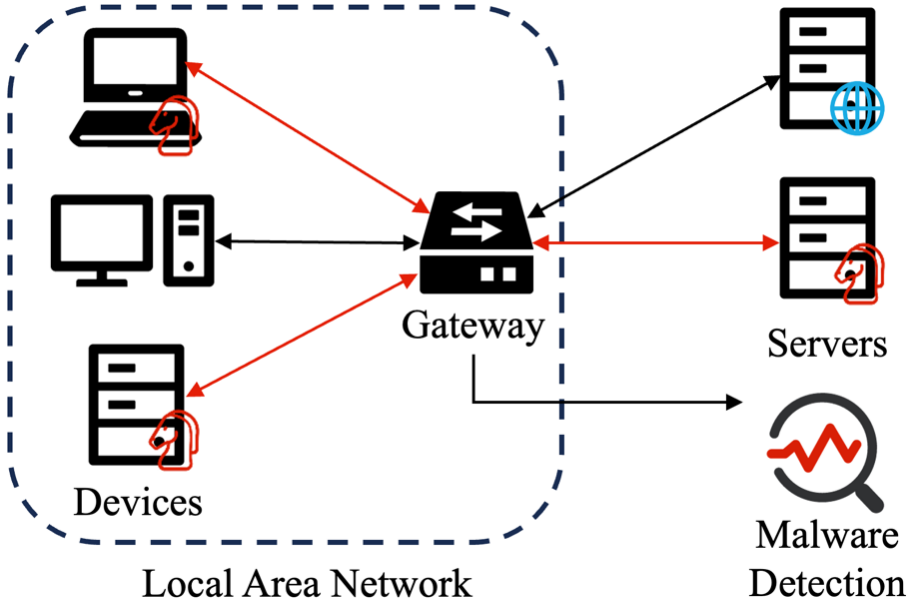
# Adaptive Detection of Encrypted Malware Traffic via Fully Convolutional Masked Autoencoders

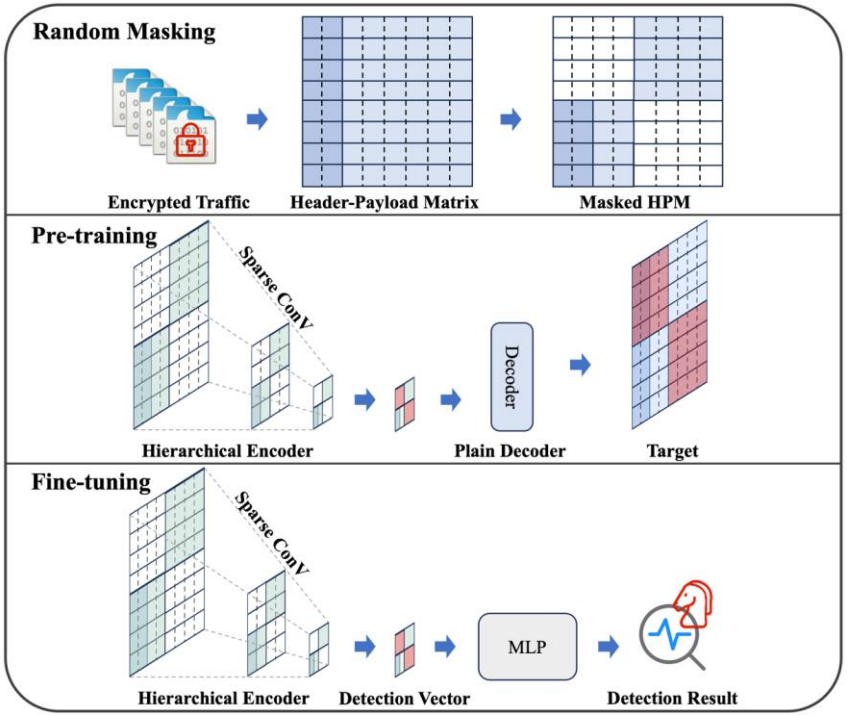
**Jizhe JIA, Meng SHEN, Qingjun YUAN, Yong LIU, Jing WANG, Jian KONG, Liang HUANG, Haotian HE, Liehuang ZHU**

Frontiers of Computer Science , DOI: 10.1007/s11704-025-41273-9

# Problems & Ideas

- Problems of conventional malware traffic detection approaches:
  - Existing malware traffic detection techniques rely on a sufficient amount of labeled data readily available for model training, limiting the capability of transferring to new malware detection.
- Ideas: A novel adaptive encrypted malware traffic detection method, Malcom, based on fully convolutional masked autoencoders to detect malware traffic.



# Main Contributions

- Contributions:
  - A novel traffic representation named Header-Payload Matrix (HPM) based on the Open System Interconnection (OSI) reference model to extract discriminative features;
  - An adaptive encrypted malware traffic detection method, Malcom, based on fully convolutional masked autoencoders;
  - Extensive experiments on a real-world traffic dataset to evaluate the performance of Malcom in two typical scenarios, i.e., a few-shot learning scenario and an imbalanced dataset scenario.

**Table 4** The few-shot learning evaluation results of ST-Graph, CBSeq, FC-Net, and Malcom under various training samples.

| N | Malware | ST-Graph [7] | | | CBSeq [5] | | | FC-Net [11] | | | Malcom | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | F1 | Pre | Recall | F1 | Pre | Recall | F1 | Pre | Recall | F1 | Pre | Recall |
| 5 | Dridex | 83.36 | 90.33 | 81.67 | 78.77 | 92.59 | 70.9 | 72.04 | 56.30 | 100.0 | 94.88 | 95.34 | 94.42 |
| | Emotet | 82.35 | 90.12 | 80.51 | 81.06 | 89.96 | 74.65 | 92.29 | 90.57 | 94.07 | 85.02 | 81.91 | 91.35 |
| | Geodo | 82.08 | 92.37 | 78.34 | 82.33 | 96.30 | 74.70 | 88.89 | 90.50 | 87.32 | 90.29 | 87.05 | 95.64 |
| | Miuref | 69.17 | 86.59 | 65.90 | 62.04 | 95.65 | 49.94 | 93.39 | 94.13 | 92.65 | 90.66 | 87.47 | 95.83 |
| | Zeus | 78.99 | 88.72 | 76.71 | 41.84 | 76.07 | 32.12 | 81.17 | 95.90 | 70.37 | 90.57 | 87.20 | 95.64 |
| | TrickBot | 71.31 | 86.82 | 68.18 | 94.22 | 92.40 | 96.12 | 83.88 | 82.80 | 84.98 | 86.20 | 82.62 | 93.84 |
| | **Average** | 77.88 | 89.16 | 75.22 | 73.38 | 90.50 | 66.41 | 86.86 | 86.53 | 89.90 | **92.06** ↑5.20 | **88.72** | **95.67** |
| 10 | Dridex | 85.45 | 86.01 | 85.07 | 43.19 | 35.65 | 54.77 | 87.07 | 80.50 | 94.81 | 99.32 | 99.32 | 99.32 |
| | Emotet | 83.61 | 85.99 | 82.55 | 93.04 | 93.48 | 94.77 | 91.49 | 98.29 | 85.57 | 97.58 | 96.18 | 99.14 |
| | Geodo | 74.91 | 91.50 | 69.35 | 93.94 | 95.92 | 95.63 | 98.39 | 97.30 | 99.50 | 97.37 | 95.87 | 99.06 |
| | Miuref | 83.67 | 89.43 | 82.11 | 60.37 | 87.13 | 46.47 | 85.15 | 91.49 | 79.63 | 98.90 | 99.63 | 98.20 |
| | Zeus | 85.49 | 91.14 | 84.11 | 89.20 | 92.00 | 91.88 | 82.03 | 92.00 | 74.01 | 95.78 | 93.57 | 98.46 |
| | TrickBot | 70.50 | 70.30 | 70.70 | 72.08 | 93.93 | 60.30 | 90.53 | 89.34 | 98.25 | 95.17 | 92.84 | 97.63 |
| | **Average** | 80.61 | 85.73 | 78.98 | 75.30 | 83.02 | 73.97 | 89.11 | 90.59 | 88.63 | **97.35** ↑8.24 | **96.24** | **98.64** |
| 15 | Dridex | 85.56 | 89.94 | 84.31 | 93.98 | 95.68 | 95.47 | 80.22 | 73.37 | 88.48 | 99.55 | 99.55 | 99.55 |
| | Emotet | 75.97 | 88.43 | 73.30 | 92.50 | 89.60 | 94.65 | 93.80 | 90.52 | 97.33 | 96.79 | 97.02 | 96.57 |
| | Geodo | 89.83 | 94.19 | 88.26 | 87.31 | 95.92 | 76.64 | 98.40 | 99.99 | 97.50 | 98.61 | 97.77 | 99.51 |
| | Miuref | 88.75 | 92.08 | 87.87 | 58.79 | 90.27 | 45.27 | 93.37 | 94.67 | 92.10 | 99.44 | 91.74 | 97.93 |
| | Zeus | 90.62 | 92.93 | 89.99 | 81.31 | 90.15 | 76.94 | 83.54 | 92.47 | 76.18 | 96.10 | 96.36 | 95.84 |
| | TrickBot | 80.75 | 81.32 | 80.31 | 96.18 | 97.14 | 97.05 | 85.56 | 96.35 | 76.94 | 95.20 | 92.77 | 98.23 |
| | **Average** | 85.25 | 89.82 | 84.01 | 84.34 | 93.13 | 81.00 | 89.20 | 91.23 | 88.09 | **97.62** ↑8.42 | **95.87** | **97.94** |
| 20 | Dridex | 87.15 | 89.25 | 86.35 | 96.22 | 96.34 | 96.13 | 85.45 | 77.89 | 94.63 | 99.86 | 99.87 | 99.86 |
| | Emotet | 87.44 | 90.68 | 86.47 | 81.33 | 92.21 | 74.56 | 95.32 | 99.19 | 91.75 | 97.15 | 97.32 | 96.99 |
| | Geodo | 81.87 | 89.94 | 78.34 | 94.00 | 92.11 | 95.97 | 96.30 | 100.0 | 92.86 | 99.56 | 99.85 | 99.28 |
| | Miuref | 82.73 | 89.58 | 80.99 | 93.48 | 93.05 | 93.97 | 90.64 | 95.58 | 86.18 | 99.89 | 99.82 | 99.96 |
| | Zeus | 92.45 | 93.99 | 92.03 | 85.82 | 81.70 | 90.39 | 79.52 | 95.83 | 67.95 | 96.83 | 96.96 | 96.71 |
| | TrickBot | 86.07 | 91.13 | 84.79 | 68.58 | 93.90 | 56.00 | 97.10 | 94.80 | 99.52 | 99.46 | 99.12 | 99.81 |
| | **Average** | 86.29 | 90.76 | 84.83 | 86.57 | 91.55 | 84.50 | 90.72 | 93.88 | 88.82 | **98.79** ↑8.07 | **98.82** | **98.77** |

**Table 5** The evaluation results of ST-Graph, CBSeq, FC-Net, and Malcom under different imbalance ratios of benign and malware traffic.

| $\beta$ | Malware | ST-Graph [7] | | | CBSeq [5] | | | FC-Net [11] | | | Malcom | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | F1 | Pre | Recall | F1 | Pre | Recall | F1 | Pre | Recall | F1 | Pre | Recall |
| 1:1 | Dridex | 85.45 | 86.01 | 85.07 | 43.19 | 35.65 | 54.77 | 87.07 | 80.50 | 94.81 | 99.32 | 99.32 | 99.32 |
| | Emotet | 83.61 | 85.99 | 82.55 | 93.04 | 93.48 | 94.77 | 91.49 | 98.29 | 85.57 | 97.58 | 96.18 | 99.14 |
| | Geodo | 74.91 | 91.50 | 69.35 | 93.94 | 95.92 | 95.63 | 98.39 | 97.30 | 99.50 | 97.37 | 95.87 | 99.06 |
| | Miuref | 83.67 | 89.43 | 82.11 | 60.37 | 87.13 | 46.47 | 85.15 | 91.49 | 79.63 | 98.90 | 99.63 | 98.20 |
| | Zeus | 85.49 | 91.14 | 84.11 | 89.20 | 92.00 | 91.88 | 82.03 | 92.00 | 74.01 | 95.78 | 93.57 | 98.46 |
| | TrickBot | 70.50 | 70.30 | 70.70 | 72.08 | 93.93 | 60.30 | 90.53 | 89.34 | 98.25 | 95.17 | 92.84 | 97.63 |
| | **Average** | 80.61 | 85.73 | 78.98 | 75.30 | 83.02 | 73.97 | 89.11 | 90.59 | 88.63 | **97.35** ↑8.24 | **96.24** | **98.64** |
| 5:1 | Dridex | 49.58 | 42.75 | 59.00 | 27.69 | 16.07 | 100.0 | 53.56 | 100.0 | 36.57 | 98.20 | 97.12 | 99.36 |
| | Emotet | 62.07 | 54.55 | 72.00 | 31.41 | 18.63 | 100.0 | 71.48 | 100.0 | 55.61 | 96.89 | 94.85 | 98.73 |
| | Geodo | 58.26 | 51.54 | 67.00 | 25.64 | 14.71 | 100.0 | 65.09 | 96.98 | 48.98 | 95.69 | 93.44 | 98.42 |
| | Miuref | 42.93 | 41.90 | 44.00 | 12.50 | 6.57 | 100.0 | 70.51 | 100.0 | 54.45 | 97.78 | 96.49 | 99.21 |
| | Zeus | 53.94 | 46.10 | 65.00 | 27.45 | 17.07 | 70.00 | 64.74 | 97.94 | 48.35 | 93.33 | 90.29 | 97.48 |
| | TrickBot | 24.58 | 27.85 | 22.00 | 54.90 | 43.75 | 73.68 | 64.74 | 97.94 | 48.35 | 93.97 | 93.98 | 93.96 |
| | **Average** | 48.56 | 44.12 | 54.83 | 30.79 | 19.48 | 90.61 | 65.02 | 98.81 | 48.72 | **95.98** ↑30.96 | **94.36** | **97.86** |
| 25:1 | Dridex | 18.61 | 10.28 | 98.00 | 14.63 | 8.16 | 70.59 | 75.40 | 96.33 | 61.95 | 96.47 | 94.45 | 98.72 |
| | Emotet | 20.14 | 11.20 | 100.0 | 35.71 | 55.56 | 26.32 | 48.65 | 90.00 | 33.33 | 95.88 | 93.71 | 98.50 |
| | Geodo | 19.12 | 10.57 | 100.0 | 8.23 | 4.29 | 100.0 | 72.43 | 93.49 | 59.12 | 93.98 | 91.12 | 97.75 |
| | Miuref | 19.23 | 10.64 | 100.0 | 21.88 | 15.22 | 38.89 | 71.24 | 96.89 | 56.33 | 95.30 | 92.90 | 98.27 |
| | Zeus | 19.17 | 10.66 | 95.00 | 2.63 | 1.44 | 15.79 | 33.75 | 91.89 | 20.67 | 91.18 | 87.70 | 96.44 |
| | TrickBot | 20.06 | 11.15 | 100.0 | 14.82 | 8.39 | 63.16 | 18.35 | 95.12 | 10.16 | 90.77 | 87.17 | 96.39 |
| | **Average** | 19.39 | 10.75 | 98.83 | 16.32 | 15.51 | 52.46 | 53.30 | 93.95 | 40.26 | **93.93** ↑40.63 | **91.19** | **97.68** |
| 50:1 | Dridex | 14.03 | 7.54 | 100.0 | 12.50 | 11.77 | 13.33 | 60.11 | 98.80 | 43.19 | 94.81 | 91.33 | 98.56 |
| | Emotet | 13.80 | 7.42 | 99.00 | 4.80 | 2.46 | 100.0 | 23.45 | 100.0 | 13.28 | 93.13 | 87.15 | 100.0 |
| | Geodo | 14.29 | 7.69 | 100.0 | 12.12 | 13.33 | 11.11 | 55.06 | 99.32 | 38.08 | 90.22 | 83.69 | 97.84 |
| | Miuref | 13.82 | 7.43 | 99.00 | 9.93 | 5.69 | 38.89 | 39.07 | 86.84 | 24.47 | 92.05 | 86.90 | 97.84 |
| | Zeus | 13.85 | 7.67 | 99.00 | 4.61 | 2.75 | 14.29 | 74.52 | 96.69 | 60.62 | 89.25 | 80.58 | 100.0 |
| | TrickBot | 14.23 | 7.44 | 100.0 | 5.24 | 2.92 | 25.00 | 55.84 | 98.71 | 38.93 | 85.89 | 75.48 | 99.64 |
| | **Average** | 14.00 | 7.53 | 99.50 | 8.20 | 6.49 | 33.77 | 51.34 | 98.39 | 36.43 | **90.89** ↑39.55 | **84.19** | **98.98** |