

Robust Open-Set Classification of Encrypted Network Traffic under Packet Loss and Partial Observation

¹Dr. Dharavath Ravindar, ²Mr. Bodla Bobbilaraja

¹Assistant Professor and Head of the Department, Department of Computer Science and Engineering, GATE Institute of Technology and Sciences, Ramapuram(V), Chilkur(M), Kodad, Suryapet(D)-508206

¹Email: ravindershanthi@gmail.com

²Lecturer , Department of Computer Science, MJPT BC Welfare Residential Degree College(Men), Nagarjuna Sagar, Nalgonda(D)-508202

²Email: bobbiliraaja@gmail.com

ABSTRACT

The rapid adoption of encrypted communication protocols has improved network privacy and security, but it has also reduced the visibility available to conventional traffic classification systems. Network operators increasingly need to identify applications and traffic behaviors without inspecting payload contents. This paper presents a robust open-set classification framework for encrypted network traffic under packet loss and partial observation. The proposed approach treats traffic classification as an open-set problem in which previously unseen applications must be distinguished from known traffic classes rather than being forcibly assigned to an existing category. The framework combines flow-level statistical features, packet-size and timing characteristics, sequence-aware representation learning, and an unknown-class rejection mechanism. To model realistic network conditions, controlled packet loss, truncated flows, and limited observation windows are introduced during evaluation. A confidence-based rejection layer is used to separate reliable known-class predictions from uncertain or novel traffic. The overall workflow includes traffic collection, preprocessing, partial-observation simulation, feature extraction, robust representation learning, open-set decision making, and performance analysis. The framework is designed to improve reliability when encrypted flows are incomplete or when traffic belonging to classes not present during training appears during deployment. The study also discusses privacy, deployment, class imbalance, and the limitations of metadata-based traffic analysis.

Keywords

Encrypted traffic, open-set recognition, network traffic classification, packet loss, partial observation, flow classification, machine learning, deep learning, anomaly detection, network security.

I. INTRODUCTION

Encryption has become a fundamental component of modern computer networks. HTTPS, TLS, VPNs, QUIC, and other secure communication mechanisms protect the confidentiality and integrity of network data. At the same time, encryption prevents traditional deep packet inspection systems from directly using application payloads for traffic identification. Network administrators therefore increasingly depend on observable information such as packet sizes, packet directions, timing, burst patterns, flow duration, packet counts, and byte counts.

Many existing traffic classification systems are formulated as closed-set classification problems. In a closed-set setting, the classifier assumes that every test sample belongs to one of the classes observed during training. This assumption is difficult to satisfy in operational networks because applications, services, protocols, and user behaviors continuously change. A model trained on a fixed collection of applications may encounter traffic that does not correspond to any known class. If the classifier is forced to select one of the known labels, the resulting prediction can be misleading.

Another practical challenge is incomplete observation. Packet loss may occur because of congestion, wireless interference, routing conditions, sampling, capture limitations, or monitoring constraints. A classifier may also receive only the first part of a flow because a monitoring system begins recording after a connection has started or stops before the flow terminates. Therefore, a robust system should not depend on complete packet sequences.

This paper proposes a robust open-set classification framework that jointly considers unknown traffic, packet loss, and partial observation. Instead of relying on payload inspection, the approach extracts encrypted-flow metadata and learns representations that remain useful when portions of the traffic sequence are unavailable. An open-set rejection mechanism then estimates whether a sample is sufficiently similar to known classes or should be treated as unknown.

II. LITERATURE SURVEY

1. Deep Packet: A Novel Approach for Encrypted Traffic Classification Using Deep Learning — Lotfollahi et al. This work demonstrates that deep learning can learn useful representations from encrypted traffic characteristics and reduce dependence on manually designed features.
2. Towards Open Set Deep Networks — Bendale and Boulton. This research formalizes open-set recognition for deep networks and introduces mechanisms for rejecting inputs that are not adequately represented by known training classes. The concept is relevant to encrypted traffic because real deployments can contain previously unseen applications.
3. Encrypted Traffic Classification Using Statistical and Machine Learning Features. Research in encrypted traffic analysis has shown that packet length, direction, timing, burst behavior, and flow duration can provide information for application classification even when payloads are encrypted.
4. Machine and Deep Learning for Encrypted Traffic Classification. Survey literature describes the use of classical machine learning, convolutional models, recurrent models, and sequence-learning approaches for encrypted traffic

classification and identifies challenges involving dataset shift, encrypted protocol evolution, class imbalance, and generalization.

5. Open-World Network Traffic Recognition. Open-world monitoring research emphasizes that a deployed classifier must identify novel traffic rather than assigning every observation to a known class. Unknown detection and controlled model adaptation are therefore important complements to conventional classification.

III. EXISTING SYSTEM

Existing encrypted traffic classification systems commonly use supervised machine learning or deep learning models trained on a predefined set of traffic classes. Typical features include packet length sequences, packet direction, inter-arrival time, flow duration, packet counts, byte counts, and burst statistics. Classifiers such as Random Forest, Support Vector Machine, gradient boosting, CNN, RNN, and transformer-based models can map these features to application labels.

However, many systems assume that the classes available during testing are the same as the classes used during training. This closed-set assumption can cause an unknown application to be incorrectly classified as a known application. Performance can also decrease when only a short observation window is available or when packets are missing.

Another limitation is that classification performance is often reported using overall accuracy without explicitly measuring unknown-class rejection or robustness to packet loss. A model may obtain high closed-set accuracy while still producing a high number of false known predictions for unseen traffic. Such behavior is undesirable in security monitoring because unfamiliar flows may be incorrectly treated as familiar.

IV. PROPOSED SYSTEM

The proposed system introduces a robust open-set learning pipeline for encrypted network traffic. The framework does not inspect application payloads. Instead, it uses metadata and sequence-level characteristics that remain observable

when traffic is encrypted. The main stages are traffic acquisition, preprocessing, flow construction, partial-observation generation, feature extraction, robust representation learning, open-set classification, unknown rejection, and performance evaluation.

During preprocessing, packets are grouped into bidirectional or unidirectional flows according to the selected monitoring configuration. Timestamp information is used to derive inter-arrival times, while packet lengths and directions are retained as observable sequence information. Payload bytes are excluded from the feature representation. To reproduce incomplete network conditions, packet-loss masks and observation-window truncation are applied during evaluation.

The feature representation combines statistical and temporal information. Statistical features include total packets, total bytes, average packet length, minimum and maximum packet length, packet-length variance, flow duration, and directional byte counts. Temporal features include inter-arrival-time statistics, burst duration, packet-rate measures, and sequence ordering. These features are normalized before model training.

A robust classifier is trained on known traffic classes. During inference, the model produces class scores together with a confidence or distance measure. If the evidence for all known classes is below the rejection threshold, the flow is assigned to an unknown class. This prevents the system from forcing every observation into a known application category. The framework also supports adaptive observation lengths. Predictions can be generated from an early segment of a flow and refined when additional packets become available. This allows monitoring systems to operate when full-flow information is unavailable. The system can therefore report known-class predictions, unknown-flow rejection, and confidence information rather than relying only on a single final label.

V. SYSTEM ARCHITECTURE

The proposed architecture follows the workflow: Encrypted Network Traffic → Flow Construction → Preprocessing →

Packet-Loss and Partial-Observation Module → Feature Extraction → Robust Representation Learning → Open-Set Classifier → Unknown Rejection → Classification and Visualization.

The first module collects encrypted packet traces from an authorized monitoring environment. The Flow Construction module groups packets into flows and preserves packet direction and timing information. The Preprocessing module removes invalid records, handles missing values, normalizes numeric features, and prepares sequences for model input.

The Packet-Loss and Partial-Observation module creates realistic incomplete observations. Packet-loss simulation removes a controlled portion of packets, while partial observation restricts the available sequence to a defined observation window. The same procedure can be used during robustness evaluation at multiple loss rates and observation lengths.

The Feature Extraction module generates packet-size, timing, direction, burst, and flow-statistical features. The Robust Representation Learning module converts these observations into a compact representation that captures traffic behavior. The Open-Set Classifier predicts known classes while the Unknown Rejection module examines confidence or feature-space distance before accepting the predicted class.

Finally, the Visualization and Reporting module presents class predictions, unknown-flow counts, rejection rates, and robustness measurements for different packet-loss and observation conditions. The complete architecture supports privacy-aware network monitoring without requiring plaintext payload access.

Encrypted Traffic	Flow Construction	Preprocessing	Partial Observation	Feature Learning	Open-Set Decision	Known / Unknown Output

Fig. 1. Proposed architecture for robust open-set encrypted traffic classification.

VI. IMPLEMENTATION

The proposed framework can be implemented using Python with standard network-analysis and machine-learning libraries. A packet-processing component converts authorized packet captures into flow-level records. Pandas and NumPy can be used for preprocessing and statistical feature construction. Scikit-learn can provide baseline classifiers and evaluation measures, while PyTorch or TensorFlow can be used for sequence representation learning.

The implementation should divide traffic into training, validation, and testing sets without allowing flows from the same communication session to leak across partitions. Known classes are used for supervised training, while one or more additional classes are held out from training to represent unknown traffic during open-set evaluation. Packet-loss and partial-observation transformations should be applied independently so robustness can be measured under different operating conditions.

The principal experimental variables are packet-loss ratio and observation length. Evaluation can compare complete observations with progressively shorter observations and several controlled packet-loss levels. In addition to accuracy, the evaluation should include known-class macro-F1, unknown-class detection rate, false acceptance of unknown traffic as known, and an open-set measure such as AUROC.

A practical implementation should also record inference time and memory requirements because network monitoring systems may need near-real-time classification. Threshold selection for unknown rejection should be performed using a validation set rather than tuning directly on the final test set.

VII. PERFORMANCE EVALUATION

Performance evaluation should focus on robustness rather than a single closed-set accuracy value. The first experiment evaluates classification on complete known flows. The second introduces packet loss at controlled levels and measures the change in classification performance. The third limits the observation window and evaluates whether the model can make useful decisions from partial flows. The fourth introduces traffic classes that were not used during

training and measures the system's ability to reject them as unknown.

The recommended measures are Accuracy and macro-F1 for known-class classification; Unknown Detection Rate for unseen classes; False Known Rate, measuring the fraction of unknown traffic incorrectly accepted as a known class; and AUROC for confidence-based unknown rejection. A robustness curve can also plot packet-loss ratio or observation length against the selected performance metric.

Evaluation Condition	Input Condition	Primary Metric	Purpose
Closed-set baseline	Complete known flows	Accuracy / Macro-F1	Normal classification
Packet-loss robustness	Controlled packet loss	Macro-F1 / degradation	Resilience to missing packets
Partial observation	Short observation windows	Accuracy / F1	Early-flow classification
Open-set evaluation	Known + unseen classes	Unknown detection / AUROC	Unknown rejection

Table 1. Recommended evaluation protocol. Insert numerical results after experiments are completed.

VIII. ADVANTAGES

- Supports encrypted traffic classification without requiring payload decryption.
- Explicitly models previously unseen traffic through open-set rejection.
- Evaluates realistic packet-loss and partial-observation conditions.
- Combines temporal, directional, packet-size, and flow-statistical information.
- Can provide an early prediction before the complete flow is available.
- Can be integrated into network monitoring and security analytics systems.

- Provides evaluation measures beyond conventional closed-set accuracy.

IX. LIMITATIONS

The framework depends on metadata patterns that may change when protocols, applications, network paths, or traffic-generation behaviors change. Encrypted traffic can also be intentionally shaped or padded, which may reduce the usefulness of packet-size and timing features. Open-set rejection is sensitive to threshold selection, and a threshold that works for one deployment may not transfer directly to another. Dataset representativeness is another limitation; laboratory traces may not capture the diversity of operational networks. Traffic analysis based on metadata should be deployed only with appropriate authorization and privacy safeguards.

X. CONCLUSION

This paper presented a robust open-set classification framework for encrypted network traffic under packet loss and partial observation. The approach addresses three practical issues that are often separated in conventional traffic-classification studies: encrypted payloads, incomplete observations, and previously unseen traffic. By combining observable flow characteristics with robust representation learning and an explicit unknown-class rejection mechanism, the framework is designed to avoid forcing unfamiliar traffic into known application categories.

The proposed evaluation methodology emphasizes robustness under controlled packet loss, limited observation windows, and held-out traffic classes. This provides a more realistic basis for assessing encrypted traffic classifiers intended for operational network environments. Future experimental work should validate the framework on multiple traffic datasets, protocols, network conditions, and observation lengths, and should report reproducible quantitative results together with computational cost and privacy considerations.

XI. Future Scope

Future research can extend the framework toward online and continual open-set learning, allowing newly observed traffic

classes to be incorporated after validation. Transformer-based sequence models, contrastive learning, and self-supervised pretraining can be investigated when labeled encrypted traffic is limited. Federated learning may also be explored for collaborative model development without centralizing raw traffic traces. Further work can study adversarial traffic shaping, protocol evolution, encrypted DNS and QUIC traffic, cross-network generalization, and edge deployment. Explainable AI methods could provide interpretable evidence based on packet-size, timing, direction, and flow-level characteristics while preserving payload confidentiality.

XII. REFERENCES

- [1] G. Aceto, D. Ciunzo, A. Montieri, and A. Pescapé, "Mobile Encrypted Traffic Classification Using Deep Learning," *IEEE/ACM Network Traffic Measurement and Analysis Conference (TMA)*, pp. 1–8, 2018, doi: 10.23919/TMA.2018.8506558.
- [2] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Encrypted and VPN Traffic Using Time-Related Features," *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 407–414, 2016, doi: 10.5220/0005740704070414.
- [3] A. Bendale and T. E. Boulton, "Towards Open Set Deep Networks," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1563–1572, 2016, doi: 10.1109/CVPR.2016.173.
- [4] V. Taylor, R. Spolaor, M. Conti, and I. Martinovic, "AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic," *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, doi: 10.1109/EuroSP.2016.40.
- [5] P. Sirinam, M. Imani, M. Juarez, and M. Wright, "Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning," *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 1928–1943, 2018, doi: 10.1145/3243734.3243768.

- [6] V. Rimmer, D. Preuveneers, M. Juarez, T. Van Goethem, and W. Joosen, "Automated Feature Extraction for Website Fingerprinting through Deep Learning," 2017.
- [7] S. E. Oh, S. Sunkam, and N. Hopper, "p-FP: Extraction, Classification, and Prediction of Website Fingerprints with Deep Learning," 2017.
- [8] A. Sharma and A. H. Lashkari, "A Survey on Encrypted Network Traffic: A Comprehensive Survey of Identification/Classification Techniques, Challenges, and Future Directions," *Computer Networks*, vol. 257, article 110984, 2025, doi: 10.1016/j.comnet.2024.110984.
- [9] S. Han, H. Zhang, M. Lu, S. Guo, B. Tian, and J. Wang, "A Comprehensive Survey on Encrypted Network Traffic Classification," *Computer Networks*, vol. 287, article 112524, 2026, doi: 10.1016/j.comnet.2026.112524.
- [10] Y. Wang, Y. Xiang, J. Zhang, and S. Yu, "A Survey of Techniques for Internet Traffic Classification Using Machine Learning," *Computer Networks*, 2008.
- [11] G. Aceto, A. Montieri, D. Ciunzo, and A. Pescapé, "Mobile Encrypted Traffic Classification Using Deep Learning: A Systematic Evaluation," *IEEE/ACM Network Traffic Measurement and Analysis Conference*, 2018.
- [12] A. H. Lashkari, G. Draper-Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Tor Traffic Using Time-Related Features," *related encrypted traffic analysis literature*, 2017.
- [13] M. Lotfollahi, M. J. Siavoshani, R. Shirali Hossein Zade, and M. Saberian, "Deep Packet: A Novel Approach for Encrypted Traffic Classification Using Deep Learning," *Soft Computing*, 2020.
- [14] T. E. Boulton, S. Cruz, A. R. Dhamija, M. Gunther, J. Henrydoss, and W. J. Scheirer, "Learning and the Unknown: Surveying Steps Toward Open World Recognition," *Proceedings of the AAAI Conference on Artificial Intelligence*, 2019.
- [15] W. J. Scheirer, A. de Rezende Rocha, A. Sapkota, and T. E. Boulton, "Toward Open Set Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 7, pp. 1757–1772, 2013.