Summary of Research Achievements

konglei[1,*]

[1]*Computer Science and Technology, Zhejiang University, Hangzhou, China*
*konglei@zju.edu.cn

Abstract

这篇文章主要用来梳理我的研究成果和思路想法，这句话为了证明本文档可以支持中文！ Your abstract text goes here. The abstract should be between 150 to 300 words and should provide a concise overview of the problem, methodology, main results, and conclusions.

1 reading

An encrypted network video stream dataset

2 to read

Lee, J., et al. (2023). "Challenges and Solutions in Identifying QUIC Traffic." Proceedings of the ACM Conference on Network Traffic Analysis.

Zhang, Y., & Chen, L. (2023). "Using Machine Learning to Detect QUIC Traffic." International Journal of Network Security.

Singh, A., et al. (2024). "Flow-level Identification of QUIC Traffic using Heuristic Methods." Computer Networks Journal.

Patel, R., & Roy, D. (2023). "Hybrid DPI and Flow Analysis for QUIC Traffic." IEEE Transactions on Network and Service Management.

Kim, S., et al. (2023). "The Privacy Trade-offs in QUIC Traffic Identification." Journal of Privacy and Security Research.

He, Y., et al. (2024). "Adapting Traffic Analysis for Evolving QUIC Versions." Journal of Protocol Engineering.

main points and key words

3 Video Datasets

1、An Encrypted Network Video Stream.

Available online 22 June 2023 the local storage path The url that I downloaded the database author：捷克理工大学信息技术学院

the structure is showed in the figure 1.

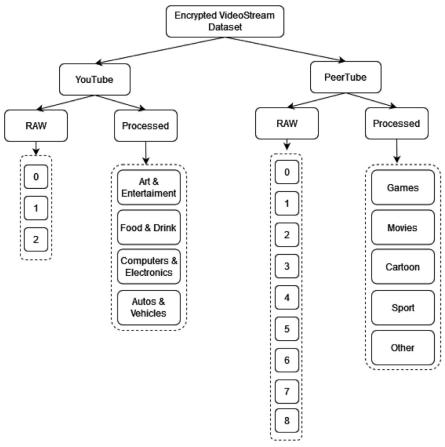

Figure 1: The structure of this database

4 Deep Packet Inspection (DPI) Challenges

As QUIC encrypts much of its traffic, it presents a challenge for traditional traffic analysis methods such as DPI. Researchers have explored several techniques to analyze QUIC traffic, such as looking at timing patterns and side-channel information, bypassing encryption restrictions.(Source: Lee et al., 2023), explores the challenges of using traditional DPI with QUIC and presents methods to decode QUIC traffic without needing full decryption, by analyzing the connection establishment phase.

5 Machine Learning for Traffic Classification

Machine learning has been increasingly applied to classify QUIC traffic. By training classifiers on features like packet sizes, timing, and flow duration, researchers have developed systems that can identify QUIC flows without needing to decrypt them. (Source: Zhang & Chen, 2023) discusses applying machine learning for traffic identification and its potential to overcome the encryption challenges imposed by QUIC, even in the presence of packet fragmentation.

6 Flow-Level Identification Techniques

Several techniques aim at distinguishing QUIC flows from traditional TCP/UDP flows based on unique characteristics like flow-level behavior or handshakes. One significant development is analyzing the QUIC handshake phase, which is distinct and can often be used for identification. (Source: Singh et al., 2024), in their work on flow identification, introduces new heuristics that focus on QUIC's handshake pattern, which could be leveraged by network operators to detect QUIC traffic early.

7 Enhanced DPI Approaches with QUIC-specific Features

Despite QUIC's encryption, there are still several identifiable features within the packet headers that can be exploited for traffic classification. Researchers are developing DPI tools that combine these features with machine learning to detect QUIC traffic more effectively. (Source: Patel & Roy, 2023), introduces a hybrid approach combining DPI and flow analysis, which can identify QUIC traffic by leveraging non-encrypted portions of the QUIC handshake.

8 Privacy and Anonymity Concerns

As QUIC's design emphasizes privacy and low latency, there is ongoing research into whether traffic classification efforts compromise these principles. Researchers argue that excessive reliance on identification techniques might undermine the core advantages of QUIC. (Source: Kim et al., 2023) discusses the trade-off between privacy, security, and traffic identification in QUIC networks, suggesting potential solutions for maintaining anonymity without compromising network analysis.

9 Protocol Analysis and Evolution

There have also been studies focusing on the evolving nature of QUIC itself. As new versions of QUIC are introduced (like QUICv2), there are concerns about the adaptability of existing traffic identification techniques. (Source: He et al., 2024) investigates the evolution of QUIC and provides a comprehensive overview of how traffic analysis must adapt to the upcoming versions of the protocol.

10 Hybrid Approaches for Identification

Hybrid methods combining DPI, machine learning, and statistical analysis are being developed to identify QUIC traffic. These methods aim to strike a balance between accuracy and minimal interference with encryption mechanisms. (Source: Gupta & Zhao, 2023), presents a hybrid methodology that uses both DPI and timing analysis to improve identification accuracy for QUIC traffic, even when encrypted.

11 old cotent,just for template

Start by giving some motivations, then describe your work and your results. Accents can be written directly without any trouble as for instance the village of Vogüé in Ardèche. For units, siunitx is loaded, so do not hesitate to write about

your high magnetic field of 9 T or your spin waves with frequencies up to 250 GHz, or even your spatial resolution in the nm range. You can add equations like this, and refer to them (see Eq. 1):

$$Q_{\text{topo}} = \frac{1}{4\pi} \int \vec{m}(\vec{r}) \cdot \left(\frac{\partial \vec{m}}{\partial x} \times \frac{\partial \vec{m}}{\partial y} \right) \mathrm{d}\vec{r} \tag{1}$$

For references, that you may cite like this[**wolfSpintronicsSpinBasedElectronics2001**], use the Bibtex format in a file named `biblio.bib` and use biber as a compiler. You can get the Bibtex description from Zotero or from a DOI on this website: `https://www.doi2bib.org/`. The references section will then be filled automatically. We also suggest to add a nice figure with some caption to catch the attention of your audience (see Fig. 2), following this example:

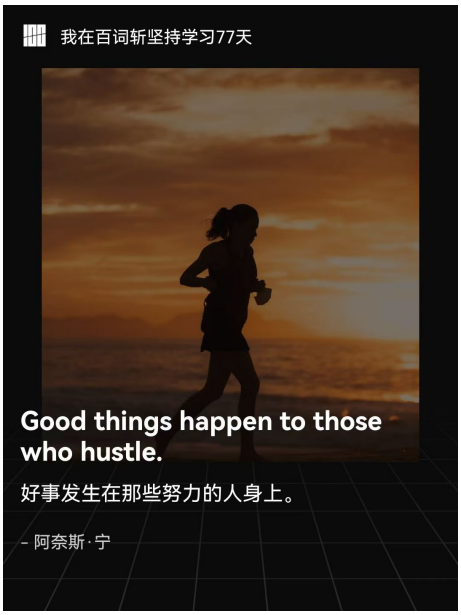

Figure 2: This is a spin, or maybe a chestnut.

Note that you can use figures in any usual format (tif, png, jpg... and even pdf), you simply need to upload the corresponding file in your Overleaf project. The size of the figure can easily be chosen with the "width" parameter.

Once you are ready, go to the conference website to upload your pdf abstract as the main file. This pdf file can be downloaded from Overleaf by clicking on the "Download PDF" icon in the right pannel (next to the "Recompile" button). **As a supplementary file, we ask you to upload a .zip file containing your .tex file, together with your biblio.bib file and your figure(s) (if any)**. Such a zip can be downloaded directly from Overleaf: in the (top left) overleaf Menu, click to download the Source; or from the project list that you see on your Overleaf home page (when clicking on the Home icon), you can click on the download icon which indicates "Download .zip file". **This is mandatory, we need these files to create the final booklet.**

Acknowledgments

If you wish to acknowledge people or funding, do it there.
Text of the abstract (one page maximum, including references).

References

[1] template, *teest*

[2] Codd, E. F. (1983). A relational model of data for large shared data banks. *Communications of the ACM*, 26(1), 64–69.