

## **GRAIN: Granular multi-label encrypted traffic classification using classifier chain**

### **ABSTRACT**

Granular traffic classification categorizes traffic into detailed classes like application names and services. Application names represent parent applications, such as Facebook, while application services are the individual actions within the parent application, such as Facebook-comment. These granular classes are still insufficient to keep pace with modern applications that offer various services. Accordingly, this paper further divides the application service class into inter-application and intra-application services to provide more insights. Interapplication service refers to a similar service between different parent applications, such as Facebook-comment and Youtube-comment, whereas intra-application service differentiates services within the same parent application, such as Facebook-comment and Facebook-post. Most studies focus on classification at the application name and inter-application service levels. In contrast, classification at the intra-application service level receives far less attention due to its complexity despite providing the highest flexibility. Therefore, this paper presents GRAIN, a granular multi-label approach to classify encrypted traffic at all three levels of granular classification: application name, inter-application and intra-application service levels using a classifier chain. GRAIN chains two random forest classifiers to produce a multi-label classification using seven novel statistical features based on packet payload length. The utilized features are independent of the packet payload content, thus unaffected by packet encryption and preserving user privacy. Our performance evaluation showed that GRAIN achieved an average F-measure of 99% at the application name level, 93% at the inter-application service level and 88% at the intra-application service level. To test for robustness, we compared GRAIN against four baseline classifiers and the ISCX VPN-nonVPN public dataset in which GRAIN maintained its comparable performance across all tests.