Experiment Results Report

Ondřej Sedláček
CESNET
Prague, Czech Republic
ondrej.sedlacek@cesnet.cz

January 30, 2024

Contents

1 Statistics of Module Data Counts

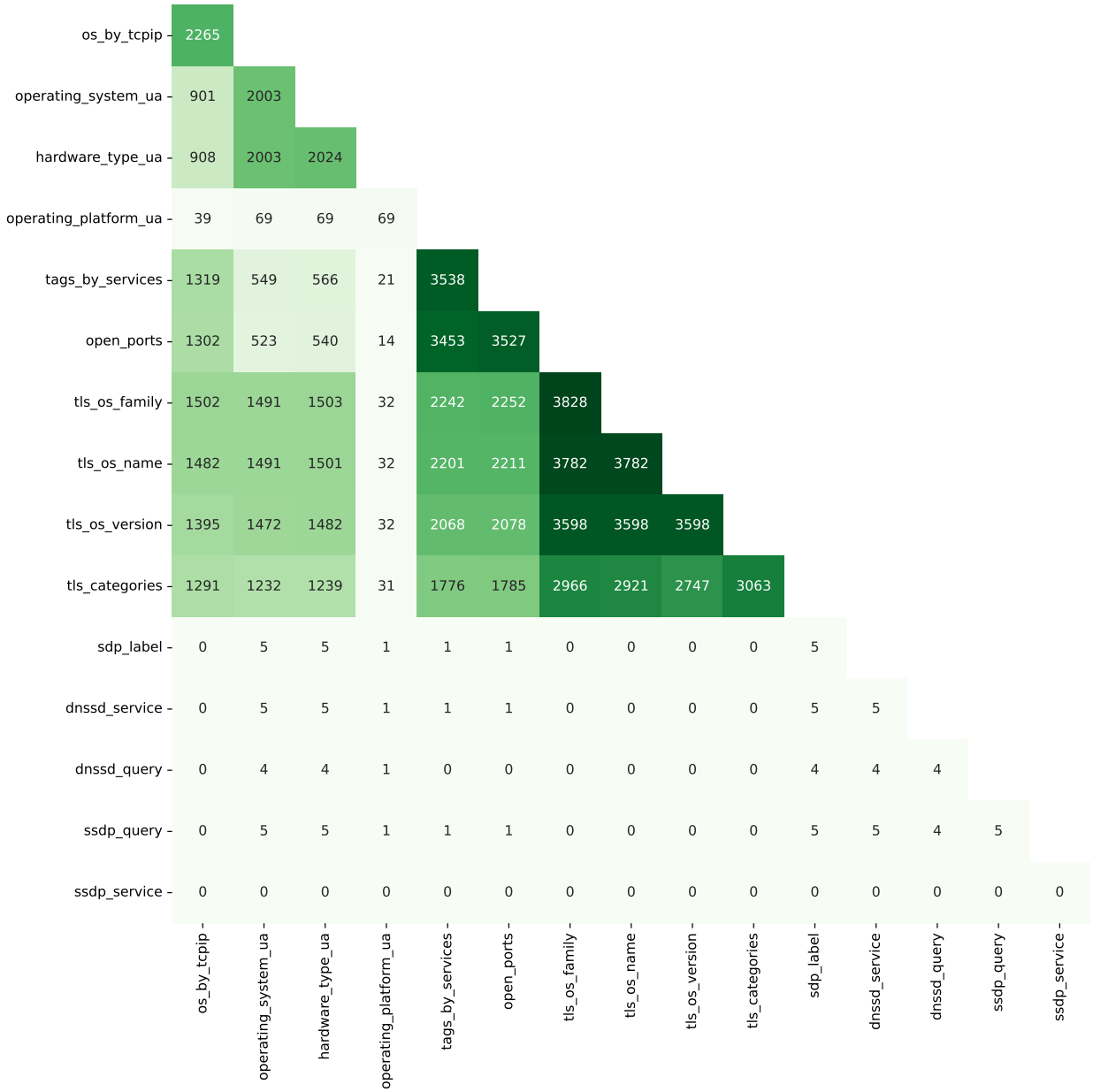

Figure 1: **Counts of overlapping attribute data.**

Index	1	2	3
http_ua	1506	457	40
os_by_tcpip	707	1171	387
os_by_tls	1809	1586	387
sdp_labels	5	0	0
tags_by_services	962	567	387

Table 1: **Number of sessions containing data from individual modules.** Shown in relation to the current number of data sources.

Index	1	2	3
sum	3483.0	1662.0	387.0
ratio	0.630	0.300	0.070

Table 2: **Number of sessions in relation to the current number of data sources.** Data from the http_ua module are not included in the sum.

2 Experiments

2.1 Metrics of Individual Modules

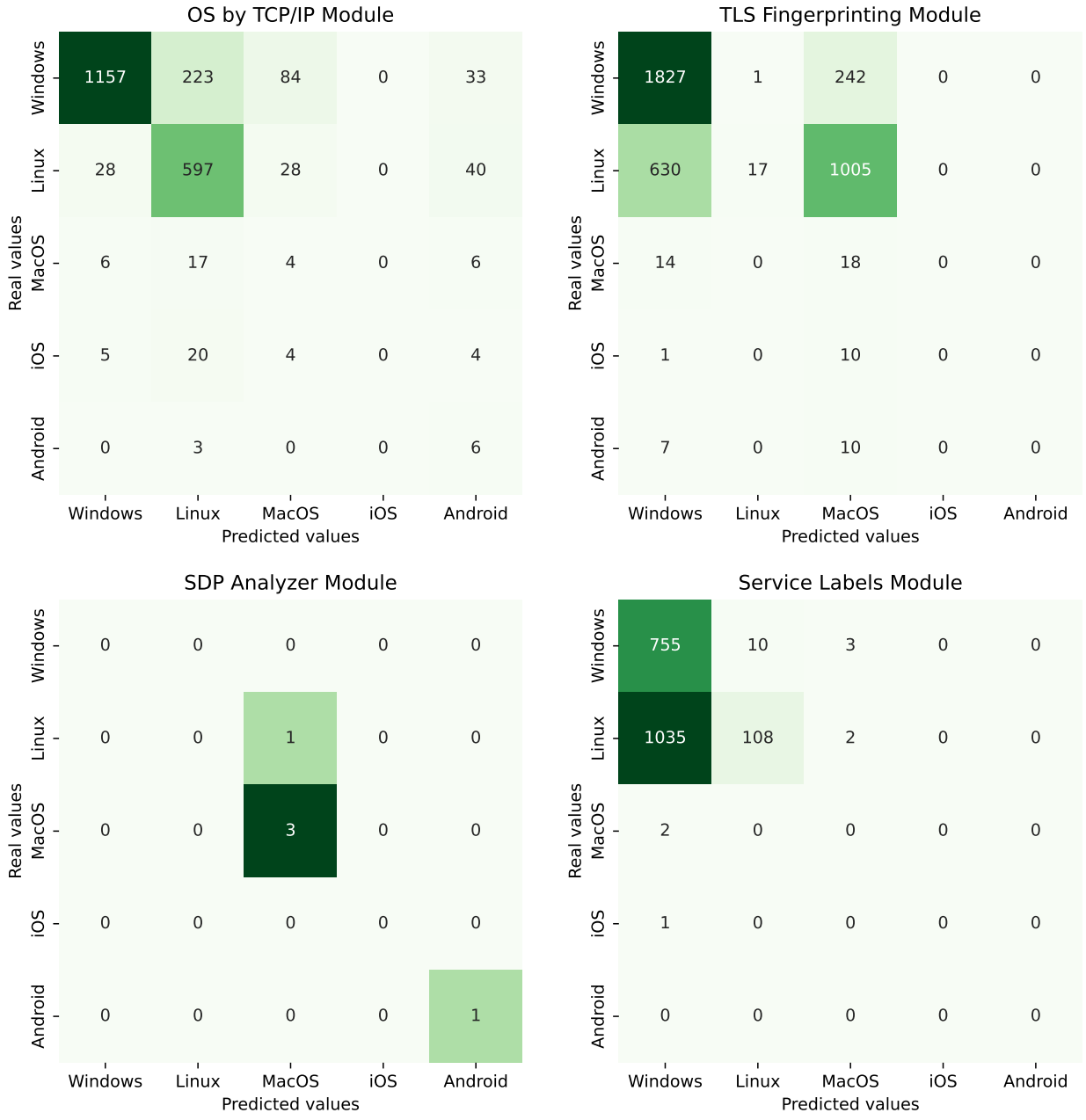

Figure 2: **Confusion matrices of individual modules.**

Index	os_by_tcpip	os_by_tls	sdp_labels	tags_by_services
Precision	0.853	0.816	0.650	0.716
Recall	0.779	0.492	0.800	0.450
F1 Score	0.804	0.449	0.714	0.339
Accuracy	0.779	0.492	0.800	0.450

Table 3: **Metrics of individual modules.**

2.2 Rule Training

Index	D-S1	D-S2	WMV	DSGD	ORA	DT	RF	AB
Precision	0.752	0.748	0.742	0.758	0.796	0.754	0.755	0.748
Recall	0.759	0.756	0.750	0.765	0.802	0.767	0.769	0.759
F1 Score	0.752	0.748	0.743	0.757	0.794	0.759	0.760	0.751
Accuracy	0.759	0.756	0.750	0.765	0.802	0.767	0.769	0.759

Table 4: **Metrics of combination methods using trained rules.**

Index	D-S1	D-S2	WMV	DSGD	DT	RF	AB
Precision	0.944	0.939	0.932	0.952	0.754	0.755	0.748
Recall	0.947	0.942	0.935	0.954	0.767	0.769	0.759
F1 Score	0.947	0.943	0.935	0.954	0.759	0.760	0.751
Accuracy	0.947	0.942	0.935	0.954	0.767	0.769	0.759

Table 5: **Metrics of combination methods using trained rules, normalized to the oracle.**

2.3 Modulation of Belief Mass

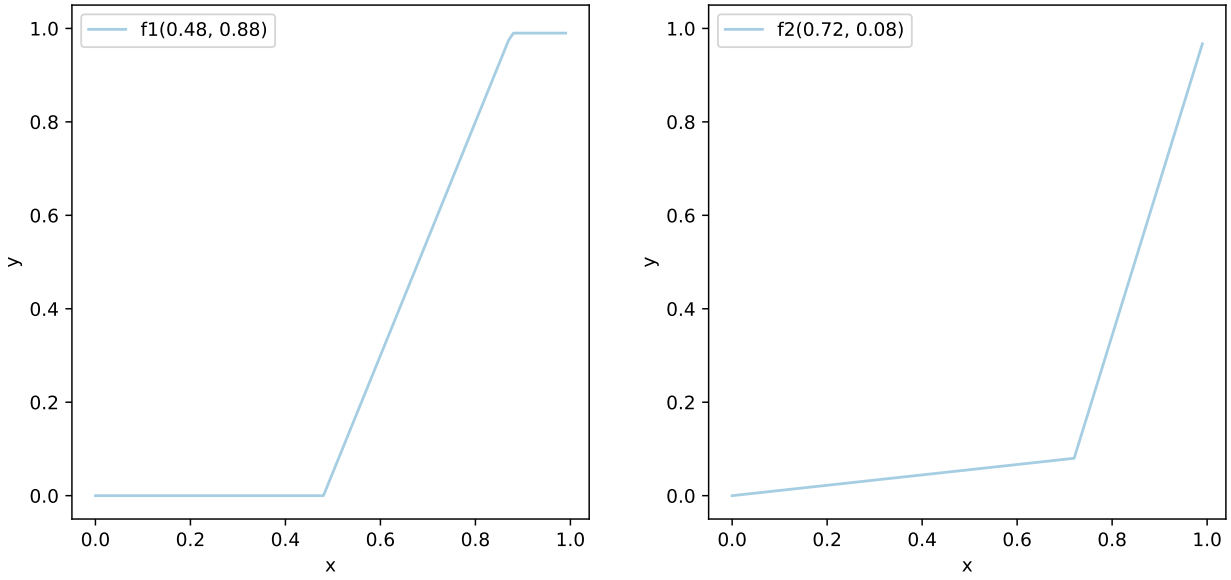

Figure 3: **Functions f_1 and f_2.**

Index	Precision	Recall	F1 Score	Accuracy
f1(0.48, 0.88)	0.745	0.751	0.747	0.751
f2(0.72, 0.08)	**0.765**	**0.767**	**0.759**	**0.767**

Table 6: **Metrics of combination methods using modulated belief mass.**

2.4 Conclusion

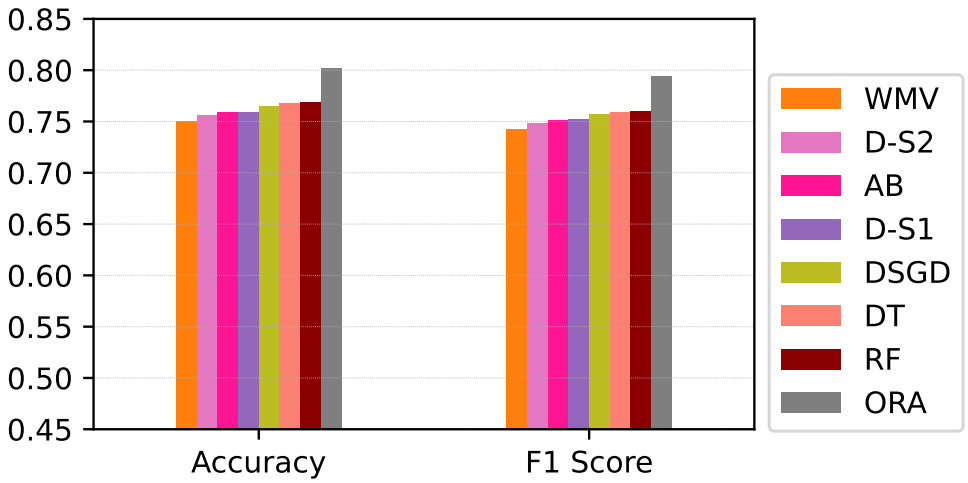

Figure 4: **Comparison of metrics of tested methods.** Legend: *WMV* – Weighted majority voting, *D-S1* – D-S method of confusion matrix distribution, *D-S2* – D-S method of two focal hypotheses, *DSGD* – D-S method optimized using the gradient descent algorithm, *DT* – Decision tree, *RF* – Random forest, *AB* – AdaBoost, *ORA* – Oracle.

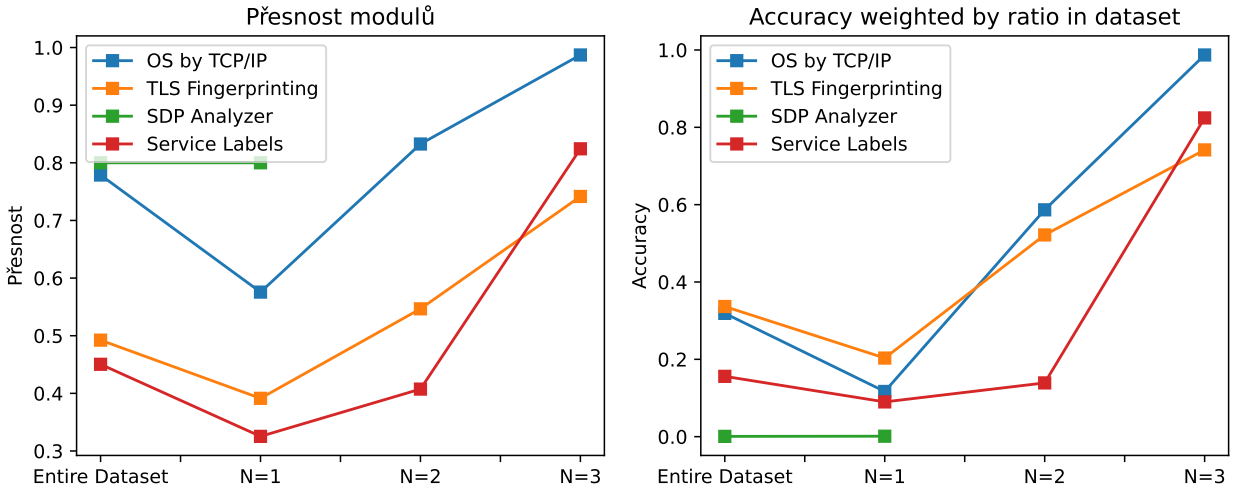

Figure 5: **Relation of modules' accuracy to the composition of the dataset.**

3 Generated Rules

```
#get_replacement_mf_single_class_optimized, optimized using f2, params (0.72, 0.08)
OperatingSystem.Android
  0.990: {'name': 'hostname', 'value': re('(?i)Android')} in .sdp_label

OperatingSystem.Linux
  0.990: contains('Fedora') in .tls_os_name
  0.990: contains('Debian') in .tls_os_name
  0.990: 'Sierra' in .tls_os_name
  0.874: 'High Sierra' in .tls_os_name
  0.722: contains('UNIX') in .tags_by_services
  0.539: 'Catalina' in .tls_os_name
  0.384: contains('Mac OS') in .tags_by_services
  0.079: re('(?i)(Linux|Orbis OS)') in .os_by_tcpip
  0.074: re('(?i)Debian') in .os_by_tcpip
  0.070: re('(?i)CentOS') in .os_by_tcpip
  0.066: contains('Windows') in .tags_by_services
  0.064: re('(?i)openSUSE') in .os_by_tcpip
  0.064: re('(?i)Ubuntu') in .os_by_tcpip
  0.059: 'Mojave' in .tls_os_name
  0.050: contains('Android') in .os_by_tcpip

OperatingSystem.MacOS
  0.990: 'El Capitan' in .tls_os_name
  0.4 - 0.8: [
    '_adisk._tcp.local' in .dnssd_query
    '_airport._tcp.local' in .dnssd_query
    '_apple-mobdev._tcp.local' in .dnssd_query
    contains('_apple-mobdev2._tcp.local') in .dnssd_query
    '_apple-pairable._tcp.local' in .dnssd_query
    '_ippusb._tcp.local' in .dnssd_query
    '_pdl-datastream._tcp.local' in .dnssd_query
    '_printer._tcp.local' in .dnssd_query
    '_ptp._tcp.local' in .dnssd_query
    '_rdlink._tcp.local' in .dnssd_query
    '_rfb._tcp.local' in .dnssd_query
    {'service': '_sftp-ssh._tcp.local'} in .dnssd_service
    {'service': '_ssh._tcp.local'} in .dnssd_service
    '_uscans._tcp.local' in .dnssd_query
    '_uscan._tcp.local' in .dnssd_query
    '_meshcop._udp.local' in .dnssd_query
  ]
  0.179: {'name': 'hostname', 'value': re('(?i)MacBook')} in .sdp_label

OperatingSystem.Windows
  0.990: contains('Windows 7') in .tls_os_name
  0.893: contains('Windows') in .os_by_tcpip
  0.104: contains('Windows 8.1') in .tls_os_name
  0.082: contains('Windows 10') in .tls_os_name
  0.078: contains('Mac OS X') in .os_by_tcpip
  0.068: contains('Windows 8') in .tls_os_name
  0.056: contains('Ubuntu') in .tls_os_name

OperatingSystem.iOS
  0.1 - 0.3: [
    '_airplay._tcp.local' in .dnssd_query
    '_raop._tcp.local' in .dnssd_query
    '_companion-link._tcp.local' in .dnssd_query
  ]
```