L-017

# 複数 TLS セッションの解析に基づくサービス同定の精度に関する一考察
# Accuracy of Service Identification based on Inspection of Multiple TLS Sessions

原 雅貴[†1] 韮澤 慎之介[†1] 中尾 彰宏[†2] 小口 正人[†3] 山本 周[†2] 山口 実靖[†1]
Masaki Hara[†1] Shinnosuke Nirasawa[†1] Akihiro Nakao[†2] Masato Oguchi[†3] Shu Yamamoto[†2]
Saneyasu Yamaguchi[†1]

## 1. はじめに

大規模災害時には輻輳が発生するため，被災者に必要なサービスを優先的に転送するようなトラフィック制御が求められると考えられ，そのためにはフローからサービスを同定する必要がある．簡易なサービス同定手法として，通信先 IP アドレスやポート番号を用いる手法があるが，同一の IP アドレス，ポート番号で動画共有サービス，クラウドサービス，メールサービスなどの複数のサービスを提供している場合は同定が困難となる．この課題を解決するために，過去に筆者らは IP アドレスやポート番号を用いずにフローからサービスを同定する，複数 TLS セッションの解析に基づいたサービス同定手法[1]を提案した．同手法では TLS セッションのクラスタリングに 2-gram 出現頻度を用いている．しかし，*n*-gram の *n* の最適値に関する考察がされていない．

本稿では，1-gram と 3-gram を用いた TLS セッションのクラスタリングの精度の評価を行い，適切な *n*-gram の *n* についての考察を行う．

## 2. TLS セッション

### 2.1 TLS セッション確立手順

TLS セッションの確立手順のうち，TLS プロトコルバージョンおよび暗号スイートの決定からサーバ証明書および公開鍵の送信までは平文で通信が行われるため，DPI などを用いてペイロードを解析することによりサービスの特徴などを抽出することが可能であると考えられる．また，共通鍵の送信以降は暗号化されて通信が行われるため，解析により特徴を抽出することは困難であると予想される．

### 2.2 TLS セッションのクラスタリング

近年の Web 上のサービスでは，単一の Web サイトと通信した際でも，複数の TCP コネクションが確立される．そして，各 TCP コネクションにて TLS セッションの確立が行われる．各 TCP コネクションにて確立される TLS セッションの非暗号部のデータは全て同一ではなく，1 サービスの中の通信であっても異なる．そして我々の研究[1]により，これらは *n*-gram 出現頻度の相関係数が高い少数のグループに分類できることが分かっている．例を図 1 に示す．サービスと通信した際，各 TCP コネクションで TLS セッションが確立される．各 TLS セッションの *n*-gram 出現頻度の比較を行うと，相関係数が高い例と低い例に分かれる．相関係数が高い例を同一グループとしてクラスタリングを行うと，図内左のメールサービスの例ではグループ A の出現回数は 4 回，グループ B の出現回数は 2 回となる．このように，

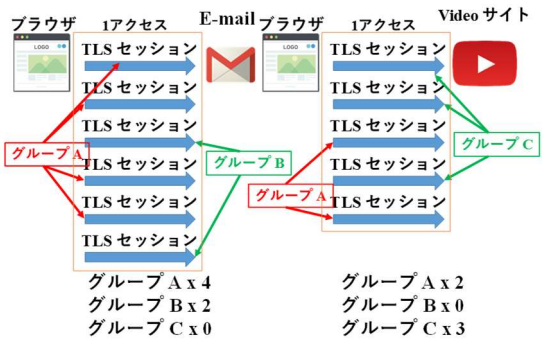


図 1 TLS セッションのクラスタリング

*n*-gram 出現頻度の相関係数の比較により，TLS セッションはクラスタリングすることが可能である．文献[1]では，2-gram を用いることにより適切にクラスタリングできることが確認されている．

## 3. サービス同定

筆者らが過去に提案したサービス同定手法として複数 TLS セッションの解析に基づいたサービス同定手法[1]がある．当該手法では，サービスにアクセスした際に確立される全てのコネクションに対して TLS セッション確立に用いられるフローの非暗号部の *n*-gram 出現頻度を調査し，コネクションの *n*-gram 出現頻度同士の相関係数を求め，相関係数が高いコネクション同士を同一グループに分類している．そして，各グループの出現回数に対して我々が修正したマンハッタン距離を計算し，最も距離が小さいサービスを同定結果として出力している．

当該手法の Google15 サービスにおける同定成功率は 93%[1]となり高い精度でサービス同定が実現できていることが確認されている．また，コネクションのクラスタリングは 2-gram により行われており，クラスタリングの適切さの評価も行われており，異グループに属する 2 コネクションの相関係数が，同一グループに属する 2 コネクションの相関係数を上回る例がなく，クラスタリングが適切に行われていることが確認されている．ただし，より計算量の少ない 1-gram，より計算量の多い 3-gram においても適切にクラスタリングできるかなどの評価はされていない．

## 4. 評価

本章にてクラスタリングに対する 1-gram，2-gram，3-gram の適切性の評価を行う．

Google15 サービスと複数回通信を行い，各 TLS セッション確立フローを 13 グループに分類した．今回，TLS セッションが分類されるグループ数は 13 としたが，これは各 TLS セッションの 2-gram 出現頻度の相関係数が 0.95 を超えるもの同士を同一グループとして分類した結果である．同一グループ内フロー間の 2-gram 出現頻度の相関係数の分布と，異グループフロー間の相関係数の分布を図 2 に示す．同一

[†1] 工学院大学大学院 工学研究科 電気・電子工学専攻
[†2] 東京大学 大学院 情報学環
[†3] お茶の水女子大学 理学部 情報科学科

グループ内フロー間では最低でも 0.974 の相関係数が得られており，異グループフロー間では最高でも 0.939 しか得られていない．すなわち，異グループフロー間の相関係数が同一グループ内フロー間の相関係数を上回る事例は存在していないことが分かる．

次に，2-gram 出現頻度を用いてクラスタリングを行った各 TLS セッションに対して 1-gram 出現頻度の相関係数を求めた．同一グループ内フロー間の 1-gram 出現頻度の相関係数の分布と，異グループフロー間の相関係数の分布を図 3 に示す．同一グループ内フロー間では最低でも 0.993 の相関係数が得られており，異グループフロー間では最高でも 0.989 しか得られていない．よって，2-gram 出現頻度を用いた場合と同様に 1-gram 出現頻度を用いた場合も異グループフロー間の相関係数が同一グループ内フロー間の相関係数を上回る事例は存在していないことが分かる．すなわち，閾値を 0.990 とすることにより 1-gram を用いてもクラスタリングは適切に行えることが分かる．しかし，1-gram 出現頻度を用いた場合の同一グループ内フロー間の相関係数の最低値と異グループフロー間の相関係数の最大値の差が小さいことから，サービス数の増加などによりクラスタリングが適切に行えない事例が生じる可能性が予想される．

次に，3-gram 出現頻度を用いてクラスタリングを行った．各 TLS セッションの 3-gram 出現頻度の相関係数が 0.95 を超えるもの同士を同一グループとして分類した結果，グループ数は 13 となった．同一グループ内フロー間の 3-gram 出現頻度の相関係数の分布と，異グループフロー間の相関係数の分布を図 4 に示す．同一グループ内フロー間では最低でも 0.962 の相関係数が得られており，異グループフロー間では最高でも 0.910 しか得られていない．よって，2-gram 出現頻度を用いた場合と同様に 3-gram 出現頻度を用いた場合も異グループフロー間の相関係数が同一グループ内フロー間の相関係数を上回る事例は存在していないことが分かる．また，3-gram 出現頻度を用いた場合の同一グループ内フロー間の相関係数の最低値と異グループフロー間の相関係数の最大値の差が 2-gram 出現頻度を用いた場合より大きいことが分かる．

本評価から，*n*-gram の *n* を大きくすることにより計算量は増加するが，同一グループ内フロー間の相関係数の最低値と異グループフロー間の相関係数の最大値の差が大きくなることが分かる．このことから，クラスタリング時間の短縮を重要と考える場合は 1-gram を用いることが適切であり，多くの状況では高い精度でクラスタリングできると期待できると言える．また，精度を重要視する場合は 3-gram を用いることが適切であり，さらにサービス数を増加させても適切なクラスタリングを行えると期待できる．

## 5. おわりに

本稿では，TLS セッションの解析に基づいたサービス同定手法の *n*-gram の *n* に関する評価と考察を行った．

今後は TLS セッションの Protocol Data Unit の解析を行っていく予定である．

### 謝辞

本研究は JSPS 科研費 26730040, 15H02696, 17K00109 の助成を受けたものである。

本研究は、JST、CREST JPMJCR1503 の支援を受けたものである。

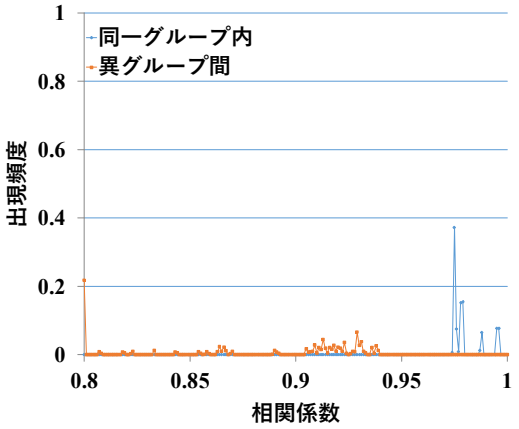


図 2 同一グループ内フロー間，異グループフロー間の相関係数（2-gram）

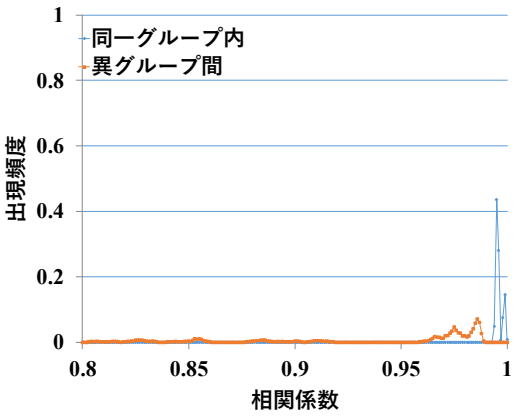


図 3 同一グループ内フロー間，異グループフロー間の相関係数（1-gram）

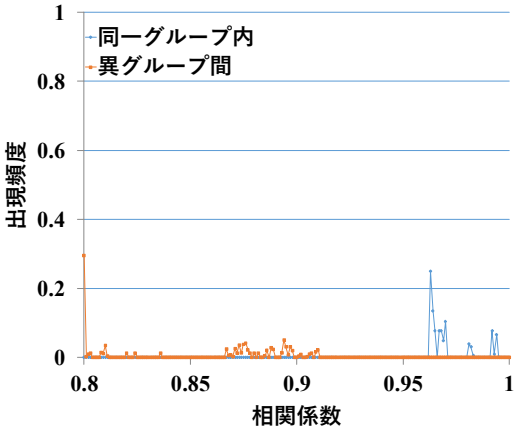


図 4 同一グループ内フロー間，異グループフロー間の相関係数（3-gram）

### 参考文献

[1] M. Hara, S. Nirasawa, A. Nakao, M. Oguchi, S. Yamamoto, and S. Yamaguchi, “Service Identification by Packet Inspection based on N-grams in Multiple Connections,” 7th International Workshop on Advances in Networking and Computing, 2016.