

2024年8月27日
第27回 ICN研究会ワークショップ

CCN網において関係匿名性を実現する 軽量匿名通信プロトコル^[1]

吉仲 佑太郎¹, 北 健太郎¹, 武政 淳二¹, 小泉 佑揮¹, 長谷川 亨²

¹ 大阪大学 大学院情報科学研究科 ² 島根大学 材料エネルギー学部

* 本研究は, JSPS 科研費 23H03383 によるものである.

盗聴によるプライバシーリスク

■ 大規模監視は攻撃である

RFC 7258: Pervasive Monitoring Is an Attack [2] (発表者訳)

IETF コミュニティによる技術評価によれば、大規模監視はインターネットのユーザと利用機関に対する攻撃である。(中略)

ここで、“攻撃”という用語は、通信者自身の同意を得ずに、通信者の意図を損なうような行動を指す。(中略)

攻撃とは、攻撃の実行者の動機には関わらない概念であり、大規模監視の動機は、国家レベルの無差別監視から、合法だがプライバシーを顧みない企業の目的、犯罪者による非合法的な行動まで、多岐にわたる。

■ 盗聴によるプライバシーリスク

IP網における盗聴

送信者と受信者のIPアドレスが漏洩する

- 送信者のIPアドレス: 漏洩する 😈
- 受信者のIPアドレス: 漏洩する 😈
- サーバ名: 漏洩しない ✓
DoHによるDNSメッセージの暗号化や、
TLS 1.3によるSNIの暗号化等により、秘匿可能
- データ名, データ: 漏洩しない ✓
TLS等によるエンド・ツー・エンド暗号化により秘匿可能

CCN網における盗聴

コンシューマに関する情報は秘匿されるが、
データに関する情報が多く漏洩する

- コンシューマの身元: 漏洩しない ✓
PITが返送路の情報を持つため、1st ホップ以外では秘匿可能
- サーバ名 (プレフィックス): 漏洩する 😈
名前によるルーティングを行うため、開示が不可避
- データ名 (サフィックス)・データ: 漏洩する 😈
キャッシュの検索・共有を行うため、開示が不可避

CCN網における匿名性

■ 望ましいプライバシー概念: **関係匿名性**

「誰であるか」と「何をするか」の切り離し
Decoupling who you are from what you do [3]

- 誰であるか: ユーザの身元 (e.g., アドレス, 識別子, 公開鍵)
- 何をするか: ユーザの行動 (e.g., 通信相手の身元, 要求するデータ, 実行する計算)

IP網における関係匿名性: 送信者-受信者・リンク不可能性 [3, 4]

送信者のIPアドレスと受信者のIPアドレスの両方を
特定することが、攻撃者にとって困難である

(送信者匿名性: sender anonymityまたは
受信者匿名性: receiver anonymityが満たされること)

- ホスト指向のネットワークアーキテクチャに依存する概念
- 上位層によりサーバ名・データ名・データ名が自明に
満たされること (秘匿性の実現) が前提

CCN網における関係匿名性: コンシューマ-データ・リンク不可能性 [1]

コンシューマの身元と、コンシューマが要求するデータの
両方を特定することが、攻撃者にとって困難である

(コンシューマ匿名性: consumer anonymityまたは
秘匿性: confidentiality が満たされること)

- プロデューサの身元 (プレフィックス) だけでなく、同時に
サフィックス, データも秘匿する必要

[3] Schmitt, Paul, et al. "The decoupling principle: A practical privacy framework." *Proceedings of the 21st ACM Workshop on Hot Topics in Networks*. 2022.

[4] Pfitzmann, Andreas, and Marit Hansen. "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management." (2010).

[5] Kuhn, Christiane, et al. "On Privacy Notions in Anonymous Communication." *Proceedings on Privacy Enhancing Technologies* 2019.2: 105-125.

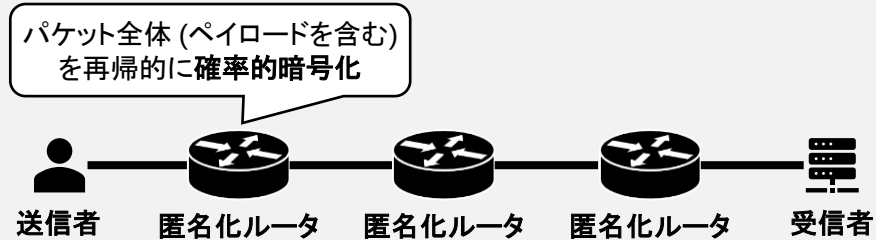
CCN網における軽量匿名通信

■ 軽量匿名通信プロトコル [6, 7]:

Torに代表されるOnion Routingと比較し、緩和された攻撃者モデルのもとで、通常の通信と遜色ない性能の匿名通信を実現する

- 限局的攻撃者の想定: 経路上の高々一つのノードのみを影響下に置く攻撃者を想定する
- ビットリンク可能性の許容: 経路上の匿名化ルータにおいて、ペイロードに対する暗号化・復号を行わない

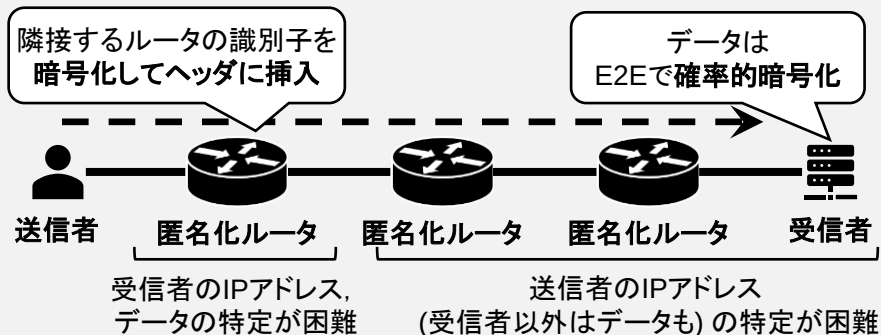
IP網におけるOnion Routing (e.g., Tor [8])



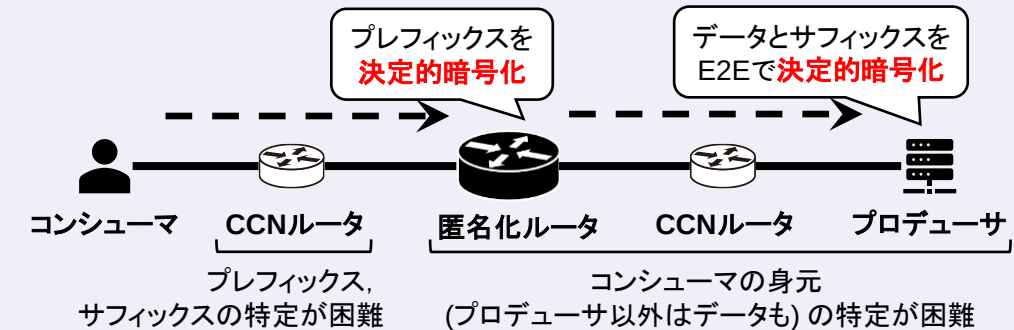
CCN網におけるOnion Routing (e.g., ANDaNA [9])



IP網における軽量匿名通信 (e.g., PHI [7])



CCN網における軽量匿名通信 (提案手法 [1])



[6] Hsiao, Hsu-Chun, et al. "LAP: Lightweight anonymity and privacy." 2012 IEEE Symposium on Security and Privacy. 2012.

[7] Chen, Chen, and Adrian Perrig. "PHI: Path-hidden lightweight anonymity protocol at network layer." Proceedings on Privacy Enhancing Technologies 2017.1 (2017): 100-117.

[8] Dingledine, Roger, Nick Mathewson, and Paul F. Syverson. "Tor: The second-generation onion router." USENIX security symposium. Vol. 4. 2004.

[9] DiBenedetto, Steven, et al. "ANDaNA: Anonymous Named Data Networking Application." Network and Distributed System Security (NDSS) Symposium, 2012.

ありがとうございました.