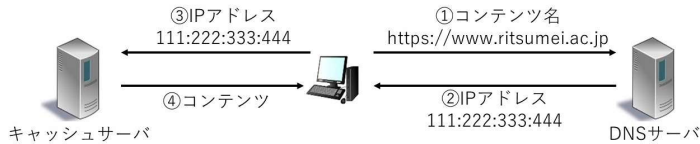


NDNにおけるプライバシー保護を考慮したアクセス制御方式

1. 研究の背景

■ 現在のIPネットワーク

- Domain Name System (DNS)
 - コンテンツの名前をDNSサーバに問い合わせることでIPアドレスを取得(名前解決)
- Content Delivery Network (CDN)
 - 要求ユーザの位置に基づき、近くに存在するキャッシュサーバからコンテンツを配信

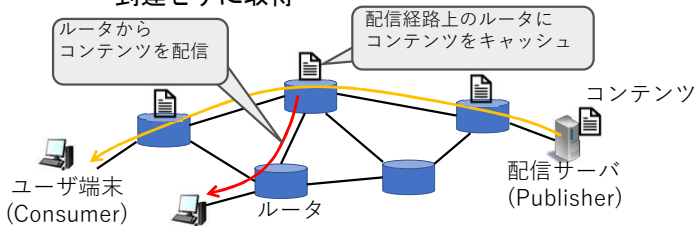


■ IoTでの問題点

- コンテンツ名が温度や位置情報といった曖昧な名称になるためDNSサーバによるIPアドレス解決が困難

■ Named Data Networking (NDN)

- 情報指向ネットワーク (ICN: Information-Centric Networking)の一種
 - コンテンツ名によるルーティング
 - DNSによる名前解決が不要
 - ルータがコンテンツをキャッシュ
 - 他ユーザからの要求も、コンテンツのあるサーバまで到達せずに取得



2. ICNの課題

■ ICNのPublisherによるアクセス制御

- ICNは要求のほとんどがPublisherには到達不可
- ルータによるアクセス制御
 - プロキシサーバや属性ベース暗号等
 - Netflix等の大規模PublisherのNDN移行が困難

■ プライバシー漏洩の課題

- ICNはコンテンツ名を平文で要求
- 盗聴によるプライバシー漏洩の問題

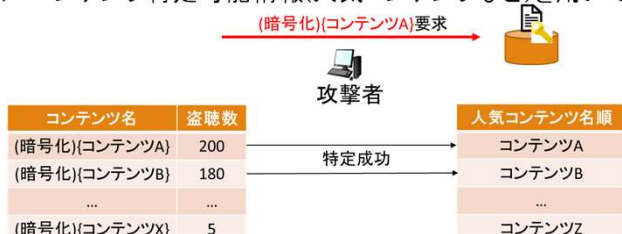
■ コンテンツ名暗号化による課題

- プライバシー保護を解決する手法
- 頻度攻撃の影響

3. 頻度攻撃

■ 暗号化コンテンツ名を特定する攻撃

- コンテンツ特定可能情報(人気コンテンツなど)を用いて特定



4. 研究の目的

■ ICNでのPublisherによるアクセス制御

- 閲覧者限定のコンテンツに対するアクセス制御が必要
- ICNではPublisherによるアクセス制御が困難

■ プライバシー保護を目的としたコンテンツ名暗号化

- コンテンツ名を平文で要求
- 盗聴によるプライバシーの漏洩問題

5. 提案方式の動作

■ Publisherのコンテンツ公開

- コンテンツをコンテンツ鍵で暗号化
- コンテンツ名を変更して公開

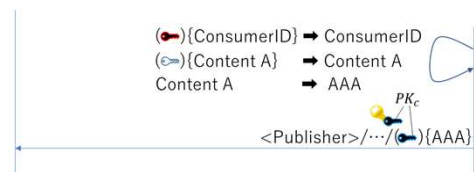
■ Consumerの初回Interest

- 変更後のコンテンツ名取得&コンテンツ鍵取得&アクセス制御
- コンテンツ名とConsumerIDを暗号化
 - コンテンツ名暗号化によるプライバシー保護
- 暗号化により固有の要求名で常にPublisherに到達
 - Publisherによるアクセス制御の実現



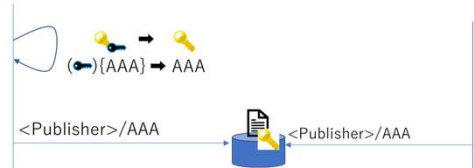
■ Publisherのアクセス制御&応答 packets

- 初回InterestのConsumerID復号
- Consumerの公開鍵で要求コンテンツ名に変換
- 公開済みコンテンツ名およびコンテンツ鍵を暗号化して返送



■ Consumerのコンテンツ要求

- コンテンツ鍵をConsumerの秘密鍵で復号
- 公開済みコンテンツ名をConsumerの秘密鍵で復号
- 公開済みコンテンツ名を使用してコンテンツ要求
- コンテンツ鍵を用いてコンテンツ復号



6. 今後の予定

■ 性能評価

- ネットワーク全体のキャッシュヒット率評価
- 頻度攻撃に必要な情報量から適切な鍵交周期の数値評価