SDN を用いた NDN のアクセス制御方式

1. はじめに

Information-Centric Networking (ICN) が現在最も注目を集めている. ICN のアーキテクチャの一つにNamed Data Netwoking (NDN) があり, NDN のキャッシュ技術は重要な研究分野である. コンテンツが公開されるとユーザの要求に応じてコンテンツの配信が行われ, コンテンツ配信に応じて配信経路上のルータにキャッシュが行われる. このキャッシュ機能により, コンテンツ要求の効率が大幅に向上する.

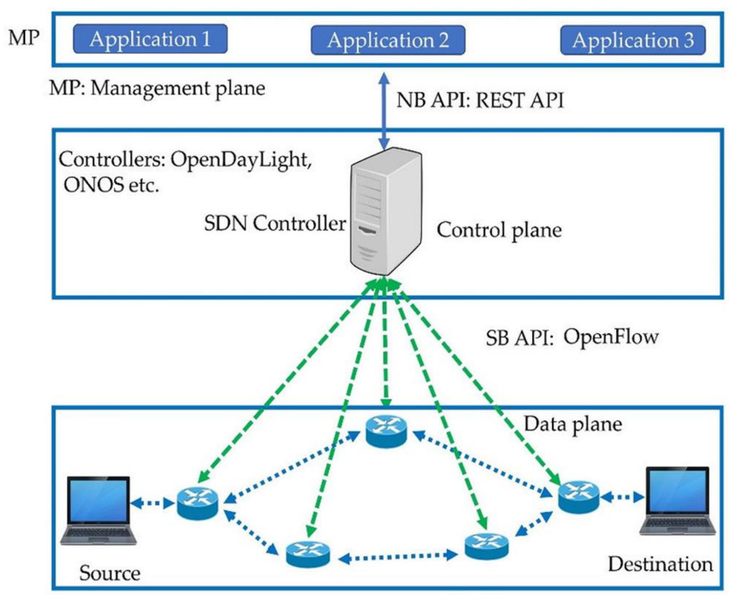
しかし, パブリッシャはキャッシュ機能によりコンテンツのアクセス状況を制御することができない. そのため, コンテンツに対するセキュリティのリスクが存在する. 従来のネットワークにおけるアクセス制御は, データチャネルベース(パブリッシャーはアクセス者の身元を知り、アクセスを許可するかどうかを決定することができる) であり, NDN におけるアクセス制御はコンテンツベースであるため, 異なるアクセス制御技術を必要とする.

2. 研究の目的

- ルータのアクセス制御を行うSDNを用いたNDNアーキテクチャの構築
- 期限があるCPABEを使用し、データのセキュリティをさらに強化

3.SDN

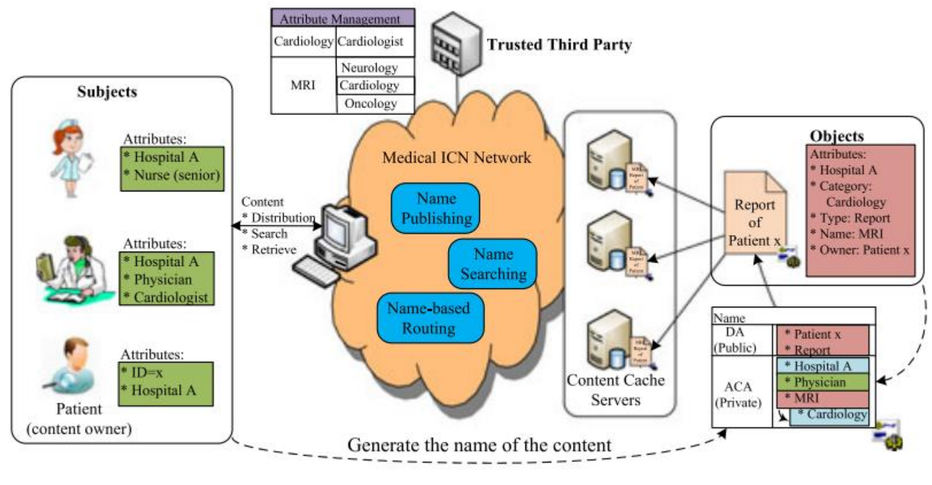
SDN(Software Defined Networking), ソフトウェアを介してネットワークを構成する機器を一括して制御する技術



ルータやサーバ、スイッチなど、ネットワークを構成している機器をソフトウェアを介して一括制御することで機器設定やネットワーク構成を柔軟に変更できる

4.CPABE

属性ベース暗号(Ciphertext-Policy Attribute-Based Encryption：CP-ABE)は, ユーザの属性を秘密鍵に, 復号条件(ポリシー)を暗号文に関連付けることにより, ポリシーを満たす属性を有するユーザーのみ暗号文を復号することが可能な公開鍵暗号方式である.

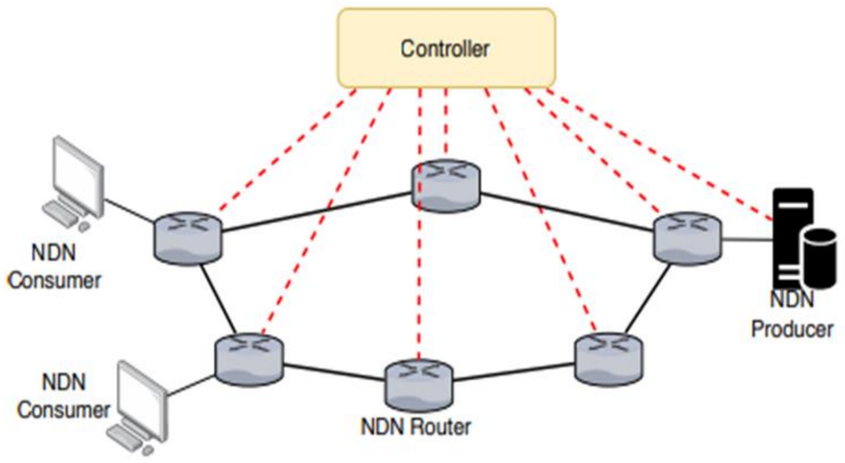


1つの暗号文に対して復号可能なユーザーが複数存在するようにできるため, 機密情報を複数のユーザーで共有したい場合に効率よく暗号化できる.

例えば、属性A、B、C、Dがあったとき、「AかつB」、「AまたはBまたはC」、「『AかつB』または『CかつD』」といったように、様々な制御条件を組み込むことができる。このように、属性ベースにすることで、コントロールの”柔軟性”と”自動化”を実現することができる.

4.提案方式

- CPABE
  - 暗号文/秘密鍵に期限を追加
  - 取り消しリストは期限切れ前に権限を取り消されたユーザを追加



- SDN
  - コントローラがCPABEの鍵を生成するセンターとユーザの権限管理センターとして機能
  - コントローラは全てルータ配下のユーザの情報を収集し、該当エリアのACLを生成して指定ルータに配信する

5. 今後の予定

- 提案方式のInterestパケット構成/処理ステップによると理論的なパケット大きさと処理時間を評価
- アクセス制御メカニズムの安全モデルを評価
- 提案方式が従来方式とユーザの取り消し時間の比較
- 提案方式が従来方式とのACL数の比較
- 提案方式が従来方式との暗号文サイズの比較
- 評価結果によに不足点の解決策を検討