

受信者の匿名性を送信者に対しても確保可能な DHT を利用した匿名通信路構築手法の提案

A Proposal of DHT-based Anonymous Routing for Preserving Pseudonymity of Message Receivers

及川 一樹* 王家宏* 児玉 英一郎* 高田 豊雄*
Kazuki Oikawa Jiahong Wang Eiichiro Kodama Toyoo Takata

キーワード 分散ハッシュテーブル, オニオンルーティング, 双方向匿名通信

現在, P2P ネットワーク技術は一般的なものとなり, BitTorrent といったファイルの転送を行うアプリケーションや, 映像配信を行うアプリケーションなどに広く利用されている.

P2P ネットワーク技術には中央に管理用サーバを持つハイブリッド P2P 型や, すべてのノードが対等な関係にあるピア P2P 型などの種類がある. ピア P2P 型は管理用サーバが不要で単一故障点が存在しないという点などで優れており, 問題点だったデータの探索効率が悪いという点も, 分散ハッシュテーブルに代表される構造型ネットワークの登場により解決され, 今後も様々な用途に活用されると考えられている.

分散ハッシュテーブルとは, ハッシュテーブルを複数のノードで管理する技術で, 各ノードをハッシュ値空間に写像し, その空間を各ノードで分割管理することで, ピア P2P 型でありながら, スケーラビリティに優れた探索を可能にする. そのため, 分散ハッシュテーブルでは, 各ノードにハッシュ値が割り当てられ, その値をキーにした探索が行われる.

この分散ハッシュテーブルを利用することにより, キーを宛先としたメッセージの送受信ができるようになるため, 仮名 (Pseudonym) をキーとすることで, インスタントメッセージなどといったアプリケーションがサーバレスで実現できるようになる. しかし, 分散ハッシュテーブルには匿名性が無いため, 宛先となるキーを知ることができれば, そのキーと IP アドレスの組み合わせが漏洩してしまい, 匿名性 (Pseudonymity) が確保できな

い. この問題は, インスタントメッセージのようなアプリケーションを想定した場合, 宛先となるキー (仮名) を信頼できる知人以外には漏らしてはならないことを意味し, 仮名を利用する意味が無くなってしまう.

既存研究として, 分散ハッシュテーブルを利用して匿名通信路を構築する手法は幾つか提案されているが, 内部告発といった送信者の匿名性が重要視される場面での利用を想定しているため, 送信者の匿名性や, 第三者に対する受信者の匿名性は確保されている. しかし, 宛先として分散ハッシュテーブルにおいてノードに割り当てられるキーを利用するため, 宛先を知っている送信者に対して受信者の匿名性は確保されていない.

そこで我々は, 分散ハッシュテーブルにオニオンルーティングを組み合わせることで, 匿名性を維持したまま自分宛のメッセージを受信することが可能な, 双方向匿名通信路の構築手法を提案する.

本提案では, 受信者の匿名性を送信者に対しても確保するため, 宛先として利用するキーと IP アドレスの組み合わせが特定できないようにする. そのため, 宛先として利用するキーと, 分散ハッシュテーブルにおいてノードに割り当てられるキーとを分離し, 組み合わせが特定できないようにした. 他にも本提案では, 送信者の匿名性を確保し, サーバレスでも運用可能なため, スケーラビリティに優れた手法となっている.

* 岩手県立大学大学院, 〒 020-0193 岩手県岩手郡滝沢村滝沢字菓子 152-52, Iwate Prefectural University, 152-52, Sugo, Takizawa, Takizawa village, Iwate 020-0193