L-034

P2P ネットワークおけるノードを階層化した公開鍵分散管理方式

Hierarchical Public Key Management for P2P Network

中山 誠也† 武田 敦志‡,† 北形 元†,§ チャクラボルティ デバシシュ§ 白鳥 則郎†,§
Seiya Nakayama Atsushi Takeda Gen Kitagata Debasish Chakraborty Norio Shiratori

1. まえがき

P2P ネットワークはサーバとなる計算機を必要としないため，従来のサーバ・クライアントモデルのネットワークと比べて，利便性や耐障害性などにおいて優れているが，端末間の認証が難しいという問題がある．既存手法である PKI[1]では，認証局と呼ばれるサーバが公開鍵などの認証情報を集中管理するため，特定のサーバが存在しない P2P ネットワークへの適用は難しい．

そこで本稿では，P2P ネットワークに参加するそれぞれの計算機端末（以降ノードと呼ぶ）が公開鍵を効率的に分散管理する手法を提案する．この手法ではネットワークに参加するノードの階層化を行うことで，携帯端末などの計算能力が低いノードであっても正しい公開鍵を取得し，端末間の認証を行うことが可能となっている．

2. 関連研究

サーバを必要としない公開鍵管理方式として PGP[2]がある．PGP は各ノードの利用者間の信頼関係を活用することにより，信頼できるノードを介して新たな公開鍵を収集することで，認証局を必要としない分散型の公開鍵管理を実現している．しかし，PGP は新たな公開鍵を検索するための仕組みを持たず，計画的な信頼の輪を形成することが出来ないため，任意のノードの公開鍵を入手するために，全てのノードの公開鍵を入手する必要がある．そのため，各ノードは公開鍵を管理するために多大なメモリ量を必要とし，必要な公開鍵を入手するために多くの通信メッセージを必要とする．

HDAM(Hash-based Distributed Authentication Method)[2]は，信頼の輪と分散ハッシュテーブル(DHT)を用いることで，適用するネットワークを限定せずに，効率的な分散認証を実現している．しかし，HDAM を用いると，ネットワークに参加するすべての計算機端末に一定の負荷が生じてしまうため，センサや携帯端末などの低性能なノードの参加に対応することが難しいという課題がある．

3. 提案：Hierarchical HDAM(HiHDAM)

3.1 HiHDAM の概要

提案手法では，効率的に公開鍵を分散管理するために仮想的にオーバーレイネットワークを構築する．その際，高性能端末を親ノードとし，ハッシュリング上に配置する．親ノードは，ハッシュリングにおいて自身の位置から正の方向に $2^k (k = 0,1,2,\cdots)$ 以上離れたノードのうち最も近い位置に配置されたノードの公開鍵と自身の子ノードの公開鍵を管理し，必要に応じて公開鍵の配布の中継を行うことで効率的な分散認証を実現する．ノード数が n のとき，親ノードに必要となる計算機資源（CPU，メモリなど）は $O(\log_2 n)$ である．また，低性能端末は子ノードとし，ハッシュリング上に配置せず，親ノードを介して必要な公開鍵を入手できるようにする．こうすることで，子ノードはハッシュリング上で行われる公開鍵の分散管理や公開鍵の配布の中継を行わなくてよいため，これに伴う暗号の復号化や電子署名の検証を行う必要がなくなる．これにより，低性能端末を子ノードとして参加させることが可能となる．図 1 に提案手法における公開鍵の分散管理の例を示す．

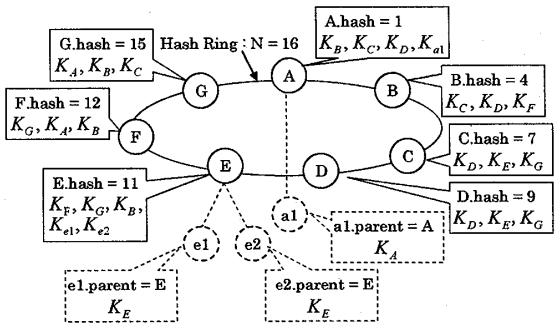

図 1 公開鍵の分散管理

3.2 ノードの参加手順

ノード n が HiHDAM に参加するときの前提条件として，n はすでに HiHDAM に参加している任意のノード g と公開鍵を交換済みであるものとする．図 2 にノード Z がノード B を介して HiHDAM に参加する際の例を示す．以下，本例をもとに処理手順を述べる．

1. Z はハッシュリング上で自身の正側に隣接するノード G の公開鍵 K_G を B から取得する．
2. Z は自身が公開鍵を管理すべきノード G,A,C の公開鍵を G から取得する．
3. G は自身の公開鍵を所有しているノード F,E,D,C に対して，信頼の輪の再構築を通知する．この通知を受けたノードのうち，F,E,D は Z の公開鍵 K_Z を G から取得する．

ノード数が n のとき，新たな親ノードが HiHDAM に参加するのに必要な通信データ量は $O(\log_2 n)$ である．また，Z が子ノードだった場合，Z は B を通して自身の親となるノードの公開鍵を取得することで HiHDAM に参加する．

3.3 ノードの離脱手順

親ノードが HiHDAM から離脱する場合，離脱ノードはハッシュリング上で隣接するノードに離脱通知を行い，この通知に従って隣接ノードは離脱ノードが存在しない信頼の輪を再構築する．このとき，離脱ノードの子ノードは，隣接ノードの子ノードとして HiHDAM に参加し直す．ノード数が n のとき，親ノードの離脱に必要な通信データ量は $O(\log_2 n)$ である．また，子ノードが HiHDAM から離脱する場合，自身の親ノードに離脱を通知することで，HiHDAM から離脱する．

†東北大学大学院情報科学研究科
‡東北文化学園大学知能情報システム学科
§東北大学電気通信研究所

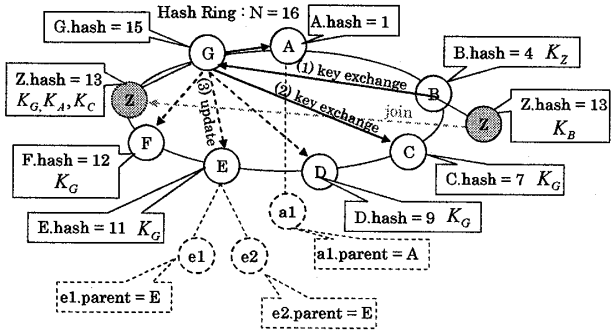

図 2　ノードの参加手順

4. 評価

4.1 シミュレータの概要

HiHDAM の特性を評価し，提案手法の有効性を示すために，Java を用いて P2P ネットワークの動作シミュレータを設計・実装した．このシミュレータは，ネットワークに参加するノードをエージェント（ノードエージェント）として実現したもので，ノードエージェント間でメッセージを送受信する際の通信をシミュレートする．図 3 にノードエージェントの状態遷移図を示す．ノードエージェントはネットワークに参加していない状態 (S_{out}) とネットワークに参加している状態 (S_{in}) を持つ．ノードエージェントは (S_{out}) の時に確率 P_{Login} でネットワークに参加し，状態 S_{in} に移行する．同様に S_{in} の時は確率 P_{Logout} でネットワークから離脱し，S_{out} に移行する．また，S_{in} の時は，確率 P_{Update} で自身の公開鍵を更新し，確率 $P_{Request}$ でランダムに決定された受信ノードに対して公開鍵を要求するメッセージを送信する．

以上の動作を行うシミュレータを用いて，各ノードが管理する公開鍵数と各ノードが処理するメッセージ数を計測し，HiHDAM と従来手法(HDAM)の比較評価を行った．今回ノードエージェントの設定パラメータは，$P_{Login} = 1.0$，$P_{Logout} = 0.45, P_{Update} = 0.05, P_{Request} = 0.5$ とした．また，提案手法における親ノードの割合はノード全体の 3 割とした．

4.2 各ノードが管理する公開鍵数

図 4 に，ネットワークに参加しているノード数と，各ノード 1 台あたりが最低限管理しなくてはならない公開鍵の数の関係を示す．従来手法の場合，ネットワークに参加するノードが増加するに従い，すべてのノードが保持する公開鍵の数も増加していくことがわかる．これに対し提案手法においては，子ノードが保持しなくてはならない数は参加ノードの数にかかわらず常に 1 個だけであった．また，親ノードが保持しなくてはならない公開鍵数も従来手法におけるすべてのノードが管理する公開鍵の数とほぼ同程度の量に抑えることが出来た．よって，提案手法は低性能端末のノードでも参加可能なスケーラブルな分散管理方式であるといえる．

4.3 各ノードが処理するメッセージ数

図 5 に，ネットワークに参加しているノード数と，各ノード 1 台あたりが処理するメッセージ数の関係を示す．従来手法では，ネットワークに参加するノードが増加するに従い，すべてのノードに生じる負担が増加していることがわかる．これに対し，提案手法の子ノードが処理するメッセージは極めて少なく，提案手法は低性能端末のノードでも公開鍵の確実な配布を受けることが出来るスケーラブルな分散管理方式であるといえる．

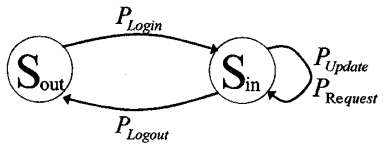

図 3　ノードエージェントの状態遷移図

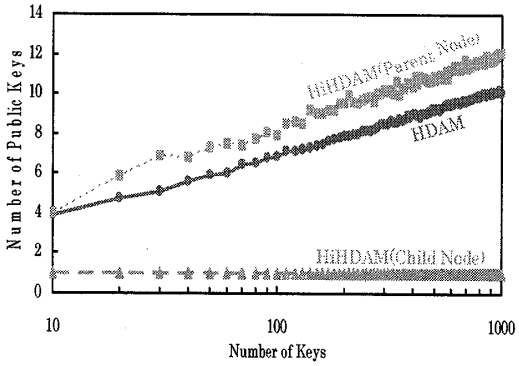

図 4　ノード数と公開鍵数の関係

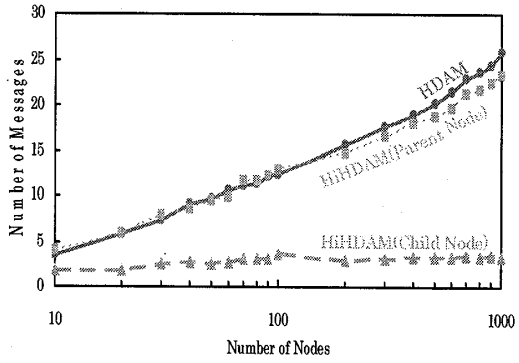

図 5　ノード数とメッセージ数の関係

5. むすび

本稿では，信頼の輪と分散ハッシュテーブルを用いてネットワークに参加するノード全体で公開鍵を効率的に分散管理する手法 HiHDAM を提案した．HiHDAM では，ネットワークに参加するノードを階層化することで，センサや計算機端末などの計算能力が低いノードであっても要求した公開鍵を確実に受け取ることが出来る．コンピュータシミュレーションにより，HiHDAM は従来手法に比べ，利便性とスケーラビリティに優れていることを確認した．

参考文献

[1] R Housley, et al. Rfc 3280: Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile, 2002

[2]Garfinkel, S.: PGP : Pretty Good Privacy, Oreilly and Associates Inc. 1994.

[3]Takeda A, et al. Proposal and Performance Evaluation of Hash-based Authentication for P2P Network, IPSJ Journal, Vol.50, No.2, pp.737-749 2009.