6D-1

DHTにおける認証ノードに対する評価値を考慮した分散認証手法の提案*

真下 洋† 新崎 裕隆‡ 上田 真太郎‡ 重野 寛†
慶應義塾大学理工学部† 慶應義塾大学大学院理工学研究科‡

1 はじめに

P2P システムにおいて，悪意ある参加者が多数のノードを参加させてシステムの掌握，妨害を試みる攻撃 Sybil Attack [2] がある．それに対して，DHT (Distributed Hash Table) において新規ノードの加入の是非を多数決で決定する分散認証手法 Self-Registration [3] が提案されている．本論文では，Self-Registration を元に，認証ノードに対する評価値を導入することによって，よりセキュアな分散認証を行う手法 Self-Registration with Judgement Evaluation (SRJE) を提案する．SRJE と Self-Registration について，悪意あるノードのネットワークへの侵入防止効果を，シミュレーションにより比較評価する．

2 背景

以下では，本論文で DHT スキーマとして使用している Chord [1] と，Sybil Attack，Self-Registration について説明する．

2.1 Chord

DHT の最も代表的なスキーマに，Chord がある．Chord は，Chord リングと呼ばれる 1 次元環状の ID 空間にノードとコンテンツを配置する．検索等の際には，ID をキーとするクエリを Chord リングに沿って時計回りに転送して目的のノードまでルーティングする．また，あるノードから反時計回りに見た時の最隣接ノードを predecessor という．

経路中のノードがクエリの転送を怠ったり，多数のノードが一斉に離脱したりしてしまうと，システムが機能しなくなるという問題がある．

2.2 Sybil Attack

DHT を利用する P2P ネットワーク，多数のノードを操る悪意ある参加者がシステム全体に影響を及ぼすことが可能となる．1 参加者 (IP アドレス) が多数のノードを利用してシステム全体を掌握してしまう攻撃を Sybil Attack という．[2] では，信頼できる中央認証サーバを用いない限り解決は難しいと主張している．

2.3 Self-Registration

Self-Registration は Sybil Attack に対して分散的なアプローチからその抑制を試みたものである．各参加者にノード数制限をかけ，1 参加者のノード ID を複数の認証ノードに登録し，同じ参加者が次に新規ノードをネットワークに参加させようとした時に，認証ノードの多数決で可否を決める．

対して悪意あるノードは，制限数を越えたノードを参加させ，そうでないノードを参加させまいとする．これらの達成を誤認証という．

Self-Registration は，悪意ある参加者の割合が低い場合は効果を発揮する．[3] では，悪意ある参加者の割合を $p_p = 0.02$ として効果を確認している．しかし，p_p が増加すると，早々にノード数制限が破られてしまう．

3 SRJE の提案

Self-Registration で誤った認証が成功するのは，悪意ある認証ノードが認証ノードの過半数を占めた時である．正常な認証ノードが多勢を占めている時に，悪意ある認証ノードが偽りの判断を他認証ノードに送ると，その判断は特異な判断となる．よって，この段階でそのノードをマークしておくと，別の認証の機会に判断の重みを下げることができ，悪意ある認証ノードが過半数を占めても predecessor が適切な判断を下すことが可能になる．そこで，各ノードが他ノードに対する評価値を保持し，判断に利用する認証手法 Self-Registration with Judgement Evaluation (SRJE) を提案する．新規ノードは参加の際，自分を登録する r 個の認証ノードを決定する．j 番目 $(1 \leq j \leq r)$ の認証ノード ID は，$regId_i^j = hash(j \oplus ipAddress_i)$ で決定される．これらのノード ID をキーとして，join クエリを送信する．

*Proposal of Decentralized Authentication Technique for DHT using Evaluations of Authentication Nodes
†Faculty of Science and Technology, Keio University
‡Graduate School of Science and Technology, Keio University

join クエリを受け取った認証ノード n_j は，新規ノードの ID の真正性と制限数非超過の確認を行い，自身の判断 $J_j(=1\ or\ -1)$ を決定し他認証ノードに送る．一定時間判断を収集してして，$J=\{J_i|1\leq i\leq r\}$ と，自身の保持する評価値テーブルから求めた重み $E=\{E_i|1\leq i\leq r\}$ の内積をとり，その正負で最終的な決断 D_j を決定し，predecessor に自分の判断として送る．predecessor は自分の評価値テーブルを参考に，それらの集計を行い，新規ノードの参加の可否を決定する．

ここで，評価値は上がることはなく，評価値テーブルには評価の下がったノードのみが追加される．また，自身の評価値 E_j は他の評価値よりも高く設定し，不変とする．

4 シミュレーションによる評価

JAVA で Self-Registration と SRJE のシミュレーションモデルを実装し，時間経過に伴うネットワーク全体のノード数変化を調べた．なお，シミュレーションの始めに正常なノードを 50 ノード参加させている．

4.1 実験環境

表 1 にシミュレーション条件を示す．

表 1: シミュレーション条件

悪意のある参加者の割合 p_p	0.15
認証ノード数 r	10
1 参加者当たりのノード制限数 a	2
シミュレーション時間 [tu]	4500
ノードのライフタイム [tu]	750
参加者参入間隔 [tu]	1.5

4.2 評価

図 1 に，Self-Registration を用いた場合のシミュレーション結果を示す．ここで，Well は正常なノード数，Mal は悪意のあるノード数，Expected はシミュレーション条件から期待される悪意のあるノード数である．図 1 から，ノード数制限が破られ，悪意のあるノードが急増していることが判る．

表 1 に示した以外の条件（乱数シード）を変えてシミュレーションを行ったところ，1 度も成功しなかった．ここで，成功とは悪意あるノード数が全体の半数を超えないことを指す．

図 2 に，SRJE を用いた場合のシミュレーション結果を示す．lower Expected は，図 1 の Expected に対応する期待値である．図 2 より，悪意あるノード数はほぼ許容可能な値を維持しており，急激に増えたり過半数を越えたりしていない事が判る．

SRJE を用いた場合，成功率は 70% であった．

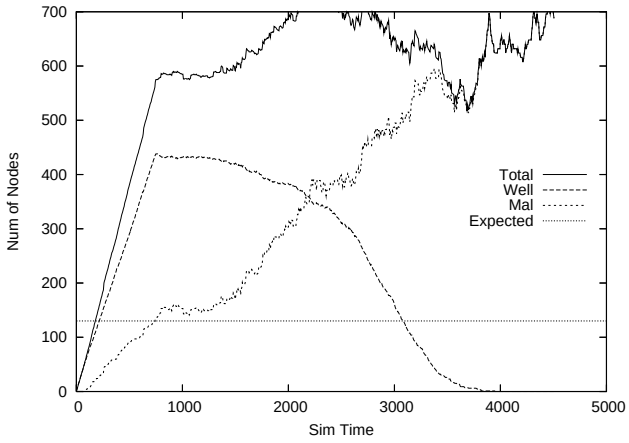

図 1: Self-Registration の失敗

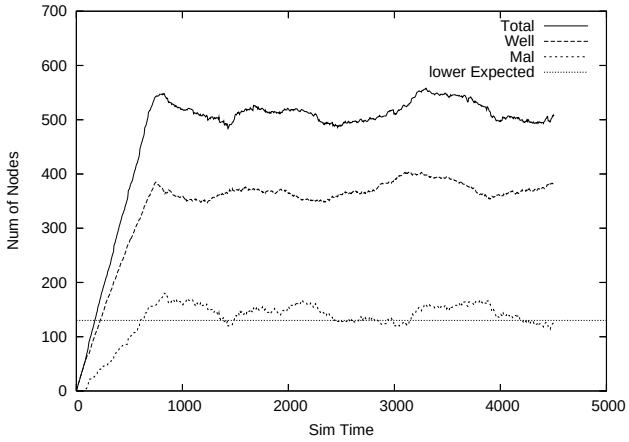

図 2: 時間経過に伴うノード数の変化

5 まとめ

本論文では，DHT における Sybil Attack を抑制する分散認証手法 Self-Registration を改良した手法を提案した．シミュレーションを行い評価した結果，悪意ある参加者の増加に対し，Self-Registration よりも耐性があることを確認した．

謝辞

本研究の一部はグローバル COE プログラム「アクセス空間支援基盤技術の高度国際連携」により行われた．

参考文献

[1] Ion Stoica et al,“ Chord: A scalable peer-to-peer lookup service for internet applications ”, In Proc. of the 2001 ACM SIGCOMM Conference, pp.149-160, 2001.

[2] J. Douceur,“ The Sybil Attack ”, IPTPS ’02, pp.251-260, 2002.

[3] J. Dinger et al,“ Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration ”, ARES ’06, pp.756-763, 2006.