

A-004

DHT ルーティングシステムにおけるデータ分割配置手法の検討

A Note on Data Fragmentation and Distribution Scheme for DHT Routing System

原田 脩平[†] 石川 康太[†] 新井 雅之[†] 福本 聡[†] 岩崎 一彦[†]
 Syuhei Harada Kota Ishikawa Masayuki Arai Satoshi Fukumoto Kazuhiko Iwasaki

1. はじめに

近年 P2P (Peer-to-Peer) システムが発展を遂げてきた。特に、分散ハッシュテーブル (DHT: Distributed Hash Table) の登場によってシステムのスケーラビリティが向上した。しかしながら、現状の DHT システムではデータの漏洩や、データの紛失といった問題がある。

本研究では、そうした問題を考慮して、DHT ルーティングにおけるデータ分割配置手法を提案する。提案手法では中国人の剰余定理を用いたデータの符号化・復号手法を用いてデータの断片化を行い、その各断片をネットワーク上のノードに分散配置する。ノード障害下における提案手法の有用性を解析およびシミュレーションによって評価する。

2. 先行研究

DHT システムでは、各ノードはコンテンツデータと隣接ノード情報の他にデータの位置情報をハッシュ表として保持する。DHT では、このハッシュ表を利用してルーティングを行う。

Kong らは代表的な DHT システムのスケーラビリティを評価した [1]。ノード障害率一定の条件下でノード数を無限大としたとき、任意の生存ノードに到達可能であればそのシステムはスケーラブルであると定義し、RCM (Reachable Component Method) 手法による解析の結果、Hypercube 型、Ring 型、XOR 型システムがスケーラブルであることを示している。

また、Chessa らは、モバイルワイヤレスネットワークにおいて、データを断片化し、ネットワーク上に分散配置することでデータの機密性を確保する手法を提案した [2]。データの符号化・復号手法として、RRNS (Redundant Residue Number System) を適用している。RRNS では、元となるデータは s 個に分割され、 t 個の冗長な断片が付加される。 $(s+t)$ 個の断片のうち、 s 個の断片を取得することで元データを復号することができる。符号化・復号には互いに素な自然数の組を鍵として用い、セキュリティ向上に寄与している。

3. DHT ルーティングにおけるデータ分割配置手法

本研究では、DHT システムにおけるデータ分割配置手法について提案する。

提案手法では、データを持つノードは RRNS を用いてデータを $(s+t)$ 個に断片化し、一意にファイル名を付加する。次に、これらの断片データに対しファイル名からハッシュ値を計算し、ハッシュ値を基にネットワーク上のノードへ分配する。分配方法として、同一ノードへの重複を許す場合と許さない場合が考えられる。これらは分配に関するコストとセキュリティのトレードオフの関係にある。

データを取得したいノードはデータのファイル名から断片データのハッシュ値を計算し、それを基に、並列に探索を開始する。 $(s+t)$ 個の断片データのうち s 個を取得したら探索を終了し、得られた s 個の断片データによって元データの復号が完了する。

図 1 にデータの断片化と分配の概要図を示す。この例においてデータは 3 個に分割され、2 個の冗長な断片が付加されている。したがって、データを取得したいノードはこれら 5 個の断片のうち 3 個を取得できれば元データを復号できる。RRNS によってデータの機密性や、耐損失性の向上、探索遅延に関する性能改善が期待される。

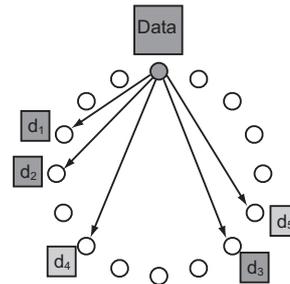


図 1: データの断片化と分配の例 ($s=3, t=2$)

4. データ分割配置手法の評価

4.1 データ取得率の解析的評価

データ取得率 $R(q)$ を以下のように定義し、Hypercube、Ring および XOR を対象として、解析的に評価を行う。ただし、 q はノード障害確率とし、障害発生時にはノードは応答不能となることを想定する。

- $R(q)$: ノード障害確率 q のもとで、最終的に目的のデータを取得できる確率。

[†]首都大学東京 大学院 システムデザイン研究科, Graduate School of System Design, Tokyo Metropolitan University

提案手法において、 h ホップ目に断片データが存在し、取得可能となる確率を $G(h, 1)$ とする。また、 h ホップ目に断片データが存在し、取得不能となる確率を $G(h, 0)$ とする。ノード数を N 、最長となるホップ数を $d (= \log N)$ とするとき、同一ノードへの重複分配を許す場合の $R(q)$ は式 (1) のように得られる。図 2 は Ring, Hypercube

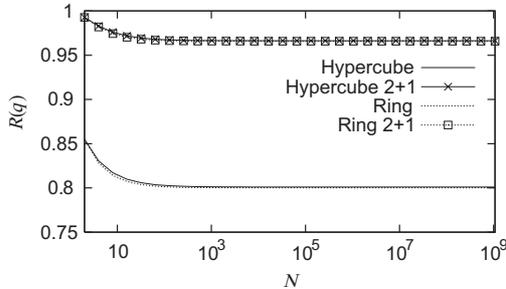


図 2: ノード数に対するデータ取得率 ($q = 0.10$)(Ring, Hypercube)

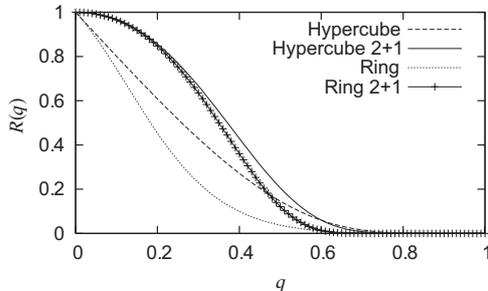


図 3: q に対するデータ取得率 ($N = 2^{30}$)(Ring, Hypercube)

$$R(q) = \sum_s \sum_{\substack{\text{for all combi} \\ \text{of } (x_1, x_2, \dots, x_{s+t}) \\ 0 \leq x_i \leq d}} \sum_{\substack{\text{for all combi} \\ \text{of } (y_1, y_2, \dots, y_{s+t}) \\ y_i \in \{0, 1\}, \sum y_i = k}} \prod_{i=1}^{s+t} G(x_i, y_i) \quad (1)$$

における $q = 0.10$ の際のノード数に対するデータ取得率の数値例である。図中の (2+1) で示されるグラフは、提案手法において $s = 2, t = 1$ とした場合を表している。いずれのシステムも従来手法に比べ提案手法の方が高いデータ取得率を達成しており、提案手法はスケーラビリティを改善することを示している。

図 3 は Ring, Hypercube における $N = 2^{30}$ の場合の、ノード障害確率に対するデータ取得率の変動を示す。これから、提案手法を適用することによって、高いデータ取得率を達成できることが判る。

重複分配を許さない場合の解析および数値例については、紙面の都合で省略する。

4.2 データ探索時間・アクセスコストのシミュレーションによる評価

提案手法におけるデータ探索時間およびアクセスコストを次のように定義し、Hypercube および Ring を対象として、シミュレーションによって評価する。

データ探索時間: データ探索に要する平均ステップ数。

アクセスコスト: データ探索に要する平均アクセス数。ただし、1 アクセスに要する時間を 1 ステップと定義する。

データ探索時間のシミュレーションについて、Hypercube の結果を図 4 に示す。提案手法における取得可能時の探索時間は、分割数 > 冗長数の場合、従来手法よりも時間がかかることが判る。逆に、分割数 \leq 冗長数の場合、提案手法が従来手法よりも短時間で探索を終了する。

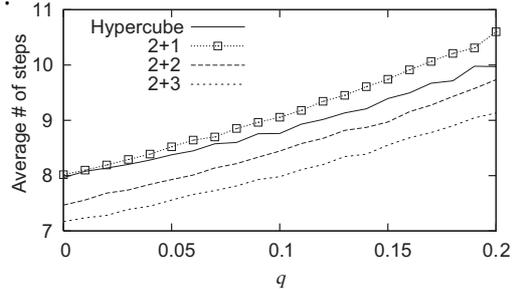


図 4: 取得可能時のデータ探索時間 ($N = 2^{16}$) (Hypercube)

アクセスコストに関しては総分割数が大きくなるほど増加し、同じ総分割数の場合は、冗長度が高くなるほど低く抑えられることが判った。詳細については紙面の関係で省略する。

5. まとめ

本研究では、DHT システムにおけるデータ分割配置手法を提案した。代表的な 3 個の DHT システムに対しこれを適用した。データ取得率について解析的に評価を行い、データ探索時間およびアクセスコストについてシミュレーションで評価を行った。データの断片化により、スケーラビリティを改善できること、断片データの冗長度を高めることで、データ取得に要する時間を短縮できることを示した。

ノード探索の際のアクセス数の増大が欠点であるため、提案手法はトラフィックの負荷を許容できる環境において有用な手法であると言える。

今後の課題として、ノードの参加および離脱を考慮した動的な解析を行うことなどが挙げられる。

参考文献

- [1] J. S. Kong, A. Bridgewater, and V. P. Roychowdhury, "A General Framework for Scalability and Performance Analysis of DHT Routing Systems," Proc. DSN, pp. 343-354, 2006.
- [2] S. Chessa and P. Maestrini, "Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks," Proc. DSN, pp. 207-216, 2003.