

LL-013

## ピアツーピアシステムにおける不正ノードの動的回避 Dynamic Avoidance of Illegal Nodes in P2P System

佐藤 一帆<sup>†</sup>  
Kazuho Sato

吉田 紀彦<sup>†</sup>  
Norihiko Yoshida

### 1. はじめに

P2P システムは、コンテンツの所在情報の検索方法によって HybridP2P と PureP2P に分けられる。このうち、Gnutella に代表される PureP2P システムは、単一障害点となるサーバが存在しないため耐障害性が高いとされる。しかし、Gnutella で用いられているコンテンツの検索方法は、検索のための情報がノード間を伝わる過程で書き換えられる可能性がある。検索情報の書き換えを行う不正なノードをシステムから隔離することが望ましいが、情報は複数のノードを経由しており、その過程を把握するノードは存在しないため、不正なノードの特定は困難である。

そこで、本研究では Gnutella の検索における検索情報の書き換え問題を解決するため、情報を書き換える不正なノードを回避する方法を提案する。

### 2. Gnutella 型の P2P における障害

HybridP2P においてはサーバが単一障害点であり、サーバに障害が起きるとシステム全体の機能が停止する可能性がある。しかし、システムはサーバにより管理されているため、サーバに障害が起きなければ個々のノードの障害が他のノードに波及することはない。

一方、Gnutella のような PureP2P においては単一障害点は存在せず、システム全体の耐障害性は高い。だが、ノード同士が直接情報を交換しながら動作するため、個々のノードの障害が周囲のノードに悪影響を与えることがあり得る。ここでは、Gnutella 型の P2P システムにおける障害について検討する。

#### 2.1 ノードの故障

ノードの故障とは、ノードが停止・もしくは意味のない応答を返す状態をいう。これにより、故障ノードとの通信ができなくなり、また故障ノードの先に存在するノードとの通信も不可能になる。しかし、PureP2P では各ノードは対等な役割を果たすため、故障ノードへメッセージを送ることを止め、他のノードにメッセージを送ることで障害を回避できる。

#### 2.2 妥当でないメッセージ

妥当でないメッセージとは、システム全体に悪影響を及ぼすような内容を含むメッセージを指す。例えば Gnutella において TTL(TimeToLive) が非常に大きな Ping パケットが送られた場合 [1]、そのパケットはネットワーク中に転送され続けることになり、ネットワークの負荷を高めることになる。同様の問題は、あるノードがパケットを過剰に送出し続けた場合にも発生する。

これらの問題に対しては、各ノードが受信したメッセージの妥当性をチェックすることにより解決できる。メッセージ中の TTL やペイロードのチェックを行い、妥当で

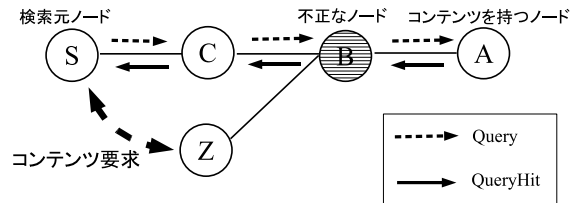


図 1: QueryHit の書き換え例

ないメッセージであると判断したら破棄する。メッセージを過剰に送出するノードに対しては、接続を切断することも考えられる。

#### 2.3 メッセージの書き換え

これは、悪意を持ったノードやバグを含んだノードによって、転送の際にメッセージの内容が書き換えられることである。図 1 に示した、Gnutella における QueryHit パケット中の応答ノード IP アドレスの書き換えは、その代表的な例である。この例は、検索元ノード S が送った Query に対してコンテンツを持つノード A が QueryHit を返すが、ノード B によってコンテンツを持つノード A の位置情報がノード Z に書き換えられたものである。このように、検索情報が書き換えられると、正しくコンテンツを発見することができなくなる。同様に、Query が書き換えられる場合やノードが誤った QueryHit を返す場合でも、コンテンツの発見が正しく行われれないという問題が起きると考えられる。

メッセージの書き換えが行われても、妥当性が保たれている限り破棄の対象とはならないため、書き換えられたメッセージが次々に転送されていくことになる。上の例では、コンテンツの取得に支障が出るまで QueryHit パケットの書き換えがあったことは検出されない。つまり、検索元ノードのみが書き換えを検出可能である。しかし、QueryHit パケットはいくつかのノードを経由しているため、検索元ノードから、書き換えを行ったノードを特定することはできない。このため、QueryHit パケットを書き換えるようなノードの影響を取り除くことは困難である。以下では、メッセージの書き換えを行うノードを不正ノードと呼ぶこととする。

### 3. 不正ノードの動的回避

2.3 で述べたように、PureP2P システムではメッセージの書き換えを行うノードが特定できないため、その影響を取り除くことが難しい。

[2] では、分散ハッシュテーブルを用いた P2P システムにおいて、悪意のあるノードが存在していても、正しいメッセージ転送がなされる手法が提案されているが、これは構造化されていない P2P システムには適用できない。また、自律分散系における耐故障性の研究では、

<sup>†</sup>埼玉大学 Saitama University

ノード間で情報を交換し合うことで障害を起こしているノードを特定し、障害隔離と復旧を行うアルゴリズムが提案されている [3][4]。しかし、この方法も P2P システムへの適用は困難である。

そこで、本研究では Gnutella における QueryHit の書き換えに対して、不正ノードを動的に回避する方法を提案する。

### 3.1 隣接ノードの評価

不正ノードの位置を特定する方法として、ノード間で特別な情報を交換し合い、その情報に基づいて各ノードが障害を起こしている不正ノードの位置を判断することが考えられる。[3][4] では、ノードが相互に障害を検査し、検査結果を交換・総合することで故障ノードの位置を特定するが、P2P システムでは 1 ノードあたりの隣接ノードの数が少ない場合があるため、十分な数の検査結果を交換することができず、この方法を用いて不正ノードの位置決定を行うことは難しい。さらに、他ノードの情報を利用して不正ノードの位置を特定する方法は、悪意を持ったノードが偽の情報を送ることにより、妨害される可能性がある。そこで、提案手法では特別な情報を交換せず、各ノードが利用した QueryHit の正当性によりノードを評価することとする。また、QueryHit が書き換えられたものであっても、それが隣接ノードで書き換えられたものなのか、隣接ノードの先に存在するノードで書き換えられたかを区別することはできない。しかし、隣接ノードもしくはその先に不正ノードがあるのは明らかであるので、どこで書き換えられたかを考えずに、隣接ノードについてのみ評価することとする。

### 3.2 不正ノードの回避

不正ノードの影響を回避するためには、必ずしも接続を切り離す必要はなく、Query を不正ノードに到達させなければよい。Query が到達しなければ書き換えを受けるとはなくなるため、不正ノードの影響を回避したといえる。Query の到達範囲を制限するためには TimeToLive(TTL) が使われるが、これを不正ノード回避に利用する。具体的には、隣接ノードの評価に応じて TTL を減らして Query を送信することで、不正ノードへの Query 到達を回避する。また、他ノードが送信した Query に対しても TTL を余計に減らす操作を行い、他ノードが不正ノードに Query を送信することも回避する。他ノードが送信する Query に対しても TTL を減らす操作により、自ノードの評価が下がることを防ぐこともできる。

### 3.3 詳細設計

不正ノードの回避のために、各ノードが行うべき具体的な動作は次のとおりである。ノードは隣接するすべてのノードに対しそれぞれペナルティを設定する。ペナルティの最小値は 0、最大値は Query の TTL の最大値である。そして、ノードは自分宛の QueryHit を評価し、不正な QueryHit を受信したときはその QueryHit を転送してきた隣接ノードのペナルティを増やす。逆に、正常な QueryHit を受信したときはペナルティを減らす。こうして決まる各隣接ノードのペナルティの値に従い、ノードが Query を送信する場合には、式 (1) のように Query

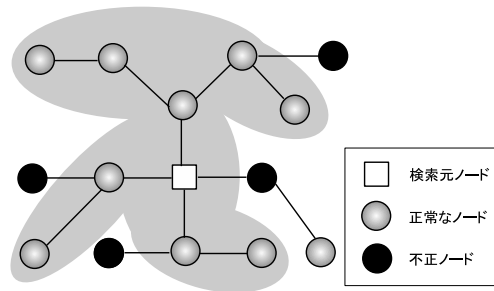


図 2: 提案手法による Query 到達範囲 (灰色部) の例

の初期 TTL から隣接ノードごとにペナルティの値だけ減らして送信する。

$$TTL = (\text{初期 TTL}) - (\text{ペナルティ}) \quad (1)$$

また、受信した Query を転送する際にも、式 (2) に従いペナルティの値だけ TTL を余分に減らす。

$$TTL = (\text{受信 Query の TTL}) - \{1 + (\text{ペナルティ})\} \quad (2)$$

以上のような動作により、正常なノードから送信する Query が、不正なノードに到達しなくなる。図 2 に、提案手法により Query 到達範囲内から不正なノードがなくなる様子を示す。

## 4. 実験と評価

提案手法を評価するため、以下のようなシミュレーションを行った。ノード数 1000、うち不正ノードが 50 個含まれ、1 ノードあたり 4 つのリンクを持つネットワークを作り、正常なノードがそれぞれ 1 つのコンテンツを保持するとして、ノードはランダムに選んだコンテンツを検索するものとした。不正ノードは QueryHit パケットの、コンテンツを保持するノードの所在情報を書き換える動作をする。検索は、Gnutella と同様 flooding によって Query を転送していくことでコンテンツを保持するノードを探すものとした。なお、TTL の初期値は 7 である。このような条件でランダムにノードを選んで検索動作を行い、1000 回の検索要求発生を 1 ステップとし、1 ステップごとに全不正ノードに到達した Query の数と検索成功数を計数した。提案方法を使用した場合 (Penalized)・使用しない場合 (non Penalized) の不正ノードへの Query 到達数を図 3 に、検索成功数を図 4 にグラフで示す。

図 3 の結果から、提案手法により不正ノードへの Query 到達が抑えられたことがわかる。これにより、QueryHit を書き換えられる可能性が減少するため、不正ノードの影響を回避することができたといえる。検索成功数については、提案手法を用いると図 4 のように一度減少し、その後時間の経過とともに増えていくという結果になった。初期の成功数の減少は、シミュレーションを開始した段階では不正ノードの回避が十分に行われておらず、ペナルティの増加が多発して TTL が下がるためである。そして、ある程度不正ノードが回避されると、正常な QueryHit の受信により正常なノードへのペナルティが減少して成功数が回復する。

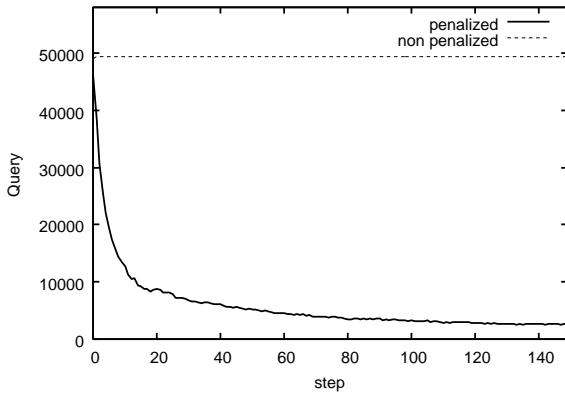


図 3: 全不正ノードへの Query 到達数

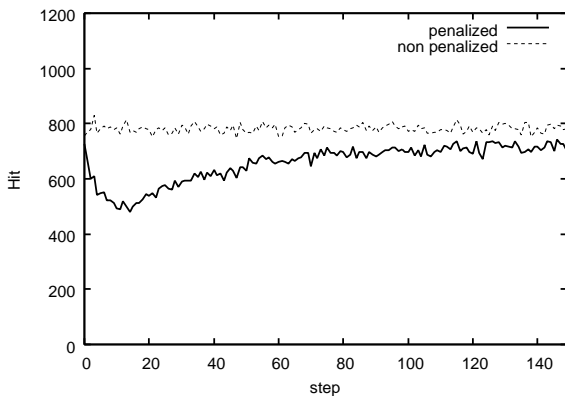


図 4: 検索成功数

実験では、提案手法を用いた場合に検索成功数の低下が見られた。これは、Query の到達範囲が縮小されたことにより、検索能力が低下したことによるものである。また、Query の到達範囲を縮小してしまうと、正常な QueryHit を受信する可能性が減少するため、正常なノードへ与えたペナルティが解消しにくいことも原因となっている。

## 5. 検討と考察

提案手法は、Query の TTL を変化させるものであるが、提案した動作とは別に TTL を書き換えるノードが存在した場合を検討する。まず、TTL が非常に大きな値に書き換えられた場合には、2.2 で述べた TTL が非常に大きい Ping パケットと同様、TTL を調べ、メッセージを破棄する動作を各ノードが行えばよい。さらに、TTL が非常に大きなメッセージを送信もしくは転送するノードは、不正なノードとして取り扱うことができる。TTL が減らされる場合では、提案した手法とまったく同じ動作であり、検索ノードが直接検出できるような問題は起こらない。TTL が通常の動作であり得る範囲で増やされた場合には、Query 到達範囲が広がるために不正ノードまで Query が到達する可能性がある。しかし、この場合には TTL を書き換えたノードが不正な QueryHit を転送することになり、ペナルティが増加する。このため

結果的に Query の到達範囲から TTL を書き換えるノードが取り除かれる。

また、提案した動作では、間欠的にメッセージを書き換えるノードを回避することはできない。これを解決するために、ペナルティの増減を、一回ごとの QueryHit の妥当性だけでなく、不正な QueryHit 数を考慮することが考えられる。すなわち、各隣接ノードから受け取った不正な QueryHit 数をカウントし、それに応じて一回のペナルティの増加分を高めていく方法である。

さらに今後の課題として挙げられることは、検索成功数の改善である。このために、隣接ノードへのペナルティの与え方や Query 到達範囲の縮小の解消を検討する必要がある。提案手法では Query 到達範囲を縮小しすぎる傾向にあったので、到達範囲をどのように回復するかが重要となる。また、Query 到達範囲の縮小問題に対して ExpandingRing[5] 等の別の検索方法を用いることも考えられる。また、実際のシステムではノードの参加・離脱が頻繁に起こることが考えられるため、隣接ノードが変化する場合の対応も検討しなければならない。

## 6. まとめ

本研究では、Gnutella の検索において、検索情報の書き換えを行う不正ノードの影響を回避する手法を提案した。提案手法は隣接ノードに対して QueryHit に応じてペナルティを設定し、ペナルティに応じて Query の TTL を減らし不正ノードへの Query 到達を抑える、というものである。シミュレーションの結果、提案手法により不正ノードに到達する Query の数を減少させることには成功した。しかし、Query 到達範囲の縮小による検索能力の低下が見られた。

## 参考文献

- [1] Jnutella.org <http://www.jnutella.org/>
- [2] Miguel Castro, Peter Druschel, Ayalvadi Ganesh, Antony Rowstron, Dan S.Wallach, "Secure routing for structured peer-to-peer overlay networks", Usenix Symposium on Operating Systems Design and Implementation, 2002
- [3] 香田 徹, "t 重故障同時診断可能システム", 電子情報通信学会論文誌 Vol.J61-D, No.9, pp.680-687, 1978
- [4] 溝口博三, 下川俊彦, 吉田紀彦, 牧之内顕文, "故障耐性のある自律分散系", 第 14 回情報処理学会九州支部研究会論文集, pp.322-329, 2000
- [5] Q.Lv, P Cao, E. Cohen, K. Li, S. Shenker, "Search and Replication in Unstructured Peer-to-Peer Networks" Proceedings of 16th ACM International Conference on Supercomputing, 2002
- [6] 佐藤一帆, "ピアツーピアシステムにおける不正ノードの動的回避方式", 埼玉大学卒業論文, 2005