

オニオンルーティングの経路制御方式の提案

Proposal on path control for onion routing

佐藤 直[†]
Naoshi Sato

李 岩[†]
Ri Gan

1. まえがき

近年、インターネットの通信経路を秘匿する匿名通信技術が普及しつつある。本文では代表的な匿名通信技術／サービスであるオニオンルーティング（以下 OR と示す）[1]を対象に、中継ノードの選択制御、経路の最適化を目的とした経路制御を提案し[2]、性能評価をおこなったので検討結果を報告する。

2. オニオンルーティングの概要

OR はユーザホストが中継ノードとして機能するオーバーレイネットワーク技術／サービスであり、ルーティングとパケット転送は概ね以下の①、②の過程で実施される。

①OR サービスを提供するサーバ（OR サーバと呼ぶ）は予め登録されている参加ホスト（ノード）のなかから中継ノードとして利用可能なノードをランダムに複数ノード（具体的には3ノード）を選択して経路を生成する。

②送信ホストと中継ノード間で多重にパケットを暗号化して受信ホストに転送する。

以上から、第三者が送信ホストや受信ホストを特定することが困難になり、通信の秘匿性を保つことができる。

3. オニオンルーティングの課題

OR を適用すると情報の漏えいなどを防止できるが、ユーザホストをランダムに選択して中継ノードとして用いることから、一般的なパケット転送に比べ、接続（コネクション確立）特性、伝送特性、信頼性の面で劣るという課題がある。

4. エニーキャストと最短経路制御の適用の提案

上述の課題を解決するため、エニーキャスト[3]と最短経路制御を用いた経路制御方式を提案する。

ここで、エニーキャストは、マルチキャスト技術を用いて複数ホストのなかから「最も近い」ホストを選択して通信する技術である。また、最短経路制御として TCP/IP ネットワークで広く適用されている OSPF (Open Shortest Path First) [4]の経路制御の仕組みを利用する。

本提案の経路制御のイメージを図 1 に示す。同図で、送受信ホスト間を接続する 3 つの中継ノード（入口、出口、転送ノード）を決定する。最初に、送信ホストと受信ホストはそれぞれエニーキャストにより、最も近いノードを選択し、入口ノードと出口ノードとする。次に、最短経路制御により、入口ノードと出口ノードを最短で結ぶ転送ノードを選択する。なお、中継ノードの選択制御、経路制御の前提として、OR 参加ノードのネットワークトポロジ情報とノード間の伝送遅延情報が OR サーバに収集され、全ノードに再配布されるものとする。なお、図 1 には、信頼性向上対策として、転送ノードが故障した場合、他のノードが転送ノードとして代替する冗長経路のイメージも示した。

以上のように、提案方式ではエニーキャストと最短経路制御を併用することにより、OR における経路の最適化を図る。

5. 性能評価

従来方式と比較しながら提案方式の性能を評価する。評価項目は接続特性と伝送特性で、具体的には、接続（コネクション確立）特性は接続可検出時間と接続不可検出時間、伝送特性は伝送遅延時間とする。なお、1 回の制御動作は 1 つのコマンドにより実行され、実行に要する時間は 1 秒とする。中継ノードの利用可否も 1 秒以内で判断するものとする。

5.1 接続特性

接続特性として接続可検出時間と接続不可検出時間を評価する。ここで、接続可検出時間とは、OR サーバが送信ホストからの依頼を受けて以降、正常に稼働しており OR サービスに供することの可能な中継ノードを 3 つ以上検出するまでに要する時間とする。すなわち、OR サービスが提供可能と判断できるまでの時間を指す。また、接続不可検出時間とは、利用可能な中継ノードが 2 以下であることを検出するまでに要する時間とする。すなわち、OR サービスが提供不可能と判断できるまでの時間を指す。

従来方式では、OR サーバは ping コマンド等により個別に中継ノードが正常か否かを検査している。上述したように、このコマンド実行に要する時間は 1 秒で、中継ノードの利用可否も 1 秒以内で判断するものとする。

(1) 接続可検出時間

従来方式の接続可検出時間を考える。従来方式では参加ノードが中継ノードとして利用可能か否かをひとつずつ検査する。検査開始直後に調べた 3 ノードが全て正常であれば接続（サービス提供）可能なため、接続可検出時間の最

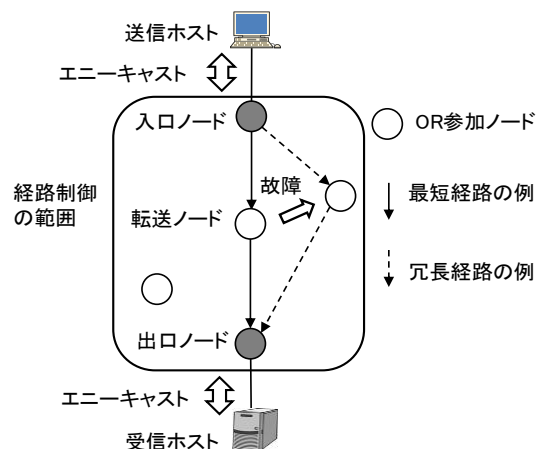


図 1 エニーキャストと最短経路法の適用によるオニオンルーティングの経路制御

[†] 情報セキュリティ大学院大学

小値は3秒である。いま、検査対象となる参加ノードの数を n (≥ 3)、各参加ノードが障害でORに利用できない確率、すなわち、不稼働率を p とする。接続可能な場合、最後の検査ノードは正常と判断されることを考慮すると、接続可能検出時間の期待値は、次式で与えられる。

$$\frac{\sum_{k=3}^n k(k-1)(k-2)p^k}{\sum_{k=3}^n (k-1)(k-2)p^k} \quad (1)$$

式(1)の特性を図2に示す。同図から、従来方式の接続可能検出時間は、 p が小さければ n によらず、ほぼ3秒とみなせることがわかる。 p が1に近くなると急激に大きくなることもわかる。

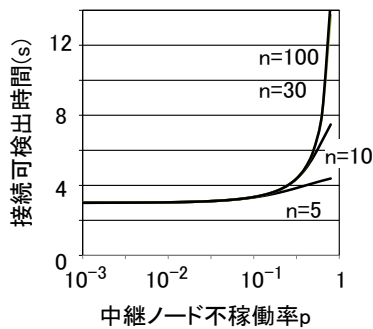


図2 従来方式の接続可能検出時間

提案方式では、送受信ホストがエニーキャストで参加ノードを独立かつ同時に検査するとして、接続可能検出時間は1秒である。

(2)接続不可検出時間

従来方式の接続不可検出時間について考える。 n 個の参加ノード中、正常なノードが2個以下と判断できるのは、 $n-2$ 回以上検査した場合である。すなわち、 $n-3$ 回目以前の検査では検査していない参加ノードが3個以上残っているから接続不可と判断できない。そこで、 $n-2$ 、 $n-1$ 、 n 回目の検査で接続不可と判断できる確率を求め、接続不可という条件のもとで接続可能検出時間を求める。この場合の接続不可検出時間の期待値は次式で与えられる。

$$\frac{n + (n-1)(n-2)(1-p) \left\{ 1 + \frac{(n-2)}{2}(1-p) \right\}}{1 + (n-2)(1-p) \left\{ 1 + \frac{(n-1)(1-p)}{2} \right\}} \quad (2)$$

式(2)の特性を図3に示す。図において、接続不可検出時間は p によらずほぼ $n-2$ (秒) となっている。これは、式(2)からも確認できる。すなわち、同式は、 $1 \gg p$ とすると、 $1/(n-1)+n-2$ と近似されるため、 $n \gg 1$ で $n-2$ となることがわかる。

なお、接続不可検出時間の場合と同じ理由により、提案方式の接続不可検出時間も1秒である。

5.2 伝送特性

送受信ホスト間は図1のように4リンクで構成される。

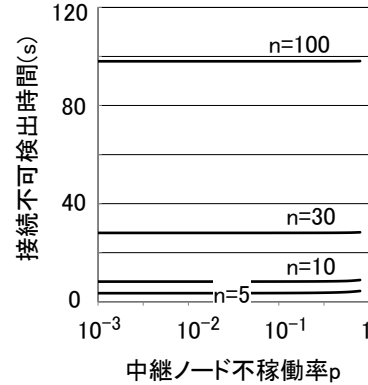


図3 従来方式の接続不可検出時間

ここで、簡単のため、各リンク（ノード間）の遅延は全て1ms～100msで一様分布すると想定し、伝送遅延を計算機シミュレーションした結果を表1に示す。従来方式では、3つの中継ノードをランダムに選択するため、ノード間の平均遅延は約50msであり、送受信ホスト間遅延の平均値は n によらず約200msになることがわかる。提案方式では最短経路となるように3つの中継ノードが選択されるため、 n が増えると伝送遅延が短縮されることがわかる。

表1 伝送遅延時間の計算機シミュレーション結果

参加ノード数 n	送受信ホスト間の平均伝送遅延時間 (ms)	
	従来方式	提案方式
5	200	85
10	201	48
30	202	31
50	201	14
100	201	9

6. 匿名性に関する考察

提案方式により通信路が固定化してしまい、従来方式の匿名性が劣化するという課題について考察する。提案方式において、同一送受信ホストで通信を繰り返す場合は同一経路となる可能性が大きい、通信ごと前回までに使用した中継ノードの全てあるいは一部を除いて経路制御などの対策をとることでこの課題は解決できると考えられる。

7. むすび

本検討ではエニーキャスト技術と最短経路法を利用して、オニオンルーティングの経路を最適化する手法を提案した。今後は実環境で提案の有効性を検証する予定である。

文 献

- [1]Tor プロジェクトホームページ, <https://www.torproject.org/index.html> (2013年7月確認)
- [2]李岩, 佐藤直, "オニオンルーティングにおける経路制御の研究," 2013年信学全大, B-7-59 (2013年3月)
- [3]C. Partridge, T. Mendez and W. Milliken, "Host Anycasting Service", IETF RFC1546 (Nov. 1993)
- [4]J. Moy, "OSPF Version 2", IETF RFC2328 (Apr. 1998)