P2P を用いたインターネット経路ハイジャック検知システム

根本 昂†　　鈴木 常彦‡

†中京大学 情報科学研究科 情報科学専攻　　‡中京大学 情報理工学部 情報システム工学科

1　はじめに

インターネットの経路交換プロトコルである，BGP(Border Gateway Protocol) において、近年では、経路ハイジャックとよばれる「経路の乗っ取り」が頻繁に起きており、ハイジャックされた本来のアドレス所有者が正常な通信が出来なくなるだけではなく，ハイジャックされたネットワークに繋ぎにいったホストも被害を受ける．

本稿はこの問題に対し、繋ぎにいくネットワークが本物のアドレス所有者のネットワークかどうかを調べることでハイジャックされているか否かを判定する。その判定には、公開鍵アルゴリズムを用いてチャレンジ＆レスポンス認証を行い、アドレス所有者本人なら正常な応答を返すだろうという推測に基づく。

2　関連研究

経路ハイジャック問題に対して有効な手段として、IRR (Internet Routing Registry) を用いた研究が盛んにおこなわれている。[1][2][3] しかし、IRR を基盤にした経路ハイジャック検知は、情報の登録数や信憑性の観点から [4]、完璧な検知システムとは言い難い。

3　提案方式概要

本稿の提案する手法は、DHT(Distributed Hash Table) と呼ばれる構造化オーバーレイネットワークを用いて、ネットワーク同士を公開鍵暗号方式を用いて互いに認証しあい、その信頼の輪をもって、現在繋がっているネットワークがアドレス所有者本来のネットワークかどうかをチェックする。また、DHT のアルゴリズムには Chord を用いており、その探索にかかるオーダは $O = log_2 N$ であることが立証されている。本システムでは、Chord の実装に、OverlayWeaver[5] を用いており、DHT の部分は、全て OverlayWeaver に任せている。

4　新規参入時のステップ

オーバーレイ認証ネットワークへの新規参入時、どのようなステップを経るか、具体例を用いて説明する。新規参入したいネットワーク 192.168.2.0/24 が参加を完了するまでのステップを、図 1 に表す。まず、192.168.2.0/24

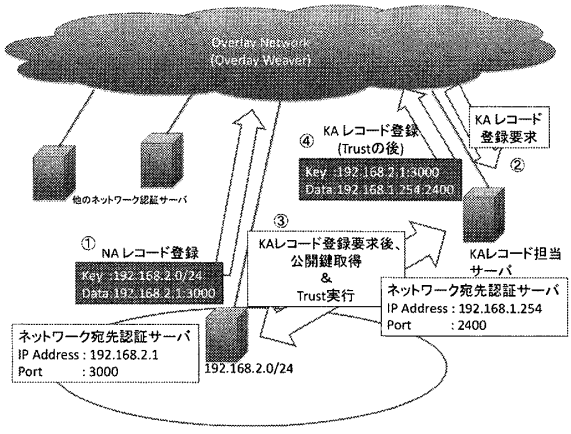

図 1: システム　概要

の中に、サーバを設置しなければならない。このサーバは、外部からチャレンジ＆レスポンスをかけられることになる。図中の 192.168.2.1 がそれにあたる。最初に、192.168.2.0/24 の新規参入を知らせる NA(Network Authority) レコードをオーバーレイ認証ネットワークに登録する。このレコードの実体の所有者は、Overlay-Weaver の実装に依存しており、Chord アルゴリズムによって決定づけられている。今回は、既にオーバーレイ認証ネットワークに認証が済んでいる 192.168.1.254 が実体を持っている。この場合、KA(Key Authority) と呼び、直ちに新規参入のネットワークに、一定時間のチャレンジ＆レスポンスをかける。ここで、認証が終了すると、KA は対象ネットワークの公開鍵を KA レコードとして登録する。この登録をもって、192.168.2.0/24 はオーバーレイ認証ネットワークに参加が完了したといえる。

5　認証時のステップ

具体的な認証プロセスがどのようにしておこなわれるか説明する。既にオーバーレイ認証ネットワークに参

Internet Prefix Hijack Detection Using P2P Network
†Takashi NEMOTO　‡Tsunehiko SUZUKI
†Graduate School of Computer and Cognitive Science , Chukyo University
‡School of Information Science and Technology, Chukyo University

加済みのネットワーク 192.168.2.0/24 が、本物のネットワークかどうか調べたい。まず、192.168.2.0/24 の NA レコードを問い合わせる。その data 部が NA なので、更に先の data 部をキーに問い合わせると、KA が探し出せる。これで、KA に公開鍵を要求する。これでネットワーク宛先認証に必要な公開鍵は手に入れた。ここでようやく 192.168.2.0/24 のチャレンジ&レスポンスを開始する。ランダムな文字列を生成し、これを先の手に入れた公開鍵で暗号化し、NA レコードの data 部のサーバに送信する。復号に成功した場合のみネットワーク宛先認証が完了したと認める。

6 評価

ランダムに選んだネットワーク宛先認証サーバに認証要求のクエリを投げ、その時間を計測した。

受け取ったサーバは、対象のネットワークから NA レコード検索、KA レコード検索、公開鍵要求と遷移し、取得した NA レコードの data 部に記述されている IPaddress:port に、先ほど手に入れた公開鍵を用いてランダムな文字列を暗号化して送る。そうすると、サーバが平文を返すので、それが送ったものと正しいかチェックする。この作業の繰り返しを 3 回おこない、最終的な結果を検証用プログラムに返す。また、このクエリを出してから、判定が返ってくるまでの時間を計測し、合わせて出力する。

この要求と応答をそれぞれ 10 繰り返した結果が以下の表 1 である。

NW 数	1	100	200	300
平均完了時間 (sec)	2.1	2.0	2.8	2.1

表 1: 検証結果

7 平均認証完了時間

前項の結果から、クエリを出してから判定が返ってくるまでの時間に注目すると、ネットワーク宛先認証サーバが 1 台である時と 300 台であるときがほぼ同じであることが分かる。これの結果は、検証環境のネットワーク遅延がほぼ無いに等しいからである事に起因すると仮定した。そして、この値からインターネット上での遅延を考慮し、平均 RTT を元に計算、予想を立てた。図 2 は、RTT が 100 msec であった時のネットワーク数増加に対しての平均認証完了時間のである。

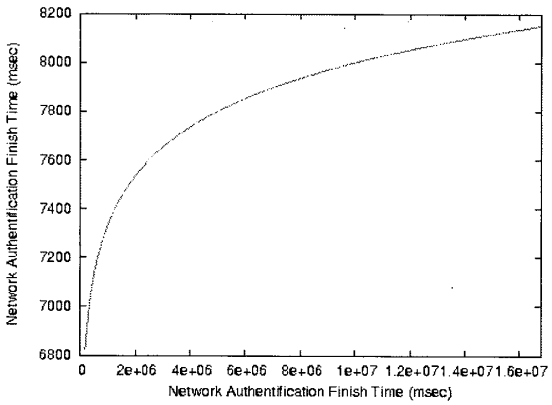

図 2: RTT=100 の場合

8 まとめ

公開鍵認証を用いて相手先を正しく認証する技術で重要なのは、公開鍵を安全に配ることと、それが信用できるかどうかである。この点に関して、オーバーレイ認証ネットワークのレプリケーション機能とネットワーク宛先認証サーバの冗長化で安全性を確保した。また、経路ハイジャックだけでなく、相手が本物かどうか見分けるのに公開鍵を用いることで、信頼性の高い認証がおこなうことができた。しかし、本システムはまだまだ信頼性を高める必要があり、多数一致による公開鍵の信頼度重み付けや、ネットワークのプレフィックスが固定長なのも大きな課題である。

参考文献

[1] 吉田友哉. Irr を用いた次世代 bgp 経路制御アーキテクチャーの提案. 電子情報通信学会技術研究報告, Vol. 106, No. 462, pp. 7–12, 20070111.

[2] 田原光穂, 立石直規, 松葉啓, 瀬社家光. As パス詐称経路ハイジャックの検出手法の検討 (ネットワーク管理). 電子情報通信学会技術研究報告., Vol. 108, No. 481, pp. 41–45, 20090305.

[3] 大島利充, 田原光穂, 小池和郎. ハイジャック経路監視方法に関する研究 (品質とコスト・及び一般). 電子情報通信学会技術研究報告. TM, テレコミュニケーションマネジメント, Vol. 104, No. 326, pp. 7–12, 20040923.

[4] 長橋賢吾, 江崎浩. インターネットルーチングレジストリにおける経路整合度の評価に関する研究. 電子情報通信学会論文誌. D-I, 情報・システム, I-情報処理, Vol. 87, No. 5, pp. 553–560, 20040501.

[5] 首藤一幸, 田中良夫, 関口智嗣. オーバレイ構築ツールキット overlay weaver. 情報処理学会論文誌, Vol. 47, No. 12, pp. 358–367, 20060915.