

2-2 セキュア・オーバーレイネットワークの設計とフェーズ1 開発

2-2 Design and Phase-1 Development of Secure Overlay Networks

門林雄基 中尾康二 滝澤 修

KADOBAYASHI Youki, NAKAO Kouji, and TAKIZAWA Osamu

要旨

近年、アプリケーション層における単一障害点を解消するための手段としてオーバーレイネットワークが注目されている。本稿ではオーバーレイネットワークにおける経路制御のセキュリティに焦点を当て、脅威モデルの構築と対策方式の提案を行う。提案方式はブラインド転送、分散型の信頼錨、抜き打ち検査からなる。提案方式は先行研究とは異なり、信頼錨を前提としている点が特徴である。また本稿では、先行研究の成果を基に脅威モデルの再構築を試みた。さらに、アプリケーションごとに異なる脅威モデルに合わせてセキュア・オーバーレイを組み立てる必要があることから、セキュリティ高度化グループではセキュア・オーバーレイの基本的機能を提供するソフトウェア・フレームワークの開発に取り組んでいる。最後に、本フレームワークのフェーズ1 開発の概要について述べる。

Recently, overlay networks are gaining attention as a means to eliminate single point of failure in the application layer. This paper focuses on secure routing in overlay networks. A threat model is presented, along with our countermeasure proposal. Our proposal consists of blind forwarding, distributed trust anchor, and probabilistic testing. Unlike previous contributions on this topic, our proposal is based on trust anchor. Furthermore, we attempt to reconstruct the threat model, based on the insights gained from previous contributions. We also briefly describe our phase-1 development efforts of a software framework that implements essential functions of secure overlay. Our software framework attempts to address application-specific threat models.

[キーワード]

オーバーレイネットワーク, セキュア・オーバーレイ, ブラインド転送
Overlay networks, Secure overlay, Blind forwarding

1 まえがき

今日、Web サイトや各種のサーバに対するサービス妨害攻撃(DoS: denial of service)や、分散型サービス妨害攻撃(DDoS: distributed denial of service)が問題となっている。これらの攻撃はシステムの単一障害点となり得るルータやサーバを特定し、攻撃を行うものである。この問題の対策として、OSI 参照モデルの各層において単一障害点を解消することが求められている。

本研究では、下位層における単一障害点を回避し、またアプリケーション層における単一障

害点を解消するための手段としてオーバーレイネットワークに注目する。オーバーレイネットワークはエンドホスト同士がアプリケーション層においてネットワークを構成する技術の総称であり、Rendezvous(近接性の維持)、Location(資源探索)、Routing(経路制御)を中心とする諸機能を持つ。

しかしながらオーバーレイネットワークは敵対ノードの挿入に対して脆弱であるといった問題が知られており、これらの問題を克服したセキュア・オーバーレイの実現が求められている。セキュア・オーバーレイを設計する上で、脅威モ

デルと対策方式に関する取組は必要不可欠であるが、先行研究 [1] - [4] ではビザンティン障害を含む最も難しいクラスの脅威モデルを取り扱っており、有効な対策方式を見いだせていない。

本論文では、より易しい問題に対する基本的な理解を基に、安全なオーバーレイネットワーク構築に向けて段階的なアプローチを試みる。まずオーバーレイネットワークの諸機能におけるセキュリティ確保について考察し、既存の問題領域との関連付けを試みる。セキュア・オーバーレイでは特に、経路制御におけるセキュリティ確保が新たな問題領域であると考えられるので、本論文では経路制御のセキュリティを主に取り扱い、脅威モデルの構築と対策方式の提案を行う。

次に、セキュア・オーバーレイではアプリケーションごとに異なる脅威モデルを取り扱う必要があることを指摘する。情報通信研究機構セキュリティ高度化グループでは、個々の脅威モデルに合わせたセキュア・オーバーレイを実現するためのフレームワークの構築を進めている。最後に、フェーズ1開発の成果を簡単に紹介する。

2 オーバーレイネットワーク

まず、オーバーレイネットワークについて説明する。オーバーレイネットワークはネットワーク層における接続性を前提として構築されるネットワークで、通常アプリケーション層において実装される。オーバーレイネットワークとしては様々な方式が提案されており、それらは加入方法や近接性の維持方法 (Rendezvous)、資源探索の方法 (Location)、経路制御の方法 (Routing) によって特徴付けることができる。以降、これをオーバーレイネットワークの3側面と呼ぶ。

例えば Chord [5] ではオーバーレイに参加するノードと、ノードが保持する資源を SHA-1 等のハッシュ関数によって単一のリング上に射影し、リング上の順序関係を利用して効率的な経路制御を行う。単一のリング上でノードと資源の順序関係が明確に定義されることにより、「どのノードがどの資源を持っているか」といったディレクトリ機能をハッシュ関数で代替することがで

き、資源探索が容易になる。また、そのような順序関係により「どのノードまで検索を飛ばしてよいか」ということが明確となり、経路制御の効率化を図ることができる。

Chord ではリング上の任意のノードに対し加入要求を送ることができ、またリング内の識別子を指定してノードや資源にアクセスすることができる。識別子空間を環として解釈するか、あるいは二進木として解釈するか、といった点において大きな自由度があり、これらに呼応した様々な経路制御アルゴリズムが存在する。具体的には、リングのほか、メッシュ、木構造など、様々なトポロジを利用した方式が提案されている [6] [7]。

次にオーバーレイネットワークにおける経路選択モデルについて述べる。IP ネットワークにおける経路選択は最長一致アルゴリズムに基づくものであるが、オーバーレイネットワークでは、ハッシュ関数等によって射影された識別子空間における近接性は実ネットワークにおける近接性と関連がないため、最長一致アルゴリズムのみを用いた場合、ネットワーク層からみて最適でない経路選択となる。この問題を軽減するため、近接性を考慮した経路選択手法が数多く提案されている。それらは大きく以下の3種類に大別できる [8]。

- ・PNS (Proximity Neighbor Selection) : 経路表に記載するノードはノードの近接性に基づいて決められる。
- ・PRS (Proximity Route Selection) : 経路表に記載した複数のノードのうちどれを使うかは、ノードの近接性に基づいて決められる。
- ・PIS (Proximity Identifier Selection) : 識別子はノードの近接性に基づいて付与される。

前述の Chord は最も簡単な経路制御モデルを採用しており、純粹に識別子空間における順序関係によって経路表に記載されるノードが決定される。PNS、PRS 等は実ネットワークにおける近接性を考慮するための改良であり、多くの経路制御アルゴリズムに導入することができる。

オーバーレイの機能モデルとしては、これまで DHT、DOLR、CAST が提案されている [9]。DHT (Distributed Hash Table) はハッシュテーブルをオーバーレイ上に分散するもので、(key,

value) ペアを共有するアプリケーションに適している。DHT では、単一オーバーレイ上のどのノードでも (key, value) ペアを put/get できる。DOLR (Decentralized Object Location and Routing) は分散ディレクトリサービスの一種であり、ある ID を持つ最寄りのオブジェクトにメッセージを届ける。DOLR では、単一オーバーレイ内に同一 ID を持つオブジェクトが複数存在してもよい。CAST はグループ内通信を行うもので、グループへの加入・離脱、グループ内メンバーへのマルチキャストやエニキャストを提供する。先の文献では、これらの機能モデルはすべて KBR (Key-Based Routing) という下位レイヤを使って実装できると述べている。

3 関連研究

ここではオーバーレイネットワークの諸機能におけるセキュリティについて考察し、既存の問題領域及び先行研究との関連付けを試みる。以下では、オーバーレイの3側面のそれぞれについて述べる。

まず、近接性の維持 (Rendezvous) において必要となるセキュリティ機能は、真正性、乱用対策及び DoS 対策である。真正性の実現方法としては、信頼錨 (trust anchor) を外部に求める方法があり、PKI、PGP、IC カード等が考えられる。乱用対策としては、チューリングテスト、クレジットカード課金、ハードウェアトークン、インセンティブに基づくノード評価[10]などの方式が知られている。DoS 対策としては、メモリ律速の逆問題[11]、閾値暗号を応用したシングル・サインオン認証サーバ[12]、メッセージ受信ノードの冗長化[13]等の手法が知られている。

資源探索において必要となるセキュリティ機能は、秘匿性、一貫性、可用性である。これらはそれぞれ、対称鍵暗号、ハッシュ関数、複製あるいは erasure coding によって実現することができる。

経路制御において必要となるセキュリティ機能は、責任追跡性、信頼性、可用性である。先行研究[1]～[4]では経路の挿入攻撃、メッセージ転送時のビザンティン障害などの問題が指摘されているが、上記の要件をすべて満たす経路制

御方式は提案されていない。その他のセキュリティ機能についても研究がなされている。匿名性については Herbivore[14]が提案されており、また分散保持されたデータの永続性については LOCKSS[15]が提案されている。

総論として、オーバーレイにおけるセキュリティを実現するためには、オーバーレイの3側面それぞれにおけるセキュリティ機能を組み合わせる必要がある。しかしながら関連研究のいずれにおいても、このような視点が欠けている。本研究では、この視点から脅威モデルの再構築を試み、経路制御における対策方式の提案を行う。

4 経路制御における脅威モデル

ここでは経路制御に対し、以下のような脅威モデルを想定する。

- ・T-1: 少数のノードが敵対的行動を取ることはあるが、多くのノードは正しい振る舞いをする。
- ・T-2: 多くのノードが DoS/DDoS 攻撃の対象となり得る。
- ・T-3: 敵対者は単一地点で盗聴できるが、多くの地点で盗聴することはできない。

T-1 の結果として、少数の敵対ノードは、クエリを誤った宛先に転送したり、クエリ転送を拒否したり、誤った経路を挿入したりする可能性がある。また、T-2 の結果として、多くのノードが通信不能となる可能性がある。

オーバーレイの脅威モデルは、開放型のオーバーレイと閉域型のオーバーレイで若干異なる。閉域型のオーバーレイにおいて、網内に敵対ノードが存在しない場合は T-2、T-3 のみが脅威となり得る。少数の敵対ノードが存在する場合は、これに T-1 が加わる。一方、開放型のオーバーレイでは多数のノードが加入し、敵対ノードとなる可能性がある。

T-1 において敵対ノード数に制限を加えているのは、問題のクラスを制限するためである。また関連研究でも触れたように、チューリングテストやクレジットカード課金等の手法を用いることで、一人の利用者が複数ノードを操作する可能性を減らし、敵対ノード数を抑えることが

できるため、敵対ノード数を制限しない Sybil attack のような脅威モデルと比較してより多くのケースを取り扱うことができると考える。

また、次節で述べるブラインド転送を用いることにより、敵対ノードが経路制御を攻撃する動機付けを減らすことができる。

5 セキュア・オーバーレイの方式設計

本研究では、オーバーレイネットワークの経路制御における責任追跡性、信頼性、可用性を実現することを試みる。これらの性質を実現するため、三つの提案を行う。まず、利害の一致しない複数のコミュニティが単一オーバーレイ上に多重化されていることを前提とし、ブラインド転送を提案する。次に、アクセスの主体と客体だけでは責任追跡性や信頼性を実現できないという考察に基づき、ONOC (Overlay Network Operation Center) を信頼錨とする方法を提案する。次に、クエリ発生後に一定の確率で検査パケットを送ることで、クエリ転送妨害を検出する方法を提案する。

5.1 ブラインド転送

以下では、クエリの始点・終点ノードの IP アドレスやホスト名、AS 番号といったネットワーク層の属性 (以下、「ネットワーク属性」と呼ぶ。) を隠ぺいしたままクエリを転送する方法をブラインド転送と呼ぶ。ここではまず、ブラインド転送の必要性について論じる。

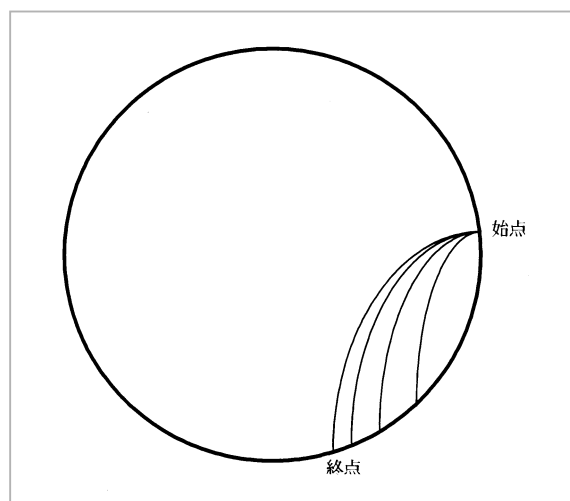


図1 繰り返し型のクエリ転送

一般的に、一部のコミュニティのみが利益を享受できるインフラストラクチャは他のコミュニティからの攻撃を受けやすいと考えられる。そうだとすると、相反する利害関係を持つ複数のコミュニティが単一のオーバーレイに依存することで、オーバーレイが攻撃を受けなくなる可能性がある。つまりオーバーレイを攻撃することは結果的に自らのコミュニティの一部を攻撃することになり、意味がないという状況を作り出すことが重要だと考えられる。

例えばインターネットにおける DoS では、ネットワーク属性からあるホストが攻撃対象になり得るかどうかを容易に判断できる。その結果、日本のサーバを他国から攻撃するといった、コミュニティ間の緊張関係に基づく攻撃が成立している。オーバーレイではこの問題を解決できる可能性がある。例えば、オーバーレイのトポロジを知っているだけではネットワーク属性を知ることができないようにオーバーレイを構成することができる。

クエリに対する妨害は、クエリの発信者と宛先のネットワーク属性が分かっている場合のみ意味がある。クエリを転送するとき、これらの属性が分からないようにすれば、妨害は意味をなさない。このようなブラインド転送による選択的妨害の無力化を実現するためには、再帰型のクエリ転送を実現する必要がある。

オーバーレイにおけるクエリ転送方法としては、繰り返し型と再帰型がある。繰り返し型では、資源探索を行うノードが経路表に基づいて次ホップにクエリを送り、目的とする資源に到達するまでクエリを繰り返し送るというものである (図 1)。この場合、クエリは始点ノードを中心としてスター状に送られる。この結果、始点ノードのネットワーク属性はクエリを送ったすべてのノードに露呈することになる。

これに対し、再帰型のクエリ転送では始点ノードのネットワーク属性を知り得るのは始点ノードの次ホップのみである。再帰型では、始点ノードが次ホップにクエリを送り、次に次ホップが自らの経路表に基づいてクエリを転送する。これを目的とする資源に到達するまで再帰的に行う。その結果、クエリは始点ノードから終点ノードへ飛び石状に送られる (図 2)。このため、

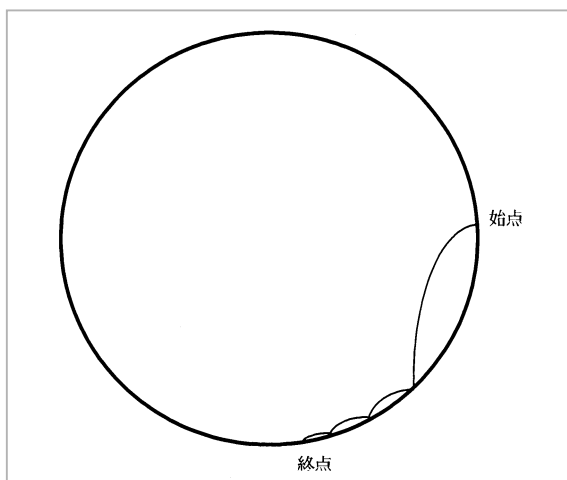


図2 再帰型のクエリ転送

始点ノードのネットワーク属性が近傍ノード以外に露呈することはない。

5.2 分散型の信頼錨

オーバーレイにおける責任追跡性、信頼性を実現し、また可用性を制御するためにはアクセスの主体・客体のみでオーバーレイを構成するだけでは不十分であり、第三者に情報を集める必要がある。ここではオーバーレイの管理主体として ONOC (Overlay Network Operation Center) を置くことを考える。ONOC において各ノードから情報を集め、各ノードの信頼性を前後のノードからの報告との整合性に基づいて評価することを考える。また、ONOC において複数のノードからの記録を取ることで責任追跡性を確保できると考えられる。また、ONOC において全体の可用性を計算し、信頼性の低いノードを排除したり、データの冗長性を増すなどの手法で可用性を制御することができると考えられる。具体的な手法は、次節で各ノードからの報告データを説明した後述べる。

次に ONOC の構成方法について述べる。ONOC が単一ノードである場合、それ自身が単一障害点となりオーバーレイの可用性を損なう危険性がある。このため、ONOC を閉域型オーバーレイとして構成するのは自然である (図 3)。ONOC は開放型オーバーレイではないため、ONOC に対し DoS 攻撃を行うことは容易ではないと考えられる。ONOC における DoS 対策方式については次節で述べる。

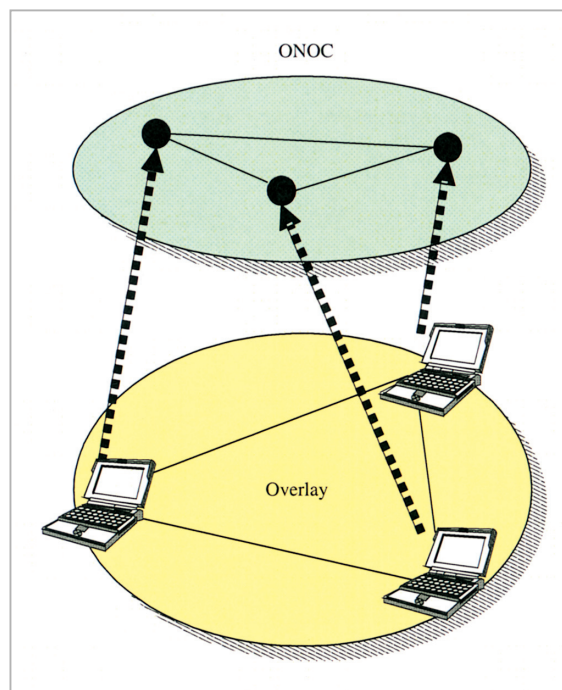


図3 オーバーレイと ONOC の関係

5.3 抜き打ち検査

ONOC でオーバーレイの責任追跡性・信頼性・可用性を確保するためには、理想的にはすべてのパケットを監視すればよい。しかしこれは通信オーバーヘッドや領域計算量の面からみて現実的ではないため、ここでは一定の確率で抜き打ち検査を行う方法を提案する。各ノードは、クエリ転送時に検査パケットを受け取る可能性を知ることができず、また検査パケットを受け取ったときにクエリ転送行為を証明する必要があるため、クエリを廃棄したり誤ったあて先に送ることは困難である。以下では特にクエリを対象として述べるが、各々の経路制御アルゴリズムで必要となるノード追加、削除等のメッセージにおいても同じ考え方が適用できる。

抜き打ち検査は、始点ノードがクエリを送った後に一定の確率で検査パケットを送ることで実現される。クエリを廃棄したり、クエリを誤ったノードに転送した場合に、そのことを高い確率で検知できることが望ましい。このため、まずクエリと同一の始点・宛先アドレスを用い、クエリ送出後、一定時間経過後に検査パケットを同一経路へ送る。経路途中のすべてのノードは、検査パケットを受け取ると転送記録を ONOC へ送る。検査パケットでは検査対象とす

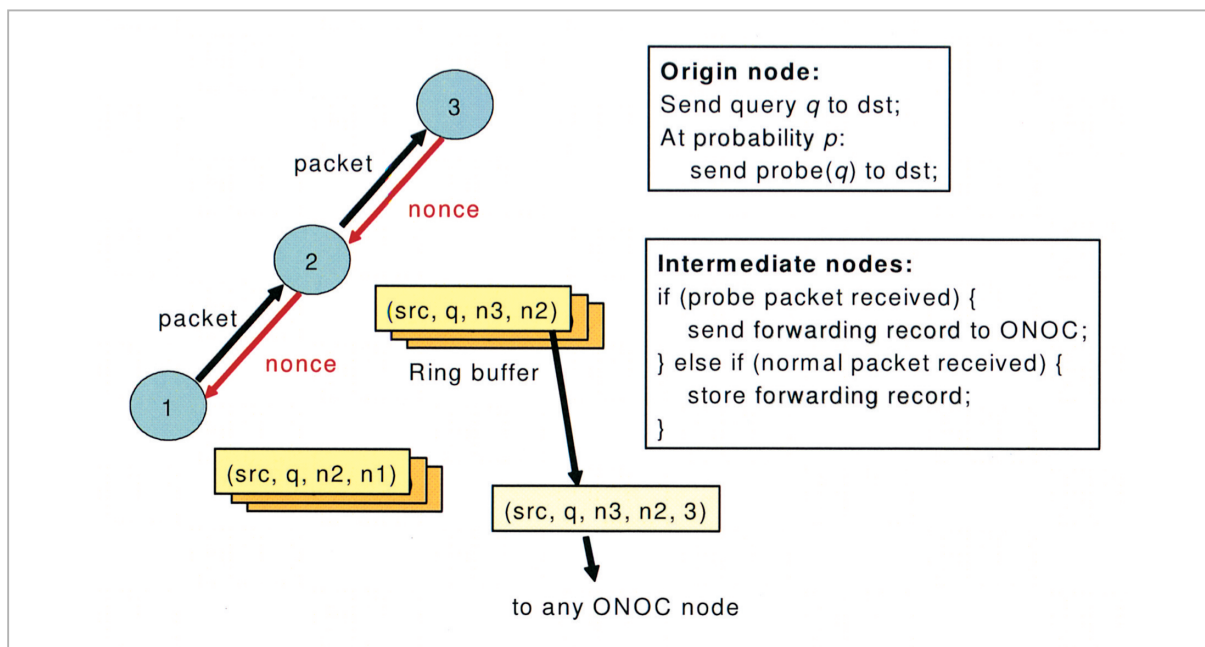


図4 転送報告と検査パケット

るクエリをクエリ ID によって指定する。各ノードは、クエリの転送記録をリングバッファに保持する。

次に検査パケットの送出タイミングについて述べる。検査パケットの送出遅延が大きいとリングバッファから転送記録が消えてしまうため、送出遅延は適度に短くしなければならない。一方、クエリ直後に検査パケットを送った場合、検査パケットが来たクエリだけを転送するといった選択的攻撃が可能になるため、送出遅延を極端に短くすることも望ましくない。

次に転送記録の内容について述べる。転送記録を作成するため、各ノードは次ホップとの間で以下のような情報交換をしなければならない。まずパケットを次ホップに送るとき、次ホップから乱数を受け取る。同様に、前段からパケットを受け取るとき、自身の乱数を送る。これにより、すべてのノードで (src, query-id, next-hop-nonce, my-nonce) がリングバッファに記録される。これが転送記録である。検査パケットを受け取った場合、転送報告を ONOC に送ることで自身がクエリ転送を妨害していないことを証明できる。転送報告の内容は、(src, query-id, next-hop-nonce, my-nonce, next-hop) からなる (図 4)。なお始点ノードでは始点アドレスに加えて宛先アドレスも ONOC に報告する。また、あ

て先ノードでは next-hop を空のまま報告する。

ONOC では前段のノードの next-hop-nonce が次段のノードの my-nonce と一致することを確認すれば、クエリを破棄されていないことが分かる (図 5(a))。あるノード以降からの転送報告が来ない場合、クエリが破棄されたか、あるいは前段のノードで検査パケットが破棄されたことが分かる。また、誤ったノードにクエリが転送された場合は、経路制御アルゴリズムで規定されているノード ID とクエリの順序関係が破られるので検出可能である。

複数のノードが結託し、転送報告をねつ造することも考えられる。この場合、次ホップが転送報告を送らなかったノードであると判定されてしまう危険性がある。この問題への対策として、nonce の生成方法に time-released key chain を応用すればよい。ONOC は同一ノードから送られてくる nonce の系列の一貫性をハッシュ関数によって検査することができるため、前段のノードが next-hop-nonce を偽造した場合これを検知できる (図 5(b))。

次に ONOC における DoS 対策方式について述べる。各ノードは、転送報告を ONOC に送るときに $H(\text{my-nonce}, \text{my-hop})$ を (next-hop-nonce, next-hop) 等のタプルとともに送る。H はハッシュ関数である。これにより、前段のホップから

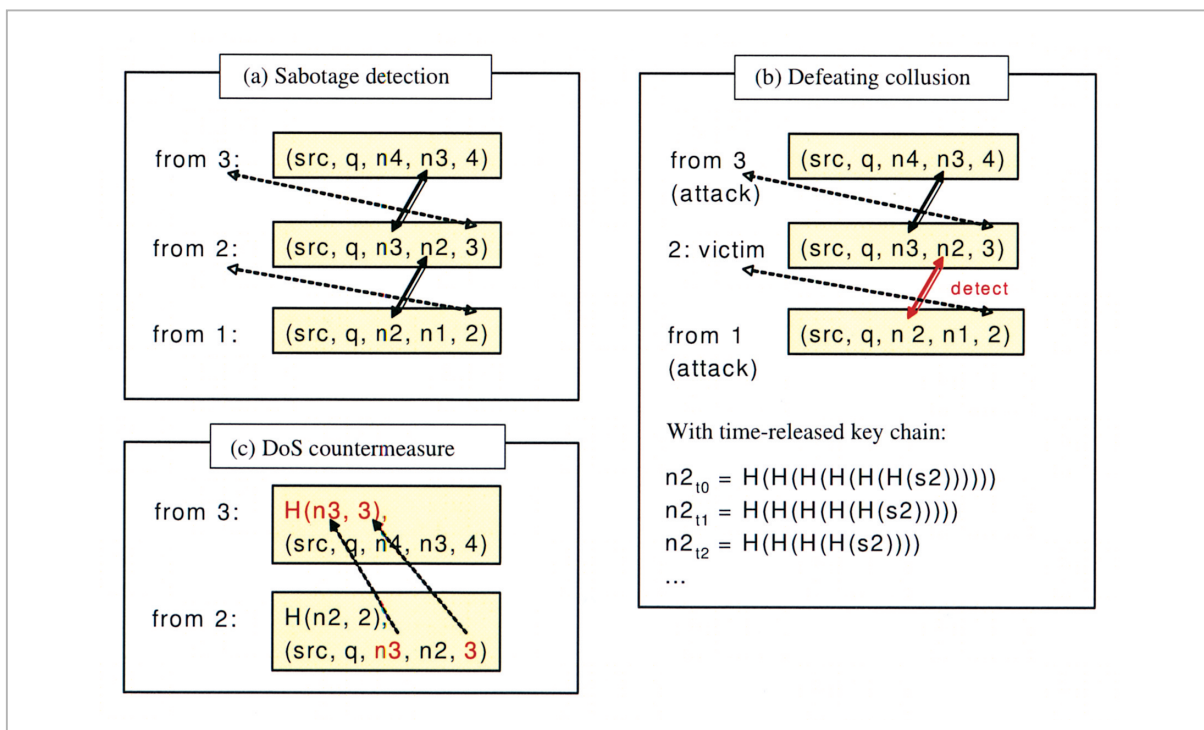


図5 転送報告を用いたクエリ転送行為の確認

送られた (next-hop-nonce、next-hop) から計算したハッシュ値と、パケット内のハッシュ値を比較することで、DoS パケットを容易に廃棄できる (図 5(c))。

同様に、ONOC から各ノードへ通知するとき転送報告に含まれる乱数を使うことで、通知の真正性を確保することができる。これにより、例えば複製や erasure coding の冗長性を上げるなどの対策をオーバーレイに指示することができ、可用性を制御することが可能となる。

6 セキュア・オーバーレイの実現に向けて

4 では、オーバーレイネットワークの経路制御における脅威モデルについて述べ、次に 5 では、経路制御において責任追跡性、信頼性、可用性を実現するための方式を提案した。しかしながら 3 で述べたように、セキュア・オーバーレイの実現に当たっては Rendezvous、Location におけるセキュリティ確保も重要である。

Rendezvous、Location において用いることができる技術はアプリケーションやプラットフォームによって制約される。例えばアプライアン

スに内蔵されたプログラムが自動的にオーバーレイに加入する場合、乱用対策としてはチューリングテストよりハードウェアトークンのほうが適している。これに対し、インスタント・メッセージング用途では、SPIM (IM におけるメッセージ大量送信攻撃) 対策として、チューリングテストやノード評価を導入することが求められる。また不特定多数の利用者に対するアプリケーション層マルチキャスト用途では、セッションの秘匿性は求められず、一貫性のみが要求されると考えられる。一方、グループウェア用途ではアプリケーション層マルチキャストであっても、秘匿性・一貫性の双方が要求される。

このようにセキュア・オーバーレイの構築に当たっては、アプリケーションごとに異なる脅威モデルを取り扱う必要があり、個々のセキュア・オーバーレイで暗号方式や認証・加入方法を選べることが重要である。現在、セキュリティ高度化グループではセキュア・オーバーレイの基本的機能を提供するソフトウェア・フレームワークの開発に取り組んでいる。以下では、昨年度の成果であるフェーズ 1 開発の概要について述べる。

6.1 フェーズ 1 開発

本フレームワークは、セキュア・オーバーレイに関する方式研究を行うための電子的研究開発設備として必要なソフトウェアを設計・実装したものである。したがって前節で述べた方式は、本フレームワーク上に実装することで有効性を実証することができる。また、先行研究[1]~[4]では方式提案を裏打ちする実装がなく、有効性を第三者が実証することが困難であったが、本フレームワークをソフトウェア・バスとし、提案方式の流通を容易にすることで問題を解決することができると考えられる。

本フレームワークは C++ で実装されており、FreeBSD、Linux、MacOS X、Windows をはじめとする主要なオペレーティングシステム上で動作する。また C++ で記述されているため、Java で記述された既存のオーバーレイ向けツールキット等と比較して軽量であり、1 台の端末で 60 ノード程度を動作させても支障ない。このため小規模な計算機クラスタであっても、大規模なオーバーレイ・ネットワークを構成して実験を行うことができる。C++ で実装しつつ、プログラムの移植性を高めるために、通信ライブラリとして ACE、暗号化ライブラリとして Crypto++、GUI ライブラリとして Qt を用いている。これにより Java VM のような実行時オーバーヘッドの高い実装方式を用いることなく、かつプログラムの移植性の高さを実現している。

また、本フレームワークでは経路制御アルゴリズムとして Chord、Pastry を実装することで、セキュア・オーバーレイの方式研究において前提条件となる部分での敷居の高さを解消できていると考える。また、たんに Chord、Pastry の実装を提供するのではなく、これらを組み合わせた方式[3]や、複数経路を組み合わせた拡散通信[14]などの有力な提案をそれぞれ Multiroute、DC-net のクラスとして実装し、提供している。

さらに、本フレームワークでは KBR (Key-Based Routing) API に基づいてクラス設計を行っており、オーバーレイの機能モデルとして DHT のほか、DOLR、CAST なども実現可能である。現在のところ DHT が実装されており、(key, value) ペアの put/get が可能である。このほか key に対する send/receive を行う簡単な

API が実証目的で実装されており、これを用いて publish/subscribe モデルなどが実現できる。またプロトコル設計上の工夫がなされているので、単一のオーバーレイ上で複数の機能モデルを用いることもできる。

このほか、C++ を用いているため、用途に合わせてテンプレート・パラメータを指定してインスタンス化できるという点や、複数のオーバーレイを同時に使い分けられる点、DHT オブジェクトを first-class object であるかのように扱えるという点も利点であるといえる。

また、暗号化・ハッシュ等の機能をストリームに対するフィルタとして追加することができ、アプリケーションに大幅な変更を加えることなく資源探索における秘匿性、一貫性を確保することができる。Crypto++ では、暗号化アルゴリズムとしては AES、IDEA、RC5 など実装されている。また署名アルゴリズムとしては、SHA-1、SHA-384、MD5 など実装されている。なお、本フレームワークではオーバーレイで用いる識別子のビット長は自由に変更できるため、かりに SHA-1 の衝突困難性が破られたとしてもアプリケーション開発時に回避することは容易である。

7 むすび

オーバーレイネットワークのセキュリティ機能を Rendezvous(近接性の維持)、Location(資源探索)、Routing(経路制御)の3側面からとらえ、各側面におけるセキュリティ機能を組み合わせる必要があることを指摘した。特に経路制御について脅威モデルを構築し、対策方式を提案した。提案方式は、ブラインド転送、分散型の信頼錨としての ONOC、抜き打ち検査からなる。アプリケーションは Rendezvous、Location のそれぞれにおいて異なるセキュリティ要件を有するため、オーバーレイの基本的機能を C++ フレームワークとして提供し、これを既存の認証・暗号化・ハッシュ等のモジュールと組み合わせることでセキュア・オーバーレイが実現できると考える。今後、本フレームワークを活用してセキュア・オーバーレイの方式研究ならびに実証研究を進めていく予定である。

参考文献

- 1 E.Sit and R.Morris : "Security considerations for peer-to-peer distributed hash tables", IPTPS, 2002.
- 2 J.R.Douceur : "The sybil attack", IPTPS, 2002.
- 3 M.Castro, P.Druschel, A.Ganesh, A.Rowstron, and D.S. Wallach : "Secure routing for structured peer-to-peer overlay networks", OSDI, 2002.
- 4 A.Singh, M.Castro, P.Druschel, and A.Rowstron : "Defending against eclipse attacks on overlay networks", ACM SIGOPS European Workshop, 2004.
- 5 I.Stoica, R.Morris, D.Karger, M.F.Kaashoek, and H.Balakrishnan : "Chord : A scalable peer-to-peer lookup service for internet applications", SIGCOMM, 2001.
- 6 A.Rowstron and P.Druschel : "Pastry : Scalable, decentralized object location and routing for large-scale peer-to-peer systems", Middleware, 2001.
- 7 D.M.Petar Maymounkov : "Kademlia : A peer-to-peer information system based on the XOR metric", IPTPS, 2002.
- 8 K.Gummadi, R.Gummadi, S.Gribble, S.Ratnasamy, S.Shenker, and I.Stoica : "The impact of dht routing geometry on resilience and proximity", SIGCOMM, 2003.
- 9 F.Dabek, B.Zhao, P.Druschel, J.Kubiatowicz, and I.Stoica : "Towards a common api for structured peer-to-peer overlays", IPTPS, 2003.
- 10 M.Feldman, K.Lai, I.Stoica, and J.Chuang : "Robust incentive techniques for peer-to-peer networks", ACM Electronic Commerce, 2004.
- 11 M.Abadi, M.Burrows, M.Manasse, and T.Wobber : "Moderately hard, memory-bound functions", NDSS, 2003.
- 12 W.K.Josephson, E.G.Sirer and F.B.Schneider : "Peer-to-peer authentication with a distributed single sign-on service", IPTPS, 2004.
- 13 A.D.Keromytis, V.Misra and D.Rubenstein : "SOS : Secure overlay services", SIGCOMM, 2002.
- 14 S.Goel, M.Robson, M.Polte and E.G.Sirer : "Herbivore : A scalable and efficient protocol for anonymous communication", Technical Report TR2003-1890, Cornell University Computing and Information Science, 2003.
- 15 P.Maniatis, M.Roussopoulos, T.Giuli, D.S.H.Rosenthal, M.Baker, and Y.Muliadi : "Preserving peer replicas by rate-limited sampled voting", SOSP, 2003.



かどばやし ゆう き
門林雄基

情報通信部門セキュリティ高度化グループ専攻研究員 博士(工学)
オーバーレイネットワーク、ネットワークセキュリティ



なみざわ おさむ
滝澤 修

情報通信部門セキュリティ高度化グループ主任研究員 博士(工学)
コンテンツセキュリティ、非常時防災通信

なか お こう じ
中尾康二

情報通信部門セキュリティ高度化グループリーダー
情報セキュリティ技術