Host Identity Protocol を用いた、ユビキタスネットワークのセキュアな提供方法

Providing Ubiquitous Networks Securely Using Host Identity Protorol

高橋　暁弘 †　　前田　朋孝 †　　岡部　寿男 ‡
Akihiro Takahashi†　　Tomotaka Maeda†　　Yasuo Okabe‡

1　はじめに

あらゆる情報端末や電子機器が、有線や無線の多様なネットワーク接続の機能を持つようになった今日、それらをあらゆるところで利用可能にするユビキタスネットワークの実現が期待されている。理想的なユビキタスネットワークにおいては、ユーザはどこに行ってもそこに何らかのネットワークがある限り、それを介してインターネットに接続できる。そのためには、ネットワークの設置者である管理者が、来訪者である不特定多数のユーザに対して、利用者登録などの手間なしにネットワークを貸すことができることが必要である。また同時に、ユーザによる不正アクセスや違法行為等が生じた際には、管理者は利用者を追跡し特定することができるようになっている必要がある。

そうした期待に伴い、新幹線や様々な場所で利用できる、公衆無線インターネット接続サービスが多数展開されている。大別して通信事業者（Internet Service Provider : ISP）によって運用されるものや、基地局（アクセスポイントなど）設置者が運用するものがある。こうしたネットワークサービスのうち、ISP などによる有償のサービスではなく、FON[1] や eduroam[2] といった、基本的に無償でインターネットへの接続性を提供するようなサービスの事を、我々は開放型ユビキタスネットワークアーキテクチャと呼んでいる。

こういったネットワークサービス提供者側は、匿名でのサービス利用による不正を防止する責任がある。例えば、外部への不正アクセスや、匿名での誹謗中傷・違法コンテンツ（映像・ドキュメントなど）の送信などを防がなければならない。しかし、認証などを何も行わずただサービスを提供するだけでは、ユーザが匿名でサービスを利用できてしまい、不正を防止・抑止する事ができない。このため、管理者はユーザの認証を行う必要があり、公衆無線インターネットサービスにおける ISP ではユーザの個人情報を保持している。これにより、もし不正が起こった場合、管理者に対して被害者からのクレームが送られる。被害者からは IP アドレスしか辿れないため、ユーザが誰か分からないためである。これも管理者にとって負担である。そのために、ユーザごとに識別子 (ID) を付与する事が考えられる。

また、開放型ユビキタスネットワークにおいては、管理者は通信事業者であるとは限らない。そのため、管理者が不正を働いていない事が保証されなければ、ユーザは安心してネットワークを利用できず、管理者自身も不正を働いていない事を主張できない。あるいは、攻撃者が管理者に不正をおしつけて言い逃れする可能性が考えられる。管理者が不正を働いておらず、攻撃者が不正を行った上で言い逃れができないようにする事、すなわち否認不能性の確保が必要である。

本研究では、ネットワークを誰もがセキュアに提供するために、Host Identity Protocol (HIP) [3][4] を応用する。HIP ではホストそれぞれが世界で一意に定まるような ID を持っているため、認証を行う事ができる。すなわち、もしインシデントが発生しても、その ID を用いてユーザを特定する事が出来る。更にエンドポイント間でのセキュリティプロトコルであるため、管理者が不正を働いていない事の証明（否認不能性）も確保できている。これを利用する事で、管理者が誰にでもネットワークを貸す事ができるようなモデルを提案する。その上で、運用上の HIP のみを通すネットワークの安全性、実際にパケットからユーザを追跡する具体的な方法について考察を行う。

以下の構成を述べる。2 章で FON や eduroam といった関連事例を紹介し、3 章で問題定義を行う。4 章で HIP を紹介し、5 章でモデルを提案し、考察を行う。最後に 6 章でまとめとして、結論と今後の課題を述べる。

2　関連研究

ISP といった事業者による公衆無線サービスが多数展開されている一方で、FON や eduroam といったローミングサービスがいくつか運営されている。本章ではこれらのサービスについて紹介し、更に VPN を用いた開放型ユビキタスネットワークモデルである、みあこ

† 京都大学大学院情報学研究科, Graduate School of Informatics, Kyoto University
‡ 京都大学学術情報メディアセンター, Academic Center for Computing and Media Studies, Kyoto University

ネット方式 [5] についても紹介する。

2.1 FON

FON は、FON 基地局を設置した会員は他の会員が設置した基地局を利用できる、というモデルの会員制サービスである。認証としては、管理者は FON 基地局を購入・設置し会員登録を行い、基地局管理者＝ユーザとなるモデルのため、FON の運用チームが行っている。基地局管理者は、利用ログなどをとる事を強制されておらず、管理者の負担はそこまで大きくない。しかし、一度 Web による認証を通過するとそれ以降の通信のチェックを行わない為、通信を乗っ取られるおそれがある。すなわち、否認不能性が確保されているとはいえない。

2.2 eduroam

eduroam は、欧州を中心に大学間のローミングを行う枠組みであり、世界規模の取り組みである。こういったサービスでは、RADIUS による認証連携や IEEE802.1x に基づく EAP-TTLS 認証を行っている。しかし RADIUS 認証などにおいては、管理者は信頼されており、不正を働く事がない、という前提のものであった。すなわち、否認不能性が十分に確保されていない。また、管理者は認証結果により通信を制御するため、認証のログを取っておく必要がある。

2.3 みあこネット方式

大平らは公衆無線インターネットアクセスサービスをセキュアに提供するための方法について議論している [6]。二つのモデルが考察されており、一つはアクセスポイントにおいて認証のトランザクションをリレーするかパススルーするモデル、もう一つはトンネル方式で通信を行うかエンドツーエンドのセキュリティプロトコルを利用するモデルである。古村らはみあこネット (Mobile Internet Access in KyotO : MIAKO)[7] と称するモデルを提案している。みあこネットは大学などの非営利組織により運営されている。みあこネットは VPN (Virtual Private Network) プロトコルとして Microsoft PPTP (Point to Point Tunneling Protocol) を用いた、IEEE802.11b に基づいた公衆無線インターネットサービスである。VPN を用いてデータを暗号化しているため、管理者は不正を働く事ができず、濡れ衣を着せられる事がない。すなわち、否認不能性は確保されている。更に、VPN サーバ運用者が認証記録の管理を行うため、管理者は認証のログを取る必要はない。接続性提供者とユーザの管理を分割することで、双方の管理負担を軽減しており、同時にセキュリティ面の向上をはかっている。大平らは、このみあこネットを用いて実証実験を行っている [8]。

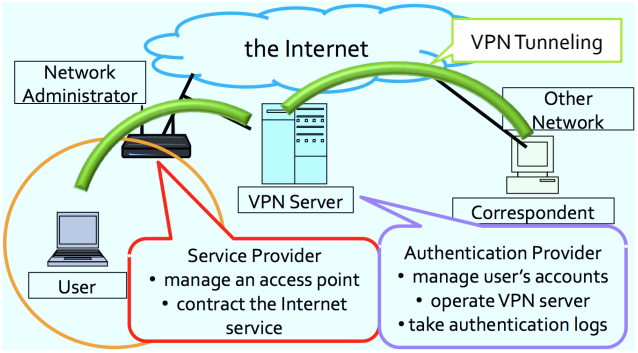

図 1: みあこネット方式

3 問題定義

基地局設置者が運用する開放型ユビキタスネットワークにおいて、ユーザは通常、基地局設置者が提供する回線を通して通信相手と通信する。ここでいう基地局設置者とは、例えば ISP の回線を借りている人が無線基地局を設置したりして利用者に提供している場合である。しかし 1 章で述べたように、基地局設置者（ネットワーク管理者）には、匿名での利用による不正アクセスを防止する責任があり、つまりユーザが誰であるか判別できなければならない。すなわち、セキュアなユビキタスネットワークの実現のためにはインシデントが発生した時にユーザを特定するため、ユーザの認証を行う事が求められる。それはアカウントの管理やネットワーク利用状況のログの記録を行わなければならない事を意味しており、管理者にとって負担となる。また、インシデント発生時における問い合わせも、管理者にとって負担となる。ユーザに IP アドレス以外の ID を付与し、通信相手が誰と通信しているか明らかな状態で通信を行えるようにする事でこの問題は解決できる。

その上で、誰もがネットワークを提供できるようにするためには、認証の管理コストを軽減、あるいは分担する事が望ましい。また、管理者が信頼されているわけではないため、不正を働いていない事の証明（否認不能性）が必要となる。

本研究では、HIP を応用したモデルを提案する事で、これらの問題を解決する。HIP はエンドポイント間で動作するセキュリティプロトコルであり、データが暗号化されている。このため否認不能性の確保が可能である。また、HIP ホストはそれぞれ一意に定まる ID を持っているため、通信相手は誰と通信しているのか明

らかである。更に、これを利用して DNS サーバに認証機能を持たせる事を提案する。

一方、2 章で述べたように、RADIUS や VPN サーバを用いて認証を行う仕組みが考えられている。これらの方法により、管理者は RADIUS サーバあるいは VPN サーバに認証機能を任せる事ができる。すなわち、管理者は接続機能を管理し、認証担当者は認証機能を管理する、といった管理コストの分担が可能となっている。認証機能の分担、管理者による認証ログの記録、否認不能性の確保についてまとめたものが以下の表 1 である。

表 1: モデル比較

	認証機能	認証ログ
FON	FON チーム	不要
eduroam	RADIUS サーバ	必要
みあこネット方式	VPN サーバ	不要
提案手法	DNS サーバ	必要
	否認不能性	—
FON	NG	—
eduroam	NG	—
みあこネット方式	OK	—
提案手法	OK	—

また、みあこネット方式においてはユーザは必ず VPN サーバを経由して通信を行わなければならない（図 1）。例えば、同一ネットワークにいるユーザ同士が通信を行おうとしても、そのために必ずいくらかのオーバヘッドが発生してしまうといった問題が存在する。提案手法では、この問題も解決できる。

以下、本研究で用いる HIP について基本的な要素を紹介し、提案手法がこれらの問題をどのように解決しているか述べる。更にその上での運用上の問題、すなわち管理者はどの程度ログを記録する必要があるのか、どのようにしてパケットを制限するのか、インシデントが発生した際にどのように追跡するのか、内包するリスク（防止できない攻撃）といった項目について考察を行う。

4 Host Identity Protocol

HIP は、盗聴やその他の脅威に対するセキュリティ面を強化したエンドポイント間で動作するプロトコルである。更に拡張として mobility や multi-homing をサポートしている [9]。本章では、セキュアなユビキタスネットワークの実現に関して重要だと思われる、HIP の基本的なアーキテクチャについて紹介する。

4.1 Locator/ID Split

従来のインターネット接続では、ホスト識別子（誰が通信しているのか : ID）とトポロジーの場所（どこから通信しているか : Locator）を同じ IP アドレスが示しているため、ユビキタスネットワークにおけるあらゆるニーズに対する柔軟な対応が難しいと考えられる。例えば、移動体が別のネットワークにシームレスに接続したい場合、などである。この場合、ID を変更せずに、Locator のみを変更する必要がある。

そこで、これらを分けて考える事を、Locator/ID 分離（ID/Locator Split）と呼ぶ [10][11]。HIP ではこのコンセプトに従い、ID として Host Identity 及び Host Identity Tag を用い、Locator として IP アドレスを用いる。

4.2 Host Identity, Host Identity Tag

HIP では、全てのホストが公開鍵と秘密鍵のペアを持っている。これらは一意に決まるもので、そのため全ての HIP ホストは認証可能である。これらの鍵はデフォルトでは RSA アルゴリズムに従って自己生成される、512, 1024, 2048bits の bit 列である。これを Host Identity (HI) と呼ぶ。

Overlay Routable Cryptographic Hash Identifiers (ORCHID)[12] に従って HI のハッシュをとり、IPv6 のアドレス長と同じ 128bits に直したものを HIT と呼ぶ。HIT は IPv6 の特殊クラスとして用いられる。HIT 及びホストの公開鍵は、DNS に保存される。

HIP では、これら HI と HIT をホストの識別子として用いる。また、HIT の最後の 32bits を LSI (Local Scope Identifier) と呼び、ローカルでの動作をサポートする。これらの構成を図 2 に示す。

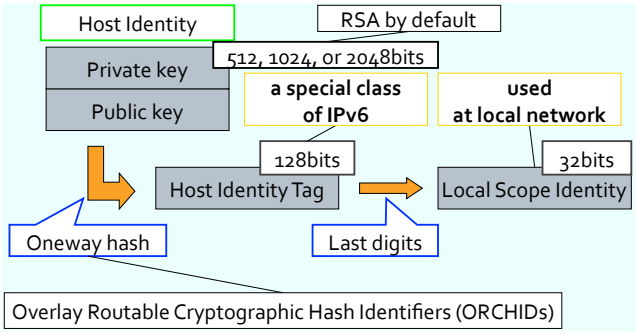

図 2: HI, HIT

4.3 Base Exchange

HIP では、ホストはセッションの始めに Base Exchange と呼ばれる鍵交換を行う。Base Exchange は 4way hand-shake プロセスであり、I1, R1, I2, R2 と呼ばれる HIP パケットで構成される。Diffie-Hellman 鍵交換 [13] を用い、お互いを認証する。HIP の通信は IPsec の ESP モードにより暗号化されており、このためパケットの盗聴やなりすましといった攻撃に対してよりセキュアな通信が可能となっている。

Base Exchange の様子を図 3 に示す。

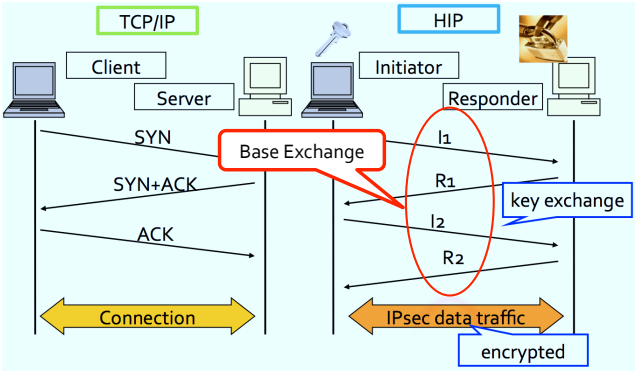

図 3: Base Exchange

5 モデルの提案と考察

提案モデルについて、3 章で述べた項目に関して、実現、あるいは考察するべき問題を以下にまとめた。

5.1 認証機能のコストの分担

5.2 否認不能性の確保

5.3 追跡可能性の確保

5.4 運用上の留意点

5.4.1 管理者によるパケットの制限方法

5.4.2 記録するログ

5.4.3 防止できない攻撃

5.1 認証コストの分担

本研究で提案するモデルとして、2 章で紹介したみあこネット方式のようなモデルを想定する。文献 [8] において、大平らはみあこネット方式におけるコスト負担を以下のように分担している。

- 認証提供者
  - ユーザアカウントの発行・管理
  - 認証用サーバの運用
  - ユーザ認証記録の管理
- 接続サービス提供者
  - 無線基地局の設置、設定管理
  - インターネット接続回線の契約

本研究において、認証提供者はとりもなおさず DNS 運用者の事となる。4.2 節で述べたように、HI 及びホストの公開鍵は DNS に保存されている [14]。HIP はこれらの情報を認証に使用するため、DNS のセキュリティは重要である。このため、HIP では DNS Security Extension (DNSSEC)[15][16] の利用を強く推奨している。DNSSEC は、電子署名を利用し DNS レコードが確かに信頼された DNS からのものである事、改ざんされていない事を保証する仕組みである（図 4）。すなわち、例えば DNS キャッシュポイズニング [17] のような攻撃に対するセキュリティが強化されている。本研究のモデルにおいても、その重要さから DNSSEC の利用を前提とする。DNSSEC によって守られている DNS レコードは、図 5 に示されるように”信頼の連鎖”と呼ばれる仕組みでルート DNSSEC サーバによってドメイン単位でその出自の確かさが保証される。

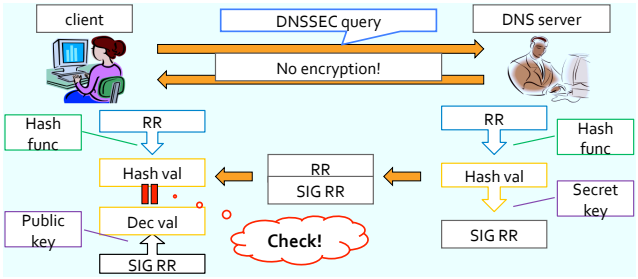

図 4: DNSSEC

本研究では、以下のように認証機能のコストを分担する。

- 認証提供者…DNS 運用者
  - DNSSEC サーバの運用
  - サーバへのユーザの登録
- 接続サービス提供者…ネットワーク管理者
  - 無線基地局の設置、設定管理
  - インターネット接続回線の契約
  - ログの記録

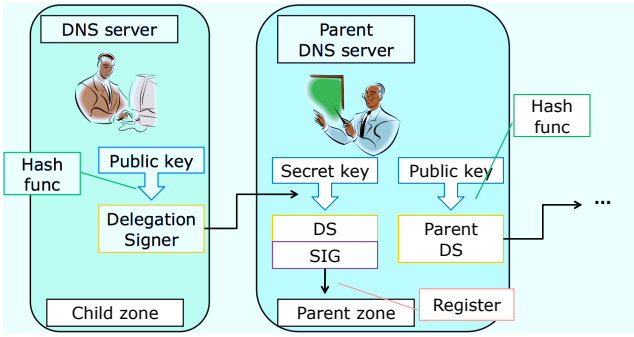

図 5: DNSSEC 信頼の連鎖

本研究では、DNS 運用者は予めユーザを登録し、HIP の ID と本人情報との紐付けを行っていると想定する。これにより、管理者は有事の際には DNS 運用者に問い合わせる事によって、ユーザが誰であるか追跡出来る。提案モデルを表したものが、図 6 である。

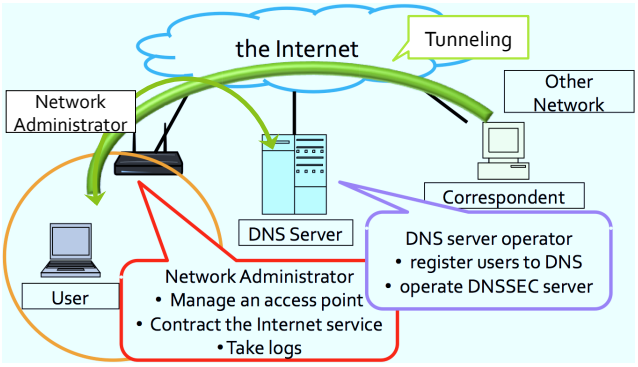

図 6: 提案するモデル

5.2 否認不能性の確保

従来のインターネットアクセスサービスにおいては、悪意のあるネットワーク管理者がパケットを改ざんしたり、なりすまし攻撃（IP スプーフィング）を行う可能性が存在した。また、管理者が攻撃を行っていない事を第三者によって明らかにできない。そのため、悪意のあるユーザが誰かを攻撃したとしても言い逃れでき、管理者に対しての負担となっている。しかし、本研究におけるネットワークではユーザと通信相手がお互いに認証されているため、管理者が不正をしていない事が分かる。通信者同士のパケットは、DNSSEC を TTP（Trusted Third Pirty：信頼できる第三者機関）として用いて彼ら自身か管理者によって検証が可能である。更に事前に認証を行っているため、通信相手は誰と通信しているかが明らかである。もしインシデントが発生した際、攻撃者が管理者に濡れ衣を着せることができない。

また、HIP における Base Exchange 以降の通信は、みあこネット方式と同様、IPsec の ESP モードにより、暗号化されている。また、Base Exchange では HI や HIT、IP アドレス以外の情報は確認できる状態で（平文で）含まれていない。つまり、管理者は Base Exchange パケットをチェックしてユーザを検証する事は可能であるが、ユーザのデータ通信の内容を盗聴したり、改ざんしたりする事は不可能である。すなわち、ユーザから盗聴などの疑いをかけられる事を避ける事ができる。

従って、提案するモデルにおいて否認不能性は確保されているといえる。

5.3 追跡可能性の確保

HIP パケットを確認すれば、管理者はユーザが誰か特定できるのだろうか。データ通信自体は暗号化されているが、Base Exchange パケットはそうではない。管理者のネットワークにいるユーザを A、通信相手を B とし、A から B へ通信する場合を考えると、実際の通信のスキームと確認できる主なデータの流れは以下のようになる。

1. A: DNS サーバへ問い合わせ、B の名前解決を行う。
2. A: I1 パケット→ B へ
   - A と B の HIT 及び IP アドレス（これらは以下の Base Exchange パケット全てに含まれる）
3. B: R1 パケット→ A へ
   - B の HI（公開鍵）、B の署名
4. A: I2 パケット→ B へ
   - A の HI（公開鍵）：これは暗号化するか平文か選択可能、A の署名
5. B: R2 パケット→ A へ
   - B の署名

ここで、A が送信する I2 パケット内の HI はオプションで平文で送信する事ができる。本研究でのモデルの利用においては、管理者のチェックのためにユーザは平文で I2 を送信する必要がある。これらに含まれるそれぞれの HI から、DNS に登録されたものかどうか、更にユーザの身元を追跡する事が可能である。署名というのは、パケットがそれぞれの秘密鍵で署名されている、という事である。ユーザ同士は署名を検証しあい、

パケットの送信者が確かである事、改ざんされていない事を確認できる。

つまり、管理者が間に入ってパケットを記録し、I2 パケットで平文送信を義務化すれば DNS へチェックすることができる。整理すると、DNS へ聞きにいけるのは HIT と HI（公開鍵）である。一方、DNS レコードには HIT、公開鍵が記録されているので、DNS に登録されているユーザかどうか確認する事が可能である。

したがって、管理者は Base Exchange だけ見ておけば、きちんと HI の確認を行う事が可能である。情報は Base Exchange から十分取得できるといえる。

5.4 運用上の留意点

管理者がネットワークを運用する上での観点から以下の点について考察を行う。

- 管理者によるパケットの制限方法
- 記録するログ
- 防止できない攻撃

5.4.1 管理者によるパケットの制限方法

管理者は、HI 及び HIT を Base Exchange から取得できる。これらの HI 及び HIT を DNS と照合することで、管理者はパケットのユーザ及び通信相手が正規のものであると確認できる。更にその DNS 運用者に確認する事で、ユーザの身元を追跡できる。すなわち、管理者は Base Exchange パケットを確認し、不正な HI 及び HIT を持つパケットの通過を制限する事ができる。

また、管理者はパケットの対応関係も保持しておく必要がある。対応関係とはつまり、ある I1 パケットに対する R1 パケット、それに対する I2 パケット、といった関係である。この対応関係を管理者が把握しておくことで、例えば I1 パケットのみを送りつけてくるといったような、Base Exchange のプロセスに従わないようなパケットも検知することができる。

Base Exchange 以降のパケットではデータは暗号化されているため、管理者は IP アドレスとの対応、及び IPsec パケットであるという情報を用いて、通信を制限する。

つまり、管理者は HI 及び HIT を元に Base Exchange パケットを制限し、IP アドレスとの対応によりデータ通信パケットを管理する。

5.4.2 記録するログ

本研究での提案モデルにおいては、いつ、誰がネットワークに接続していたかを把握するために、管理者はログを記録しておく必要がある。インシデントが発生した際にユーザを追跡するための情報は、Base Exchange パケットから取得する事ができる。また、Base Exchange が終了しなければ通信を行う事はできないため、管理者は正規に行われた Base Exchange パケットの組み合わせ（I1, R1, I2, R2）を記録しておけば良いと考えられる。

5.4.3 防止できない攻撃

本研究の提案モデルにおいて、盗聴や改ざん、DNS キャッシュポイズニングによるフィッシングなどについてセキュリティ面が強化されている一方、いくつか防止できない攻撃も残されている。

- 帯域消費型の DoS 攻撃（図 7）
- ユーザ側と通信相手が結託している場合

一般に、DoS 攻撃や DDoS 攻撃への対策は困難である。本研究におけるモデルにおいても、ネットワークに対してパケットを大量に送信し、帯域を輻輳させるタイプの DoS 攻撃、あるいは DDoS 攻撃に対しては、従来のインターネット環境における対策と同様、対処を行う事が必要である。例えば帯域制限や ICMP パケットのシャットアウト、ファイアウォールの利用といった対策を用いるべきである。

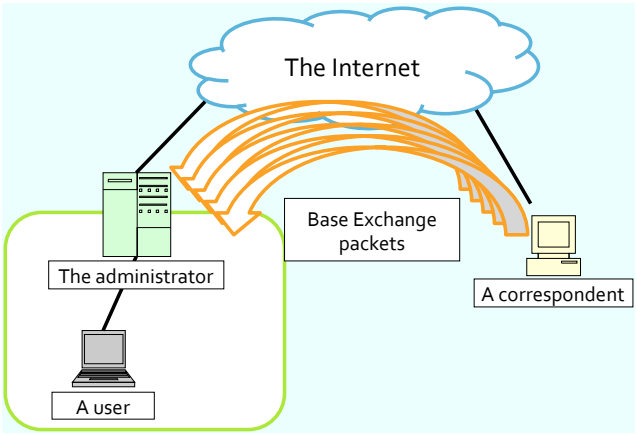

図 7: DoS 攻撃

また、ユーザ側と通信相手が結託している場合とは、次のような場合である。例えば、ある正規のユーザが通信を試み、ある通信相手と正規の Base Exchange を完了させる。ユーザ側のネットワークにいる攻撃者は、そのユーザの IP アドレスを確認する事が出来るため、その IP アドレスを用いて IPsec パケットを偽装し、通信を乗っ取る事が出来る。通常であれば通信相手との

暗号化鍵を取得する事ができないため、実際に通信を行う事は不可能である。しかし、通信相手も結託しており事前に鍵を共有していた場合、管理者は IP アドレスによりパケットのフィルタリングを行っているため、管理者のネットワークを使った、悪意のある者同士の通信を許してしまう事になる。

以上の議論をまとめたものが以下である。

1. 防止できる攻撃
    - パケットの盗聴、データの改ざん
    - DNS キャッシュポイズニング
2. 防止できない攻撃
    - 帯域消費型の DoS 攻撃
    - ユーザ側と通信相手が結託している場合の通信の乗っ取り

6 まとめ

本研究では、HIP を用いてユビキタスネットワークをセキュアに提供する方法を提案した。DNS 運用者に認証機能を任せる事で、ネットワーク管理者とのコスト負担の分担を実現した。

盗聴や改ざんに対してのセキュリティに加えて、DNSSEC の利用により、DNS キャッシュポイズニングやフィッシングに対してのセキュリティ面も強化されている。しかしその一方で、DoS 攻撃やユーザ側のネットワークにいる攻撃者と通信相手側のネットワークにいる攻撃者が結託している場合の通信の乗っ取りといったリスクを内包している事も分かった。

管理者は Base Exchange パケットを確認する事で、ユーザの追跡を行う事が可能である。しかし HIP ではデータの暗号化が行われるため、管理者は盗聴などを行う事ができない。また、通信者同士がお互いに認証してから通信しているため、攻撃者が管理者に濡れ衣をきせ、言い逃れする事を防止している。すなわち、否認不能性が確保されているといえる。

本研究のモデルにおいては、管理者は誰がネットワークを利用していたかを把握するために、Base Exchange のログを記録しておく必要がある。また、管理者は Base Exchange パケットの対応関係を確認し、不正なパケットを制限できる。

今後の課題としては、実際に動作環境を構築しこれらの考察をより深め、提案したモデルの妥当性を検証し、モデルの評価を行う事が挙げられる。更に、管理者によるパケットフィルタリングや記録するログのフォーマットについて考察し、実装を行いたいと考えている。

参考文献

[1] FON. http://www.FON.com/.

[2] eduroam. http://www.eduroam.org/.

[3] R.Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture. In *RFC 4423*, May 2006.

[4] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. In *RFC 5201*, Apr. 2008.

[5] MIAKO. http://www.miako.net/.

[6] K. Ohira, Y. Huang, Y.Okabe, K. Fujikawa, and M. Nakamura. Security Analysis on Public Wireless Internet Service Models. In *WMASH '05*, pp. 107–110, Sept. 2005.

[7] Takaaki Komura, Kenji Fujikawa, and Yasuo Okabe. The MIAKO.NET public wireless internet service in Kyoto. In *Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, WMASH '03, pp. 56–63, 2003.

[8] Kenji Ohira, Atsushi Sumioka, Yuki Kitaoka, Takaaki Komura, Kenji Fujikawa, and Yasuo Okabe. Design and Management of the MIAKO.NET Public Wireless Internet Access Service. *The Transactions of the Institute of Electronics, Information and Communication Engineers*, Vol. J93-B, pp. 759–768, 2010.

[9] P. Nikander, T. Henderson, C. Vogt, and J. Arkko. End-Host Mobility and Multihoming with the Host Identity Protocol. In *RFC 5206*, Apr. 2008.

[10] V.P. Kafle, H. Otsuki, and M. Inoue. An ID/locator split architecture of future networks. In *Second ITU-T Kaleidoscope event on INnovations for Digital Inclusion*, 2009.

[11] V.P. Kafle, K. Nakauchi, and M. Inoue. Generic identifiers for ID/locator split internetworking. In *First ITU-T Kaleidoscope event on Innovation in NGN*, 2008.

[12] P.Nikander, J. Laganier, and F. Dupont. An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID). In *RFC 4843*, 2007.

[13] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, No.6, pp. 644–654, Nov. 1976.

[14] P. Nikander and J. Laganier. Host Identity Protocol (HIP) Domain Name System (DNS) Extension. In *RFC5205*, Apr. 2008.

[15] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. In *RFC4033*, Mar. 2005.

[16] DNSSEC - The DNS Security Extensions - Protocol Home Page. `http://www.dnssec.net/`.

[17] D. Atkins and R. Austein. Threat Analysis of the Domain Name System (DNS). In *RFC 3833*, Aug. 2004.