マルチメディア通信と分散処理 71−12
（１９９５．７．１３）

移動ホスト認証を考慮した資源割り当て機構の提案

小林 和真† 山口 英† 山本 平一†

†奈良先端科学技術大学院大学情報科学研究科

内容梗概

本稿ではInternet環境での移動ホストにおけるホスト認証の必要性について議論し、移動ホスト認証のためのモデルとしてパスポートモデルを提案する。このモデルは移動ホスト毎に用意されるディジタル署名つきの識別情報(PASSPORT)を用いた認証に基づいている。またこのモデルの実装例として、移動ホスト認証を考慮した資源割り当て機構であるDHCPAプロトコルを提案する。

Dynamic Host Configuration for Mobile Host with Authentication

Kazumasa Kobayashi† Suguru Yamaguchi† Heiichi Yamamoto†

†Graduate School of Information Science, Nara Institute of Science and Technorogy

Abstract

This paper focuses technical requirements for authentication of mobile hosts in the Internet environment. We introduced the Passport Model, in which all the mobile hosts exchange the PASSPORT with resource management server suppoting mobile hosts on the each network. The PASSPORT is a special data with the digital signature assign to each mobile hosts. Based on this model, we proposed the DHCPA protocol which is a security enhancement of the DHCP protocol. In this paper we discuss the design and the implimentation of the DHCPA protocol.

1 はじめに

コンピュータ関連技術の急速な進歩にともなってコンピュータも小型軽量化が進んでいる。これにより従来のワークステーションに匹敵する能力を持つシステムを簡単に持ち運ぶことができるようになってきた。利用者にとって必要な計算機利用環境をそのまま持ち運べ、かつインターネットへと接続できるホストを実現できれば、移動した先や移動中などさまざまな場所で自由にコンピュータを用いた作業を行うことができる。このような環境を実現する技術は従来のコンピュータの利用形態に大きな変革をもたらす技術となり得る。このように一般に利用者とともに移動しネットワークに接続されるホストを「移動ホスト」(Mobile Host)と呼んでいる。

これらを背景としてインターネットでは移動ホストに対応するために数多くのプロトコルや実装が提案され実用化を目指した研究が行われてきている。しかしながらインターネットにおいて移動ホストに対応した環境を実際に構築してみると、さまざまな問題点が明らかになってきた。そのひとつが移動ホストの認証である。

ホストが移動した先でも移動前と同様にインターネットのサービスを利用するためには、移動の前後で同一のホストであることを示す必要がある。本稿では移動ホスト認証のための汎用モデルとしてパスポートモデルを提案し、さらにネットワーク資源の割り当て機構であるDHCP(Dynamic Host Configuration Protocol)を拡張して資源割り当てにおけるホスト認証問題の解決手法を提案する。

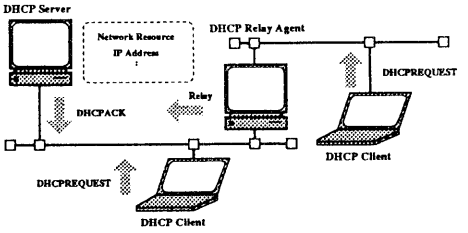

図 1: DHCP

2 移動ホストと資源割り当て機構

2.1 関連技術

移動ホスト環境の実現には幾つかの技術的な課題を克服しなければならない。ここでは環境構築に必要な関連技術を紹介するとともに本稿で解決を目指す課題について述べる。

2.1.1 移動ホスト識別技術

インターネットでは、ネットワークに接続されたホストを識別するためにIPアドレスを用いてホスト自身の識別と接続位置に関する情報を表現している。このため移動ホストの場合、移動先での接続に新たなIPアドレスを必要とし、結果的に移動前と別のホストとして識別されてしまう。

この問題を解決するためにいくつかの提案が行われている。その代表的なものは、移動ホストのIPアドレスを変更せず移動先のネットワークでトンネリングの技術を用いて仮想的に本来のネットワークに接続してしまう方法である。この方法はIETF(Internet Enginiaring Task Force)のMobile-IP WGで採用されている方法である[1]。

WIDEプロジェクトでは、VIP(Virtual Internet Protocol)[2][3]を提案し移動ホスト環境を実現している。この方法では接続位置に関する情報のみをIPアドレスで表現し、ホスト自身の識別をIPアドレスとは分離してVIPアドレスで表現している。これによりホストがネットワーク上を移動してもホスト自身の識別情報であるVIPアドレスは一定となり移動した後も同じホストとして識別できる。

2.1.2 資源割り当て機構

移動ホストに対応するためのこれらの提案では、ほとんどの場合移動した先で何らかのネットワーク資源を必要とする。また従来から用いられてきたXターミナルやディスクレスクライアントには起動時にサーバの情報やBootプログラムなどのネットワーク資源の割当を要求するものも存在する。このような要求に対応するためにインターネットではいくつかの資源割当機構が提案されている。

BOOTP(Bootstrap Protocol) [4]は、ホストに設定するIPアドレスやBootプログラムなど要求されたネットワーク資源をユーザの介在無しに割当てることができるプロトコルである。

DHCP(Dynamic Host Configuration Protocol) [5][6][7]は、BOOTP上位互換の資源割り当てプロトコルであり、ユーザの介在無しに動的な資源の割り当てができ、かつ割り当てた資源の回収が可能なプロトコルである。

DHCPはネットワーク資源の割り当てを行うDHCPサーバと資源を要求するクライアント、要求を中継するリレーエージェントから構成される(図1参照)。

2.2 移動ホスト認証の必要性

BOOTPプロトコルやDHCPプロトコルでは、資源の割り当てに際して割り当てるホストの認証をまったく考慮していない。これらのサーバはどのようなクライアントからの割り当て要求に対しても要求に応じて資源を割り当ててしまう。

DHCPは割り当て要求を行うクライアントと

してXターミナルやディスクレスワークステーションなど処理能力が著しく低いホストを想定している。これらのホストの場合は資源割り当て時に複雑な認証処理を行わせることが能力的にも非常に困難であり、装置の設置場所も一定で認証を考慮する必要性が少ないと考えられてきた。

しかしDHCPクライアントを標準で装備しているWindowsNT3.5の出現や携帯型のノートパソコンの普及など、資源割り当て時の認証の必要性は急速に高まっている。特に無線Ethernetや赤外線(IR)通信装置のような無線ネットワークの場合は無線が届く範囲内であれば簡単にネットワークに接続でき、自動的に割り当てられたアドレスでネットワークを利用できるためセキュリティ保全上明らかに好ましくない。

そこで本稿では移動ホストの認証を考慮した資源割り当て機構を提案し、この問題の解決を試みた。

3 パスポートモデルの提案

3.1 パスポートモデル

我々が海外に出かける場合、自分自身の身元を証明するためにパスポートを所持する。パスポートによって他国への入国が許可され現地での活動を許される。本稿で提案する移動ホストのための認証機構モデルではこのパスポートの概念を用いる(以下パスポートモデルと呼ぶ)。

パスポートモデルでは移動ホストの身元を証明するために識別情報であるPASSPORTをホスト毎に用意する。PASSPORTは移動ホストの所属する組織(サイト)の責任において発行され、移動ホストの身分を保証する。またこのPASSPORTを発行するサーバをホームサーバと呼ぶ(図2参照)。

PASSPORTには移動ホストを認証するために必要な情報を記述する。また、実社会のパスポートでは身分照合にサインを用いているが、このモデルではディジタル署名をホストの照合に用いる。表1に実社会のパスポートとこのモデルとの対応を示す。

移動ホストの接続予定先のサイトによっては

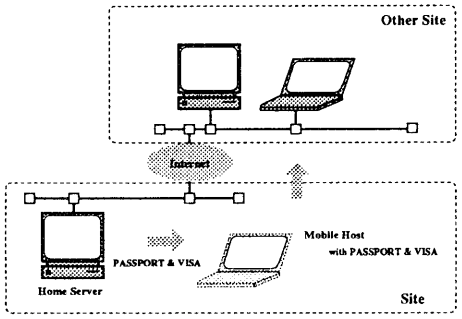

図2: パスポートモデル

	パスポート	PASSPORT
通用範囲	国交のある国	交流のあるサイト
発行者	国(外務省)	サイト(ホームサーバ)
照会方法	サイン	ディジタル署名

表1: パスポートとPASSPORTの比較

事前に接続認可を取るなどサイト固有の認証条件を付加する必要があるかもしれない。そのためにパスポートモデルではこのような条件を規定するためにVISAの概念を導入する。

PASSPORTやVISAに実際に記載される暗号鍵や認証情報については特に規定しない。移動ホストの認証に必要な情報が与えられ何らかのメカニズムで認証処理を行うことができれば良い。

3.2 ディジタル署名

パスポートモデルではディジタル署名による認証を想定している。一般的なディジタル署名では受信者 R と送信者 S の間で次の3つの条件を満足する必要がある。

1. R が受信したメッセージが確かに S が送信したものであると確認できること。
2. R を含む第三者 T が S のメッセージを偽造できないこと。
3. S がメッセージを R 宛に送信した事実を送信後に否定できないこと。

ディジタル署名に利用可能な暗号系にはDESなどの慣用暗号系とRSAなどの公開鍵暗号系が

Step 1 :	$Cypher$	$\leftarrow$	$E\{D\{Message\}^{K_S}\}^{K_{R^{-1}}}$
Step 2 :	*send Cypher to R*		
Step 3 :	$Message$	$\leftarrow$	$E\{D\{Cypher\}^{K_R}\}^{K_{S^{-1}}}$

K_S : Sender Secret Key
$K_{S^{-1}}$: Sender Public Key
K_R : Receiver Secret Key
$K_{R^{-1}}$: Receiver Public Key

表 2: 公開鍵暗号による直接署名法

ある。慣用暗号系を用いる場合には送信者と受信者の間で鍵を共有しなければならない。このため送受信者の組合せの数だけ鍵を用意しなければならずInternet環境では現実的ではない。また署名法には、受信者が受信したメッセージの正当性を直接確認する直接署名法と、信頼できる第三者を調停者としてメッセージの正当性を確認する調停署名法がある。

確実なディジタル署名を実現するには第三者による調停署名法を用いるべきである。しかし、現在のインターネット環境では調停者である第三者の正しさを認証することは非常に困難であることが予想される。そこで本稿では公開鍵暗号による直接署名方式(表2参照)を用いることにする。

この方法では前述のディジタル署名の3の条件を満足することはできないが、移動ホストからのメッセージの認証確認と送信メッセージの偽造を防ぐことが可能である。

4 DHCPAの提案

パスポートモデルを資源割り当てプロトコルである DHCP に適用した例として DHCPA(DHCP with Authentication) を提案する。ただしディジタル署名で必要な暗号系で用いる暗号鍵の配送については本稿では議論しない。

4.1 DHCPAの構成要素

DHCPA は認証処理を行い資源を割り当てるサーバ (DHCPA Server) と資源割り当て要求を出すクライアント (DHCPA Client)、PASSPORTを発行するホームサーバ(DHCPA Home Server) から構成される (図3参照)。

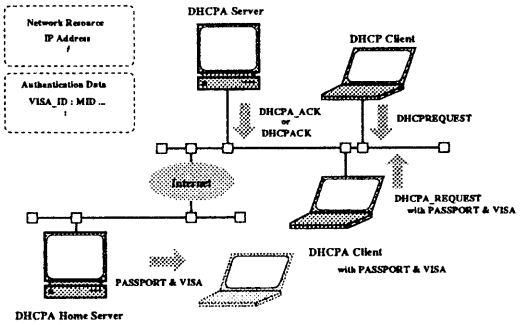

図 3: DHCPA

DHCPA サーバは移動ホストである DHCPA クライアントからの割り当て要求に含まれる PASSPORT を用いてホスト認証を行い資源の割り当てを実行する。認証機構以外は通常の DHCP と同様に動作する。

4.2 DHCPA の PASSPORT

DHCPA PASSPORT に含まれる情報を次に示す。

- ホームサーバの IP アドレス
- クライアントの MID(Mobile ID)
- ディジタル署名されたクライアントの認証情報
  - ホームサーバの秘密鍵で暗号化されたクライアントの公開鍵
  - クライアントの秘密鍵で暗号化された VISA とタイムスタンプ

ホームサーバはクライアント (移動ホスト) 毎に固有の PASSPORT を発行する。またディジタル署名には公開鍵暗号法である RSA[8] と MD5[9] を用いているが、これ以外の署名法にも対応できるよう設計を行った。

5 DHCPA の設計と実装

5.1 DHCPA プロトコル

DHCPA サーバと DHCPA クライアント間での認証処理に必要な情報を、DHCPA では

DHCPA Handle Strings(18)			
code(1)	HL(1)	MT(1)	version(1)
Home Server IP Address(4)			
Mobile Host ID(4)			
PL(1)	PT(1)	CT(1)	notuse(1)
PASSPORT Field(PL)			

code : DHCPoption Code field(future)
HL : DHCPA Header Length
MT : DHCPA Message Type
version : DHCPA Version
PL : Passport Field Length
PT : Passport Field Type
CT : Crypt Type

図 4: DHCPA Header Format

PASSPORT Field
$E\{K_{M^{-1}}\}^{K_H}$
$E\{VISA, timestamp, MD5[VISA, Timestanp]\}^{K_M}$

K_H : Home Server Secret Key
K_M : Mobile Host Secret Key
$K_{M^{-1}}$: Mobile Host Public Key

図 5: PASSPORT Field

DHCP プロトコルのオプションである Class-identifier オプションに記述する。このオプションを用いてクライアントを Class 別に分類し Class 毎にサーバ側で異なる処理を行わせることが許されている。DHCP Class-identifier オプションに記述する DHCPA の Header Format を図 4に示す。

5.2 DHCPA PASSPORT Field

PSAAPORT Field は、認証情報などを格納するフィールドである。このフィールドの長さは DHCP オプションの制約から 220 バイトに制限されている。

このフィールドには、DHCPA クライアントの認証処理に用いられる情報が格納される。

図 5は DHCPA Header に含まれる PASSPORT Field を示している。DHCPA ホームサーバの秘密鍵 K_H で暗号化された DHCPA クライアントの公開鍵 $K_{M^{-1}}$ と、VISA と要求時のタイムスタンプを DHCPA クライアントの秘密鍵 K_M で暗号化した認証情報が含まれている。

0x00	: DHCPA_QUERY message
0x01	: DHCPA_OFFER message
0x02	: DHCPA_REQUEST message
0x03	: DHCPA_ACK message
0x04	: DHCPA_NAK message
0x05	: DHCPA_RELEASE message
0x06-ff	: future use

表 3: DHCPA Message Type

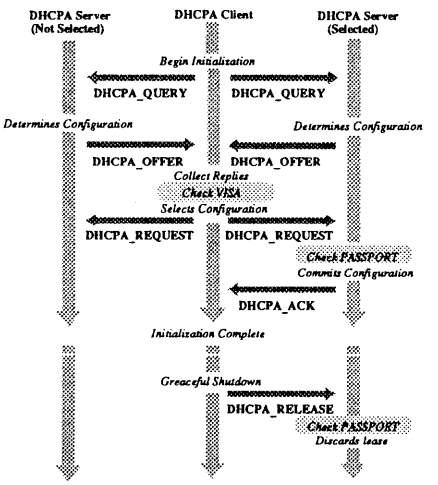

図 6: DHCPA プロトコルの処理の流れ

5.3 DHCPA パケットの送信

DHCPA では認証情報を含んだパケットを DHCP Class-identifier オプションとして送信することで DHCP との完全な互換性を維持しながら認証機構を実現している。DHCP の各フェーズで Class-identifier オプションを利用して DHCPA パケットを送信し認証情報の交換を行っている。

DHCPA Message Type フィールドは、サーバ/クライアント間で送受信される DHCPA パケットを識別するために利用する。DHCPA プロトコルで用いる DHCPA Message を表 3に示す。

次に DHCPA クライアントの認証処理の流れを図 6に示す。

1. クライアントは接続要求を受け付けてく

れるサーバを特定するため DHCPDISCOVER とともに DHCPA_QUERY を送信 (Broadcast) する。

2. DHCPA サーバは要求のあったクライアントに対して DHCPOFFER とともに DHCPA_OFFER を送信する。

3. クライアントは受け取った DHCPOFFER と DHCPA_OFFER からサーバを選択し DHCPREQUEST と DHCPA_REQUEST を送信 (Broadcast) する。

4. DHCPA サーバは資源の割り当てが可能なら DHCPACK を DHCPA_ACK とともに送信する。もし資源の割り当てが不可能なら DHCPNAK を DHCPA_NAK とともに送信する。

5.4 DHCPA の評価

DHCPA により移動ホストからの割り当て要求に応じ移動ホスト認証を行った後にネットワーク資源を割り当てる資源割り当て機構を実現できた。また DHCPA はサーバ、クライアントとも DHCP と完全に互換性があり、従来の DHCP 環境でもそのまま利用することが可能である。

5.4.1 DHCPA の安全性

DHCPA の認証の強度はディジタル署名で用いた RSA 暗号の強度に依存している。また DHCP オプションの制限から鍵の長さが制限されているためより安全な認証強度を求める事は困難である。現在の実装では DHCP との互換性を考慮し可能な範囲で安全性を確保している。

6 まとめ

移動ホストの実現を目指したいくつかの提案がインターネットでは行われている。移動ホストは移動した先のネットワークに接続するために IP アドレスなどのネットワーク資源を必要としている。しかしながら、現状の DHCP などは、移動ホストの認証をまったく考慮しておらず、移動ホストからの割り当て要求に従って、そのまま資源の割り当てを行っている。

こうした現状を踏まえ、本稿では移動ホスト環境におけるホスト識別のための汎用的なモデルとしてパスポートモデルを提案した。パスポートモデルは移動ホスト毎に身元を保証するための個別の PASSPORT を所有させこれによりホストの認証を行うモデルである。さらにパスポートモデルを資源割り当てプロトコルである DHCP に適用し、これを拡張した DHCPA プロトコルの設計と実装を行った。これにより移動ホストの認証を考慮した資源割り当て機構の構築を行いその有効性を検証した。

謝辞

本研究を行うにあたり貴重なアドバイスを頂いた (株) ソニーコンピュータサイエンス研究所の寺岡文男氏をはじめ WIDE プロジェクトの皆様に感謝します。

参考文献

[1] C. Perkins. Internet Draft — IP Mobility Support, May 1995.

[2] Fumio Teraoka and Mario Tokoro. Host Migration in Virtual Internet Protocol. In *Proceedings of Inet'92*, June 1992.

[3] WIDE Project. 移動ノード. In *1992* 年度 *WIDE* プロジェクト研究報告書, 1993.

[4] B. Croft and J. Gilmore. Bootstrap Protocol(BOOTP). RFC 951, September 1985.

[5] R. Droms. Dynamic Host Configuration Protocol. RFC 1531, October 1993.

[6] 村井 純 富永 明宏, 寺岡 文男. 動的ホスト設定プロトコル (DHCP) の実装の評価. In 情報処理学会マルチメディア通信と分散処理ワークショップ論文集, November 1993.

[7] WIDE Project. 移動計算機の支援. In *1993* 年度 *WIDE* プロジェクト研究報告書, 1994.

[8] R. L. Rivest, A. Shamir, and L. Adleman. A method of obtaining digital signatures and public-key cryptosystems. In *Communication of ACM, Vol21, No.2*, Feburary 1978.

[9] R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, April 1992.