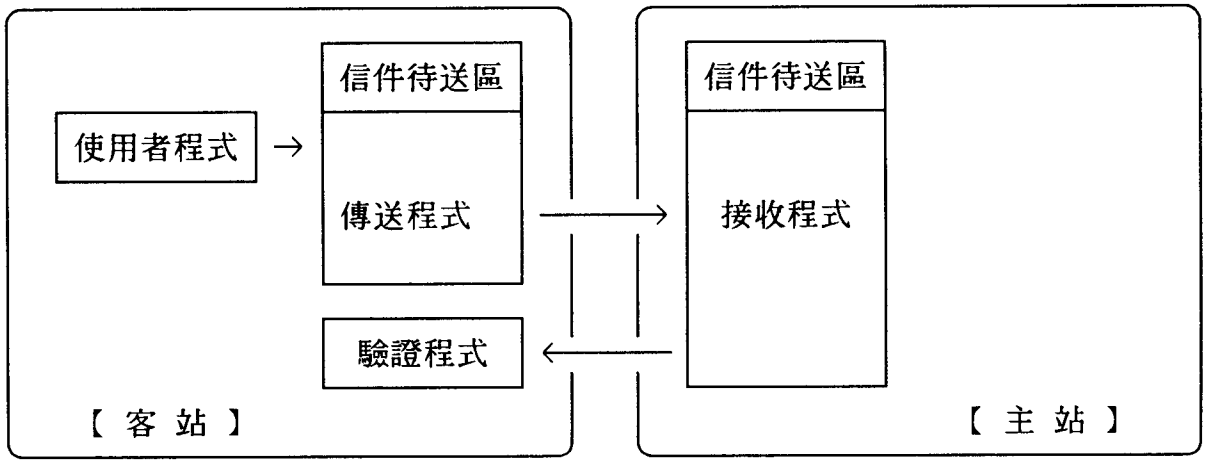
3.3 在Mail主站上的防匿方法

我們在第二章第三節曾提到有些匿名者知道如何與主站上的接收程式直接溝通，根本就不理會我們所修正的傳送程式。因此，我們在此亦將驗證協定的技術引用在Mail的防匿機制上。其運作方式如下圖：



使用者程式：任意編寫稿頭與文稿。

```
From: fake@shost.edu.tw
To: ruser@rhost.edu.tw
Subject: test

Here comes the mail body
```

傳送程式：檢查稿頭，確定各欄位如From是否齊全，若有缺則予補齊，並加蓋郵戳(Received)，再將信函傳送給主站。

```
To: ruser@rhost.edu.tw
Subject: test
Received: by shost.edu.tw
Message-Id: <datenumber@shost>
From: fake@shost.edu.tw
Date: April 15, 1994

Here comes the mail body
```

接收程式：接收客站送來的信函，並向客站上的驗證程式查詢傳送者的資料，且將查詢結果寫入郵戳(Received)中。

```
To: ruser@rhost.edu.tw
Subject: test
Received: by shost.edu.tw
Received: by rhost.edu.tw
          from fake@shost.edu.tw
Message-Id: <datenumber@shost>
From: fake@shost.edu.tw
Date: April 15, 1994


Here comes the mail body
```

圖3.4 具防匿功能的主、客端程式處理Mail的過程

由於在Mail的稿頭中並無類似於News中的Nntp-Posting-Host欄位，而且Mail中的From欄位牽涉到複雜的重寫規則，並不適合加入驗證程式所得到的傳送者資料，因此我們選定郵戳Received作爲我們填入驗證資料的欄位。

3.4 其它的防匿方法

我們在第二章第四節曾提到兩個在News上的防匿構想，但是很顯然的這些構想並不適用於Mail上。這是因爲News的投送通常是發生在某些特定的主、客站上，而Mail的傳送卻可以在任意的兩站之間產生。因此，若是改變了SMTP原有的協定，將會導致信件無法傳送。