

### 2.3 在 News 主站上的防匿方法

上一節所述的簡易防制方法，只能應用在我們管理範圍內的客站。因為對那些不在我們管理範圍內的客站而言，我們無法修正其投送程式。然而即使是在我們管理所及的客站上，我們仍然無法用修正後的投送程式來防止匿名文件的發生。因為匿名者可以利用他自己的投送程式來投送匿名文章，根本不需理會我們所修正的投送程式。因此，強化主站上接收程式的功能，就變得格外地重要。

由於驗證協定 (Identification Protocol) 在 TCP/IP 網路上已逐漸被各種作業系統採用，而且很多伺服器程式 (server programs) 已經具有和遠端驗證協定程式溝通的能力 [1]。因此，我們將利用驗證程式來加強防匿措施——當文章被投送時，主站上的接收程式將向客站上的驗證程式查詢投送者的身份，並將其記錄於文章的稿頭中。其運作方式如下圖：

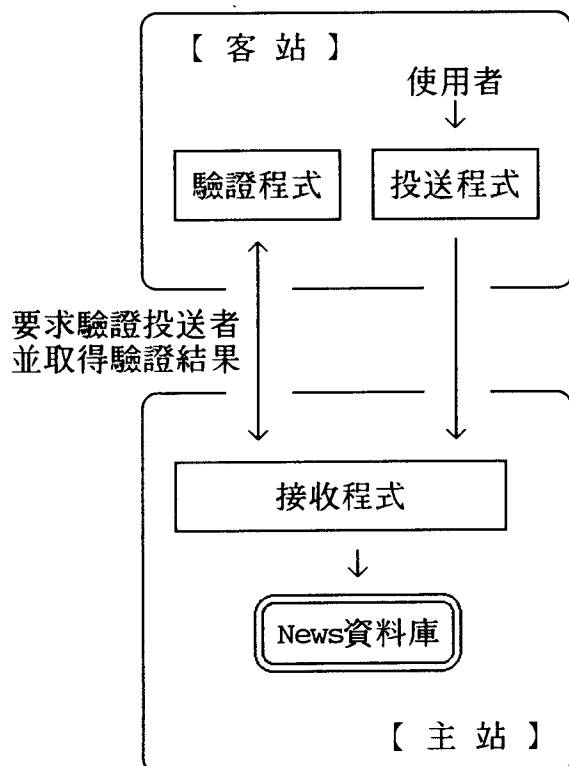


圖 2.4 NNTP 與驗證協定的運作模式

[1] 例如 tcpd—the tcp wrapper。

其運作步驟如下圖：

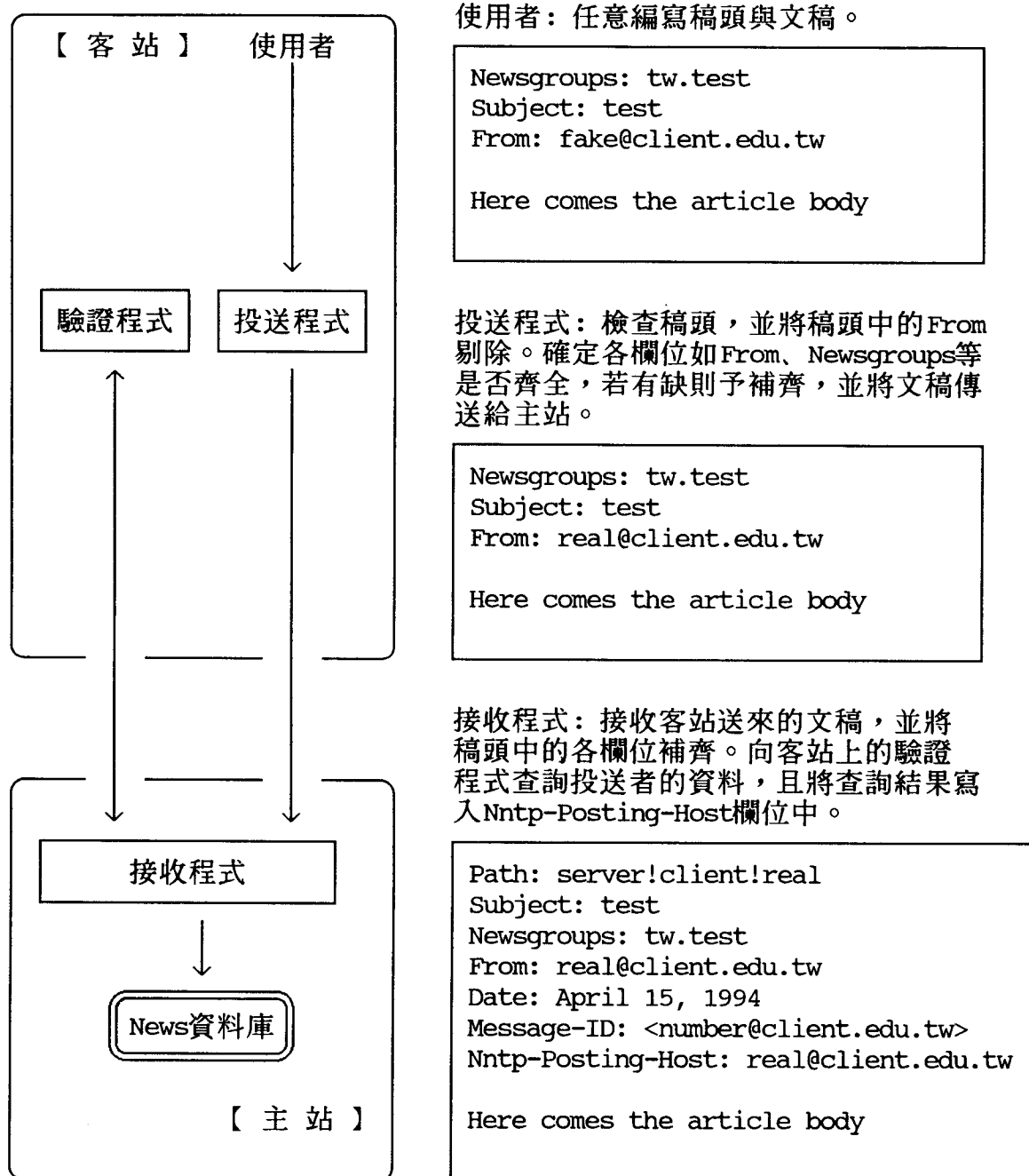


圖2.5 具防匿功能的主、客端程式處理News的過程

我們曾經評估過將投送者資料植入標準欄位From或Path的可行性，但由於From欄位的資料關係到客站隱域名稱(hidden domain)的設定與使用者別名(alias name)的使用，而Path欄位更牽涉到News主站間資料交換的效率，所以我們才選定Nntp-Posting-Host作為填入投送者

資料的欄位。雖然 Nntp-Posting-Host 並非 RFC1036 所定義的標準欄位 [1]，但是此欄位已經廣泛地被採用於 News 系統中。而且其原先所含的基本資料為客站的地址，因此將投送者的資料加於此欄位是非常合適的。

對於沒有驗證程式的客站而言，本節所提出的防匿方法顯然無法奏效，但是我們可以用管制投送的方式來加強。例如我們可以預先在主站上設定某些客站的投送是可以接受的 [2]，但要先確定這些客站都有驗證程式。或者我們不預先在主站上做任何限制投送的設定，但是當接收程式無法從客站取得投送者的資料時 [3]，該篇文稿將不被接受。

雖然圖 2.5 所示的防匿措施已經能夠避免絕大部份匿名電子文件的發生，但是我們仍要注意某些讓匿名者有機可乘的漏洞：

- 接收程式處理稿頭的方式

有些接收程式處理稿頭的方式是 "照單全收，遇缺則補。" [4] 在此情況下，匿名者只要投送一篇含有 Nntp-Posting-Host 欄位的文稿給主站，就能夠輕易地得逞。此外，Path、Date、Message-ID 等欄位所含的資料對防匿工程來說是非常重要的，因為我們可以從這些資料推算出匿名的時間與地點。因此，接收程式在處理稿頭時一定要對這些欄位嚴加管制。

- 接收程式對上游餵送源 (newsfeed) 的管制

到目前為止，我們一直都是針對投送 (posting) 模式中的各種缺點而提出各種防匿措施。對於熟悉 NNTP 協定的匿名者

---

[1] RFC1036 定義的標準欄位只有 From、Date、Newsgroups、Subject、Message-ID、Path。

[2] 例如 INN 中的設定檔 nnrp.access，NNTP 中的設定檔 nntp\_access。

[3] 發生這種情況的原因，主要是因為客站沒有驗證程式；但也可能是因為網路太過壅塞，投送者的資料無法在反應時間 (response time) 內傳回主站。當我們在使用驗證程式時，要特別注意第二種情況的發生。

[4] nntpd 即是以此種方式處理稿頭，in.nnrpd 則否。

而言，NNTP中的傳送 (transmitting) 模式提供了另一條可匿名的管道。如果我們在傳送模式下也用驗證程式來把關，那麼驗證程式將會投下大量的虛功去驗證彼端的傳送者 [1]。幸好某些 News 系統可以指定上游餵送源 [2]。如此一來，非餵送源上的使用者將無法再以傳送模式來匿名。

## 2.4 其它的防匿方法

根據前兩節的分析，我們知道任何嚴密的防匿措施都必須由主站與客站相互配合才能竟其功。準此要領，我們提出另外兩種方法：

### - 秘密協定法

我們可以讓主、客程式在 NNTP 的架構下，增加一個特別的協定，如 HELO。若是主站在接受客站的投送前，沒有收到來自客站的 HELO 訊息，則客站所投送的文章將不會被主站接受。如此一來，我們才能保證主站所接受的文稿投送，都已經被具有防匿功能的客站投送程式處理過。

### - 秘密欄位法

客站在投送文稿時，必須在稿頭中加一個虛擬欄位如 "Null:"。當主站收到含有此特殊欄位的文稿時，會將文稿收存，並將 "Null:" 剔除。反之，主站將不接受任何不含 "Null:" 欄位的文稿投送。如此我們才能保證主站所接受的文稿投送，都已經被具有防匿功能的客站投送程式處理過。

---

[1]亦即彼端的 News 系統管理者，如 news。

[2]例如 INN 可以在 hosts.nntp 中指定上游的餵送源。