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。