第三十一屆全國資訊安全會議
基於命名資料網路且具匿名性之檔案傳輸機制

黃建廷 [1] 林浩陽 [2] 黃晏林 [3] 郭信男 [4] 范俊逸 [5*]
國立中山大學資訊工程學系 [1, 2, 3, 4, 5]
yles.94214@gmail.com [1]
2998kevin@gmail.com [2]
gcobs179865@gmail.com [3]
bluedunk@gmail.com [4]
cifan@mail.cse.nsysu.edu.tw [5*]

摘　要

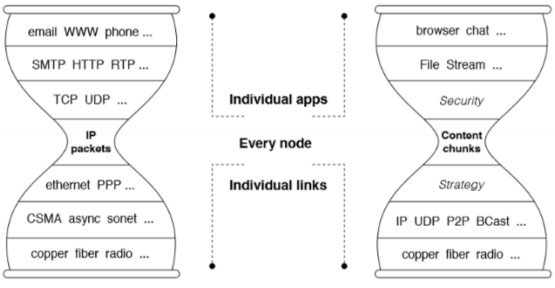
命名資料網路（Named Data Networking, NDN）是以解決現今人們對於網路的需求為目標而設計的未來網路架構。以資料中心網路（Content-Centric Networking, CCN）為基礎，延續其以資料作為中心的概念，它能解決 IP 協定在人們對於網路的需求下遭遇的問題與困難，例如：使用者在網路中的匿名性、資料傳輸的安全性、資料取得的路徑、傳輸過程中的封包暫存、IP 位址空間耗盡等問題。儘管帶著許多優勢，NDN 仍是尚未完善的網路架構，例如：公鑰取得方式及封包命名標準等皆尚未有定論，加深其實現的難度。為解決上述 IP 所遭遇的問題，建設更符合現今需求的網路環境，本次研究預計將以 NDN 的理論為主，以 CCN 的概念為輔，配合密鑰生成中心生成可信任公鑰與私鑰，實作出 NDN 網路架構，並在其以資料為中心的基礎上，預期將加入新的特性與細節，使之更為完善。

關鍵詞：命名資料網路、匿名性、數位簽章、密鑰生成中心

1. 前言

現在人們使用網路的網路層協定主要是奠基於 IP－以主機為中心的網路架構，所有資料的取得途徑都是連接至擁有該資料的主機並索取資料。在網路的發展下，伴隨著物聯網、社群網路等的出現，民眾對於網路的使用及需求已漸漸傾向於去中心化網路。現今網路架構仍存在著許多問題。舉例來說：在 IP 網路中。路由器經由封包標頭檔（IP header）上的 IP 位址欄位，決定其傳輸的方向。而傳送方與接收方在溝通過程中傳輸的封包，可被惡意使用者（e.g. Man in the middle）攔截以獲得兩端使用者的身分。因此，使用者的 IP 位址可以被任何人知道，令其身分暴露在網路中、造成匿名安全性問題；再舉一個例子：民眾經常需要藉由社群網路發布自己的資料（或者檔案）或接收其他人的資料，此時就需要先連接至離自己地理位置較遠的社群網路服務伺服器，再從伺服器連接至欲溝通的人，儘管處在同一區域網路中，甚至就在彼此身邊。

為解決上述問題，Van Jacobson 等人提出命名資料網路（Named Data Networking, NDN）[1]這個未來的網路架構，NDN 提倡以資料中心網路（Content-Centric Networking, CCN）[2]為基礎，延續其以資料作為中心的概念，將封包命名，並以包含其名稱的請求來找尋網路中對應的資料，不同於 TCP/IP 網路經由 IP 位址標示封包傳輸的目的地，換句話說，使用者要求檔案的方式是告訴網路要求檔案的名稱，而不是告訴其要傳送目的位置。在 OSI 模型中，儘管 NDN 在網路架構第四層中取代 IP 位置（圖一），卻保留 TCP/IP 網路細腰架構的優勢－讓檔案經由頂層到底層時必定會經過 IP 協定，反之亦然，使得網路架構各層的設計更加容易，也造就現今網路的順利發展。除 OSI 模型第四層之外，NDN 其上下兩層的協定分層也與 TCP/IP 網路不同：分別是 Security 和 Strategy。簡要來說，Security 層使得資訊安全安保護可以在資料本身上實行，而不像 IP 需要在兩個主機間的整個傳輸過程中進行維護，Strategy 層則讓網路層更利於與第二層同時建立多種類型的連線。



圖一 IP 與 NDN 的協定分層架構

在 NDN 中，封包被區分為興趣封包與資料封包，興趣封包可供檔案要求者（consumer）標示要求的檔案名稱，資料封包則是包含著檔案內容並讓檔案生產者（producer）傳至網路中。NDN 路由器可經特定演算法決定是否將資料封包暫存至暫存區中，而興趣封包則可經由路由器轉發至暫存著對

* 本研究接受科技部編號：109-2813-C-110-017-E 研究計畫經費補助

應資料封包的路由器，再將其對應資料封包回傳至檔案要求者。本團隊將在文獻探討中詳細說明 NDN 運作方式。

2. 研究動機與目的

了解 NDN 的架構後，以資料為中心的特性更符合今日使用者的需求，在此網路架構下，凡舉上述資料擁有者匿名安全性問題與封包傳輸路徑的例子，抑或是現今 IP 網路遭遇的其他問題，例如：IP 位址空間不足或是需要在應用層才能外加安全機制保護資料的傳輸等，都能被解決或改善。因此在本論文中，本團隊將實作並模擬 NDN 網路的運作，藉由其特性，解決現今網路遭遇的問題與困難，並嘗試讓 NDN 的架構更為完善，使其更接近人們可使用並依賴的網路架構。

在此論文中，預計在模擬 NDN 的同時，展示它與 IP 之間的明顯差異，並證明 NDN 將更符合於現今需求的網路架構。在下方將列出本論文目標與期望。

(1) 資料傳輸安全性：NDN 對封包進行的安全保護（包含完整性與不可否認性）是基於附在封包上的數位簽章，不同於 IP－需要在兩個端點的應用層上進行對封包的安全保護。
(2) 使用者的匿名性：由於在 NDN 中沒有 IP 位址的概念，使用者間不會知道互相的 IP 位址，在封包上也沒有賦予 IP 相關的任何訊息，因此除了檔案要求者與檔案生產者以外的使用者皆無法從攔截的封包中取得雙方身分資訊，只有檔案要求者可以經由驗證檔案生產者的公鑰了解其身分，因此達成在網路中溝通的兩方的匿名性。本團隊將使用 TCP Socket 去模擬 NDN，在實作上使用者只會知道其相鄰的（與之連接）路由器 IP 位址，不同於 IP 中，使用者會知道其所有溝通對象的 IP 位址。
(3) 傳輸過程中的封包暫存：路由器處理到達的封包並決定其轉發方向時，透過演算法決定是否將封包暫存至暫存區中，不同於 IP 路由器，在處理完封包的轉發後就刪除它。
(4) 取得較合適的資料路徑：因封包在路由器的暫存，路由器可轉發對於檔案的請求，並在尋找到暫存目標檔案的路由器後回傳目標檔案，將其以檔案請求的原轉發路徑傳輸至檔案要求者，相比於 IP 網路，要求者需先連接至檔案生產者（若不知道檔案生產者的 IP 位址，還需先連接至提供瀏覽器服務的伺服器），方可要求檔案。
(5) 解決 IP 位址空間不足：檔案要求者會在封包的名稱欄位上填入要求檔案的名稱，並送至網路中尋找擁有對應名稱的檔案，而其名稱欄位在本論文中配置 32 位元組的空間，相比於 IP 網路的 IP 位址不管 IPv4 抑或是 IPv6 都有位址空間耗盡問題，NDN 的封包名稱不會有空間的限制。

3. 文獻探討

此部分將說明本研究其理論架構，將包含 NDN 的架構、數位簽章與 KGC 和可信任的公鑰。

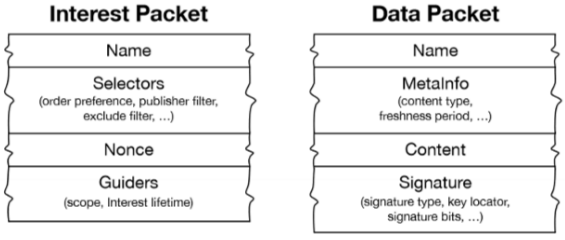
3.1 NDN 架構

命名資料網路[1,2]是一個正在發展中的未來網路架構之一，相較於現今的 IP 網路以使用者做為中心，專注在”Where”－資料在哪裡，命名資料網路是一個以資料作為中心的網路結構，專注在”What”－資料本身。命名資料網路取得資料的來源可以是任何地方，不像傳統 IP 網路取得資料只能侷限在終端設備中。

在傳統的 IP 網路中，封包的傳輸方向是由其中的 IP 位置來決定，但在命名資料網路中則是由封包中的 Name 來決定，因此這個新的網路架構的封包設計會和傳統的不一樣。命名資料網路中有兩種封包：興趣封包（Interest packet）及資料封包（Data packet），兩者有各自不同的封包欄位（圖二）。

- **興趣封包**：包含 Name（想要搜尋的資料名稱）、Selector（設定資料的範圍及其定義）、Nonce（防止封包迴圈的發生）等欄位。使用者會將想搜尋的資料名稱放入封包中傳入命名資料網路，而路由器則會經由 Name 將興趣封包轉發到檔案提供者或暫存著資料封包的路由器。
- **資料封包**：包含 Name（資料名稱）、MetaInfo（主要設定資料的有效時間）、Content（資料的內容）、Signature（數位簽章等資訊）。當興趣封包傳輸到檔案提供者或暫存著對應資料封包的路由器時，會將對應的資料封包以興趣封包傳來的原路徑以反方向傳回去到使用者，並會在封包上加入數位簽章以達成資訊安全的不可否認性及完整性。

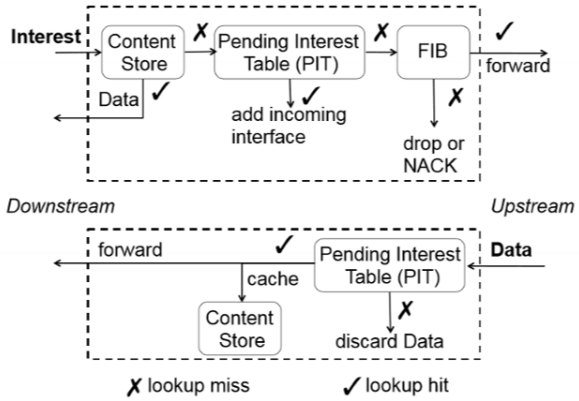
除此之外，命名資料網路的封包有兩種命名原則，第一種是直接使用與內容語意上相關或使用者可直接理解的字詞，例如：一部電影名稱或某人的名字。第二種為階層式的形式命名，可以經由不同長度的字串組成，例如：國立中山大學資訊工程學系學生程式作業的檔案可以命名為”/NSYSU/CSE/student/homework.cpp”，其命名的原則跟 URL 十分相似。



圖二 封包格式

NDN 路由器需要一個轉發策略（Forwarding Strategy Module）以及三個資料結構（Pending Interest Table, Forwarding Information Base, Content Store）來達成完整的資料傳輸。

- **Content Store (CS)**：用於暫存資料封包，提供其他使用者可以直接取得資料。是否暫存曾經轉發過的資料封包，取決於路由器本身的機制，並且盡可能的留下重複使用率較高的資料，例如：當日新聞或熱門影片。
- **Pending Interest Table (PIT)**：紀錄尚未被滿足的興趣封包及其來源。當興趣封包被路由器轉發時，會紀錄其資訊在 PIT 條目中，而當資料封包回傳至路由器時，會將資料封包回傳至興趣封包的來源，並將其資訊由 PIT 中移除。
- **Forwarding Information Base (FIB)**：用於查詢並轉發資料的潛在來源位置。命名資料網路本身可以避免迴圈，所以允許同時發送多個請求。
- **Forwarding Strategy Module (FSM)**：有一系列的封包轉發政策，在特殊情況下甚至可以直接丟棄興趣封包，例如：興趣封包被當作是 DoS 攻擊的一部分時。



圖三 路由器處理封包流程

如上方的圖三所示，當暫存器收到興趣封包時：第一步檢查 CS 中是否暫存著對應的資料封包，如果有就回傳資料封包；如果沒有，檢查此興趣封包的資訊是否列在 PIT 紀錄中，且記錄有相同 Name 的封包，如果有就只需佇列至 PIT 列表中，不用再轉發一次其封包；如果沒有相同的紀錄，則必須除了新增其資訊至 PIT 列表之外，查詢 FIB 並轉發興趣封包到資料潛在來源；若 FIB 還是找不到該封包的資料來源時，興趣封包會被丟棄。

當找到對應的興趣封包時，資料封包會被資料提供者回傳到路由器中，並會查詢 PIT 列表是否有使用者要求其資料，如果有就將資料封包繼續回傳至前一個使用者或路由器，將資料刪除自 PIT 列表，並將封包暫存至 CS 中；如果 PIT 中找不到相應的紀錄，代表可能等待的時間過長，已放棄此封包，這時路由器會丟棄這個封包。

3.2 數位簽章

訊息發佈的目的是為讓人們知道訊息，因此沒必要對訊息做加密，但是必須排除訊息被他人偽造，同時也要避免接收到假消息，因此才會有數位簽章[3, 4, 5]存在的必要。

數位簽章目的是為了要確保所收到資料封包的來源是可信的，不會是來自不明人士發送的可疑資料。在數位簽章中，訊息提供者會傳送訊息與簽章兩個文件，而訊息接收者會在收到這兩個文件後，會去證明這個簽章是否屬於傳送者的，如果證實如此的話，就可以保證訊息的來源。

在數位簽章的過程中，訊息提供者會使用私鑰來對雜湊過後的訊息作簽名，然後公布對應的公鑰，而訊息接收者會用公鑰來對簽名做驗證，並將解密的結果與訊息做比較。如果比較結果正確的話，訊息就會被保留，否則就會直接拋棄這個訊息。

可靠的加密演算法可以增加數位簽章的安全性，在良好的數位簽章下，將可以保證這個資料封包沒有被篡改(訊息完整性)，亦可以確認這個資料封包的來源(訊息確認性)，同時也保證訊息提供者曾經上傳過這個資料封包(不可否認性)，藉此來增加使用者的安全性。

3.3 KGC 與可信任公鑰

儘管有簽章來保護資料的安全性，若無法取得正確與可信任的公鑰來認證簽章，也是徒勞無功，因此需要確保自己可以取得合法來源，換言之來源正確的公鑰。而 Key Generation Center（KGC）[6, 7]就是一個取得可信任公鑰的管道，KGC 負責生成所有用戶的私鑰與公鑰並將其儲存在自己的鑰匙清單中，且會利用安全通道將私鑰傳至用戶，用戶也可以向 KGC 要求其他用戶的公鑰，以此認證簽章。此部分於研究方法中將更為詳細的說明使用者取得可信任公鑰的流程。

4. 研究方法

本團隊預計在此節說明各部份實作方式。於 4.1 中說明路由器如何處理各種封包（包含興趣封包、資料封包、測試封包等），4.2 說明數位簽章的雜湊與簽名實作方式，4.3 說明獲得可信任公鑰並認證簽章的流程。

4.1 NDN 封包架構

考量到檔案生產者可能同時擁有檔案要求者的身分，本次研究不同於 Jacobson 與其他學者提出的 NDN 封包格式[2]，將興趣封包與資料封包設定為相同的格式，但保留原格式中各欄位設計的用意與功能。以下將介紹封包各欄位的設計與用途。

(1) **Name**：紀錄資料的命名欄位，本次研究使用

類似於 URL 的格式將封包命名，並利用字元“/”將資料名稱分割成各個片段，例如：有一圖片名稱為 picture.jpeg，並且其大小大於 NDN 封包的 MSS（Maximum Segment Size），其在網路中的資料封包將被命名為 picture.jpeg/0、picture.jpeg/1 等等。需注意的是上述字元與部分命名片段的用途是標示資料在網路中傳輸時封包排序（Sequencing），因此並不包含於實際資料名稱中。

(2) **Type**：標示出封包的種類（e.g.興趣封包、資料封包）以供路由器辨認並執行對應的處理。其種類依序為興趣封包（Type = 1）、資料封包（Type = 2）、測試封包（Type = 3）、請求連線封包（Type = 4）、成功連線封包（Type = 5）、中斷連線封包（Type = 6）、以及失敗連線封包（Type = -1）。在章節 4.3 及 4.4 會詳細說明路由器處理每一種類封包的流程。

(3) **Nonce**：其為一隨機的 32 bits 值，用途為避免路由器轉發封包時遭遇封包迴圈。在後續章節會詳細說明其如何抑止封包迴圈發生。

(4) **Timestamp**：記錄產生封包的時間。路由器中記錄著興趣封包以及資料封包的生命週期，當封包到達路由器時，此欄位紀錄的時間將被與當下的時間進行對比。若路由器發現此封包存在時間超過了生命週期，會將其丟棄。

(5) **Length**：紀錄封包包含標頭檔、內容以及簽章的大小。

(6) **Content**：紀錄要傳輸的內容。其中 MSS 會被記錄在使用者端（檔案要求者、檔案生產者），資料大小若大於 MSS，將被切分成大小等於或小於 MSS 的資料片段以進行傳輸。

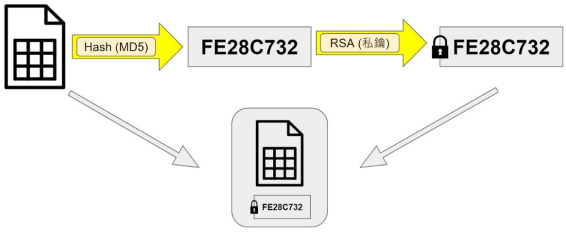
(7) **Signature**：將命名欄位（name）與資料片段（content）合併並執行簽名產生一個將命名欄位與資料片段配對在一起的簽章。若只將上述兩者其中一部分做簽章，將有封包命名欄位或內容在傳輸過程中遭受竄改的風險。

4.2 數位簽章之雜湊與簽名

數位簽章的實作分為兩個部分：雜湊和加密，而在 Jacobson 與其他學者提出的架構中[1]中，對於實踐數位簽章的演算法沒有明訂規範並認為檔案生產者可以自行決定使用的演算法，因此本次研究決定分別使用 MD5 和 RSA 實作數位簽章，其中值得注意的是儘管 MD5 已被破解且被證實存在弱點，本研究仍因實作考量而選用 MD5 來執行資料的雜湊，並在之後改進為使用現今通用的雜湊演算法，例如：SHA-256。

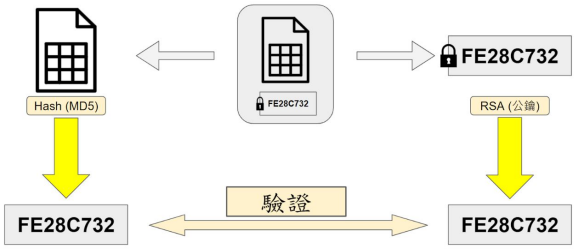
對於數位簽章的實作方法，MD5 的部分使用網路上其他作者撰寫的程式碼[8]來執行，而 RSA 的部份藉由實作大數運算來實行運算，並利用快速冪次演算法和蒙哥馬利約分來進行加速，也因為沒有使用到更多的演算法，本次研究把金鑰的長度設為 248 bits。

本團隊實作數位簽章的流程如下：每當檔案提供者要送出新的資料封包前，首先會先用 MD5[5]將資料做雜湊，MD5 會將資料轉換成長度固定為 16 Bytes 的雜湊值，之後利用檔案提供者自己的私鑰用 RSA 加密演算法[4]把雜湊值做加密，加密後的值將會作為資料的簽名，並且簽名會與資料一起被放進資料封包裡面傳送出去（圖四）。



圖四 簽名流程

當使用者接收到資料封包後，會先將資料封包拆分成資料與簽名兩部分，先用公鑰將簽名做 RSA 解密，然後將資料用 MD5 做雜湊，雜湊後的結果與 RSA 解密後的結果做驗證（圖五），如果結果相同，就可以驗證這個資料來自可靠的來源，如果結果不同，則檔案接收者會將此資料封包丟棄。



圖五 認證簽章

4.3 路由器模擬流程

本小章節將分別說明路由器之間的連線、處理興趣封包的流程、以及處理資料封包的流程，並附上對應的模擬流程指令。

(1) **路由器之間的連線**：NDN 路由器與 IP 路由器相同的擁有許多埠以和相鄰路由器或使用者連接。本章節著重在說明路由器之間的連線，與使用者的連線則將在章節 4.4 中詳細說明。

一個路由器在啟動時便會建立一以 passive open 模式建立連線的 TCP socket（接待 socket）等待連線請求，而主動與其他節點建立連線的路由器則將額外建立一 socket 並以 action

open 的模式送出連線請求。如此在分別一主動一被動的情況下建立路由器間的連線。

指令：connect IP PORT（連線至 IP 位址 IP、埠號 PORT 的路由器）

(3) **處理興趣封包流程**：使用封包的 Nonce 欄位判斷路由器是否已經接收過此封包，當收到興趣封包時，將會先比對 PIT 內存放的興趣封包，如果其中已存在名稱相同且 Nonce 相同的封包，表示已接收過相同來源的興趣封包，路由器會直接拋棄此興趣封包並且不會更新收到此封包的埠至 PIT 中。若沒有在 PIT 中找尋到相同的興趣封包紀錄，路由器會將此封包與他的來源埠紀錄在 PIT 內並轉發至相鄰路由器或使用者。

路由器隨時計算著興趣封包的存活時間。每隔固定的時間就會檢查 PIT 內是否有存放過久的興趣封包，並且把所有過期的興趣封包拋棄。

(4) **處理資料封包流程**：路由器收到資料封包時，會先將資料封包存入 CS 內，然後查看 PIT 內是否存在對應此資料封包的興趣封包，並順著興趣封包的來源埠回傳資料封包至相鄰路由器。

本研究使用 LRU 快取演算法（Least Recently Used）存放資料封包，此演算法會判斷最近使用的資料是熱門資料，且有很大的機率會再一次被使用。每當路由器收到資料封包時會將資料封包放在 CS 內的第一個欄位，並且當 CS 的內存不夠用的時候，會將存放在 CS 內最後一個資料封包丟棄，若 CS 內有資料被再次使用，路由器會將此資料在 CS 內的位置更新至 CS 內存的第一個欄位，藉此降低此資料封包被丟棄的機率。

4.4 使用者模擬流程

本小章節將依序說明使用者（包含檔案生產者、檔案要求者）連線至路由器、送出興趣封包、處理資料封包、處理興趣封包、送出資料封包、以及中斷與路由器之連線的流程，並如同章節 4.3 附上模擬軟體之對應指令（command）。上述前兩項為檔案要求者執行的流程；後兩項則為檔案生產者處理流程。

(1) **連線至路由器**：使用者經由 active open 的模式與路由器建立 TCP 連線，再傳送請求連線封包至路由器以模擬與相鄰 NDN 路由器建立連線的過程，值得注意的是，雖然以使用者的角度，自己是與路由器建立連線，實際上路由器就是包含在整個網路中的其中一個節點，使用者就如同藉由相鄰路由器與整個網際網路建立連接並溝通，接下來本團隊也會以此概念說明其他的模擬流程。

送出連線封包後，收到來自路由器的成功連線封包代表與整個網路成功建立連線，反之，收到失敗連線封包則代表著建立連線失敗。

指令：connect IP PORT（連線至 IP 位址 IP、埠號 PORT 的路由器）

(2) **送出興趣封包**：將欲獲得的資料（e.g. m）名稱依章節 4.1 所提的封包命名規則命名第一個興趣封包（e.g. m/0）並傳送至網路中，再將送出的封包名稱新增至興趣佇列中，此佇列的用途在於紀錄已送出要求但尚未被滿足的興趣封包名稱，需注意的是使用者端擁有自行決定的封包等待時間，若對應的資料封包沒有依時間內送達，此興趣名稱會從佇列中被清除並不再等待對應資料封包。

在收到對應資料封包後將下一個興趣封包（e.g. m/1）傳送至網路中，依此類推。

指令：request IDENTITY FILE（對於網路送出檔案生者 IDENTITY 的資料 FILE 的對應要求）

(3) **處理資料封包**：收到資料封包後，依封包名稱至興趣佇列中搜尋對應興趣封包名稱，搜尋到結果後此封包以檔案生產者 *IDENTITY* 之公鑰進行驗證以確保其屬於合法來源（細節將在章節 4.5 中說明），最後確認此封包是否為資料的最後一個封包以決定是否傳送下一個興趣封包至網路中。

(5) **送出資料封包**：本次研究將其分成兩種上傳方式：主動上傳資料封包至網路中、被動上傳對應資料封包至網路中。兩者皆經由資料佇列上傳資料封包至網路，換句話說資料佇列會自動依其紀錄之順序將資料封包上傳。本項流程會說明主動上傳的流程，被動上傳則將在處理興趣封包的流程中說明。

在主動上傳中，將欲上傳之資料切分為多個適合上傳至網路中的片段（大小等於或小於 MSS），依序命名並新增其名稱至資料佇列中。

軟體模擬指令：upload FILE（將資料 FILE 主動上傳至網路中）

(4) **處理興趣封包**：在被動上傳中，依收到的興趣封包名稱將對應的資料片段新增至資料佇列中，舉例來說，收到興趣封包 m/1 後，將其新增至佇列中，而佇列將由資料的第 MSS+1 個 bytes 至 2*MSS 或資料的最後一個 bytes 填入資料封包中並上傳至網路中。

(5) **中斷與路由器之連線**：將興趣佇列與資料佇列強制清空並傳送中斷連線封包之至相連路由器，隨後經由 active close 模式關閉 TCP

socket。

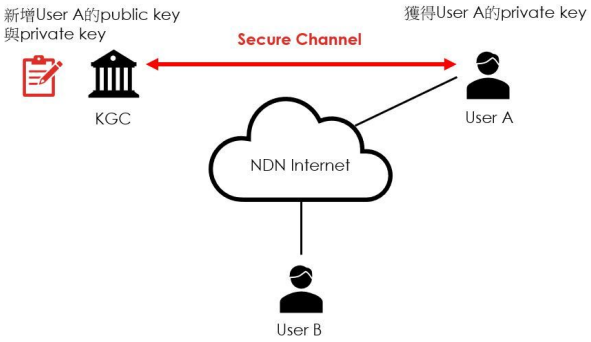
指令：disconnect（與目前連線之路由器斷開連線）

其他指令：test（送出測試封包以觀察網路狀態，節點連線狀態與轉發路徑）

4.5 公鑰取得與簽章認證

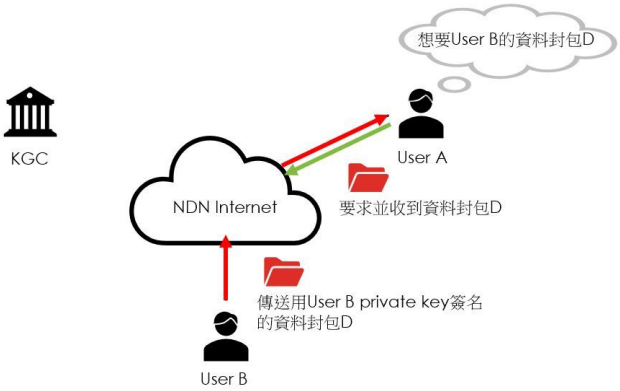
取得可信任公鑰並認證其合法來源是實作 NDN 中不可或缺的一環，少了它，儘管有簽章附在資料封包上做安全保護，檔案要求者還是有可能取得惡意使用者的公鑰，並認證惡意取相同名稱的封包而不自知。以下是配合 KGC 取得可信任公鑰並認證合法來源的流程。

(1) 每一個使用者在加入網路前都會與 KGC 建立安全通道以交換訊息－KGC 生成 User A 的公鑰與私鑰且存至自己的列表中，並將其私鑰傳給 User A，安全通道可以像是使用者本人至臨櫃註冊使用此 NDN 網路，並取得自己的私鑰（圖六）。



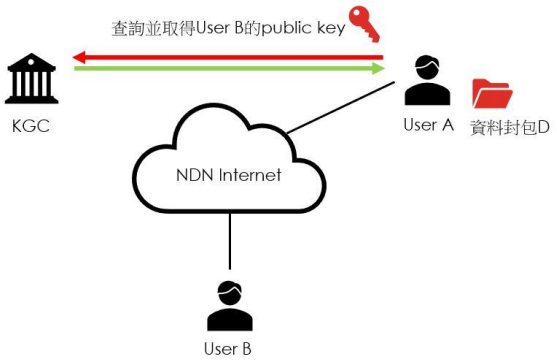
圖六 建立安全通道

(2) 假設 User A 想要 User B 的資料 D（假設資料 D 僅有一個資料封包內容的大小），並已向 NDN 網路要求且取得資料 D，如圖七，但 A 不能確定自己收到的資料是否為源自於 B，因為有可能另一位檔案生產者在刻意或無意間上傳同樣名稱但內容不同的資料 D。



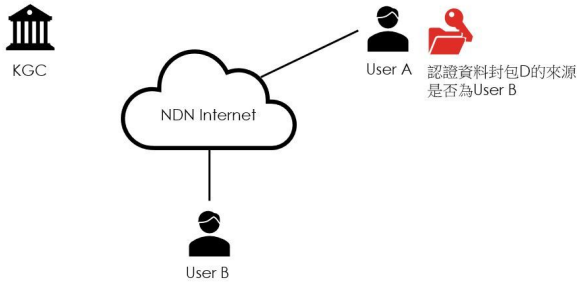
圖七 送出要求並收到封包

(3) 在 NDN 的資料封包中都附著一個數位簽章，User A 認證此資料 D 是源自於 User B 的方式是：用 B 的公鑰認證附在資料 D 上的簽章，而取得可信任公鑰的方式是：直接跟 KGC 索取公鑰，在實作上，將使用者直接連接至 KGC 的 IP 位址並要求 User B 的公鑰，如圖八。



圖八 向 KGC 取得公鑰

(4) 最後將取得的公鑰直接對收到的資料 D 做認證，確認資料 D 的來源是否為合法來源 User B，如圖九。



圖九 認證簽章

5. 研究成果

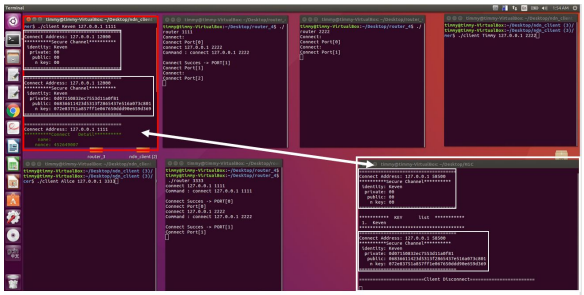
本節中，將會說明本研究實作步驟，5.1 解釋使用者如何加入至網路，5.2 至 5.4 說明檔案生產者傳檔案至網路、檔案要求者要求並取得檔案的步驟，5.5 則說明如何認證封包的合法來源。

本論文實作的網路，將以三個路由器、三個使用者以及 KGC 為範例進行展示，其連接方式如圖十，檔案要求者為紅色的框，檔案生產者為藍色的框，KGC 以及路由器皆為白色的框。

圖十 網路中路由器與使用者的連接方式

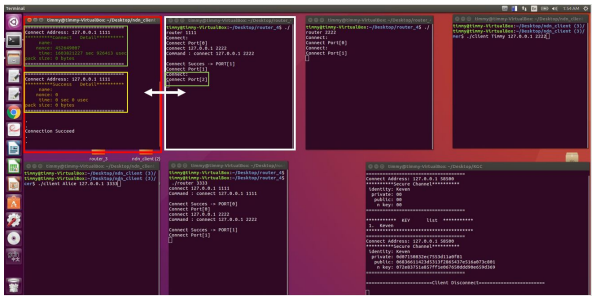
5.1 使用者加入網路

使用者與 KGC 建立安全通道交換資訊，KGC 紀錄使用者的私鑰與公鑰至自己的清單，使用者則從 KGC 取得自己的私鑰與公鑰。如圖十一中的 Consumer A 直接連接 KGC，與之溝通並取得自己的私鑰與公鑰(圖中的白色細框為包含著私鑰與公鑰的封包)，KGC 則儲存 User A 的公鑰與私鑰在自己的清單中。



圖十一 與 KGC 交換資訊並取得私鑰

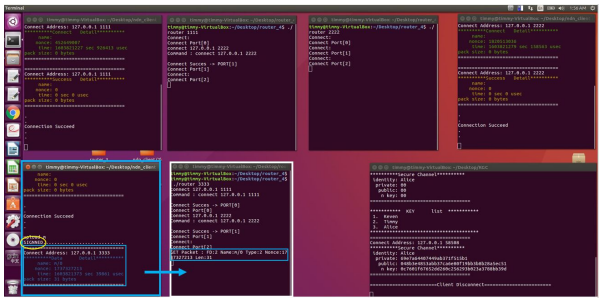
與 KGC 溝通後，使用者與最相鄰的路由器連接。如圖十二，Consumer A 與相鄰的 Router 1 連接(圖中綠色細框為要求連線的封包，黃色細框則為連線成功的封包)。



圖十二 與相鄰之路由器連接

5.2 檔案上傳

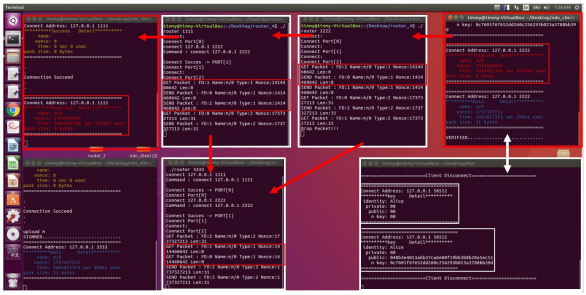
檔案生產者將要上傳的檔案與名稱合起來做雜湊並簽名、將簽章附在資料封包上、再上傳至 NDN 網路中與自己相鄰的路由器。如圖十三，Producer C 將檔案 m 做雜湊並簽名形成簽章，再將附有簽章與檔案 m 的資料封包(圖中藍色細框)傳至相鄰的 Router 3。



圖十三 將資料封包上傳至網路

5.3 檔案要求

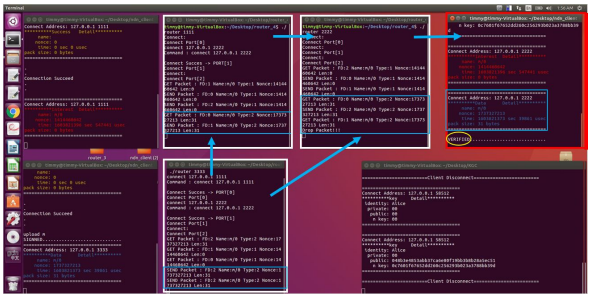
檔案要求者對相鄰的路由器送出要求檔案的興趣封包。網路中的路由器若無暫存對應的資料封包，會將興趣封包廣播至相鄰的路由器或使用者，直到暫存著對應資料封包的路由器，除此之外，若路由器收到多個相同來源且相同要求的興趣封包，只會處理第一個到達的封包，並忽視其他較晚到達的封包。如圖十四，Consumer B 送出要求 m 的興趣封包(圖中的紅色細框)，並以紅色的箭頭的方向將封包廣播，直到暫存著內容為 m 的資料封包的 Router 3，同時，連接至 KGC 並索取 Producer C 的公鑰，如白色箭頭所示，以用來認證未來收到的資料封包的來源。



圖十四 檔案要求者送出興趣封包

5.4 檔案轉發

暫存著對應資料封包(圖中的藍色細框)的路由器將其依原路徑回傳至檔案要求者。如圖十五，Router 3 暫存著內容為檔案 m 的資料封包，因此將其依藍色箭頭的方向，以原路徑回傳至 Consumer B。



圖十五 路由器轉發資料封包

5.5 驗證檔案合法來源

檔案要求者向 KGC 索取檔案生產者的公鑰，以此來認證封包中的簽章確認封包的來源。如圖十五，Consumer B 利用已取得的公鑰認證資料封包的來源。

5.6 研究結果

本團隊展示出 NDN 的精神與符合今日對網路

的使用需求的特點，包含下列五項：

(1) **在封包上就完成傳輸的安全性**：將資料的名稱與內容合併後再做簽章以保護檔案生產者的真實性（Authentication）與資料內容的完整性（Integrity），經由此確保封包的內容無法被隨意竄改，也無法使用相同名稱但不同內容的封包進行仿造。

(2) **以維護使用者匿名性的方式上傳或取得封包**：在本次研究上，就算檔案生產者與檔案要求者以外的使用者從兩者溝通中攔截封包也無法竊取其身分資訊，經由 NDN 封包中。儘管本次研究模擬的 NDN 是基於 TCP/IP 的傳輸協定，攔截者也只能從 IP 封包中得知傳輸路線中上一個路由器的 IP 位址，藉此達成溝通雙方在網路中的匿名性。

(3) **路由器的封包暫存**：路由器將到達的資料封包暫存於 CS。不同於 IP 路由器在轉發完封包後就將其丟棄。

(4) **較合適的檔案取得路徑**：因路由器對於封包的暫存，對於已經被要求過的封包，使用者可以更快速且用更合理的路徑的取得它。

(5) **封包命名不會有空間不足及耗盡問題**：在本次研究中，使用 32bytes 的空間去儲存封包的名稱，若未來仍遇上欄位空間不足的問題，可仿照 TCP 封包中的 Option 欄位定義額外的命名空間，使其擁有高可擴展性（Scalability）。因此相較於 IPv4 和 IPv6，幾乎不可能遇到封命名空間不足的問題。

在實作與討論的同時，本團隊在實作中也發現 NDN 架構設計上的缺漏，舉例來說：Named Data Networking 中所提的路由器處理資料封包順序（PIT、CS）會導致檔案生產者想主動上傳檔案至網路時，資料封包因在 PIT 中沒有對應的興趣封包紀錄而遭到刪除，因此將資料封包的處理順序 PIT 以及 CS 對調，讓使用者可以隨意上傳資料封包至網路中。

6. 結論

在這次的研究中，本團隊使用 Unix Socket 來模擬命名資料網路的架構，在這架構中，路由器的角色很類似生活中的伺服器，負責服務網路上的使用者，而使用者的角色類似客戶端，向路由器上傳資料或者請求資料。

在傳輸資料的過程中，為避免使用者收到仿造的同名資料，本團隊實作數位簽章，利用 MD5 和 RSA 來執行數位簽章，同時也製作密鑰生成中心（Key Generation Center）給予使用者可信任的公鑰。藉由數位簽章與金鑰生成中心來維護命名資料網路中使用者的資料傳輸安全性。

在這個科技發展快速的時代，使用 IP 所衍生的問題逐漸地顯現出來，雖然命名資料網路仍在研發中，有許多內容及細節尚未定型。但是相信在未來命名資料網路的發展下，其越來越完善的架構能完整的展現其特色，除了給人們快速搜尋資料的能力，也為物聯網等將會普及的科技發展帶來很大的幫助。

參考文獻

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking Named Content,” Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, 2009.

[2] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, kc claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang and Beichuan Zhang, “Named Data Networking”, ACM SIGCOMM Computer Communication Review, Volume 44, Number 3, July 2014.

[3] Whitfield Diffie, Martin E. Hellman, “New Directions in Cryptography”, IEEE Transaction on Information Theory, IT-22(6):644-654, Nov. 1976.

[4] Rivest, R., Shamir, A., and Adleman, L. “A method for obtaining digital signatures and public-key cryptosystems”, Comm. ACM 21, 2(Feb. 1978), 120-126.

[5] Rivest R., “The MD5 message-digest algorithm”, IETF Network Working Group, RFC 1321, Apr. 1992.

[6] S. S. AI-Riyami and K. G. Paterson. “Certificateless public key cryptography”, In Proc. ASIACRYPT 2003, pages 452-473. Springer-Verlag, 2003. LNCS 2894.

[7] Pei-Shan Yang, “File Transfer Protocol with Producer Anonymity for Named Data Networking”, 2020.

[8] https://www.itdaan.com/tw/959f63517fa2b8404a741d192982c8c2