108年度臺東區網中心暑期研習課程

基于軟體定義以及雲霧協同技術構建下一代大規模網路的智慧合法監聽及分析系統

賈文康

2019.8.14

大綱

- 合法監聽系統介紹
- 合法監聽技術與架構
- 軟體定義網路
- 智慧合法監聽內容分析系統
- 雲端計算、霧計算、雲霧協同計算
- 監聽執行點選擇與路由設計
- 多監聽業務執行點與多監聽中心聯合部署策略
- 監聽回傳路由與流量聯合調度技術
- 基於雲霧協同計算的分散式智慧DPI加速器部署及資源優化
- 結論與建議

為何須要合法監聽系統(1/2)

- 近年來，網路犯罪事件頻傳，包括網路詐騙、洩密、不當資訊、妨礙名譽、侵犯版權、散佈病毒、駭客入侵、癱瘓攻擊等網路犯罪手法與日俱增，已嚴重影響社會治安穩定與正常發展，另一方面，現代戰爭的模式已逐漸趨向資訊化及電子化，因此資訊戰或稱為網路戰等相關問題開始廣受關注。電話**合法監聽（LI；Lawful Interception）**是警檢調國安機構，監控嫌疑犯或處理犯罪活動，行之有年的主要手段之一。
- 合法監聽是一種根據法律授權(e.g, 美國的通信協助執行法(CALEA)、中華民國的通信保障及監察法、中國大陸的網絡安全法...)，在沒有完善法源依據以前，這種行為被稱為竊聽(Wiretapping)，自從通信網路一出現，這種行為就存在了。在現代司法體系中，實現合法監聽，尤其是對內容的實時訪問，可能需要專門的手續，並得到來自具有相關權限的部門的適當的許可，由執法部門、監管部門或行政部門及情報部門按照當地法律以分析或取證為目的，對電信通信的數據進行監聽攔截獲取。這些數據一般而言主要包含網絡管理信息，在少數情況下，還包含通信的內容。
- 合法監聽系統是指在通信和電話網絡中的一種設施，它允許擁有法庭指令或其他合法授權的執法機構，選擇性地竊聽個人用戶。大多數國家都要求那些獲得合法執照的電信運營商，在他們的網絡上提供合法的監聽節點和網路設備用於通信監聽。

為何須要合法監聽系統(2/2)

- 2001年911事件發生後，美國聯邦調查局(FBI) 和美國司法部於2003年7月向聯邦通訊委員會(FCC，Federal Communications Commission)聯合遞交了一份要求修改電話監聽法規的提案。該提案中指稱未來寬頻數據網路勢必將取代現有的窄頻電話網路，Internet已經成為國家安全的一大威脅，這一發展趨勢為恐怖份子、間諜和各種犯罪份子提供了更「安全」的連繫管道，為了彌補這個漏洞，具體建議今後任何一家一二類電信運營商，都必須按規定在其網路系統中安裝網路資訊監聽裝置，以配合警方對可疑的網路用戶進行電子監察，防止罪犯利用Internet逃避合法的法律監視。
- 以網際網路自由主義的觀點出發，認為政府的介入會侵害網路隱私，嚴重影響網際網路開放自主的傳統和特性，用戶的電子郵件、網頁瀏覽和線上聊天等任何活動也都可能連帶受到監控。
- 另一派的觀點，則是認為既然網際網路有提供語音電信服務之事實，即可以視為傳統電話所延伸的一種新興媒介，故應該納入既有電話監聽法規的規範，也不致損害傳統電話公司的利益。
- 雖然仍有侵害人權與隱私的疑慮，某些先進國家的情治單位，甚至廣泛地面向一般大眾的通聯記錄及通信內容進行不合法的“無差別”監聽與分析(譬如美國國家安全局的棱鏡計畫)。這種類型的監聽系統所攔截的海量資料，已經超越以人工進行分析處理的可能性，大規模監聽自動分析系統框架，在先進國家科研單位檯面下，早已經進入以人工智慧、大資料分析的新興科技戰場。

傳統電信業務的合法監聽技術

- 在傳統的公用交換電話網絡 (PSTN)、無線和有線系統中，合法監聽一般是通過直接訪問那些正在承載被監聽對象的通話的機器設備或數字交換機來實現的，無論是否是公網甚或私用網路。
- 傳統有線電話(PSTN)得以經由在電信機房的交換裝置掛設監控設備，截聽某些通訊內容的前提，在於傳統電信技術係以分層傳輸，集中交換的設計特性實現，使用者以用戶終端裝置(電話機)，經由唯一的呼叫識別方式(電話號碼)，透過唯一的電路(用戶迴路)接取，在電話連接建立(撥號接通)的過程，會有唯一路徑被指派，因為計費的需要，所有撥打行為都會留下完整的通聯記錄(CDR；Call detail Record)，並據以向使用者收費；因此只要得知使用者E.164國際電信交換碼(電話號碼)，即可了解應透過何台終端設備予以截聽，並由電信公司的施工記錄中輕易得知使用者所在的實際位置，即使漏失內容的截聽，至少還留下完整的通聯記錄可供事後調閱。。
- 行動電話(PLMN)因為有無線電波在空氣中自由傳播的行為，所以除了與上述傳統有線電話相仿，在電信機房內基地台後方進行監聽的方式外，也多了一種可直接在靠近使用者一定範圍內，以特殊無線電波截收裝置，擷取談話內容，再加以解譯的方式，第一代的AMPS系統甚至於不需要任何解碼程序，只要對準正確頻道直接收聽即可。第二代(GSM/DCS/CDMA)以後的行動電話系統都已經加上一定程度的加密編碼傳送機制，安全性已較第一代的AMPS系統提高。此外，基地台用戶定位功能也非常重要。
- 由於其集中性質，在傳統電信網路中實現合法監聽，實踐容易但成本高昂。在過去的二十年中，隨著分封交換網路及網際網路的引入，新興網路應用推陳出新、網路流量持續暴增，從根本上改變了合法監聽的實現方式(語音導向→數據導向)。以網路電話(VoIP)的監聽為例，係透過IP封包傳遞為基礎，相較於傳統電信則更有難度，今日在Internet運作合法監聽系統已經成為一項艱難的工作。

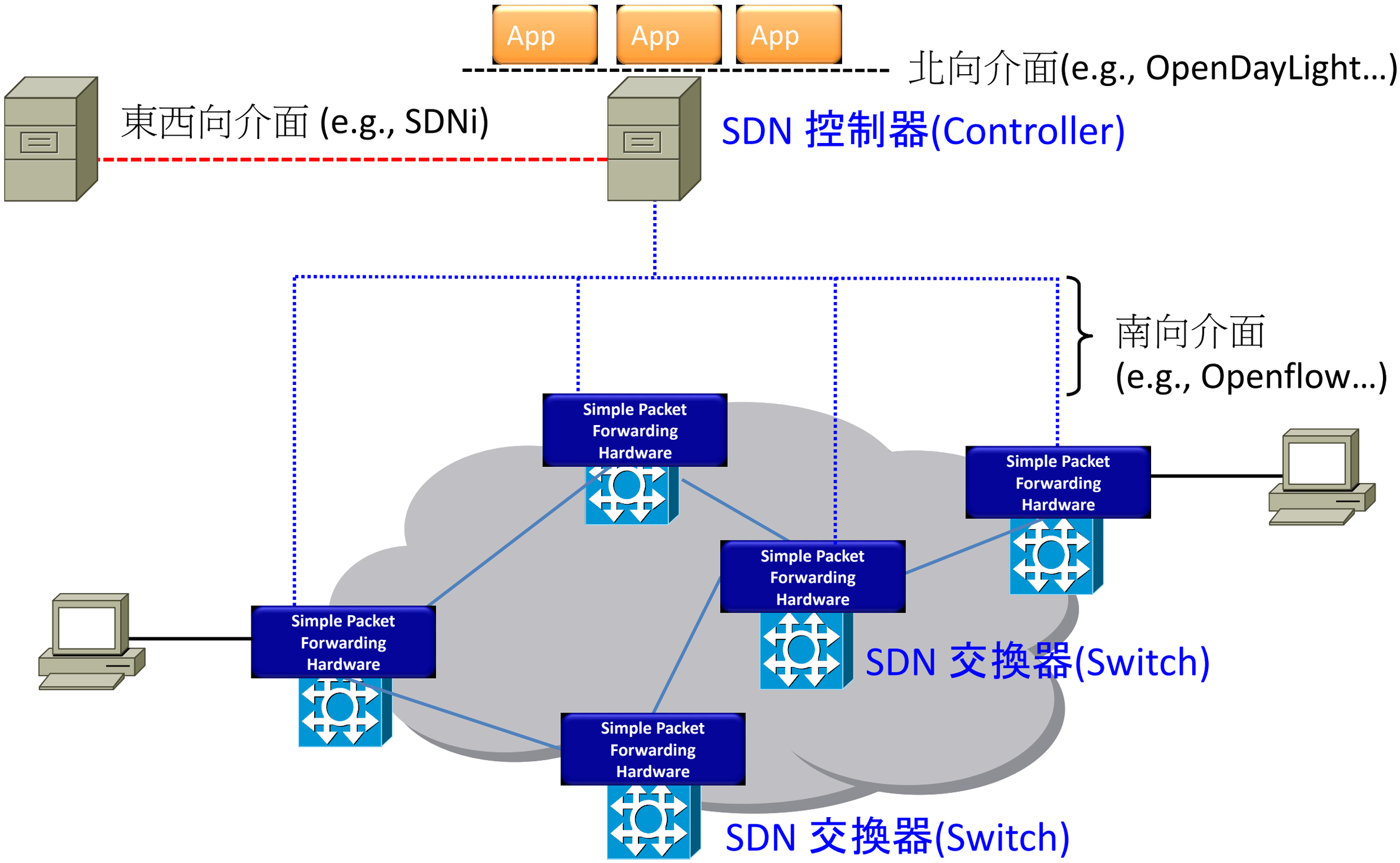
合法監聽的系統架構

- 司法管轄機構試圖定義一個系統性的和可擴展的監聽架構，與網絡運營商相互協作，這個架構不僅僅適用於傳統的有線和無線語音呼叫，還包括基於IP的服務，該架構要求通過幾個步驟來實現：
  - 採集(Collection)，與被監聽目標相關的「呼叫」數據和內容被從網絡上抽取出來。
  - 轉換(Mediation)，數據被格式化，以符合特定的標準。
  - 回傳(Transmission)，將數據和內容轉發到執法機構(LEA)。
  - 分析(Analysis)，執法機構以人力或自動化軟體對被攔截的數據和內容進行分析。
- 為了確保系統性地進行攔截監聽，同時也降低攔截監聽的解決方案的成本，全球的行業組織和政府機構都嘗試了將合法監聽背後的技術流程進行標準化(IETF、3GPP、ITU-T...)。其中歐洲電信標準化協會(ETSI)已經成為世界性的合法監聽標準的主要推動者。
- 監聽攔截系統採集兩大類數據：
  - 呼叫數據在歐洲被稱為與攔截有關的信息(Intercept Related Information(IRI))，而在美國則被稱為呼叫紀錄或數據(CDR/Call Data)包含關於目標通信的信息，包括語音呼叫的被叫方（例如被叫號碼）、呼叫來源（主叫方的電話號碼），呼叫時間、呼叫時長等。
  - 通話內容就是承載該呼叫的數據流，合法監聽的管理功能也被包含在該架構中，它涵蓋了跨運營商攔截通話的建立和釋放、目標識別等。
- 為了防止調查被泄露，司法管轄機構要求要求電信服務供應商安裝一個合法攔截網關(Leagal Interception Gateway，簡稱LIG)，以及合法攔截節點 (Legal Interception Nodes，LIN)。合法監聽系統可能被設計為以一種隱藏的方式進行，與電信運營商無關。呼叫數據和內容通常是由網絡運營商，通過一條數據專線(LL)或基於IP的虛擬專用網(VPN)，以加密的格式發送回執法機構(LEA)的。

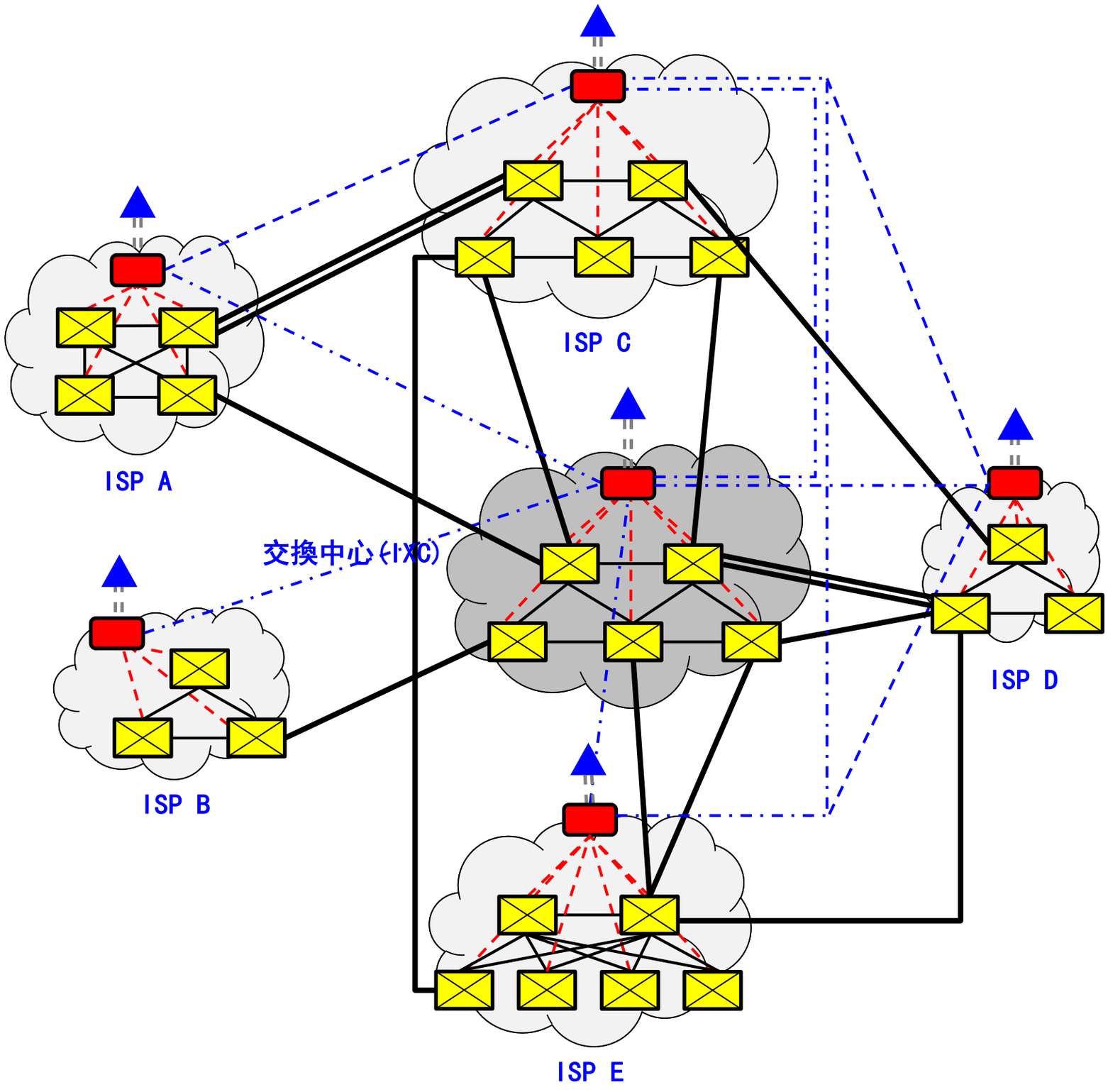
以軟體定義網路(SDN)為基礎的監聽系統

- 隨著軟體定義網路(SDN)技術的推出，提出以邏輯集中的、開放的、可程式設計的控制平面，透過統一的、標準化的介面與資料平面交互，使得控制平面和資料平面解耦並得以獨立演進，並讓網路管理人員可以掌握全域網路視圖，對網路進行靈活配置和管理，降低整體運營成本，並且方便新協定的開放和部署。
- 雖然目前SDN主要市場仍聚焦於區域網路，但現有廣域互聯網架構在不久的將來，也有機會在SDN控制器間通信(SDNi)和軟體定義廣域網路(SD-WAN)等技術的成熟和加持下，逐步移轉到以SDN技術的層面上發展。
- 下圖中呈現出這種以SDNi(Inter SDN Controller Communication)技術連接多個SDN區域網，組成以軟體定義為基礎的大規模廣域互聯網範例，呈現下一代基於SDN組網技術融合的Internet互聯互通狀態。SDN技術預期將大幅改變現有互聯網監聽基礎設施的運作架構，獲得最佳佈署彈性(Flexibility)、高擴展性(Scalability)、高可靠性(Reliability)、高可用性(Availability)、可維護性(Maintainability)、可服務性(Serviceability)等優勢。

軟體定義網路(SDN; Software-defined Network)



以SDNi 技術連接SDN 區域網形成以軟體定義為基礎的大規模廣域網

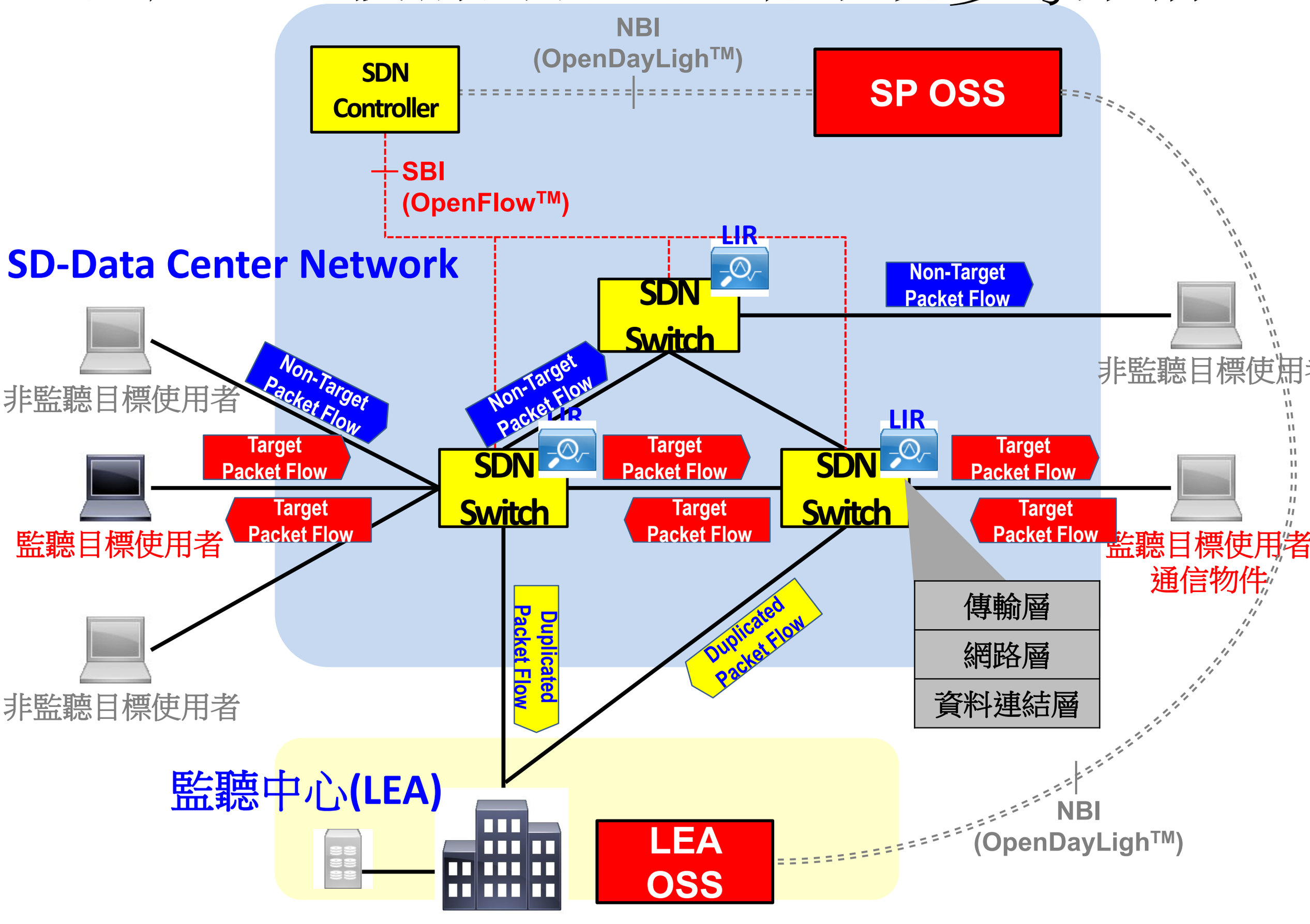


跨控制器介面(SDNi)
南向控制面介面(SBI)
北向控制面介面(NBI)
用戶資料連結
SDN控制器(Controller)
SDN交換器(Switch)
運營支撐系統(OSS)

基於SDN技術的合法監聽系統

- 一旦法律程式完備，監聽主管機關透過SDN控制器的北向介面(亦稱為SDN API)發佈並控管欲監控的範圍，運營商可透過SDN的南向介面下令給實際維運網路設備(SDN交換器)進行分散式流量攔截複製，即透過遠端遙控方式對相應預設條件要求，將特定受到監聽目標使用者的流量鏡射(Mirror)到特定埠，為保留原始資料連結層或IP層包頭，再進一步透過穿隧技術(Tunneling)打包後將流量轉發到監聽中心(LEA)執行監聽。
- 以SDN為基礎的合法監聽系統無須再進入運營商機房佈署專用的、額外的監聽設施，不再受限於固定的監聽攔截執行節點；甚至監聽執行點無須設置在運營商內網，佈署在相鄰運營商關鍵路徑上執行監聽即可，以避免驚動監聽目標或卸載運營商的流量。
- 一旦受監聽的流量過大，有可能對運營商網路造成擁塞瓶頸，侵害運營商與消費者的權益；亦或對監聽專線造成擁塞，治安單位漏失重要監聽資訊，影響到破案的契機。面對緊急網路攻擊情境，監管單位不再只是被動搜集犯罪證據，基於上述框架，監管單位可以主動下達對攻擊發起源頭執行網路阻斷命令，從根本上斷絕網路恐攻於境外。

基於SDN 技術的合法監聽系統參考架構



基於SDN+雲霧協同技術的合法監聽+分析一體化系統(1/3)

- 傳統資訊安全保護模式隨著“大數據(Big Data)”分析技術的出現，對於潛在的資料安全威脅可以通過大資料更加主動通過檢測而發現。通過掃描攔截到的的大量用戶往來數據，對其內容進行資料分析和安全分析，發現潛在的危險隱患，提前識別威脅。
- 目前許多種新的資訊技術可滿足上述在IP網路中提供強化通信監察的功能，其中“深度封包檢測(Deep Packet Inspection；DPI)”是一種先進的包過濾方法，它在開放系統互相連線(OSI)參考模型的應用層中起關鍵作用。使用DPI技術可以發現、識別、分類、重新路由或阻止具有特殊資料或代碼有效載荷的資料包，相對於SDN網路自帶的“淺度封包檢測(Shallow Packet Inspection；SPI)”只能檢測L4層以下的資料包表頭，後者難以發現這些隱藏在載荷內容中的威脅；在攻擊發生之前，DPI可提前發現潛在的威脅，作出預測並示警，從而對可能發生的攻擊作出提前判斷並在攻擊發生之前建立防禦手段。
- 傳統上監聽系統以人工監聽後進行後分析處理，為增加監聽系統即時分析威脅的性能，FBI早已在電話網絡構建語音自動分析引擎，以人工智慧軟體自動分析截聽的語音通話流中預設的敏感字眼，或以敏感字眼作為啟動監聽的關鍵字。

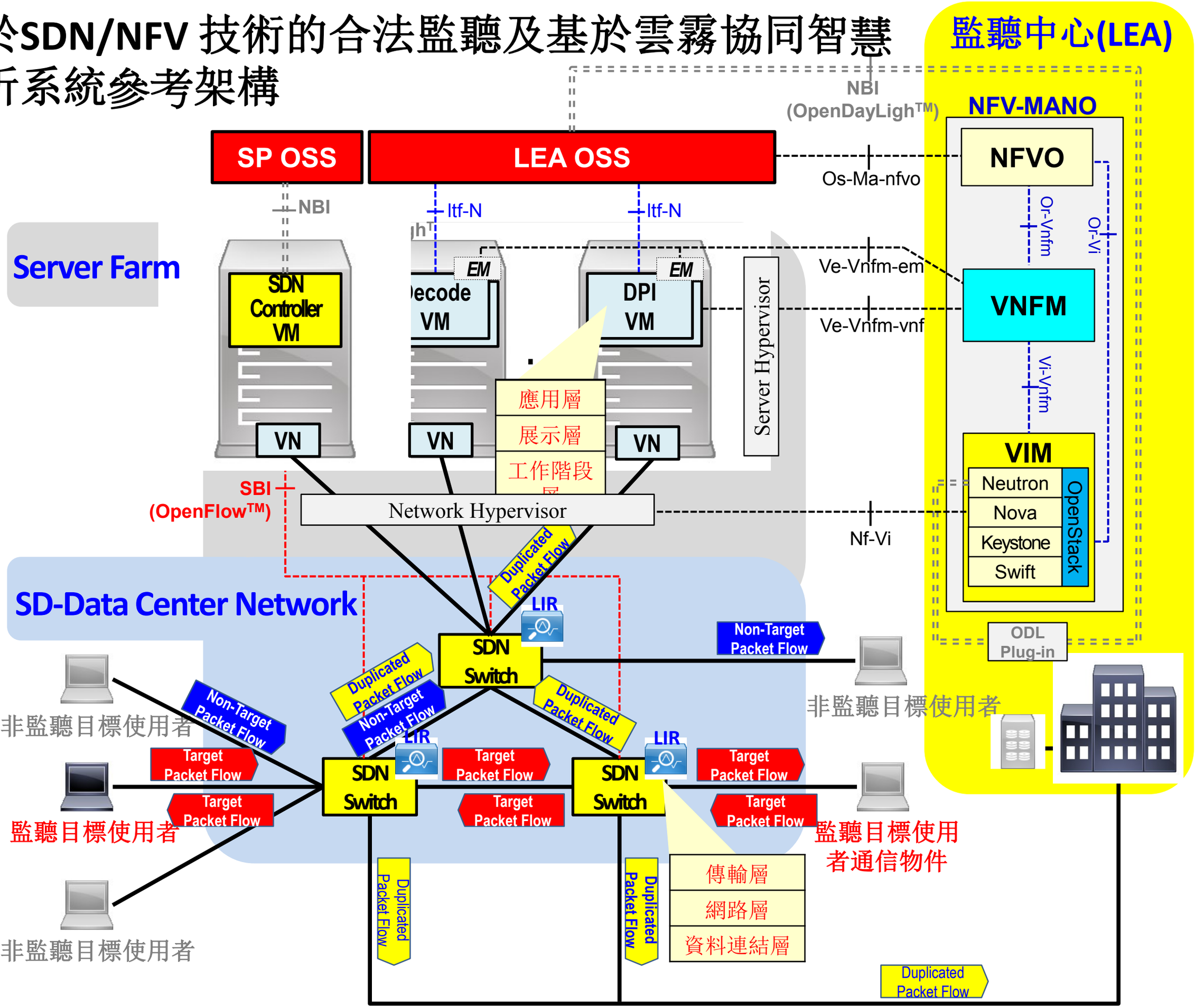
基於SDN+雲霧協同技術的合法監聽+分析一體化系統(2/3)

- 隨著人工智慧相關技術的發展，電腦被賦予理解、預測、環境適應等智慧，進而驅動商業創新，並為各行各業帶來巨大的商業價值。DPI技術也發展出結合“機器學習(Machine Learning)”等人工智慧進階分析能力。原則上，合法監聽的DPI應用情境僅需要進行較簡化的訓練計算，與主流應用需要用到大量計算以應付訓練與複雜推論計算的任務不相同；即便如此，其推論工作所需要的計算量也相當驚人。
- 為解決分析監聽內容的大量計算需求，大型高效能計算系統，如超級電腦或平行計算與分散式運算系統常被開發與建設於特定場域(通常是資料機房)，以期有效管理與使用大量的計算資源，來大幅縮短對大量資料進行計算所需時間。
- 因應“雲端計算(Cloud Computing)”和“虛擬化(Virtualization)”技術的推動，可提供每秒10萬億次以上的強大運算能力，DPI分析程式可以化身為虛擬機器(VM)型態，借助網路功能虛擬化技術，透過高速互聯網接入“雲端資料中心(Cloud Datacenter)”，按需進行分析運算，並允許管理人員按需調整處理容量、記憶體空間、存儲容量、網路頻寬與其它規格，使得計算環境可以獲得極大的彈性與擴充力。即使伺服器位於異地資料中心，管理人員也可調整多個伺服器的網路架構，這是實體資料中心無法實現的目標。

基於SDN+雲霧協同技術的合法監聽+分析一體化系統(3/3)

- 構建滿足上述DPI即時使用分析任務需求的高效能計算系統，成本非常高昂，但是其性能還難以被當前的市場接受。“邊緣計算(Edge Computing)”或稱“霧運算(Fog Computing)”是近年來新提出的概念，兩者都是一種分散式運算的架構，可視為雲端計算概念的延伸，它將原本雲端計算中完全由中心節點處理大型應用服務，包括應用程式、資料等加以分解，切割成更小更容易管理的切片，由網路中心節點，分散到邏輯網路上的低成本邊緣運算裝置(或是一種小型資料中心)去處理。
- 考慮海量的資料上傳雲端執行，再回饋到終端，不僅浪費網路傳輸、存儲等資源，還影響資料處理效率；邊緣運算裝置融合網路、計算、存儲、應用核心能力的開放平臺，就近提供邊緣智慧服務，或進行分散式網路封包傳輸通信；引進邊緣節點後，由於這些節點更接近使用者終端裝置及資料來源頭，可以加快資料的訪問處理與傳送速度，減少時延。
- 邊緣計算體系中，還需要與雲計算互補協同，雲計算聚焦於非即時、長週期、策略面的資料分析，能夠在業務決策面發揮重大功能；反之，邊緣計算聚焦即時、短週期、技術面的資料分析；雲霧兩方結合成的“雲霧協同計算(Cloud-Fog Coordinated Computing)”創建行業數位化轉型：雲計算通過大資料分析優化輸出的業務規則也可以下發到邊緣側，邊緣終端裝置基於新的業務規則進行業務執行的進一步優化處理。
- 以雲霧協同計算為基礎的DPI功能，運用在智慧型監聽架構體系中，監聽前建置的攔截規則機制、監聽中主動預警與緊急應變，以及監聽後復原追蹤識別偵查等傳統資訊安全保護模式的“保護-檢測-回應-恢復(PDRR)”程序。

基於SDN/NFV 技術的合法監聽及基於雲霧協同智慧分析系統參考架構



NFV-MANO參考架構

- ETSI提出的NFV-MANO(NFV Management and Orchestration)開放架構為分層模組化設計，階層之間的通信和介面採用產業標準協定，以確保模組間的互通性，使得此平臺具有開放和模組化的性質。NFV-MANO分層管理三大核心系統：
  - **基礎設施層(NFV Infrastructure；NFVI)**將實體計算/儲存/網路等資源通過虛擬化轉換為一個基礎設施資源池，以提供上層應用程式運行的虛擬化平臺。
  - **虛擬網路功能層(Virtual Network Functions；VNF)**即監聽核心網路功能，只是每個原本實體化網路元件都被映射為一個虛擬網路元件，由NFVI承載，並提供所需的虛擬化計算資源，大多數已有DPI網路元件都可直接在VM上運行。
  - **營運支援管理層(OSS)**提供監聽中心管理層協作能力，並為虛擬化及商業/服務模式進行必要的修改和調整，以應付更多樣化的監聽與分析業務需求，如網路切換、加值服務鏈等。

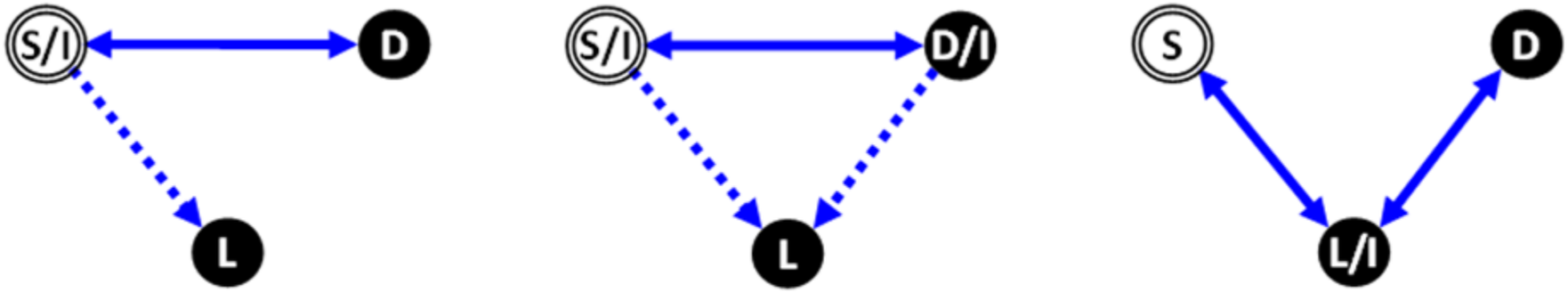
- 以OSI七層通信模型來劃分，與SDN的搭配大致以第四層(傳輸層)為界；**在OSI第四層以下適合由監聽執行點(IEP)的SDN交換器進行處理，**包括流量檢測、擴展包頭浮動欄位解析、流量分類與過濾、相關流量歸類、回傳流量隧道協議封裝等各類初級SPI處理的工作；**在OSI第四層以上，適合由沿路的邊緣運算裝置(SDN交換器)進行處理，**包括私有協議流量識別與鑒別、流量標注(包指紋)、IP地址定位、移動IP位址關聯、資料清洗或削減冗餘數據、資料轉換、資料規約、文本內容關鍵字過濾、加密內容強制解密、各類特徵提取(包含文本流關鍵字比對標注、語音流文本化、圖像向量化、視頻流特徵標注)等DPI分析的任務子集；
- 另一種部署在**“後臺”**的**“雲端伺服器”**，通常位於監聽中心內部，用以連結控制前臺終端系統，並適時分析搜集到的初級資料，進行進一步的分析彙整，並依據相應的分析結果，即時生成新的政策，並依據這些政策的層級，分別以SDN的方式部署到SDN交換器、或以NFV的方式部署到前臺霧節點的計算單元。

監聽執行點選擇與三點間路由理論

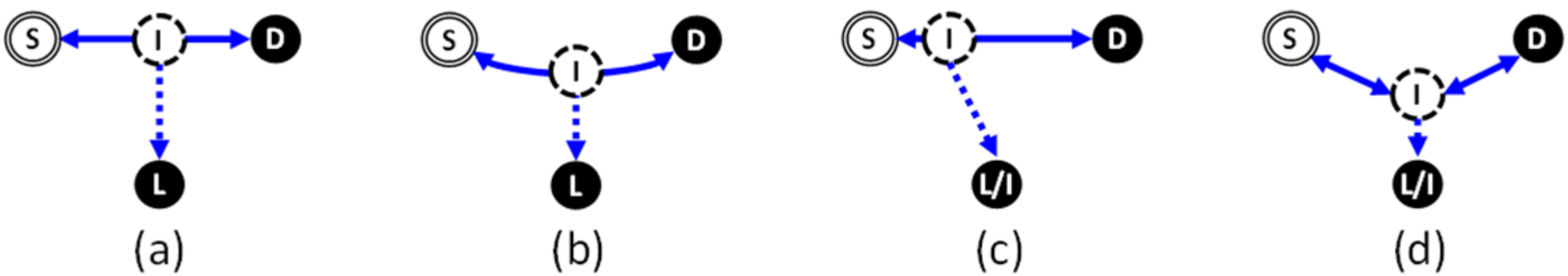
- 合法監聽執行點選擇問題(IEP Placement Problem)，也稱為監聽執行點部署問題或安置問題，以及其衍生出來的來源-目的-監聽中心“三點間最短路徑(Fermat-Point Routing)”這類三點間路由優化問題
- 監聽執行點的選定目標，必須極大化避免原始被監聽目標流量和監聽複製回傳流量，在相同鏈路上重複傳輸兩次的網路次優化問題(Sub-Optimal)。
- 監聽執行點選擇與三點間最短路徑優化演算法本質上可規約為同一個問題，一旦決定監聽執行點的位置，在來源S-目的D-監聽中心L三點間即可由第四點—監聽執行點I會面，在滿足S-I、D-I、以及L-I三條路徑同時最短的限制條件下，可以回答三點間最短路由求解問題，以滿足監聽系統需求。
- 此外，這類安置問題也非常關心監聽執行點的生成的監聽流量，對全域網路流量的影響，進而最小化網路代價，即整個網路中的總流量是本研究內容的重要研究目標；另外考慮監聽回傳路徑上，監聽回傳流量與背景流量間相互競爭共用鏈路的頻寬有限，因擁塞所引發的使用者服務品質變化，將隨著監聽業務強度增加。

監聽執行點選擇與三點間路由理論

S: Source; **D:** Destination **I:** Interception **L:** LEA

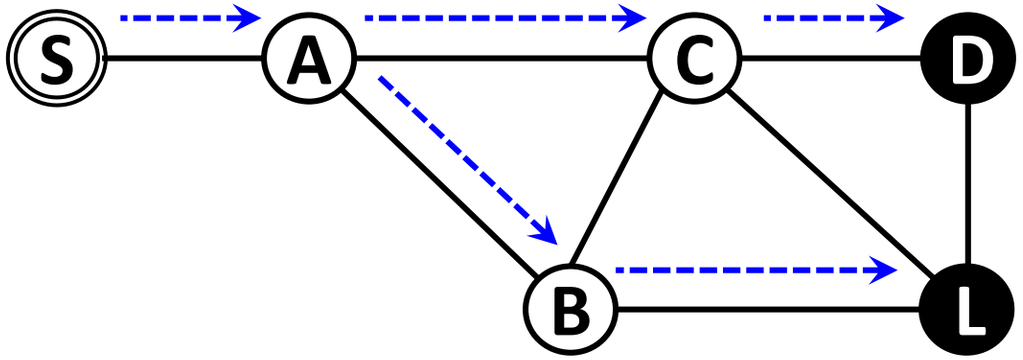


傳統網路: (a) 來源/目的端雙向流量合併攔截模型；(b)來源/目的端單向流量分離攔截模型；(c)阻斷攔截模型

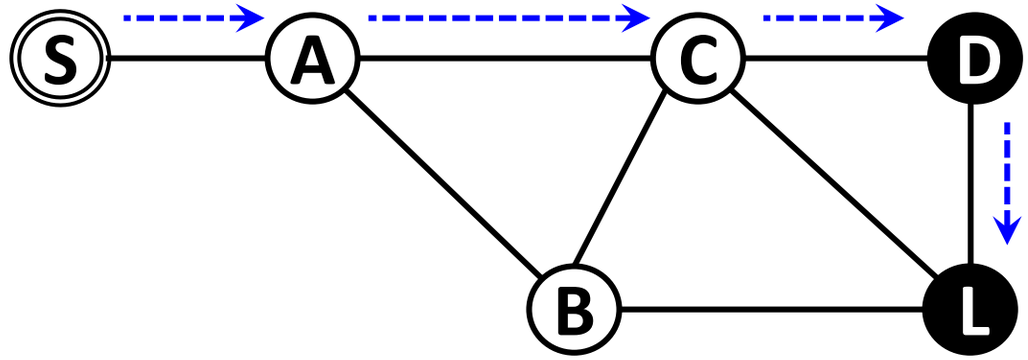


SDN網路: (a)T攔截模型；(b)ECMP-T攔截模型；(c)雙播攔截模型；(d)費馬點攔截模型

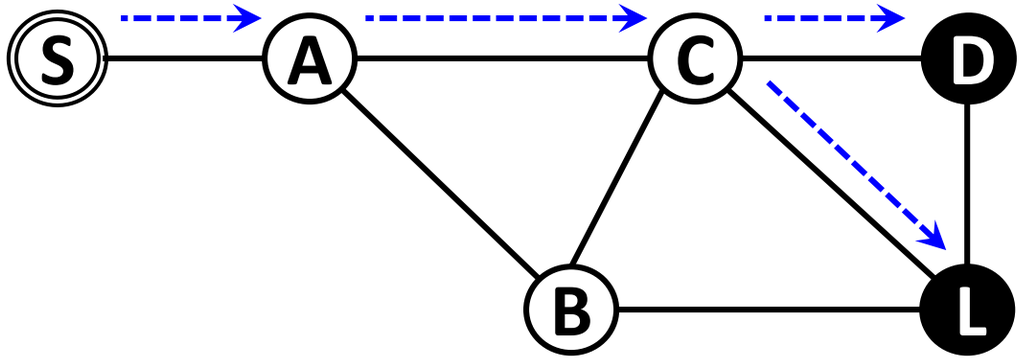
監聽執行點過早分枝問題



(a)



(b)



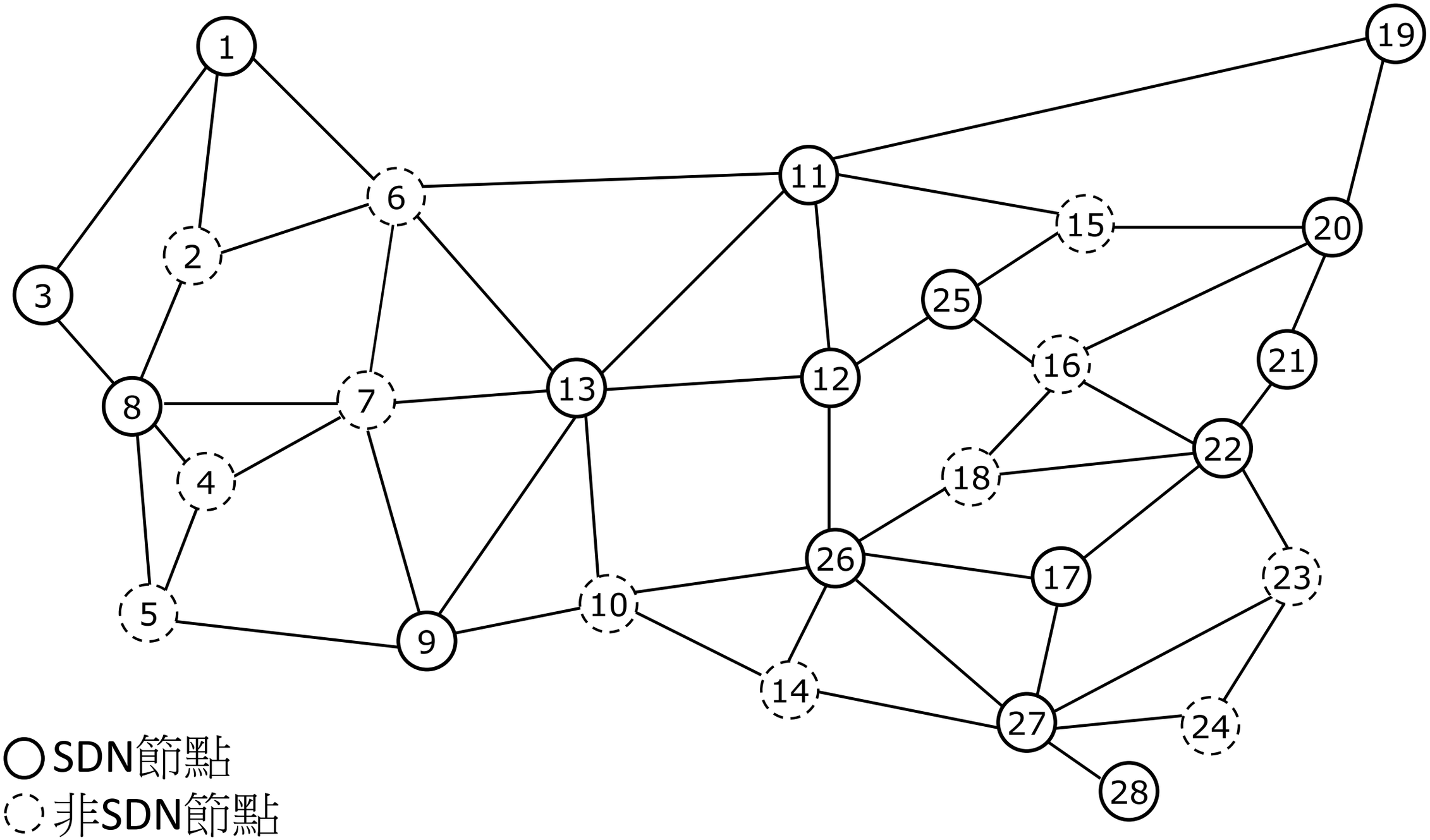
(c)

- 目前已提出的三點間路由方法中，以雙播(Bicasting)為例仍存在“過早分支問題(Premature Branch Problem)”，雙播雖然解決了在相同鏈路上重複傳送的問題，但分支時間的早晚會影響最少的網路代價和最低回傳時延的多重目標；
- 理論上只要發生上述現象，來源S-目的D-監聽中心I三點間也可證明無法滿足最短路徑，或是其監聽執行點的位置非全域最優。

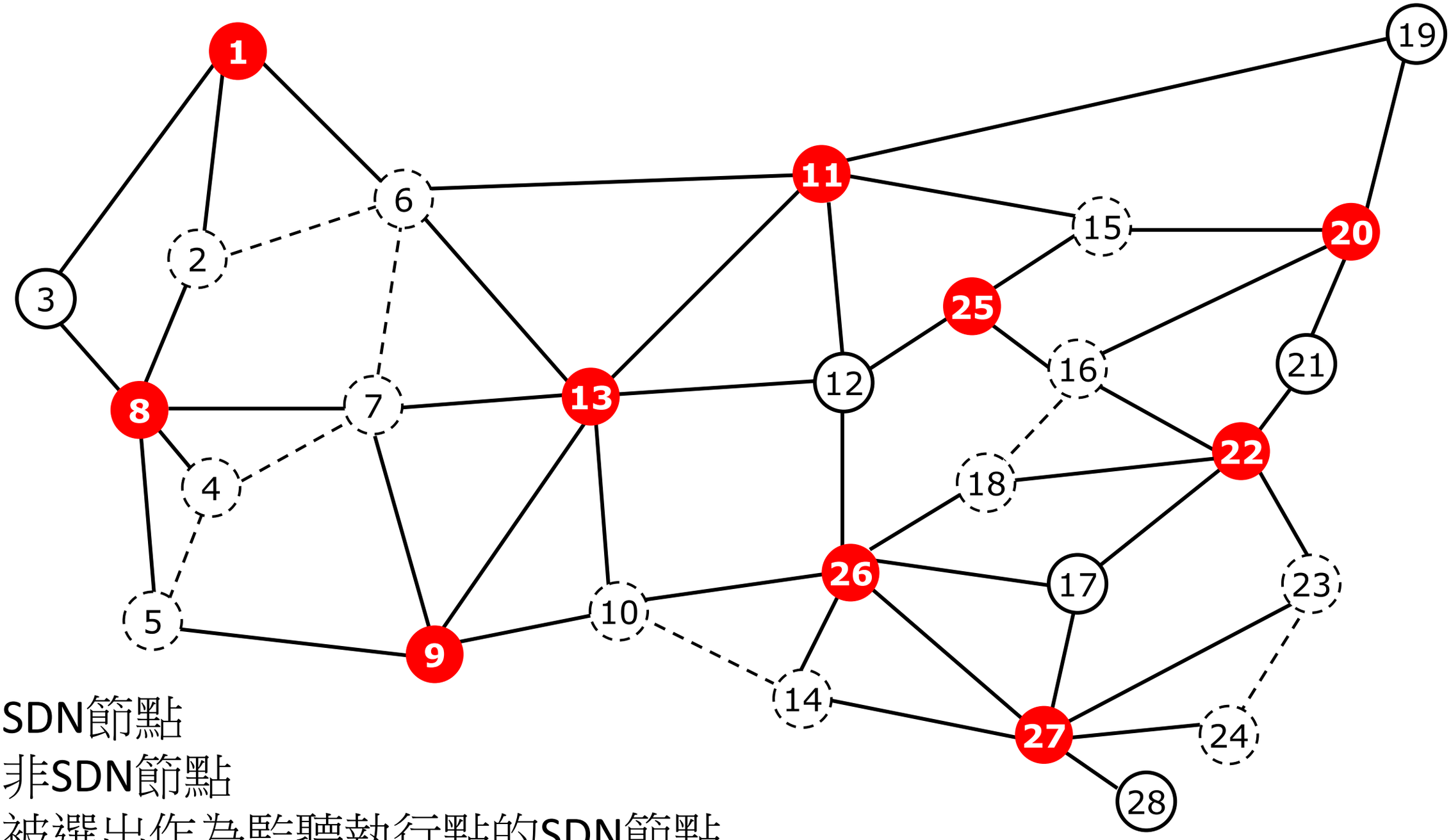
多監聽業務執行點與多監聽中心聯合部署策略

- 現實互聯網多監聽執行點部署問題，不會單純地符合三點間單一資料流程的微觀視角；大規模互聯網中的上億個節點間，擁有非常動態複雜的流量矩陣關係並交互影響，考慮某個I節點可滿足監聽S-D間業務流的需求，但同時也有成千萬個其他監聽目標節點對間的業務流，亦可能同時流經I點，因此多監聽執行點部署問題，必須全域考慮與所有被監聽目標的位置關聯性。
- 大多網路優化部署問題都可以規約為圖論最小頂點覆蓋問題(Minimum Vertex Cover Problem；MVCP)來求其解決方法，監聽執行點的部署問題也不例外。
- 此外，大規模互聯網面向軟體定義組網技術遷移過程中，可能面臨軟體定義與非軟體定義(Non-SDN)網路節點混合部署的情況，在這種情境下，並非任意節點均可通過軟體定義功能擔當起監聽執行點的角色；因此上述問題必須轉換為限制最小頂點覆蓋問題(Restricted Minimum Vertex Cover Problem；RMVCP)，屬於約束子問題的參數化頂點覆蓋問題的變形,學界至今還沒有找到一個有效的多項式演算法，是國內外學者研究的熱點問題之一。
- 在多監聽執行點部署演算法的基礎上，考慮在網路中部署多個監聽中心的條件下，引用最小成本分組(Grouping)演算法探討多監聽中心的佈局問題，由對全域網路流量的影響中，構築滿足最少數量監聽中心和最大網路規模間關係的全域優化問題；並進一步探討全域網路的監聽運行成本代價、監聽流與用戶資料流程的傳輸品質(QoS)等，也是很重要的研究議題。

限制性最小監聽執行點覆蓋優化部署問題



限制性最小監聽執行點覆蓋優化部署範例



SDN節點

非SDN節點

被選出作為監聽執行點的SDN節點

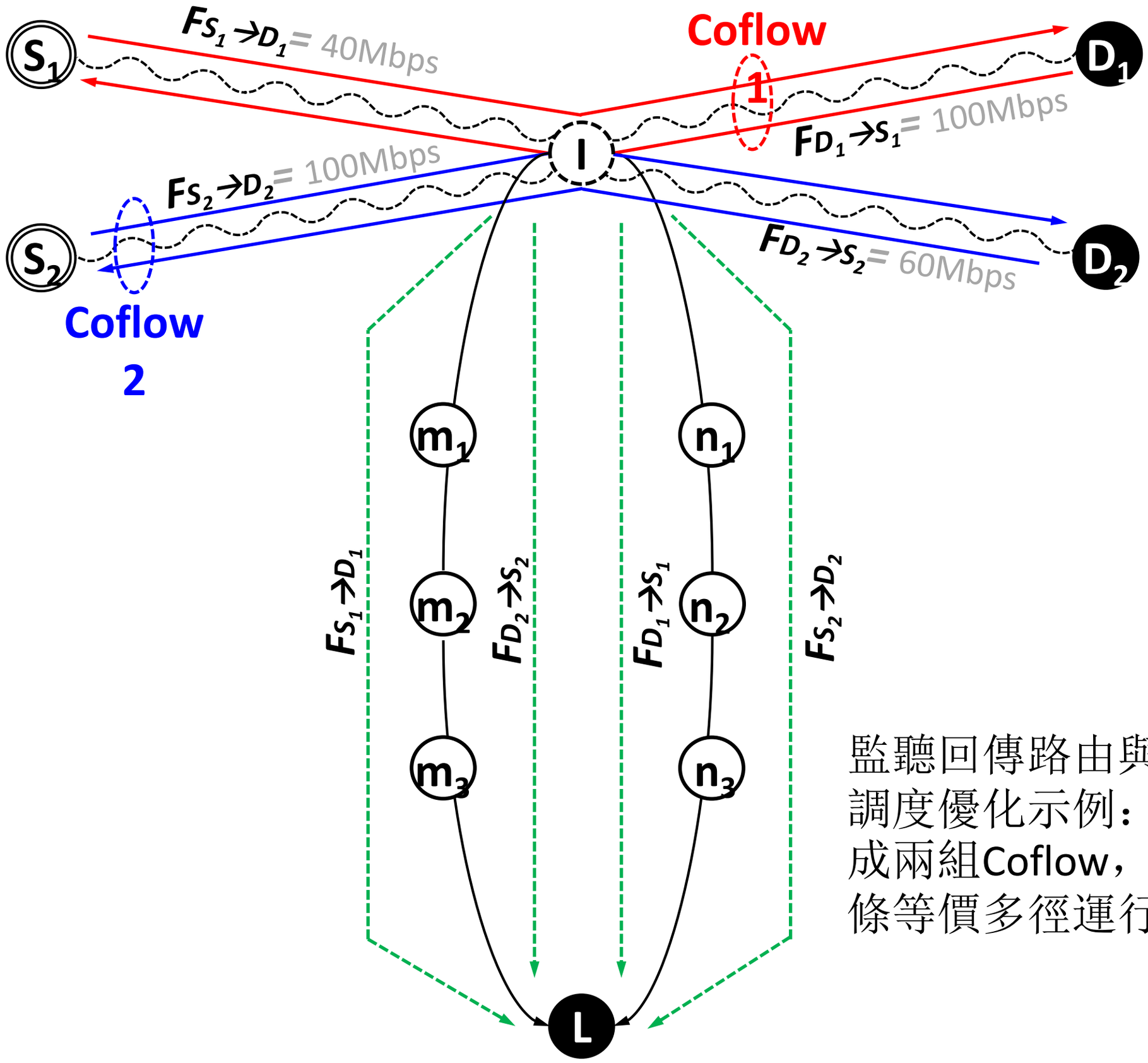
監聽覆蓋鏈路

監聽未覆蓋鏈路

監聽回傳路由與流量聯合調度技術

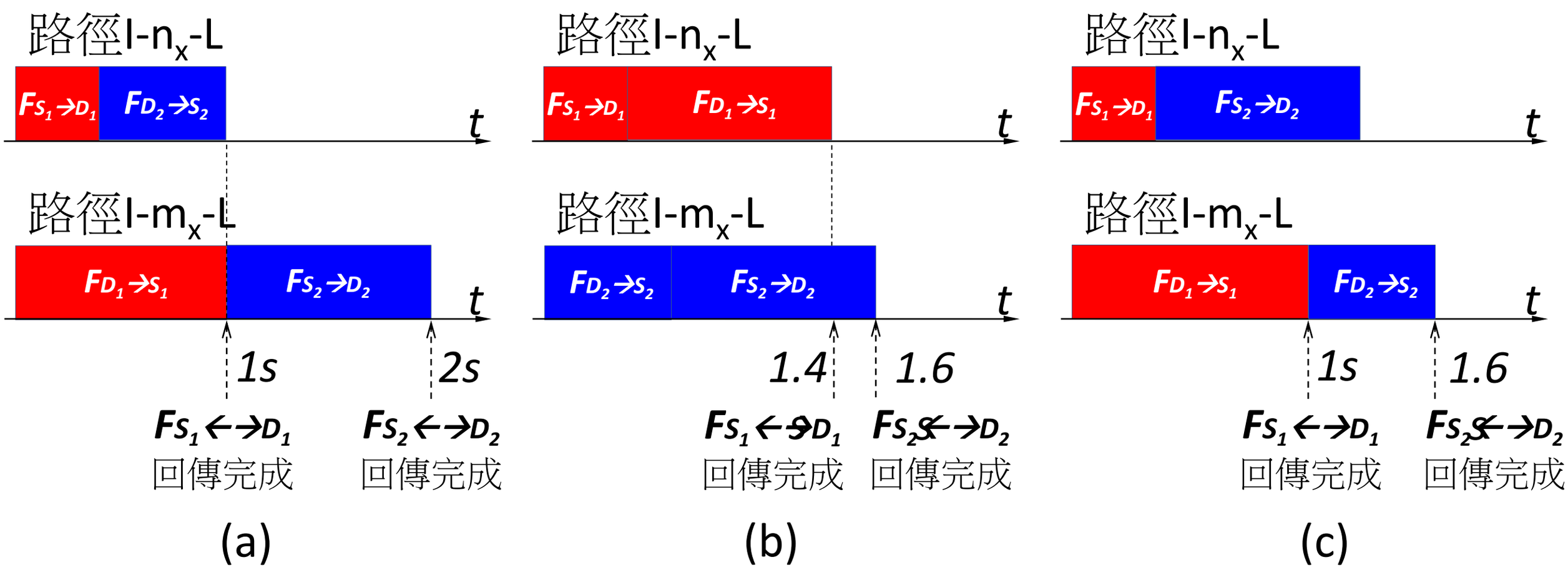
- 基於SDN的新型監聽系統可以通過已有互聯網基礎設施回傳截獲到的監聽流量，即I-L監聽內容回傳路徑也借路於互聯網，監聽業務的成本可以降低、監聽的業務流量可以容易擴展、監聽回傳流擁有相當數量的冗余鏈路或路徑可供選擇，單點故障的風險也會獲得進一步的保障。對監聽回傳流量的路徑選擇進行優化，關係到監聽回傳系統在網路流量的需求是否能獲得有效滿足，以及是否互聯網頻寬資源都得到有效的利用；以及和減少對最終使用者的服務品質影響，並進一步提高監聽業務的服務品質與性能、以及任務吞吐率。
- 既有互聯網端到端的流量矩陣模式，將受到在原始流量矩陣外，額外加入的監聽回傳流量而改變。為精確瞭解整個網路的流量矩陣所受到的影響，必須求解加入監聽回傳流量後的網路“**最大流量問題(Maximum Flow Problem)**”；以進一步進行聯合優化以逼近最優策略；
- 將基於監聽流中有關連性的單向流組成的Coflow為單位進行優化調度，讓監聽中心儘早收齊所有具有相關性的Coflow，為下一步分析程式達成對傳輸完成時間的優化目標。我們擬修訂並擴展REPIER演算法，探討多個相關的監聽流量Coflow(主要是上下行或同來源節點)，通過等價多徑路由回傳到監聽中心的優化調度策略。
- 隨著監聽業務量增加，整體網路的流量矩陣受到影響而造成擁塞現象，將嚴重影響用戶端到端的服務品質，因此監聽回傳流量與背景流量間競爭有限網路頻寬引發的服務品質變化也非常值得探討；並嘗試進一步在演算法中考慮加入網路擁塞的參數，使得擬發展的演算法得以自我調整(Adaptive) 擁塞的鏈路情況並加以回避，形成監聽回傳流多路徑負載平衡(Load Balance)及監聽路徑故障切換的方案。

監聽回傳路由與流量聯合調度問題



監聽回傳路由與流量聯合調度優化示例：四條流構成兩組Coflow，嘗試在兩條等價多徑運行傳輸調度

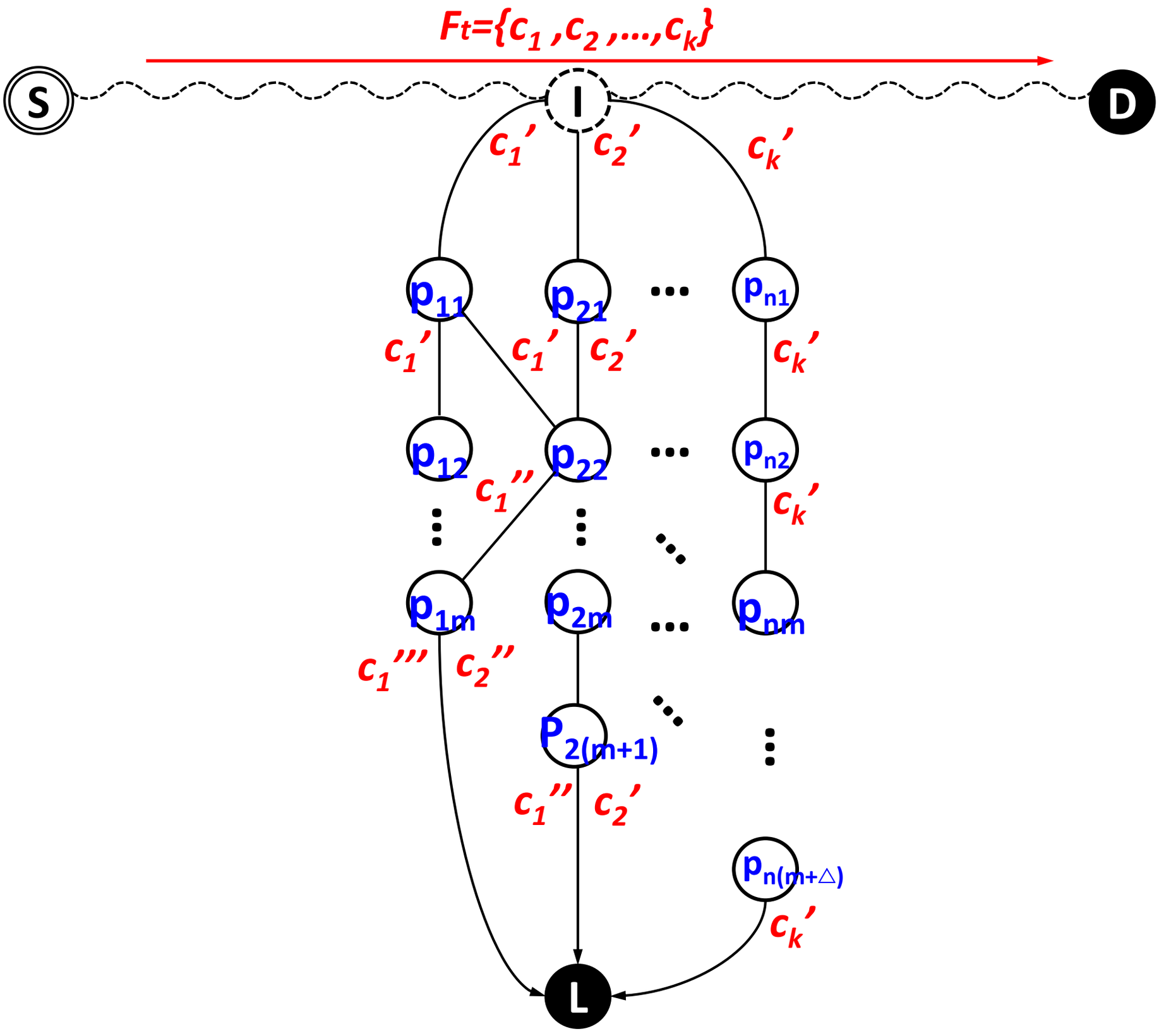
三種監聽回傳路由與流量聯合調度策略



高可靠監聽路由多路徑網路編碼傳輸方法

- 監聽系統I、L節點可能具備多宿主(Multi-homing)性質，以及與I-L路徑具備多路徑(Multi-path)的並行資料傳輸能力，從而獲得提高可靠度、提升傳輸輸送量，降低端到端傳輸時延等。
- 在網路流量理論中，源節點向目的節點發資料流程量，其最大流量值等於最小切割的每一條鏈路的總和，即Ford-Fulkerson證明的“**最大流最小切割**”定理。
- 近年來，一些研究人員提出採用網路編碼(Network Coding；NC)來進一步提高網路的輸送量，網路編碼的基本思想是允許網路的路由節點參與編解碼的資訊交換技術，允許來自不同鏈路的資訊進行編碼聚合，編碼後的資料再被中間結點以組播方式在多路徑間進行並行轉發，目的結點可依據相應的編碼係數進行解碼，從而還原出原始資料。網路編碼概念的提出，首次將網路和路由有機融合為一體，建立了一種全新的網路架構。
- 不同于傳統資訊傳輸方法,通過網路編碼可以將傳輸過程中的資訊流再次進行壓縮，推翻了獨立比特不能再被壓縮的立論，從而破解了網路傳輸**中香農(Shannon)資訊理論上界不可達**的問題。
- 此外，由於資訊被打散到多個路徑上，其通信保密性也大幅提升，非法竊聽者難以取得完整資料，這也是監聽回傳系統特別需要的特性。

高可靠監聽路由多路徑網路編碼傳輸方法

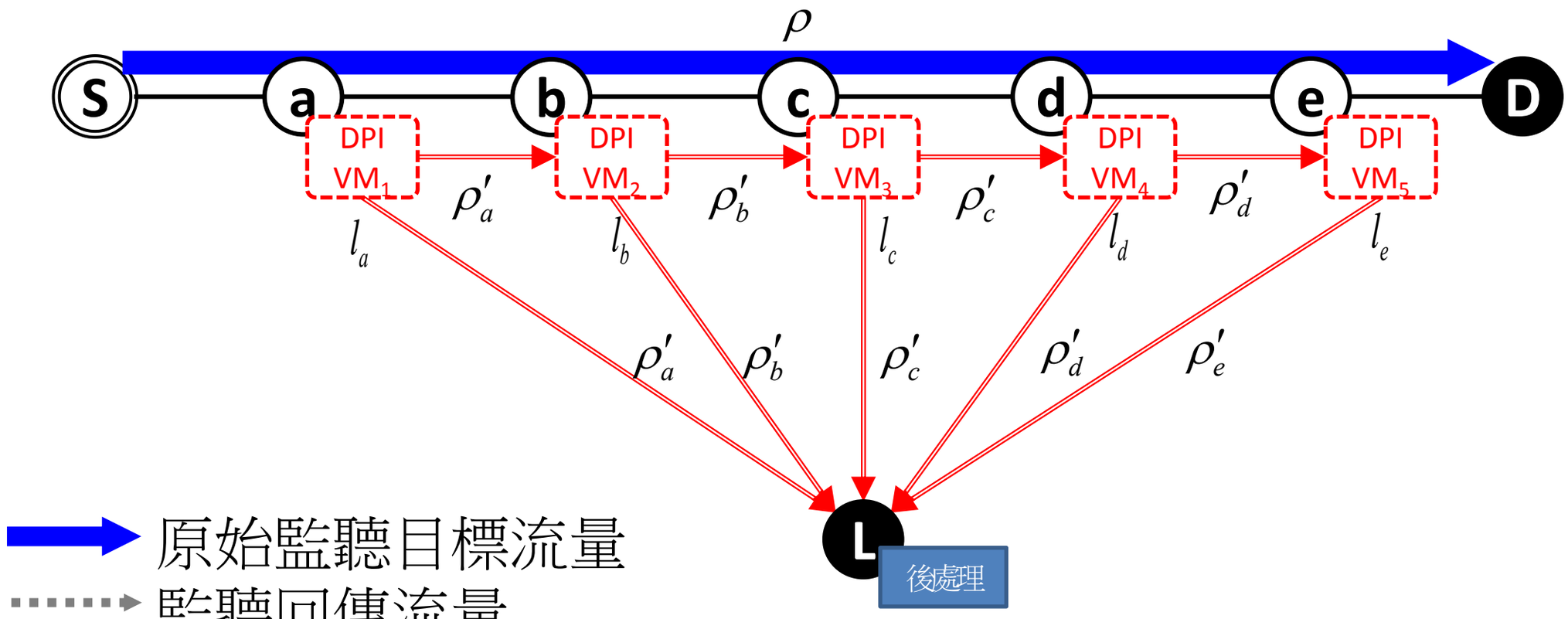


基於雲霧協同計算的分散式智慧DPI加速器部署及資源優化

- 監聽系統除了網路流量具有資料密集的特性外，同時也完全符合計算密集的定義；如何在智慧化網路中部署監聽內容分析處理節點，是下一代網路監聽系統的關鍵問題之一。下一代監聽模式預期將結合人工智慧深度包檢測自動分析技術，對各類型的被監聽流量內容(包含網頁,社群網路,電郵,遠端登入,遠程桌面,VoIP等)進行全自動分析工作，以大幅減少人工介入分析判讀的工作量；該問題關係到監聽系統所截獲的資料，是否能以最快的速度運行分析工作，同時極大化減少網路監聽回傳流量佔用運營頻寬，以及盡可能提高這些高價計算資源的利用率。
- 面向處理不同的被截獲的監聽業務流量，假設所有的分析子功能間沒有嚴格的執行順序關係，那麼就非常適合在監聽回傳路徑沿路上，部署各種不同類型的預處理分析功能子集，使得監聽回傳流量在回到監聽中心前，即預先完成部分或全部的初階(亦可稱為前處理或預處理)分析工作。
- 這種資源子集部署問題可歸納成圖論中的“**彩虹路徑問題(Rainbow Path Problem)**”，求解k種顏色是否能滿足彩虹連結的問題也稱為k-Rainbow Path Problem，而限制條件k歸納到本研究內容的研究即為監聽內容分析虛擬化子功能元件數量、或視為沿路節點具備霧計算能力的數量。
- 全域策略分配的Palette演算法，是基於無向無環圖論演算法，僅限於並無先後執行順序的預處理功能子集；同時原始的Palette模式也並未考慮在多路徑的情境下，無功能相互依賴性的監聽內容分析功能子集，也可以部署至多路徑上進行平行加速處理，以極大化提升在監聽回傳沿路上順帶進行預處理的效能。

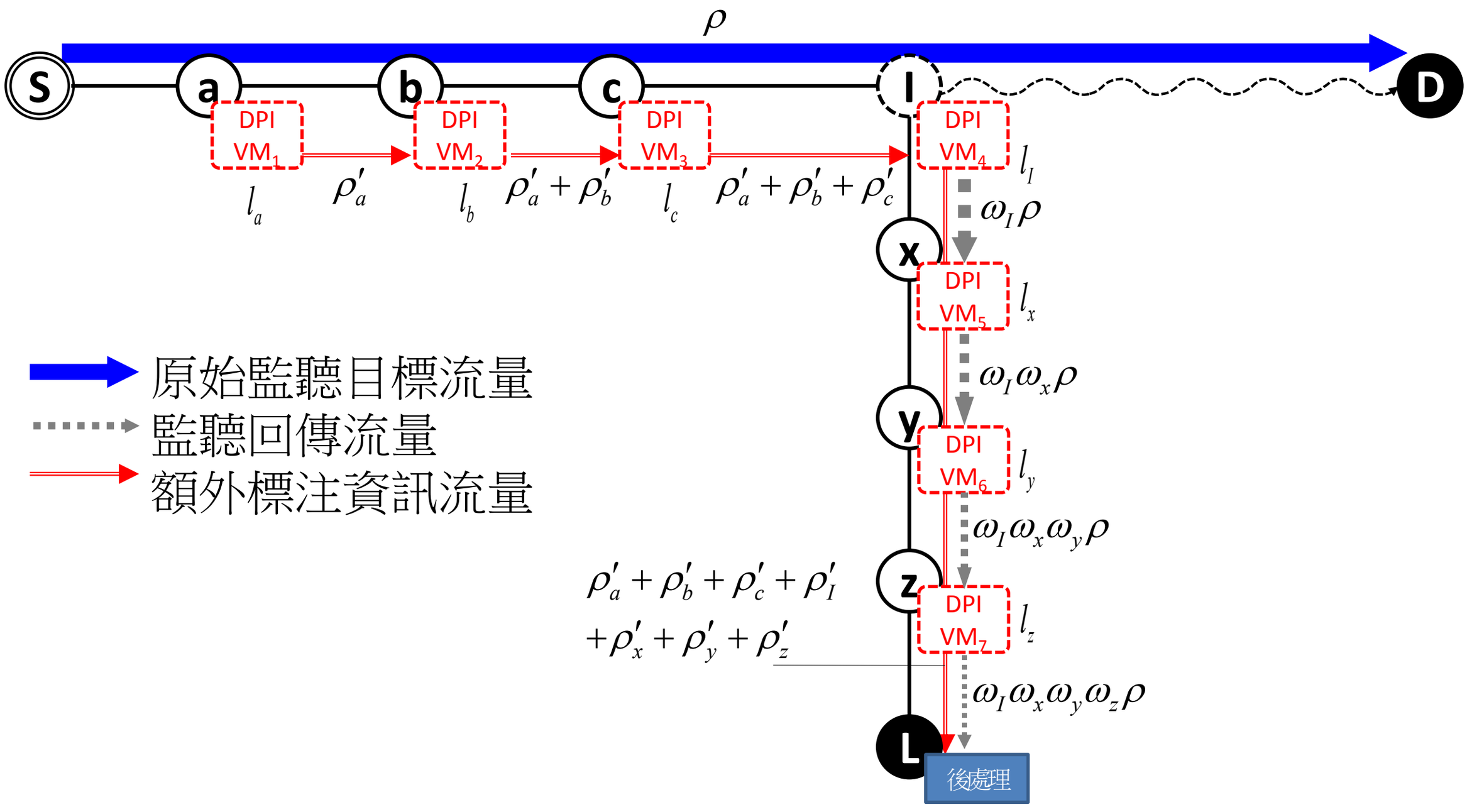
在S-D路徑上的霧節點運行監聽內容分析工作

分析工作100%由霧節點完成，監聽流量不需回傳至L點



DPI分析功能子集在霧計算節點的分散式部署與優化技術

在S-I-L路徑上的霧節點運行監聽內容分析工作

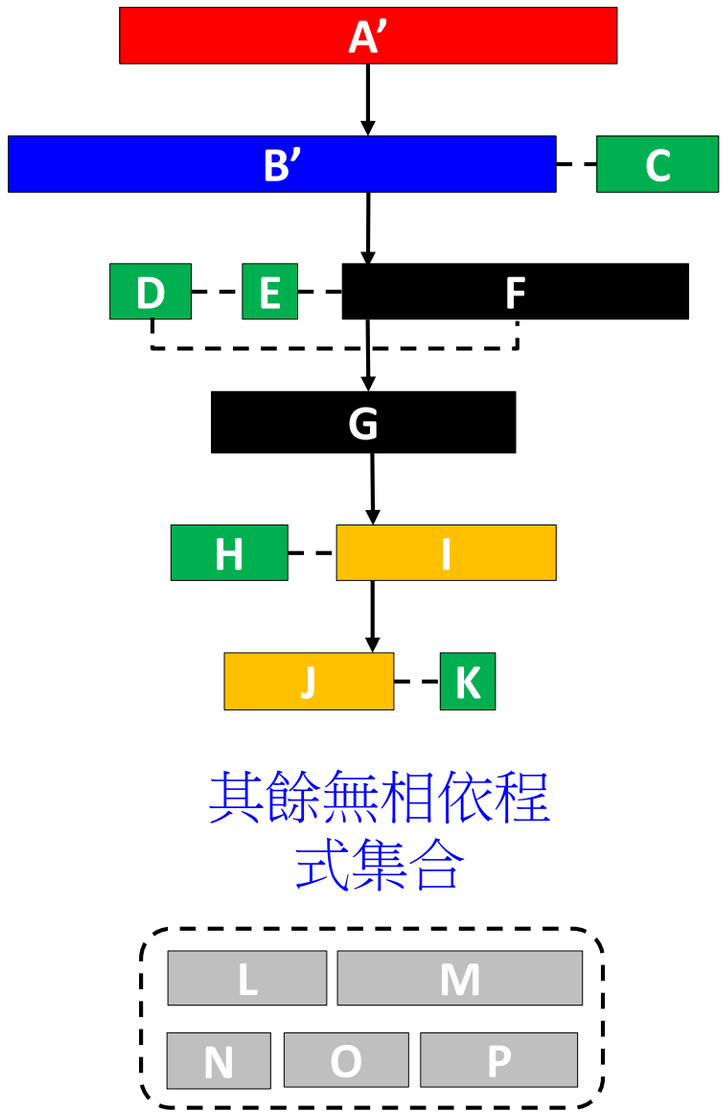


基於多徑路由的DPI分析功能子集分散式霧節點資源調度與優化技術

- 實務上，多樣化的霧節點預處理功能子集間，往往存在嚴格的先後依賴關係(Dependency)；為此必須求解霧節點計算資源優化部署演算法：
- 首先將上述彩虹路徑問題擴展為“**拓撲排序(Topological Sorting)問題**”，讓監聽回傳流量依序被預先部署至沿路的霧計算節點依預設執行順序，進行各DPI功能子集的預分析程式。
- 另外，考慮**分群(Clustering)演算法**，將全域監聽預處理的子功能個體通過演算法把功能相依的個體分到同一個子集內，安排一個子集任務最有利的策略是分配在同一個霧計算節點內，以減少不同子功能間溝通產生額外的網路開銷。
- 上述算法目標在於尋找DPI分析任務的最小執行時間，而對於霧節點計算資源的利用率較不重視；為滿足資源利用率問題，在分配無嚴格相依順序的副程式時運用“**背包問題(Knapsack problem)**”演算法求解，以滿足最大利用效率問題。以上所有多目標規劃任務可以使用**動態規劃(Dynamic programming)**方法建立融合模式並求解，運用至本課題的霧計算節點資源配置問題上，其效能目標在同時滿足最多的DPI分析任務可以在最短路徑上被分配完成、並減少分析計算任務的完成時間、降低霧節點間交互的網路流量開銷、以及減少計算霧節點資源閒置所導致的浪費。此外，演算法本身的時間及空間複雜度也將被考慮。

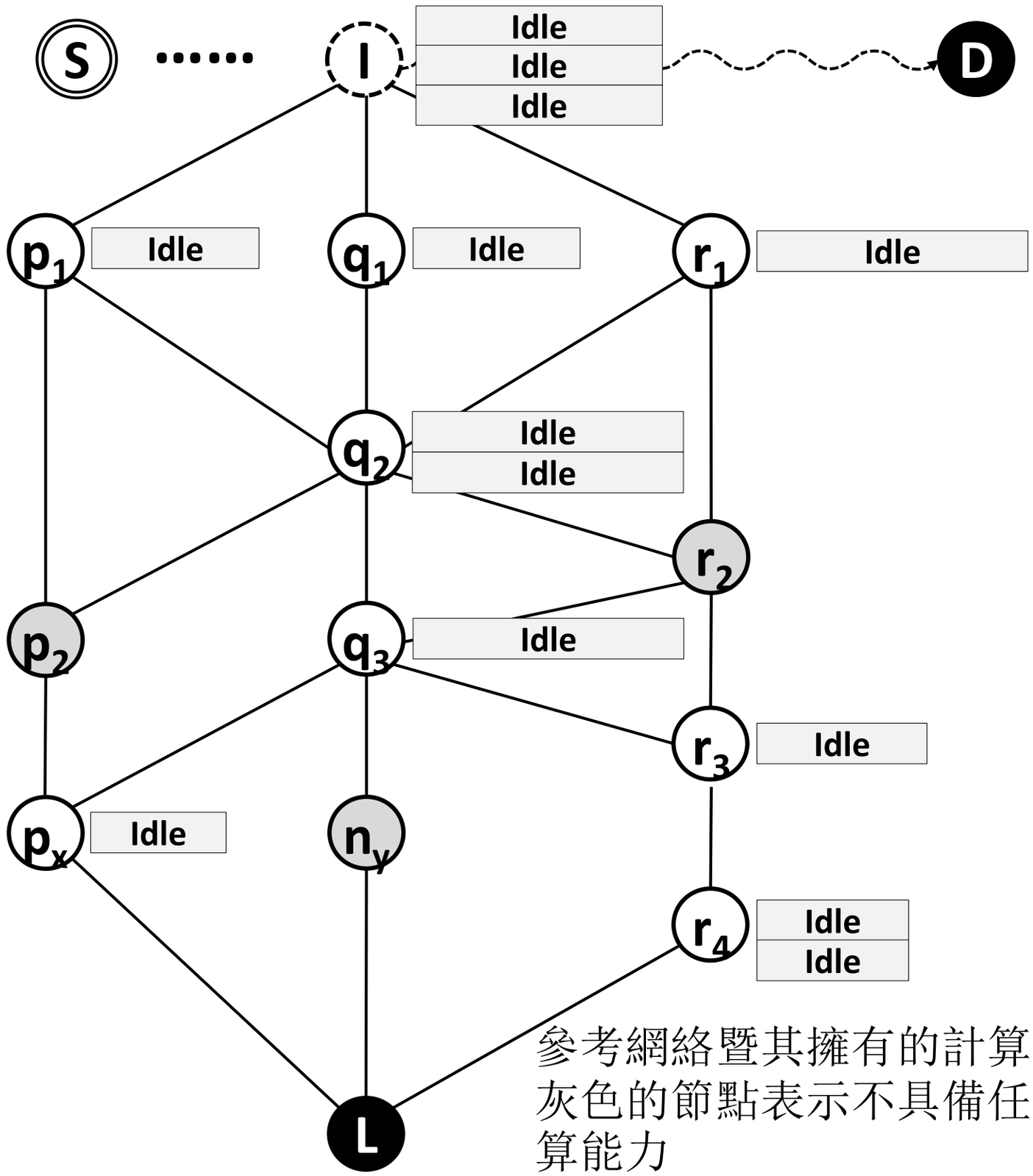
基於多徑路由的DPI分析功能子集分散式霧節點資源調度與優化問題

嚴格相依程式拓樸順序



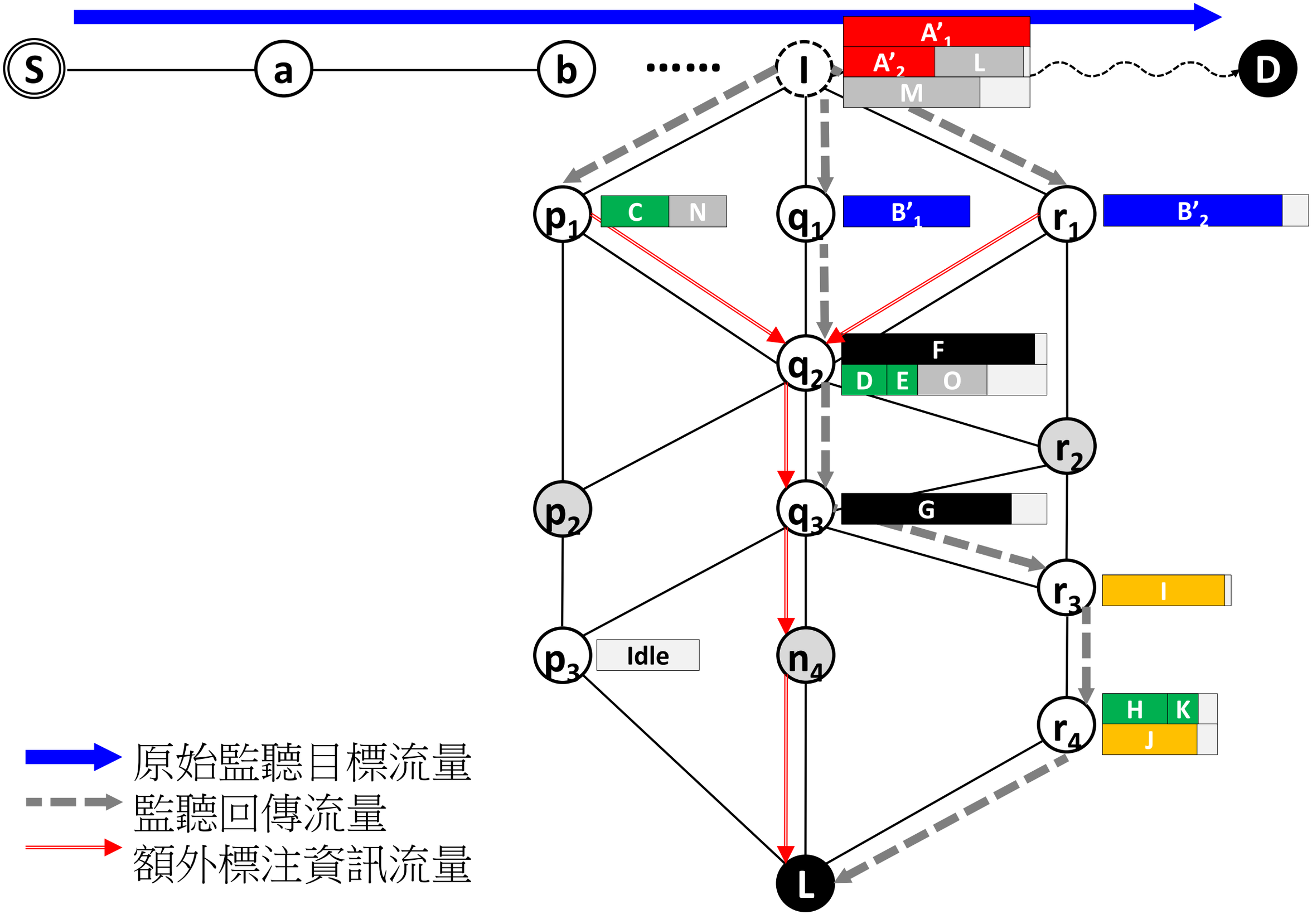
其餘無相依程式集合

分析功能子集即執行順序關係，其中虛線代表無順序相依性，A’B’具程式可分割性，其餘程式不可分割



參考網絡暨其擁有的計算資源，灰色的節點表示不具備任何計算能力

將前述工作調度至網路後的優化結果示例



結論與建議

- 為了提高下一代基於SDN技術組成的大規模網路(Large-Scale Networks)甚至於網際網路規模網路(Internet-Scale Networks)，其合法監聽暨分析系統架構自：
  - 網路拓撲
  - 網路流量
  - 計算資源

  三個角度切入，
- 通過網路拓樸理論建構、理論複雜度分析、高效能演算法設計與驗證、電腦模擬與實驗平臺構建，使合法監聽系統佈署在通信業務流量以每年100倍增長幅度下的互聯網等級大規模網路中，能夠符合：
  1. 更大的網路規模
  2. 更廣的覆蓋面
  3. 更高的部署彈性
  4. 更大的監聽業務量(傳輸量)
  5. 更即時的分析性能
  6. 更高的可靠性
  7. 更完美的服務品質
  8. 更深層的威脅鑒識能力
  9. 更低的開銷與更合理的建置與運營成本等
- 期望達到攔截分析一體化、監聽計算與監聽流量雙重卸載、加速威脅鑒識決策能力、並符合成本效益的下一代網路智慧監聽及分析系統。

Q&A

懇請各位專家批評指正！