以 SIP 為基礎合法監聽之研究

劉大川　　宋嘉銘　　彭俊豪　　蔡文能
交通大學計算機與網路中心
{ ltc, chiaming, thpeng, tsaiwn }@faculty.nctu.edu.tw

摘要

當 VoIP(Voice over IP)想要商業化並在市場上開始提供通話服務時，都會被國家的法律要求提供犯罪者的電話監聽。在這篇論文所提架構下的合法監聽，是以 SIP(Session Initiation Protocol)網路協定為基礎來提出一個架構，另外合法監聽有一些基本的要求，例如不能讓監聽目標發現受到監聽等等，本研究所提架構也能符合這些要求。

關鍵詞：網路電話，合法監聽。

Abstract

For VoIP(Voice over IP) to be commercialized, it must support Lawful Interception(LI) which the Law Enforcement Agency(LEA) of the country asks for. The LI-supported VoIP architecture we proposed in this paper is based on SIP(Session Initiation Protocol). Certain basic requirements are required for a lawful interception system. The architecture we proposed meets the requirements which a lawful interception system must fulfill.

Keywords: Lawful Interception, VoIP.

1. 前言

隨著網際網路的成長，在網路上的應用也變得越來越多，網路電話(VoIP)是近幾年快速興起的應用，其原理是將通話語音經由 IP 網路封包交換技術傳送的新電話服務。網路電話是一個無法擋的潮流，以交大學生為例，大約每五人就有三人在 TANet 上使用 Skype 網路電話，且這個比率持續增加中。

傳統 PSTN(Public Switched Telephone Network)和 GSM(Global System for Mobile Communication)[23]已經有一套正在運行的架構可以讓司法單位監聽使用傳統電話和行動電話通話的使用者。關於網路電話合法監聽與安全性雖然已有許多討論[1, 2, 4, 6, 7, 8, 9, 10, 22]，但是目前還無法達到此目的，因此在這裡希望可以提出一套讓 VoIP 有合法監聽功能的架構。

2. 背景知識

2.1 電話網路的監聽方法

依照通訊保障及監察法，只要有足夠的事實可以證明相監聽的對象有相關罪嫌，就可以申請通訊監察書，通訊監察書應記載下列事項：案由及涉嫌觸犯之法條、監察對象、監察通訊種類及號碼等足資識別之特徵、監察處所、監察理由、監察期間及方法、聲請機關、執行機關。

前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權核發，審判中由法官依職權核發，但是該管檢察官可以口頭通知執行機關先予執行通訊監察。圖 1為公眾交換電話網路的監聽架構。

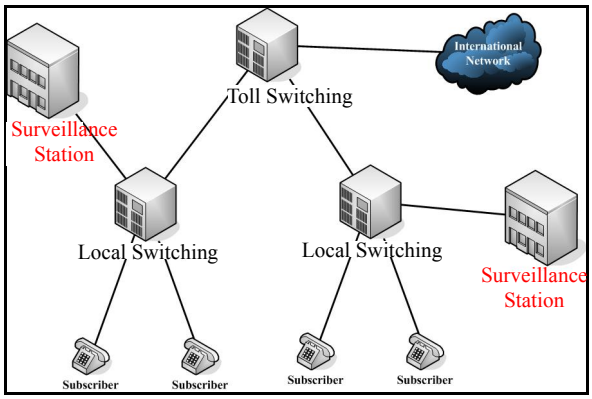

圖 1　公眾交換電話網路監聽架構

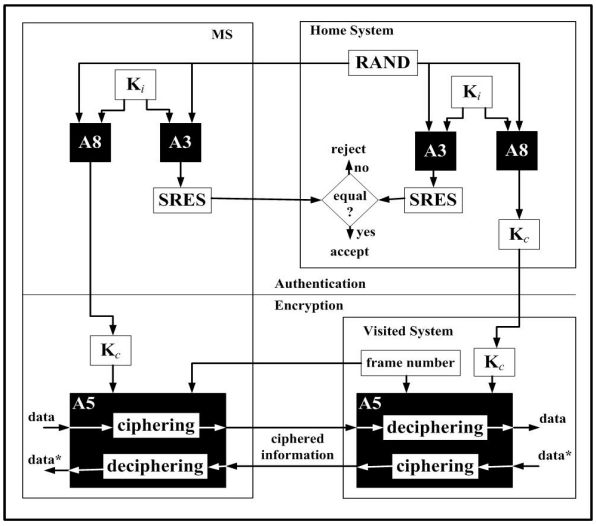

圖 2　GSM 認證和加密架構圖

GSM 的安全性分成二種，一種是認證，一種是加密，認證是為了確認是否為合法的用戶，所以使用者通話都需要認證，加密則是因為 GSM 的通

話因為經由無線電波傳送，容易被有心人士從中攔截，取得通話內容，因此需要將通話加密，圖 **2**是 GSM 認證和加密架構圖[24]。

2.2 網路電話簡介

網路電話是將聲音數位化之後，以一個個封包的方式，透過 IP 架構的網路傳送到收話端 。

Voice over IP 簡單來說，即是將聲音數位化之後，以一個個封包的方式，透過 IP(Internet Protocol)架構的網路傳送到收話端，因成本更加低廉，所以廣受業界的矚目與推廣。

網路電話通訊協定

為了可以順利的在公眾的 IP 網路上建立連線並傳送聲音的封包，一套公認的通訊協定(Protocol)是必要的。網路上兩大網路通訊協定訂定組織：ITU(International Telecommunication Union) 與 IETF(The Internet Engineering Task Force)分別都訂定了適用於網路電話連線建立與中斷的通訊協定。

SIP：Session Initial Protocol [16]，於 1999 年 3 月定義於 RFC 2543，再版定於 RFC 3261。為一套點對點(Peer to peer)以及主從式(Client/Sever)的傳輸架構，與 SDP(Session Description Protocol, RFC 2327)[17]、RTSP (Real-Time Streaming Protocol, RFC 2326)、SAP (Session Announcement Protocol, RFC 2974)合為 IETF 多媒體資料與控制架構(Multimedia data and control architecture)。SIP 最大的好處即為簡單、彈性佳，適合用於智慧型掌上產品的開發。

2.3 Session Initial Protocol (SIP)

Session Initial Protocol，簡稱 SIP，是由 IETF 於 1999 年訂定出來的應用層(Application-Layer)通訊協定，主要是為了多媒體通訊的建立、修改與中斷而訂定。

SIP 為一個主從式(Client-Server)的架構，由用戶端(Client)發出需求(Request)，伺服器端(Server)接收到需求後，視情形發出適當的回應(Response)給用戶端。

SIP 訊息傳送

SIP 是一個以文字為基礎(Text-base)的通訊協定，使用 ISO 10646 定義的字元，並使用 UTF-8 的方式編碼，所以 SIP 的訊息看起來類似於 HTTP[11]的訊息。用文字基礎傳送的缺點是與使用二進位方式表示的訊息相較，較占傳輸頻寬。

SIP Request 訊息可分為六個基本類型：

1. INVITE：用來發出邀請、開起連線的訊息。
2. ACK：用來確認最後的 Response 已收到。
3. BYE：用來結束連線用的訊息。
4. OPTION：用來詢問伺服器的負載量等訊息。
5. CANCEL：用來停止一個暫時行的 Request。
6. REGISTER：由 SIP User 發出，做為登入或註冊用的訊息。

圖 3 即為 SIP 建立通話時的訊息傳遞流程。

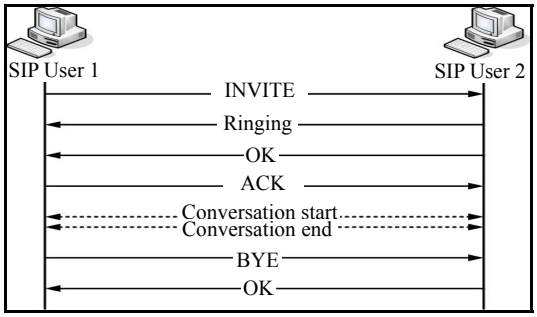

圖 3 基本 SIP 建立通話流程

3. 3. 相關研究

3.1 以 H.323 為基礎的四種合法監聽方法

以 H.323[21]為基礎的研究中，[22]提出四種在網路電話上的監聽方法，第一種是在閘道器(Gateway)上監聽，第二種是修改 Gatekeeper 使被監聽的網路電話封包會經過監聽的機器，第三種是網路電話的封包一定會經過監聽的機器，最後一種是把監聽的機器和交換器或集線器連接起來，只要是監聽的封包都會複製一份到監聽的機器。

在閘道器上監聽

在閘道器上監聽這種方法可以用在當 H.323 網路電話打到公眾交換電話網路的時候，這裡的閘道器指的是連接 H.323 和公眾交換電話網路的機器，它可以在 H.323 和公眾交換電話網路的網際網路通訊協定之間做轉換。因為所有的通話都會經過這台閘道器，所以可以在這裡監聽，當閘道器發現有通話需要被監聽時，它會將通話內容複製一份到一台專門放監聽資料的機器上。

利用 Gatekeeper 將被監聽的通話導向監聽設備

在 H.323 通訊協定中，gatekeeper 負責通話建立的工作，因此可以修改 gatekeeper 來達到監聽的目的。在 H.323 網路裡面增加一台監聽設備，儲存監聽的資料，再來就是修改通話建立的流程，讓被監聽的通話導向監聽設備，這樣就可以把通話內容記錄下來，所以原本通話會變成發話端跟監聽設備建立連線，以及監聽設備跟收話瑞建立連線。在 H.323 訊息中，RAS 是 Registration, Admission and Status，ARQ 是 Admission Request，ACF 是 Admission Confirm。

固定路徑監聽

這個方法是在 H.323 網路裡面加入一台監聽設備，並且讓所有的通話都一定經過這台監聽設備，無論通話是否需要被監聽。

隨機處理模式監聽

這個方法是將全部的交換器或是集線器都跟

監聽設備做連接，並且這些交換器和集線器都必須讓所有經過它們的封包都複製一份到監聽設備那邊去，這樣一來就可以達到監聽的效果，所以監聽設備必須能夠過濾並取出所有封包的內容，而且它會有一份清單，根據那份清單來判斷哪些通話需要監聽。**表 1**為比較說明。

表 1　四種方法優缺點比較

	在閘道器上監聽	用 GK 監聽	固定路徑監聽	隨機處理監聽
偵測性	不會	會	不會	不會
攔截通話	部份	全部	全部	全部
通話品質	不受影響	受影響	受影響	不受影響

3.2 思科提出的 IP 網路合法監聽架構

思科提出一個可以提拱 IP 網路合法監聽的架構[1]，如**圖 4**，它可以提供基本的監聽功能，在這個架構下監聽可得兩種資料，一是通話內容，也就是被監聽者所有的談話都被記錄下來，另一種是監聽相關資訊(Intercept Related Information)，簡稱 IRI，IRI 指的是和監聽目標有相關的資訊，例如雙方的電話號碼，或是監聽目標曾經播過哪些電話。

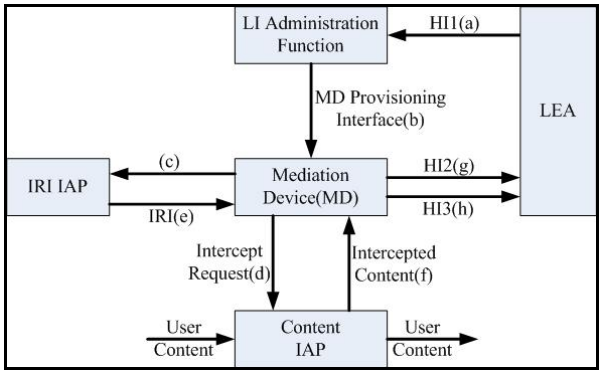

圖 4　思科監聽架構

以下介紹架構中的各個構成要素：

- LI 管理功能(LI Administration Function)：當司法單位得到法院的指令或授權，可以用這個管理功能來執行監聽。
- 調解設備(Mediation Device，MD)：MD 要求 IAP 進行監聽，並收集 IAP 回傳的結果，將這些結果轉換成司法單位要求的格式，最後才送給司法單位。
- 監聽設備(Intercept Access Point，IAP)：用來執行監聽動作的設備。IAP 有二種類型，一種負責提供通話內容，一種負責提供 IRI。
- 通話內容監聽設備(Content IAP)：用來監聽經由 IP 網路傳送通話內容的設備。
- 相關資訊監聽設備(IRI IAP)：用來提供監聽相關資訊的設備。
- 司法單位(Law Enforcement Agency，LEA)：司法單位會送出監聽要求給服務提供者，之後再接收監聽結果。

表 2是監聽介面的說明表。

表 2　監聽介面

界面(Interface)	說明
(a) HI1	Handover Interface 1 – 管理介面，司法單位經由這個介面傳送監聽資訊給管理功能
(b)MD Provisioning	調解設備(Mediation Device)供應介面，傳送一些參數給 MD，例如：監聽目標的資料、監聽持續時間、監聽類型等等…
(c) IRI IAP Provisioning	為了取得監聽目標的 IRI 而提供更詳細的監聽目標資料，監聽持續時間等等…
(d) Content Intercept Provisioning	提供資料給負責監聽通話內容的 Content IAP
(e) IRI to MD	負責記錄 IRI 的設備傳送 IRI 給 MD
(f) Content to MD	負責監聽通話內容的設備傳送監聽結果給 MD
(g) HI2	Handover Interface 2 – MD 傳送 IRI 給司法單位的介面
(h) HI3	Handover Interface 3 – MD 傳送通話內容給司法單位的介面

思科提出的合法監聽架構，是大概地說明合法監聽可能需要哪些設備配合，每個設備應該負責做什麼事情，是一般的合法監聽架構，但是細部方面沒有做詳細的說明，也沒有針對網路電話加以討論，所以如果電信業者想要真正應用在現實生活中，還有一段差距。

4. 以 SIP 架構為基礎之合法監聽功能

4.1 系統簡介與假設

我們提出的系統架構結合了思科(Cisco)提出的合法監聽架構和 SIP 網路協定的架構，讓使用 SIP 網路協定建立的網路電話可以提供合法監聽的功能。

而且這個架構符合合法監聽的三項要求：一，不會讓監聽目標發現自己受到監聽；二，假如司法單位除了要監聽通話內容，還需要監聽相關資訊的話，必須要提供給司法單位；三，監聽結果有加密的話，必須提供加密的金鑰給司法單位。

除此之外我們提出的架構也具有安全性，並假設使用者傳送出來的所有 SIP 訊息一定會經過 SIP

代理伺服器，而且使用者需要認證才可以使用網路電話的服務，也就是說使用者為撥打電話的一方，或是接受電話的一方，一定要先經過認證並通過才可以，這個假設亦符合電信業者的營運目的。**圖 5** 說明 SIP 合法監聽網路示意圖。

4.2 系統架構

在這裡我們提出的系統架構是參考思科提出的合法監聽架構以及 SIP 網路協定架構，架構中有七種元件，每種元件負責不同的功能，我們會在後面做進一步的說明。

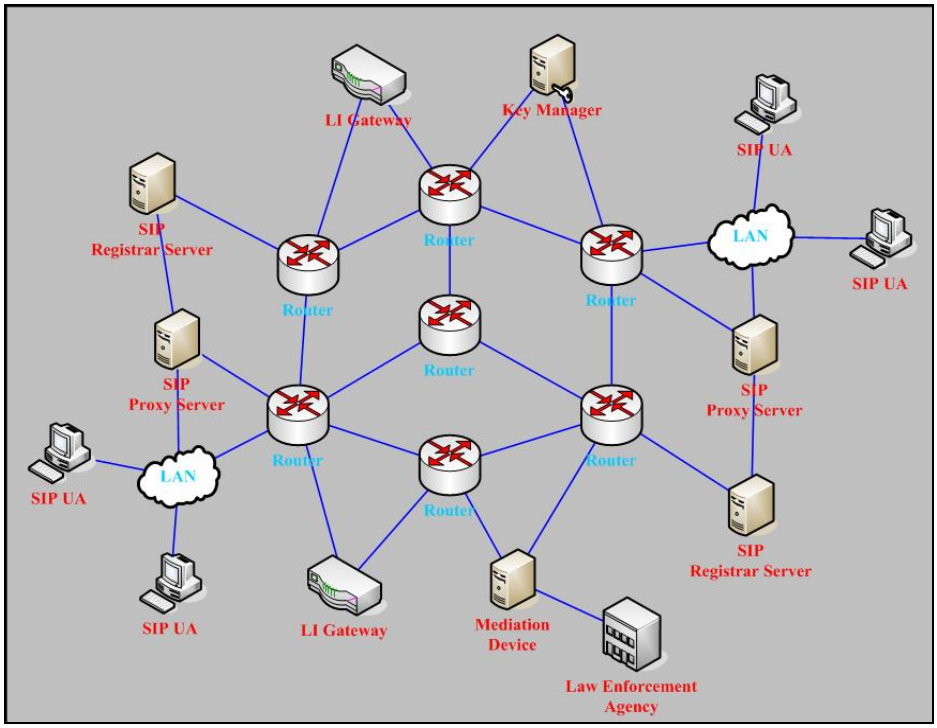

圖 5 SIP 合法監聽網路示意圖

在這個架構中之下，能使 SIP 提供合法監聽的功能，而且不會更改原本 SIP 的架構，除了可以提供合法監聽的功能之外，這個架構也可以讓提供網路電話服務業者向網路電話客戶收取使用費，如何能達成這個目的，在於我們假設所有的 SIP 訊息都會經過 SIP 代理伺服器，所以每一通網路電話的建立時間和結束時間都會被記錄在這台 SIP 代理伺服器，網路電話服務業者就可以用這個記錄向每位客戶寄發帳單，依照客戶使用情形收取服務費。

以**圖 6**為例，SIP User 1 會發出 INVITE 的 SIP 訊息(1)，代理伺服器(Proxy Server)收到訊息之後，會向註冊伺服器(Registrar Server)確認 SIP User 1 的認證資料(2,3)，認證通過並且經過授權後，代理伺服器才可以讓 SIP User 1 撥打網路電話，再來會將 INVITE 訊息傳送到 SIP User 2 那邊的代理伺服器(4)，代理伺服器再將訊息傳送給 SIP User 2(5)。

如果 SIP User 2 要回應這通網路電話，會回傳一個 OK 的訊息(6)，代理伺服器接收到 SIP User 2 的訊息，同樣會向註冊伺服器確認 SIP User 2 的認證資料(7,8)，確定有權限可以接這通網路電話之後，才會將 OK 的訊息傳送給 SIP User 1 那邊的代理伺服器(9)，代理伺服器再將訊息傳送給 SIP User 1(10)，並透過 SDP 訊息指定 SIP User 1 和 SIP User 2 通話所使用的 RTP[12]連線要和哪一台合法監聽閘道器做連線。

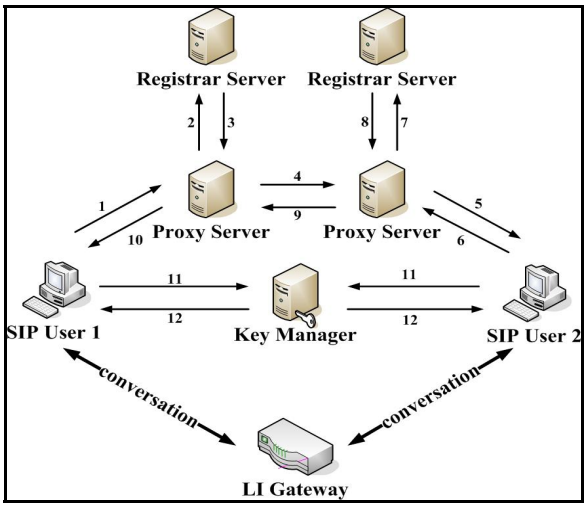

圖 6 SIP 結合合法監聽的範例

接下來 SIP User 1 和 SIP User 2 會需要加密通話內容的金鑰，而這把金鑰是由金鑰管理元件(Key Manager)所產生並且維護，金鑰管理元件負責管理所有 SIP 建立通話之後將通話加密所用的金鑰，可以說是非常重要的部份，所以需要安全的控管。SIP User1 在和 SIP User2 建立通話連線之前，會先跟金

鑰管理元件建立加密的連線(11)(例如用 Diffie-Hellman 或是 RSA 交換金鑰)，SIP User 2 同時也跟金鑰管理元件建立加密的連線(11)，接著金鑰管理元件會把之後通話加密所使用的金鑰傳送給 SIP User 1 和 SIP User 2(12)。

最後 SIP User 1 和 SIP User 2 都會跟合法監聽閘道器建立連線，這時候 SIP User 1 和 SIP User 2 就可以開始通話，而且這些通話都會用金鑰管理元件所產生的金鑰來加密，也就是說合法監聽閘道器所監聽的通話是經過加密的，這樣可以防止電信業者私自取得通話內容。

在這個架構中，由 SIP 代理伺服器進行 IRI IAP 的工作，而通話監聽功能(Content IAP)則由合法監聽閘道器(LI Gateway)所取代，為了讓司法單位可以解密監聽結果，金鑰管理元件會將通話加密金鑰送到調解設備，再由調解設備送給司法單位，為了避免被有心人士從中攔阻，破解這把金鑰，以增進系統安全性的考量下，我們將金鑰管理元件和調解設備合而為一，這樣就可以降低通話加密金鑰在網路上傳送的風險。

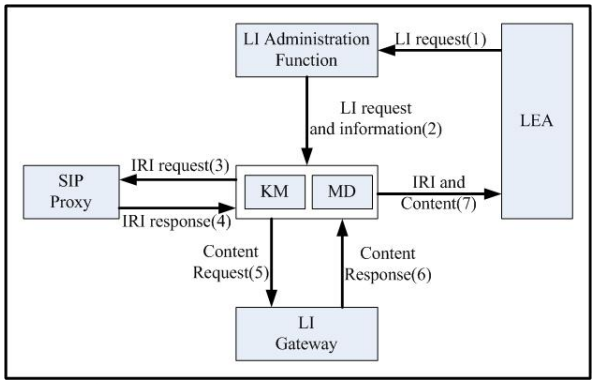

圖 7　系統架構圖

圖 7是系統的架構圖，當司法單位從法官或是檢察官那裡取得通訊監察書之後，就可以開始執行監聽流程。首先，司法單位發出合法監聽要求給合法監聽管理功能(1)，合法監聽管理功能收到司法單位的監聽要求之後，會把監聽的格式和要求傳送給調解設備(2)，調解設備接收到資料之後，就開始執行監聽的流程，他會先判斷使用者所在的網路負責的 SIP 代理伺服器，發出監聽相關資訊的要求(3)，因為 SIP 代理伺服器會紀錄 SIP 使用者所傳送過的訊息，所以它可以提供監聽通話的相關資料，回傳給調解設備(4)。

在 SIP 通話建立成功而且通話雙方準備開始傳送語音資料時，金鑰管理元件會和通話雙方建立安全連線(如：RSA 或 Diffie-Hellman)，並產生一把通話加密金鑰，利用安全連線將金鑰傳送給通話雙方，這時候調解設備會發出通話監聽要求給合法監聽閘道器(5)，告訴合法監聽閘道器 LI ID 以及監聽結果回傳位址，此時合法監聽閘道器就會開始複製監聽通話，並將複製結果回傳到調解設備(6)，最後調解設備會把監聽相關資訊和監聽通話結果收集起來，並把結果轉換成司法單位要求的格式，最後將這些監聽結果回傳給司法單位(7)，同時因為金鑰管理元件和調解設備合而為一，所以調解設備也可以知道通話加密金鑰的內容，因此回傳的監聽結果也會包含這把通話加密金鑰，有了這把通話加密金鑰，司法單位可以把加密的監聽結果解密，得到法庭上所需要的監聽內容。

4.3 系統元件

在我們的架構中會用到 SIP 網路協定中 SIP 代理伺服器以及 SIP 註冊伺服器，其中 SIP 代理伺服器需要做一些修改。

SIP 註冊伺服器(SIP Registrar Server)

SIP 註冊伺服器負責 SIP 使用者的註冊以及認證的動作，其負責任務與一般 SIP 註冊伺服器相同。

SIP 代理伺服器(SIP Proxy Server)

在我們的合法監聽架構下，SIP 代理伺服器除了原來該有的功能外，還有一項重要的任務，提供監聽相關資訊給調解設備，因此代理伺服器要做一些修改，得以記住監聽通話的建立時間、結束時間、持續時間、IP 位址、還有使用者曾經撥打給哪些人，成功多少通話、失敗多少通話等等以供司法單位在偵辦案件的需要。這些資訊最後要整理傳給調解設備，讓調解設備將這些監聽相關資訊送到司法單位 LEA。

SIP 代理伺服器的另外一項功能就是指定 SIP 使用者通話 RTP 連線和哪一台合法監聽閘道器連接，當 SIP 的訊息最後出現 OK 的時候，SIP 代理伺服器就會在 SDP 訊息裡面加入合法監聽閘道器的 IP 位址，如此一來 SIP 通話時的 RTP 連線就會和合法監聽閘道器做連接，可以監聽雙方的通話。

除了 SIP 相關元件外，還必須有合法監聽所需的元件說明如下。

合法監聽管理功能(LI Administration Function)

合法監聽管理功能為司法單位執行監聽的使用介面，司法單位藉由這個管理功能輸入監聽目標的資料、監聽時間，以及監聽回傳結果的要求格式。LI 管理功能的使用權必須嚴密控制。

調解設備(Mediation Device)

調解設備是合法監聽管理功能和真正執行監聽的元件之間的溝通橋樑，當它接收合法監聽管理功能傳來的監聽要求，它會指定監聽目標所在的 SIP 代理伺服器提供監聽相關資料，以及網路電話通話經過的合法監聽閘道器執行通話監聽的動作，調解設備收集代理伺服器回傳的監聽相關資料，再將監聽結果回傳給司法單位。

合法監聽閘道器(LI Gateway)

為了能監聽網路電話，我們在網路上新增一個元件叫做合法監聽閘道器，然後將受到監聽的通話都導向 LI Gateway，LI Ggateway 負責監聽通話內

容。首先金鑰管理元件會傳送監聽資料給合法監聽閘道器，這份資料包含了合法監聽的編號、通話雙方的 IP 位址、監聽結果回傳 IP 位址，接著合法監聽閘道器會跟通話雙方各自建立連線，此時通話雙方會開始傳送語音資料，合法監聽閘道器會把通話雙方傳送過來的語音資料複製，然後傳送到調解設備，由調解設備整合結果之後傳送到司法單位。

金鑰管理元件(Key Manager)

為了要讓網路電話既有安全性又可以合法監聽，我們加入了此金鑰管理元件。

金鑰管理元件的功能是負責產生網路電話通話加密的金鑰，並且管理所有網路電話通話使用的金鑰，當使用者成功建立網路電話之後，在還沒開始傳送語音資料之前，通話雙方會先跟金鑰管理元件建立安全的連線。建立安全連線之後，金鑰管理元件會產生一個通話加密金鑰，並透過安全連線傳送給通話雙方，通話雙方必須用這把金鑰加密通話。

4.4 系統安全性與可行性

4.4.1 安全性

我們提出的合法監聽系統架構中，金鑰管理元件和調解設備是最重要的一環，金鑰管理元件負責產生網路電話通話加密用的金鑰，並且管理所有目前在使用網路電話通話的金鑰，而調解設備則是負責要求監聽相關資訊和監聽通話內容的設備，所以這二種元件都需要有很高的安全性，並且屬於公正的第三方所擁有，這樣可以避免電信業者可以輕易的存取或控制這二種元件。

通話加密

在我們的合法監聽架構之下，所有網路電話的通話，都會被金鑰管理元件產生的金鑰加密，所以在傳送過程就算被有心人士取得，也無法知道裡面的內容，加密金鑰只有通話雙方，以及金鑰管理元件才知道。所以可以保證通話內容是安全的。

司法單位或電信業者無法單方面進行監聽

將監聽通話內容解密取得真正的通話內容以做為法庭上的證據，必須用到通話加密金鑰。但是為了防止司法單位，或電信業者沒有授權而任意監聽，本架構利用電信業者和司法單位的公開金鑰對通話加密金鑰做二次加密，解密的時候必須電信業者和司法單位的私密金鑰才足以解密。因此能達到防止司法單位或電信業者單方面的任意監聽。

4.4.2 可行性

我們提出的合法監聽系統架構，可以符合合法監聽的三項要求。第一項是不能讓監聽目標發現自己受到監聽，第二項是除了提供通話監聽內容之外，還要提供監聽相關資訊，第三項是如果通話內容經過加密的話，需要將加密的金鑰送給司法單位，讓司法單位可以把加密的通話內容解密。

不讓監聽目標發現

在我們的合法監聽架構之下，我們會有一台以上的合法監聽閘道器，這個設計有二個好處，一個就是可以混淆監聽目標的注意，另一個是可以分散通話，以達到負載平衡(load balance)的狀態。

當網路電話建立通話的時候，SIP 代理伺服器會將合法監聽閘道器的位址傳送給通話雙方，通話雙方各自與 LI Ggateway 建立連線。可是 SIP 代理伺服器每次給通話雙方的位址可能不一樣，這樣就可以防止監聽目標發現自己受到監聽。另外 SIP 代理伺服器可以根據合法監聽閘道器的使用狀態，來判斷要讓通話雙方使用哪一台閘道器，這樣就可以達到負載平衡的目標。

提供監聽相關資料

合法監聽的第二項要求，司法單位要求的監聽結果，可以分成三種，一種是只要監聽通話內容、一種是只要監聽相關資料、最後一種是二者都要，也就是說監聽通話內容和監聽相關資料都要傳送給司法單位，所以當司法單位要求監聽相關資料時，合法監聽架構需要可以提供。

在我們的合法監聽架構下，要提供監聽相關資訊給司法單位，監聽相關資訊指的是和監聽目標有相關的資訊，包含了建立這通網路電話所傳送的訊息、控制網路電話的訊息、時間流程、如果可以的話甚至地理位置也算在裡面，舉凡電話號碼、電腦 IP 位置、通話時間等等，都可以是監聽相關資訊。我們可以讓 SIP 代理伺服器來達成這個要求，因為每一通網路電話的建立、修改、刪除都會經過代理伺服器，所以可以從代理伺服器取得通話建立時間、通話結束時間、通話持續時間、甚至連打過哪些網路電話，哪些通話建立成功、哪些通話建立失敗等等資訊都可以從代理伺服器取得，等到被監聽的通話結束之後，代理伺服器會把監聽相關資訊結果回傳給調解設備，調解設備再把結果以司法單位要求的格式封裝，最後傳送給司法單位，因此我們的合法監聽架構可以符合第二項要求。

將通話加密金鑰送給司法單位

合法監聽的第三項要求，假如通話內容是由電信業者所加密的話，要讓司法單位有辦法解開加密的通話內容。採用的方法是，電信業者除了把加密過的通話內容傳送給司法單位，還要把加密通話用的金鑰傳送給司法單位，讓司法單位可以用這把金鑰解開加密的通話內容。

在我們的合法監聽架構下，只要讓金鑰管理元件把通話加密金鑰傳送給調解設備，調解設備再把通話加密金鑰傳送給司法單位，司法單位就可以用這把金鑰解開加密過的通話，達成第三項要求。

5. 系統模擬結果

5.1 模擬環境

我們模擬所使用的硬體方面，CPU 為 Intel Pentium-M 1.8 GHz 的筆記型電腦用 CPU，1GB 的 SDRAM。在軟體方面，使用的作業系統是 Microsoft Windows 2000 server，網路傳輸模擬所使用的模擬器為 Network Simulation 2，NS2 是跑在 Cygwin 上。

5.2 網路傳輸模擬

我們假設合法監聽閘道器為一台個人台腦，對外的頻寬為 100Mbps，我們想要模擬這台合法監聽閘道器在不同的語音編碼下，可以承受多少通監聽通話，而不會發生封包遺失(Packet lost)的情形。模擬的網路環境有 5 個網路節點(node)，路由器(router)0 和路由器 1 為網路電話封包來源，所有的網路電話都會經過這二台路由器，而傳送到合法監聽閘道器那邊，路由器 2 為合法監聽閘道器網路封包出去會經過的第一個路由器，所以所有的封包都會經過這台路由器，合法監聽閘道器連接路由器 2，路由器 3 為合法監聽閘道器傳送監聽結果給調解設備(MD)會經過的路由器，所有經過的連線傳送延遲(Link propagation delay)皆為 10ms，圖 8為模擬網路環境。

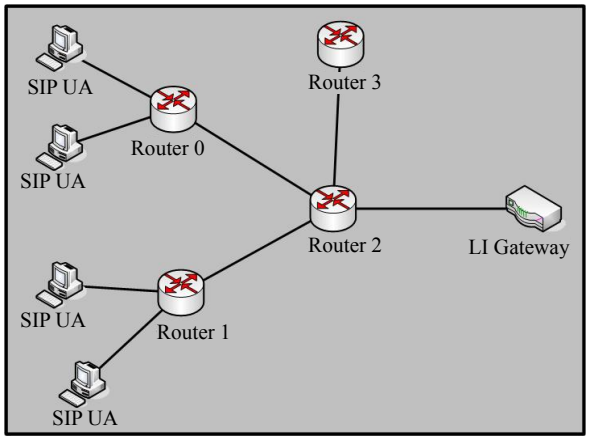

圖 8 模擬網路環境

在這裡我們模擬了 5 種由 ITU-T 所定義的聲音編碼方法：G.711、G.726、G.728、G.729、G.723.1，我們模擬網路電話的通話數跟封包遺失率的關係，從通話數 100 開始，一直模擬到通話數 1000，不過 G.711 在通話數 100 的時候還是有封包遺失，最後我們將模擬結果做成**表 3**。

每種聲音壓縮方法都有一個監聽通話數臨界點，當超過之後會開始發生封包遺失。在此論文所提出的監聽架構模擬中，封包遺失在同時監聽通話數少於 100 通時很少發生；如果採用 G.723.1 或 G.729 則監聽閘道器更可承受同時多達 500 通的監聽電話。

6. 結論

在本篇論文中，我們提出一套能提供合法監聽的網路電話架構，以思科(Cisco)公司所提出的合法監聽架構為基礎，再加入 SIP 網路協定和 Key Manager 以及 LI Gateway 合法監聽閘道器，讓以後提供 IP 網路電話服務也可以合乎法律的合法監聽要求。

最後我們對 LI Gateway 模擬不同的聲音編碼方法和不同的通話數對封包遺失率有什麼樣的關係。並從模擬結果得知合法監聽閘道器對每種聲音編碼方法的最大通話數。

表 3 監聽通話數與封包遺失率模擬結果

通話數	G.711 遺失率%	G.723.1 遺失率%	G.726 遺失率%	G.728 遺失率%	G.729 遺失率%
100	3.5	0	0	0	0
200	36.17	0	7.33	0	0
300	50.33	0	26.06	12.94	0
400	62.67	0	40.25	27.29	0
500	70.07	0	47.73	38.43	0
600	75.03	5.47	55.58	45.75	0
700	78.60	11.64	61.90	50.81	4.4
800	81.27	16.77	66.67	56.92	9.94
900	83.33	23.69	70.33	61.67	14.37
1000	85	29.63	73.30	65.5	19.32

參考文獻

[1]Baker, F., "Cisco Lawful Intercept Control MIB", Work in Progress, April 2004.

[2]Chia-Ming Sung; Ching-Cheng Lo; June-Hao Peng; Wen-Nung Tsai; “A study on VoIP Security”, International Computer Symposium, Dec. 2004, Page(s):1230 - 1237

[3]C. Déchaux and R. Scheller. What are GSM and DCS. Electrical Communication, 2nd Quarter 1993

[4]ETSI ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".

[5]ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

[6]ETSI TS 33.108 v6.7.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover Interface for Lawful Interception (Release 6).

[7]ETSI TS 101 331, Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies.

[8]ETSI TR 101 943: “Lawful Interception(LI); Concepts of Interception in a Generic Network Architecture”, October 2004.

[9]ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[10]ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G security;

Lawful interception architecture and functions (3GPP TS 33.107)".
[11]IETF, Fielding, R., et al, "RFC2616: Hypertext Transfer Protocol -- HTTP/1.1", June 1999.
[12]IETF, H. Schulzrinne, et al, “RFC1889: RTP: A transport Protocol for Real-Time Application”, January 1996.
[13]IETF, IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.
[14]IETF, Klensin, J., "RFC2821: Simple Mail Transfer Protocol", April 2001.
[15]IETF, Postel, J., et al, "RFC959: File Transfer Protocol", STD 9, October 1985.
[16]IETF, Rosenberg, J., et al, "RFC3261: SIP: Session Initiation Protocol", June 2002.
[17]IETF, RFC2327, SDP: session description protocol, 1998
[18]ITU-T Recommendation H.225.0. "Call Signaling Protocols And Media Stream Packetization For Packet-Based Multimedia Communication System", International Telecommunication Union, November 2000
[19]ITU-T Recommendation H.245. "Control Protocol For Multimedia Communication", International Telecommunication Union, July 2001
[20]ITU-T Recommendation H.248.1, Gateway Control Protocol: Version 2, May 2002.
[21]ITU-T Recommendation “H.323, Packet-based Multimedia Communications Systems”, International Telecommunication Union, Nov. 2000.
[22]Milanovic, A.; Srbljic, S.; Raznjevic, I.; Sladden, D.; Matosevic, I.; Skrobo, D.; “Methods for lawful interception in IP telephony networks based on H.323**”,** EUROCON 2003. Computer as a Tool. The IEEE Region 8 Volume 1, p22-24 Sept. 2003, Page(s):198 - 202 vol.1
[23]Torbjorn Nilsson. Toward a new era in mobile communications. http://193.78.100.33/ (Ericsson WWW server).