如何強化網路電話通訊雙方身份鑑別與通信資料不可否認性，已成為網路電話發展兩個重要議題。本研究在不修改現有通信架構下，實作具有錯誤回復機制 RTP 隱藏通道，用來攜帶身分識別資訊，解決身分鑑別與不可否認性問題。錯誤回復機制可以克服 RTP 封包遺失所造成隱藏資訊遺漏。相較於相關研究，本研究可以用較低成本提供網路電話使用者一個可選擇性身分鑑別安全機制。

1.緒論

以 TCP/UDP 為基礎網路電話(VoIP)，由於繼承基礎通信協定缺點，將蒙受冒用、中間人攻擊等威脅[7]。英國 Royal Mail 資訊安全長警告，不當使用網路電話應用軟體，可能讓企業暴露於駭客攻擊與惡意程式威脅中，更可能因此而洩露公司重要機密[4]。根據 IDC(2005)針對 2006 年亞太區（日本除外）資訊電信所做十大預測，身份鑑別與登入管理(Identity and access)將會是矚目焦點[6]。

整體 VoIP 的發展將由企業將帶動成長，如何透過身份識別與通信資料繫結(Binding)，確保通信不可否認性(non-repudiation)是網路電話商業發展另一個挑戰[12]。

1.1 研究背景

網路電話相關通信協定中，以 IETF 所制定 SIP(Session Initiation Protocol)占大多數。SIP 負責協調雙方開啟通信確認階段工作（call signaling)，媒體訊息串流傳遞則是透過 RTP(Real-time Transport Protocol)來進行。目前為止，研究網路電話中身份鑑別方法，都集中在利用 SIP 通信協定處理該類問題。本研究將利用 RTP 通信協定同時解決身分鑑別與不可否認性問題。研究中假設目前數位認證（Digital Certificate）機制已十分完善，本研究將不再深入探討使用者身份辨識合法性議題。

1.2 研究動機與目的

網路電話目前以 SIP/RTP 為基礎架構，由於 SIP 封包並未進行任何加密動作，使通信過程中身份與認證資訊很容易被網路封包搜集工具所偵測[7]。SIP 通信過程中可能經過許多不同主機與設備，要提供在 Internet 上達到 End to End 安全機制，仍存在許多有待克服與標準化議題。雖然有研究透過 RTP 進行身分鑑別，但利用 UDP 來傳送 RTP 封包，可能面臨封包遺失[3]，而造成隱藏資訊無法完整被傳遞問題。

本研究以 SIP/RTP 網路電話為背景，在不修改通信協定下，實作 RTP 上具錯誤回復資訊隱藏技術，用來攜帶可供身分識別資訊，解決身分鑑別與不可否認性問題。利用里德所羅門碼錯誤回復機制可以克服封包遺失所造成隱藏資訊遺漏。

2.文獻探討

本研究探討技術領域包括網路電話通話基礎通信協定、SIP 安全機制、QoS、資訊隱藏（Information Hiding）與 Error Correction 技術。

2.1 網路電話通話基礎通信協定

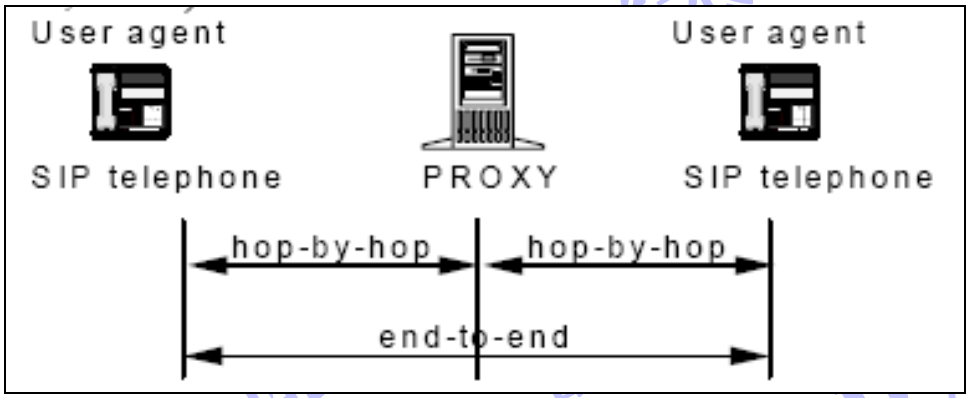
在網路電話相關通信協定中，SIP 通訊協定，已逐漸取代最初所發展 H.323。 3GPP 指出 SIP 是下一代網路關鍵通信協定[8]。SIP 負責建立發/受話雙方初始連線後，藉由 RTP 來達成語音影像傳輸。RTP 用來傳遞媒體資訊，利用時間戳記(Timestamp)，達到同步能力，序號用來決定是否有封包遺失等資訊。

RTP 可以用來傳送普通格式或已經被定義格式資訊。其中 1972 年 CCITT 所制定 PCM 標準 G.711 是

一個廣泛被使用網路語音電話格式，速率為 64kbit/s，相當於 12 bits 線性量化的非線性量化 μ 律或 A 律。

2.2 網路電話安全機制發展與分析

Rosenberg(2002 年)研究指出明文式 SIP 訊息會遭受到 Spoofing、Hijacking 與訊息被修改問題。Geneiatakis(2005)研究也發現惡意 SIP 訊息將導致不合法存取 [8]。SIP 安全架構可被分成兩類，分別是 End to End 與 hop by hop [10]。利用 SIP 建立通信階段保護是目前為止，網路電話發展核心問題與方向。



SIP 是一個發展中通信協定，特別是 Security 這個議題，在 2002 年 SIP RFC3261 定稿後，各種安全應用規範逐漸被產出。已提出安全機制中，提供相對安全選擇性方案，卻也隱含某些實現議題。Arkko(2003)也提出了，使用者應該有能力依據自己需求選擇需要的安全機制[8]。針對 SIP 所提出相關解決方案分析如下：

(1).HTTP Digest authentication： Ferguson and Schneier(2003)指出這樣的機制可能遭受到 man in the middle attacks、DoS。

(2).IP sec：在 Internet 運用上，會產生嚴重 Overhead。

(3).TLS 與 SIPS：缺乏 PKI 設施，造成在 Internet 上實現障礙。

(4).S/MIME：與 IPsec 一樣會造成 Overhead，也因為缺乏 PKI 設施，而形成在 Internet 上實現障礙。

由上面分析發現利用這些機制均存在實現 End to End 安全通道潛在成本考量，國際大廠對於網路電話與安全性解決方案仍處於發展階段，舉例而言：國際設備大廠 Juniper 就針對企業個別需求提出個別方案、Nortel 則將焦點放在 Intranet 與 VPN 上面。

2.3 QoS

對於 IP 語音 QoS 衡量上分兩個構面來討論，客觀方面包括四個方向，分別為建立時間、封包遺失率(Loss Rate)、抖動(Jitter 延遲變化)與點對點延遲（latency）[3]。主觀方面可直接以人類感受給分平均主觀評價等級(MOS)[3]進行衡量。

本研究中，影響 QoS 因素包括了：

(1). 利用 UDP 來傳送 RTP 封包，由於面臨封包遺失，將影響語音輸出品質。

(2).資訊隱藏會破壞語音原始資料，同時，實作資訊隱藏演算時間，可能進一步造成 RTP 封包延遲。

2.4 資訊隱藏(Information Hiding)

透過資訊隱藏技術，可以將認證(Authentication)資訊隱藏至標的物中，進行保護。資訊隱藏兩個重要特性為：不可感知（nonperceptual）與強健性（robustness）。

(2006)利用最低位元 (LSB)方法，將欲隱藏資訊隱藏至 G.711 語音資料取樣點最小位元中。觀測平均主觀評價等級來衡量此方法對語音品質影響程度，可以發現人耳無法辨識改變後差異[11]。 此方法可使原來音訊誤差不至於被擴大，而達到資訊隱藏目的。

2.5 Error detection and correction

錯誤回復，通常必須附加容錯資料(redundant data)，使遭受破壞或遺失資料，可以被還原。里德所羅門碼具有封包或位元缺損補償機能，早期被視為錯誤修正碼標準，運用於大量儲存系統中，用來處理成片干擾(brust) [13]，另一個著名應用，是 PDF417 二維條碼[4]。PDF417 可從受損條碼中讀回完整資料(Moore, 1994)，彈性容錯能力，提供不同回復能力，最高可達 50%。

里德所羅門原理將資料分成一個固定大小區塊，並透過有限場(finite field)所表示多項式係數來編碼[4]。里德所羅門碼區塊以 (n, k) 表示，n 代表編碼後每個 block symbol 數，k 是每個 block 被編碼原始資料，t 表示最多可以處理錯誤數，關係式為 n = k + 2t。解碼部分可表示為 r(x) = v(x) + e(x)，r(x)指接收端收到訊息，v(x) 是原始里德所羅門碼編碼，e(x)為雜訊，利用 v(x)所包含糾錯碼，可在容許錯誤數內，幫助求解回正確資訊。r(x)錯誤可分成兩類型， E 錯誤(Erasure Correction)，是由於 v(x)資訊遺失所造成，此類型為已知位置錯誤。T 錯誤(Error Correction)是由於 e(x) 造成 v(x)內含錯誤資訊，此類型錯誤回復需要求出資料發生錯誤位置並求出正解值。

3.研究設計

本研究利用里德所羅門糾錯功能，實作至具有資訊隱藏技術之 RTP 模組內。利用此模型來驗證資訊遭受封包遺失後回復效果。進一步評估與證明本研究架構可行性。

3.1 實驗系統架構

圖 2 為本研究系統架構，被請求端先將取樣語音訊號轉成 G.711 編碼。同時，要隱藏資訊先依里德所羅門碼資料區塊大小進行切割，並對每個區塊進行糾錯碼編碼與轉成 Bit Stream 後，以 LSB 方法依序隱藏至 RTP 封包中(圖 3)。請求端收到包含隱藏資訊 RTP 封包後，一方面將封包輸出成語音訊息，另一方面將隱藏資訊取出，並依序填回每個里德所羅門碼區塊，在面臨有限封包遺失與雜訊干擾情況下，糾錯碼用來進行錯資訊回復解碼，以回復遺失或錯誤資訊。

系統實作將利用 WinRTP(V2.1)模組與 Schifra Reed-Solomon ECC Library(V0.01)來完成系統模型建立。

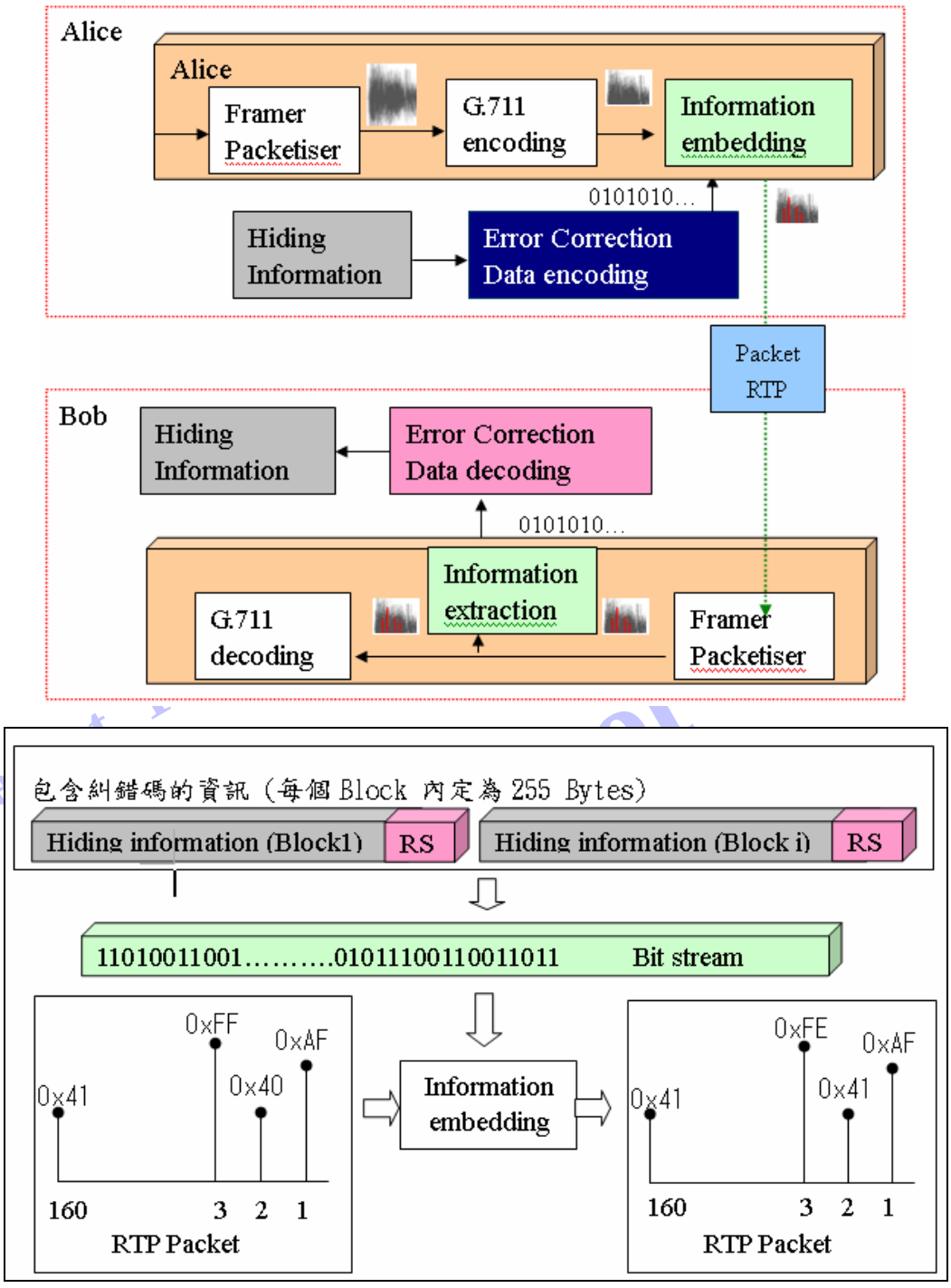


圖 1 資訊隱藏方法示意圖

3.2 系統溝通機制

研究系統中必須實作可以讓通訊雙方進行身分識別資訊交換溝通機制，來完成身份鑑別作業。通信雙方將透過交互傳送如表 1 隱藏控制資訊、參數與身份辨識資訊來完成身份鑑別作業交握，訊息溝通過程如圖 4 所示，雙方端點透過所設計的協定來進行控制訊號的交換，藉此啟動身份識別。

表 1 身份辨識作業溝通機制

請求端	被請求端	傳送碼
請求認證		控制資訊：CREQ
	傳送作業參數	控制資訊：CSTR 實驗相關參數。
接收參數		控制資訊：CACK
	傳送資料	控制資訊：D 隱藏資料長度(n)
資料接收		控制資訊：CDAT
	傳送完成	控制資訊：CEND
認證失敗		控制資訊：CROK
認證成功		控制資訊：CRNG

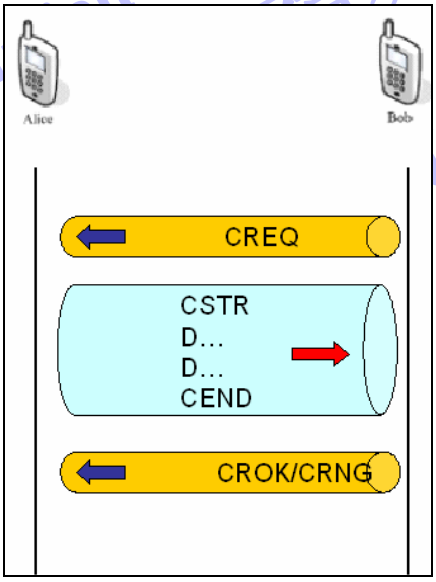


圖 2 隱藏資訊傳遞交握程序

3.3 實驗參數

表 2 說明針對本研究系統進行實驗相關參數。實驗將以 RTP Payload G.711 語音資訊為背景，進行身份辨識資訊隱藏。每個 RTP 封包含 160 個取樣點，每秒將傳送 50 個封包。由於 G.711 格式在封包遺失率達 10%時，聲音品質為可接受的最下限，因此實驗將以 10%封包遺失率為界限。實驗將以 LSB 方法實作資訊隱藏，固定傳送 1024Bytes 資訊，以調整糾錯碼長度與每個封包隱藏資訊長度來評估實驗系統績效值。

表 2 實驗參數資訊

實驗參數	選擇性
RTP Codec	G.711 A 律
RTP 長度	20ms

里德所羅門碼區塊長度	255 (Bytes)
資訊隱藏方法	1 (Bits):LSB
傳送資料量	1024 Bytes
封包遺失率極限值	10%
糾錯碼長度	16,32,64(Bytes)
資訊隱藏長度	5,10,15(Bytes)

3.4 研究系統評估要素

系統實驗中，必須進行評估要素包含：

(1).語音品質：資訊隱藏演算法，可能對語音處理產生延遲。聲音資訊內容由於被隱藏資訊破壞，也可能影響使用者對語音品質感覺。評估語音資訊隱藏造成主、客觀語音品質變異程度，將可用來了解實驗方法合理性。

(2).成本要素：研究透過資訊隱藏方法傳遞識別資訊，由於隱藏資訊容量限制，研究將必須耗用時間成本獲取安全性。實驗將了解不同傳輸環境造成傳輸時間變異程度，提供給使用者，用來選擇不同安全機制所必須耗用成本比較。依據實驗參數，可以預估本實驗固定傳輸 1024Bytes 資訊量傳輸時間如表 3。

(3).回復績效：不同糾錯等級會影響資料傳輸長度，也會影響實驗承受封包遺失程度。(表 4)

表 3 資訊隱藏傳輸時間預測

糾錯碼長度 (Bytes)	單一封包資訊隱藏量(Bytes)	傳送區塊數	單一區塊封包數	預估時間 (ms)
16,32	5	5	51	5100
16,32	10	5	26	2600
16,32	15	5	17	1700
64	5	6	51	6120
64	10	6	26	3120
64	15	6	17	2040

表 4 糾錯等級承受封包遺失門檻預估

糾錯碼長度 Bytes	資訊隱藏長度 Bytes	傳送資料量 Bytes	單一區塊封包數(個)	遺失封包門檻值(個)	可承受封包遺失機率
16	5	1275	51	3	5.9%
16	10	1275	26	1	3.8%
16	15	1275	17	1	5.9%
32	5	1275	51	6	11.8%
32	10	1275	26	3	11.5%
32	15	1275	17	2	11.8%
64	5	1530	51	12	23.5%

64	10	1530	26	6	23.1%
64	15	1530	17	4	23.5%

4.實驗與評估

4.1 系統實作展示

本研究透過系統實作測試績效平台，透過此一績效平台進行可行性與最佳門檻值測試，系統主實驗操作區如圖 5，紅色區塊標示受話方 SIP URL 及身份辨識操作結果。綠色區塊表示 SIP 通信建立過程，包括了 INVITE、100 Trying、180Ringing、200 OK 與 ACK。藍色區塊表示所收到流程控制資訊包括 CREQ、CACK 與 CROK 等資訊。操作區如紫色區塊，可用來撥號(Dial)、允許接聽(Accept)拒絕接聽(Reject)、結束通話(Bye)、身份辨識與查看 Log(View Log)。左下方黑色區塊用來顯示接收封包統計資訊，如圖 5 所示，本系統收到 1200 個 RTP 封包，遺失 27 個封包，遺失率為 2.25%。

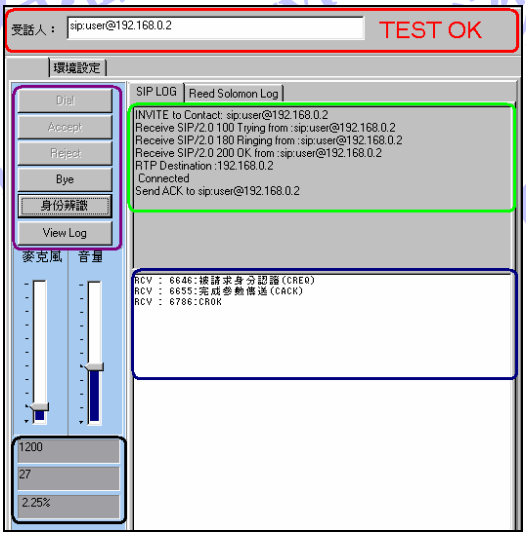


圖 3 實驗系統操作區畫面

實驗 Log 統計功能用來紀錄實驗相關設定參數與績效數據，例如圖 6 所示，本次實驗中第三個里德所羅門碼區塊(Block # 2)中編號第 14、15 個封包遺失，但這無礙於後續辨識，因為里德所羅門區塊糾錯碼提供復原能力，將兩個遺失封包 30Bytes 資料順利回復。資料傳送時間花費 1.793 秒。

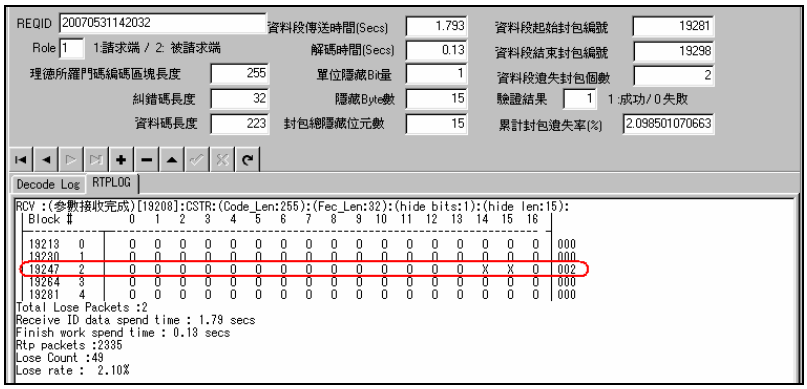


圖 4 實驗 Log 統計功能畫面

4.2 平台測試與評估效能

本研究目標以建構一個資訊隱藏通道，提供使用者作為可選擇性安全機制。為完成這樣目標，必須進行相關要素評估條件與實驗結果如下：

4.2.1 語音品質評估

客觀語音品質評估利用 FlukeNetwork Protocol Expert 語音品質量測工具，對區域網路與廣域網路上兩組端點進行對照組(不實施身份辨識)與實驗組(實施身份辨識) 進行語音品質實驗數據蒐集，來了解研究系統對品質影響變異程度。由表 5 證明本研究系統對語音品質(延遲)並無顯著影響，語音品質衡量指標(MQS、R Factor)也在可接受範圍(MQS > 3.6、R Factor > 70)。

主觀語音品質評估，是用來了解實施資訊隱藏技術後，使用者對於語音品質主觀感覺。本實驗透過 10 位使用者對採用 LSB 方法後語音進行平均主觀評價等級(MOS)評估，由評估所得數據 3.94(MOS 良:3.5~4)了解，實驗所採 LSB 對語音主觀品質影響有限。

表 5 客觀語音品質評估數據表

	LAN		WAN	
	對照組	實驗組	對照組	實驗組
R Factor	93	93	88	87
MQS	4.18	4.17	4.04	4.03
Packets(Rec.)	6208	5483	6979	6673
Lost Rate	0.00	0.00	1.8%	1.7%
Delay (ms)	3.74	4.97	65.02	43.39
Jitter(ms)	2.28	6.16	4.16	6.17

4.2.2 系統傳輸成本評估

系統傳輸成本評估利用區域網路與廣域網路(校園網路對 8M/512K ADSL)兩個環境，來對不同實驗組合進行傳輸成本評估，透過表 6 時間測量表與表 3 預估值比較，在區域網路上兩端點，傳輸成本差異約在 6%。廣域網路上兩端點與預估值差異擴大到 25%~46%。

由語音品質實驗了解到廣域網路相對於區域網路有更多延遲，延遲因素可能是造成廣域網路必須要更多時間來實作身份辨識溝通機制，因此廣域網路傳輸成本較區域網路嚴重。

表 6 身份辨識時間測量表 (unit:ms)

糾錯碼長度 Bytes	資訊隱藏長度(Bytes)					
	5 Bytes		10 Bytes		15 Bytes	
	LAN	WAN	LAN	WAN	LAN	WAN
16	5402	6540	2774	3601	1811	2432
32	5402	6806	2748	3528	1807	2483

64	6441	7653	3276	4102	2157	2796

4.2.3 傳輸資訊回復績效

回復績效實驗將透過校園網路(100M)對 ADSL(8M/512K)寬頻網路進行雙向身份辨識實驗，依據資訊隱藏長度(5,10,15Bytes)與糾錯碼長度(16,32,64Bytes)組合，每組實驗進行 50 次身份辨識作業。利用 FlukeNetwork PE 語音品質工具蒐集資訊發現，在(512K[被認證端]->100M)環境中，16Bytes 糾錯碼，20 分鐘封包遺失率為 2.3%，瞬間最高遺失率為 3.91%(30 秒)，450 次身份辨識作業中，遭遇 260(58%)次封包遺失，透過糾錯碼機制，可以回復 144 次有封包遺失情形，利用 32Bytes 糾錯碼，資訊回復成功率最低具有 78%(隱藏長度為 15Bytes)，利用 64Bytes 糾錯碼，資訊回復成功率最低為 90%(隱藏長度為 10Bytes)。在(100M[被認證端]->8M)環境中，20 分鐘封包遺失率為 1.7%，瞬間最高遺失率為 3.91%(30 秒)，450 次身份辨識作業中，遭遇 204(45%)次封包遺失狀況，透過糾錯碼機制，可以回復 200 次有封包遺失情形，利用 16Bytes 糾錯碼，資訊回復成功率最低達到 96%(隱藏長度為 10,15Bytes)，利用 32、64Bytes 糾錯碼，資訊回復成功率可實現 100%。相關數據參考表 7。

表 7 身份辨識資訊回復成功率統計表(各 50 次)

實驗環境	糾錯碼長度	資訊隱藏長度(Bytes)		
		5	10	15
512k -> 100M	16	38.0%	32.0%	64.0%
	32	92.0%	84.0%	78.0%
	64	96.0%	90.0%	94.0%
100M -> 8M	16	100.0%	96.0%	96.0%
	32	100.0%	100.0%	100.0%
	64	100.0%	100.0%	100.0%

5. 結論與未來研究發展

本實驗評估結果顯示，研究系統在 RTP 模組中加入糾錯碼與資訊隱藏機制，使實作隱藏通道具有錯誤回復機能，確實能有效克服傳輸過程封包遺失問題，在較低寬頻環境中，利用 64Bytes 糾錯碼，成功回復率達 90%以上，在較高寬頻環境中，利用 32Bytes 糾錯碼，成功回復率達 100%。實驗同時證明本研究方法對於語音品質影響並不顯著。因此，本研究方法可以提供一個可選擇性安全機制，透過隱藏資訊傳遞，來強化使用者鑑別與不可否認性價值。

本研究也引發某些議題，可作為未來研究發展參考：

(1).演算法改進：分析回復失敗數據發現(圖 7)，研究採用依序隱藏演算法對於連續封包遺失承受力不足，必須利用較長糾錯碼來提高單一區塊封包遺失門檻(黃線)，如何改善演算法，分散封包遺失風險，使研究架構不受區塊遺失封包門檻限制，達到利用傳輸較少糾錯碼達到更佳回復率，假設里德所羅門碼區塊編號為 i，n 為必要傳送區塊數，Zi(b,f,h)表示單一區塊遺失封包個數，每個區塊長度表示為 b，糾錯碼長度條件表示為 f，隱藏資訊長度表示為 h，每個區塊遺失封包門檻個數表示為 P(b,f,h) ，目前演算法所造成回復失敗公式可表示如(式)1，只要其中有一個區塊封包遺失個數大於區塊遺失封包門檻值就會造成回復失敗。可以被檢討改進公式如(式)2，如能尋找符合此條件式，系統在頻寬變窄情況下，預期辨識率成功率可以再提高，相關演算法改進，是本研究再可深入探討議題。

$$MAX_{i=0}^{n-1}(Z_{i(b,f,h)}) > P_{(b,f,h)} \quad \text{(式) 1}$$

$$\sum_{i=0}^{n}(Z_{i(b,f,h)} > \sum_{i=0}^{n}(P_{(b,f,h)}) \ ) \quad \text{(式) 2}$$

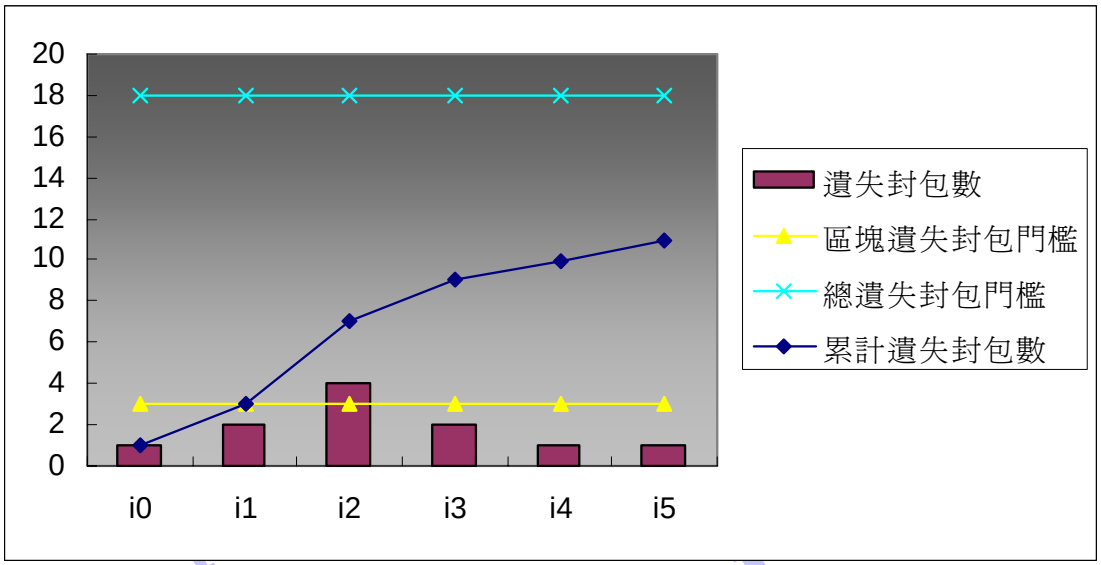


圖 5 資訊隱藏傳輸失敗門檻示意圖，里德所羅門碼區塊(255, 191)

(2).完整架構研究：本研究以探討隱藏通道作業為主，架構中並未實作後續身份辨識機制，未來可加入此議題，以補充研究完整性。

(3).多元網路環境測試：本研究回復績效實驗利用單一廣域網路完成數據蒐集，面對多元網路環境，未來希望能夠利用更多不同網路環境來測量影響績效因素，使本研究架構可適用各種不同網路環境。

Acknowledgement

This work was supported in part by TWISC@NCKU, National Science Council under the Grants NSC 96-2219-E-006-009.