如何强化网路电话通讯双方身份鉴别与通信资料不可否认性，已成为网路电话发展兩个重要议题。本研究在不修改现有通信架构下，实作具有错误回復机制RTP隐藏通道，用來携带身分識別信息，解决身分鉴别与不可否认性问题。错误回復机制可以克服RTP封包遗失所造成隐藏信息遗漏。相较于相关研究，本研究可以用较低成本提供网路电话使用者一个可选择性身分鉴别安全机制。

1.绪論

以TCP/UDP为基础网路电话(VoIP)，由于继承基础通信协议缺点，将蒙受冒用、中间人攻击等威胁[7]。英国Royal Mail信息安全长警告，不当使用网路电话应用软件，可能让企业暴露于黑客攻击与恶意程序威胁中，更可能因此而泄露公司重要机密[4]。根据IDC(2005)针对2006年亚太区（日本除外）信息电信所做十大预测，身份鉴别与登入管理(Identity and access)将会是瞩目焦点[6]。

整体VoIP的发展将由企业将带动成长，如何透过身份識別与通信资料系结(Binding)，确保通信不可否认性(non-repudiation)是网路电话商业发展另一个挑战[12]。

1.1研究背景

网路电话相关通信协议中，以IETF所制定SIP(Session Initiation Protocol)占大多數。SIP负责协调双方开启通信确认阶段工作（call signaling），媒体讯息串流传递则是透过RTP(Real-time Transport Protocol)來进行。目前为止，研究网路电话中身份鉴别方法，都集中在利用SIP通信协议处理该類问题。本研究将利用RTP通信协议同时解决身分鉴别与不可否认性问题。研究中假设目前數位认证（Digital Certificate）机制已十分完善，本研究将不再深入探讨使用者身份辨識合法性议题。

1.2研究动机与目的

网路电话目前以SIP/RTP为基础架构，由于SIP封包并未进行任何加密动作，使通信过程中身份与认证信息很容易被网路封包搜集工具所侦测[7]。SIP通信过程中可能经过许多不同主机与设备，要提供在Internet上达到 End to End 安全机制，仍存在许多有待克服与标准化议题。虽然有研究透过RTP进行身分鉴别，但利用UDP來传送RTP封包，可能面臨封包遗失[3]，而造成隐藏信息无法完整被传递问题。

本研究以SIP/RTP网路电话为背景，在不修改通信协议下，实作RTP上具错误回復信息隐藏技术，用來携带可供身分識別信息，解决身分鉴别与不可否认性问题。利用里德所羅门码错误回復机制可以克服封包遗失所造成隐藏信息遗漏。

2.文献探讨

本研究探讨技术領域包括网路电话通话基础通信协议、SIP安全机制、QoS、信息隐藏（Information Hiding）与Error Correction技术。

2.1网路电话通话基础通信协议

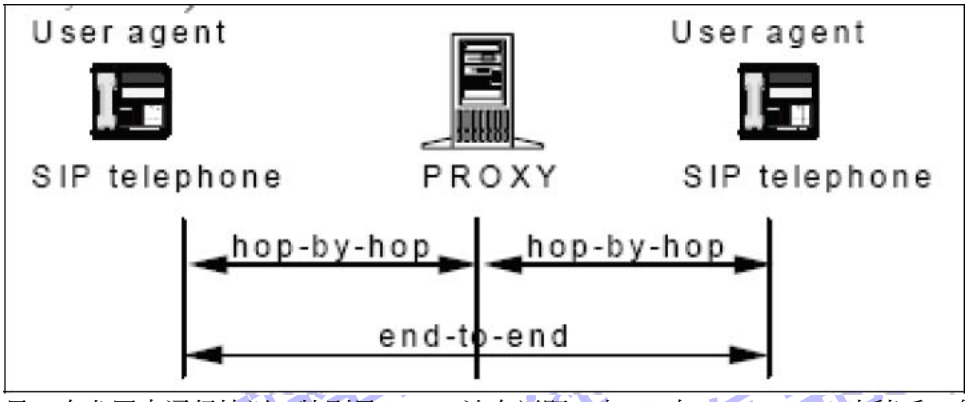
在网路电话相关通信协议中，SIP通讯协议，已逐渐取代最初所发展H.323。 3GPP指出SIP是下一代网路关键通信协议[8]。SIP负责建立发/受话双方初始連线后，藉由 RTP 來达成语音影像传输。RTP用來传递媒体信息，利用时间戳记(Timestamp)，达到同步能力，序号用來决定是否有封包遗失等信息。

RTP可以用來传送普通格式或已经被定义格式信息。其中1972年CCITT所制定PCM标准G.711是一个广泛被使用网路语音电话格式，速率为64kbit/s，相当于12 bits线性量化的非线性量化μ律或A律。

2.2 网路电话安全机制发展与分析

Rosenberg(2002年)研究指出明文式SIP 讯息会遭受到Spoofing、Hijacking与讯息被修改问题。Geneiatakis(2005)研究也发现恶意SIP 讯息将导致不合法存取 [8]。SIP安全架构可被分成兩類，分別

是 End to End 与 hop by hop [10]。利用SIP建立通信阶段保护是目前为止，网路电话发展核心问题与方向。



SIP是一个发展中通信协议，特别是Security这个议题，在2002年SIP RFC3261定稿后，各种安全应用规范逐渐被产出。已提出安全机制中，提供相对安全选择性方案，却也隐含某些实现议题。Arkko(2003)也提出了，使用者应该有能力依据自己需求选择需要的安全机制[8]。针对SIP所提出相关解决方案分析如下：

(1).HTTP Digest authentication： Ferguson and Schneier(2003)指出这样的机制可能遭受到 man in the middle attacks、DoS。

(2).IP sec：在Internet运用上，会产生严重Overhead。

(3).TLS与SIPS：缺乏PKI设施，造成在Internet上实现障碍。

(4).S/MIME：与 IPsec 一样会造成Overhead，也因为缺乏PKI设施，而形成在Internet上实现障碍。

由上面分析发现利用这些机制均存在实现End to End 安全通道潜在成本考量，国际大厂对于网路电话与安全性解决方案仍处于发展阶段，举例而言：国际设备大厂Juniper就针对企业个别需求提出个别方案、Nortel则将焦点放在Intranet与VPN上面。

2.3 QoS

对于IP语音 QoS 衡量上分两个构面來讨論，客观方面包括四个方向，分别为建立时间、封包遗失率(Loss Rate)、抖动(Jitter 延迟变化)与点对点延迟（latency）[3]。主观方面可直接以人類感受给分平均主观评价等级(MOS)[3]进行衡量。

本研究中，影响QoS因素包括了：

(1). 利用UDP來传送RTP封包，由于面臨封包遗失，将影响语音输出质量。

(2).信息隐藏会破坏语音原始资料，同时，实作信息隐藏演算时间，可能进一步造成RTP封包延迟。

2.4 信息隐藏(Information Hiding)

透过信息隐藏技术，可以将认证(Authentication)信息隐藏至标的物中，进行保护。信息隐藏兩个重要特性为：不可感知（nonperceptual）与强健性（robustness）。

(2006)利用最低位 (LSB)方法，将欲隐藏信息隐藏至G.711语音资料取样点最小位中。观测平均主观评价等级來衡量此方法对语音质量影响程度，可以发现人耳无法辨識改变后差異[11]。 此方法可使原來音讯误差不至于被扩大，而达到信息隐藏目的。

2.5 Error detection and correction

错误回復，通常必须附加容错资料(redundant data)，使遭受破坏或遗失资料，可以被还原。里德所羅门码具有封包或位缺损补偿机能，早期被视为错误修正码标准，运用于大量储存系统中，用來处理成片干扰(brust) [13]，另一个著名应用，是PDF417二维条形码[4]。PDF417可从受损条形码中讀回完整资料(Moore, 1994)，弹性容错能力，提供不同回復能力，最高可达50%。

里德所羅门原理将资料分成一个固定大小区块，并透过有限场(finite field)所表示多项式系數來

编码[4]。里德所羅门码区块以 (n, k) 表示，n 代表编码后每个block symbol 數，k 是每个block 被编码原始资料，t 表示最多可以处理错误數，关系式为 n = k + 2t。译码部分可表示为r(x) = v(x) + e(x)，r(x)指接收端收到讯息，v(x) 是原始里德所羅门码编码，e(x)为噪声，利用v(x)所包含纠错码，可在容许错误數內，帮助求解回正确信息。r(x)错误可分成兩類型， E错误(Erasure Correction)，是由于v(x)信息遗失所造成，此類型为已知位置错误。T错误(Error Correction)是由于e(x) 造成v(x)內含错误信息，此類型错误回復需要求出资料发生错误位置并求出正解值。

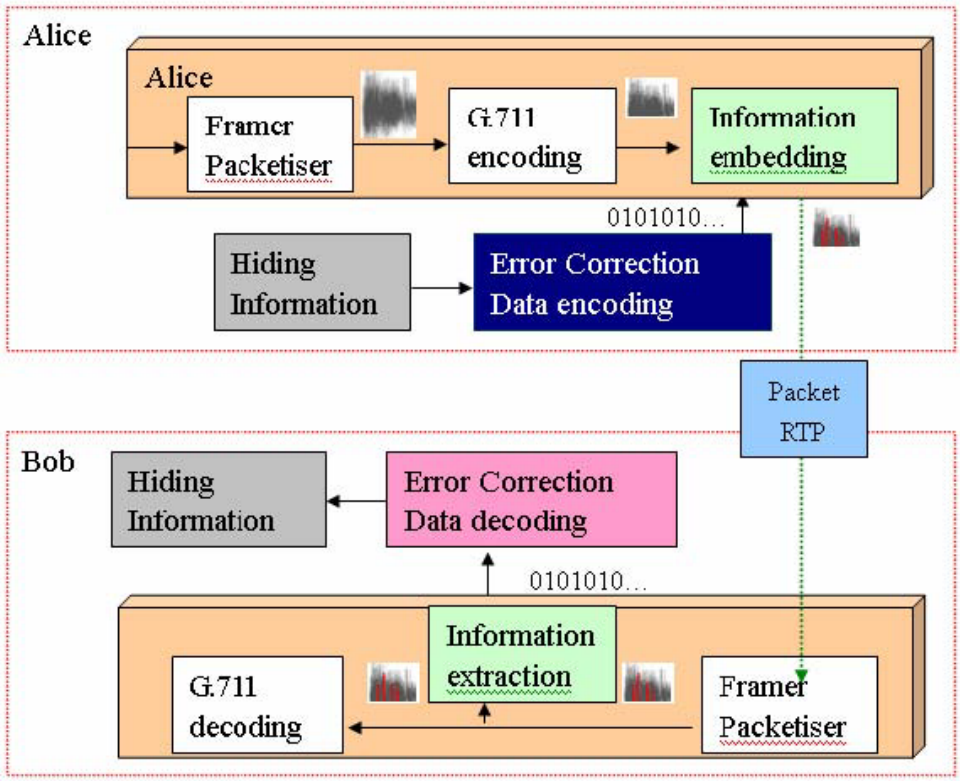
3.研究设计

本研究利用里德所羅门纠错功能，实作至具有信息隐藏技术之RTP模块內。利用此模型來验证信息遭受封包遗失后回復效果。进一步评估与证明本研究架构可行性。

3.1 实验系统架构

图2为本研究系统架构，被请求端先将取样语音讯号转成G.711编码。同时，要隐藏信息先依里德所羅门码资料区块大小进行切割，并对每个区块进行纠错码编码与转成Bit Stream后，以LSB方法依序隐藏至RTP 封包中(图3)。请求端收到包含隐藏信息RTP封包后，一方面将封包输出成语音讯息，另一方面将隐藏信息取出，并依序填回每个里德所羅门码区块，在面臨有限封包遗失与噪声干扰情况下，纠错码用來进行错信息回復译码，以回復遗失或错误信息。

系统实作将利用WinRTP(V2.1)模块与Schifra Reed-Solomon ECC Library(V0.01)來完成系统模型建立。



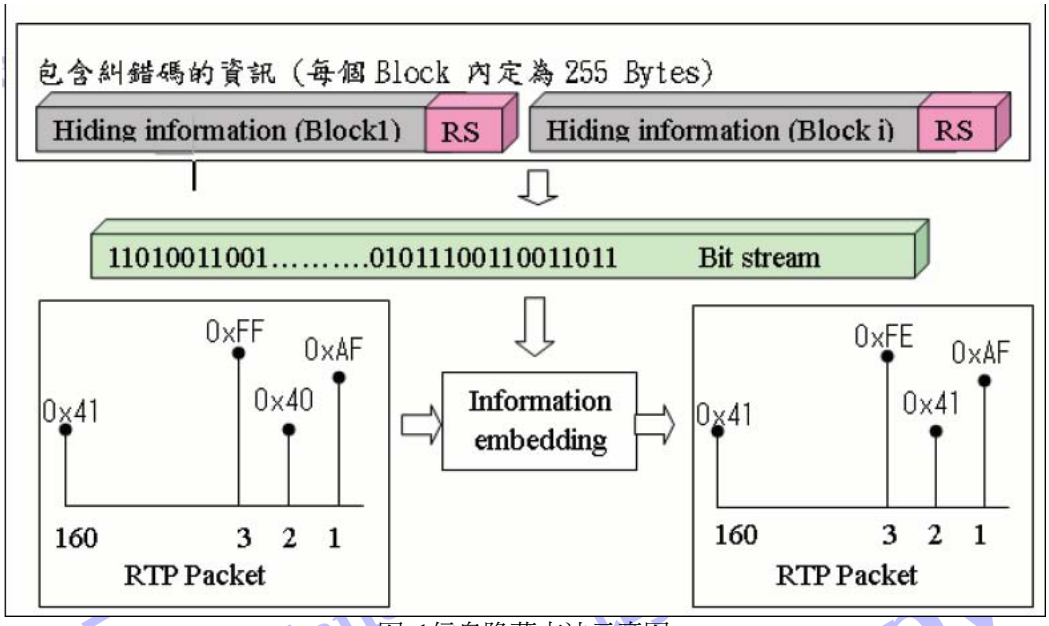


图 1信息隐藏方法示意图

3.2 系统沟通机制

研究系统中必须实作可以让通讯双方进行身分識別信息交换沟通机制，來完成身份鉴別作业。通信双方将透过交互传送如表1隐藏控制信息、参數与身份辨識信息來完成身份鉴別作业交握，讯息沟通过程如图4所示，双方端点透过所设计的协议來进行控制讯号的交换，藉此启动身份識別。

表 1 身份辨識作业沟通机制

请求端	被请求端	传送码
请求认证		控制信息：CREQ
	传送作业参數	控制信息：CSTR 实验相关参數。
接收参數		控制信息：CACK
	传送资料	控制信息：D 隐藏资料长度(n)
资料接收		控制信息：CDAT
	传送完成	控制信息：CEND
认证失败		控制信息：CROK
认证成功		控制信息：CRNG

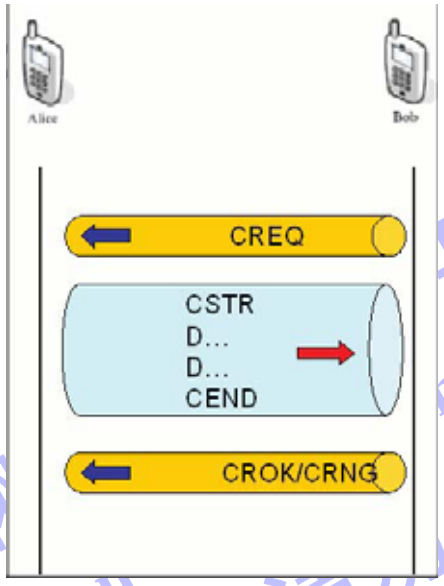


图 2隐藏信息传递交握程序

3.3 实验参數

表2說明针对本研究系统进行实验相关参數。实验将以RTP Payload G.711语音信息为背景，进行身份辨識信息隐藏。每个RTP封包含160个取样点，每秒将传送50个封包。由于G.711格式在封包遺失率达10%时，声音质量为可接受的最下限，因此实验将以10%封包遺失率为界限。实验将以LSB方法实作信息隐藏，固定传送1024Bytes信息，以调整纠错码长度与每个封包隐藏信息长度來评估实验系统绩效值。

表 2实验参數信息

实验参數	选择性
RTP Codec	G.711 A律
RTP 长度	20ms
里德所羅门码区块长度	255 (Bytes)
信息隐藏方法	1 (Bits):LSB
传送资料量	1024 Bytes
封包遺失率极限值	10%
纠错码长度	16,32,64(Bytes)
信息隐藏长度	5,10,15(Bytes)

3.4 研究系统评估要素

系统实验中，必须进行评估要素包含：

(1).语音质量：信息隐藏算法，可能对语音处理产生延迟。声音信息内容由于被隐藏信息破坏，也可能影响使用者对语音质量感觉。评估语音信息隐藏造成主、客观语音质量变異程度，将可用來了解实验方法合理性。

(2).成本要素：研究透过信息隐藏方法传递識别信息，由于隐藏信息容量限制，研究将必须耗用时间成本获取安全性。实验将了解不同传输环境造成传输时间变異程度，提供给使用者，用來选择不同安全机制所必须耗用成本比较。依据实验参數，可以预估本实验固定传输1024Bytes信息量传输时间如表3。

(3).回復绩效：不同纠错等级会影响资料传输长度，也会影响实验承受封包遗失程度。(表4)

表 3信息隐藏传输时间预测

纠错码长度 (Bytes)	单一封包信息隐藏量 (Bytes)	传送区块數	单一区块封包數	预估时间 (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纠错等级承受封包遗失门坎预估

纠错码长度 Bytes	信息隐藏长度Bytes	传送资料量 Bytes	单一区块封包數(个)	遗失封包门坎值(个)	可承受封包遗失机率
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.实验与评估

4.1 系统实作展示

本研究透过系统实作测试绩效平台，透过此一绩效平台进行可行性与最佳门坎值测试，系统主实验操作区如图5，红色区块标示受话方SIP URL及身份辨識操作结果。綠色区块表示SIP通信建立过程，包括了INVITE、100 Trying、180Ringing、200 OK与ACK。藍色区块表示所收到流程控制信息包括CREQ、CACK与CROK等信息。操作区如紫色区块，可用來拨号(Dial)、允许接听(Accept)拒绝接听(Reject)、结束通话(Bye)、身份辨識与查看Log(View Log)。左下方黑色区块用來显示接收封包统计信息，如图5所示，本系统收到1200个RTP封包，遗失27个封包，遗失率为2.25%。

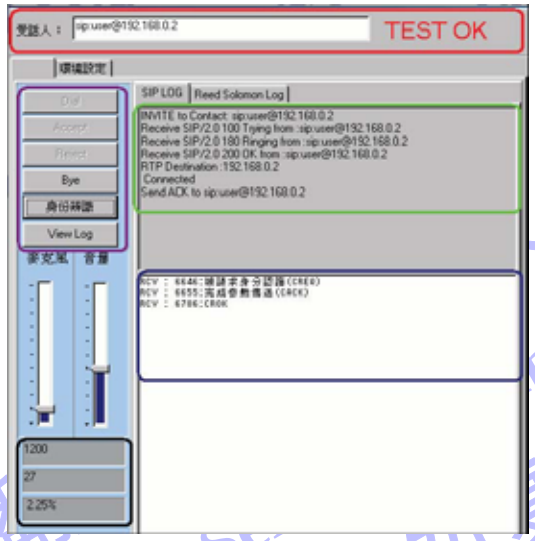


图 3实验系统操作区画面

实验Log统计功能用來纪錄实验相关设定参數与绩效數据，例如图6所示，本次实验中第三个里德所羅门码区块(Block # 2)中编号第14、15个封包遗失，但这无碍于后续辨識，因为里德所羅门区块纠错码提供復原能力，将兩个遗失封包30Bytes资料顺利回復。资料传送时间花费1.793秒。

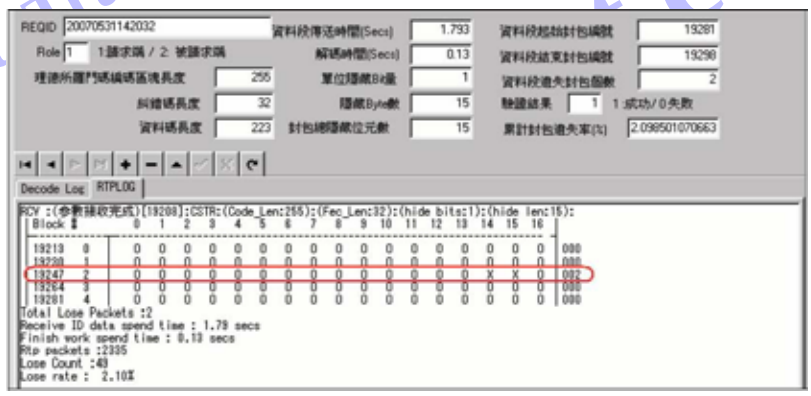


图 4 实验Log统计功能画面

4.2 平台测试与评估效能

本研究目标以建构一个信息隐藏信道，提供使用者作为可选择性安全机制。为完成这样目标，必须进行相关要素评估条件与实验结果如下：

4.2.1 语音质量评估

客观语音质量评估利用FlukeNetwork Protocol Expert语音质量量测工具，对区域网路与广域网路上兩组端点进行对照组(不实施身份辨識)与实验组(实施身份辨識) 进行语音质量实验數据搜集，來了解研究系统对质量影响变異程度。由表5证明本研究系统对语音质量(延迟)并无显著影响，语音质量衡量指针(MQS、R Factor)也在可接受范围(MQS > 3.6、R Factor > 70)。

主观语音质量评估，是用來了解实施信息隐藏技术后，使用者对于语音质量主观感觉。本实验透过10位使用者对采用LSB方法后语音进行平均主观评价等级(MOS)评估，由评估所得数据3.94(MOS良:3.5~4)了解，实验所采LSB对语音主观质量影响有限。

表 5客观语音质量评估數据表

	LAN		WAN	
	对照组	实验组	对照组	实验组
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 系统传输成本评估

系统传输成本评估利用区域网路与广域网路(校园网路对8M/512K ADSL)两个环境，來对不同实验组合进行传输成本评估，透过表6时间测量表与表3预估值比较，在区域网路上兩端点，传输成本差異约在6%。广域网路上兩端点与预估值差異扩大到25%~46%。

由语音质量实验了解到广域网路相对于区域网路有更多延迟，延迟因素可能是造成广域网路必须要更多时间來实作身份辨識沟通机制，因此广域网路传输成本较区域网路严重。

表 6身份辨識时间测量表 (unit:ms)

纠错码长度 Bytes	信息隐藏长度(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 传输信息回復绩效

回復绩效实验将透过校园网路(100M)对ADSL(8M/512K)宽带网路进行双向身份辨識实验，依据信息隐藏长度(5,10,15Bytes)与纠错码长度(16,32,64Bytes)组合，每组实验进行50次身份辨識作业。利用FlukeNetwork PE语音质量工具搜集信息发现，在(512K[被认证端]->100M)环境中，16Bytes纠错码，20分钟封包遗失率为2.3%，瞬间最高遗失率为3.91%(30秒)，450次身份辨識作业中，遭遇260(58%)次封包遗失，透过纠错码机制，可以回復144次有封包遗失情形，利用32Bytes纠错码，信息回復成功率最低具有78%(隐藏长度为15Bytes)，利用64Bytes纠错码，信息回復成功率最低为90%(隐藏长度为10Bytes)。在(100M[被认证端]->8M)环境中，20分钟封包遗失率为1.7%，瞬间最高遗失率为3.91%(30秒)，450次身份辨識作业中，遭遇204(45%)次封包遗失狀况，透过纠错码机制，可以回復200次有封包遗失情形，利用16Bytes纠错码，信息回復成功率最低达到96%(隐藏长度为10,15Bytes)，利用32、64Bytes纠错码，信息回復成功率可实现100%。相关数据参考表7。

表 7 身份辨識信息回復成功率统计表(各50次)

实验环境	纠错码长度	信息隐藏长度(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.结論与未來研究发展

本实验评估结果显示，研究系统在RTP模块中加入纠错码与信息隐藏机制，使实作隐藏通道具有错误回復机能，确实能有效克服传输过程封包遗失问题，在较低宽带环境中，利用64Bytes纠错码，成功回復率达90%以上，在较高宽带环境中，利用32Bytes纠错码，成功回復率达100%。实验同时证明本研究方法对于语音质量影响并不显著。因此，本研究方法可以提供一个可选择性安全机制，透过隐藏信息传递，來强化使用者鉴别与不可否认性价値。

本研究也引发某些议题，可作为未來研究发展参考：

(1).算法改进：分析回復失败数据发现(图7)，研究采用依序隐藏算法对于連续封包遗失承受力不足，必须利用较长纠错码來提高单一区块封包遗失门坎(黄线)，如何改善算法，分散封包遗失风险，使研究架构不受区块遗失封包门坎限制，达到利用传输较少纠错码达到更佳回復率，假设里德所羅门码区块编号为i，n为必要传送区块數，Zi(b,f,h)表示单一区块遗失封包个數，每个区块长度表示为b，纠错码长度条件表示为f，隐藏信息长度表示为h，每个区块遗失封包门坎个數表示为P(b,f,h) ，目前算法所造成回復失败公式可表示如(式)1，只要其中有一个区块封包遗失个數大于区块遗失封包门坎值就会造成回復失败。可以被检讨改进公式如(式)2，如能寻找符合此条件式，系统在频宽变窄情况下，预期辨識率成功率可以再提高，相关算法改进，是本研究再可深入探讨议题。

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

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

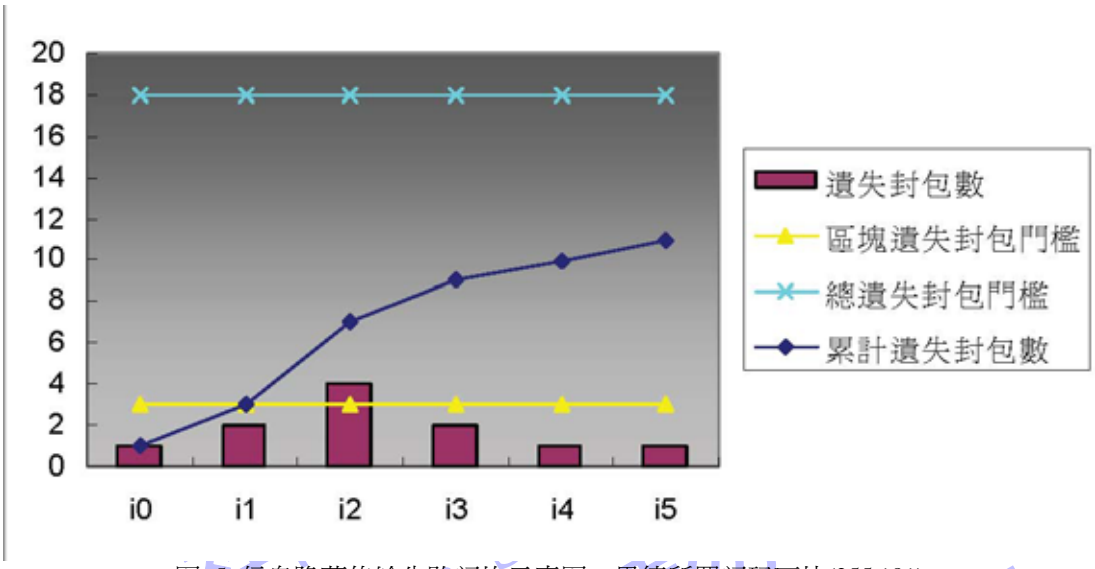


图 5 信息隐藏传输失败门坎示意图，里德所羅门码区块(255,191)

(2).完整架构研究：本研究以探讨隐藏信道作业为主，架构中并未实作后续身份辨識机制，未來可加入此议题，以补充研究完整性。

(3).多元网路环境测试：本研究回復绩效实验利用单一广域网路完成數据搜集，面对多元网路环境，未來希望能够利用更多不同网路环境來测量影响绩效因素，使本研究架构可适用各种不同网路环境。

Acknowledgement

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