數位版權管理系統之高可靠度金鑰傳送機制之研究

黎明富　　吳俊輝
私立長庚大學電機工程學系
mfli@mail.cgu.edu.tw

摘要

數位版權管理(Digital Rights Management，DRM)乃是數位多媒體系統重要的一環。因為數位內容必須經由數位版權管理的運作，才可能受到安全的保護，而相關的智慧財產權(Intellectual Property)也才能獲得有效的保障。因此，本論文將針對數位內容的數位版權管理(Digital Right Management)技術做深入的探討與研究，並提出一種高可靠度的金鑰傳送(Key Delivery)技術，使其具備高可靠度(High Reliability)與低延遲(Low Delay)的優點，藉以提升隨選(On Demand)互動數位多媒體(Interactive Digital Multimedia)系統的服務品質。

關鍵詞：數位版權管理，智慧財產權，隨選互動數位多媒體，金鑰傳送。

1. 前言

近幾年來，世界各國陸續開播數位電視(Digital TV)頻道，也將在未來幾年內逐漸停播類比電視頻道。因此，數位電視所需的數位內容(Digital Content)與數位電視相關技術的產業也正在蓬勃發展。其中數位內容的發展已經受到大家的重視，從前所慣稱的 3C 產業現在已經將數位內容納入，稱之為 4C 產業。而在數位電視系統中，除了傳統的廣播方式(Terrestrial/Satellite Broadcast)外，更為大家所嚮往的是隨選互動的數位電視(Interactive Digital TV on Demand)，如網路電視 IPTV。然而數位內容透過網路來傳送，如何確保其服務品質(QoS)，將是一大挑戰。除此之外，如何確保數位內容的安全性，且能在網路上被合法的使用，更是數位多媒體系統業者所關心的課題。

除了上述的數位電視系統外，包括 3G 手機、個人通訊設備如 PDA 等，也都以朝向能夠接收多媒體影音串流(Streaming)服務為目標，為達成這個目標，於是由許多業者共同成立了開放式行動聯盟(Open Mobile Alliance，OMA)，負責制定與研擬相關的規範與協定，以促進相關產業的發展，其中如 OMA 所制定的有關 DRM 的規範 1.0 及 2.0 版[1]。而在網際網路上的多媒體串流服務(Multimedia Streaming Service)，如 MP3 音樂播放服務，以及 P2P 多媒體影音下載平台系統，亦正方興未艾，逐步成長中。這種多媒體影音服務的趨勢將是未來科技新產業的發展重心所在，而所需要的數位內容需求將更殷切。

有關數位內容的安全保護一般稱為數位版權管理(Digital Rights Management)，內容提供者(Content Providers)花了巨資製作數位內容，如果在網路上被不斷的竊取與盜拷使用，將使內容提供者遭受巨大的損失，根據國際智慧財產權聯盟(International Intellectual Property Alliance， IIPA)在 1998 年之前的估算，美國每年在動畫影片因缺乏安全控管而損失的營收金額約 1.3 億美元，而音樂媒體方面的營收損失則約為每年 1.7 億美元[2]。如此巨額的營收損失，將會降低數位內容提供者產製數位內容的意願，這對數位電視產業的發展會有很嚴重的不良影響。基於此種理由及保護智慧財產權的觀念，數位版權管理可說是在數位電視產業中所有業者最關注的問題。

數位版權管理的做法很多，其中被認為最有效的方法便是將數位內容加密(Encryption)後再儲存到視訊伺服器(Video Server)供用戶點選收視。在這樣的數位版權管理系統中，牽涉的技術包括影片加解密(Encryption and Decryption)技術、金鑰安全與管理(Key Storage and Management)技術、客戶端認證(Authentication)及金鑰傳送(Key Delivery)技術等。在資料安全領域裡，經過多年的發展，加密技術、金鑰安全管理與客戶認證方面可說已很成熟[3,4,5]，且已有標準規範的產生，只需在實際的網路運作環境中做一些參數的調整與設定便可，但金鑰的傳送成功與否永遠與網路的品質好壞有關，到目前為止尚未有十全十美的金鑰傳送協定存在。試想當客戶訂閱了加密影片，卻因金鑰的遺失而無法收視該訂閱影片時會產生什麼樣的後果呢?當然會讓使用者降低收視加密影片的意願，這便又會對優質影片製造商產生打擊。所以本論文擬針對金鑰傳送的技術做一深入的探討與研究，期能提出一套有效的方法來解決金鑰傳送的問題。

本論文的其他章節內容如下：在第 2 節中，我們將介紹數位版權管理系統的架構與運作流程，第 3 節則是提出一種可行的金鑰傳送機制，第 4 節則是針對所提出的金鑰傳送機制之效能進行比較與分析，最後第 5 節則是我們的結論。

2. 數位版權管理系統架構

一個包含數位版權管理系統的隨選互動數位多媒體系統大致如圖 1 所示。其中數位版權管理系統主要包含兩個部分：加密伺服器(Encryption Server)與授權伺服器(License Server)。加密伺服器負責執行影片的加密作業，加密的過程則如圖 2 所示，數位內容經由選定的內容金鑰(Content Key)透

過適當的加密演算法(如 DES、AES)進行影片內容加密，同時內容金鑰會以服務金鑰(Service Key)再加密成一授權控制訊息 ECM(Entitlement Control Message)，此 ECM 訊息再置入加密影片的標頭(Header)裡，如此便產生所謂的加密影片。接著，加密完成的影片便可上載到所有的視訊伺服器(Video Server)上，並在網頁伺服器(Portal Server)上加入該加密影片的服務選項(流程 S_0)，以供客戶點選。

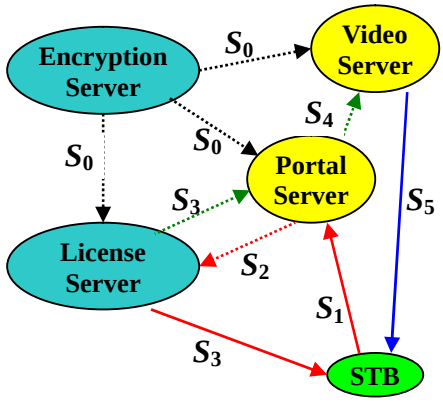

圖 1 數位多媒體系統架構與運作流程圖。

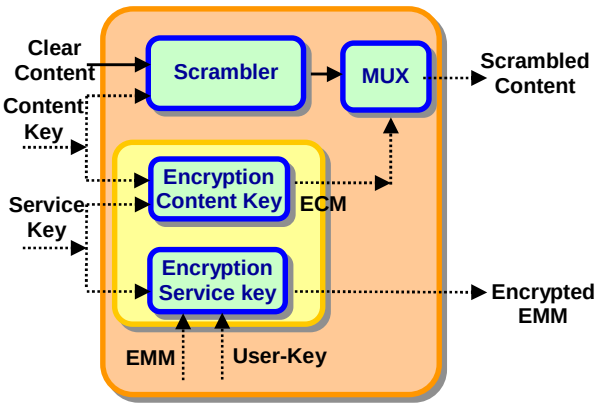

圖 2 數位內容加密系統區塊圖。

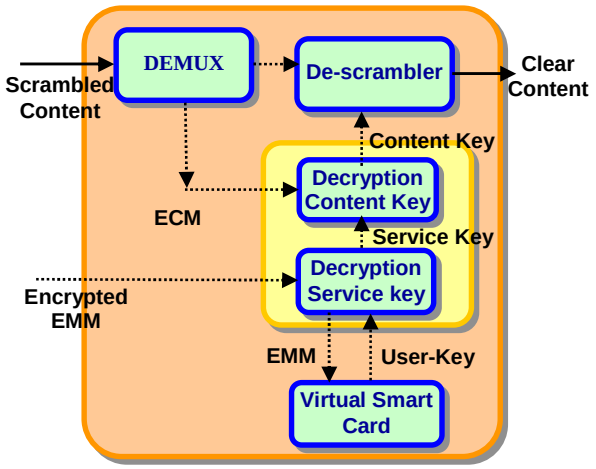

圖 3 數位內容解密系統區塊圖。

當客戶點選加密影片後，此點選請求便會抵達網頁伺服器(流程 S_1)，網頁伺服器會馬上將該客戶的訂閱請求通知授權伺服器(流程 S_2)，接著授權伺服器便回覆認可訊息(Acknowledgement)給網頁伺服器，同時授權伺服器也會立即送出該加密影片的金鑰及授權訊息 EMM(Entitlement Management Message)給客戶端的機上盒 STB(Set-Top-Box) (流程 S_3)，而網頁伺服器在接收到授權伺服器的確認訊息後，即可確認客戶的訂閱請求成功，於是馬上通知視訊伺服器送出該客戶所訂閱的加密影片(流程 S_4)，最後視訊伺服器便開始輸出(Streaming)該影片到客戶的機上盒(流程 S_5)。

客戶端機上盒接收到加密影片的串流後，便以所收到的 EMM 來解密該影片，其解密過程則如圖 3 所示。其中的 EMM 是把服務金鑰及授權訊息(如觀賞期限資訊)經由該客戶的公開金鑰(User Public Key)以 RSA 演算法加密後再經由網路送出，客戶端機上盒收到該加密的 EMM(Encrypted EMM)後，即可用存在虛擬智慧卡(Virtual Smart Card)裡的私密金鑰(Private Key)來解出 EMM，接著再使用 EMM 內所含的服務金鑰來解加密影片所分流(De-multiplexing)出來的 ECM，如此才可拿到包裝在 ECM 內的內容金鑰，並用它來解密加密影片。上述的架構與機制一般是應用在隨選(On Demand)視訊系統上，然而加密伺服器亦可對即時廣播(Live)的視訊做即時(Real Time)的加密，但在目前的商用系統中，對於廣播頻道的存取控制(Conditional Access，CA)較少使用此種方式，故本論文將只針對隨選視訊系統的環境來做探討。

3. 高可靠度的金鑰傳送機制

加密伺服器對影片加密所使用的金鑰一般是存放在授權伺服器的資料庫中，當用戶點選加密影片時，授權伺服器便會將該影片的金鑰進一步處理後(通常以公開金鑰方式加密)再傳送到用戶的機上盒。而在此種數位版權管理系統中，加密伺服器與授權伺服器一般都設置在一安全機房(Secured Room)中，因此各伺服器間的資訊傳送可透過跳線(Cross-Over)的方式或內部網路(Intranet)來完成，故基本上是安全且可靠的。唯有授權伺服器傳送給用戶端機上盒時，會有安全性與可靠性的問題需要加以評估，本研究即是針對此問題做探討。

在安全性方面，首先是授權伺服器與用戶端機上盒的認證(Authentication)，目前的作法是在機上盒生產時即將私密金鑰埋入機上盒內，並在用戶申請安裝機上盒時，會先透過供裝流程由服務管理系統(Service Management System，SMS)及數位版權管理系統進行認證與啟動(Activation)，當完成機上盒的認證作業後，機上盒便會擁有一完整的私密金鑰(Private Key)，並將之存放在記憶體內，因為這種方式是透過軟體來執行，所以一般稱此方式為虛擬智慧卡(Virtual Smart Card)，如圖 3 所示。唯有通過服務管理系統(SMS)與數位版權管理系統(DRM)此兩系統認證的機上盒，才會擁有虛擬智慧卡，也才有可能享受此系統的所有加密影片服務。因此，用戶

端機上盒點選加密影片後，經過 SMS 與 DRM 認證無誤後，授權伺服器便會將該影片的金鑰以 RSA 公開金鑰系統的技術加密後再傳送給機上盒，若此加密後的金鑰成功送達機上盒後，機上盒便可利用認證完成時所事先埋在機上盒(虛擬智慧卡)的私密金鑰來解開影片的服務金鑰與內容金鑰，接著便可對加密影片進行解密。由於採用 RSA 公開金鑰系統來進行金鑰的傳送與認證，在安全性上已可達到相當的水準，故此部分並非本論文所要著墨的核心。

本文擬研究的課題主要在於金鑰傳送的可靠度(Reliability)上，由於網路可能會有瞬斷或中繼節點緩衝器溢位(Buffer Overflow)的現象發生，所以可能造成傳送資料的遺失(Loss)。如果所傳送的授權訊息(EMM)遺失則用戶機上盒便無法對加密影片解密，如此會造成無法收視的問題，所以必須針對網路遺失問題設計一種可靠的傳送協定來遞送 EMM。首先，大家會馬上想到採用連接導向的 TCP 連線方式來達成可靠的金鑰傳送，的確，TCP 是一可靠的傳輸方式，但是 TCP 需要事先建立連線，所以會耗費一些連線建立時間，此為其第一個缺點。其次，對伺服器而言，如果每傳送一筆金鑰便要建立一條連線並且維持該連線至金鑰傳送完成，此種方式會佔去很多伺服器的資源，對授權伺服器而言，要以 TCP 連線方式來傳送金鑰，是很難達到同時支援大量用戶的需求的。如果無法即時迅速的將金鑰傳送到機上盒，同時又無法支援大量用戶同時使用，那便不是一個好的數位版權管理系統。因此，為了克服上述兩項缺失，我們只好採用非連接導向的 UDP 傳送方式來遞送金鑰，由於 UDP 不必事先建立連線，所以能夠縮短金鑰抵達的時間，同時也不會耗費太多伺服器資源，所以可以支援大量用戶同時使用的需求。但採用 UDP 的唯一缺點便是當資料遺失時，無法像 TCP 一樣自動重送，不過卻可透過用戶端機上盒的回覆認可(Acknowledgement)與伺服器的 Timeout 機制來達成。其中一種做法是機上盒每次在播放加密影片前先檢查該影片金鑰是否存在，若不存在則主動發出請求，要求授權伺服器遞送金鑰，直到收到金鑰為止。此種方法的好處是可以達到 100%的成功率，但達成的時間長短卻無法預期，且機上盒必須在每次播放影片前都得先做檢查，也可能影響機上盒的效能，同時經由機上盒發出授權請求給 DRM 系統，亦會產生 DRM 系統遭受惡意攻擊的另一種風險。因此，本文亦不建議採用此種方法。

基於上述的說明，本文擬提出一種可行的機制並加以分析。此方式是授權伺服器每次會將金鑰以相同的 UDP 封包送出 M 個，同時對這 M 個封包啟動一相同的 Timeout 計時器，而這 M 個 UDP 封包儘可能經由不同的 port 輸出，以達到多路徑(Diverse Paths)的目的，當此 M 個封包中的任何一個封包成功抵達機上盒後，機上盒便會回覆一認可訊息給授權伺服器，若 M 個封包全部遺失，則授權伺服器會在 Timeout 後以相同的方式重送該金鑰，若在重複 K 次後仍未成功，則放棄傳送此金鑰。我們稱此種方式為重複授權多路徑法(Duplicate Entitlements in Diverse Paths with Pipeline, DEDPP)。

4. 數值分析與結果

我們將利用理論與模擬的方法來評估 DEDPP 金鑰授權傳送法，所採用的架構與圖 1 相同，差別只在於我們假設從授權伺服器到客戶端機上盒存在多條路徑(Path)，如圖 4 所示，此假設是合理的，因為通常基於網路的穩定性及備援機制的考慮，確實需要建構數條獨立的傳送路徑。其次，我們假設金鑰在任一條路徑上因中繼設備(如交換機或路由器)緩衝器(Buffer)溢位而造成遺失的機率為 p，稱此為連線遺失率(Link Loss Probability)，而客戶點選加密影片的事件遵循波以松分佈(Poisson Distribution)。

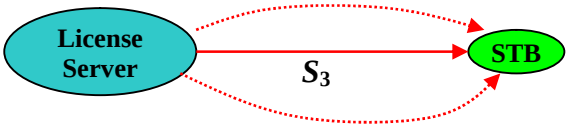

圖 4 授權及金鑰傳送架構圖。

首先，分析金鑰傳送失敗的機率 P_{loss}，在 DEDPP 方法中，授權伺服器每次會送出 M 個授權金鑰，若此 M 個授權金鑰全部遺失，則會在 Timeout 後重新再送出 M 個授權金鑰，如此重複 K 次，故傳送失敗的情況為此 KM 個金鑰全部遺失時才會發生，所以在 DEDPP 中，授權金鑰傳送失敗的機率為

$$P_{loss} = p^{KM} \text{。} \tag{1}$$

其次，有關授權金鑰傳送的延遲(Delay)分析部分，假設 Timeout 時間設為定值 T_O，授權金鑰的傳輸時間為定值 T_K，而所有中繼節點，如路由器(Router)、交換機(Switch)或數位用戶迴路存取多工器(DSLAM)所造成之總延遲(含排隊延遲及處理延遲)為隨機變數 T_R。同時我們亦假設所有用戶與授權伺服器的距離成均勻分佈，於是路徑的傳遞延遲(Propagation Delay)則為均勻分佈的隨機變數 T_P。於是，在 DEDPP 傳送法之金鑰平均傳送延遲則為

$$\begin{aligned}
\overline{D}_{DEDPP} &= (T_K + \overline{T}_R + \overline{T}_P)(1-p^M) \\
&\quad + (T_O + T_K + \overline{T}_R + \overline{T}_P)(1-p^M)p^M + \cdots \\
&\quad + ((K-1)T_O + T_K + \overline{T}_R + \overline{T}_P)(1-p^M)p^{(K-1)M} \\
&= \sum_{i=0}^{K-1} (iT_O + T_K + \overline{T}_R + \overline{T}_P)(1-p^M)p^{iM} \\
&= T_O\left[\frac{p^M(1-p^{(K-1)M})}{1-p^M} - (K-1)p^{KM}\right] \\
&\quad + (T_K + \overline{T}_R + \overline{T}_P)(1-p^{KM}).
\end{aligned} \tag{2}$$

接下來，我們透過電腦模擬的方式來與理論分

析結果做驗證，有關模擬的相關參數詳見表 1。而在此模擬的例子中，為了簡化授權金鑰的模擬，我們先將中繼節點路由器等設備移除，即在我們的模擬中，我們令$T_R = 0$。將來我們擬對金鑰傳送網路(Key Delivery Network，KDN)架構另行提出新架構與設計，並進行詳細的分析。

表 1 模擬所使用的網路參數。

模擬參數	數值	說明
T_K	20μs	授權金鑰傳輸時間
$\overline{T}_P$	55μs	平均傳遞延遲，假設傳遞延遲為一介於(10~100μs)的均勻分佈
T_O	420μs	Timeout 時間設為最大傳遞延遲之 4 倍加上傳輸時間
λ	5000/sec	訂閱請求到達率

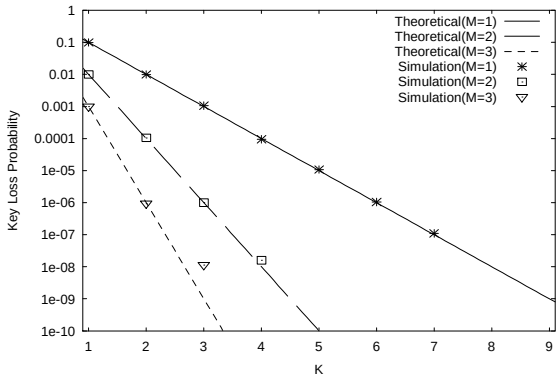

圖 5 金鑰遺失率與 *K* 值的關係圖。

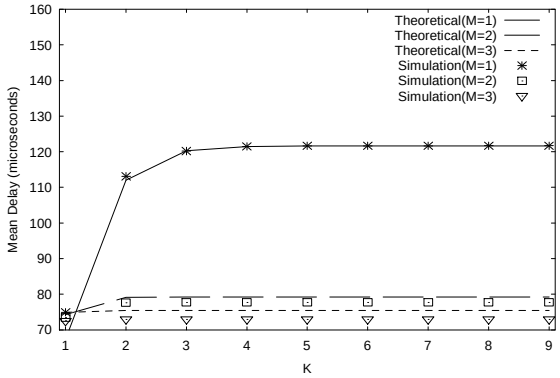

圖 6 金鑰平均傳送延遲與 *K* 值的關係圖。

圖 5 為在連線遺失率 $p = 0.1$下所得到的金鑰傳送失敗率(Key Loss Probability)與重複次數 *K* 之關係圖。其中曲線部分為理論計算的結果，即根據方程式(1)所計算出來的曲線，而打點的部分則是模擬的結果。從圖 1 我們可看出當固定 *K* 值時，*M* 值越大，則金鑰傳送失敗的機率就越低。但根據方程式(1)，只要 *KM* 值相同，則金鑰傳送失敗的機率就相同，因此若在相同的金鑰傳送失敗機率要求下，*M* 值越大，*K* 值就越小，但 *K* 值越小到底會有何好處呢?圖 6 說明 *K* 值與金鑰傳送成功的平均延遲之關係，其中連線遺失率亦固定為 $p = 0.1$，曲線部分是根據方程式(2)所計算出來的，結果顯示 *K* 值越大，其延遲也遞增，特別是從 $K = 1$ 增加至 $K = 2$ 時變化最明顯，之後在 $K \geq 3$ 後逐漸進入穩定的飽和狀態(Saturation)。此說明若在相同的金鑰遺失率要求下，即 *KM* 固定，則 *K* 值越小或 *M* 值越大，則傳送成功的金鑰平均延遲就會越低，效能自然越好。

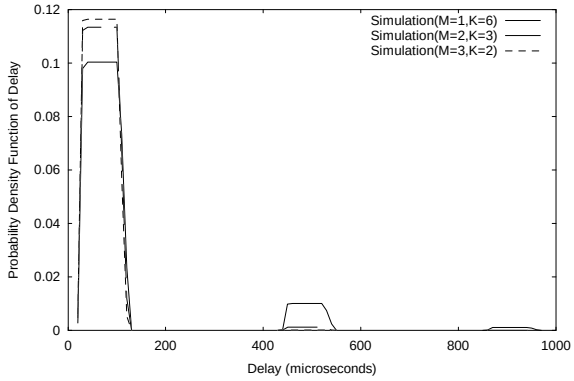

圖 7 金鑰傳送延遲之機率密度分佈圖。

圖 7 表示傳送成功的金鑰延遲機率密度分佈圖(Probability Density Function)，同樣是在 $p = 0.1$的情況下所得到的結果，在此三種模擬的參數中，*KM* 值都相同(*KM* = 6)，所以金鑰遺失的機率相同，但是 *M* 值越大，其金鑰傳送的延遲分佈在較小值的比例就越高，其平均延遲也就越小，而在圖 7 中，延遲主要分佈在三個區間，約(10~120μs)、(420~530μs)及(840~950μs)間，第二個區間即是經過一次 Timeout 後重送成功的金鑰之延遲，第三個區間則是經過兩次 Timeout 後重送成功的金鑰延遲。當重送次數 *K* 值越大，延遲分佈比率即迅速減少，這是因為重複傳送越多次，傳送失敗的機率就越來越低了，於是需要再重送的比率即大幅減少之故。

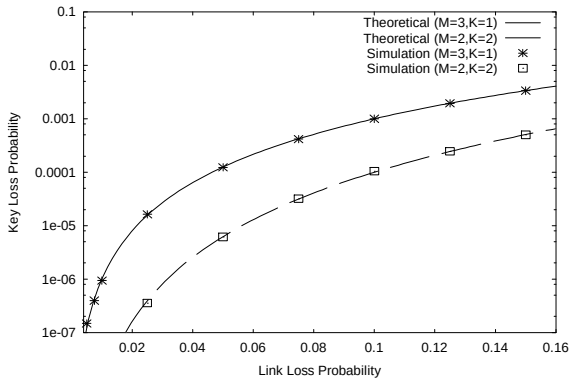

圖 8 金鑰遺失率與連線遺失率的關係圖。

圖 8 則是金鑰傳送遺失的機率與連線遺失機率(Link Loss Probability)的關係圖，曲線是根據方程式(1)所得到的結果，配合模擬的結果做驗證。連線遺失率越高，金鑰傳送失敗的機率也越高，同時我們也發現 *KM* 之乘積越大，金鑰傳送的失敗率也越低，此完全可由方程式(1)得到驗證。

綜合以上的結果，我們認為重複授權多路徑法 DEDPP 可在適當的 K 與 M 值下得到令人滿意的效能，通常可取較小的 K 值與較大的 M 值，即可同時達到低金鑰遺失率與低延遲的要求，證明重複授權多路徑法 DEDPP 是一種優良的金鑰傳送方法。

5. 結論

本文簡單介紹了隨選互動多媒體系統的架構，其中包括數位版權管理系統與視訊服務管理系統。我們特別針對數位版權管理系統做詳細的剖析，包括加密與解密的方法及相關的待解問題，特別是在金鑰傳送協定上。於是我們提出重複授權多路徑法 DEDPP 來達到高可靠度與低延遲的要求，根據分析與模擬的數值結果，讓我們驗證了重複授權多路徑法 DEDPP 的優越性。然而尚有一些細節部分仍有待進一步深入探討與研究，包括如何設計一個良好的金鑰傳送網路(Key Delivery Network，KDN)，以降低網路的金鑰遺失率(Key Loss Rate)，同時如何分析在此金鑰傳送網路下的效能，將是我們未來努立的方向。

參考文獻

[1] OMA Digital Rights Management version 1.0 & 2.0, *http://www.openmobilealliance.org*.

[2] F. Hartung and F. Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications," *IEEE Communications Magazine*, pp. 78-84, Nov. 2000.

[3] W. Jonker and J. P. Linnartz, "Digital Rights Management in Consumer Electronics Products," *IEEE Signal Processing Magazine*, pp. 82-91, March 2004.

[4] Y. Jeong, K. Yoon, and J. Ryou, "MPEG-2 Streaming Protection Scheme for Digital Rights Management," *IEICE Trans. on Information and Systems*, Vol. E87-D, No. 12, pp.2594-2601, Dec. 2004.

[5] G. Hanaoka, K. Ogawa, I. Murota and G. Ohtake, "Managing Encryption and Key Publication Independently in Digital Rights Management Systems," *IEICE Trans. on Fundamentals*, Vol. E87-A, No. 1, pp.160-172, Jan. 2004.