Journal of Universal Computer Science, vol. 15, no. 5 (2009), 1023-1041
submitted: 1/8/08, accepted: 28/2/09, appeared: 1/3/09 © *J.UCS*

Protecting Mobile TV Multimedia Content in DVB/GPRS Heterogeneous Wireless Networks

Shiguo Lian
(France Telecom R&D (Orange Labs) Beijing, China
shiguo.lian@orange-ftgroup.com)

Yan Zhang
(Simula Research Laboratory, Oslo, Norway
yanzhang@ieee.org)

Abstract: Normally, the multimedia content provider and network service providers are separated in mobile TV systems. The TV programs are broadcasted from the content provider to the mobile terminals through Digital Video Broadcasting Transmission System for Handheld Terminals (DVB-H), and the access information is unicasted from the service provider to the user via General Packet Radio Services (GPRS) networks. Due to the network architecture heterogeneity, protocols variation and algorithms difference, securing mobile TV content is becoming a significant challenge. In this paper, we present the architecture, protocol, user identification and digital right management (DRM) for protecting mobile TV multimedia content. The network architecture describes the integrated DVB-H and GPRS to provide secure mobile TV services. The efficient protocols and algorithms are proposed to encrypt the content and also decrypt the coded content. The user identification is able to identify the legal user by matching the username-password pair or the scanned fingerprint. The DRM is able to protect the data from both DVB-H and GPRS. Following this framework, the illegal usage of the mobile TV services can be efficiently prevented and the real-time multimedia Quality-of-Service (QoS) with respect to delay can be guaranteed. The real implementation has demonstrated the effectiveness of the multimedia content protection in the heterogeneous mobile networks. In addition, the delay is sufficiently low to provide live TV.

Keywords: Mobile TV, Digital Rights Management (DRM), Video Scrambling, Fingerprint Matching, User Identification, Secure Multimedia Distribution, DVB-H, GPRS
Categories: D.4.6, H.5.1, H.5.5, H.4.0, H.5.0, H.1.1, H.3.7, H.5.0

1 Introduction

Multimedia is becoming an indispensable component in the daily communications and services. The media may include data, text, image, audio and video. Ubiquitous computing is emerging as the requirement and capability to provide mobile services anywhere, anytime and anyone with the rapid development of wireless technologies. The requirements on multimedia services and the ubiquity capability demand the seamless integration of these two aspects. Mobile TV is an emerging and promising killer application in this scenario.

Currently, mobile TV can be transmitted over Digital Video Broadcasting

Transmission System for Handheld Terminals (DVB-H) [DVB, 2004] or Global System for Mobile communications/General Packet Radio Service (GSM/GPRS) [GSM/GPRS, 2008]. However, either DVB-H or GSM/GPRS alone is unable to provide secure and efficient mobile TV service. DVB-H provides the specification bringing broadcast services to mobile handsets. Compared with other TV systems, it focuses on the additional features to meet the specific requirements of handheld and battery-powered receivers. For example, the time slicing technology is used to significantly reduce power consumption for small portable and handheld terminals. However, since DVB-H only offers the downstream channel at high data rate, the close interactions between users and the service providers are not well supported. On the other hand, GPRS is an added packet-oriented service available to GSM users. GPRS is a best-effort service and hence the Quality of Service (QoS) is not guaranteed. With the data rate provision 56-114 kbps, GPRS can be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS) and Internet services (e.g. email and web browsing). For mobile TV services, GPRS is not suitable due to the limited bandwidth and low scalability to support large number of users at the same time.

In the literature, the study [MOBISERVE, 2005] presents a typical scenario in realizing mobile TV application by integrating DVB-H and GPRS networks. The TV programs are broadcasted to mobile phones through DVB-H. The service request and payment is accomplished through GPRS channel. With the access right information from GPRS channel, a person is able to decrypt and play back the TV programs. However, in this scenario, the digital rights management (DRM) [DVB-CPCM, 2007] [OMA DRM, 2006] is still an open issue due to the network architectures heterogeneity, protocols variation and algorithms difference in hybrid wireless networks. DRM aims to provide TV content protection and to secure user interaction. In addition, DRM is an enabling technology for profitable business models and user content control during TV programs distribution. DRM concerns not only the content delivery but the content lifecycle management. Hence, the TV content should be only accessible to the authorized users. In homogeneous wireless networks, there are DRM for broadcasting and DRM for mobile communications. In the context of broadcasting, DVB-H content protection & and copy management (DVB CPCM) [DVB-CPCM, 2007] specifies the content protection and copy management of commercial digital content delivered to consumer products. CPCM is designed in protecting all types of content, including audio, video and associated applications and data. However, CPCM only defines the mechanism for designing a secure system, and it does not describe the detailed functionalities like encryption, authentication, authorization and tracking. For mobile communications, Open Mobile Alliance DRM (OMA DRM) [OMA DRM, 2006] specifies the digital rights management. It defines the format and the protection mechanism for content and the rights objects, and also the security model for management of encryption keys. Before the content is delivered over networks, it is securely packaged to protect it from unauthorized usage. The content issuer transmits DRM content and a rights issuer produces a rights object with the encryption keys. Additionally, OMA DRM defines the super distribution mechanism, which is able to

redistribute the DRM content from one terminal to other terminals.

Secure content transmission protects the content when it is transmitted from the sender to the receiver. The content security includes confidentiality and integrity. Confidentiality refers to the situation that only the authorized user can access the content. Integrity indicates whether the content has been changed during its transmission. Various approaches have been proposed for secure content transmission. Conditional Access (CA) systems [Lian et al., 2008][Lian et al., 2009][Park et al., 2006] [Pescador et al., 2006] for home TV can provide secure TV program distribution from the broadcaster to TV sets. Several techniques have been standardized, e.g. ISMACryp [ISMACryp, 2004], SRTP [SRTP, 2002] and IPSec [IPSec, 2008]. ISMACryp defines the encryption and authentication for MPEG-4 [MPEG-4, 2006] data streams in the application layer. SRTP defines the encryption and authentication in the transport layer. IPSec encrypts and authenticates IP packets in the network layer. The secure transmission in higher layer can achieve higher security. For instance, ISMACryp is capable of achieving end-to-end security while IPSec can only realize peer-to-peer security.

Broadcast encryption provides the solution for encrypting broadcast content in order to confirm that only the authorized users can decrypt the content. The biggest challenge for broadcast encryption is that unsubscription of some users should not affect the remaining users. The typical attack is collusion attack, in which, several users work together to decrypt the content. Till now, some means have been proposed to solve this problem. For example, the encryption schemes based on public key setting [Naor et al., 2000][Dodis et al., 2002][Boneh et al., 2005a][Boneh et al., 2005b][Park et al., 2008] aim to get the tradeoff between the security and other performances (e.g., transmission cost or storage cost). In Advanced Access Content System (AACS) [AACS, 2005], the tree-based key arrangement method is proposed to eliminate any desired subset of users, which stores the keys in the DVD disk. In practice, the tamper-resistant cards [Smart, 2008] are used to impose physical restraints on a user learning their own decryption keys, which stores the keys and executable programs. However, most of the broadcast encryption methods transmit the key together with the content, which makes it difficult to assign different usage rights (play once, play twice, view only, downloadable, etc.) to different users. Additionally, they do not support the user feedback.

It is summarized that there are no feasible DRM solutions for the mobile TV system operating in heterogeneous wireless networks. Furthermore, mobile terminals may be subjected to loss, comparing with home TV. As a consequence, preventing the illegal usage of the mobile TV services is also significant. Motivated by these, we present the architecture, protocol, user identification and DRM mechanisms for protecting mobile TV multimedia content. The network architecture describes the integrated DVB-H and GPRS to provide secure mobile TV services. The efficient protocols and algorithms are proposed to encrypt the content and also decrypt the coded content. The user identification is able to identify the legal user by matching the username-password pair or the scanned fingerprint. The DRM is able to protect the data from both DVB-H and GPRS. Following this framework, the illegal usage of the

mobile TV services can be efficiently prevented and the real-time multimedia QoS with respect to delay can be guaranteed. The real implementation has demonstrated the effectiveness of the multimedia content protection in the heterogeneous mobile networks. In addition, the delay is sufficiently low to provide live TV.

The rest of the paper is organized as follows. Section 2 presents the secure mobile TV infrastructure and describes the protocols and algorithms. Section 3 shows the real implementation and the numerical results. Finally, Section 4 concludes the paper.

2 Secure Mobile TV Scheme

2.1 The Architecture of the Secure Mobile TV System

The proposed secure scheme aims to protect mobile TV services in heterogeneous mobile networks. A user may request mobile TV services in a variety of program channels. With different bandwidth provision and media requirement, different networks should be employed to transmit different data. With the advantage of high bandwidth, the DVB-H network is able to transmit multimedia contents, e.g. video, audio and image. On contrast, the GPRS network can be employed to transmit the service requests and permissions between the terminal and the service provider. The secure scheme is able to achieve three objectives. Firstly, the TV multimedia content should be protected against unauthorized users. Secondly, the access right for the authorized users can be differentiated. Finally, only the identified user has the capability to request the TV service through his/her mobile terminal.

Fig.1 shows the architecture of the proposed secure mobile TV mechanism. The infrastructure has four components: Content Server, Content Provider, Service Provider and mobile terminal. The content server has the capability of scrambling the TV content and delivers the scrambled content to the content provider. Additionally, the content server forms the service guide containing the content list based on the service request and sends the service guide to the service provider. For the mobile terminal with a TV player, it receives the scrambled content from the content provider. Then, the mobile terminal receives the user access right information from the service provider and descrambles the content with the SIM Card under the control of the user right. The fingerprint scanner in a mobile terminal can authenticate the user and is able to prevent illegal user from using the mobile TV service.

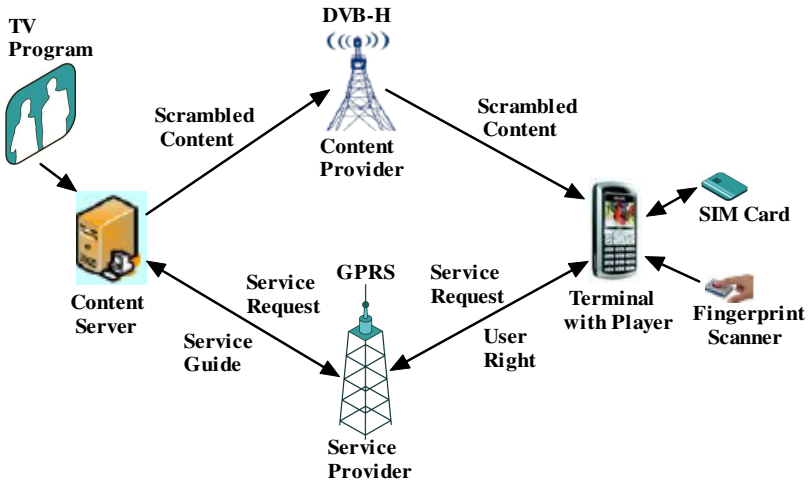


Figure 1: The Architecture of the Secure Service System

2.2 Procedures in Securing Mobile TV Services

There are two phases in protecting the mobile TV content, i.e., the generation of scrambled content and management information, and the descrambling of TV content. In the first phase, the content server generates the scrambled content and also the Entitlement Management Message (EMM). In particular, the scrambled content is composed of the content itself and the Entitlement Control Message (ECM) that contains the scrambling key while the EMM has the user access right for the TV content. The generated scrambled content and management information are transmitted to a mobile terminal from the content provider and service provider, respectively. In the second phase, a mobile terminal requests the mobile TV service, receives the multimedia content and management information, and descrambles the TV content. Fig. 2 shows the details in the second phase.

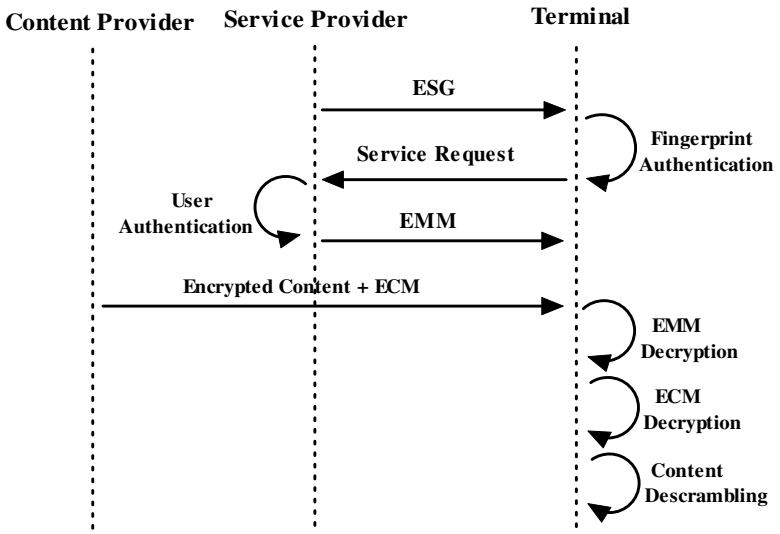


Figure 2: The procedure of securing mobile TV service

The service provider broadcasts the Electronic Service Guide (ESG) to potential users. ESG includes the TV channels, TV programs and time table. At a time, a user sends a service request to the service provider through the terminal in case the user fingerprint can be authenticated. This will guarantee that only the subscribed user can use the own terminal to use the mobile TV service. The fingerprint authentication will be presented in detail in Section 2.5. Following this, the service provider authenticates the user by identifying the unique information in the SIM Card. After being successfully authenticated, the user's service information is stored in a database. Here, the information may include the requested programs, service lasting time and payment. With the successful authentication, the service provider transmits the EMM contains the user access right to the mobile terminal. Then, the terminal decodes the EMM from the service provider and then decodes the ECM and the content from the content provider. Finally, Terminal plays back the decoded TV program on the basis of granted access right.

In the secure system, there are three significant challenges: service acquisition and user authentication, content scrambling and right management, and user identification.

2.3 Service Acquisition and User Authentication

This procedure is responsible for information transmission and authentication, which has three steps, i.e., Service Request, User Authentication and EMM transmission. To implement this procedure, various approaches [DVB-CPCM, 2007] [ISMACryp, 2004] [Tsai et al., 2006] [European, 1997] can be used. In this work, we employ the 2-pass acquisition protocol recommended by DVB CPCM and ISMACryp. In addition, mutual authentication is adopted. We set K_{SS} and K_{SP} as the service provider's secret

key and public key respectively. Let K_{US} and K_{UP} denote a mobile terminal secret key and public key, respectively. The service provider stores K_{SS}, K_{SP} and K_{UP} while the mobile terminal stores K_{US}, K_{UP} and K_{SP}. Let V denote the user's service information, including the user ID, the requested programs, service lasting time and payment.

1. Service Request

The mobile terminal computes the following message and sends it to the service provider.

$$V_E = \mathrm{E}(V \,\|\, \mathrm{E}(\mathrm{H}(V), K_{US}), K_{SP}) . \tag{1}$$

Here, V_E represents the encrypted and signed service information, E() denotes the public encryption operation, H() refers to the hash function, and ‖ stands for the concatenation operation. In other words, the service information V is firstly signed by the user and then encrypted by the service provider's public key K_{SP}.

2. User Authentication

The service provider decrypts the received service information with the secret key K_{SS}, and obtain

$$\mathrm{D}(V_E, K_{SS}) = V \,\|\, \mathrm{E}(\mathrm{H}(V), K_{US}) . \tag{2}$$

Here, D() is the decryption operation of the public cipher. Then, the service provider computes a hash value H(V) from V and decrypts the encrypted hash $\mathrm{E}(\mathrm{H}(V), K_{US})$ with the user's public key K_{UP} according to

$$\mathrm{D}(\mathrm{E}(\mathrm{H}(V), K_{US}), K_{UP}) = \mathrm{H}(V) . \tag{3}$$

Finally, by comparing the computed hash value with the decrypted hash value, the service provider can determine whether the user is the right one.

3. EMM transmission

The service provider processes the EMM and then sends it to the mobile terminal.

$$EMM_E = \mathrm{E}(EMM \,\|\, \mathrm{E}(\mathrm{H}(EMM), K_{SS}), K_{UP}) . \tag{4}$$

Here, EMM_E is the encrypted and signed copy of EMM. The mobile terminal receives the EMM_E and decrypts it according to the following formula

$$\mathrm{D}(EMM_E, K_{US}) = EMM \,\|\, \mathrm{E}(\mathrm{H}(EMM), K_{SS}) , \tag{5}$$

The terminal is able to authenticate whether the message is transmitted by the service provider with the similar method used for user authentication.

2.4 Content Scrambling and Right Management

As indicated in Section 2.1 and Section 2.2, a mobile terminal receives two data streams. One data stream is composed of the scrambled content and ECM. Another data stream is unicasted through GPRS, including the EMM information.

Fig. 3 shows the generation and decoding procedures of the scrambled content, ECM and EMM. The content server pre-determines the parameters K_C, K_E, Access Criteria and TV Content. The service provider is aware of K_M and User Right. Here, Access Criteria refers to the operation type applicable to the TV content. It can be view-only, view twice, view and record. User Right contains the operation type that is

permitted for the user to operate the TV content. K_C, K_E and K_M are the keys used to control the encryption of TV Content, Access Criteria and User Right, respectively. It is noteworthy that K_M is securely stored in both the service provider and a mobile terminal.

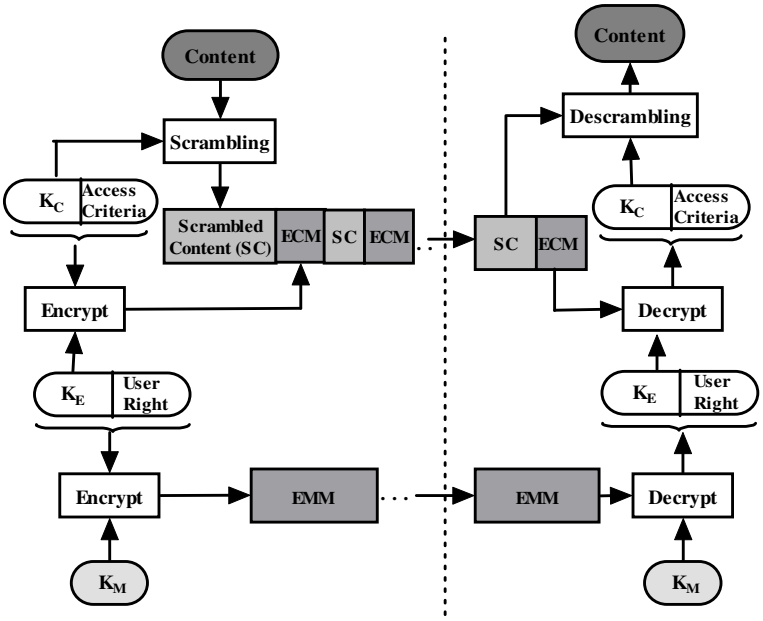


Figure 3: Methods for content scrambling and right management

At the sender side, the scrambled content, ECM and EMM are generated based on the following reasoning.

Firstly, the TV content is scrambled with the help of K_C. The scrambling algorithm can be selected from the existing block ciphers [Mollin, 2006], e.g. 3DES, AES and IDEA. Hence, the scrambling operation is defined as

$$SC = \mathrm{S}(C, K_C) \tag{6}$$

where S() is the scrambling operation, C is the TV content, and SC is the scrambled content.

Secondly, the ECM composed of K_C and Access Criteria (AC) is encrypted with block ciphers [Mollin, 2006] with K_E. That is, the encrypted ECM is given by

$$ECM = \mathrm{E}(K_C \,\|\, AC, K_E) \tag{7}$$

where E() represents the encryption operation and "‖" is the concatenation operation. As a consequence, both the scrambled content and ECM are broadcasted to users through DVB-H network.

Thirdly, the EMM composed of K_E and User Right (UR) is encrypted with block ciphers [Mollin, 2006] under the control of K_M. That is, the EMM encryption is given by

$$EMM = \mathrm{E}(K_E \| UR, K_M) \tag{8}$$

Hence, the encrypted EMM is unicasted to users through GPRS network.

At the mobile terminal side, the EMM, ECM and scrambled content are decoded. Firstly, the EMM is decrypted with the same cipher used for encryption under the control of K_M, which recovers both K_E and User Right (UR). The EMM decryption is defined as

$$K_E \| UR = \mathrm{D}(EMM, K_M) \tag{9}$$

where D() is the decryption operation. Secondly, the ECM is decrypted with the same cipher under the control of K_E, which recovers both the K_C and Access Criteria (AC). The ECM decryption is expressed as

$$K_C \| AC = \mathrm{D}(ECM, K_E) \tag{10}$$

Finally, the TV multimedia content is descrambled with the key K_C. After this operation, the terminal is able to recover and watch the TV content. The descrambling operation is defined as

$$C = \mathrm{DS}(SC, K_C) \tag{11}$$

where DS() refers to the descrambling operation. C denotes the recovered TV content. SC represents the scrambled content.

2.5 User Identification Based on Fingerprint Authentication

The user identification module is integrated at the mobile terminal in order to enhance the security of the mobile TV system. The user identification mechanism is able to guarantee that only the user who inputs the right user name and password can request the mobile TV service. Additionally, the fingerprint based user identification is introduced as an alternative selection to increase the usability [Miklos, 2000] [Jain et al., 1997]. This functionality can prevent the illegal usage and hence avoid the profit losses of the mobile terminal owner and service provider.

1. Secure Service Request

A user should input the personal identification when clicking the ESG (Electronic Service Guide) for requesting mobile TV service. Here, two kinds of modes are supported, i.e., username-password pair and user fingerprint. Fig. 4 shows the four parts in achieving successful and secure service request. At the starting point, the user selects the input mode for personal identification, i.e., fingerprint input or not. If the fingerprint input mode is select, then the user fingerprint is scanned by the fingerprint scanner in the terminal. In case the scanned fingerprint matches with the one stored in the SIM Card, and the service request is permitted. The fingerprint match [Miklos, 2000] is a mature technique and has been widely used in various applications, which has also been used in the terminal protection [Chen et al., 2005] [Yi, 2004]. On the other hand, if username and password pair is selected as the input mode, the user is remaindered to input the username and password. If both the username and the password are same to the ones stored in the SIM Card, then, the service request is allowed. The username-password pair matching has been widely used in various services [Authentication, 2006].

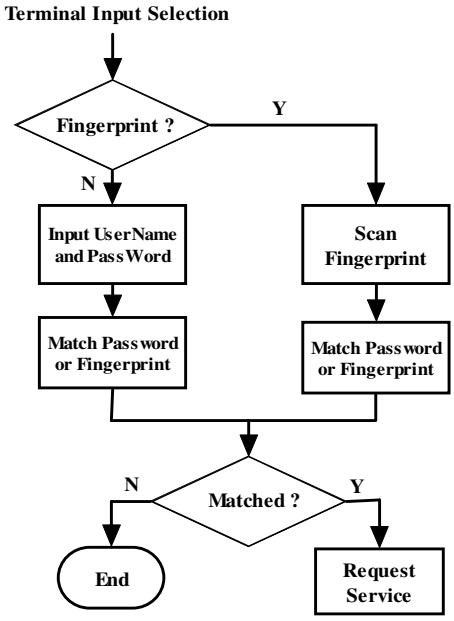


Figure 4: Secure service request based on two input modes

2. Secure Fingerprint Update

Considering that the Terminal may be used by different family members or friends, the right to request mobile TV service should also be transferable. For example, User A that is the original owner of a terminal may transfer the terminal to User B. User A has the right to request mobile TV service. If User B wants to request the mobile TV service with the same terminal, he should update the fingerprint together with User A. To achieve, a secure fingerprint update is necessary. Fig. 5 shows the fingerprint updating process. The user requests the fingerprint updating operation that determines whether the fingerprint is firstly updated or not. If it is the first time, the user is requested to input the old password. If this password matches with the one in the SIM Card, then the user is requested to input the new fingerprint and the new fingerprint is registered. Otherwise, the updating process is failed and the old fingerprint stored in the SIM Card is not changed. In case it is not the first time to update the fingerprint, then the user is requested to input the old fingerprint. If the fingerprint is same as the one stored in the SIM Card, then the user can input and register a new fingerprint. Otherwise, the fingerprint updating is failed.

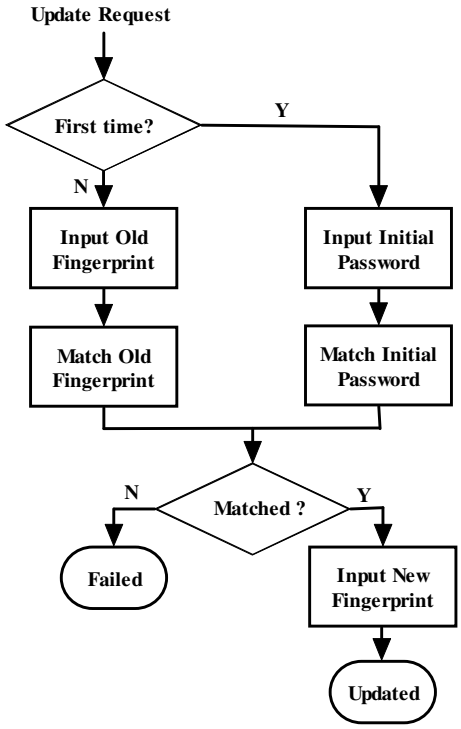


Figure 5: The fingerprint update procedure

3 Implementation and Numerical Results

3.1 Functional Modules in Terminal and SIM Card

In the implementation, various functional modules are integrated in a terminal and the SIM Card. In a terminal, the GSM module, Descrambler and Fingerprint Scanner are integrated. In these components, the GSM module is in charge of the signal transmitting and receiving, message edition and telephone number storing. The Descrambler descrambles the TV content with the key decrypted by SIM Card. The Media Player plays back the TV content descrambled by the Descrambler. The Fingerprint Scanner scans user fingerprint and sends it to the SIM Card. In the SIM Card, the user control module and fingerprint module are integrated together with the operator module. Here, the operator module stores the user information, payment information and operator information that are used to realize common communications controlled by the corresponding operator. The User Control Module is in charge of decrypting user access rights like EMM and ECM. It also produces the content scrambling key for the Descrambler in the terminal. The Fingerprint Module stores the initial password that is used for fingerprint update, stores the username-password pair and user fingerprint that are used for user identification, and realizes

username-password matching and fingerprint matching.

Among all the modules in the terminal and the SIM Card, three ones are in close with the system's security: the Descrambler, the User Control Module and the Fingerprint Module. AS a result, they are implemented in trust-computing modules, making difficult to be eavesdropped.

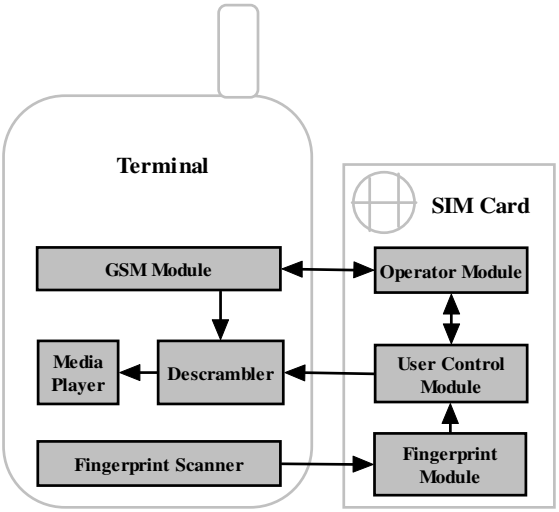


Figure 6: The functional modules in Terminal and SIM Card implementation

3.2 Content Scrambling and Access Right Encryption

The mobile TV program is encoded with MPEG-4 [MPEG-4, 2006], packaged with RTP, and transmitted through IP. The content scrambling can be achieved in different layers by different means. Fig. 7 shows a possible scrambling method, i.e., IP layer by IPSEC, RTP layer (transport layer) by SRTP, or MPEG-4 layer (application layer) by ISMACryp. It is believed that the application layer implementation is more suitable to guarantee end-to-end security, taking into account the fact that the TV content can be stored in a terminal or redistributed to other terminals. Hence, the AES-based scrambling algorithm proposed in IMSACryp [ISMACryp, 2004] is employed to scramble the encoded TV content. The access right information including ECM and EMM are encrypted by the AES cipher with the CTR mode.

MPEG-4	ISMACryp/AES CTR	Application Layer
RTP	SRTP	Transport Layer
IP	IPSEC	Network Layer

Figure 7: Different modes for content scrambling

3.3 Video Content Scrambling

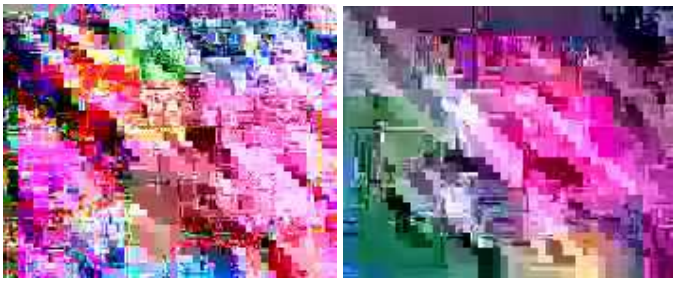
In this subsection, we will demonstrate the effect of scrambling. The video content in TV program is encoded with MPEG-4 AVC/H.264 [MPEG4, 2000a] and the audio content is encoded with AAC (Advanced Audio Coding) [MPEG4, 2000b]. Fig. 8 shows an example with scrambled video frames. It is clear that the scrambled video content is too chaotic to be understandable. This makes the TV program unreadable for the unauthorized users who have no legal keys.

(a) Original (b) Scrambled

(c) Original (d) Scrambled

Figure 8: Examples of video content scrambling

On the other hand, since the scrambling operation is applied to the encoded data stream. Without the correct descrambling key, the decoded TV content will be unreadable. Additionally, the scrambled content is sensitive to the key. Fig. 9 shows the sensitivity of key on the descrambled TV content. The original video content is scrambled by K_{C0}="0123 4567 89ab cdef 0123 4567 89ab cdef". Then, the video is descrambled by K_{C1}="1123 4567 89ab cdef 0123 4567 89ab cdef" and K_{C0}="0123 4567 89ab cdef 0123 4567 89ab cdef", respectively. The comparison demonstrates that the user is able to recover the video content with the correct key. For a video with minor different key, the video content is still chaotic and unreadable. As a consequence, the scrambling algorithm is very sensitive to the key.



(a) Scrambled by K_{C0} (b) Descrambled by K_{C1}

(c) Descrambled by K_{C0}

Figure 9: Key sensitivity of video content scrambling. (K_{C0}="0123 4567 89ab cdef 0123 4567 89ab cdef", K_{C1}="1123 4567 89ab cdef 0123 4567 89ab cdef")

3.4 Quality of Service

For a mobile TV system, time delay of multimedia services is of the most importance. Two kinds of time delay should be considered, i.e., initial service delay and media processing delay. Initial service delay refers to the time delay caused by service initialization or service alteration. The smaller the initial service delay, the less time the user needs to wait. Media processing delay denotes the time duration of the media content processing operations, such as receiving, decoding, descrambling and playing. The media processing operations are normally efficient and do not affect much on the real-time playing. In the following, we will qualify the time delay in the proposed scheme.

A terminal should interact with the service provider, decrypt the EMM and ECM, and descramble the TV content. Hence, there is a delay in the initial playing back especially when the user requests the service at first time or changes the service. The simulation environment is as follows: 5MHz bandwidth of DVB-H, 1 transmitter, 3 channels, 5 users, and QCIF video frame. If not specified, the view-only access criterion is evaluated. When the user requests the new service, the Terminal needs to send a request to the service provider, receive EMM from the service provider, and decrypt EMM, ECM and TV content. This leads to the maximal initial time delay. After the test, the delay is about 6 seconds. If no new service is requested, for example, the user only changes the TV channel, the Terminal needs to select the TV content, and decrypt ECM and TV content. Since the interaction with the service

provider and EMM decryption are skipped, the delay is reduced to about 2 seconds. Without the security operations, the initial time delay of requesting services and changing services can be controlled within 3 seconds and 1 second, respectively. The security operations may cause delay in service initialization. These delays are acceptable in some extent when there are few requests to change the services.

In most scenarios, only TV content needs to be descrambled, while ECM or EMM needs only to be decrypted occasionally, e.g., without Service Request or without TV channel changes. In these cases, the computational efficiency of content descrambling determines the suitability for live TV. Let the time ratio between descrambling and decoding denote the performance metric for the descrambling operation. In a TV program, the video content has a much larger volume than other types of media, e.g. audio content and title, the performance of video content descrambling determines the TV program descrambling. For the sake of simplicity and without loss of generality, we evaluate the video descrambling. The time ratio (Tr) between video descrambling and video decoding is given by

$$\mathrm{Tr} = \frac{T_{ds} - T_d}{T_d}. \tag{12}$$

where T_d denotes the decoding time of a video sequence and T_{ds} denotes the combined decoding and descrambling time of the same video sequence. In the simulation, the descrambling algorithm is ISMACryp AES CTR [ISMACryp, 2004], and the video decoder is MPEG4 AVC/H.264. Table 1 shows the typical results. The time ratio is always smaller than 0.3. This indicates that the descrambling operation has much lower complexity than decoding. Since video decoding is efficient for real-time applications, descrambling operation will have insignificant effect on the real-time playing back on the live TV.

Video sequences	*Size*	*Time ratio between descrambling and decoding (Tr)*
Foreman	QCIF	0.20
Football	QCIF	0.23
Mother	QCIF	0.28
Stefan	QCIF	0.18
Tempete	QCIF	0.26

Table 1: The time ratio between descrambling and video decoding

To reduce the time ratio, the partial encryption may be adopted [Lian et al., 2006][Lian, 2008][Lian et al., 2007]. In this case, 1/n of the TV content is encrypted with AES CTR and other (n-1)/n of the content by XOR operation. Compared with AES CTR, XOR operation is much more efficient. Although the decoding time T_d keeps unchanged, T_{ds} can be reduced considerably, which will eventually leads to a smaller Tr. Fig. 10 shows the relation between the time ratio Tr and the encrypted data ratio 1/n. With larger n, the time ratio decreases. When n is no smaller than 4, the time ratio

keeps no higher than 0.1, which is much better for real-time playing of live TV.

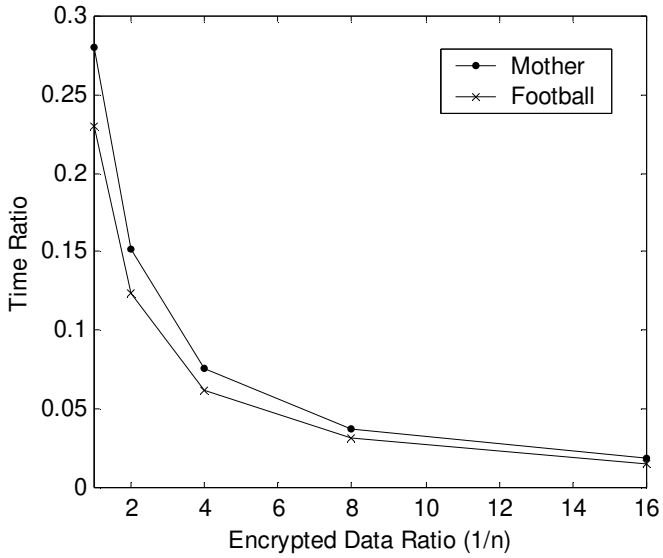


Figure 10: Relation between time ratio and the encrypted data ratio

3.5 Comparison with existing broadcast encryption schemes

The proposed scheme is different from most of the broadcast encryption algorithms. Firstly, in the proposed application scenarios, both broadcast and unicast networks are involved. The GPRS network provides the way for user interaction, and the user right is unicasted to the user (mobile terminal) through GPRS network, since different user has different user right (access criteria, e.g., free view, once view, or twice view). Compared with existing broadcast encryption schemes [Boneh et al., 2005b] [Park et al., 2008], the proposed scheme can assign different user different rights and is easy to realize the personalization. For example, User A can only view the content once, while User B can view the content twice. User A can only view the content but not download the content, while User B can download it. Additionally, the GPRS network provides an interaction channel between users and service provider. For example, users can request, select or cancel the services through this channel. The disadvantage is the transmission cost of the service provider. As shown in Table 2, compared with the schemes, the proposed scheme has higher transmission cost.

Schemes	*Efficiency(transmission cost for n users)*	*Support user rights*	*Support user feedback*
The scheme [Boneh et al., 2005b]	$O(\sqrt{n})$	No	No
The scheme [Park et al., 2008]	O(1)	No	No
Proposed scheme	O(n)	Yes	Yes

Table 2: Performance comparison between different broadcast encryption schemes

4 Conclusions and Future Work

In this paper, the secure framework is presented with the aims to provide copyright protection in mobile TV multimedia content. The scrambled TV content and user access right are independently transmitted to mobile terminals such that only the authenticated terminals have the access right and capability to descramble the TV content. In the real implementation, the TV content and user access right are delivered through DVB-H and GPRS networks, respectively. The result indicates that the DVB/GPRS heterogeneous networks integration is able to make full use of the two networks advantages with respect to bandwidth, data rate and implementation complexity. The result also shows that the transmission delay is insignificant to support live TV in mobile terminals. To improve the efficiency, especially the transmission cost, is the future work.

References

[Authentication, 2006] Authentication with Resin. http://www.caucho.com/resin-3.0/security/authentication.xtp.

[AACS, 2005] Advanced Access Content System (AACS). http://www.aacsla.com/home

[Boneh et al., 2005a] Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. In Eurocrypt'05, 2005, Springer LNCS, vol. 3494, pp. 440–456

[Boneh et al., 2005b] Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In CRYPTO'05, 2005, Springer LNCS, vol. 3621, pp. 258–275.

[Chen et al., 2005] Chen, X., Tian, J., Su, Q., Yang, X., Wang, F.: A Secured Mobile Phone Based on Embedded Fingerprint Recognition Systems. Lecture Notes in Computer Science, Springer Berlin/Heidelberg, Volume 3495, pp.549-553, 2005.

[Dodis et al., 2002] Dodis, Y., Fazio, N.: Public key broadcast encryption for stateless receivers. In DRM Workshop'02, Springer LNCS, vol. 2696, pp. 61–80, 2002.

[DVB, 2004] Digital Video Broadcasting (DVB), Transmission System for Handheld Terminals (DVB-H). ETSI, November 2004.

[DVB-CPCM, 2007] Digital Video Broadcasting Content Protection & Copy Management (DVB-CPCM), DVB Document A094 Rev. 1, July 2007.

[European, 1997] European Telecommunication Standard, GSM 03.20: Digital cellular telecommunications system (Phase 2C), Security related network functions, August 1997.

[GSM/GPRS, 2008] GSM/GPRS (Global System for Mobile communications/General Packet Radio Service), http://en.wikipedia.org/wiki/GSM.

[IPSec, 2008] IPSec (IP Security). http://en.wikipedia.org/wiki/IPSec.

[ISMACryp, 2004] ISMACryp 1.1 (ISMA Encryption & Authentication Specification 1.1). http://www.isma.tv/.

[Jain et al., 1997] Jain, A., Hong, L., Pankanti, S., Bolle, R.: An identity authentication system using fingerprints. In Proc. IEEE, 1997, 85(9): 1365-1388.

[Lian et al., 2006] Lian, S., Liu, Z., Ren, Z., Wang, H.: Secure Advanced Video Coding Based on Selective Encryption Algorithms. IEEE Transactions on Consumer Electronics, Vol. 52, No. 2, pp. 621-629, May 2006.

[Lian et al., 2007] Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption and watermarking in compressed video data. IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 6, 774-778, June 2007.

[Lian, 2008] Lian, S.: Multimedia Content Encryption: Techniques and Applications. Auerbach Publication, Taylor & Francis Group, 2008.

[Lian et al., 2008] Lian, S., Liu, Z.: Secure Media Content Distribution Based on the Improved Set-Top Box in IPTV. IEEE Transactions on Consumer Electronics, Vol. 54, No. 2, pp. 560-566, May 2008.

[Lian et al., 2009] Lian, S., Zhang, Y.: Handbook of research on secure multimedia distribution. IGI Global (formerly Idea Group, Inc), 2009.

[Miklos, 2000] Miklos, Z., Vajna, K.: A fingerprint verification system based on triangular matching and dynamic time warping. IEEE Trans. Pattern Analysis and Machine Intelligence, 2000, 22(11): 1266-1276.

[Mollin, 2006] Mollin, R.: An Introduction to Cryptography, 2nd edition. CRC Press, 2006.

[MOBISERVE, 2005] MOBISERVE (New mobile services at big events using DVB-H broadcast and wireless networks), FP6-2005-IST-61-045410. ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_fp6_mobiserve_en.pdf.

[MPEG4, 2000a] MPEG4 Part 10 (ISO/IEC 14496-10): Advanced Video Coding (AVC): A codec for video signals which is technically identical to the ITU-T H.264 standard.

[MPEG4, 2000b] MPEG4 Part 3 (ISO/IEC 14496-3): Audio: A set of compression codecs for perceptual coding of audio signals, including some variations of Advanced Audio Coding (AAC) as well as other audio/speech coding tools.

[MPEG-4, 2006] MPEG-4. http://en.wikipedia.org/wiki/MPEG4.

[Naor et al., 2000] Naor, M., Pinkas, B.: Efficient trace and revoke schemes. In Proceedings of the 4th International Conference on Financial Cryptography (FC'00), Springer LNCS, vol. 1962, pp. 1–20, 2000.

[OMA DRM, 2006] Open Mobile Alliance, Digital Rights Management 2.0 (OMA DRM 2.0), 03 Mar 2006.

[Park et al., 2006] Park, S., Jeong, J., Kwon, T.: Contents Distribution System Based on MPEG-4 ISMACryp in IP Set-top Box Environments. IEEE Transactions on Consumer Electronics, Vol. 52, No. 2, pp. 660-668, MAY 2006.

[Park et al., 2008] Park, J., Kim, H., Sung, M, Lee, D.: Public Key Broadcast Encryption Schemes with Shorter Transmissions. IEEE Transactions on Broadcasting, Vol. 54, No. 3, pp. 401-411, 2008.

[Pescador et al., 2006] Pescador, F., Sanz, C., Garrido, M., Santos, C., Antoniello, R.: A DSP Based IP Set-Top Box for Home Entertainment. IEEE Transactions on Consumer Electronics, Vol. 52, No. 1, pp. 254-262, FEBRUARY 2006.

[Smart, 2008] Smart Card. http://en.wikipedia.org/wiki/Smart_card

[SRTP, 2002] Secure Real-time Transport Protocol (SRTP) Security profile for Real-time Transport Protocol. IETF Request for Comments document, RFC 3711, 2002.

[Tsai et al., 2006] Tsai, Y., Chang, C.: SIM-based subscriber authentication mechanism for wireless local area networks. Computer Communications 29 (2006) 1744-1753.

[Yi, 2004] Yi, J.: A Mobile Phone Comprising Recognition Sensor of Fingerprint. WO/2004/098083.