Introduction and Security Analysis to Digital Video Broadcasting - Handheld

Leyla Roohi, Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
Noorfadzilla Abd Yusuf, Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia

DVB-H (Digital Video Broadcasting - Handheld) is the mobile TV standards, which is widely used in European countries and many others. It is a technical specification for bringing broadcast services to mobile handsets and plays a very significant role in the modern day Mobile-TV. Unfortunately, threats to the security of its network and communication systems are not usually main concerns. In this paper, a brief history of DVB-H and DVB-H world standards is talked about. Readers can find a concise description of the DVB-H system besides, two security frameworks in DVB-H: OMA-BCAST and IPDC standards. Last but not least, threats of the DVB-H system as well as possible mitigations are reviewed.

Categories and Subject Descriptors: COMPUTING [**C.2**] COMPUTER-COMMUNICATION NETWORKS

General Terms: Broadcasting

ACM Reference Format:
Leyla Roohi and Noorfadzilla Abd Yusuf, **Introduction and Security Analysis to Digital Video Broadcasting - Handheld**, *International Journal of Computer Communications and Networks (IJCCN)*, 3(2), pp 28–45, 2013

1. INTRODUCTION

Due to rapid growth of using mobile phones, this device becomes a part of todays humans life using it for many applications from a simple camera, MP3 player, FM radio to now mobile TV. Technology has shifted the handset from a simple calling and answering device to being a part of an advanced entertainment, Internet access, gaming, office application, mobile commerce and utility device. Mobile TV is a very important tool for live TV and many useful applications like, videoconferencing, video file sharing and group working.

Generally the transmission of TV programs or video for a range of wireless devices is called mobile TV. The programs can be transmitted in a broadcast mode, multicast and even unicast mode to be delivered to a user on demand. The mobile TV transmissions can be via the terrestrial medium or delivered via high-powered satellites directly to mobiles.

DVB-H is a mobile TV technology that is an extension of digital video terrestrial technology or DVB-T [Broadcasting 2009]. DVB-H launched after a series of successful trials in Pittsburgh, Barcelona, Oxford [Protection 2006], and other sites that proved they could bring digital video broadcasting to millions of handhelds under a new technology[Elisa et al.]. Other mobile TV technologies like 3G oprators in the United States of America, Japan, and Europe had been offerd streaming video services and live TV as well. In South Korea services using digital multimedia broadcasting technologies and in Japan the 3G FOMA services began in 2005 and 2002. Mobile TV application of the handsets has been tested in several situations in recent years. Telenor Norway, for example, had broadcast the 2005 Winter Olympics held in Torino live, along with the highlights and other features, for mobile users on 3G networks [TV et al.]. When the FIFA games started in Germany in June 2006, the towering TV transmitters of Berlin, Munich, Frankfurt, Rome, and Milan [TV et al.], as well as a number of

other European cities, broadcast the matches live for mobile TV users for the first time in the history of FIFA. According to vast applications of mobile TV in different technologies, from DVB-H to 3G networks, security of the contents that broadcast via these networks is a big concern.There are many attackes and vulnarabilities in mobile TV due to inherent charachterastices of broadcast networks. DVB-H has introduced two frameworks to provide the security: IP Data Cast (IPDC) and OMABCAST. However, there are vulnarabilities and attackes for these two.

The rest of this paper is structured as follows: DVB-H Standards and System Description are introduced in Section 2and 3. DVB-H Structure is in Section 4. In Section 5, security in DVB-H is dicussed. IPDC and OMA-BCAST Convergence is in section 6. Section 7, is about content and service protection in IPDC and OMABCAST. In Section 8, the similarities and differences between two frameworks are discussed. Threats and vulnerabilities are reviewed in Section 9 and potential solutions to the security threats are introduced in Section 10. Finally conclusion is presented in Section 11.

2. DVB-H STANDARDS

The DVB-H system can be precisely defined as a transmission system built out of several DVB standards. ETSI standard EN 302 3048 has defined a DVB-H system in the Open Systems Interconnection (OSI) framework as a combination of technology elements of the physical layer, elements of the data link layer, and service information. ETSI EN 300 744, 4, ETSI EN 301 1929, ETSI EN 300 46810 are the main standards composing the system in these three layers[26].

3. SYSTEM DESCRIPTION

DVB-H is based on IP based transport. Video is typically carried using MPEG-4/AVC (H.264) coding of video signals, which can provide a QCIF coding at 384 kbps or less. Even a CIF video can be coded at 1 Mbps by using H.264 encoders. These encoders can work on real-time TV signals and provide MPEG-4/AVC-encoded output in IP format. As it is based on IP transport, DVB-H can support video and audio coding other than MPEG-4/AVC. Fundamentally, as an IP transport, it ultimately can support any AV stream type. In addition to MPEG-4, Microsoft VC-1 coding format is set out in the DVB-H standards. The resolution and frame size can be selected by the service provider to meet the bit rate objectives. The data is then transmitted by using an IP datacast.

In a typical DVB-H environment a number of TV and audio services may be encoded by a bank of encoders. All these encoders are connected by an IP switch to an IP encapsulator, which then combines all the video and audio services as well as the PSI and SI signals and ESG data into IP frames. The IP encapsulator also provides for channel data to be organized into time slices so that the receiver can remain active only during the times for which the data for the actively selected channel is expected to be on air(Fig 1). Another responsibility of IP encapsulator is providing a more advanced forward error correction code, which can deliver reliable signals in typical mobile environments.

Generally the data rate at the output of an IP encapsulator under DVB-H will be dependent on the modulation type used as well as the bandwidth available. Typically a DVB-H multiplex would be 11 Mbps of data, which could generate a carrier, e.g., 78 MHz when modulated. This can be compared with a 21-Mbps multiplex for DVB-T service in the VHF band. The effectively lower transmission rate for DVB-H is due to a higher level of forward error correction applied to make the transmissions more robust for the handheld environment [Leadership 2010].

The output of the IP encapsulator, which is in ASI format, is then modulated by a COFDM modulator with 4k or 8k) carriers. The COFDM modulation provides the necessary resilience against selective fading and other propagation conditions. The 4k mode has been made, as part of the DVB-H standards, for use in DVB-H as 2k carriers would not give adequate protection against frequency-selective fading and also provide for a smaller cell size owing to the guard interval requirement for single frequency

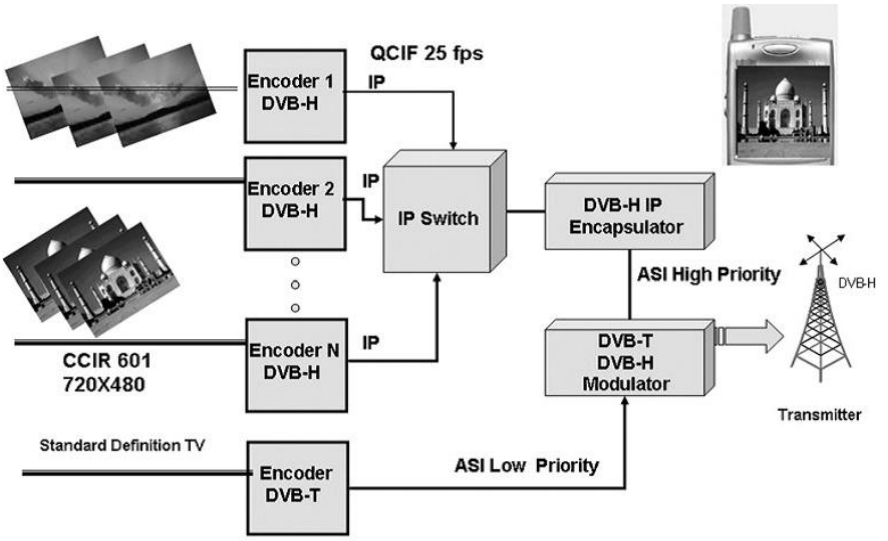

Fig. 1. A DVB-H MOBILE TV TRANSMISSION

networks (SFNs). At the same time the 8K carrier mode has the carriers placed too close in frequency for the Doppler shifts to be significant for moving receivers. The 4 k mode provides a better compromise between the cell size and the Doppler effects due to motion.

However, it should be recognized that the carrier mode actually used would depend on the frequency band employed. The modulation used for each of the carriers can be with QPSK, 16QAM, or 64QAM that DVB-H standard provides for COFDM modulation, which is suitable for SFNs. The system uses GPS-based time clocks and time stamping to ensure that all the transmitters in a given area can operate synchronously, which is needed for SFNs. This also implies that repeaters can be used in the coverage area at the same frequency and these repeaters serve to add to the signal strength that is received at the mobile.

4. SECURITY IN DVB-H

Two aspects of security can be examined in DVB-H including attackers view and insiders view. Attackers refer to those who threat the system, while insiders refer to those who want to protect the system from attackers. From insiders view, there are two main frameworks for DVB-H in order to protect the content and services. These frameworks are OMA-BCAST and IPDC [32] which are described here.

The Open Mobile Alliance (OMA) [Lian and Zhang 2009] has been working on a common standard for transport level security as well as content security in a frame work is called OMA-BCAST. The OMA-BCAST has been conceived as a broadcast-level security system that can work for all standards of mobile TV and multimedia transmissions, including DVB-T-, DMB, DVB-H, 3 GPP[Management and AllianceTM], and 3 GPP2[Alliance 2009] based systems. The advantage of OMABCAST as conceived by OMA is that such systems can be used independent of the operator or network.

The specification of the other approach, DVB-IPDC [32], was produced by the DVB ad hoc group Convergence of Broadcast and Mobile Services CBMS, which was formed in March 2001. In 2004, the group released a first set of detailed technical specifications for an IPDC in DVB-H system. DVB IP datacast has been defined within the framework of DVB-H and existing cell Phone networks. A DVB IP datacast system can thus be described as a system combining a unidirectional point-to-multipoint

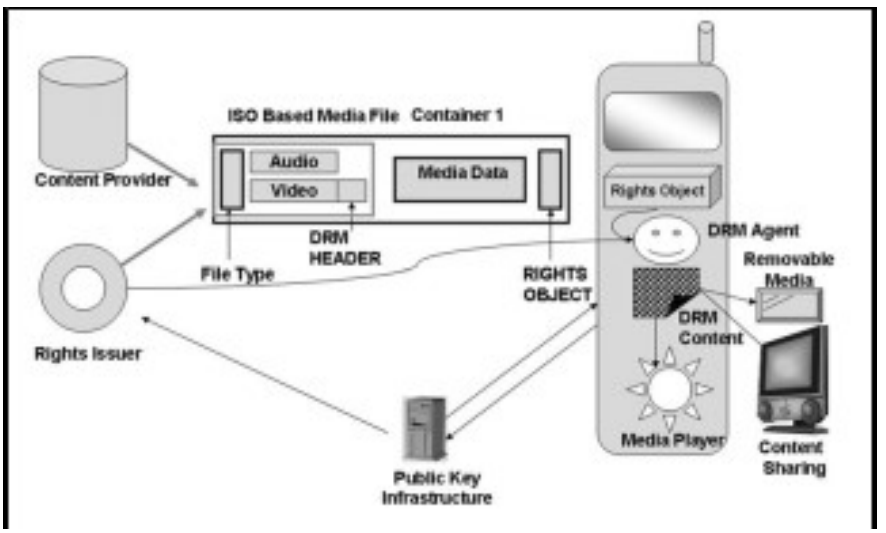

Fig. 2. DRM 2.0 OPERATION

DVB-H broadcast path with a bidirectional interactivity path, typically a cellular communication network such as General Packet Radio System (GPRS) or Universal Mobile Telecommunications System (UMTS). Both paths are based on the IP protocol, hence the IP datacast name. IP datacast also makes the very large amount of existing IP-based digital content services available with little or no modifications required for broadcasting over DVB-H: video streams, web pages, music files, software, and so on.

DVB-H is not restricted to a physical layer as it was first in mind, it is planned to be finally used with all DVB mobile video systems like DVB-SH, and i[14]n a larger perspective with all systems offering an IP interface

5. 5 IPDC AND OMA-BCAST CONVERGENCE

In business area, content owners are more concerned about the content security of individual items, e.g., pictures, video, music, e-books, programs, and games than the security of the transmission systems that protects the revenues of the pay-TV operators.

Pirate sharing of copyrighted videos and music, has led the multimedia industry toward the content digital rights management (DRM). DRM dictates rights of viewing or listening, reading, or forwarding each item which can be controlled by the license holders [Functioning et al.].

The OMA DRM 1.0 was released in November 2002. Release1 was always considered as temprorary until DRM 2.0 was finalized and released in December 2004. Release 2.0 is a practical version which provides for the use of the PKI for key management and higher level of security in end-to-end DRM systems. DRM 2.0 defines actors, which define various roles in the DRM management process. Main structure of DRM consists of a DRM agent, content provider, a right issuer and a certification authoithy [Hand-in hand et al.] [Wright 2006]. Figure 2 shows DRM 2.0 structure.

DRM 2.0 specifies the use of various protocols for operating in the PKI environment such as the 128-bit AES and RSA-PSS (signature algorithm). It specifies a DRM content format (DCF) for discrete objects such as pictures and a packet sized data format for continuous video (e.g., in streaming video).

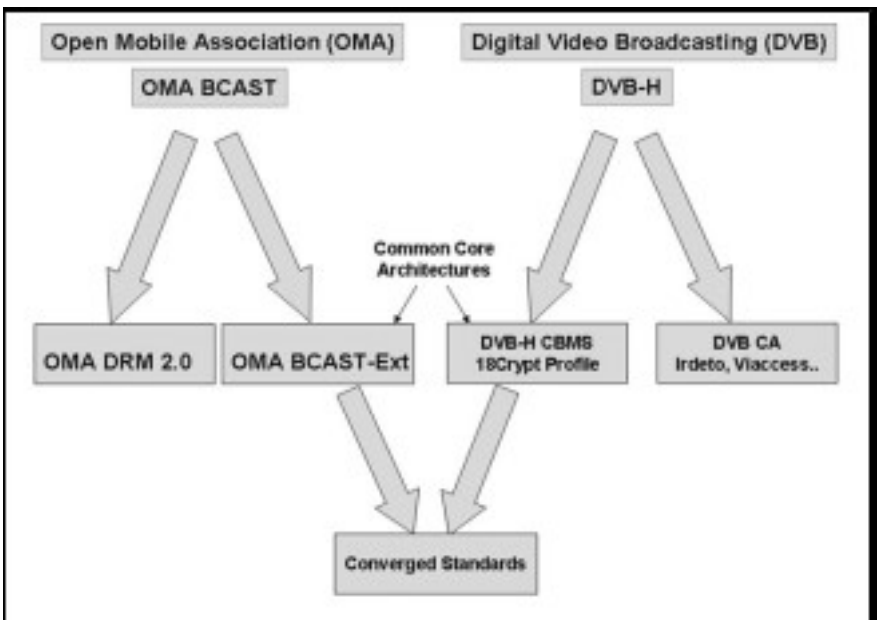

Fig. 3. CONTENT SECURITY IN MOBILE TV INDUSTRY

OMA DRM 2.0 [Buburuzan et al. 2007] is primarily meant for content security and rights management for downloadable objects. As there are no mechanisms for continuous change of keys in OMADRM 2.0, It is not scalable to provide broadcast mode content security.

Later, both DVB and OMA were working toward open standards for broadcast level content security. Under DVB the initial Digital Video Broadcasting-Convergence of Broadcasting and Mobile Services (DVB-CBMS) was progressed. The DVB-CBMS specifications were released in December 2005, while the OMA-BCAST specifications were set for 2007 release.

The DVB-CBMS is supported by a number of operators and handset manufacturers, including Nokia. Both DVB-CBMS and OMA-BCAST have common core architecture and four-level key structures. The DVB-CBMS release is based on a profile called 18Crypt. The 18Crypt profile is also an option in OMA-BCAST and is based on OMA DRM 2.0[Buburuzan et al. 2007].

The OMA-BCAST as an umbrella standard is expected to provide content level security under OMA DRM 2.0 and broadcast security through extensions to the DRM for live TV (Figure 3). 18Crypt profile is set to exclude as a common profile for implementation of open content protection systems as well [Lian 2009].

6. SERVICE AND CONTENT PROTECTION OVERVIEW ON IPDC AND OMA-BCAST

IPDC and OMA-BCAST apply as two frameworks for service and content protection in DVB-H. To achieve these frameworks, IPDC and OMA BCAST released two documents as SPP [15] (service purchase and protection) and SCPMBS [33] (Service and Content Protection for Mobile Broadcast Service).

6.1 Service Purchase and Protection in IPDC

The SPP in DVB-IPDC is based on a four-layer model Figure 4 At the fourth level, the content and services are encrypted by Traffic Encryption Key (TEKs). The encryption can be performed on the link layer, on the session layer or on the content layer, while the TEKs change frequently in order to prevent

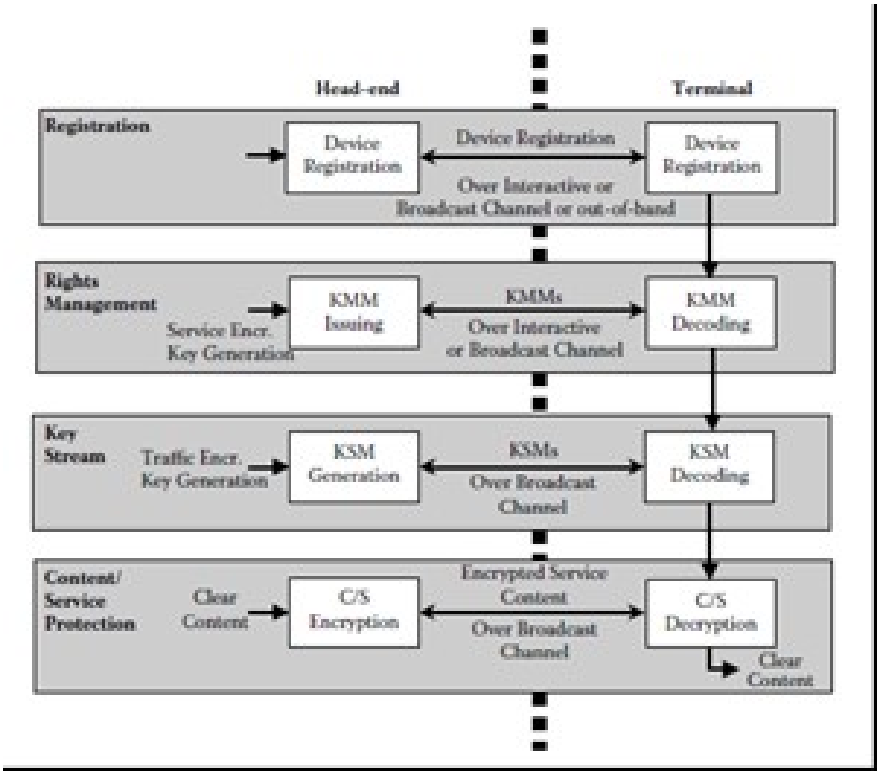

Fig. 4. DVB-IPDC SPP MODEL

real-time key distribution attacks. IPDC use IPSEC, ISMACryp, or SRTP for encryption but IPSEC and ISMACryp is strongly recommended [Lian 2010] [Mason 2006].

The third level or key stream layer is responsible for the delivery of the service encryption keys (SEK). SEKs are TEKs keys that are encrypted and are transmitting over so-called Key Stream Messages (KSMs) via the DVB-H channel.

The rights management layer grants access rights to content and service to the requesting devices. The authorization can, for example, be in the form of a service encryption key that can be used to access the KSMs. These messages, called the key management messages (KMMs) or entitlement management messages (EMMs) can be delivered via the DVB-H channel or the interactive network.

The first-level layer in this model is responsible for registration of the devices. In the SPP model, this may be performed via an out-of-band interface (for example, by buying a prepaid card), via the broadcast channel or the interactive channel.

The IPDC specification defines an overall option that slightly changes the procedures at the key stream, rights management, and registration layers level. The first solution called 18Crypt profile can use a solution based on the digital rights management (DRM 2.0) specifications both for registration and for rights management over an interactive channel and specifies a set of protocols to be used for outof- band channels, in a fashion already used by existing cellular nrtworks.

The second solution is called the IPDC SPP Open Security Framework or OSP. The major difference between the two is that 18Crypt is fully specified with respect to the four-layer model of IPDC SPP, while the OSF considers key stream and rights management to be private and only defines an interface

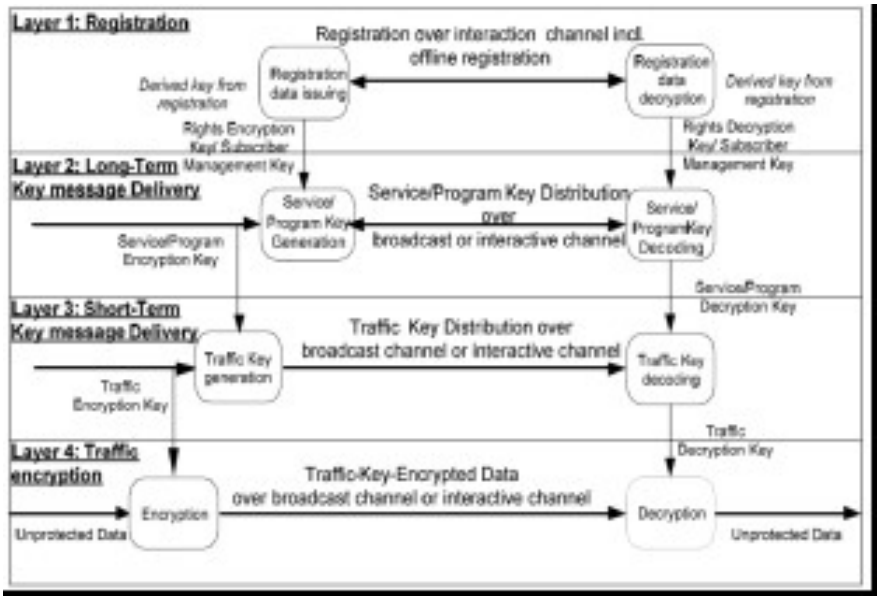

Fig. 5. OMABCAST 4-LAYER SCPMBS STRUCTURE

that can be used to interact with any external key management system[Broadcasting] [Study]. In both cases, the encryption at the content/service protection layer remains identical.

6.2 SCPMBS in OMABCAST

Just like SPP, OMABCAST working group defined two profiles for more flexibility on user terminal side: DRM profile and Smart Card profile. DRM profile uses DVB SPPs 18Crypt profile and uses the OMA DRMv2 [Buburuzan et al. 2007] mechanisms for rights management and key material exchange and also registration .Although this profile can support interactive channel with DRM2 profile, the focus is on broadcast properties and out-off-band channels.

Moreover, Smart card profile [Study] needs interactive channel all the time for key management and registration. It use 3GPP MBMSs key management and USIM/(R-)UIM/CSIM smartcard for key generation and key management as well.Same as IPDC, OMABCAST follows 4-layer model Figure 5. At fourth layer the content is encrypted by traffic encryption keys (TEK). The method of encryption is used can be different kinds. At third layer TEK is generated and sent as an encrypted message over Short Term Key Messages (STKM). TEK is encrypted by Service or Program Encryption Key (SEK/PEK).

At second layer SEK and PEK keys are generated and sent over long term key message (LTKM). STKMs contain content IDs for the program or service. Devices use this ID to identify which Long Term Key message (LTKM) to use for decryption of Short Term Key messages.

Finally, at first layer, depending to key management profile used DRM2 or smart card, Rights Encryption Key (REK) or the Subscriber Management Key (SMK) is used to protect the LTKM delivery. REK or SMK are generated from registration in this layer.

7. IPDC AND OMABCAST DIFFERENCES AND SIMILARITIES

As the OMA BCAST and IPDC stem from different Back grounds (cellular and broadcast), there are particularities that makes them suitable for different deployment scenarios and different kinds of net-

work operator. However, there are a lot of similarities between these two regarding to used technologies and also created market [Buburuzan et al. 2007].

Advanced Encryption Standard (AES) 128 and authentication algorithm HMAC-SHA-1-96 are the examples of similar technologies which have been used in IPDC and OMABCAST in different layers. IPDC and OMABCAST present similar authentication and encryption method on protecting content and stream in different layers like link layer, session layer and content layer.

Moreover, both solutions use the OMA DRMv2 [Buburuzan et al. 2007] framework for rights management and extension profile for stream content. However, the IP Data cast OSF supports the use of another rights management framework.

8. SECURITY THREATS AND VULNERABILITIES

The security treats in DVB-H can come from various ways and domain. It can be attacks on the protocol, attacks on the key, attacks on the media flow and attacks on the encryption and decryption modes.

8.1 SERVICE ROBBERY

Service Robbery is the most common threat in broadcast system. Fundamentally, broadcast system has two properties [16]: 1) All users received the same signal and 2) Broadcaster has no access and control who will receive the signal. Thus, Conditional Access System [16][25] are designed to ensure that only legitimate subscribers can receive the content that been broadcast. Practically, it is achieved by Content Encryptions and Content Key Delivery via the secure channel to each of entitled users. Due to the issue in key deliverables such as number of keys to be sent, keys are broadcast to all users but in parallel message are sent to the users whether or not they are entitled to use the key. Conditional Access System [Tu et al.] commonly depend on the operator business models such as subscription , Pay-per-view, Pay-per Time or others various conditional Access model. This mechanism can prevent from service robbery.

Tim Wright [Lian et al. 2009] in his paper highlights security attacks on the protocol and the content itself. He divides the attack into three parts which are: 1) Extraction of the keys from legitimate users terminal, 2) Distribution of the keys to non-legitimate user, and 3) Insertion of the keys by non-legitimate user.

—Key extraction attack: Key extraction is when one of the keys (service keys, Traffic Encryption Keys and primary keys) is extracted from the authorized receiving terminal. Attack in on the primary keys in the 18Crypt specification and main key in the USIM in the Smartcard profile

—Ditribution key attack: The attacks occur when service keys are extracted from the terminal of legitimate user, then the key is distribute to be used in un-legitimate users mobile terminal.

—Re-insertion key attack: Traffic key is encrypted with a service key to be delivered directly to the mobile terminal using the broadcast key stream layer. Attacker may use the traffic keys obtain to re-insert into an unauthorized terminal. The keys can be used to decrypt the key stream message obtained on the broadcast system.

8.2 DENIAL OF SERVICES

Beyond Service Robbery, Denial of Services could be one of the attacks in the integrity of the broadcast services. [16] illustrated the DoS attack into two: 1) Service Corruption and 2) Service Replacement. Service corruption is when attackers launch or inject corrupted packets in the system to harm the system and stop the operation In order to prevent from this attack, an integrity check approach based on cryptographic is used where the integrity messages is insert into the broadcast data. If the message cannot be confirmed, the broadcast data will be ignored and the receiver will stop its operation. Another

concern of denial of service attack is Service replacement where valid data is replaced with other data. This attack sometimes called as broadcast terrorism in reference to the pirate broadcast that partly replaced the sports channel over a Chinese satellite broadcast during the 2002 Soccer World Cup. Cryptographic approach such as hashing can be used to protect and authenticate from such integrity attacks. The receiver will compute the integrity check on the data and compared with the transmitted value. If it is not match, the receiver will stop the operation and display the error messages. Although these service corruption and service replacement are possibly happened in the broadcast services, but it haves more concern on attacker sides as they have to invest a lot of money for the costly equipment and takeover the central head-end. Thus, the best protection for this attack as highlighted by [16] is the physical security protection for broadcasting infrastructure compared to cryptographic mechanism protection.

According to [17] [Joan et al. 2001], three main domains in video streaming that could possibly been attack and cause the denial of service (DoS) to the system are: (i). Session Initiation Protocol (SIP), (ii) media flow and (iii) IP. Session Initiation Protocol (SIP) is used for session management between the client and server. As highlighted in [17], SIP is most vulnerable to many threats and requires strong protection against attacks. There are four common attacks against SIP[Chen 2006].

Invite Flooding Attack: P-CSCF (Proxy Call State Control Function) is overload with an SIP invitation message that sent by an attacker. When there is incoming invitation message, P-CSCF will parse, modify, forward and save the states of transaction. If there are non-stop incoming messages from an attacker at one time, this cause the traffic become congested and it may fail to response to messages sent by legitimate user.

—Register Flooding Attack: Attacks in Register Flooding are same with Invite Flooding Attack. An attacker manipulates the register method in two ways i.e. Legitimate and fake message flooding. For legitimate message, the attacker uses the valid account to send the messages but for fake message, the attacker sent the fake request to the SIP.

—Invite Response Flooding Attack: Using Brute Force Attack, an attacker try to crack the authentication ID by launch an invitation message to be response by the register.

—The Cancel Attack: An attacker may use the cancel method by pretending to be a legitimate user and cancel an Invite Request sent by P-CSCF.

According to [Joan et al. 2001], Real Time Transport Protocol (RTP) and Real Time Transport Secure Protocol (RTSP) are the protocols used for media streaming for multimedia mobile broadcasting. The well-known attacks on the media flow protocols that cause the Denial of Service (DoS) are:

—Jitter Attack: The attacker sends RTP packets to media client with garbage contents including random data in packet header and payload. So the media client receives the bad quality of multimedia.

—Session Tear down Attack: To terminate the media session, the BYE request is used. In order to tear down a session, an attacker may send a faked BYE request to multimedia server via P-CSCF. As a result, multimedia server immediately stops the RTP flow.

—Session Modification Attack: By using the offer-answer model, a successful Invite Request established both a dialog between two user agents and a session. The purpose of Re-Invite method is to modify the actual session. The modification may change the address or ports, deleting a media stream, adding a media stream and so on. Therefore by sending the forged Re-Invite message, the attacker could launch a Denial of Service attack to enforce any unauthorized modification.

Several possible attacks on transport and IP layers can cause the Denial of Services (DoS) attack as highlighted in [Joan et al. 2001].

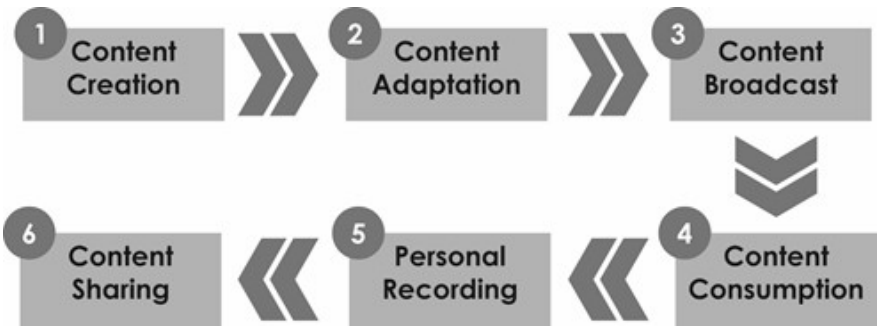

Fig. 6. MOBILE BROADCASTING CONTENT LIFE CYCLE

—TCP SYN Flooding Attack: SYN flooding attack is a TCP layer flooding attack. By creates number of half-open connections, an attacker send SYN messages to a targeted server with a spoofed return address that cause the server never received the final ACK. As a result, an at-tacker creates increasing number of pending connections, causing the buffer and memory to overflow. The attacker could also use multiple hosts to launch distributed SYN flooding attack.

—ACK Flooding Attack: ACK flooding attack is same with SYN flooding attack but it launch in reverse direction by exploiting the answer packets. An attacker send packets to randomly chosen destination IP addresses and forges the sources address of the packets to the victims address.

—Smurf Attack: ICMP echo request packets directed to IP broadcast address from remote location to cause a denial-of-services attacks. An at-tacker creates ICMP echo request packet by spoofing his address and creates forged packets containing the victims IP address as source address. This attack cause the machines at the intermediarys site respond to the ICMP echo requests to overwhelm.

Suomalainen [Joan et al. 2001] in his study shows that content on mobile broadcasting goes through six phases of content life cycle as illustrated in fig 6, which different phases have different threats on it.

—Phase 1 - Content Creation: Content created for different content providers e.g.: for mobile broadcasters and fixed television broadcasters.

—Phase 2 - Content Adaptation: Mobile broadcast service providers adapt content for mobile terminal.

—Phase 3- Content Broadcast: Content transmit over the air into receiving mobile terminals.

—Phase 4 - Content Consumption: Users receive the content at real time via mobile terminal system.

—Phase 5- Personal Recording: Users may view the content receive instantly or make personal recording to view the content at later time or even view the content more than once.

—Phase 6 - Content Sharing: Users may share content with others.

In [Joan et al. 2001], mobile broadcast contents are categorized in to six (6) types as shown in table I. Different types of content have different security requirements. Subsidized content are not paid by the users but it is bare by the company that advertise the content for example the commercials content. So, this type of content is does not need any protection for piracy. Time dependent content is only for certain period of time such as news and interactive data services, though it is only for authorized users, unauthorized sharing of this type of content does not cause any significant economic threat. Location dependent content may available for a longer period of time. Although this type of content has smaller market but it is still requires content protection as it may still emerge into file sharing networks. Audio video entertainment content is the highly demand content that valuable for a longer period

Table I. TYPES OF MO-BILE BROAD-CAST CON-TENT

Type	Content Examples
Subsidized content	Commercials
Time-dependent pay-TV	News, Traffic info
Interactive data services	TV guide, games
Location-dependent pay-TV	Traffic info, tourist info
Audio content	Radio, music
Entertainment pay-TV	Movies, music videos, comedy

of time compared to others. This type of content has high potential of unauthorized sharing of being uploading and downloading into file sharing networks. However, this content is created exclusively for mobile terminals so it does not cause direct threats to the markets of high-quality content which are suitable for fixed televisions.

Four different actors with different motives and as-sets that need to be protect in mobile broadcast environment. The actors, motives and their relationship are illustrated in fig 7. Content Owners need to prevent their content from unauthorized use and sharing. They have to protect the quality of content for mobile terminals and fixed televisions are not the same quality. The content owners require the whole process of mobile content life cycle if well-protected before they are ready to release the con-tent. Secure broadcast service with high protection mechanism is important for Content broadcasters. They want to ensure that only authorized users can receive the con-tent via dedicated broadcast medium; and no others alternative channels for receiving the content.

Receiver providers need large amount of content available to make the products is desirable for common users. In order to prevent needs to support for many protection technologies and content formats, there should be only one or few protection standards that can standardized technologies to enabling interoperability.

The most important for users are the availability of the content. Users want to view the content without any security troublesome issues and by using the same interface for both protected and unprotected content. Besides that, they also need the option to make a record to view the content at their own preferred time and store the content into other devices as well.

According to Suomalainen in [Joan et al. 2001], there are three (3) main threats against three security critical phase of mo-bile broadcasting. Fig 8 illustrates relationships be-tween building blocks, threats, and security critical phases of content life cycle as well as protected content types.

—During the broadcasting phase, content may be received by unauthorized users.

—When content is consumed and in terminals memory, analog or digital copies can be taken.

—Copies of content can be shared between unauthorized users.

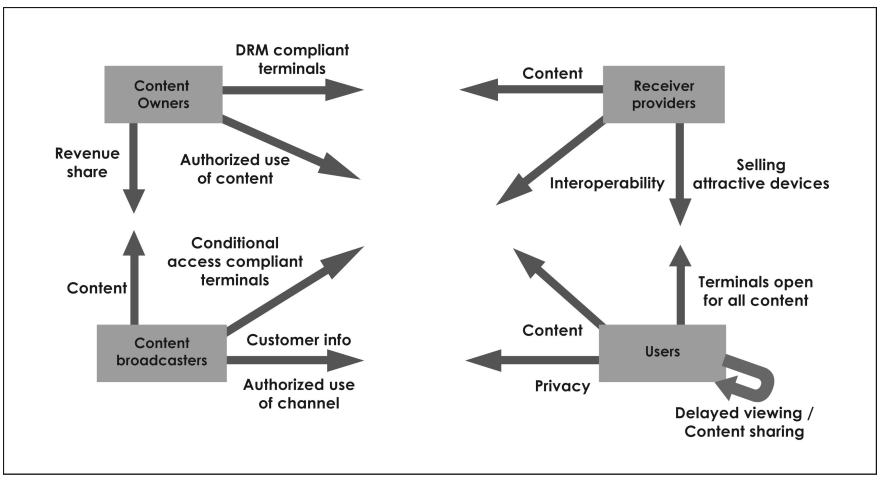

Fig. 7. ACTORS AND MOTIVES IN BUSINESS ENVIRONMENT OF MOBILE BROADCAST

9. PROPOSE SOLUTION TO THE SECURITY THREATS

9.1 PROPOSED SOLUTION BY LIAN, DONG AND WANG

A secure solution for video broadcasting has been pro-posed in [Suomalainen 2005]. It outlines three important keys i.e., business model, content encryption modes and secure inter-action protocols. The proposed secure system architecture is shown in Fig reffig:fig9. Three important keys are [TV et al.]:

—Business Model: As proposed by, Mobile terminal only decrypts and plays the base layer content; Home TV decrypts both base layer content and enhancement information. The charges for base layer content and enhancement information are based on the business model that categories into three, free model, once-pay model and twice-pay model whereby the free model is for free content, once-pay model is when only base layer content is chargeable through mobile terminal; and twice-pay model when both base layer content and enhancement in-formation are chargeable through mobile terminal.

—Content Encryption Modes: In line with the business model proposed, there are three content encryption modes to be used in order to differentiate the content. In the first mode, both base layer content and enhancement information will not be encrypting. Thus, it can be represent as C = $X||Y$ where C is encrypted content, X is the base layer content and Y is enhancement information.

—Secure Interaction Protocols: The purpose of this protocol is to provide the secure content transmission and user interaction. Fig 10 shows the secure interaction protocol process. As shown in Figure 2, there are four (4) parties that have different keys i.e., Content Server, Rights Issuer, Mobile Terminal and Home TV, as shown in table reftab:tab3 [Sher and Magedanz 2007].

In the second mode, only the base layer content is encrypted.

C= $X||Y$; where X = Ec (X, K0). Ec () is the block function, and K0 is the encryption key.

In the third mode, both base layer content and enhancement information are encrypted using 2 different keys.

C= $X||Y$; where X = Ec (X, K0) and where Y = Ec (X, K1). Ec () is the block function, and K0 is the key 1 and K1 is key 2.

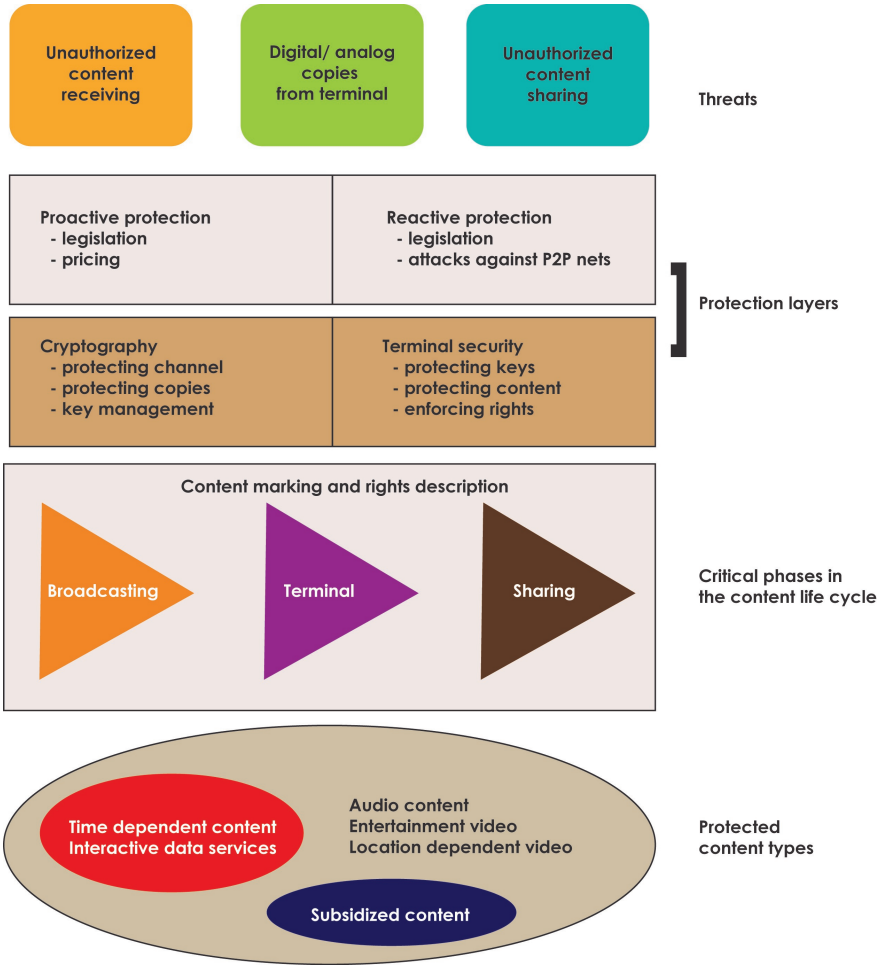

Fig. 8. Protection Layers

Different content encryption modes can be classified into three modes as shown in Table II [Sher and Magedanz 2007]. Flag F is composed of two binary bits to differentiate the different encryption modes.

These are following steps in the process:

—Mobile Terminal sends service request to Rights Issuer.

—Right Issuer then authenticates Mobile Terminal and charges the payment.

—Rights Issuer will encrypt, signs and sends User Rights to Mobile Terminal using the following encryption method [Sher and Magedanz 2007]. Rm = E (Rm || E (H (Rm),Krs), Kmp) whereby E() is the encryption function of a public cipher, H() is a hash function, Rm contains the content encryption key, K0 is the encryption flag.

—Mobile Terminal authenticates User Rights integrity, decrypts the TV content and plays the content. In content decryption, Mobile Terminal decrypts base layer X according to F. If F=01 or F=10, the content is decrypt using block decryption function X= Dc (X, K0).

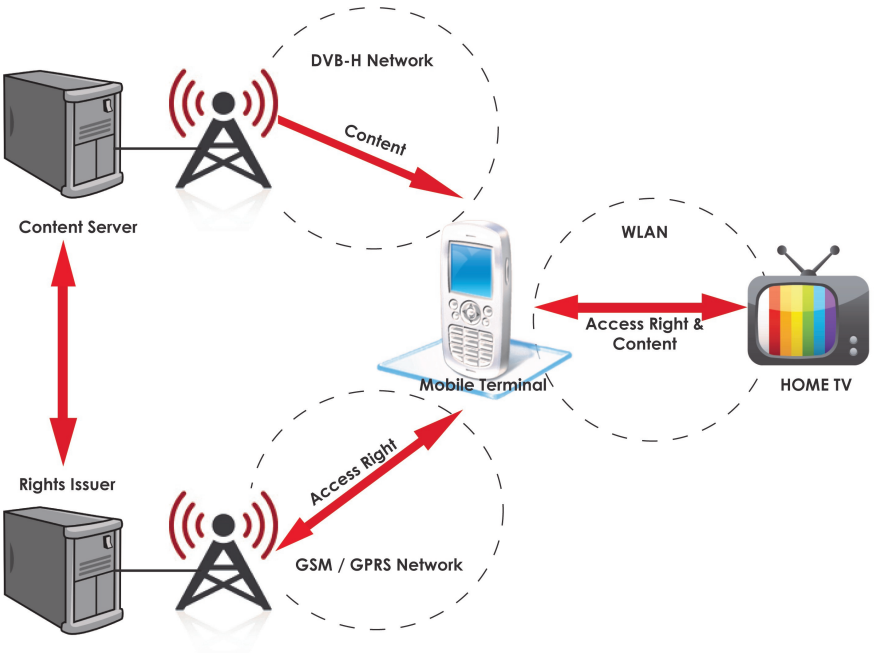

Fig. 9. Proposed Secure System Architecture

Table II. CONTENT ENCRYPTION MODES & BUSINESS MODEL

Mode	Flag (F)	Ciphertext (C)	Business Model
0	00	$X\|\|Y$	Free Channels
1	01	$X\|\|Y$	Once-pay channels
2	10	$X\|\|Y$	Twice-pay channels

(Kc Content Encryption key, Krp, Krs Right Issuers public key and secret key, Kmp, Kms Mobile Termi-nals public key and secret key, Khp, Khs Home TVs public key and secret key).

9.2 2 PROPOSED SOLUTION BY SHER AND MAGEDANZ

According to proposed security enhancement by Sher and Magedanz in [Joan et al. 2001], Intrusion Detection and Prevention system (IDP) is to enhance the existing security against Denial-of-Services (Dos) and Distributed (DDos) attacks which are difficult to eliminate by low-layer security mechanisms.

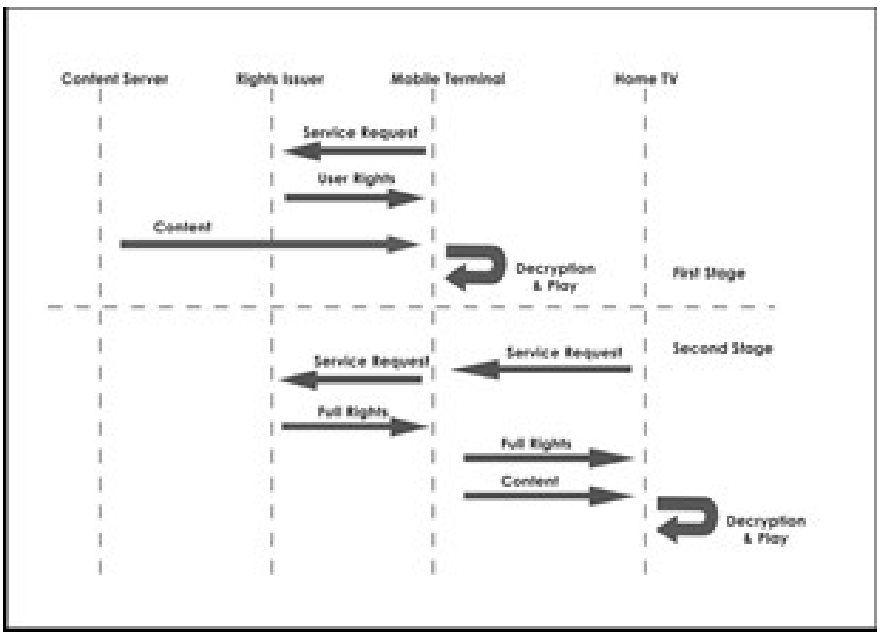

Fig. 10. Secure Interaction Protocol Process

Table III. KEY SETUP IN DIFFERENT PARTIES

Content Server	Rights Issuer	Mobile Terminal	Home TV
Kc	Krp	Kmp	Khp
	Krs	Kms	Khs
	Kmp	Krp	Kmp
		Khp	

As in Fig 11, all incoming SIP messages between client and server are passed through the IDP center that maintains a list of Partner. The SIP Stack is responsible for exchanging of SIP messages with S-CSCF via the IP multimedia Service Control Interface (ISC). Each user represents a communication partner that exchanges SIP messages with IMS based Streaming Service Enabler (SEE). A partner is identified with SIP URI. Each partner has state and number of messages sent or received Once IDP Center receives SIP message, it updates the state of corresponding partner and created a new partner if it does not exist in the list. Then the IDP filters compares it with the rules loaded in the Rule Collection. If a partner matches with any attack patterns, the IDP Center will move the partner into the blacklist which is maintains the URIs of the entire malicious communication partner. Every message sent from or to a malicious partner in the Blacklist is automatically denied by the IDP Center. Otherwise, the

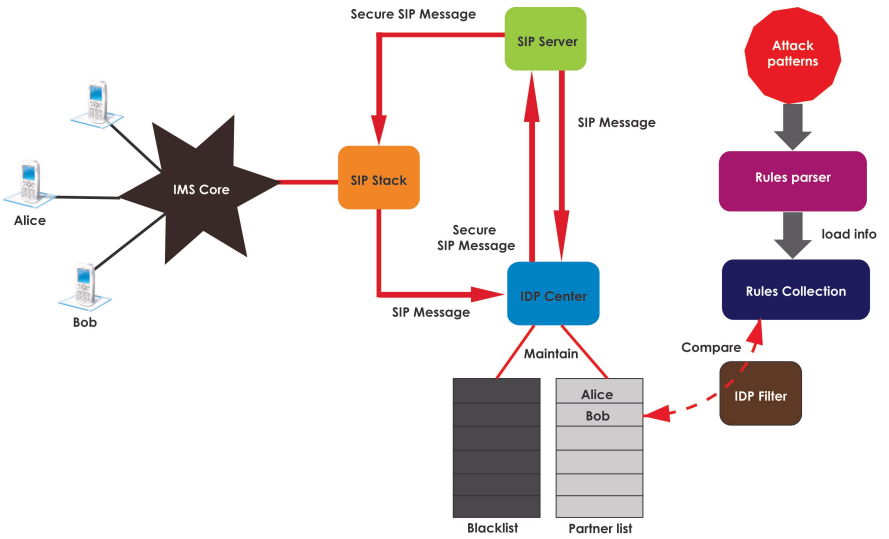

Fig. 11. Architecture of IDP for Mobile Multimedia Broadcasting

IDP system considers the incoming SIP request is secure and forward it to the SIP Server which is responsible to processes the incoming and originating SIP messages

9.3 PROPOSED SOLUTION BY LIAN AND ZHANG

The architecture of the proposed secure mobile TV mechanism as proposed by Lian and Zhang [Lian and Zhang 2009] is shown in Figure 12. They divide the infrastructure into four components: (i) Content server, (ii) Content Provider, (iii) Service Provider, and (iv) Mobile Terminal. The content server used to scrambling the TV content and delivers the scrambled content to the content provider. Content Server forms the service guide with the content list based on the service request and sends the service guide to the service provider. Mobile terminal receives the scrambled content from the content provider. Then receives the user right information from the service provider and descrambles the content with the SIM Card under user right control. Mobile Terminal authenticates the user using the fingerprint scanner to prevent from any unauthorized users to use the services. As proposed by Zhang and Lian [Lian and Zhang 2009], there are two important phases in protecting the mobile TV content: 1) the generation of scrambled content and management information and 2) the descrambling of TV con-tent as shown in Fig reffig:fig13.

9.3.1 *GENERATION OF SCRAMBLED CONTENT AND MANAGEMENT INFORMATION.* Content Server generates the scrambled content and Entitlement Management Message (EMM). The scrambled content is the combination of the content itself and the Entitlement Control Message (ECM) that contains the scrambling key; EMM contain the user right for the TV content. Then, the generated scrambled content is transmitted from content provider to mobile terminal and management information from service provider.to mobile terminal.

9.3.2 *DESCRAMBLING OF TV CONTENT.* Mobile terminal request the mobile TV service to receive the multimedia content and management information. Once authenticate, the contents are descrambles.

Service provider broadcasts the Electronic Service Guide (ESG) which includes the TV channels, TV pro-grams and time table to potential users. User sends a service request to service provider via

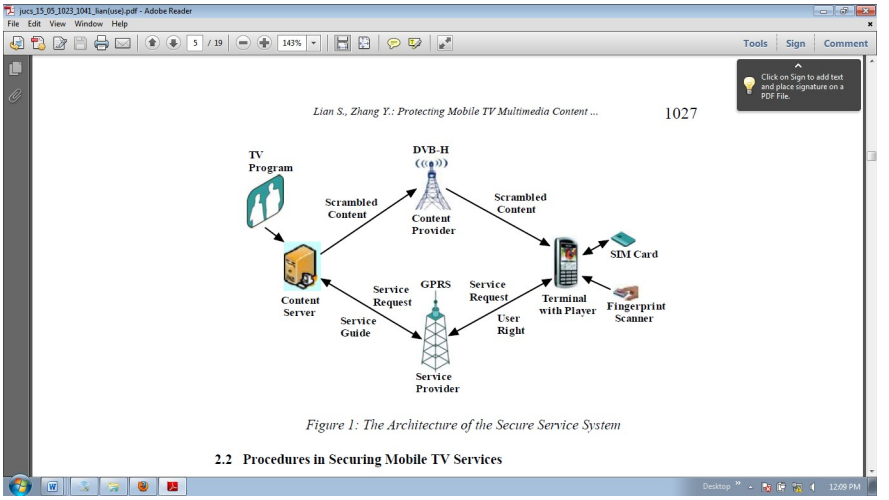

Fig. 12. The Architecture of the Secure Service System [Lian and Zhang 2009]

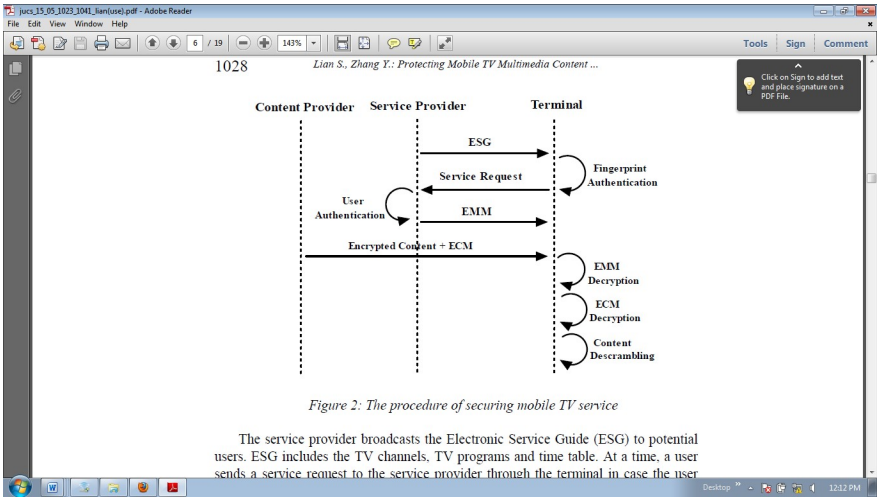

Fig. 13. The procedure of securing mobile TV service [Lian and Zhang 2009]

terminal to authenticate the fingerprint of the user. Once authenticated by identify the information in the SIM Card, the users service information is stored in a database including the requested programs, service lasting time and payment. Then the service provider transmits the EMM that contains the user access right to the mobile terminal. Terminal decodes the EMM and ECM before the TV pro-gram can be played on the terminal on the basis of granted access right.

10. CONCLUSION

In this paper, we had concise review on DVB-H system structure and standards and two important security frameworks for service and content protection in DVB-H: OMABCAST and IPDC. Moreover, we have highlighted some security threats in Digital Video Broadcasting like Service Robbery and denial-of-service attacks (Dos) also we had reviewed different threats on Session Initiation protocol

(SIP), Real Time Transport layer protocol (RTP) and IP as common and serious threats and vulnerabilities in mobile streaming services. We have also studied the proposed structure that is more secure for content encryption and content trans-mission in mobile video broadcasting. This structure is examined from three aspects, including: Business model, content encryption modes, secure interaction protocols. It can be seen, although two frameworks presented for DVB-H security (OMABCAST and IPDC) somehow simultaneously, both have more similarity than focusing on existing DVB-H security threats and vulnerabilities. Hence new consideration and updated security frameworks are needed for DVB-H with better security aspects.

REFERENCES

O. M. Alliance. 2009. *Service Guide for Mobile Broadcast Services*. 1232 pages.

D. V. Broadcasting. *Mobile TV (DVb -H) OMA BCAST SMART CARD profile*. (n. d.).

D. V. Broadcasting. 2009. EN 300 744 - V1. *6. 1 - Digital Video Broadcasting (DVB) ; Framing structure, channel coding and modulation for digital terrestrial television* 1, 1 (2009).

T. Buburuzan, G. May, and K. Daoud. 2007. *Service and Content Protection in Mobile Multimedia Broadcast Pro IEEE International Symposium on Consumer Electronics*. 16. doi:10.

Eric Y. Chen. 2006. *Detecting DoS Attacks on SIP Systems*. IEEE Workshop on VolP Management and Security.

J. K. Elisa, M. Uronen, and F. (n Virium. *d.)*. User Acceptance of Mobile TV Services. 1–88 pages.

T. H. E. Functioning, O. F. M. The Dvb-H Handbook The Functioning Tv, and Planning. *(n*. d.).

H. to-head Hand-in hand, H. L. Digital Rights Management Mckinley, and XML Security Protocols. *Management*. (n. d.).

Feigenbaum Joan, Reedman Michael J., Sander Tomas, and Shostack Adam. 2001. *Privacy Engineering for Digital Rights Management Systems*. Proceedings of the ACM Workshop on Security and Privacy in DRM.

D. I. (n Leadership. 2010. d.). *Discretix MuLian, S. Content and Service Protection for the Ubiquitous TV. Wireless Personal Communications* 10. (2010), 19–34.

S. Lian. 2009. *Secure service convergence based on scalable media coding*. Telecommunication Systems. 21–35 pages.

S. Lian. 2010. Content and Service Protection for the Ubiquitous TV. *Wireless Personal Communications* 10. (2010), 19–34.

Shiguo Lian, Yuan Dong, and Haila Wang. 2009. *A Secure for Ubiquitous Multimedia Broadcasting*. Proceedings of the 2009 IEEE ICC, Beijing, China.

Shiguo Lian and Yan Zhang. 2009. Protecting Mobile TV Multimedia Content in DVB/GPRS Heterogeneous Wireless Networks Journal of Universal Computer Science. 15, 5 (2009), 1023–1041.

Digital Rights Management and Open Mobile AllianceTM. $OMADRM-v2_0$.

S. Mobile TV. Mason. 2006. *Ebu Technical Review*. 1–7 pages.

C. Protection. 2006. *Service and content protection for mobile tv (Dvb-H) OMA BCAST SMARTCARD PROFILE*.

Muhammad Sher and Thomas Magedanz. 2007. Mobile Multimedia Broadcasting Vulnerability Threats, Attacks and Security Solutions. *Proceedings of the 9th International Conference on Mobile and Wireless Communications Networks. Cork, Ireland : September* 19-21 (2007).

I. C. (n Study. *d.)*. 3 ITALIA CASE STUDY With Nagravision Technology at its heart OPERATORS PREMIUM MOBILE TV.

Jani Suomalainen. 2005. *Content Protection and Authorized Sharing for Mobile Broadcast*. Helsinki University of Technology.

Fu-Kuan Tu, Chi-Sung Laih, and Hsu-Hung Tung. *On Key Distribution Management for Conditional Access System on Pay-TV System*.

M. TV, O. M. A. Bcast, D. R. M. Profile, O. M. A. B. Smartcard, and D. ipdc O. S. Framework. *White paper OMA BCAST Smartcard profile for unconnected devices (n*. d.).

Tim Wright. 2006. Security Considerations for Broadcast Systems. *United Kingdom: Elsevier Ltd. Page* 137 (2006).