Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **3**, July **2014**

A Novel Frequency Billing Service in Digital Television System

Cheng-Chi Lee[1,3], Chun-Ta Li[2,*], Ping-Hsien Wu[1]

[1]Department of Library and Information Science
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang Dist.
New Taipei City 24205, Taiwan, R. O. C.
cclee@mail.fju.edu.tw

[2]Department of Information Management
Tainan University of Technology
529 Zhongzheng Road, Tainan 71002, Taiwan, R. O. C.
th0040@mail.tut.edu.tw
*Corresponding author

[3]Department of Photonics & Communication Engineering
Asia University
No. 500, Lioufeng Road, Wufeng Shiang
Taichung 402, Taiwan, R. O. C.

Received March, 2013; revised January, 2014

Abstract. *DTV services are getting widespread use, requiring service providers to have effective methods for remotely configuring and managing DTV set-top boxes (STBs). Solutions for such remote management are becoming standards-based. In this paper, we first propose a secure frequency billing service in DTV broadcasting. The billing system can provide users a more convenient way for payment. For charging in traditional television, many billings are half-yearly done. However, in the proposed protocol, users can watch TV in their free time and take single billing method. As a result, users can choose the most suitable billing methods according to their requirements. Moreover, the proposed protocol is more efficient than other previously proposed protocols by eliminating exponentiation operations which are time-consuming computations. Finally, our protocol not only provides better way for DTV charging but also prevents two common serious problems in DTV broadcasting such as smart card cloning and replay attacks.*
Keywords: Digital television (DTV) broadcasting, frequency billing service, set-top box (STB), replay attack, smart card cloning

1. **Introduction.** Billing system operators are now interacting with their viewers on many levels, offering them a greater program choice than ever before. Additionally, the deployment of a security system or conditional access (CA), as it is commonly called. Network operators have begun deploying DTV services — television and content-on-demand services delivered over managed broadband networks — to the home over the past few years. As DTV services mature and become more widely deployed [6, 12, 13, 18, 19, 28], service providers must have an efficient way to remotely configure and manage DTV set-top boxes (STBs), which terminate the DTV service in the user's home, render the content for display on the TV set, and allow user interaction via a remote control. DTV

is a convergence service of broadcasting and telecommunication that delivers multimedia contents over the Internet. Recently, DTV services are being extended to mobile terminals. Mobile DTV enables to provide multimedia contents to subscribers anywhere, anytime, and even in motion through wire and wireless networks [2, 22]. Mobile DTV services are undergoing security problems such as illegal access by unauthorized users [21], session key intercepting, illegal content distribution, etc. Therefore, mobile DTV services require basic security functions like user authentication, secure key exchange [4], and contents protection.

Since most DTV broadcasting is unidirectional and there is no online authentication between the head-end and the subscriber. Thus, it may damage the benefits of DTV broadcasting system and it is important to provide mutual authentication between STB and smart card. Moreover, for security threats in DTV broadcasting, smart card cloning is a serious problem that a legal user's smart card is massively copied and this attack makes numerous illegal cards with the same ID number. Therefore, the illegal copies can be used in any STB for the purpose of unauthorized usage. Smart cards are secure and compact data carriers which have memory to store programs and multiple cryptographic keys. It restricts data access and ensures data integrity. Moreover, smart cards can be used to prove the digital identity of its cardholder by using cryptographic keys and algorithms stored in the card-protected memory. Due to popular use of smart cards, International Standards Organizations (ISO) had set up international standards for smart card applications [14, 15, 24, 31].

In this paper, we propose a frequency billing service in DTV system and it has many advantages than traditional DTV system such as performance efficiency and more types of billing methods. If a user seldom watched television programs, it is unsuitable for him/her to use the traditional way for charging. To satisfy the variety of charging situations, we propose a frequency billing protocol that the fees will be charged according to user's watching time. On the other hands, the proposed protocol only uses exclusive-or operations between smart card and STB. Thus, it is more efficient than other previous protocols such as Jiang et al.'s protocol [9] and Hou et al.'s protocol [7]. As shown in Figure 1, Subscriber Management System (SMS) provides billing system for users. Firstly, head end receives the satellite images via the encoder into digital images and sent satellite content to SMS. Then SMS will transfer a digital signal to the set-top box (STB) and users can watch the ordered channel via the STB.

The organizations of this paper are divided into four sections. We introduce related applications and existing works for DTV broadcasting in Section 1 and Section 2, respectively. In Section 3, we propose a secure billing protocol in DTV broadcasting systems. We analyze security and performance of the proposed protocol with other related protocols in Section 4. Our conclusions are presented in Section 5.

2. **Related works.** In this section, we introduce the background knowledge of conditional access system [2, 3, 8, 11, 17, 20, 27] and discuss related works in DTV broadcasting protocols. Figure 2 shows the structure of conditional access system.

In Figure 2, conditional access system included terrestrial broadcasting, transnational satellite and content providers to provide video, audio content, format, encoding and multiplexing transmission. First, the user selects a set of virtual strings for the control word (CWs). Then, virtual strings were be used to lock video programs and pseudo-random number generator was used to decode digital video and control word with an authorization key (AK). Note that the pseudo random sequence number is generated by a pseudo random sequence generator (PRG) for scrambling and descrambling the video programs. The entitlement control message (ECM) will be encrypted by using control

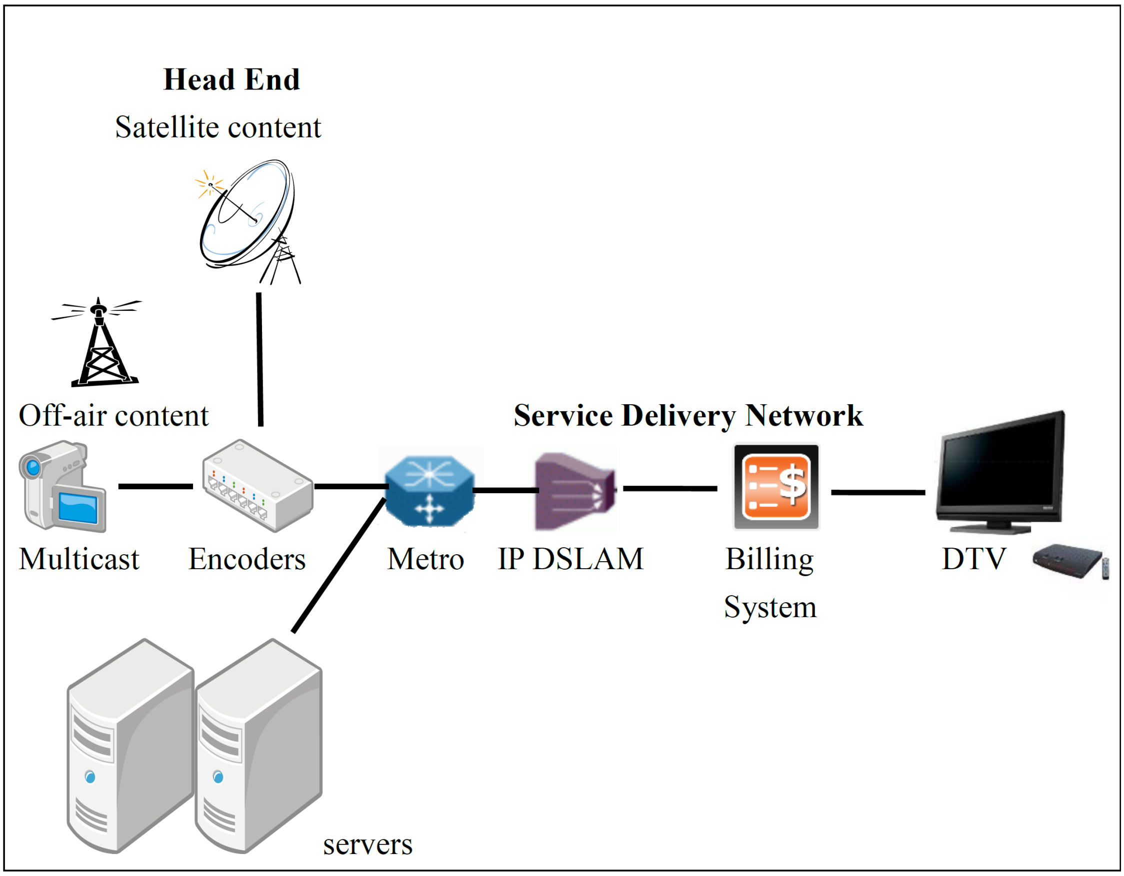

FIGURE 1. The proposed DTV structure

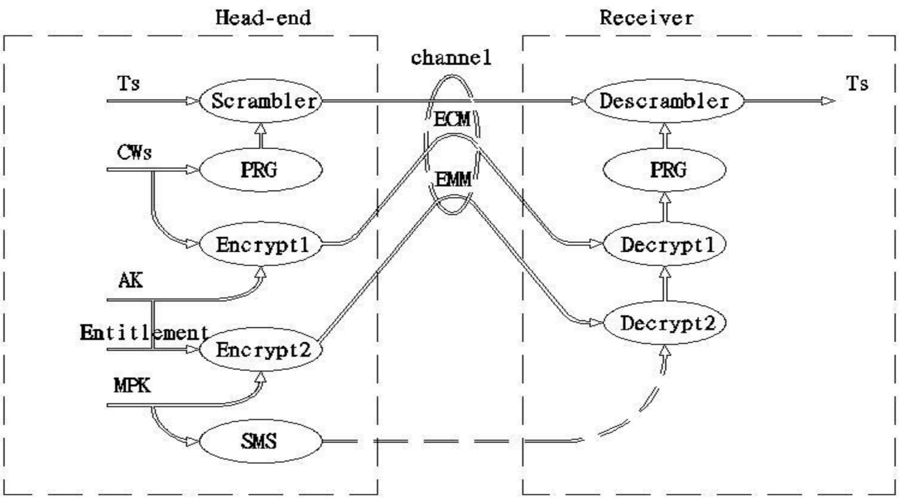

FIGURE 2. Conditional Access System [17]

word and ECM will be transferred to the corresponding channel. For the entitlement management message (EMM), AK used master private key (MPK) for encryption and a new transport stream (TS) multiplexed the scrambled program, entitlement management message and entitlement control message. The user's data management unit of the TV on the internet is liable by the subscriber management system (SMS). SMS not only encounters the charging issue or update the smart card for subscribers but also maintains each subscriber's private key and account information that contained MPK. When SMS transmits the data to the subscriber, he/she can use his/her smart card and set-top box (STB) to complete mutual authentication. On the other hands, in case of the user wants to watch subscription channels, he/she sends request messages to STB and STB receives subscriber's subscription signals from the channel. At this time, modems will reduce this signal demanded and restore the signal transferred to smart card for decryption. Finally, the smart card and set-top boxes will complete the requirements of mutual authentication and key agreement. After the control words were encrypted, the STB transmitted back to the user. When the attacker changes the control word to any decoder for decrypting the program, the system becomes unsafe. Moreover, if it does not provide mutual authentication between the STB and smart card, an attacker may launch replay attacks. Therefore, provision of mutual authentication between STB and smart card is an important issue for DTV broadcasting systems.

Diffie-Hellman [5] proposed allotment of a public key algorithm which based on discrete issues in 1976. However, their mechanism does not provide mutual authentication steps. Thus their mechanisms cannot detect man-in-the-middle attack and replay attack [1, 16, 26, 30]. In 2001, Wong et al. [29] proposed a key consultative mechanism with mutual authentication. Unfortunately, in 2003, Shim [23] found that their mechanism cannot resist key share attack. In 2004, Jiang et al. [9] proposed a key exchange protocol based on digital signatures and one-way function. The advantages of their proposed mechanism include dynamic symmetric key, mutual authentication and provision of better security. Moreover, their mechanism can change the password and prevent smart card cloning and replay attack problems. However, the traffic transmission between the STB and the smart card is not efficient. In 2007, Hou et al. [7] proposed an efficient and secure mutual authentication mechanism based on RSA in DTV broadcasting. In 2011, Lee et al. propose a new key exchange protocol with anonymity between STB and smart card in IPTV broadcasting systems [17]. However, it still requires time-consuming computations for securing data on the smart card. For charging in traditional television, many billings are half-yearly done. In this paper, we first propose a frequency billing service that

Table 1. Notations used in the proposed protocol

Notations	**Description**
ID_i	Identity of the user
C_i	Count of billing number for DTV system
PW_i	Password of the user
$\oplus$	Bitwise exclusive-or operation
$h(\cdot)$	One-way hash function
xs	Secret key of *STB*
$\|\|$	The string concatenation
no#	The registration number of the user
SMS	Smart card subscription management system
STB	Set-top box
Auth	The shared value between user, *STB* and *SMS*
Ts, Tu	Timestamps

users can choose the most suitable billing methods according to their requirements. As we have seen above, a number of user authentication protocols have been proposed in order to authenticate user legitimacy for DTV systems. However, they do not provide frequency billing services to the users and the proposed protocol provides better way for DTV charging and more efficient performance.

3. **The proposed protocol.** In this section, we propose a frequency billing service in DTV system and the proposed protocol is mainly composed of four phases, registration phase, login and authentication phase, key agreement phase, and CW transmission phase. For convenience of description, notations used in this paper are defined in Table 1.

3.1. **Registration phase.** When the frequency billing service starts, the user and SMS need to perform the following steps:

Step 1: The user selects a password PW_i and a random number α, computes $RPW = h(\alpha||PW_i)$ and sends RPW, ID_i, C_i to SMS for registration.

Step 2: When SMS receives the messages from the user, SMS computes ID_T, β and γ as follow:

$ID_T = (ID_i||C_i||no\#)$

$\beta = h\,(xs||ID_T)$

$\gamma = \beta \oplus RPW$

Where xs is the secret information generated by the SMS for STB and C_i is the number issued by SMS. C_i will store in SMS and user's smart card and it means the number of times that the user wants to watch TV.

Step 3: SMS stores γ, $Auth$ and α into user's smart card and issues it to him/her via a secure channel, where $Auth$ is the shared value between user, STB and SMS. Finally, the user stores α into smart card.

We show the flowchart of registration phase in Figure 3.

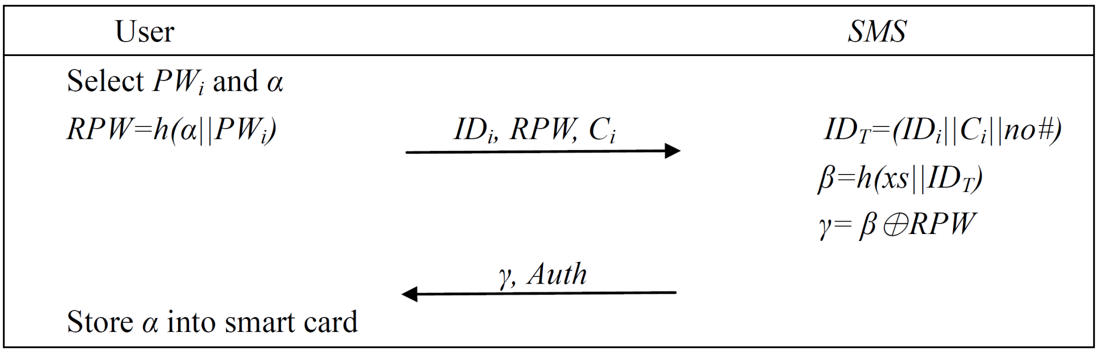

FIGURE 3. Registration phase

3.2. **Login and authentication phase.** When the user wants to use the DTV system, the user needs to complete mutual authentication with STB and he/she performs the following steps:

Step 1: The user uses the smart card and inputs the identity ID_i and password PW_i. Then smart card computes $RPW = (h(\alpha||PW_i), \beta = \gamma \oplus RPW$ and $\pi = h(Tu||\beta)$, where α is retrieved from smart card and T_u is user's current timestamp. In addition, the smart card chooses a random number ω, computes $AID_i = ID_i \oplus h(Auth\,||Tu||\,\omega)$ and sends AID_i, Tu, ω and π to STB, where $Auth$ is retrieved from smart card.

Step 2: When STB receives the message, it computes $ID_i = AID_i \oplus h(Auth\,||Tu||\,\omega)$ and checks the validity of C_i, no and ID_i. If they are valid, STB computes $ID_T = (ID_i||C_i||no\#)$ and $\beta = (xs||ID_T)$ and checks whether $h(Tu||\beta) = \pi$. If it holds, STB computes $\varepsilon = h(\pi \oplus \beta \oplus Ts)$ and sends ε and Ts to the user, where Ts is STB's current timestamp.

Step 3: When the user receives the messages from STB, it computes $\varepsilon' = h(\pi \oplus \beta \oplus Ts)$ and checks whether $\varepsilon' = \varepsilon$. If it holds, STB is authenticated by the user and the user computes the share key $K = h(\varepsilon \oplus \beta \oplus Tu \oplus Ts)$ and sends K to STB.

Step 4: When STB receives the K from user, it computes $K' = h(\varepsilon \oplus \beta \oplus Tu \oplus Ts)$ and checks whether $K' = K$. If it holds, the user is authenticated by STB and the mutual authentication between user and STB is complete. Finally, STB replaces ID_T with $ID_T' = (ID_i||C_i - 1||no\#)$ and updates smart card and SMS table.

We show the flowchart of login and authentication phase in Figure 4.

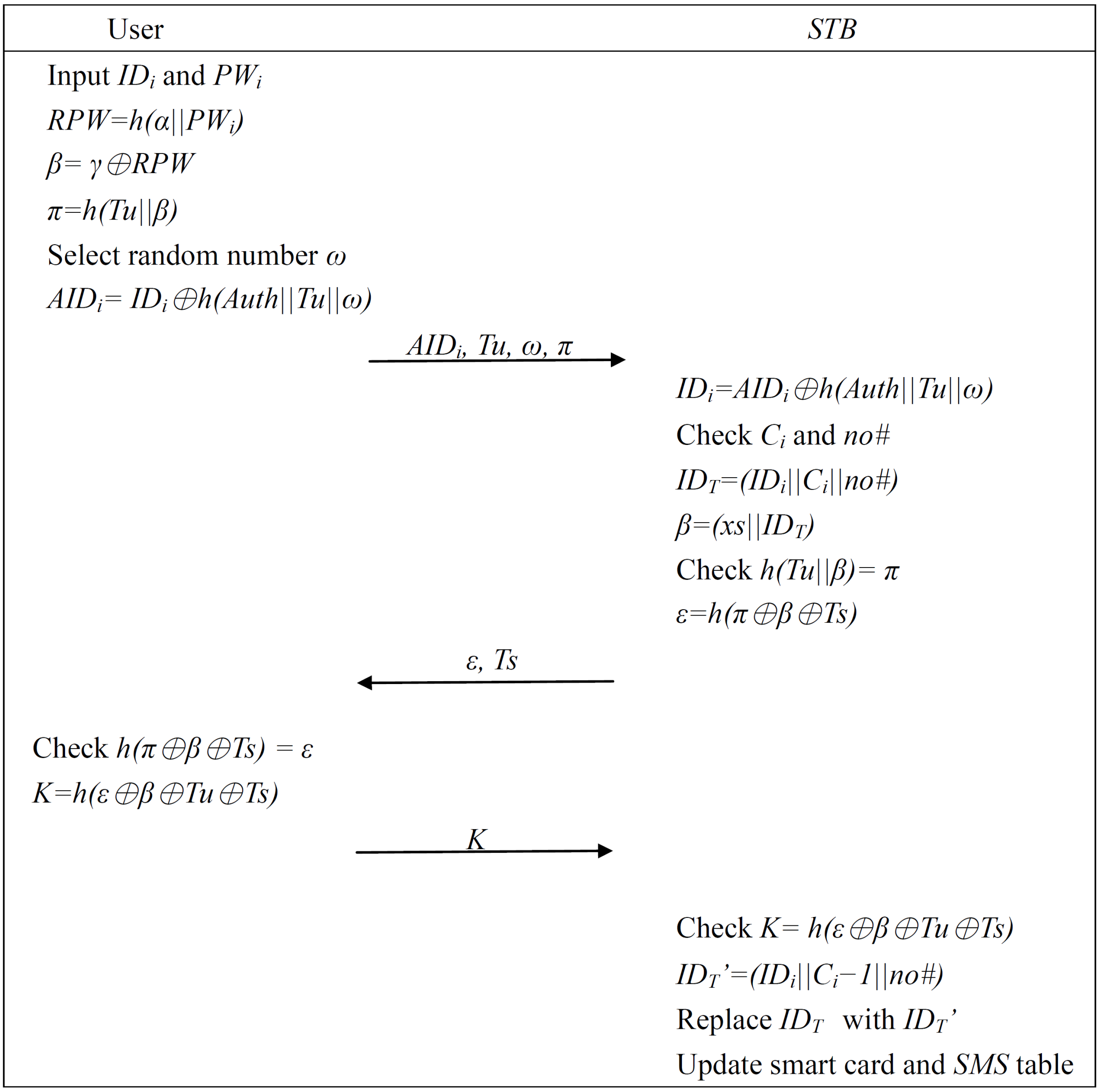

FIGURE 4. Login and authentication phase of the proposed protocol

3.3. **Key agreement phase.** After the mutual authentication procedure, the user and the STB compute $SK = h(\varepsilon \oplus \beta \oplus Tu \oplus Ts \oplus Auth)$ which is taken as their session key SK. Note that SK will be used in CW transmission phase.

3.4. **CW transmission phase.** After decrypting the CW by conditional access system, user uses SK to compute $CW_e = E_{SK}(CW)$ and sends CW_e to STB, where $E_{SK}(CW)$ is encryption of data CW using symmetric key SK. Then, STB uses the common session key SK to reveal CW by computing $CW = D_{SK}(CW_e)$, where $D_{SK}(CW_e)$ is decryption of data CW_e using symmetric key SK. Finally, the user can use CW to watch the subscribe programs.

4. **Analysis and comparison in performance and security.** In this section, we first analyze the security features of our proposed protocol. Then we evaluate the performance of the proposed protocol with other previous DTB broadcasting protocols.

4.1. **Security analysis.** As mentioned in previous works, the following security features are critical for DTB broadcasting systems and we compare the proposed protocol with Hou et al. [7], Jiang et al. [9], Jun et al. [10], Yoon and Yoo [32] and Yoon et al. [33]. The security comparisons of the proposed protocol with other previously related protocols are given in Table 2.

Table 2. Security comparisons among the related protocols for DTV broadcasting systems

	A	B	C	D	E
Proposed protocol	O	O	O	O	O
Hou et al. [7]	O	X	X	O	X
Jiang et al. [9]	X	X	X	O	X
Jun et al. [10]	O	X	O	O	X
Yoon and Yoo [32]	O	X	X	O	X
Yoon et al. [33]	O	X	X	O	X

A: Resistance of replay attack

B: Resistance of stolen-verifier attack

C: Provision of user anonymity and untraceability

D: Resistance of smart card cloning and stolen smart card attack

E: Provision of frequency billing service

O: Yes

X: No

4.1.1. **Resistance of replay attack.** The timestamps Tu and Ts are employed in our protocol to avoid the replay attacks. We assume that an attacker may retransmit the intercepted messages $\{AID_i, Tu, \omega, \pi\}$ and $\{\varepsilon, Ts\}$ in Step 1 and Step 2 of login and authentication phase, respectively. However, the user and STB can easily detect this attack by checking timestamps Tu and Ts.

4.1.2. **Resistance of stolen-verifier attack.** Because SMS does not need to maintain a password table in server side and the user secures his/her password PW and smart card. Therefore, the proposed protocol can resist stolen-verifier attacks and provides high scalability for the user addition such that it is very practical for the applications with large number of users.

4.1.3. **Provision of user anonymity and untraceability.** In the proposed protocol, the user did not transmit his/her true ID_i over a public channel and the user generated AID_i instead of ID_i, where AID_i includes ID_i as $ID_i \oplus h(Auth\,||Tu||\,\omega)$. So, an attacker has no way of guessing ID_i without $Auth$ and the proposed protocol can provide user anonymity and untraceability.

4.1.4. **Resistance of smart card cloning.** When a user's smart card is lost or stolen by an attacker, the attacker may massively duplicate the smart card and the secret information stored in the smart card may be extracted by the attacker. Since the attacker is unable to derive user's ID_i and PW_i from the smart card due to the protection of one-way hash function and the attacker does not have knowledge of STB's secret key xs. As a result, the proposed protocol can resist smart cloning and stolen smart card attacks.

4.1.5. **Provision of frequency billing service.** In the proposed protocol, the count of billing number C_i is store in user's smart card and SMS and the user needs to pass the authentication phase with STB. Moreover, after verification, STB updates old C_i with new C_i' and SMS records user's payment state in server side. Thus, the proposed billing service is suitable for DTV broadcasting systems.

4.2. **Performance analysis.** Performance cost comparisons between the proposed protocol and other five related protocols in [7, 9, 10, 32, 33] are given in Table 3. Refer to Table 3, the registration phase of our proposed protocol uses two one-way hash function computations, one exclusive-OR computation and one random number. In the login phase, the proposed protocol uses three one-way hash function computations, two exclusive-OR computations, one random number and one timestamp. In the authentication and key agreement phase, the proposed protocol uses seven one-way hash function computations, eleven exclusive-OR computations and one timestamp. For instance, as introduced in [25], one symmetric encryption/decryption is at least 100 times faster than one asymmetric encryption/decryption and one hashing operation is at least 10 times faster than a symmetric encryption/decryption in software implementation. In addition, one exponential operation is approximately equal to 60 symmetric encryptions/decryptions and it requires 0.0003s (second) to perform one one-way hashing operation, 0.0054s to perform one symmetric encryption/decryption and 0.036 to perform one point multiplication operation. In general, the computational costs of exclusive-OR operation, timestamp and random number generations are ignored because these kinds of operations have much lighter costs than one-way hash computations.

Refer to Table 4, $640T(h)$ are required for Hou et al.'s protocol,$2429T(h)$ are required for Jiang et al.'s protocol, $3028T(h)$ are required for Yoon et al.'s protocol, $1847T(h)$ are required for Jun et al.'s protocol, $509T(h)$ are required for Yoon et al.'s protocol and

Table 3. Performance comparisons among the related protocols for DTV broadcasting systems

	Registration phase	Login phase	Authentication and key agreement phase
Proposed protocol	$2T(h) + 1T(\oplus) + 1T(r)$	$3T(h) + 2T(\oplus) + 1T(r) + 1T(t)$	$7T(h) + 11T(\oplus) + 1T(t)$
Hou et al. [7]	$2T(h) + 3T(\oplus)$	$3T(h) + 4T(\oplus) + 1T(r) + 1T(e) + 1T(t)$	$5T(h) + 8T(\oplus) + 1T(r) + 1T(t) + 1T(e)$
Jiang et al. [9]	$2T(h) + 2T(\oplus) + 1T(e)$	$2T(h) + 1T(\oplus) + 2T(r) + 1T(e)$	$5T(h) + 1T(r) + 2T(e)$
Jun et al. [10]	$2T(h) + 2T(\oplus)$	$2T(h) + 2T(\oplus) + 1T(e)$	$3T(h) + 6T(\oplus) + 2T(e) + 2T(s)$
Yoon and Yoo [32]	$2T(h) + 2T(\oplus) + 1T(e)$	$2T(h) + 1T(\oplus) + 2T(r) + 1T(e)$	$4T(h) + 3T(e) + 1T(r)$
Yoon et al. [33]	$1T(h) + 1T(\oplus)$	$1T(h) + 1T(\oplus) + 1T(p) + 1T(r)$	$7T(h) + 1T(r) + 2T(\oplus) + 3T(p)$

$T(h)$: computation cost of one-way hash function
$T(\oplus)$: computation cost of exclusive-OR operation
$T(t)$: computation cost of timestamp
$T(r)$: computation cost of random number
$T(e)$: computation cost of modular exponentiation
$T(s)$: computation cost of symmetric encryption
$T(p)$: computation cost of point multiplication

$32T(h)$ are required for our proposed protocol. Obviously, in the proposed protocol, the total computational time of our protocol is lower than most of comparison protocols.

On the other hands, we present our evaluation results in this paper. DTV broadcasting protocols proposed in the literatures can be categorized into those based on RSA and ECC. We compare the proposed DTV protocol with the best protocols in each category. All protocols were done on four-core 3.0-GHz machine with 16-GB memory and the results were averaged over 500 randomized simulation runs. Experimental evaluations were implemented on our simulator written in MATLAB. Detailed results of computation costs are presented in Figure 5.

In Figure 5, the total computational time required by our protocol is 0.00976 second. And the total computational time required by Hou et al.'s [7], Jiang et al.'s [9], Jun et al.'s [10], Yoon et al.'s [32], and Yoon et al.'s [33] protocol respectively are 0.19217, 0.72976, 0.55421, 0.90851, and 0.18225 second. Therefore, it is obvious that our protocol is more efficient than other protocols.

5. **Conclusions.** User charging is one of the important issues in DTV broadcasting system that needs to be adequately addressed. In this paper, we propose a frequency billing

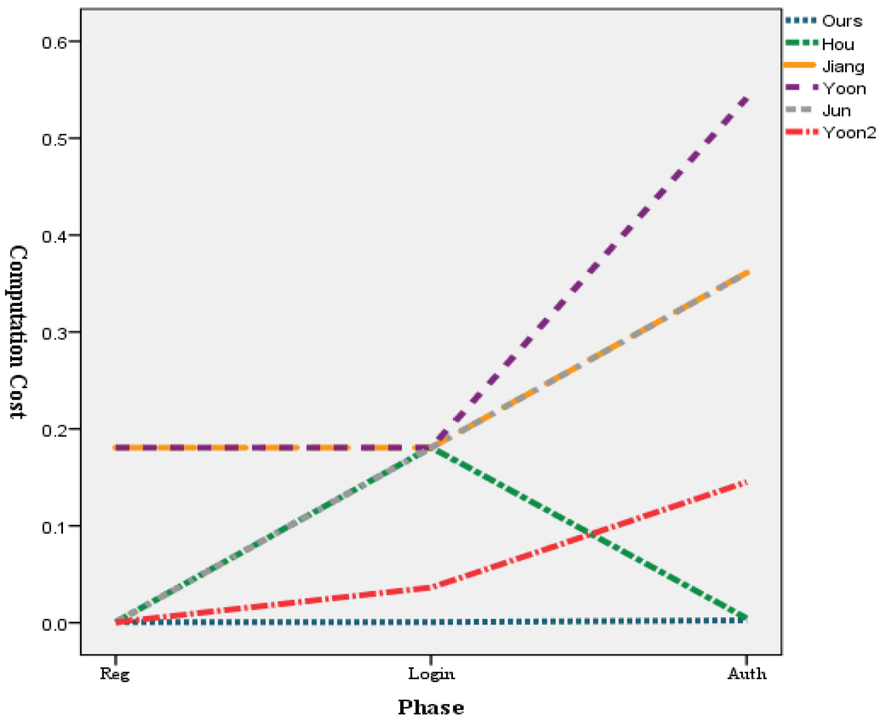

FIGURE 5. Performance evaluations

TABLE 4. Comparisons of total computation time among the related protocols for DTV broadcasting systems

	Registration phase	Login phase	Authentication and key agreement phase	Total operations	Total computation time
Proposed protocol	0.00062s	0.00063s	0.00242s	$32T(h)$	0.00976s
Hou et al.[7]	0.00063s	0.18092s	0.00455s	$640T(h)$	0.19217s
Jiang et al.[9]	0.18062s	0.18062s	0.36121s	$2429T(h)$	0.72976s
Jun et al. [10]	0.00061s	0.18061s	0.36093s	$1847T(h)$	0.55421s
Yoon et al.[32]	0.18064s	0.18062s	0.54153s	$3028T(h)$	0.90851s
Yoon et al.[33]	0.00060s	0.03632s	0.14521s	$509T(h)$	0.18225s

s: second

protocol in DTV broadcasting system. We analyze the proposed protocol with other related protocols in terms of security and performance. In brief, compared with the other related protocols, while providing relatively more security features, our proposed protocol not only provides much better security features but also achieves much higher performance efficiency. As a result, the proposed protocol is well suited for DTV broadcasting systems with low-power computing devices. Recently, cloud computing is an important research issue. In future, our scheme also can be applied in cloud computing. Besides, we also can combine our scheme with vehicle ad hoc networks (VANET).

Acknowledgment. The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 102-2221-E-030-003.

REFERENCES

[1] C. C. Chang, L. Harn, and T. F. Cheng, Polynomial-based key management for secure intra-group and inter-group communication, *International Journal of Network Security*, vol. 16, no. 2, pp. 143-148, 2014.

[2] M. G. Chung, and Y. Kim, An integrated protocol for authentication and access control in a digital TV environment, *Proc. of IEEE International Conference on Consumer Electronics*, pp. 1-2, 2008.

[3] E. Cruselles, J. L. Melus, and M. Soriano, An overview of security in Eurocrypt conditional access system, *Proc. of IEEE Global Telecommunications Conference*, pp. 188-193, 1993.

[4] T. H. Chen, G. Horng, and C. S. Yang, Public key authentication schemes for local area networks, *Informatica*, vol. 19, no. 1, pp. 3-16, 2008.

[5] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[6] M. Garcia, A. Canovas, M. Edo, and J. Lloret, A QoE management system for ubiquitous IPTV devices, *Proc. of the 3rd International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pp. 147-152, 2009.

[7] T. W. Hou, J. T. Lai, and C. L. Yeh, Based on cryptosystem secure communication between set-top box and smart card in DTV broadcasting, *Proc. of IEEE Region 10 Conference*, pp. 1-5, 2007.

[8] T. Jiang, S. Zheng, and B. Liu, Key distribution based on hierarchical access control for conditional access system in DTV broadcast, *IEEE Trans. Consumer Electronics*, vol. 50, no. 1, pp. 225-230, 2004.

[9] T. Jiang, Y. Hou, and S. Zheng, Secure communication between set-top box and smart card in DTV broadcasting, *IEEE Trans. Consumer Electronics*, vol. 50, no. 3, pp. 880-886, 2004.

[10] F. Kamperman, and B. V. Rijnsoever, Conditional access system interoperability through software downloading, *Proc. of IEEE International Conference on Information Science*, pp. 1-8, 2010.

[11] U. Horn, K. Stuhlmüler, M. Link, and B. Girod, Robust internet video transmission based on scalable coding and unequal error protection, *IEEE Trans. Consumer Electronics*, vol. 47, no. 1, pp. 47-53, 2001.

[12] W. Kanjanarin, and T. Amornraksa, Scrambling and key distribution protocol for digital television, *Proc. of IEEE International Conference on Networks*, pp. 140-145, 2001.

[13] T. Kim, and H. Bahn, Implementation of the storage manager for an IPTV set-top box, *IEEE Trans. Consumer Electronics*, vol. 54, no. 4, pp. 1770-1775, 2008.

[14] N. Kogan, Y. Shavitt, and A. Wool, A practical revocation scheme for broadcast encryption using smart cards, *ACM Trans. Information and System Security*, vol. 9, no. 3, pp. 325-351, 2006.

[15] J. S. Lee, H. S. Rhee, and D. H. Lee, Efficient and secure communication between set-top box and smart card in IPTV broadcasting, *Proc. of IEEE International Conference on Convergence and Hybrid Information Technology*, pp. 307-310, 2008.

[16] C. C. Lee, On security of an efficient nonce-based authentication scheme for SIP, *International Journal of Network Security*, vol. 9, no. 3, pp. 201-203, 2009.

[17] C. C. Lee, C. T. Li, T. Y. Chen, P. H. Wu, and C. T. Chen, A new key exchange protocol with anonymity between STB and smart card in IPTV broadcasting, *Proc. of IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 23-25, 2011.

[18] B. Macq, and J. Quisquater, Cryptology for digital TV broadcasting, *Proceedings of the IEEE*, vol. 83, no. 6, pp. 944-957, 1995.

[19] J. Moon, J. Kim, J. Park, and E. Paik, Achieving interoperability in conditional access systems through the dynamic download and execution of cryptographic software for the IPTV system, *Proc. of IEEE International Conference on Convergence and Hybrid Information Technology*, pp. 308-385, 2008.

[20] J. Moon, J. Kim, J. Park, E. Paik, and K. Park, A dynamic conditional access system for IPTV multimedia systems, *Proc. of IEEE International Conference on Systems and Networks Communications*, pp. 224-229, 2009.

[21] S. Park, and S. Jeong, Mobile IPTV: approaches, challenges, standards, and QoS support, *IEEE Internet Computing*, vol. 13, no. 3, pp. 23-31, 2009.

[22] E. Shihab, F. Wan, L. Cai, A. Gulliver, and N. Tin, Performance analysis of IPTV traffic in home networks, *Proc. of IEEE Global Telecommunications Conference*, pp. 5341-5345, 2007.

[23] K. Shim, Cryptanalysis of mutual authentication and key exchange for low power wireless communication, *IEEE communications letters*, vol. 7, no. 5, pp. 248-250, 2003.

[24] C.P. Schnorr, Efficient identification and signatures for smart cards, *Proc. of Crypto'89*, pp. 235-251, 1990.

[25] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, New York, USA, 1995.

[26] C. S. Tsai, C. C. Lee, and M. S. Hwang, Password authentication schemes: current status and key issues, *International Journal of Network Security*, vol. 3, no. 2, pp. 101-115, 2006.

[27] F. K. Tu, C. S. Laih, and H. H. Tung, On key distribution management for conditional access system on pay-TV system, *IEEE Trans. Consumer Electronics*, vol. 45, no. 1, pp. 151-158, 1999.

[28] J. S. Wey, J. Luken, and J. J. Heiles, Standardization activities for IPTV set-top box remote management, *IEEE Internet Computing*, vol. 13, no. 3, pp. 32-39, 2009.

[29] D. S. Wong, and A. H. Chan, Mutually authentication and key exchange for low power wireless communications, *Proc. of IEEE Military Communications Conference*, vol. 13, no. 3, pp. 23-31, 2009.

[30] C. C. Yang, C. C. Lee, and S. Y. Hsiao, Man-in-the-middle attack on the authentication of the user from the remote autonomous object, *International Journal of Network Security*, vol. 1, no. 2, pp. 81-83, 2005.

[31] E. J. Yoon, and K. Y. Yoo, A new secure key exchange protocol between STB and smart card in DTV broadcasting, *Proc. of the 2006 international conference on Intelligence and Security Informatics*, pp. 165-166, 2006.

[32] E. J. Yoon, and K. Y. Yoo, Robust key exchange protocol between set-top box and smart card in DTV broadcasting, *Informatica*, vol. 20, no. 1, pp. 139-150, 2009.

[33] E. J. Yoon, and K. Y. Yoo, ECC-based key exchange protocol for IPTV service, *Proc. of IEEE International Conference on Information Science*, pp. 547-552, 2011.