Symmetry **2015**, *7*, 1567-1586; doi:10.3390/sym7031567

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

Design of IP Camera Access Control Protocol by Utilizing Hierarchical Group Key

Jungho Kang [1], Jaekyung Han [2] and Jong Hyuk Park [3,*]

[1] Department of Computing, Soongsil University, 402 Information Science Building, 369 Sangdo-Ro, Dongjak-Gu, Seoul 156-743, Korea; E-Mail: kjh7548@naver.com

[2] Department of Construction Legal Affairs, The Graduate School of Construction Legal Affairs, Kwangwoon University, 20 Kwangwoon-Ro, Nowon-Gu, Seoul 139-701, Korea; E-Mail: hjk1014@kw.ac.kr

[3] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Gongneung 2-dong, Nowon-Gu, Seoul 139-743, Korea

***** Author to whom correspondence should be addressed; E-Mail: jhpark1@seoultech.ac.kr; Tel.: +82-29-706-702; Fax: +82-29-779-441.

Academic Editor: Laurence Yang

Received: 26 March 2015 / Accepted: 20 August 2015 / Published: 27 August 2015

Abstract: Unlike CCTV, security video surveillance devices, which we have generally known about, IP cameras which are connected to a network either with or without wire, provide monitoring services through a built-in web-server. Due to the fact that IP cameras can use a network such as the Internet, multiple IP cameras can be installed at a long distance and each IP camera can utilize the function of a web server individually. Even though IP cameras have this kind of advantage, it has difficulties in access control management and weakness in user certification, too. Particularly, because the market of IP cameras did not begin to be realized a long while ago, systems which are systematized from the perspective of security have not been built up yet. Additionally, it contains severe weaknesses in terms of access authority to the IP camera web server, certification of users, and certification of IP cameras which are newly installed within a network, *etc*. This research grouped IP cameras hierarchically to manage them systematically, and provided access control and data confidentiality between groups by utilizing group keys. In addition, IP cameras and users are certified by using PKI-based certification, and weak points of security such as confidentiality and integrity, *etc.*, are improved by encrypting passwords. Thus, this research presents specific protocols of the entire process and proved through experiments that this method can be actually applied.

Keywords: IP camera; access control management; hierarchical group-key; authentication; protocol

1. Introduction

It is the current trend that IP cameras have been substituting closed circuit television (CCTV) in the market of security control which uses CCTV equipment. IP cameras are a kind of network camera. Unlike CCTV models, it enables video surveillance monitoring by a web browser anywhere and anytime through a built-in web server, if it is connected to the Internet or existing network. Accordingly, it can be practically utilized and can be installed more easily, in comparison with existing CCTV models. Furthermore, thy can perform intelligent calculation, too, so that the supply of related apparatuses and services are increasingly being enlarged. Additionally, the installation cost of IP cameras is lower than CCTV [1,2]. IP cameras contain a CCTV camera, encoder, and web server with itself so that it can be easily managed even if the IP cameras are dispersedly installed. It can be accessed anywhere and anytime through the web or smartphone in real-time. However, IP cameras have weak points, too, in terms of access authority and user certification for the IP camera web server, or certification of IP cameras which are newly installed on the network [3,4].

First, when an IP camera is installed in a network, sham attacks could be caused by malevolent users because there is no system which certifies whether the newly-installed camera is a proper device or not. Second, delicate video information could be exposed because video data which is multicast to other groups is not encoded. Third, while CCTV has been used in closed environments, IP cameras are synchronized with the network so that not only permitted clients but also not-permitted persons can watch most of video if they have the IP and port information, and basic ID and password [5,6]. This is caused by a lack of policy, and is regarded as a severe weakness, too. Moreover, resources of the web server inside the IP camera can be unnecessarily wasted by registering users individually. Thus, cameras must be grouped, cameras which newly join the group must be certified, data which is multicast by the group must be encoded to be transmitted, and user certification and passwords must be encoded [7,8]. In addition to that, a method to compose groups hierarchically is required to control access according to user authorities [9,10].

2. Related Work

2.1. IP Camera System

IP camera systems transmit video on the basis of an IP network, so that it is "open" and its expandability and flexibility is better than CCTV systems. Additionally, it loads a web server inside itself and it enables monitoring through a web browser, so that monitoring is possible anywhere and anytime if the Internet is available. IP camera systems can be composed in a closed way with the network not being exposed outwards. However, when only one IP camera is installed at a distant place or a few cameras are installed to use, invasion detection and blocking systems, which are generalized in general

networks, are not composed in IP cameras and they can be vulnerable to packet sniffing and complete survey attacks by encoding and transmitting user passwords in general encoding methods [11–13].

2.2. Security Requirements of Group Keys Management

Group keys must be managed properly. In order to efficiently manage group keys which are used for the sake of message security in the environment of multipoint communication, not only must the group keys be shared securely with multiple users and be adapted to changes of members due to processes of join and withdrawal of users, but secure group keys which only member users can use must be provided [14,15]. Particularly, key renewal, which means to renew the group keys whenever members are changed, is essentially important in management of group keys. In order to deliver messages securely in multipoint communication, the existing network security requirements, such as integrity and confidentiality, are necessary, too [16,17]. In order to manage group keys securely, forward and backward secrecy must be considered to provide sercurity according to changes of members. "Forward secrecy" means that users who withdraw from the current membership cannot acquire the information of the key which is going to be used for the next group communication by using the information which they used to have. "Backward secrecy" means that new users cannot find out a session key which was previously used and cannot decode the previous contents of communication by utilizing the information which they did and will acquire when they join the group. Thus, "group key renewal" is to change the group key with new value to provide forward and backward secrecies in the group keys management method. The group key management method is divided into "centralized", "decentralized", and "distributed" methods, according to necessities of the central server. While the centralized method manages the entire group, the decentralized one manages them by separating whole groups into small, multiple groups. The distributed method does not use the server [18].

2.3. Centralized Group Key Method

2.3.1. Logical Key Hierarchy (LKH)

LKH was proposed to constitute a hierarchical structure on the base of a tree in the process of generating encoded keys and, consequently, to reduce the transmission numbers of key renewal messages in the process of key renewal due to the change of membership. The early setting protocol constitutes a logical hierarchical structure by using the users who joined at the early stage, and delivers to each user the key which is maintained by each user by using the secret key which has been shared in advance. The join protocol in the LKH method adds each user to the tree, and delivers the new keys to other users. Due to the fact that backward secrecy must be considered at this time, the entire keys which need to be delivered to users must be changed. Figure 1 shows the protocol when new members join a group.

In the withdrawal protocol of the LKH method, forward secrecy must be guaranteed, and the key which withdrawing members know must be changed in total. Figure 2 illustrates the protocol when members withdraw from the group.

The LKH has an advantage that it can use the key of the middle node as the key of the partial group by using this logical hierarchical structure [19].

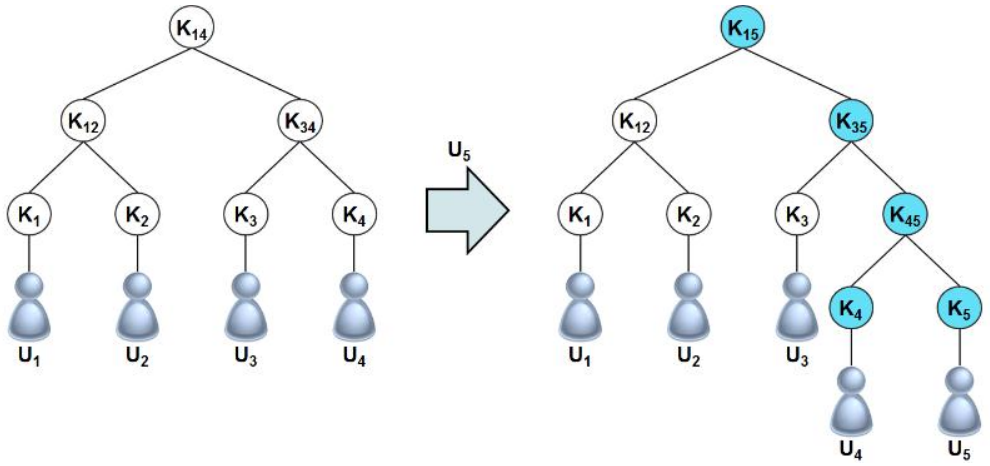

Figure 1. Join protocol of LKH.

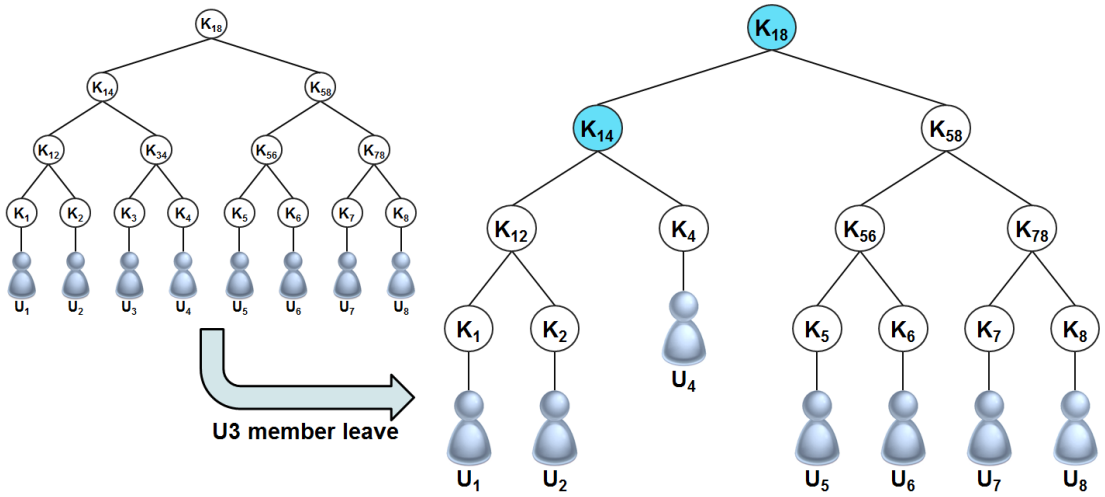

Figure 2. Withdrawal protocol of LKH.

2.3.2. One Way Function Tree (OFT)

The OFT is a one-way function tree to cut the cost of LKH in half. While one key is maintained at each node, like the LKH, the key value of the middle node is calculated by using key values of children nodes as follow:

$$K_i = f(g(K_{L(i)}, g(K_{R(i)})))$$

Unlike the LKH method, in the OFT method the number of necessary messages is reduced by half, because the existing users have already known the values of the children nodes of one side. The following Figure 3 shows the structure of one-way function tree [20].

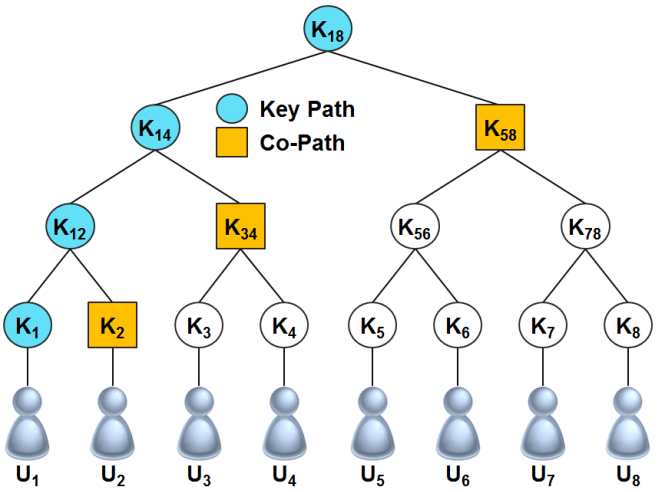

Figure 3. The structure of a one-way function tree.

2.3.3. Efficient Large-Group Key (ELK)

The ELK method renews the keys regularly by using the same PRF (pseudo-random function) as MAC (message authentication code), and can process the join without transmission cost when new members join. Although the ELK method maintains each key of each node, respectively, like the LKH and OFT methods, it does not use this key directly. On the contrary, the ELK makes four keys through MAC according to each usage and uses them. When a new member joins the group in the join protocol of the ELK method, the server determines the insertion location of the new member and becomes the brother node of the existing members. The brother node of the new member comes down one stage, and a new parent node is added. The withdrawal process of the ELK applies that of the OFT method. In the withdrawal protocol of the ELK method, when U3 withdraws, its brother node comes up one stage, and the key value which has to be changed (in order to change key values) is renewed by using the children of the right and left sides [21].

2.4. Distributed Group Key Method

2.4.1. Expansion of Diffie-Hellman Protocol

Ingemarsson *et al.* [22] proposed a group key establishment protocol by expanding the basic Diffie-Hellman protocol to a multipoint protocol. After each user exchanges one-time Diffie–Hellman keys with each other, they exchange double-point Diffie–Hellman again. If the number of participants is n, the users repeat the process n − 1 times and establish the group key. Due to the fact that in this method a man-in-the-middle attack is possible, like the previous Diffie–Hellman protocol, each value must be able to be certified. The cost of this method needs $n - 1$ rounds, and each user needs an exponentiation calculation of n times. The following Figure 4 shows the group key establishment protocol which was made by expanding the Diffie–Hellman protocol proposed by Ingemarsson *et al.* [22].

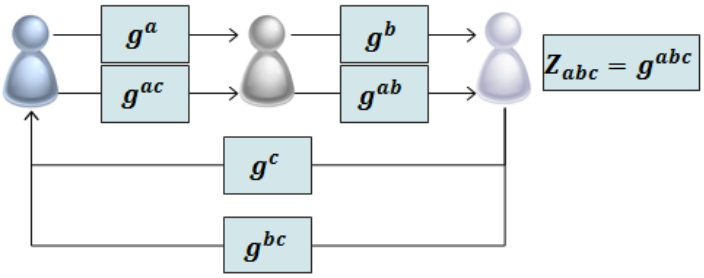

Figure 4. Distributed group key protocol of Ingemarsson *et al*. [22]

Steiner *et al.*'s [23] group key protocol reduces the average calculation cost of each user in comparison with the method proposed by Ingemarsson *et al.* [22]. Burmester and Desmedt proposed a protocol which is carried out by composing participants in the ring structure. The method is performed through the stages like Figure 5 [24].

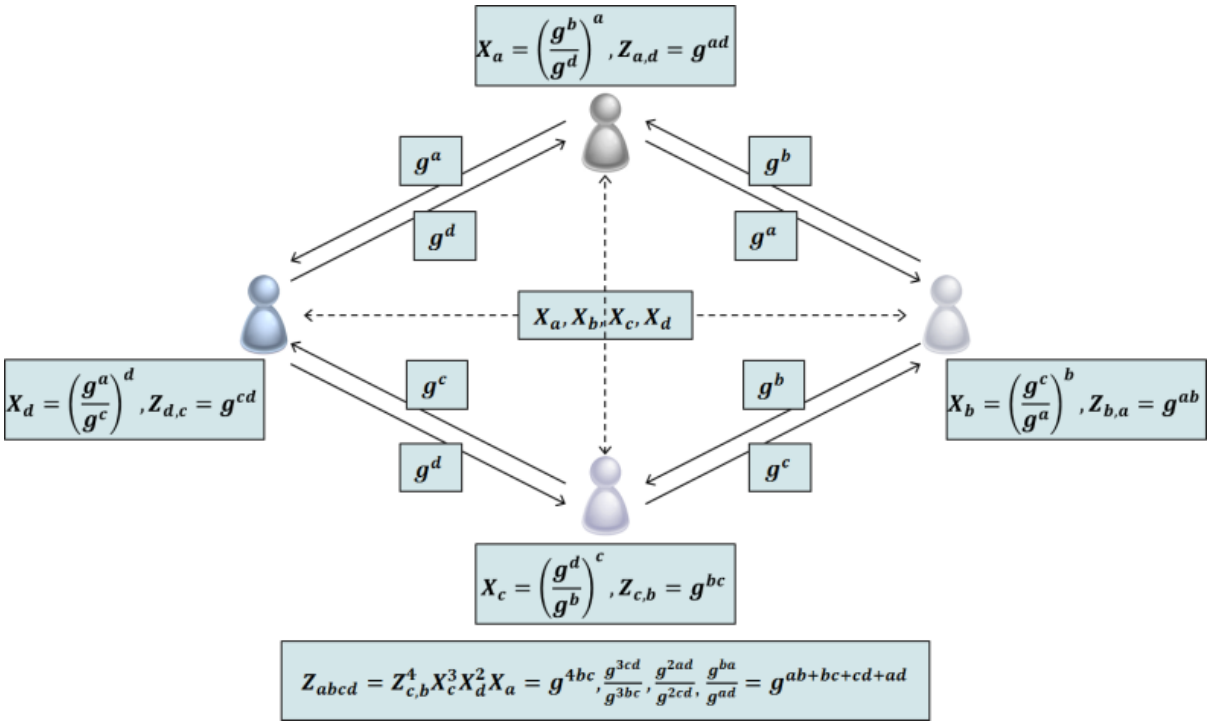

Figure 5. Distributed group key protocol of Burmester and Desmedt [24].

2.4.2. Distributed Group Key Protocol using Logical Key Tree

A distributed LKH method proposed by Perring is as similar as that of the OFT method, in terms of information which each member maintains. The following Figure 6 shows the distributed group key protocol of Perring [25].

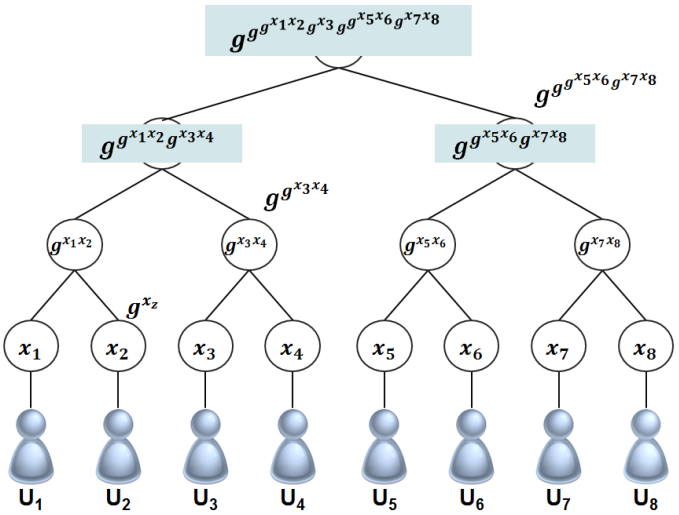

Figure 6. Distributed group key protocol of Perring.

3. Access Control Using Group Key

3.1. Composition of Proposed System

Existing IP cameras contain overall weaknesses, like the absence of management system for access authority and plaintext transmission of passwords. The access control system of the suggested IP camera in this paper has two advantages compared to the existing IP camera system. First, it can control and monitor the system safely by groups using a hierarchical group key. Second, we designed the protocol which could provide mutual authentication between IP camera systems. The overall system configuration is like that shown in Figure 7.

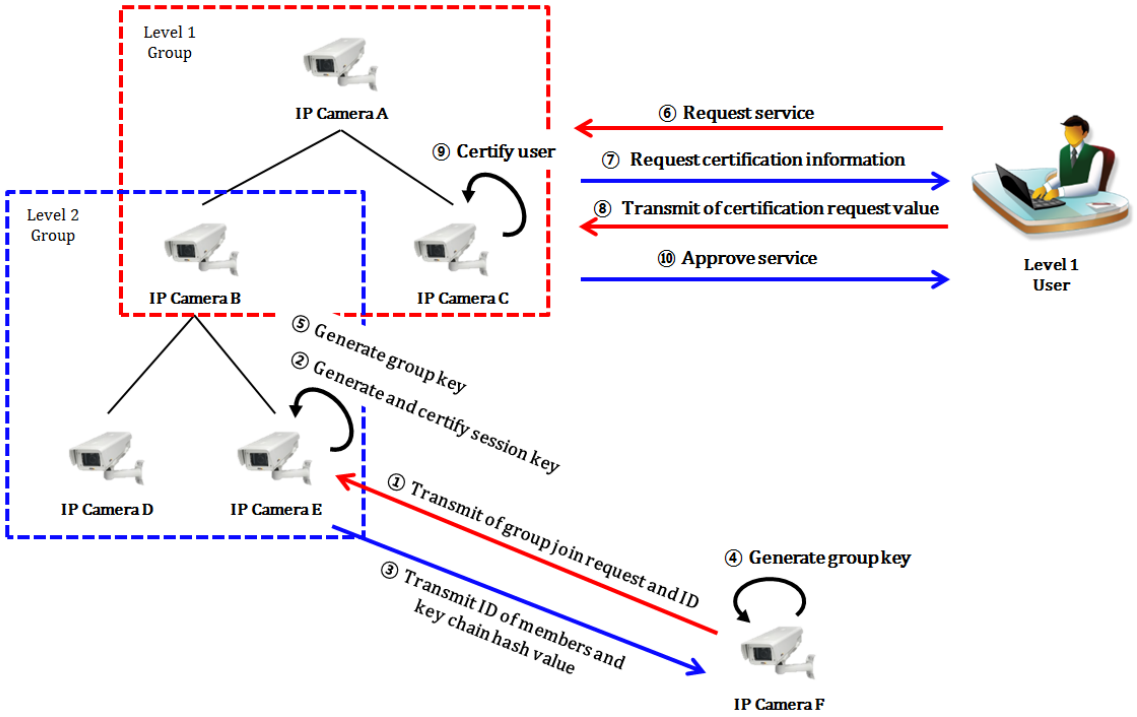

Figure 7. Proposed system arrangement.

An IP camera which wants to join the group requests its join and transmits it to a member which has already joined the group. It is assumed in the above Figure 7 of the system arrangement that each camera has its own predetermined shared value, and its certification is issued by a reliable certification institution. The existing member which receives the join request carries out the camera certification through the certification process and if the certification is successfully verified, the existing member calculates a pre-shared value, the IDs of its own and the new camera, and then generates a session key. Then, the existing member encodes the one-way hash function value, which was generated by using the IDs of the existing members and the hash chain technique into a session key, and transmits it the new member. The new member applies the Diffie–Hellman Key Agreement Method to the existing member's IDs which were transmitted and its own ID, and then generates a group ID. Then, the new member calculates the generated group ID and one-way hash function, generates a group key, and generates a secure channel. The existing member which receives the join request encodes the ID of the new member into the previous group key, and transmits it to other members. Afterwards, each member generates a new group key by using the ID of the new member which has been just transmitted.

If a member requests to join the camera server, the camera server requests the user for the certification and user information again. The user signs the user information, including the group ID which it received at the first registration with its certification, and encodes it into the public key of the camera server and transmits it. The camera server requests the access authority to the camera server, which belongs to the corresponding group ID, by using group ID, which was generated by decoding the transmitted data into its own personal key. Then, the camera server judges the response, which was received from the camera server of the corresponding group, and provides the user with service. The terms and symbols used in the proposed security protocol are shown in Table 1.

Table 1. The terms and symbols used in the proposed security protocol.

Symbols	Description
PSV	Secret Sharing Random Value
CID_X	Camera X's ID
pri_X	X's Private Key
pub_X	X's Public Key
SK_{XY}	Session Key between X and Y
E_sk	Encryption using session key
D_sk	Decryption using session key
Sig_X	Signature Value
GID_X	Camera X's Group ID
$h^n(s)$	Value executed by hash function *n* times using s as seed value
s	Random seed value generated by group leader camera
GK_X	Camera X's Group Key

3.2. Specific Protocol

3.2.1. Early Group Key Generation Protocol

According to the early group key generation protocol, each camera generates its own ID to generate a group. At this time, the leader of the group (root node of the logical tree structure) generates the one-way hash function value, too. Figure 8 shows the specific procedure of the early group key generation protocol.

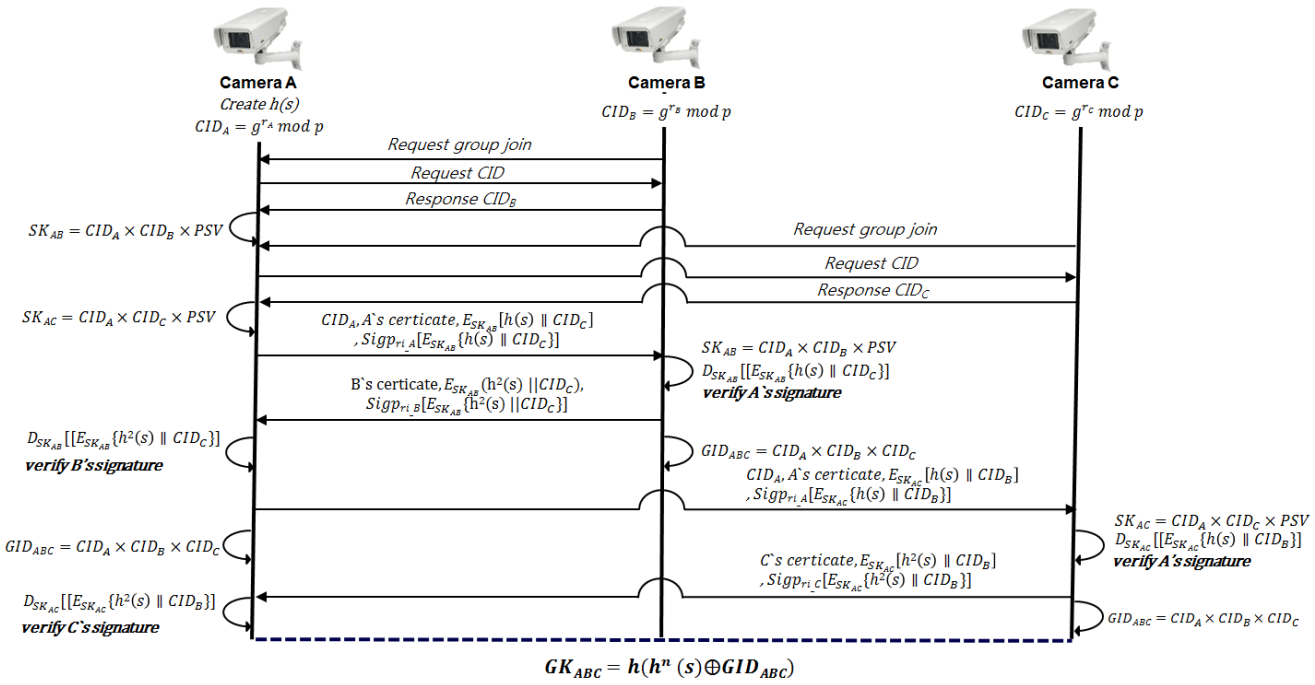

Figure 8. Early group key generation protocol.

Step 1. (B→A): In order to compose the early group, the camera B requests a group join to a camera which is going to be a root node. The input formula has a process like Formula (1):

$$\text{Request Group Join} \quad (1)$$

Step 2. (A→B): In order to compose the early group, the camera A requests a CID value when it receives a group join request. The input formula has a process like Formula (2):

$$\text{Request CID} \quad (2)$$

Step 3. (B→A): The camera B generates its own ID by using a random value and transmits it to group leader A. The formula to generate its own ID has a process like Formula (3):

$$\text{CID} = g^{r}{}_{b} \bmod p \quad (3)$$

Step 4. (A): The group leader A applies a multiplying operation to the ID of its own, the ID which was transmitted from B, a pre-shared value, and generates a temporary session key. The calculation formula has a process like Formula (4):

$$SK_{AB} = CID_A \times CID_B \times PSV \quad (4)$$

Step 5. (A→B): The group leader A signs the information, which is necessary to generate a group key, such as an ID of its own, certification, hash value and ID of other members by using its own personal key, and encodes them with the session key, which was generated in Step 4, and transmits them to the camera B. The formula to transmit information for generation of group key has a process like Formula (5):

$$\text{A's certificate, } E_{SKAB}(h(s)||CID_C),\ Sig_{pri\_A}[E_{SKAB}\{h(s)||CID_C\}] \quad (5)$$

Step 6. (B): The camera B generates a session key with the A's ID which was transmitted from the group leader A, the ID of its own, and pre-shared value. Then it decodes the encoded text. It verifies the signature value with the public key, which was acquired from the certification of A, and verifies whether it is a legitimate member or not. The formula to generate the session key has a process like Formula (6) and the formula to decode the encoded text and to verify the signature value has a process like Formulas (7) and (8):

$$SK_{AB} = CID_A \times CID_B \times PSV \quad (6)$$

$$D_{SKAB}[E_{SKAB}\{h(s)||CID_C\}] \quad (7)$$

$$\text{Verify A's signature} \quad (8)$$

Step 7. (B→A): The camera B transmits to the group leader A the signature value which was encoded with the ID of its own and the session key in order to verify whether it, itself, is a legitimate member or not. The formula to transmit has a process like Formula (9):

$$\text{B's certificate, } E_{SKAB}(h^2(s)||CID_C),\ Sig_{pri\_B}[E_{SKAB}\{h^2(s)||CID_C\}] \quad (9)$$

Step 8. (A): The group leader A decodes the encoded text which was transmitted from the member B into the session key and verifies the signature value with B's public key, which was acquired from B's certification, and then verifies whether it is a legitimate member or not. Then, the group leader A makes a group ID through a calculation of the IDs of its own, B, and other members, and generates a group key by using the hash value which it, itself, has. The certification formula to decode the encoded text and to verify member B have processes like Formulas (10) and (11), respectively, and the calculation key to generate the group key has a process like Formula (12):

$$D_{SKAC}[E_{SKAC}(h^2(s)||CID_B)] \quad (10)$$

$$\text{Verify C's signature} \quad (11)$$

$$GK_{ABC} = h(h^n(s) \oplus GID_{ABC}) \quad (12)$$

3.2.2. Group Member Withdrawal Protocol

If a withdrawal of member occurs, the group key must be renewed to secure forward secrecy. Thus, the withdrawing member has to request its withdrawal to the group leader and the group leader has to inform other members about the withdrawing member and generates a new group key. Figure 9 shows the specific procedure of the withdrawal protocol.

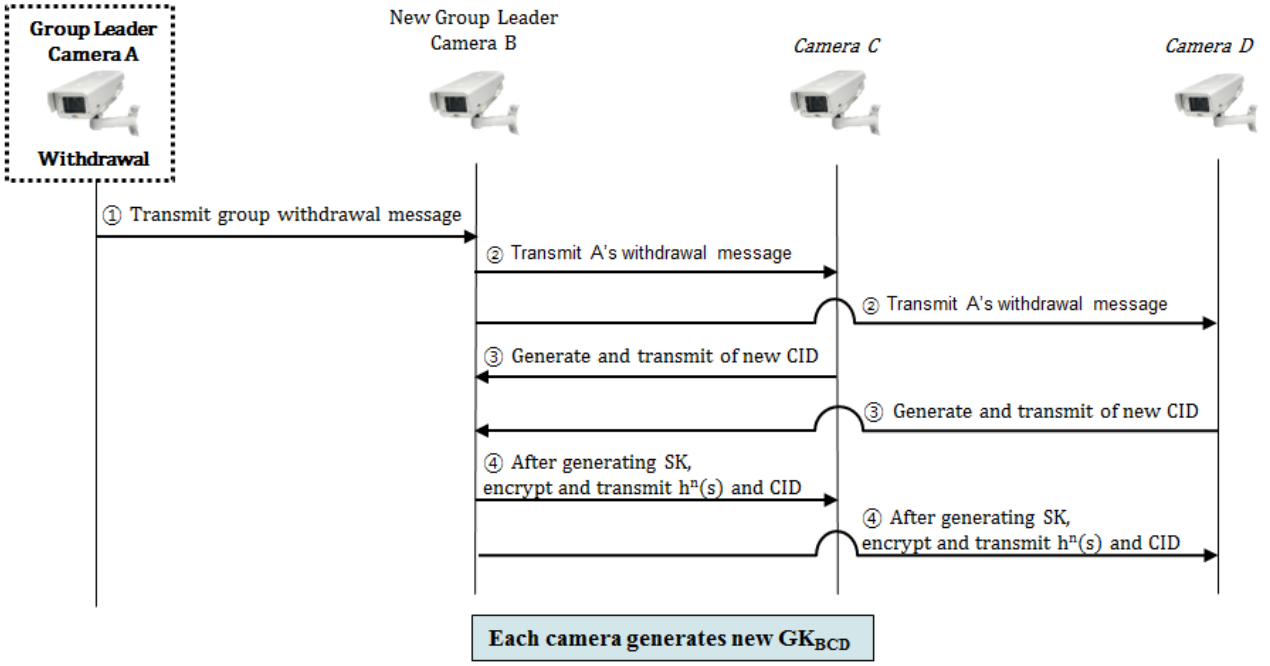

Figure 9. Withdrawal protocol.

Step 1. (A→B): The withdrawing member A transmits the withdrawal message to the member B which is going to the new group leader, and withdraws from the group.

Step 2. (B→C, B→D): The new group leader B transmits the withdrawal message of A to members C and D, and informs that the member A withdraws from the group.

Step 3. Each member which receives the withdrawal message proceeds with the same process as that from Step 3 to Step 7 of the early group key generation protocol, and generates a new group key.

3.2.3. Join Protocol

If a joining of a new member occurs in the group, the existing group key must be renewed to a new one in order to secure backward secrecy. Therefore, the joining member requests their joining to a group member, then the group member or the group leader which receives the join request has to inform other members about the joining member, and renew the existing key to a new one. Figure 10 shows the specific procedure of the join protocol.

Step 1. A new group member joining the group transmits its group join request message to an existing member.

Step 2. The group member who receives the join request message requests the ID from the joining member.

Step 3. The new member who receives the ID request message generates its own ID in the same process as Formula (3) of the early group key generation protocol, and transmits it to the existing member.

Step 4. The member which receives the ID of the new member informs other members about the joining of the new member, encodes the ID of the new member with the existing group key, and transmits it.

Step 5. Each member proceeds with the same process as from Step 4 to Step 7 of the early group key generation protocol, and generates a new group key.

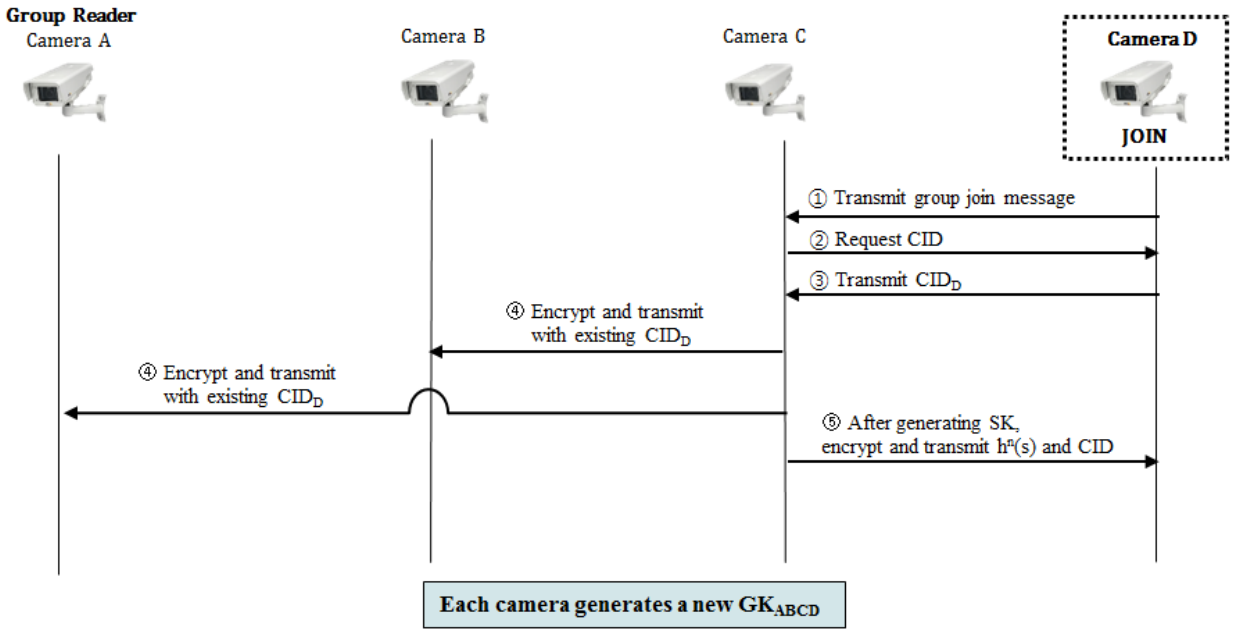

Figure 10. Join protocol.

3.2.4. User Registration Protocol

According to the user registration protocol, the root node (the leader of the highest level) assigns users with access levels according to the access authority policy, requests users to register at groups of the corresponding level, and registers users. Figure 11 shows the specific procedure of the early user registration protocol.

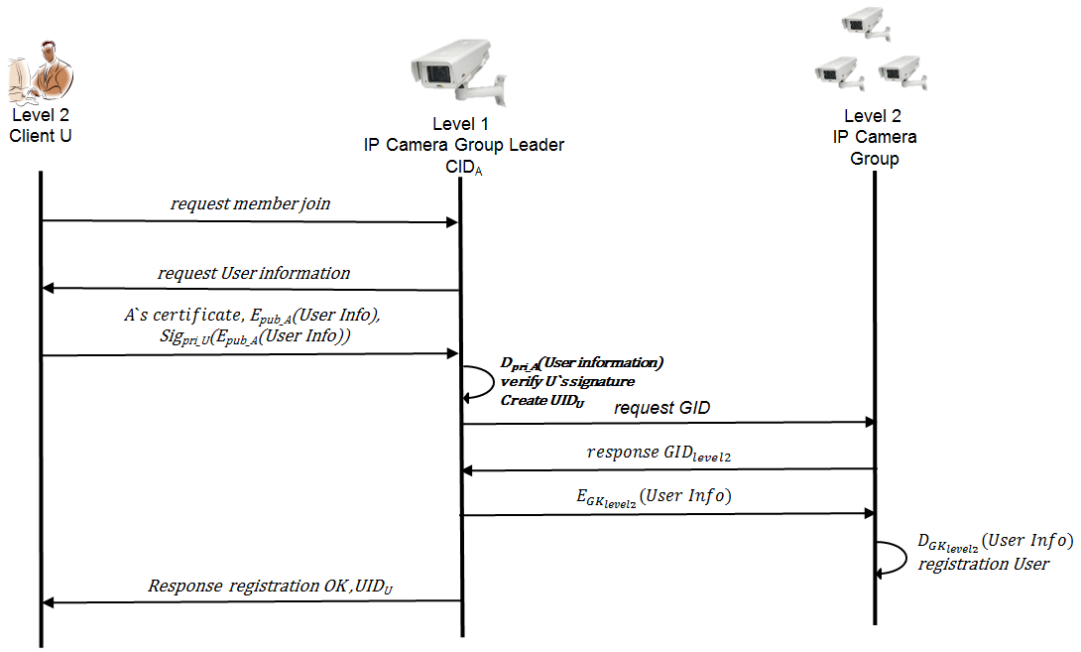

Figure 11. User registration protocol.

Step 1. (U→A) A user transmits its user registration request message to the group leader of the highest level.

Step 2. (A→U) If the group leader of the highest level receives the user registration request message, it requests the user information that wants to register.

Step 3. (U→A) The user signs its own certificate and user information with its own private key, encodes it with the public key of the group leader, and transmits it. The formula to encode with the public key and to transmit has a process like Formula (13):

$$\text{U's certificate, } E_{pub\_A}(Sig_{pri\_U}(\text{UserInfo})) \quad (13)$$

Step 4. (A): After the highest group leader A decodes its own private key, it verifies the signature value with the certification which was transmitted from the user. After the verification is approved, leader A assigns the access authority according to the access authority policy and requests the group leader of the corresponding level for its group ID. The formula to decode the transmitted message and verify the signature value has a process like Formulas (14) and (15):

$$D_{pri\_A}(Sig_{pri\_U}(\text{UserInfo})) \quad (14)$$

$$\text{Verify U's signature} \quad (15)$$

Step 5. (A→level_n Group leader): The highest group leader requests the group leader of level_n for the group ID. On receiving the response, the highest group leader encodes the user information with the group key of the corresponding level (the group key of the corresponding level can be calculated by using a hash chain.), and transmits it. The formula to encode the user information and transmit has a process like Formula (16):

$$E_{GKlevel\_n}(\text{UserInfo}) \quad (16)$$

Step 6. The group leader of the corresponding level registers the user, encodes the user information with the group key, and multicasts it to members of the same group.

Step 7. The highest group leader transmits the registration success message, user ID and the group ID of level corresponding to the access authority.

4. Realization and Comparative Analysis

4.1. Realization Environment

This realization is an experiment to form a hierarchical group between IP camera devices, to generate a group key, to transmit securely the data which can be multicasted, to control access to IP camera devices according to access authority, to encode user passwords which are transmitted in plain text and, ultimately, to complement access control in the existing IP camera environment and to enforce user passwords. Table 2 shows the realization environment of the proposed system.

Table 2. Realization environment of the proposed system.

Classification		Content
Server & Client (PC)	OS	Microsoft Window 7 Enterprise K 32 bit
	Hardware	CPU: Intel Core Quad CPU @ 2.66 Ghz RAM: 3.00 GB
	Development tool	eclipse-java-juno-win32-x86
	Password algorithm	AES128
Client (Mobile)	OS	Android JellyBean 4.1
	Hardware	CPU: 1.7 GHz Quad Core SnapDragon 600 RAM: 2 GB
	Development tool	eclipse-java-juno-win32-x86 android SDK windows
	Password algorithm	AES128

4.2. Realization Result

4.2.1. Early Group Key Generation Realization

In order to compose the first group, the highest root node (group leader) IP camera generates a hash value which is going to be used for its own ID and hash chain. The following Figure 12 shows a part to generate ID and hash value.

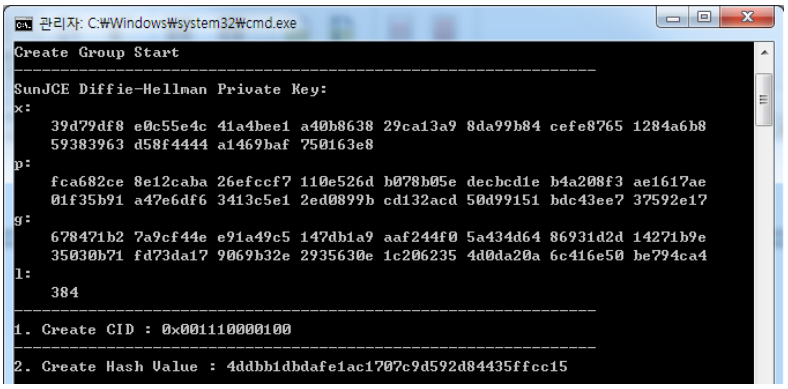

Figure 12. Generation of CID and hash value to compose the first group.

In order to compose a group, the highest root node IP camera receives the transmitted ID of other cameras and generates a session key through a calculation of its own ID and pre-shared value. The following Figure 13 shows a part to generate a session key with transmitted ID of other camera.

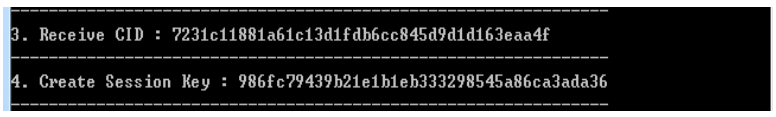

Figure 13. Generation of session key after receiving ID of other cameras.

The highest root node IP camera encodes, using AES 128, the information which other cameras need to calculate the group key with the generated session key, and transmits it to other cameras. Figure 14 shows a part to encode by AES 128 and transmit it.

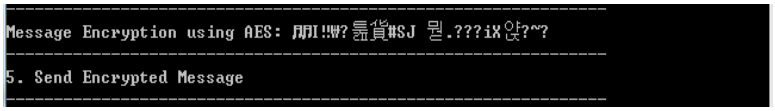

Figure 14. Encryption and transmission of AES.

Each camera receives a message which is needed to calculate the group key, decodes the session key, acquires information to calculate the group key, calculates the group ID, and generates the group key through a calculation with hash value. Figure 15 shows the calculation of group ID and generation of group key.

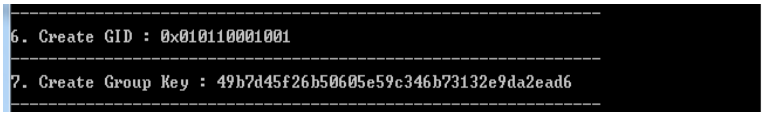

Figure 15. Generation of group ID and group key.

4.2.2. Realization of User Access Control According to Access Authority

In order to carry out camera monitoring, clients add cameras, input ID, password, group ID, and access to the camera server. If the access is permitted, clients are provided with monitoring services. The following Figure 16 shows a process to input IP and port of cameras in order to add monitoring cameras, and Figure 17 shows the realization in mobile devices.

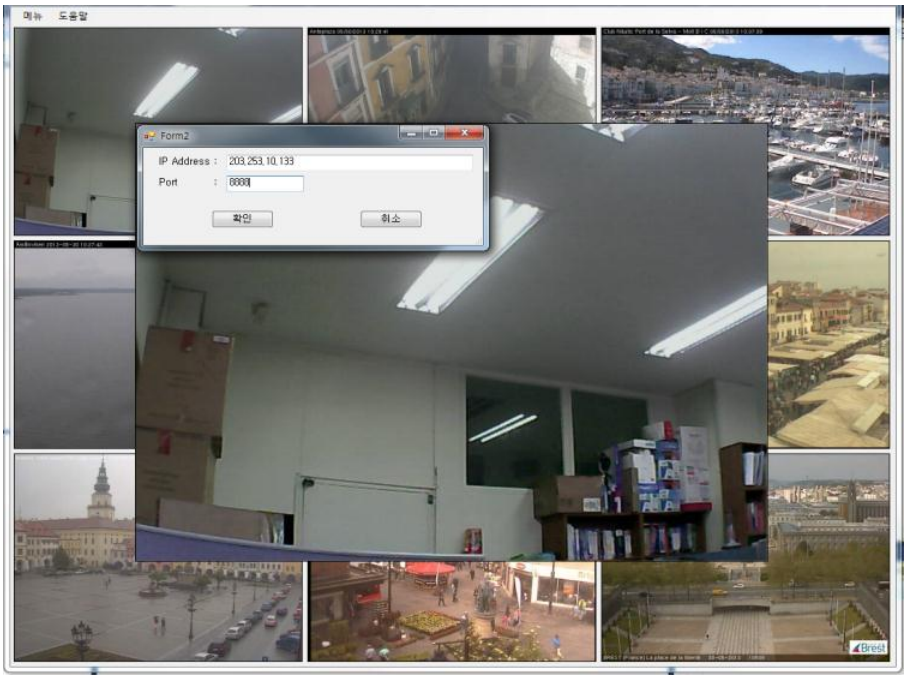

Figure 16. Process of adding cameras.

If the camera server on standby condition receives an access request from a client, it requests ID, password, and the group ID. If the server receives the user information, it verifies the group ID. Then, if the group ID is of a higher level than its own level, the camera server encodes the user information with its own group key and transmits it to the corresponding group leader to request the user confirmation. If the server receives an OK message from the corresponding group leader, it permits the client access and provides service. The following Figure 18 shows the series of the process.

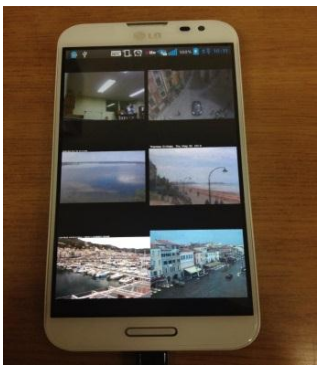

Figure 17. Mobile viewer.

Figure 18. Service request.

4.3. Comparative Analysis

This research analyzes whether the proposed system encodes the multicasting information by using the hierarchical group key, controls access efficiently according to access authority, transmits without deterioration of video quality or not, and proves the efficiency of the proposed system through a comparative analysis of the methods of existing CCTV and IP camera systems and that of the system proposed by this research.

4.3.1. Requirements for Video Surveillance System

The data which is transmitted by the video surveillance system can be divided largely into control data and video data. If some video data is leaked, only the leaked data can be threatening. However, if the control data is leaked, the effect lasts for a long time and a significant problem may occur. Therefore, the access authority to the video surveillance system needs to be enforced. Furthermore, the classification of users who can access the equipment has to be implemented according to the importance of the region which the video surveillance system monitors, and according to the title of accessing user. In addition,

if, in order to manage the camera system, a user accesses many cameras which are installed at remote places, a method to certify the remote access users and to securely maintain the generated session key after the certification is necessary.

4.3.2. Analysis of Security and Efficiency

This section conducted an analysis on such items as management policy, access authority, access denial, *etc.*, in the existing video surveillance system separately, and analyzed its efficiency, respectively. The security of the proposed system was analyzed in terms of user certification and password encryption at remote access. Table 3 describes the results of the comparative analysis of CCTV system, proxy server method, and the proposed system.

Table 3. Comparative analysis with existing systems.

Item	CCTV System	Existing IP Camera	Proposed System
Management policy	Only wired equipment can be managed	Not Supported	Group management is possible, even though installed places are different
Information modification	Information can be modified only by manager	It can be managed in camera server individually	Distributed management is possible by group leaders by grouping cameras
Access authority	Central control center	Every registered user	Management by group
Access denial	Only central control center can monitor	Random access attempts are possible	Supported
User certification	Supported	Not Supported	Supported
Password encryption	Supported	Not Supported	Supported
Support group key	Not Supported	Not Supported	Supported
Computational complexity (for group key)	–	–	LKH($O(\log_2 n)$) OFT($O(\frac{\log_2 n}{2})$)
Mutual authentication	–	–	Supported
Brute-force attack	2^{256}	2^{1024}	$2^{1024} \times 2^{256} \times i$ (i: the number of camera)

5. Conclusions

The purpose of this research was to complement the weaknesses of the existing system and show that it has limitations, which can be caused by the absence of a management system; that, when users log in, the existing system transmits the passwords in plain text so that it is vulnerable to sniffing and complete survey attack; and that anyone can access the IP cameras at remote places due to the absence of an access control system according to access authority. Accordingly, this research proposes a technique which can control the access of users without the access authority, or with a low level, by composing a hierarchical group, generating different group keys according to the class respectively, and so using different groups according to access authority.

The proposed system uses the hash chain technique in order to compose the hierarchical group keys, so that the member of a higher level can access a group of lower class by calculating the group key of the lower level. However, the member of lower level cannot access groups of a higher level because the member of the lower level cannot calculate the hash value of the group of higher level. Additionally, it certifies the legitimacy of joining members of the group by using certification and digital signatures and, therefore, secures the safety against the sham attack. Furthermore, the proposed system was designed to conduct the user certification by using certification and signature when users log in to the IP camera web server, and to encode the password which is transmitted in plain text so that it secures safety against the sniffing attack.

In order to analyze the efficiency and security from the perspective of the management of the proposed system, this research conducted the comparative analysis on such items as management policy, access authority, access denial, and user certification of a CCTV system, existing IP camera system, and the proposed system, respectively. As a result of that analysis, it has been found that the security of the CCTV system is similar to that of the proposed system because CCTV is operated in a closed system. However, the CCTV system has critical limitations in a way that it cannot be accessed from a remote place, and the entire access authorities are concentrated in the central control center, so if the central control center is attacked, the entire surveillance system can be accessed and attacked. On the contrary, the proposed system separates groups hierarchically, controls access according to each group, respectively, and provides services so that even if a part of the system does not work properly, it cannot have any effect on the monitoring service of other camera.

Conclusively, it provides the higher efficiency than any other system. The result of the comparative analysis of the proposed system and the existing IP camera system demonstrates that access control, user certification, and password encryption of the proposed system provide more secure services than those of the existing system. Even though this research realized the access authority system to IP cameras, and thus solved the problems of access control and passwords which are transmitted in plain text, there is still the possibility that the integrity of video information could be damaged. Therefore, it is suggested that more research and analyses are required to encode the video information, to apply appropriate encryption methods according to the importance of video information, consequently to maintain the confidentiality of the video information, and to prevent the deterioration of video quality in the future.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1014) supervised by the IITP (Institute for Information & communications Technology Promotion).

Author Contributions

Jungho Kang researched relation work; Jungho Kang and Jaekyung Han designed the scheme; Jungho Kang and Jong Hyuk Park performed and analyzed the data; Jungho Kang and Jaekyung Han wrote the paper.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Lee, K.J.; Park, J.S.; Kim, D.H.; Huh, M.J.; Park, J.H.; Jeon, Y.S. Analyses of Research Trends on Networked-Camera. In Proceedings of the Korea Multimedia Society Conference, Seoul, Korea, November 2010; pp. 424–426.
2. Ibrahim, N.; Mohammad, M.; Alagar, V. Publishing and discovering context-dependent services. *Hum. Centric Comput. Inf. Sci.* **2013**, *3*, doi:10.1186/2192-1962-3-1.
3. Ryu, D.H.; Han, J. *Distributed Smart Camera Systems Security Issues*; Review of KIISC; Korea Institute of Information Security and Cryptology: Seoul, Korea, 2010; Volume 20, pp. 31–42.
4. Gnanaraj, J.W.K.; Ezra, K.; Rajsingh, E.B. Smart card based time efficient authentication scheme for global grid computing. *Hum. Centric Comput. Inf. Sci.* **2013**, *3*, doi:10.1186/2192-1962-3-16.
5. Chu, H.H.; Qiao, L.; Nahrstedt, K. Secure Multicast Protocol with Copyright Protection. *ACM SIGCOMM Comput. Commun. Rev.* **2002**, *32*, 42–60.
6. Dondeti, L.R.; Mukherjee, S.; Samal, A. A Dual Encryption Protocol for Scalable Secure Multicasting. In Proceedings of the IEEE Symposium on Computers and Communications, Red Sea, Egypt, July 1999; pp. 2–8, doi:10.1109/ISCC.1999.780748.
7. Juneja, M.; Sandhu, P.S. A New Approach for Information Security Using an Improved Steganography Technique. *J. Inf. Process. Syst.* **2013**, *9*, 405–424.
8. Panduranga, H.T.; Naveen Kumar, S.K.; Sharath Kumar, H.S. Hardware Software Co-Simulation of the Multiple Image Encryption Technique Using the Xilinx System Generator. *J. Inf. Process. Syst.* **2013**, *9*, 499–510.
9. Chung, Y.; Choi, S.; Won, D. Lightweight anonymous authentication scheme with unlinkability in global mobility networks. *J. Converg.* **2013**, *4*, 23–29.
10. Vanus, J.; Kucera, P.; Martinek, R.; Koziorek, J. Development and testing of a visualization application software, implemented with wireless control system in smart home care. *Hum. Centric Comput. Inf. Sci.* **2014**, *4*, doi:10.1186/s13673-014-0019-5.
11. Bae, K.; Lee, K.; Yim, K. Proxy Server Providing Multi-level Privileges for Network Cameras on the Video Surveillance System. *Korean Soc. Int. Inf. Rev. Korean Soc. Int. Inf.* **2011**, *12*, 126–133.
12. Zheng, X.; Huang, C.; Matthews, M. Chinese Remainder Theorem Based Group Key Management. In Proceedings of the ACM Southeast Conference, Winston-Salem, NC, USA, 23–24 March 2007.
13. Chung, W.H.; Kumar, S.; Paluri, S.; Nagaraj, S.; Annamalai, A., Jr.; Matyjas, J.D. A Cross-Layer Unequal Error Protection Scheme for Prioritized H.264 Video using RCPC Codes and Hierarchical QAM. *J. Inf. Process. Syst.* **2013**, *9*, 53–68.
14. Degefa, F.B.; Won, D. Extended Key Management Scheme for Dynamic Group in Multi-cast Communication. *J. Converg.* **2013**, *4*, 7–13.
15. Goswami, K.; Hong, G.S.; Kim, B.G. A Novel Mesh-Based Moving Object Detection Technique in Video Sequence. *J. Converg.* **2013**, *4*, 20–24.

16. Ogiela, M.R.; Ogiela, U. Linguistic Protocols for Secure Information Management and Sharing. *Comput. Math. Appl.* **2012**, *63*, 564–572.
17. Ogiela, M.R.; Ogiela, U. Security of Linguistic Threshold Schemes in Multimedia Systems. In *New Directions in Intelligent Interactive Multimedia Systems and Services—2, Studies in Computational Intelligence*; Damiani, E., Jeong, J., Howlett, R.J., Jain, L.C., Eds.; Springer-Verlag Berlin Heidelberg: Berlin, Germany; Heidelberg, Germany, 2009; Volume 226, pp. 13–20.
18. Kim, C.O.; Kang, K.; Cho, Y.J. A Distributed Multicast Group Key Management Scheme for a Hierarchically Structured Network. Korea information science society. *J. Korea Inf. Sci. Soc. Data Commun.* **2011**, *38*, 22–32.
19. Pegueroles, J.; Rico-Novella, F.; Hernandez-Serrano, J.; Soriano, M. Improved LKH for batch re-keying in multicast groups. In Proceedings of International Conference on Information Technology, Research and Education 2003, Neward, NJ, USA, August 2003; pp. 269–273.
20. Sherman, A.T.; McGrew, D.A. Key Establishment in Large Dynamic Groups using One Way Function Trees. *IEEE Trans. Softw. Eng.* May **2003**, *29*, 444–458.
21. Perrig, A. Efficient Collaborative Key Management Protocols for Secure Autonomous Group Communication. In Proceedings of the International Workshop on Cryptographic Techniques and Electronic Commerce, Hong Kong, China, July 1999; pp. 192–202.
22. Ingemarsson, I.; Tang, D.; Wong, C. A Conference Key Distribution System. *IEEE Trans. Inf. Theory* **1982**, *28*, 714–720.
23. Steiner, M.; Tsudik, G.; Waidner, M. Diffie-Hellman Key Distribution Extended to Group Communication. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, New York, NY, USA, 1996; pp. 31–37.
24. Burmester, M.; Desmedt, Y. A Secure and Efficient Conference Key Distribution System. In *Advances in Cryptology, Eurocrypt*; Springer Berlin Heidelberg: Berlin, Germany; Heidelberg, Germany, 1994; pp. 275–286.
25. Perrig, A.; Song, D.; Tygar, J.D. ELK, a New Protocol for Efficient Large-Group Key Distribution. In Proceedings of the IEEE Symposium on Security and Privacy 2001, Oakland, CA, USA, 14–16 May 2001; pp. 247–262.