# Content Protective Multi-Agent Platform for MsMu Service and Pattern-Based Content Management

Yoonsik Uhm, Zion Hwang, Minsoo Lee, Jaehoon Nah, Hwangjun Song, and Sehyun Park

**Recent research on mobile Internet protocol television and digital right management (DRM) interconnections has focused on multimedia technologies designed to enhance content scalability and adaptive content distribution. However, due to the architectural and scalable limitations, recent systems are not flexible and securable with respect to their adaptive content distribution and protective policy management. Therefore, we propose a content protective multi-agent platform that provides secure multimedia services, correlation management, pattern-based management, and multi-source multi-use (MsMu)-based services. Our architecture, supported by DRM, lets us create a rich set of MsMu-based content protection and seamless multimedia services through the extension of one source multi-use (OsMu)-based content services. We have verified our platform, which provides scalable and securable services with a 17% lower service response time by using a testbed.**

**Keywords: MsMu, secured content distribution, content management, seamless multimedia service.**

## I. Introduction

With an ever increasing demand for ubiquitous multimedia services, a service platform [1], [2] has been implemented to support mobility control, handover management, content transcoding, and adaptive content distribution. Users are offered content download services and adaptive multimedia services [3] using predefined (authenticated) devices through a service provider (SP) and a set-top box. In addition, in order to solve the mobility control and device-independent management issues, the service platform implements the mobile Internet protocol television (IPTV) [4] service and the one source multi-use (OsMu)-based content service. Although the previous systems could guarantee the partial mobility management and content transcoding, it is hard to control the adaptive interconnection of the heterogeneous networks, SPs, and devices. Crucial issues such as scalability, user/content/device authentication, and secure content distribution were not adequately considered in the previous systems.

The previous systems tried to generate patterns using event management for their reasoning services. These systems implemented a conceptual and static context model instead of a service-oriented model with regard to the context characteristics. In order to increase the inference accuracy and to effectively distribute services, the system needs to control events and the service status (history) as well as the situational contexts, containing conflict, device status, device control, and so on according to its network and context convergence. With regard to the correlation between the services and the policies, the system must maintain the service status and authentication interconnection in heterogeneous environments, that is, multi-SPs, networks, users, and service domains. The policies and

Manuscript received Mar. 15, 2010; revised July 28, 2010; accepted May 6, 2010.

This research was supported by the Ministry of Knowledge Economy (MKE), Rep. of Korea, under the Home Network Research Center (HNRC)-Information Technology Research Center (ITRC) support program supervised by the National IT Industry Promotion Agency (NIPA) (NIPA-2010-C1090-1011-0010).

Yoonsik Uhm (phone: +82 2 822 5338, email: neocharisma@wm.cau.ac.kr), Zion Hwang (email: zhwang@wm.cau.ac.kr), Minsoo Lee (email: leemins@wm.cau.ac.kr), and Sehyun Park (corresponding author, email: shpark@cau.ac.kr) are with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, Rep. of Korea.

Jaehoon Nah (email: jhnah@etri.re.kr) is with the Software Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Hwangjun Song (email: hwangjun@postech.ac.kr) is with the Department of Computer Science and Engineering, Pohang University of Science and Technology, Pohang, Rep. of Korea.

doi:10.4218/etrij.10.1510.0143

information within the digital right management (DRM) must have a tightly-coupled connection and the ability to determine the adaptive services.

Recent studies on multi-source multi-use (MsMu) services and content management systems have focused on device-independent content services using scalable video coding (SVC)-based adaptive transcoding [4] and network interconnection. However, previous systems still lack an effective content and context management and protective mobility management. In order to implement the MsMu-based multimedia services, the framework needs to provide the following features: seamless service management, network interconnection, adaptive transcoding, user-centric content management, and effective content distribution network.

Seamless service management transfers the content and service status to a different system or SP. The content and the service restart on the user's device or other appliances in another service domain.

Network interconnection dynamically switches the connections (SP/system/device) according to the service status, the content information, and the device status.

Adaptive transcoding adaptively manages multimedia content according to the device status, the available bandwidth, the network status, and the authentication information. The transcoding must consider the tradeoff between the content quality and the performance, limiting the encoder complexity and transcoding delay.

User-centric content management autonomously reconfigures the device, content, and service with respect to the authentication information, the device status, the user service pattern, and the location context.

Effective content distribution network dynamically manages the content distribution and content information using cloud computing according to domain characteristics such as the location purpose, content type, user type, and mobility frequency.

The extension from OsMu to MsMu interconnects various SPs, networks, devices, and users. The MsMu platform must address a tremendous number of policy, security, and privacy problems. To implement the MsMu service and deliver ubiquitous multimedia service, the service platform needs to protect and manage the content, the context, and the services. We define the following four elements regarding content protection:

Authentication management provides for a dynamic transformation of the user, location, service, and device information to another system through user mobility. The service platform needs to manage various networks and domains based on their contexts such as user profiles, situations, events, domain-specific services, service status, location-aware policy, content information, patterns (mobility, lifestyle, and service request type), environmental information, and authentication information.

Interconnection management autonomously controls the handover and reconfigures the services containing adaptive content with respect to user mobility, authentication modification, and device/network/domain/service change. The service platform must provide a protective operation according to various situational and environmental contexts as well as authentication information.

DRM controls the digital rights provided by the content providers (CPs), SPs, and individual users using DRM and fingerprints. The service platform must apply the adaptive policy to each user, device, location, and content service.

Secure content distribution manages the content, the transcoding information, and the authentication information to effectively provide secure multimedia services using cloud computing.

Therefore, we propose a content-protective multi-agent platform that manages the MsMu services in order to achieve secure management and interconnection. We also suggest an ontology-based secure content management with pattern learning and DRM. Furthermore, we designed our platform to reflect actual activity patterns and service patterns.

The remainder of this paper is organized as follows. In section II, we discuss the related works on multimedia service platforms for providing MsMu services. In section III, we summarize the content management issues based on the MsMu scheme. In section IV, we present our content protective multi-agent platform and our ontology-based context model. In section V, we summarize our implementation and performance evaluation results. Finally, we draw our conclusions and suggest future work in section VI.

## II. Related Work

Many studies have focused on content management and service interconnection for MsMu services, which aim to enhance seamless and adaptive multimedia services. Recent works on multimedia service systems have been categorized into two types based on their architecture. The two types are the service-oriented system with a context model and the high-quality multimedia distribution system [5].

First, in keeping with the new paradigm changing from static location-aware systems to service-oriented multimedia systems using MPEG-21 digital item adaptation [6], it is necessary to resolve diverse service conflicts through accurate service prediction [7]. Domain-oriented systems [1], [8] have been devised to use context and event analysis for adaptive service prediction regarding the inhabitants in home domains. To accurately consider and manage these services [9], the system processes the various events and situations. However, excessive event processes may lead to increased resource consumption and frequent unnecessary policy modifications. Moreover, the conventional systems do not regard content protection, secured authentication interconnection, and safe content management. In order to adequately support service-oriented and personalized multimedia services, a service platform must classify events and monitor policy, authentication, digital rights, and security to meet protective multimedia service requirements.

Providing high-quality multimedia services including the future (mobile) IPTV requires the right combination of reliable IP-transport, context management, scalable transcoding [10], interoperable DRM [11], and easy accounting. Two key features, content reusability and content protection, are essential to provide protective multimedia delivery throughout the MsMu service platform. For content protection, robust and structural DRM with interconnected information is needed. Standard interfaces that can provide a common interface for transferring data between heterogeneous DRMs are required for seamless multimedia services in next generation networks.

Furthermore, to achieve an easy use of multimedia services, users will require more convenient billing methods while they roam. A user may register his or her own devices at home or the office for daily use or wish to temporarily use a device belonging to a friend. As an example of simple authentication and accounting, a user may enlist the device's IP address or MAC address in his trusted device through his 3G cellular phone using a universal subscriber identify module (USIM). The SP will then allow forwarded multimedia streaming on that device.

## III. MsMu Content Management Issues

Due to the increase in user movement and the expansion of use range, the aim of content management changes from

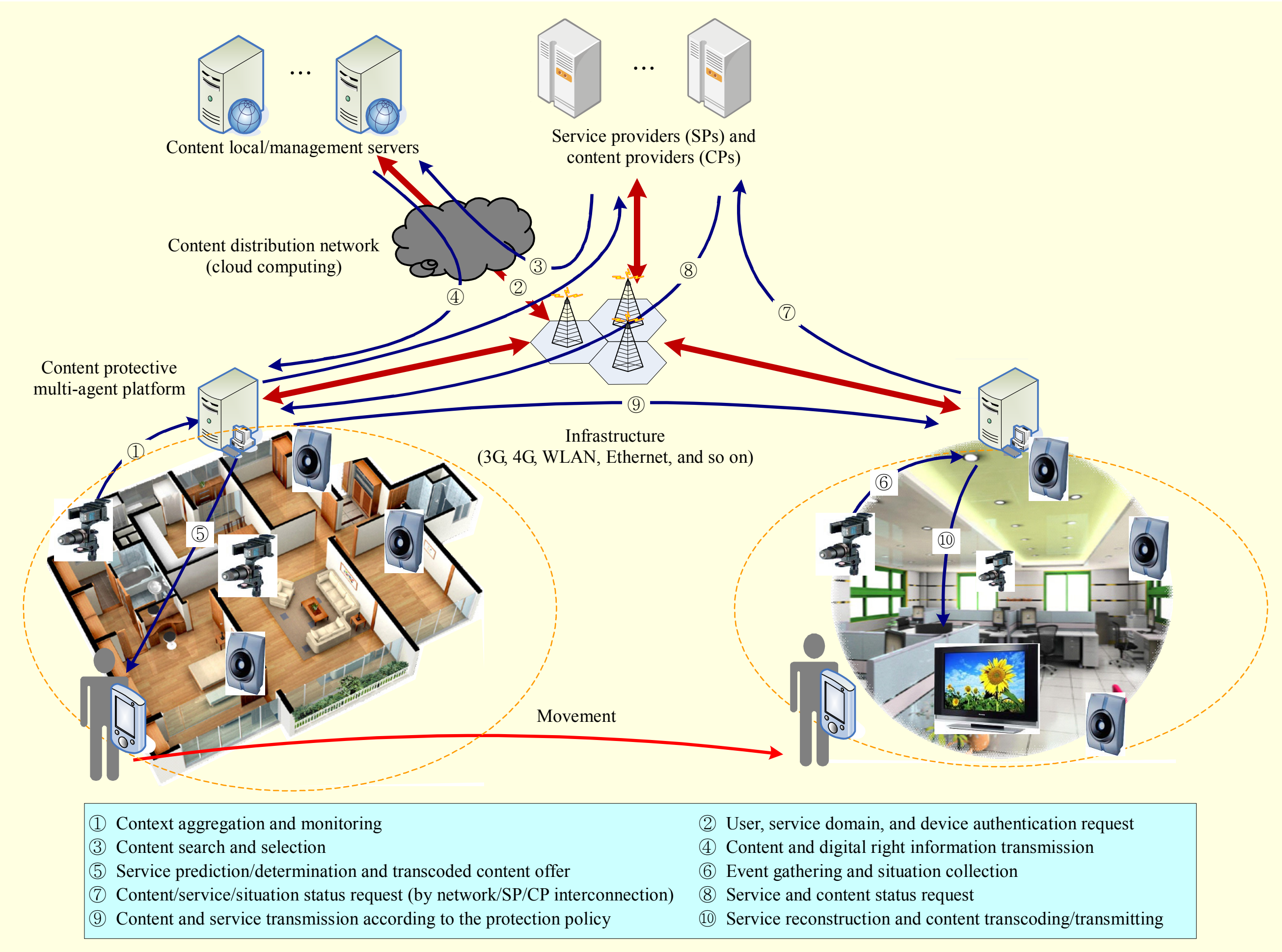
Content local/management servers
Service providers (SPs) and content providers (CPs)
Content distribution network (cloud computing)
Content protective multi-agent platform
Infrastructure (3G, 4G, WLAN, Ethernet, and so on)
Movement
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩
① Context aggregation and monitoring
② User, service domain, and device authentication request
③ Content search and selection
④ Content and digital right information transmission
⑤ Service prediction/determination and transcoded content offer
⑥ Event gathering and situation collection
⑦ Content/service/situation status request (by network/SP/CP interconnection)
⑧ Service and content status request
⑨ Content and service transmission according to the protection policy
⑩ Service reconstruction and content transcoding/transmitting

Fig. 1. MsMu-based content service and system architecture with interoperability and self-protection.

high-quality content diversity to seamless multimedia service with content protection. In MsMu environments, the content management needs to enhance the seamless service based on DRM as well as the protective content/context distribution with scalable transcoding. The MsMu platform considers the service interconnection, information interconnection (for example, content, environmental and situational context, authentication, and policy), and content scalability. The MsMu framework allows users to establish or negotiate a multimedia service which considers a complex set of access selection criteria, thereby accessing multimedia in the best possible way. In Fig. 1, the user 'Tom,' moving from a multimedia portal that distributes digital content to a 3G wireless entry point, could also decide to nomadically change the download and device. When Tom enters his home while downloading through his cellular phone, he continues to download using his home multimedia system through service convergence.

The case of MsMu service from multiple SPs is also shown in Fig. 1. A prerequisite for using the MsMu is an agreement between the home's SP and the office's SP. Also, Tom must consent to be served through office devices by the office's SP. Therefore, before Tom's multimedia can be requested from the other device which the user does not own, the home's SP must ask Tom to handle the authorization. Tom and a foreign device (office device) are registered and authenticated through the home's SP registration interface. The SP uses a short message service (SMS) for authorization. After the prerequisites are fulfilled, Tom can request a new download of authorized devices. Tom sends a download request for particular users, identified by their mobile subscriber integrated services digital network numbers (MSISDNs) or an alternative pseudonym(s), depending on the privacy solution selected. If the positioning of the office's particular MSISDN and device are authorized with Tom's consent, the request is sent to the SP. Then the SP continues downloading through the office's device by the privilege delegation using the ontology-based DRM [12].

In MsMu environments, the service platform must provide four functions for secure and protective content management: authentication continuity, device/SP/network-independent service, dynamic DRM, and adaptive transcoding.

Authentication continuity transmits the authentication, content status, and service status used to maintain the multimedia services according to the interconnections between the SPs, CPs, and networks.

Device/SP/network-independent service seamlessly switches connections during handoffs, device changes, domain changes, and situational interrupts, such as service collisions and event generation in all places.

Dynamic DRM provides content protection and resumes multimedia services according to multiple DRM processes for multiple users when the network, device, and SP are changed to another domain.

Adaptive transcoding enables scalable representation of multimedia content using SVC. With regard to the authentication information and the device profile, the system provides the transcoding content with the available quality.

Our service platform, including the protective MsMu content management scheme, provides seamlessly secure multimedia service and adaptively protective content distribution.

## IV. Content Protective Multi-Agent Platform

In order to support reusability, interoperability, robustness, and scalability, we designed a content protective multi-agent service platform that provides DRM-based content distribution, SVC-based transcoding, and secure MsMu services. Along with the emerging need for protective multimedia services, our platform learns various patterns such as user activity, device status, service status, and policy modification. We designed the context model shown in Fig. 2, which consists of classes for pattern generation and properties for context, content, and policy interconnection. To enhance the service and network interoperability based on the protective policy, our platform manages the distributed contexts, content, digital rights information, authentication, and policies.

### 1. Content and Context Management Using Ontology

To effectively manage the content and contexts, the major design goals of the context model are in classifying the environmental and situational contexts, and in organizing the correlations between the multimedia services and policies, which include authentication, security, and DRM. The context model also needs to aggregate and sort events, such as the situational changes, environmental context changes, user movements, domain changes, collisions, and device changes.

Previous context models [13]-[15] aim to manage content storage and sorting. Furthermore, conventional models [8] do not focus on the service-oriented correlation classification but on the structural (conceptual) description of the environmental contexts with plain classes such as a person, a space, an entity, a time, and an event. Although recent models include user movements and service history, these models find it difficult to provide to the MsMu service management for multi-users according to the content management, the pattern management, and the correlation representation.

Therefore, the context model must be able to predict the adaptive multimedia services using content protection and pattern generation. In order to construct patterns and

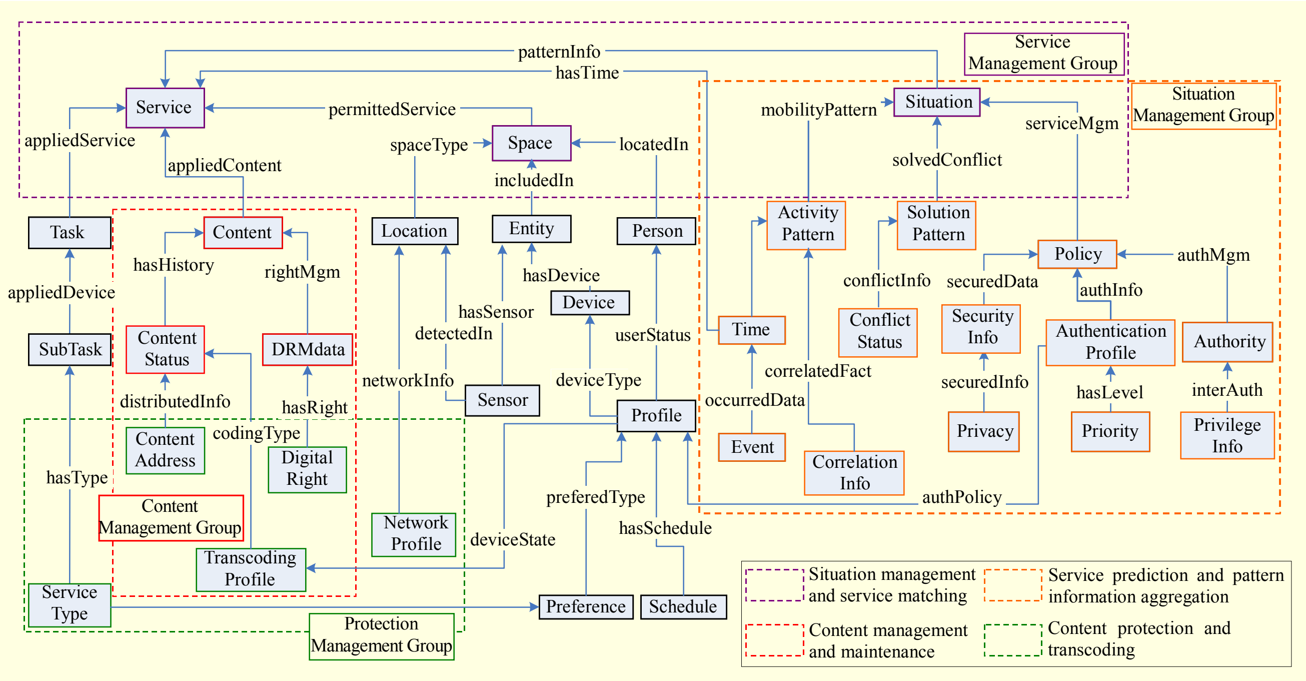

Fig. 2. Ontology-based content protection context model.

correlations, the context model must classify various factors: situational contexts, environmental contexts, interrupts, events, profiles, and preferences. Especially necessary is the profile which defines the basic context characteristics, including user, device, and space, representing properties such as age, job, location, and usage. The preference is for the priority of service, content, space, and so on. For instance, according to the service history and patterns, a user who prefers to use his or her handheld device and another user who prefers to use an appliance providing high-quality content can be offered different services and policies in the case of conflict.

To provide MsMu services with interoperability, robustness and scalability, we propose an ontology-based content protection context model that manages the correlations, descriptions, and interconnections of content, context, event, and pattern. With a well-defined and appropriate hierarchical structure using F-logic language [16], our ontology defines a set of context interconnections to describe the services, events, and status.

In order to achieve an efficient situation management, our model generates correlations and services according to the pattern analysis by using a hidden Markov model. For example, while one user is being offered multimedia service, another user enters into the same space which leads to a service conflict. For enhancing the efficiency of the pattern-based service generation, our platform requests and gathers numerous contexts such as service status, number of users, time, space profiles, device status, content status, authentication, SP information, digital rights, and user profiles. In the above case, our platform provides content to another user according to the reconstructed policies and authentication privileges, interconnecting with the DRM/SP using standard interfaces and transferring data among the heterogeneous DRMs.

Figure 2 shows our proposed model which contains classes, properties, and interconnections. The conventional model classifies conceptual classes, such as a person, an entity, a location, a sensor, a profile, and a time. In our model, the four groups are the Service Management Group, the Situation Management Group, the Content Management Group, and the Protection Management Group. Service, Space, and Situation classes, making up the Service Management Group, represent the interconnected properties for the correlation between patterns and location-based/user-centric services. This group also manages the service elements aggregated from the subclasses. The Situation Management Group provides the history of conflicts, policies, movements, and events. This group then generates the activity patterns, the conflict solution patterns, the service reconstruction patterns, the policies, and the correlations with regard to the history. In addition, this group interconnects the situational contexts with the environmental and conceptual contexts. As seen in Fig. 2, the Content, ContentStatus, ContentAddress, and DRMdata classes, making up the Content Management Group, manage the multimedia services and establish the correlations of the content service-to-space, the content-to-device, and the content-to-heterogeneous situation. The ContentAddress class aggregates the information of the content location, the digital rights, and the content status using cloud computing with a content distribution network. To ensure scalability and robustness, this class also interconnects with the ContentStatus class which controls the service history and the related SP/CP information, including authority information. The Protection Management Group represents the profiles of the content and the service status based on the DRM and SVC transcoding. The TranscodingProfile class gathers the device characteristics and user authentications from the Profile class including the AuthenticationProfile class for determining the adaptive encoding and decoding.

In order to increase the effectiveness of the pattern-based service and to enhance the robustness of the protective policy, our model classifies the situations and events and sorts the correlations between the service elements and the policy elements such as the DRM information, the transcoding profiles, the authentication information, the conflict solutions, and the interconnection data in the heterogeneous SPs/CPs/networks. In addition, our model manages the status of the authentication, patterns, the content, the privileges, and the events for content protection and seamless multimedia service.

## 2. System Architecture

In line with the protective MsMu service, we designed and implemented a content protective multi-agent platform to support content protection and seamless multimedia services as shown in Fig. 3. We developed a situation management system as discussed in detail in [17]. The proposed platform focuses on policy management, the SVC-based device-independent service, content protection, the ontology-based scalable DRM, and seamless services. Our platform predicts the adaptive multimedia services according to an event analysis and correlation determination. In order to effectively predict the services and to manage the content status, our platform consists of five parts: the Context Management Part, the Knowledge Repository, the Inference Part, the Policy and Security Part, and the Content Management Part.

The Context Management Part provides context aggregation, event analysis, context classification, and context verification. This part categorizes the input data (events and service requests) and transforms the adaptive format for context (event) storage and modification. This part transmits the threshold to the sensors according to the policies and space characteristics. The context manager gathers the events with a context correlation scheme and periodically requests the status using the network configuration. According to the service request or user profile (preference and schedule), a mining engine collects and sorts the crawling contexts from the Web. In addition, this engine selects the content information and the status with regard to the cloud computing from the content

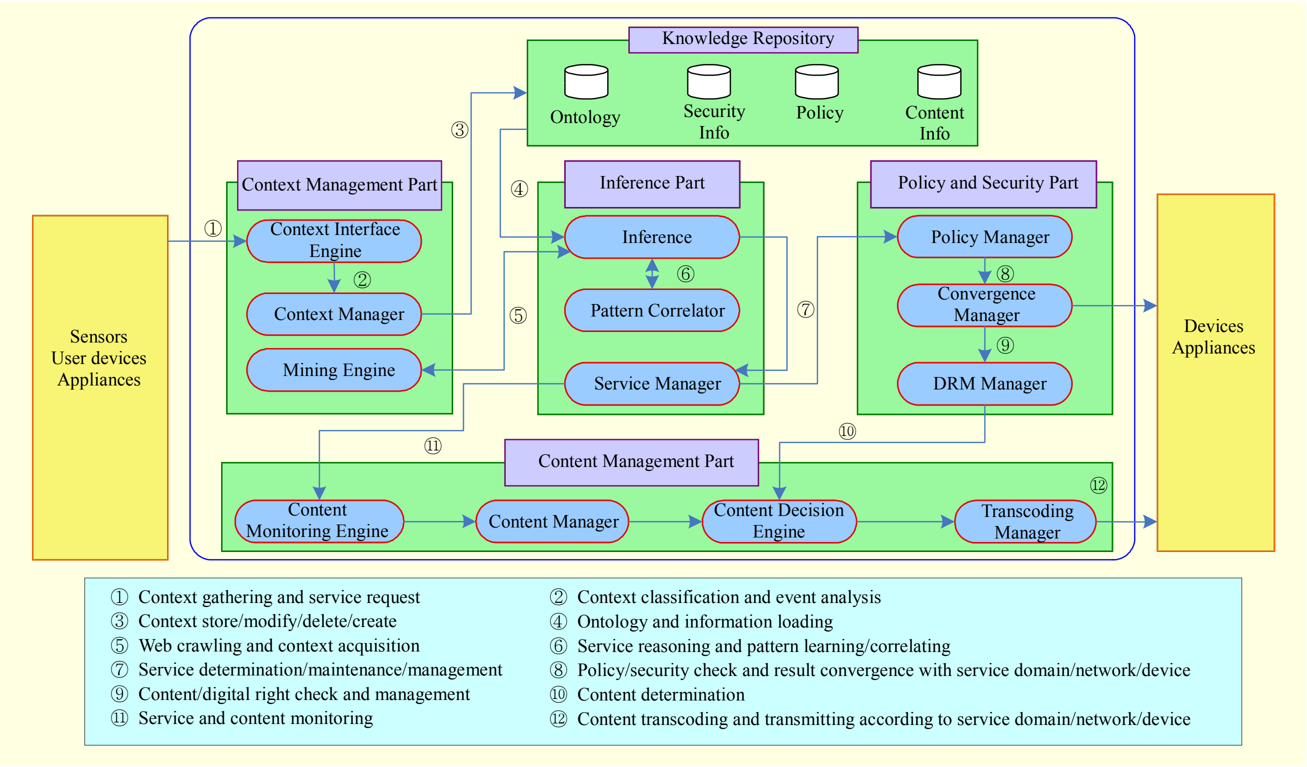
Knowledge Repository
Ontology
Security Info
Policy
Content Info
③
④
Context Management Part
Context Interface Engine
②
Context Manager
Mining Engine
Inference Part
Inference
⑥
Pattern Correlator
Service Manager
⑤
⑦
Policy and Security Part
Policy Manager
⑧
Convergence Manager
⑨
DRM Manager
Sensors
User devices
Appliances
①
Devices
Appliances
⑪
⑩
Content Management Part
⑫
Content Monitoring Engine
Content Manager
Content Decision Engine
Transcoding Manager
① Context gathering and service request
② Context classification and event analysis
③ Context store/modify/delete/create
④ Ontology and information loading
⑤ Web crawling and context acquisition
⑥ Service reasoning and pattern learning/correlating
⑦ Service determination/maintenance/management
⑧ Policy/security check and result convergence with service domain/network/device
⑨ Content/digital right check and management
⑩ Content determination
⑪ Service and content monitoring
⑫ Content transcoding and transmitting according to service domain/network/device

Fig. 3. Content protective multi-agent platform architecture.

distribution network. The mining engine also analyzes the situation instances for verifying service patterns.

The Knowledge Repository autonomously updates (stores, modifies, and deletes) the events, environmental contexts, situational contexts, service status, and policy information. Furthermore, it interconnects the contexts and services according to the context model. The Knowledge Repository interconnects with other systems or SPs/CPs using cloud computing in heterogeneous service domains, spaces, networks, and devices. An ontology-based context model connects and aggregates to the SecurityInfo, Policy, and ContentInfo DBs. The SecurityInfo DB which cooperates with SPs/CPs interconnects with the SecurityInfo, AuthenticationProfile, and Authority classes in the Situation Management Group as shown in Fig. 2. The Policy DB stores the system and rule management policies. This DB cooperates with the Policy, Privacy, Priority, and PrivilegeInfo classes for rule generation and service pattern management. The ContentInfo DB interconnecting with the DRM server, SPs, and CPs provides content profiles and policies. It cooperates with the Content Management Group and the Protection Management Group. The Knowledge Repository manages the ontology, the information about content and digital rights, and the rule set for correlation control and robust content management. The context model, including the ontology and the rule, updates and modifies the situations, the service status, and the conflict solutions.

The Inference Part predicts the adaptive services with scalable content according to the contexts and policies aggregating from the Knowledge Repository. This part determines service reconstruction with regard to the service status, events, and patterns. It decides when and which services should be provided to multi-users in various situations. The Inference Engine resolves conflicts and provides pattern-based services. To generate service patterns, the Inference Engine cooperates with the Mining Engine using the Situation Management Group. According to the situation and event analysis, the Pattern Correlator generates and represents the relationships of the service-to-activity, event-to-policy, service-to-status, service-to-conflict, and pattern-to-policy. The Service Manager monitors the service status and maintains the service policy. When a user moves to another domain or the environment changes, this manager analyzes the novel situations and determines the service reconstruction including the content retransmission with adaptive transcoding using the interconnection with the Inference Engine.

The Policy and Security Part verifies the service according to the service status, situations, and conflict status. This part establishes the service policies and the protection data. In addition, it examines the conflict solutions with respect to the situational contexts from the Situation Management Group. It also provides policy modification and the convergence management of the networks/SPs/CPs/systems. The Policy Manager provides the service construction policy and the relationship representations of the rules. To obtain conflict solutions, this manager cooperates with the patterns and profiles found in the Situation Management Group and the Protection Management Group. It performs authorization and transmits the authentication information to other SPs and systems. If a user who wants to be offered seamless service moves to another service domain and connects to another SP, this manager transmits an SMS message with a uniform resource locator (URL) and a passphrase to validate the mobile user. Authentication may be performed using the information contained within the SMS, and so the SP cannot access information about the user until the user accepts the service. The Convergence Manager transforms the services including the control messages and then transmits them to adaptive devices, networks, and service domains. The DRM Manager interconnects with DRM servers using the content distribution network. This manager verifies the content with regard to the registered (stored or controlled) rights using ontology [12] and the context model, including authority and policy. It also requests adaptive content according to the devices, user authentication information, and the network/SP status.

The Content Management Part autonomously maintains the content status and seamlessly transmits the adaptive content according to the changes in the situations in the heterogeneous environments, such as handoffs, device changes, domain changes, and situational interrupts. This part transcodes the content with regard to the authentication, device, user profile, environmental contexts, and conflict status. Moreover, it verifies the effectiveness of the distribution, management, and transcoding. The Content Monitoring Engine maintains the seamless multimedia service. This engine checks for unpredictable situational and environmental events (called interrupts) and then requests a service reconstruction with respect to the interconnection with the Inference Part. The Content Manager manages the interconnection and relationship between the content and the policy, including digital rights and authentication. This manager controls the Content Management Part and decides on the required novel content service according to the registered interconnection between the digital rights and policies. The Content Decision Engine selects and gathers the adaptive content based on the decisions from the Content Manager. This engine verifies whether or not the authentication information of users, spaces, domains, and devices contains the registration of the requested digital rights. This engine requests the adaptive content and then transmits it to the Transcoding Engine. The Transcoding Engine with SVC transforms the content for use in the available devices.

Our platform is able to predict the adaptive services using pattern generation and protects the content based on the DRM interconnection and the SVC-based transcoding. Furthermore, our platform, with ontology-based situation and content management, provides seamless multimedia services. For effective and robust content management, our platform interconnects with other SPs, devices, and systems with authentication interconnection and SVC using SVC and DRM management.

## V. Performance Evaluation

### 1. Implementation and Testbed Evaluation

Our adaptive evaluation testbed and emulation system were implemented in a real-life situation under a content protective multi-agent service platform. In order to estimate the system's efficiency and robustness, we implemented our platform in both the physical and virtual domain. We developed an emulation system that simulates avatars moving in the service domain and interconnects with the service platforms in the physical environment. We monitored and gathered the activity patterns and service history in the living space and office. We applied the acquired real patterns of the user activity and service status to the emulation system. The emulation system implemented a physical region of 214 m$^2$. We developed the emulation system with the service platform using JAVA SDK 1.4 and the Open Service Gateway initiative (OSGi) framework as shown in Table 1. Our service platform was implemented as a set of running applications, called bundles (Java archives). The emulation system was synchronized with situations from the two types of testbed environments, multi-homes, which covered a total of 214 m$^2$, and an office. The users' activities in the testbed were synchronized with the avatars' activities in the emulation system and modeled as activity patterns by the service platform. Moreover, the proposed platform predicts the services and manages the situations with respect to user mobility, motion patterns, and service conflicts.

Table 1 shows the parameters and values of the implemented service platform based on real patterns and activities. In order to implement MsMu-based heterogeneous environments, our platform consisted of multi-devices, networks, SPs, and systems. Our platform connected to SPs, devices, sensors, and systems using various network infrastructures such as Ethernet, PLC, WLAN, Zigbee, Bluetooth, and HSDPA. The middleware was implemented using OSGi based on Java, and the ontology was based on OntoStudio using F-logic. To implement the emulation system, we analyzed user activity, service requests, service status, and authentication interconnections. The distribution of the user activity is similar to a Gaussian distribution with a mean of 16 activities per hour and a standard deviation of 2.

Table 1. The implemented service platform parameters.

| Category | Parameter | Value and used program |
|---|---|---|
| End entities | Devices | TV, lamp, air conditioner, refrigerator, humidifier, audio, heater, fan, hair drier, computer, washing machine |
| | Sensors | Infrared, ultra sonic, temperature, humidity, Bluetooth sensor, and network cameras |
| | User devices | PDA phone, iPod Touch |
| System | Network infrastructure | Ethernet, PLC, WLAN, Zigbee, Bluetooth, HSDPA |
| | Middleware architecture | Java-based Open Service Gateway initiative (OSGi) |
| | Ontology and policy | OntoStudio based on F-logic |
| | Rule engine | OntoBroker-Ontoprise's Semantic Web Toolkit |
| Event | No. of user activities | 1 to 30 per hour |
| | No. of events | 1 to100 per hour |
| | No. of service requests | 1 to 24 per hour |
| | Sensor response time | 0.05 s to 0.15 s |
| | Average delay of information gathering | 0.18 s to 0.3 s |

We evaluated the reasoning and session management schemes with a multi-resolution agent in highly dynamic service scenarios (16 services with 34 classes, 134 properties, 96 relations, 1,863 instances, 42 rules, 126 queries, up to 100 users, and 60 appliances) to test how the system safely and efficiently classified the user service patterns and updated the ontology and policies [17].

### 2. Performance Analysis

In the MsMu-based heterogeneous environment, user movements lead to numerous events and interrupt according to the environmental and situational context changes and service conflicts. To increase the frequency of user movement from one domain to another, the service platform needs to interconnect with various SPs, CPs, networks, and systems. Moreover, the service platform must solve large conflicts and analyze events in order to predict adaptive multimedia services. The service platform needs to provide protective and seamless services. Therefore, we measured the service response time and

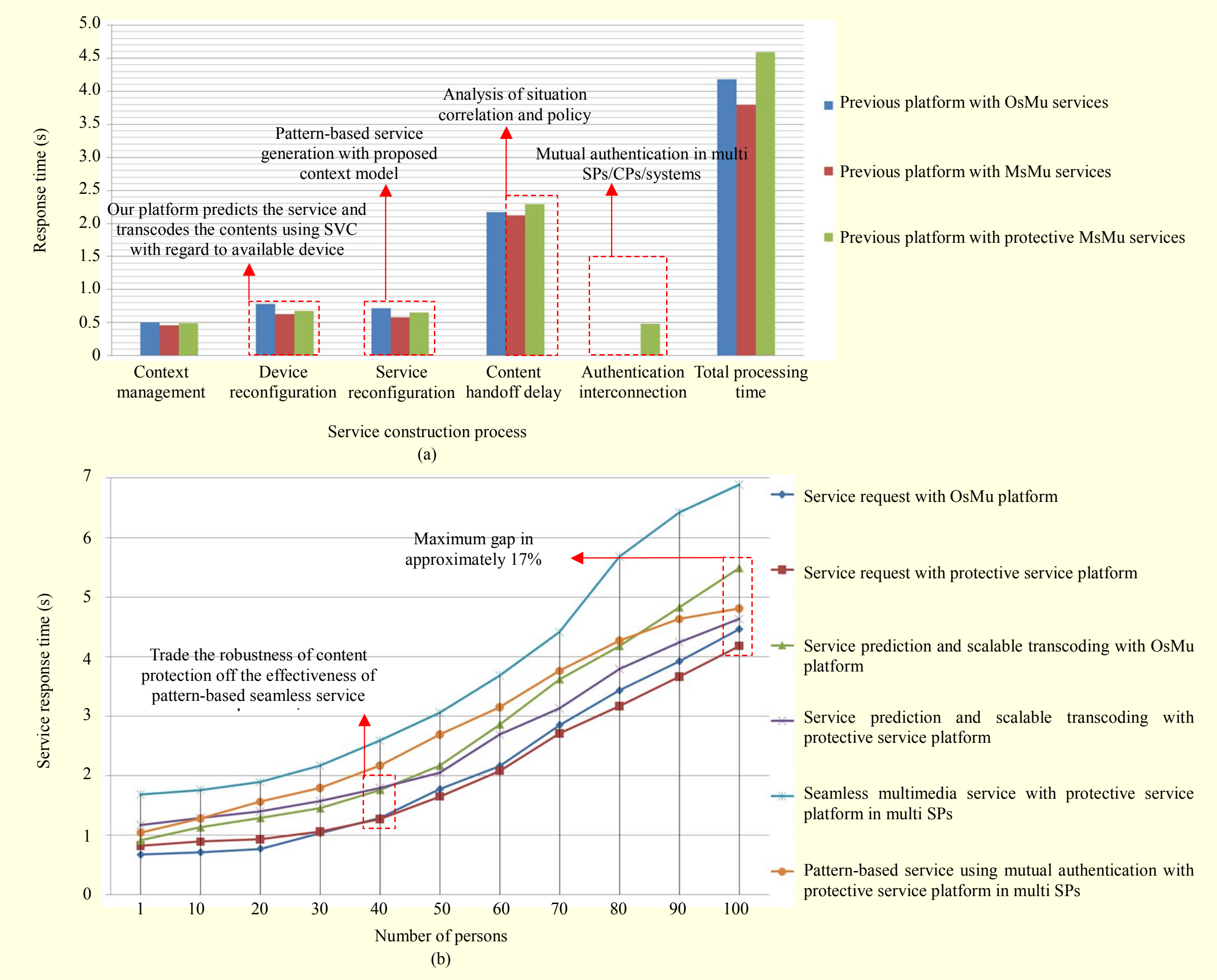

Fig. 4. Performance evaluation result: (a) processing time and (b) service response time versus number of users during OsMu, MsMu, and protective MsMu.

estimated the robustness of the content management.

Figure 4(a) shows the processing delay for three variations of the same situation (OsMu, MsMu, and protective MsMu) and an event in the same environment. Our platform requires more processing delay due to the delay of the correlation verification, pattern analysis, and policy/authentication management compared to a simple MsMu-based multimedia service platform. However, according to pattern generation and service prediction, our platform required less processing time compared to the OsMu service platform. The content protective multi-agent service platform enhances the processing time of the devices and the service reconfiguration with regard to the pattern-based conflict management and the SVC-based effective transcoding. Furthermore, our platform reduces the handoff delay for implementing seamless multimedia services according to the situation correlation analysis and policy management with the DRM and the multi-agent. Our platform provides the robustness of content protection using the authentication interconnection and ontology-based content management in multi-situations (multi-conflicts, interrupts, and events), which are highly complex environments.

As Fig. 4(b) illustrates, the service response time of our platform is more effective in high-complexity environments (multi-users, movements, and conflicts). According to the decrease of the pattern generation time by the correlation analysis and the conflict solving time by the dynamic policy modeling, the service response time decreases. Due to the service prediction and seamless multimedia service, the more the numbers of users and services increase, the less service response time is necessary in our platform as compared with the OsMu platform. As a result of a well-defined hierarchical ontology and situation correlation analysis, our platform can effectively provide pattern-based service prediction. Our platform manages a tradeoff between the robustness of content protection and the effectiveness of pattern-based seamless service in high-complexity situations (40 users). In comparison with the OsMu service platform, our platform helps the system to reduce the service response time and maintains the seamless multimedia services in high-complexity situations.

## VI. Conclusion

New trends in MsMu-based environments, including increasing user movements and demand for multimedia services, will require content protection and seamless services by the network and service convergence in various domains. In addition, an MsMu service platform needs to provide authentication information, situation management, digital rights verification, protective content distribution, and policy management. In order to enhance the robustness of the content management, we designed a content protective multi-agent service platform with an ontology-based context model. Using advanced pattern and situation management, our platform seamlessly connected to various SPs, CPs, and networks. Our platform provided pattern generation and correlation analysis for services, policies, authentication, DRM, and profiles. We implemented the proposed platform using a real testbed and emulation system. Our platform, with content and situation management, provided protective seamless multimedia services with a 17% lower service response time in heterogeneous environments.

We plan to enhance the handoff management for video streaming and an efficient authentication management mechanism. Furthermore, additional work is required to provide secure information, authority, and authentication convergence. For instance, further study is required to determine how to help various devices access the same content with one authority management through multiple access networks while simultaneously providing mobility management and controlling the routing of individual multimedia download flows between different SPs. We are currently working on intelligent devices using lightweight DRM and middleware to enhance the dynamic interconnections and policy management.

## References

[1] V. Ghini, P. Salomoni, and G. Pau, “Always-Best-Served Music Distribution for Nomadic Users over Heterogeneous Networks,” *IEEE Commun. Mag.*, vol. 43, 2005, pp. 69-74.

[2] S.J. Eom and J.H. Paek, “Planning Digital Home Services through an Analysis of Customers’ Acceptance,” *ITcon, Special Issue IT Facility Manag.*, vol. 11, 2006, pp. 697-710.

[3] J.S. Wey, J. Lüken, and J. Heiles, “Standardization Activities for IPTV Set-Top Box Remote Management,” *IEEE Internet Comput.*, vol. 13, 2009, pp. 32-39.

[4] S. Park and S.H. Jeong, “Mobile IPTV: Approaches, Challenges, Standards, and QoS Support,” *IEEE Internet Comput.*, vol. 13, 2009, pp. 23-31.

[5] L. Xiaorong, B. Veeravalli, and L. Hailong, “Multimedia Service Provisioning and Personalization on Grid-Based Infrastructures: Now and the Future,” *IEEE Multimedia*, vol. 16, 2009, pp. 36-45.

[6] “Information Technology - Multimedia Framework - Part 7: Digital Item Adaptation,” ISO/IEC 21000-7, 2004.

[7] A. Roy, S.K. Das, and K. Basu, “A Predictive Framework for Location-Aware Resource Management in Smart Homes,” *IEEE Trans. Mobile Comput.*, vol. 6, 2007, pp. 1270-1283.

[8] T. Gu, H.K. Pung, and D.Q. Zhang, “A Service-Oriented Middleware for Building Context-Aware Services,” *J. Network Comput. Appl.*, vol. 28, 2005, pp. 1-18.

[9] S. Loreto et al., “Service Broker Achitecture: Location Business Case and Mashups - Topics in Design and Implementation,” *IEEE Commun. Mag.*, vol. 47, 2009, pp. 97-103.

[10] S. Bo, T. Wai-Tian, and F. Huve, “Dynamic Video Transcoding in Mobile Environments,” *IEEE Multimedia*, vol. 15, 2008, pp. 42-51.

[11] V. Torres et al., “Open DRM and the Future of Media,” *IEEE Multimedia*, vol. 15, 2008, pp. 28-36.

[12] A. Carreras et al., “A Platform for Context-Aware and Digital Rights Management-Enabled Content Adaptation,” *IEEE Multimedia*, vol. 17, Apr. 2010, pp. 74-89.

[13] H. van Kranenburg et al., “A Context Management Framework for Supporting Context-Aware Distributed Applications,” *IEEE Commun. Mag.*, vol. 44, 2006, pp. 67-74.

[14] R. Roman, J. Lopez, and S. Gritzalis, “Situation Awareness Mechanisms for Wireless Sensor Networks,” *IEEE Commun. Mag.*, vol. 46, 2008, pp. 102-107.

[15] M. Bertini et al., “Dynamic Pictorially Enriched Ontologies for Digital Video Libraries,” *IEEE Multimedia*, vol. 16, 2009, pp. 42-51.

[16] M. Kifer, G. Lausen, and J. Wu, “Logical Foundations of Object-Oriented and Frame-Based Languages,” *J. ACM*, vol. 42, 1995, pp. 741-843.

[17] Y. Uhm et al., “Service Reconstruction for Improving Performance Using Classified Service Pattern and a Session Manager-Based Architecture in Smart Homes,” *5th IEEE Consum. Commun. Networking Conf.*, 2008, pp. 326-330.

**Yoonsik Uhm** received the BS and MS in electrical and electronics engineering from Chung-Ang University, Seoul, Korea, in 2004 and 2006, respectively. He is currently a PhD candidate at Chung-Ang University. His current research interests include ubiquitous computing, location-aware service management, context-aware middleware, and network security.

**Zion Hwang** received the BS in information systems and the MS in electrical and electronics engineering from Chung-Ang University, Seoul, Korea, in 2003 and 2005, respectively. She is currently a PhD candidate at Chung-Ang University. Her current research interests include ubiquitous computing, location-aware service management, context-aware middleware, and network security.

**Minsoo Lee** received his BS, MS, and PhD in the School of Electrical and Electronics Engineering from the Chung-Ang University, Seoul, Korea, in 2001, 2003, and 2007, respectively. He has been a research professor at Chung-Ang University Home Network Research Center (HNRC)-Information Technology Research Center (ITRC) which is supported by the Ministry of Knowledge Economy (MKE), Korea. From 2007 to 2009, he was a research scientist in the Department of Electrical and Computer Engineering at University of California Davis. His major research interests are in intelligent networking, location-aware computing, ubiquitous computing, home networks, and mobile network security.

**Jaehoon Nah** received the BS and MS degrees in computer engineering in 1985 and 1987 from Chung-Ang University, Seoul, Korea, and the PhD degree in information engineering from Hankook University of Foreign School in 2005, Yongin, Korea. He has worked with ETRI, Korea, since February 1987. He is the principal engineer and the project manager of IPTV security. He is interested in mobile IP security, P2P security, and IPTV security.

**Hwangjun Song** received the BS and MS from the Department of Control and Instrumentation (EE), Seoul National University, Korea, in 1990 and 1992, respectively, and the PhD in electrical engineering systems, University of Southern California, Los Angeles, CA, USA in 1999. From 1995 to 1999, he was a research assistant in Signal and Image Processing Institute (SIPI) and Integrated Media Systems Center (IMSC), Univ. of Southern California. From 2000 to 2005, he was an assistant professor/vice dean of admission affairs at Hongik University, Seoul, Korea. Since February 2005, he has been with Department of Computer Science and Engineering, Pohang University of Science and Technology (POSTECH), Korea. He received the Haedong Best Paper Award from the Korean Institute of Communication Science in 2005. His research interests include multimedia signal processing and communication, image/video compression, digital signal processing, network protocols necessary to implement functional image/video applications, control systems, and fuzzy-neural systems.

**Sehyun Park** received the BS and MS degrees in electronics engineering from Chung-Ang University, Seoul, Korea, in 1986 and 1988, respectively, and the PhD from the University of Massachusetts, Amherst in 1998. From 1988 to 1999, he was a member of the senior research staff at ETRI, Korea. He is currently a professor of electrical and electronics engineering at Chung-Ang University, where he established the Ubiquitous Computing and Cipher Internet Laboratory. He is the head of Chung-Ang University Home Network Research Center (HNRC)-Information Technology Research Center (ITRC) supported by the Ministry of Knowledge Economy (MKE), Korea. His major research interests include home networks, ubiquitous computing, and network security.