Journal of Universal Computer Science, vol. 15, no. 5 (2009), 1065-1080
submitted: 1/8/08, accepted: 28/2/09, appeared: 1/3/09 © J.UCS

USF-PAS: Study on Core Security Technologies for Ubiquitous Security Framework

Jong Hyuk Park
(Department of Computer Science and Engineering, Kyungnam University
Masan, Korea
jhpark1@kyungnam.ac.kr)

Abstract: Ubi-Com has emerged as an exciting new paradigm to provide intelligent computig and communications at anytime and anywhere. But, In order to take the advantages of such services, it is important that intelligent security framework be suitable for Ubi-Com. In this paper, we propose privacy and access control scheme by surveillance which is one of core security technologies for ubiquitous hybrid intelligent security framework. In this scheme, the device information and the signature information can be added to the image data obtained by the image capturing device to maintain security of the image data and use the image data as digital proof when a specific event is generated.

Keywords: Ubi-com, intelligent security framework, privacy, access control, surveillance
Categories: H.4.3, H.5.1, J.7

1 Introduction

Ubi-Com (UC) has emerged as an exciting new paradigm that includes pervasive, grid, and P2P computing to provide intelligent computing and communications at anytime and anywhere. What is called, as UC environments are expanding into our real lives and the majority of security applications are designed and developed considering the ubiquitousness, the ubiquitous service should be provided anywhere, anytime and with any device. But, In order to take the advantages of such services, it is important that intelligent security framework be suitable for UC [Newton, 05] [Cavallaro, 05] [Wickramasuriya, 05].

Nowadays most of the services are based on the identity information from the implemented authentication application which is supposed to be basically trusted. There are a number of authentication mechanisms developed and they are implemented in various applications having heterogeneous features and environments. In the real services, each entity which is going to use the service is likely to move from one space to other space. Each space may optionally adopt an authentication mechanism for identifying the entity. But it depends on the application. When some entity moves to a specific space where there is no applied authentication mechanism, but the provided service needs the identity information about the entity, then we have no method to provide the service without it.

We define a USF as Ubiquitous hybrid intelligent Security Framework (USF) to provide us with secure and intelligent services including core technologies - WSN / RFID, context awareness, information fusion, authentication, authorization & access control, surveillance , and so on [Jonghyuk, 08] (Refer to figure 1).

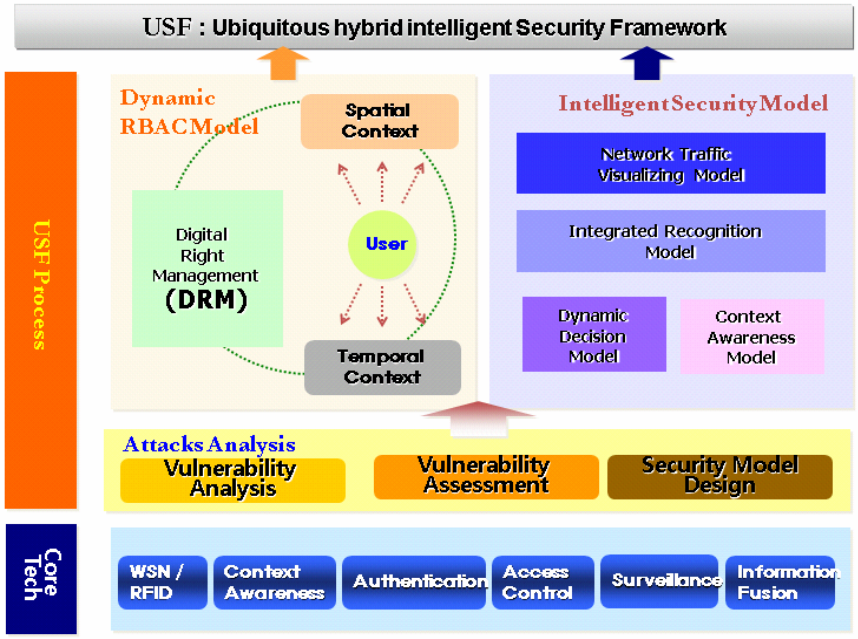

Figure 1: Ubiquitous hybrid intelligent Security Framework (USF)

Surveillance ensures that we monitor and keep track of the interesting object, which applies to a lot of security deployment including home network, USN, etc. Home network is a new IT technology environment for making an offer of convenient, safe, pleasant, and blessed lives to people, making it possible to be provided with a variety of home network services by constructing home network infrastructure regardless of devices, time, and places. This can be done by connecting home devices based on various kinds of communicating networks, such as mobile communication, Internet, and sensor network [Zhang, 05. Recently, the home network is expanding into ubiquitous computing environment, and boundaries among networks and systems tend to be obscure. However, surveillance systems are exposed to various cyber attacks of Internet, involves hacking, malicious codes, worms, viruses, DoS attacks and eavesdropping since it is connected to Internet and consists of heterogeneous network protocols [Sekiguchi, 06].

Sensor-data fusion from multiple cameras is an important problem with many potential applications. The work in multisource fusion can be divided into two categories based on camera configurations: spatially nonoverlapping and spatially overlapping. The study of [Stauffer, 00] attempts to fuse data from several nonoverlapping cameras using a Bayesian reasoning approach. Since there might be significant gaps between the fields of view of the cameras, the precision in prediction may suffer. Most fusion algorithms assume an overlapping camera configuration and concentrate on fusing local coordinate frames of multiple cameras into one global coordinate system. The DETER project [Koshimizu, 06] also uses an overlapping

camera configuration. The homography between images from two cameras is computed, the images are mosaiced together to perform seamless tracking, and all data processing is then performed in the synthesized image plane. In this paper,we use a two-level hierarchy of Kalman filters for trajectory tracking and data fusion from multiple cameras. The advantage of our formulation is that it enables both bottom-up fusion and top-down guidance and hence is robust even with partial occlusion. The Kalman filter is an important theoretical development for data smoothing and prediction. The traditional Kalman filter is a linear algorithm that operates under a predictioncorrection paradigm. The quantities of a system to be estimated are summarized in an internal state vector, which is constrained by the observation of the system' s external behavior. The prediction mechanism is used for propagating the system' s internal state over time, and the correction mechanism is for fine-tuning the state propagation with external observations [Elisa, 02].

The Kalman filter and its variants are powerful tools for tracking inertial systems. Generally speaking, the standard Kalman filter performs satisfactorily for tracking the position of a moving object. However, for tracking the orientation of an object, where the governing equations in state propagation and observation may be nonlinear, the extended Kalman filter must be used [Yoichi, 05] [Pavlidis, 01].

In this paper, we are interested in summarizing the trajectory of a vehicle, and hence only the position, not the orientation, of a vehicle is needed. We have thus employed the traditional Kalman filter for the efficient tracking purpose. In addition to the Kalman filter, the hidden Markov model (HMM)has been used for object tracking. Both the Kalman filter and HMM can be used to estimate the internal states of a system. However, HMM is not an attractive online tracking method due to its high computational intensity with respect to the number of states. For tracking objects, where the number of possible locations (number of states) of the tracked objects is theoretically infinite, the Kalman filter is the popular choice [Morellas, 01]

The remainder of this paper is organized as follows. In section 2, we describe security requirements in surveillance for Ubi-Com. In section 3, we discuss proposed USF-PAS including architecture and flows. We describe use case scenario based on USF-PAS in section 4. We analyze security and efficiency of USF-PAS in section 5. inally, we make conclusions in Section 6.

2 Security Requirements in Surveillance for Ubi-Com

System-specialized security requirements contain policy used for authentication and authorization, as well as other kinds of security enforcement. Since there are a variety of requirements on surveillance system security and enforcement points, legacy security modules can be easily deployed without complicated works to integrate them, each of them performs its' own protection job. But, this results in making the surveillance system more complicated and messy to manage. Also, because of inconsistency among the separated security modules, it may produce unexpected security holes. So, we need a specific way to enforce the security policies, and manage inconsistency among them. A surveillance device is located at the board of each space and filters accesses based on rules with the help of security modules, performing authentication, authorization, and security policy.

- ***Authentication and Privacy***: Authentication is supposed to be a most fundamental function in all security systems and a first step into other security modules or services. The purpose of authentication is to identify an entity trying to access and verify the identity information by means of a trustable mechanism. The general authentication mechanisms include ID/password-based authentication mechanism, Certificate-based authentication mechanism, authentication mechanism using biometric information. The surveillance device should provide above authentication mechanisms. A user may just choose one mechanism that he or she prefers. But, an application server is actually responsible for authenticating users and devices in most surveillance system deployed.
- ***Authorization and Access Control***: The purpose of authorization is to control access and restrict privilege and accessing right to resource even though the entity has been authenticated successfully. There are a few authorization mechanisms that are generally used: DAC (Discretionary Access Control), MAC (Mandatory Access Control), and RBAC (Role-based Access Control). The RBAC mechanism for authorizing surveillance system is suitable and guarantees extensibility and flexibility. RBAC mechanism uses role components between subjects and resources, making an offer of indirect authorization relationships.
- ***Security Policy Manger:*** Security policy manager should generate and manage the security policy specialized for surveillance system which includes authentication policy, authorization policy and other types of security policy. Considering the features of surveillance system, it must be enough easy for non IT-familiar user to use.
- ***Other Security Polices:*** Security policy should be a set of single rule consisting of condition and action. Whenever a condition is satisfied, action is performed, where the key issue is how to construct condition. Elements to be contained in condition are time (date, day, duration), event (sensor, user-triggering, state), and log(statistics). In addition, relationships (interaction, union) among above elements and support recursive structure should be defined. Building complex conditions should be possible. Time and event are the basic elements of condition and can be generally used. On the other hand, log-based condition controls access by statistics information.

3 USF-PAS

[Assumptions]

There are some assumptions for USF-PAS in this paper ;
- ✓ Surveillance camera is based on Kalman filter and HMM.
- ✓ Each space is monitored by at least single surveillance device.
- ✓ Each surveillance device has functions for collaboration with other surveillance devices for relaying entity's identity information.
- ✓ Legacy authentication applications may communicate with other surveillance device s for send/receiving identity information

3.1 USF-PAS Architecture

USF-PAS includes three main components – image capturing device, surveillance device, surveillance management server (Refer to figure 2).

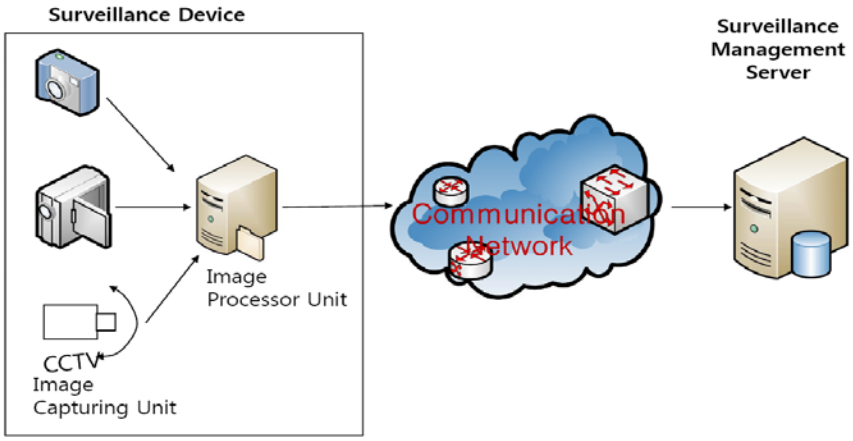

Figure 2: USF-PAS Architecture

An image capturing device captures an image and converts the captured image into image data,. A surveillance device receives and stores the image data, and a surveillance management server provides various application services using the image data stored in the surveillance device. The image capturing device includes an imaging capturing unit for converting an optical image formed through a lens into image data and an image processor for receiving the image data and adding signature information or device information of the image capturing unit to the image data.

The image capturing unit includes a lens for condensing light and a charge-coupled device (CCD) for converting the light condensed by the lens into image data, recognizes an object through the lens and images the recognized object to generate an optical image. This optical image can be converted into image data through a CCD sensor. The image data generated by the image capturing unit is transmitted to the image processor.

3.2 USF-PAS Flows

In this sub-section, we discuss three kinds of flows; device-side, server-side, and whole flow.

3.2.1 Flow of device-side at USF-PAS

The image processor receives the image data from the image capturing unit, processes the image data and embeds signature information in the image data. The image processor can be constructed as additional hardware or included in the image capturing unit. The image processor adds at least one of information on the image capturing unit and signature information to the image data transmitted from the image

capturing unit. By doing so, the image data can be protected from arbitrary access and control. The signature information can be added to the image data at regular intervals. The surveillance device stores the image data to which the information on the image capturing unit or the signature information has been added by the image processor. The surveillance device includes a storage unit capable of storing the image data having the information on the image capturing unit or the signature information added thereto and can be connected to a communication network such as the Internet or a mobile communication network to transmit the image data processed by the image processor to a communication terminal. That is, the image data processed by the image processor can be stored in the surveillance device and applied to the surveillance management server through the communication network such as the Internet (Refer to Figure 3).

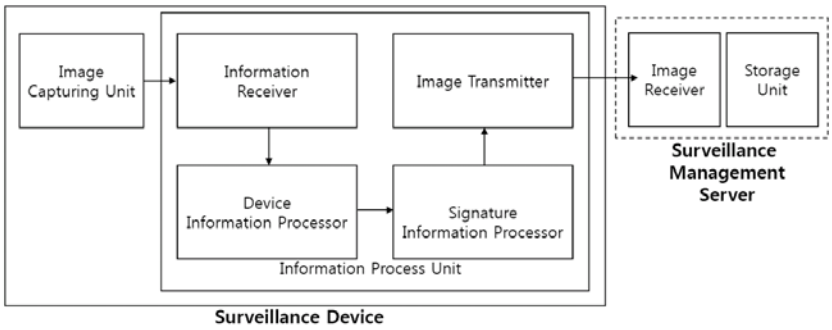

Figure 3: Flow of USF-PAS (Device-side Signature)

3.2.2 Flow of server-side at USF-PAS

The surveillance management server provides a variety of application services to a mobile terminal of a communication service subscriber using the communication network at the request of the communication service subscriber.

In another embodiment, the surveillance device can add the signature information or the information on the image capturing unit to the image data captured by the image capturing unit. In this case, the image processor transmits the image data and the information on the image capturing unit received from the image capturing unit to the surveillance device, and the surveillance device adds the information on the image capturing unit or the signature information to the image data transmitted from the image processor. The image data processed by the surveillance device can be applied to the surveillance management server through the communication network such as the Internet (Refer to Figure 4).

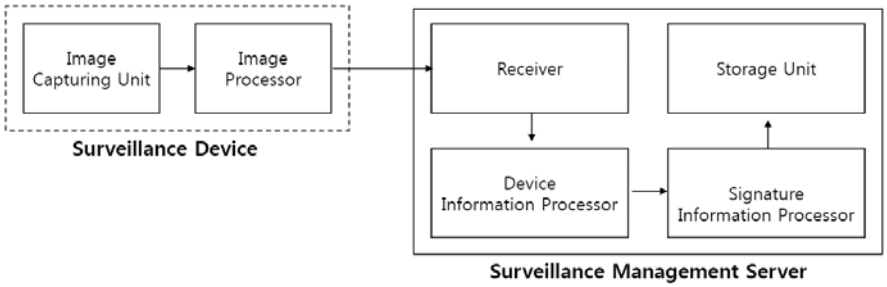

Figure 4: Flow of USF-PAS (server-side Signature)

The information receiver receives the image data generated by the image capturing unit and transmits the information to the device information processor. The information on the image capturing unit can include an identifier given to the image capturing unit or information on the place and time at which the image capturing unit obtains the image data. When the image capturing unit is a communication terminal, the information on the image capturing unit can include an identification number given to the communication terminal.

The device information processor adds the information on the image capturing unit to the image data transmitted from the information receiver. The image data can be used as digital proof of a specific event when the place and time at which the image data is captured is added thereto and the source of the image data can be easily detected when the identification number of the image capturing unit is added thereto. The device information processor transmits the image data having the information on the image capturing unit added thereto to the signature information processor.

The signature information processor can embed signature information including a predetermined encryption key in the image data transmitted from the device information processor. According to an embodiment, the signature information processor can add public key based signature information, symmetric key based signature information or public key and symmetric key based signature information to the image data.

When the signature information is added to the image data, the image data can be accessed only using a predetermined decryption key. Accordingly, the possibility that the image data is exposed to hacking or illegal copy according to arbitrary access can be reduced when the signature information is added to the image data. The surveillance management server that provides the image data to communication subscribers can provide the decryption key to only an authenticated communication subscriber through a text message to maintain security of the image data.

The image transmitter transmits the image data received from the signature information processor to the image information server. The image receiver receives the image data from the image transmitter. The storage unit stores the image data transmitted from the image receiver. The image data transmitted from the image receiver has at least one of the information on the image capturing unit and the signature information added thereto.

The surveillance device can determine whether the decryption key transmitted from the application server corresponds to the encryption key embedded in the image

data, extract the image data stored in the storage unit and transmit the image data to the surveillance management server when the surveillance management server requests the surveillance device to transmit the image data through the communication network.

The receiver included in the surveillance device receives the image data and the information on the image capturing unit transmitted from the image processor and the device information processor receives the image data and the information on the image capturing unit from the receiver and embeds the information on the image capturing unit in the image data. The signature information processor adds predetermined signature information to the image data having the information on the image capturing unit added thereto and the storage unit stores the image data including the signature information.

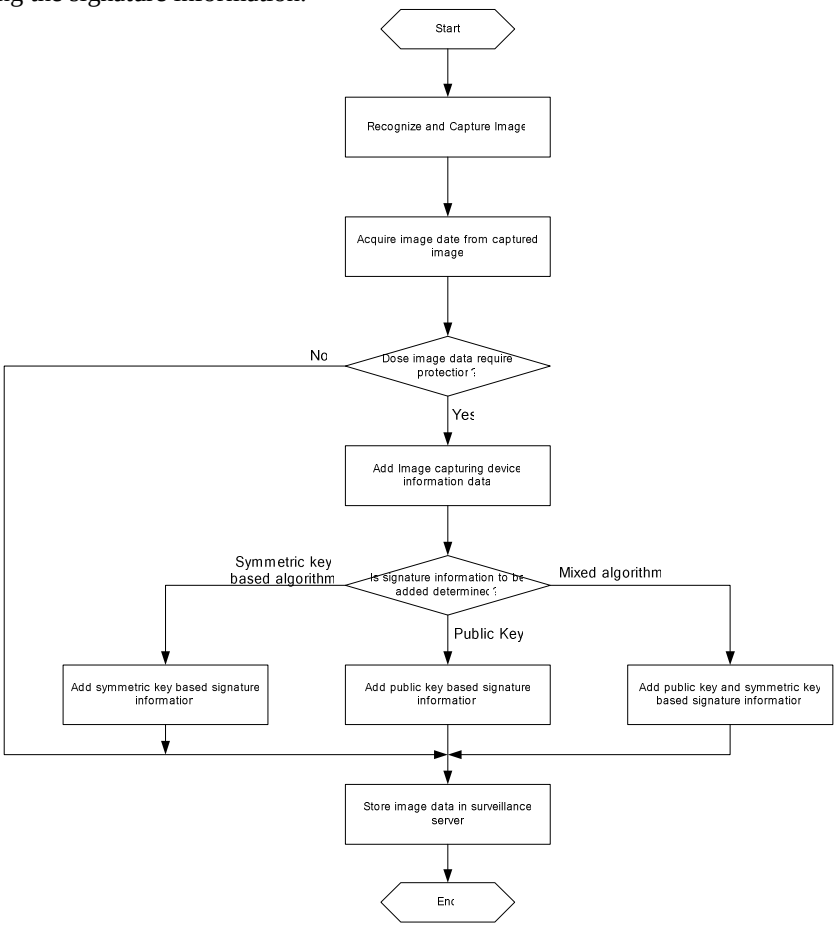

Figure 5: Whole flow of USF-PAS

The receiver receives the image data and the information on the image capturing unit from the image processor. The device information processor embeds the

information on the image capturing unit in the image data and transmits the image data to the signature information processor. The information on the image capturing unit depends on the type of the image capturing unit. The signature information processor is the same at the device-side signature.

3.2.3 Whole flow of USF-PAS

The whole flow of USF-PAS is composed of five steps as follows;

Step 1: The image capturing unit included in the image capturing device recognizes an image and captures the image.

Step 2 : The image capturing unit acquires image data from the image captured. The image data can include meta data and main data. The main data can include information on the captured image and the meta data can include information that explains the main data.

Step 3: When the image data is obtained, the image capturing device determines whether it is required to protect the image data. It can be determined whether the image data requires protection according to the type of the image capturing device or setting up by a user who captures the image.

3-1. When it is determined that the image data does not require protection, the image data is transmitted to the surveillance device without undergoing additional image data processing.

3-2. When it is determined that the image data requires protection, information on the image capturing device is added to the image data.

Step 4: When the information on the image capturing device is embedded in the image data, the type of signature information to be added to the image data is determined. The signature information can be generated according to symmetric key based algorithm, public key based algorithm or public key and symmetric key based algorithm and embedded in the image data.

4-1. When the signature information according to the symmetric key based algorithm is embedded in the image data, safe authentication is difficult to perform and an additional secret key is required although encryption speed is high due to low algorithm complexity. Accordingly, it is desirable to use the symmetric key based algorithm in consideration of data processing load applied to the image processor in the case where the image processor embeds the signature information in the image data.

4-2. When the signature information according to the public key based algorithm is embedded in the image data, safe authentication can be achieved and transmission of an additional secret key is not needed in spite of high algorithm complexity. Accordingly, it is desirable to use the public key based algorithm using the data processing speed and capacity of the surveillance device, which are greater than those of the image processor when the surveillance device embeds the signature information in the image data.

4-3. When the signature information according to the public key and symmetric key mixed algorithm is embedded, a public key is generated using the public key

based algorithm first, and then a data encryption key with respect to the public key based algorithm is generated using the symmetric key based algorithm. Although the public key and symmetric key mixed algorithm can secure safe authentication as compared to the cases where the public key based algorithm and symmetric key based algorithm are used, it is desirable to use the mixed algorithm when the surveillance device can embed the signature information in the image data because algorithm complexity is high.

Step 5: When the surveillance management server requests the surveillance device to transmit the image data through the communication network, the surveillance device can compare the decryption key transmitted from the surveillance management server with the encryption key included in the image data stored in the surveillance device to determine whether the requested image data is transmitted.

While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from the spirit and scope of the present invention as defined by the following claims. According to the present invention, image data can be protected from security infringement such as illegal copy and arbitrary transmission. Furthermore, information on the place and time at which an image is captured is added to the image data such that the image data can be used as digital proof.

4 Use case scenario based on USF-PAS

In the ubiquitous environments, each entity is likely to traverse multiple spaces, and each space implements its own authentication mechanism. It means that if an entity is going to use the service provided within a space, then it should be identified by the authentication mechanism implemented in the space. This results in the increase of user interventions, the decrease of performance and the increase of service time. To make matters worse, every space is not guaranteed by authentication mechanism. Some space adopt trusted authentication mechanisms, but others not. Therefore, we couldn’t guarantee that an entity can be authenticated in every space. Figure 6 shows the ubiquitous environment for moving entity of multiple spaces [Geon, 08].

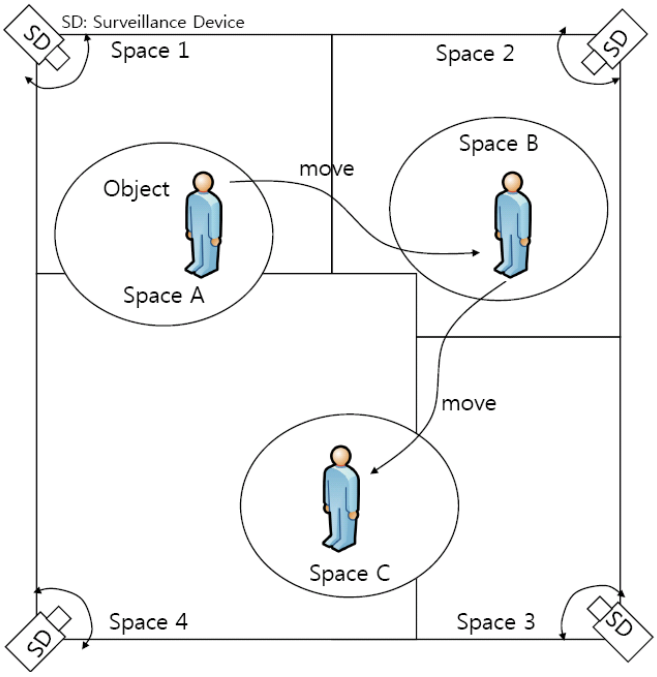

Figure 6: Entity's movement through multiple spaces in ubiquitous environment

Each space is categorized into two types: authenticated space, and not authenticated space. The authenticated space ensures that it is protected by a corresponding authentication mechanism implemented, while the not-authenticated space doesn't support any authentication mechanism which is supposed be secure.

There are a number services based on identity information such as authentication and access control, VOD services, ubiquitous health care service, object monitoring service, home network services, and so on. The above services are based on the identity and provide the differentiated service according the identity. The identity is one of the most important factors in the recent service areas, especially regarding ubiquitousness.

4.1.1 Collaboration for relaying identity

In order to provide the identity-based services, the identity information of the entity should be useful in every space. To make it possible, the not-authenticated space should support some functions for relaying the identity.

Currently, there are many researches on intelligent surveillance device and corresponding technologies. The technology on intelligent surveillance device includes object recognition and tracing. Strictly speaking, the object recognition and object tracing are not the scope of authentication. They are just for recognition. But it can be used in the new model.

Fortunately there are a number of researches on surveillance system using surveillance devices that are expected to cover all future spaces. This monitoring

system is designed for use in various locations and for simultaneous searches from different locations and offers reduced operating costs [Deok-Gyu , 06].

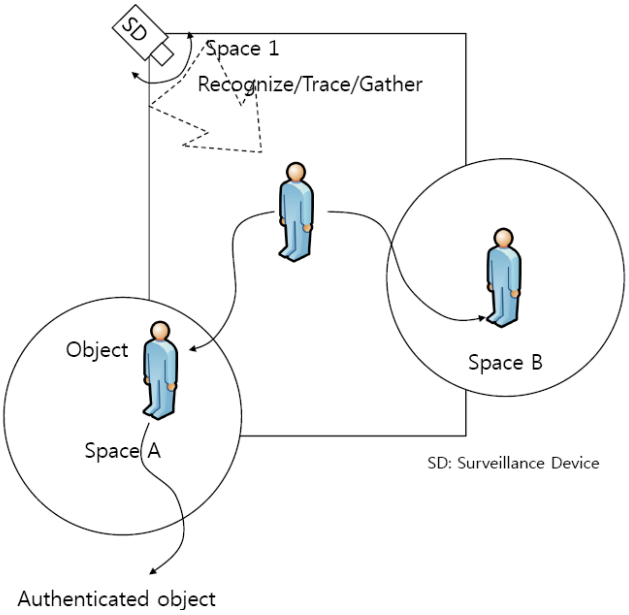

Figure 7: Identity relay using surveillance device

Figure 7 describes the overview of relaying identity using surveillance device. The space A and the space B provide their own authentication mechanism respectively. On the other hand, the space 1 doesn't support any authentication mechanism. An intelligent surveillance device is just implemented.

This example shows the hand-overs while moving from space A to space B. When the entity authenticated in space A moves toward the space B and enters into the scope of space 1, the surveillance device which is responsible for space 1 recognizes the new entrance. At this moment, the authentication application of space A transmits the entity's identity-related information to the surveillance device. The first hand-over occurs between space A and space 1.

After receiving identity-related information, the surveillance device starts tracing the entity. The procedure of object tracing may occur among multiple spaces of surveillance devices depending on application. When it moves to space B, the second hand-over occurs. During the latter hand-over, the surveillance device relays the entity's identity-related information to the authentication application of space B.

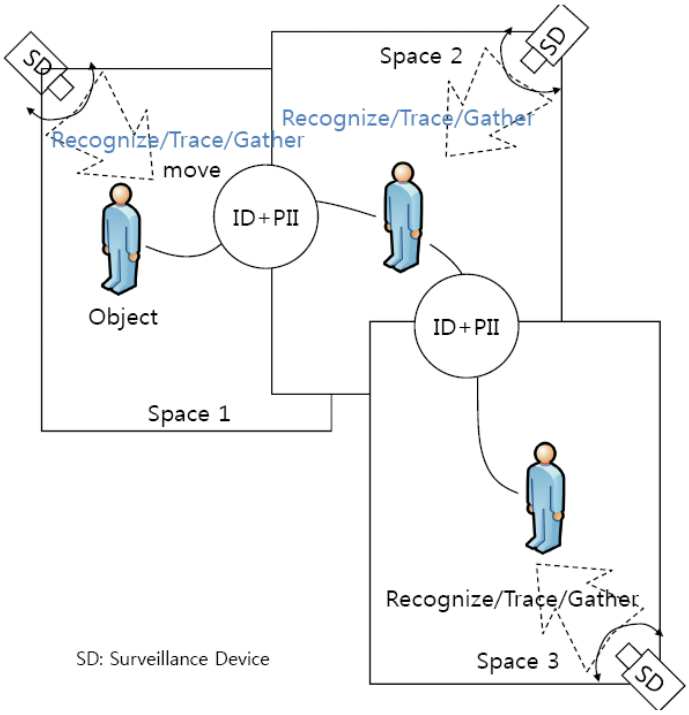

Figure 8: Hand-overs through multiple not-authenticated spaces

The PII stands for Physically Identifiable Information. In the surveillance system using surveillance device, there is no explicit method to authenticate an entity. Of course, it is possible to identify an entity according to the application environment. But in general applications, we couldn't guarantee it.

In the surveillance system, the information about physical appearance of an entity is generally used. For relaying identity information, each intelligent surveillance device performs transmitting/receiving the corresponding information, tracing entity. The information exchanged between surveillance devices consists of ID and PII. ID was produced by the authentication application of the resource and PII was from the previous surveillance device. The information contained in the PII are entity type (person, car, object, …), physical appearance (physical size, color, shape, cloth, hair, number), and location.

5 Analysis of USF-PAS

In this section, the analysis for security and efficiency of USF-PAS is discussed. For the case of security, we analyze USF-PAS based on the security requirements presented in section 2. In addition, we compare two cases - the applied security requirements and non- the applied security requirements from the aspect of the efficiency of USF-PAS.

First, we discuss security of USF-PAS considering security requirements as follows;

Authentication and Privacy: In this system, we assume that the subject of authentication is an application server. The application server is responsible for authenticating users and devices passing through it, while the surveillance device acts as a bridge between an accessing entity and the application server. The application server authenticates accesses from outdoor entities and just notifies the authenticated identity information to the surveillance device. As a result, a user can USF-PAS through the surveillance device and access the object without additional authentication process since the surveillance device trusts the surveillance manager and the notified identity information from it. It seems to be reasonable to store biometric information in surveillance device since a surveillance manager is open to public network and just managed by service provider. When the authentication server is going to authenticate an entity using biometric information, the surveillance device replaces authentication instead of it. In case of the surveillance device successfully authenticates an indoor entity, it performs the second authentication process with the application server in place of the entity, resulting in no additional logon.

Authorization and Access Control: When the authorization module receives an access request, it retrieves corresponding data from the authorization database and decides whether to permit or not. Authorization information is set by the security manager somewhere within the space, which is assumed to be trusted and the channel between them has to be secure using legacy secure mechanisms such as TLS and IPsec.

Security Policy Manger: In our USF-PAS, we use a Drag-and-Drop mechanism to establish the security policy, so anyone can handle it if he has been authenticated successfully.

Second, we explain efficiency of USF-PAC. We verify efficiency at the number of selection by comparing case of non-applied security requirements (A) with case of applied security requirements (B) when we use surveillance system of USF-PAS. As the following at the simulation graph [Fig. 9], case A got 10 as the number of selection in surveillance system. But, case B got the numbers less than case A. Generally, if most systems will consider security factors, efficiency of performance will be decreased. These values are not bad values in case B considering security requirements.

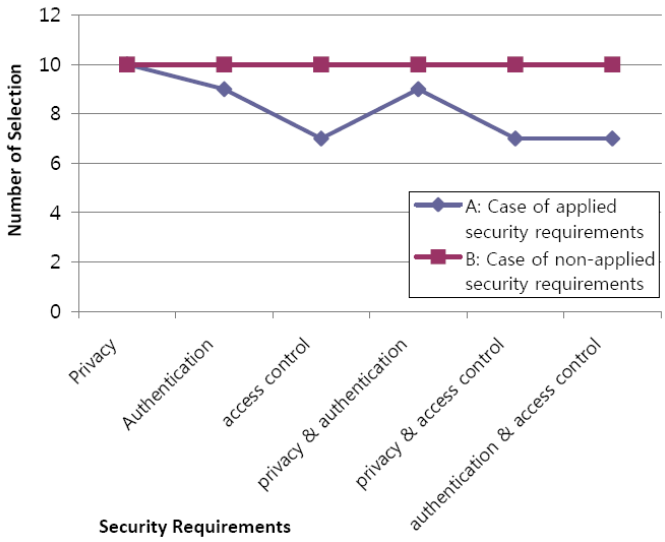

Figure 9: Hand-overs through multiple not-authenticated spaces

6 Conclusions

In the ubiquitous computing environments, there are so many heterogeneous applications around the physical world. Each application implements its own authentication mechanism depending on the purpose of service and working environment. Within the real ubiquitous world, a user would be able to use ubiquitous services without any intervention by authentication applications for identifying himself. Namely, it is recommended that authenticating process is performed without one's knowledge. However, the existing authentication mechanisms almost request user's intervention and help. So, in this paper we propose a new model for making it possible that a user can access any distributed service protected by heterogeneous applications by being authenticated only once at the initial stage. The centralized UIDM manages the object identifier that is universally unique. In addition, we proposed privacy and access control scheme for ubiquitous hybrid intelligent security framework using surveillance system based on Kalman filter and HMM for the first time.

Fortunately, spaces that are not covered by authentication applications can be managed by surveillance system using surveillance device in the near future. It means that an entity' ID can be relayed to the next application following the movement of the entity.

Acknowledgements

This work was supported by Kyungnam University Foundation Grant (Basic Research Promotion Fund), 2008.

References

[Cavallaro, 05] Cavallaro, A., Steiger, O., Ebrahimi, T.: Semantic Video Analysis for Adaptive Content Delivery and Automatic Description. IEEE Trans. Circuits and Systems Video Technology 15(10), 1200–1209 (2005)

[Deok-Gyu , 06] Deok-Gyu Lee, Seo-Il Kang, Dae-Hee Seo, Im-Yeong Lee: Authentication for Single/Multi Domain in Ubiquitous Computing Using Attribute Certification. ICCSA 2006, 326-335 (2006)

[Elisa , 02] Elisa Bertino, Moustafa Hammad, Walid Aref, and Ahmed Elmagarmid. An access control model for video database systems. In Conference on Information and Knowledge Management (2002)

[Geon, 08] Geon Woo Kim, Deok-Gyu Lee, Jong Wook Han, Sang Wook Kim, "Intelligent Security for Inter-space Surveillance Applications," MUE 2008: 419-422 (2008)

[Jonghyuk, 08] Jonghyuk Park, "Study on Ubiquitous Hybrid Intelligent Security Framework Model", Technical Report, Jan., 2008.

[Koshimizu, 06] Koshimizu, T., Toriyama, T., Babaguchi, N.: Factors on the Sense of Privacy in Video Surveillance. In: Proc. Workshop on Capture, Archival and Retreival of Personal Experiences, 35–43 (2006)

[Morellas, 01] Morellas V, Pavlidis I, Tsiamyrtzis P, Harp S, Urban surveillance systems: from the laboratory to the commercial world. Proc IEEE 89(10),1478–1497, (2001)

[Newton, 05] Newton, E.M., Sweeny, L., Malin, B.: Preserving Privacy by De-Identifying Face Images. IEEE Trans. Knowledge and Data Engineering 17(2), 232–243 (2005)

[Pavlidis, 01] Pavlidis I, Morellas V, Two examples of indoor and outdoor surveillance systems: motivation, design, and testing. In: Proc. 2nd European workshop on advanced video-based surveillance (2001)

[Sekiguchi, 06] Sekiguchi, T., Kato, H.: Proposal and Evaluation of Video-based Privacy Assuring System Based on the Relationship between Observers and Subjects. IPSJ Trans. on Computer Security Proping up Ubiquitous Society 47(8), 2660–2668 (2006)

[Stauffer, 00] Stauffer, C., Grimson,W.E.L.: Learning Patterns of Activity using Real-Time Tracking. IEEE Trans. Pattern Analysis and Machine Intelligence 22, 747–757 (2000)

[Wickramasuriya, 05] Wickramasuriya, J., Alhazzazi, M., Datt, M., Mehrotra, S., Venkatasubramanian, N.: Privacy-Protecting Video Surveillance. In: Proc. SPIE International Symposium on Electronic Imaging, vol. 5671, 64–75 (2005)

[Yoichi, 05] Yoichi, HAGIWARA, Tadasuke, FURUYA, Takeshi, SAKURADA, Takafumi, SAITO, "Surveillance camera system with a wired and wireless network", IASTED International Conference on Internet and Multimedia Systems and Applications (IMSA) (2005)

[Zhang, 05] Zhang, W., Cheung, S.S., Chen, M.: Hiding Privacy Information in Video Surveillance System. In: ICIP2005. Proc. IEEE International Conference on Image Processing, 868–871 (2005)