早稲田大学審査学位論文

博士（人間科学）

HUC-HISF: A Hybrid Intelligent Security Framework for Human-centric Ubiquitous Computing

人間中心のユビキタスコンピューティングのためのハイブリッド・インテリジェント・セキュリティ・フレームワーク

２０１２年１月

早稲田大学大学院　人間科学研究科

朴　鍾　爀

Park, Jong Hyuk

Abstract

A new computing paradigm such as ubiquitous computing is coming due to computing powers and rapid progress for networks. Such kind of paradigm offers human-centered convenient and delightful services at any time, at anywhere, and in any devices. Recently, Human-Centric Ubiquitous Computing (H-Ubi Comp) has been studied on the basis of smart space, human computer interaction, intelligent services and universal device connection. However, H-Ubi Comp is closely connected to networks and in this connection there exist essential security issues concerning security vulnerability and exposure of user's privacy. In order to provide secure H-Ubi Comp environments, we need intelligent and dynamic security frameworks suitable for H-Ubi Comp environments. The user manual authentication, static access control and management which are the key of traditional security mechanisms have lots of restrictions for being adapted in H-Ubi Comp environments.

In this thesis, I propose a hybrid intelligent security framework for H-Ubi Comp: HUC-HISF. The HUC-HISF consists of core technology layer, security layer, application and service layer. The Core technology layer contains wireless sensor network/RFID, context-awareness, mobility and information fusion which are key technologies of H-Ubi Comp, and security layer contains lightweight security algorithms, security protocols, users' privacy and security mechanisms. Finally, in application and service layer, surveillance systems and mobile IPTV for H-Ubi Comp are considered.

In this thesis, I design and simulate light-weight secure advanced cryptography algorithm, effective key distribution for secure fast hand-over, and dynamic context based access control mechanism reflecting human-contexts, and privacy-enhanced key recovery mechanisms. I also propose and analyze surveillance service and mobile IPTV service through applied-service layers.

The HUC-HISF provides an advanced key schedule of mCrypton algorithm suitable for H-Ubi Comp devices to give a better security of mCrypton against related-key rectangle attacks. We also provide wireless authentication, key establishment mechanisms suitable for H-Ubi Comp environments, secure authentications and key-exchange protocols. Furthermore, I propose dynamic human-context role based access control mechanism, and surveillance service and mobile IPTV service which are applied-services of the HUC-HISF.

Contents

List of Figures

List of Tables

Chapter 1. Introduction

1.1 Overview

New computing paradigms such as H-Ubi Comp are up and coming due to rapid advances in computing power and network development. Such paradigm changes offer convenient and delightful, human-centered services at anytime, anywhere, and in any devices. Recently, H-Ubi Comp has been studied in terms of smart spaces, human-computer interaction, intelligent services, and universal device connectivity. However, H-Ubi Comp is closely related to networks and in this realm there exist essential security issues concerning the vulnerability and exposure of users' privacy. Traditional security mechanisms require manual authentication by users, static access control and static management which significantly restrict adaptability which is absolutely fundamental in H-Ubi Comp environments. In order to provide secure, yet flexible H-Ubi Comp environments, we need intelligent and dynamic security frameworks suitable for H-Ubi Comp environments.

1.2 Scope, Aim, and Method

The HUC-HISF, the novel security framework presented in this thesis, provides an advanced key schedule of mCrypton suitable for H-Ubi Comp devices providing better security for mCrypton against related-key rectangle attacks. The framework also provides wireless authentication, key establishment mechanisms, secure authentications and key-exchange protocols suitable for H-Ubi Comp environments. Furthermore, I introduce how the HUC-HISF may be applied to dynamic human-context based access control mechanisms, surveillance service and mobile IPTV service.

1.3 State of the Problem and Motivation

We could say that today's computing technology has reached the highest level it can. Personal computers and servers have reached the highest level possible in terms of design and speed and now we are working to reduce the power consumption and heat generated by Central Processing Units (CPU), such as the major chipset, by increase its density. In addition, projects such as multi-core, multi-processor, and grid computing are enhancing computational power through the collaboration of multiple processing devices. In addition, computer network technology is bringing about development in a variety of fields including moving beyond wired communications to wireless communication, mobile communication, and lower energy communications. Recently in the United States, Juniper and Cisco have expanded the bandwidth of wired network communications by developing routers having 10Gb/s interfaces. In the case of wireless communications, 802.11/n has become commercially available and theoretically promises wireless communication speeds of up to 300Mb/s. The world of mobile communication technologies has witnessed the worldwide popularization of the smart phone and smart pad empowered with 4Generation mobile communication technologies such as Long-Term Evolution (LTE) and Wi-MAX. In addition, thanks to low-power communications technology for wireless sensor networks (WSN), research on applications such as Zigbee and Bluetooth is progressing quite rapidly and many related products are being commercialized and widely used.

Through the advancement of such computer and network technologies, complex functions are increasingly being performed remotely by servers and personal computing devices are becoming increasingly miniaturized. Accordingly we are witnessing the rise of a new services paradigm known as cloud computing. Cloud computing places great importance on inter-operability, a key providing services to devices having respectively different operating systems and hardware specifications. This development came on the back of multiple environment service technologies such as HTML5 and is transferring the life, information exchange, and transactions of offline environments onto online environments. Thanks to these developments in computer and network technology, it has become increasingly convenient for users to produce, share, and use digital information whenever and wherever they like. On the other hand, this growth of proper uses for computers and networks has been paralleled by a rise in opportunities for misuse to malicious ends. We can even see such adverse effects for the portable devises applying the newest computer and network technologies. By cracking the operating system of their portable device, users are able to acquire ultimate administrator access, circumvent the DRM inserted by device and content providers to protect their intellectual property rights, and illegally use for-pay content. Consider the following examples of Sony’s PlayStation Portable (PSP) and Apple’s iPhone, both sold worldwide. In the case of PSP, hackers developed custom firmware in order to run games illegally. With the iPhone, hackers used jailbreak to acquire maximum administrative authority for the iOS platform, disable Digital Right Management (DRM) for those contents serviced by Apple, and made cracked Apple and contents available fee of charge. Both industries and society responded to these illegal episodes in their own ways and the result for industries in cases such as the Sony PlayStation Network hacking incident is that they incur enormous damages [IEEE11].

The aforementioned Sony PSN hacking episode is merely one of the many hacking episodes that are currently underway, however the Sony incident has a special meaning. Prior to the PNS hacking incident, attacks had typically included those propagated to acquire information or administrator privileges from a single server, Distributed Denial of Service (DDoS) attacks which were primarily performed with the goal of paralyzing the service of a specific company or organization, or attacks on an individual or specific organization for the purpose of acquiring information possessed by a specific company. However after the PSN incident, America declared war on hackers, hacker groups began to direct ideologically motivated attacks against the government agencies of several countries, and these hacking attacks began to pose a national threat. We use cellular networks in my everyday lives to exchange a variety of information and access apply of services. Were these networks to ever be subject to manipulation or a denial of service attack, it is predicted that the many services using these cellular networks would be paralyzed and that a great calamity would ensue. Also cloud computing and ubiquitous computing will become the base of Internet environments of the future. As user devices become gradually lighter, complicated computing and high volume information will be provided by servers. These systems will take several forms, be applied to a variety of fields, and play an increasing role in the private lives and health of individuals and the information of organizations. As a part of this process, terminal user devices will contain important information for identifying the user's personal information contained in servers. Should this data be leaked, it could result in great harm to individuals and organizations and therefore must be distributed through secure channels. Accordingly, there is a need for research on those methods which enable services to be provided both securely and conveniently. Also, as ubiquitous computing is applied to automobiles and the area of public health, data is exchanged which contains information about individual's health or the control and condition of an automobile. Should this information be altered or made public, it could lead to dangerous situations. Even were the data not altered or leaked, should a DDoS attack or something like it suspend normal service, the likelihood of unexpected malfunctions and the resultant damage is very high.

This thesis addresses this type of service availability problems for ubiquitous computing environments and defines a security framework maximizing security. This framework proposes a cryptographic algorithm and some protocols which offer both light-weight processes and strong security.

1.4 Thesis Contribution

The expected contributions of this thesis are:

- The proposed framework provides a light-weight cryptography algorithm for security in resource-constrained applications, such as low-cost RFID tags and sensors in USN for H-Ubi Comp. It has the structure with some improvements in software and hardware efficiency under resource-restricted environments – such as ubiquitous mobile devices.
- The proposed framework provides improved security protocols for H-Ubi Comp.
  - A session key distribution mechanism for fast secure handover in wireless mobile networks such as H-Ubi Comp: The proposed mechanism is based on the stream control transmission protocol wherein a mobile node actively changes its IP address without a loss of connection.
  - A security-enhanced Key Recovery (KR) protocol and a privacy-enhanced KR protocol: The proposed protocol is based on that security-enhanced KR protocol in order to protect users' location privacy. Wireless Authentication and Key Establishment (WAKE) protocols are essential for secure information transmission for in mobile communication environments such as H-Ubi Comp.
  - A security simulation model based on Contract Network Protocol (CNP): I design and construct a general simulation environment for a network security model which coordinates by means of a contract net protocol (CNP) for the effective detection of an intrusion.
- The proposed framework provides dynamic human-context role based access control mechanism for H-Ubi Comp. It improves the existing access control mechanism based human-context (temporal and spatial information).
- The proposed framework can be applied to surveillance service and mobile IPTV service for H-Ubi Comp.

1.5 Thesis Outline

The structure of this thesis is as follows. In Chapter 2, I review research papers related to this thesis. In Chapter 3, I propose the HUC-HISF, a novel security framework for ubiquitous and human-centric computing environments. In Chapter 4, I discuss advanced mCrypton, a light-weight cryptography algorithm appropriate for the HUC-HISF. In Chapter 5, I describe security protocols fitting for the HUC-HISF and in Chapter 6, propose dynamic human-context role based access control mechanism. In Chapter 7, I discuss services such as the U-Surveillance service and the Mobile IPTV service to which the HUC-HISF may be applied. In Chapter 8, I simulate and analyze the proposed algorithms, protocols, and services for the HUC-HISF. Finally, I end in Chapter 9, with discussion and conclusions.

Chapter 2. Background

2.1 Ubiquitous Computing Vision

The words ubiquitous computing was first used by *Mark Weiser* to describe computing technology of the future. *Weiser* proposed the concept of ubiquitous computing in 1988, asserting that technology that is invisible is the most profound. Ubiquitous computing transcends the boundaries of space and time, perceiving the tasks that human are attempting to do and helps them to perform those tasks. *Mark Weiser's* concept of ubiquitous computing requires all computing devices to be connected to each other. Ubiquitous computing does not draw the users attention and it must be functional in all times and places. It also has the properties of being embedded in the objects and environment of the real world and is integrated into everyday life [We91]. This kind of ubiquitous computing is the computing technology of the future that is gradually being realized with the development of mobile telecommunication technologies, mobile devices, sensor technology, and so on.

Ubiquitous computing not only includes remote communication, fault tolerance, high availability, remote information access, distributed computing such as distributed security, but also a variety of technologies related to mobile computing and pervasive computing.

The following table lays out the various requirements that computing must satisfy in order to be deemed ubiquitous.

Table 2.1 Requirements for Ubiquitous Computing

Requirements	Description
Adaptability	• Laissez-faire approach : by each app • Application-transparent approach : fully supported by system • Application-aware approach : collaborative between app. & system • Agile approach : combined with them
Augmented Reality	• Fidelity: consistency, data type, tradeoff btw. Applications • (e.g.) sampling rate, timeliness, size, resolution, frame rate
Heterogeneity	• Integrated networks to different devices, user interaction models, radio capabilities, memory, power, processing capabilities like mobility • Multi-modality
Interoperability	• Understand the exchanged info • Provide something new originating from the exchanged info • Dynamic binding according to the change of context
Mobility	• Terminal, personal, session, service • Actual : transfer code, data, exe, state • Agent : follow nomadic user • Virtual agent: move to exe, env. • Physical agent : move to access point
Security and Privacy	• Self-healing in attacks and failures • Survival by protection (SP) : access control, encryption • Survival by adaptation (SA) : increasing key length in intrusive threat
Self-Organization	• Automatically organized • Self-learning, expert systems, chaotic theory, fuzzy logic • Spontaneous systems or dynamically re-organized software architecture

2.2 Collaboration Work and Processing based on Human-Centric Computing

Existing collaboration based on software or system vs. Human-centered computing based collaboration, software or system based shortcoming of the system to communicate with most of the human exchanges and the resulting synergy is something lacking in creation. In particular, software or system centric, the center or some parts of the features and software configuration of the joint development or joint development of exchanges in the unit, or part of the target unit was limited to that cavitation is a typical drawback [Sch11].

In terms of composing the system easy to configure, traditional computer science, consists of traditional on-course or at the stage of development, however present a variety of services, according to a variety of environments in terms of non-human-centered computing environment is a sufficient differences. Especially, the human-centered computing based collaborative processing system is configured with sufficient synergies can be triggered with the various opinions, various adjustments, a variety of environments are structured around both the ease of humans is also occurring. Therefore, there is a variety of subsequent related research. In this chapter describes the system in the study were collaboration based on Human-Centric Computing. Since several years ago, many of the systems and services and its environment has changed a lot. In particular, users of the Web environment to provide rapid information exchange model for a given service in a variety of environments has been used to organize content.

These Web services take advantage of the user-friendly tool, but also a major tool used in Service-Oriented-Architecture (SOA) as an extended automatic exchange of information with people who are for that purpose [Sch11]. However, when many people to exchange information using by Web environment, actually it is not user friendly and human-centric computing rather than only the center is composed of a thorough service. In the case of Web services to provide a variety of interfaces are configured in parallel to this, Software-Based Service (SBS) and the Human-Provided Services (HPS) should be defined first as human-centric services can be composed

2.3 Human-Provided and Software-Based Service Mixture Model

In various researches, these human-centric and software-centric model is configured with the proper convergence has been studied.

This is both human and software-centric as a model for convergence in order to satisfy the user-friendly with well-defined interfaces, and it is based on information sharing between people.

In addition, the existing problems which are the configuration of human-centered problems were to configure the current system, also the composing by using an intermediate medium layer in the context of a web-based system that contains a human-centric configuration.

Proposed in the context of Web-based human-centered interactive system consists of the following three were to form.

- **Crowdsourcing**: As a variety of related research, one of important thing is the study of Crowdsourcing. It is complexities connecting of a society, basis of involve network, incentives and aggregate behavior of groups; these are aimed [EK10]. Human computation is motivated by the need to outsource certain steps in a computational process to humans [GRS05]. An application of human computation in genetic algorithms was presented in [KGD01]. A variant of human computation called games that matter was introduced by [Ah06]. Related to human computation are systems such as Amazon Mechanical Turk1 (MTurk). MTurk is a Web-based, task-centric platform. Users can publish, claim, and process tasks. For example [SPCB07], evaluated the task properties of a similar platform in cases where large amounts of data are reviewed by humans. In contrast to common question/answer (Q/A) forums, for example Yahoo! Answers2, MTurk enables businesses to access the manpower of thousands of people using a Web services API. Mixed service-oriented systems target flexible interactions and compositions of Human-Provided and Software-Based Services [STD08]. This approach is aligned with the vision of the Web 2.0, where people can actively contribute services. In such networks, humans may participate and provide services in a uniform way by using the HPS framework [Sc09]. A similar vision is shared by [Pe10] who defines emergent collectives which are networks of interlinked valued nodes (services).
- **Interaction Modeling**: In business processes (typically closed environments), human-based process activities and human tasks can be modeled in a standardized service-oriented manner.WS-HumanTask (WS-HT) [Am07] and BPEL4People (B4P) [Ag07] are related industry standards released to address the need for human involvement in service-oriented systems. These standards and related efforts specify languages to model human interactions in BPEL [Ag07], the lifecycle of humans tasks [Am07] in SOA, resource patterns [RA07], and role-based access models [MPS08]. A concrete implementation of B4P as a service was introduced in [TPBE07]. A top-down approach, however, demands for the precise definition of roles and interactions between humans and services. The application of such models is therefore limited in crowdsourcing scenarios due to the complexity of human tasks, people’s individual understanding, and unpredictable events. Other approaches focus on ad-hoc workflows [Du04], self-contained child processes [AHEA06] based on activity theory, and task-adaptation [GPSS04] to cope with changing environmental conditions. In [MGMTM06], business activity patterns were introduced to design flexible applications.
- **Metrics and expertise mining**: Human tasks metrics in workflow management system have been discussed in [KAV02]. A formal approach to modeling and measuring inconsistencies and deviations, generalized for human-centered systems, was presented in [CNFG96]. Studies on distributed teams focus on human performance and interactions [BPW04, PD05], as well as in Enterprise 2.0 environments [BPD09]. Models and algorithms to determine the expertise of users are important in future service-oriented environments. Task based platforms allow users to share their expertise [YAA08]; or users offer their expertise by helping other users

in forums or answer communities [ACDGM08]. By analyzing email conversations [DECZ03], the authors studied graph-based algorithms such as Hyperlink-Induced Topic Search (HITS) [Kl99] and PageRank [BMW98] to estimate the expertise of users. The authors in [SA05] used a graph-entropy model to measure the importance of users. The work by [ZAA07] applied HITS as well as PageRank in online communities (i.e., a Java Q/A forum). Approaches for calculating personalized PageRank scores were introduced in [Ha02, JW03] to enable topic-sensitive queries in search engines, but have not been applied to interaction analysis (social networks). Most existing link-based expertise mining techniques do not consider information related to the interaction context.

2.4 Human Computer Interaction (HCI) for context aware ubiquitous computing

Differences of state-of-art approaches for human context acquisition in smart environments for personalization of services are also one of important issue in Human-Centric Computing research area. *Abhijan Bhattacharyya* is proposed a human conventional mobile communication technology for human context awareness in ubiquitous computing environments [Ab11]. This paper compared them based on some real-life human centric attributes which proposed a possible scheme through exploring the potential of using standard mobile communication method for human presences identifying.

Human context acquisition is an important aspect of human computer interaction (HCI) for context aware ubiquitous computing. There are many proposed and in-use techniques for achieving the purpose of human context acquisition which is the key in terms of personalization of services. However, there are some advantages and some disadvantages when we try to evaluate them in terms of real life aspects which essentially involve human factors. For example, Mobile phones can be a good choice for such a purpose by virtue of its normal course of operation in the very basic form without relying on convergence with other associated technologies like Bluetooth, WiFi, etc. However, mobile phone operations don’t have that in personalization of smart environment services compared to other approaches. This is the problem of mechanized presence detection and identification in a premise / system to perform some predefined task relevant to the identified person is not new. As a software system which gets unlocked only when the right user ID and password leading the system to activate with the settings user profile. However, these kind of conventional systems, though context aware in true sense, are not ‘unobtrusive’ so far as the HCI is considered as they require explicit human interaction to initiate the process. Following part concisely presents a survey of different dominant technologies proposed in different literatures.

- **Active Badge using modulated infrared beacon:** The Active Badge Which emits a periodic unique code in the form of a beacon by way of pulse-width-modulation of infrared signals as described in [WHFG92].
- **RFID based detection:** It uses electromagnetic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object or a person with an RFID tag. RFID tags are passive or active. Passive RFID tags receive their

power to exchange from the signal sent by the RFID reader itself. Active RFID tags are battery powered.

- **Detection using short range wireless communication – Bluetooth and WiFi:** Short range wireless communication like Bluetooth and WiFi have become a very popular choice for human presence detection [MMNV05, VMNLVPM05, SPD06, xAP08, Le08]. The devices are usually personalized and thus their addresses can be tagged with the users using them.
- **Detection based on computer vision – Face Recognition:** Face recognition using computer vision is a promising technology for presence detection in smart environment [PC00, HWRB05, IRK02, RSM04, SFV05]. This technique uses artificial intelligence (AI) on captured camera images and the identification works using a classifier which has been trained with the end users (like members of a home, preferred customers of a superstore, etc.) in advance.

This paper analysis with several issues in line with Ref. [WHFG92] and [IRK02]. That issues can be treated as real life attributes for judging the effective approaches methods like Confidence, Detection range Technical issues, Power requirement, Ease of use / unobtrusiveness, Psychological factors, and Cost effectiveness. On this wise, this paper perform a surveyed of the state-of-the approaches from computer vision to short range wireless communications and compared them against some real life issues. After this, who studied a technical feasibility for using the mobile phone. There is potential of using this conventional technology for such purpose and thereby opening up huge possibilities in context aware services through mobile HCI, By Using the standard mobile communication for presence detection and identification for personalization of services in smart environments.

In case of Ref. [Ab10] proposed different approaches to detect user's presence by a suitable IP (Internet Protocol) domain to control active hand-off between cellular and IP domain. One of the schemes used a pseudo base station that broadcasts the 'registration invitation' signal.

Pseudo a mobile phone base station would transmit back its 'registration information' containing the mobile identification number (MIN) and electronic serial number (ESN) (Figure. 2.1).

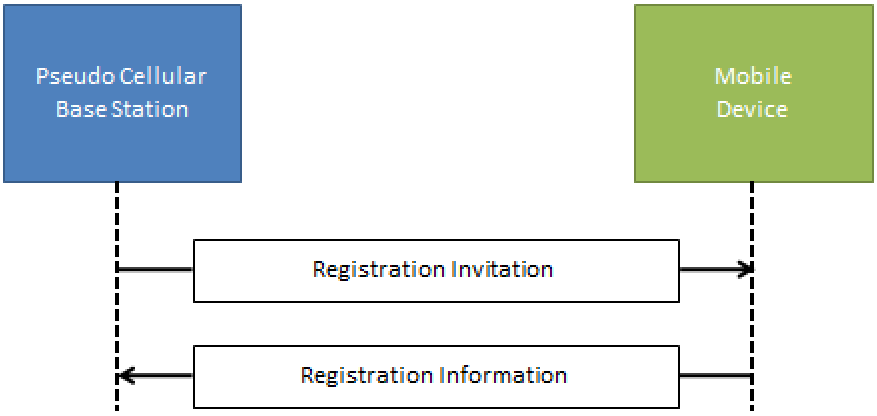


Figure 2.1 Ubiquitous Mobile Node Identify Procedure [Ab10]

These identify methods are used to route all calls to the MIN to the appropriate device and location. This approach method can be generalized and explored for providing different personalized services in a smart space like conceptualized in Figure. 2.2.

Figure. 2.2 The conceptual smart space is equipped with a gateway that the user presence through a virtual base station and controls the applications as each of the personalized requirements of the user. Through this shows, we can confirm the potential of unobtrusive use of conventional mobile communication for human context acquisition in a smart space in a very unobtrusive way.

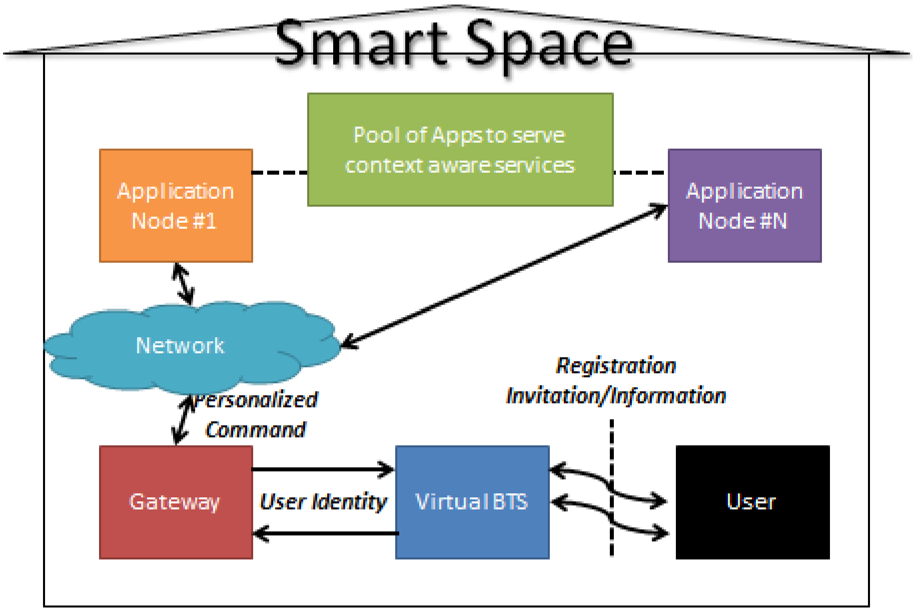


Figure 2.2 Extracting human context by mobile node identifiers in a smart space

This paper analysis of the mobile communication based scheme, First, In terms of confidence the mobile phones are very much personalized. Second, Detection range should not be a problem.

Third, this approach method does not require any additional power just to perform the detection activity unlike schemes like Bluetooth/ Wi-Fi, etc. Fourth, this scheme should be quite unobtrusive which is quite habitual and does not need to switch on additional services like Bluetooth / WiFi for this purpose. Fifth, this scheme does not add any psychological discomfort. Finally, this scheme does not incur any additional cost other than that of the mobile phone.

These kinds of points show the advantages of the proposed scheme over others. However, that needs to be addressed before arriving at an applicable solution. The major issues on this paper identifies are first, may overlap with neighboring region causing false alarm Because of broadcast nature advertiser’s radiation. Second, a breach of the standard security feature may need special permission from competent authority. Third, using the licensed band for detection need spectrum usage permission. However, it does not apply for scenarios where the premises are equipped with legitimate femto-cells like [MTRSO10].

This scheme can provide us with a very good unobtrusive HCI compared to other techniques.

Also, this issues that need to be addressed for making the proposed scheme a usable choice. And, this scheme can provide good motivation to come up with innovative solutions with mobile HCI for personalization of services in a ubiquitous environment.

2.5 Security Issues for H-Ubi Comp

We have been discussed the following traditional concept - Confidentiality, Integrity, Availability as the most principal security properties; Confidentiality is that information is only made available to those who are authorized to have it. Integrity is that only authorized users may manipulate information. Availability is that information services must be accessible to those authorized. However, in H-Ubi Comp in which wireless networks and various other network environments have been integrated, there exists a much greater likelihood of exposure to security threats compared to ordinary computing environments. Furthermore, H-Ubi Comp environments are vulnerable to additional threats not present in traditional computing environments; such threats include tampering, signal interference, and battery consumption attacks. The types of security threats arising in this kind of ubiquitous computing environment may be largely expressed as follows [CGRZ04, St02].

Table 2.2 Security Threats for H-Ubi Comp

Name	Description
Denial of Service (DoS)	• Attacks compromising availability • Consuming their resources for networking or computing • Ubiquitous computing networks dependent on multi-hop routing protocols • Occurrence of DoS in the event that a single node refuses to cooperate
Disturbing Signal	• Attacks compromising availability • Cross-talk attack
Exhausted Battery	• Ordinary message use that does not violate security • Send data request message • Send request message for network connection
IP Spoofing	• When traffic is not encrypted, then attackers can get your traffic data and be spoof your information
Malicious Code/Program	• General threat for computer networking • Violations of confidentiality, integrity, or availability
Privacy	• Leakage of personal information such as user’s location, time at which the device was used, etc.
Rogue Access Point	• Only one-way authentication is available • Unreliability of access points
Tampering devices	• Physical attack • e.g. Re-flashing firmware, Defective device, etc.

In order to respond to the security threats in Table 2.2, H-Ubi Comp must satisfy the security requirements listed as follows;

Table 2.3 Security Requirements for H-Ubi Comp

Name	Description
Confidentiality	• Key management • Data Encryption • Light-weight crypt algorithm
Integrity	• Encryption techniques for guaranteeing integrity
Availability	• Provisions for DoS attacks
Authentication	• Mutual authentication • Use dynamic key • Key distribution protocol
Access Control	• User discernment and information access control
Anonymity	• Guarantee of anonymity

2.6 Research Trends

2.6.1 H-Ubi Comp Projects

Efforts to realize ubiquitous-human centric computing may be seen around the world. Basically, both ubiquitous-computing and Human-centric computing provide us convenient lives automatically. However human-centric computing is not a device but it is based on human. These are why they are basically different. Human-centric computing demand a device, but it can be inputted by human only and it is embedded by objects which are came from human's life.

In this sub-section, these kinds of internationally researching projects are being discussed in America, Europe, and Japan [Sc03].

United States of America

- **EasyLiving**: EasyLiving refers to Microsoft’s ubiquitous computing technologies research program. When Microsoft launched the project in 1995, it announced that ubiquitous computing would be achieved through mobile computing and intelligent environments. Microsoft’s ubiquitous computing entails non-integrated computing, location sensing computing, enhanced reality and object sensing user interfaces. These resources are not connected to each other but they are able to interact through the Internet. The EasyLiving Project automatically detects when a person enters a room and sits down, it searches email or pre-selects a movie for that person to watch, and shots off the display when they stand up and leave. The project also enables a user to be logged off from one computer as they move to another and the work they processed on their desktop to be displayed on a screen [SKBMCR98].

- **CoolTown**: CoolTown refers to Hewett Packard's ubiquitous computing technology and architecture. In the virtual space of the Internet, websites such as virtual shopping malls and chat rooms are constructed to represent the information of physical objects, persons, and spaces. However, very few of the resources in those physical spaces are systematically linked to their representative virtual spaces online. Thus there is a large gap between the information online and the physical reality. HP launched this project with the aim of closely fusing physical spaces and online virtual spaces. HP coined the term "web-presence" which term refers to new web interfaces that serve as an infrastructure between people, places, and objects. Web presence systems act to maintain the automatic support and interconnectivity between all physical elements and related web pages. CoolTown is the realization of a futuristic city model that uses wired and wireless communication network technology and web-based communication. CoolTown attempted to link real-world people and objects with virtual spaces made up primarily of existing web infrastructure, and devices equipped with electronic tags, internal web servers, and close-range wireless communication. Given its goal of constructing environments to link real-world people, places, and objects to virtual worlds, CoolTown may be applied to environments such as art galleries, conference rooms, mass transportation, e-business, remote education, remove medical treatment, fire response services, and so on [Co00].
- **Smart Space**: Smart Space is a research initiative conducted by the Smart Space Lab at NIST. Smart Space is an environment meant to help people perform tasks more efficiently through embedded computers, information devices, and multimodal sensors. Smart Space provides useful services for embedded devices. As a project supporting industries that graft pervasive computing onto actual useful services relying on computers, information devices, and multimedia planted within the environment, the goal of Smart Space is to increase the efficiency of work by applying new types of information and computer functionality. The project not only researched technologies for recognizing users, but also user actions and intentions for the purpose of assessing the user's needs and predicting their next action even as they work. Perceptual interfaces, mobility and networking, pervasive devices, information access, and other technologies were used in the implementation of Smart Space [SS08].
- **Smart Room**: Smart Room is research being conducted in the MIT Media Lab and uses vision based tracking and a large-sized projection screen to interpret the actions of people as detected by camera, mikes, and various sensors installed in a room. A smart room has already been implemented that detects the identity of people presently in the room and what actions their hands are performing. Smart Room technology has also been implemented within the interior of a car and can tell when a driver turns, stops and passes. In conjunction with this project, the MIT Media Lab is conducting a number of related projects including Smart Desk, Smart Chair, and Smart Cloth [SR94].
- **Smart Dust**: Smart Dust is a project initiated at UK Berkeley in 1997 to develop small-scale perception devices. The goal of the project was to develop micro-sized

chips that contained a sensor, transmitter-receiver, and solar cell within a cubic silicon mote no larger than 1mm3, and could act as an autonomous sensor network. Smart Dust concentrated on minimizing the energy consumption of tasks and loading necessary information gathering sensors in as small a space as possible. It also aimed at using tele-communications to mutually detect each other and compute more efficiently. Applied areas of the Smart Dust project include energy management, management of product quality, management of circulation channels, military areas, and so on and implemented functions such as detection of atmospheric conditions, biochemical pollution, and movements of military troops and material [SD01].

- **Oxygen**: The Oxygen project, underway at MIT, recognizes that as computers become as plentiful and common as oxygen, there is an increasing need to build computing environments and services that meet users needs anywhere and in any place, and with natural interfaces such as voice or vision, that require no special knowledge or training [Ox00]. A number of Oxygen-type environments have been implemented, namely E21s, H21s, N21s, and O2S; each is described below.
    - E21s: computers installed in home basements, office walls, and automobile trunks
    - H21s:conversing with a screen by voice alone, this device supports any user's speech and computer use
    - N21s: a network capable of installing itself according to changes in its neighboring environment
    - O2S: software supporting services adaptable to changes in the environment or users demands
- **Aura**: The Aura Project is related to invisible computing and was begun at Carnegie Mellon University in 1999. The Aura Project asserts that the user's attention is more precious a resource of a computing system than processors and memory and thus conducted research on hardware network user interfaces and applications with the goal of creating invisible computing and information service environments that supported users, like a halo, magnifying them wherever they go [Au00].
- **Portolano**: Portolano, a project begun at the University of Washington, aimed to implement computing environments transparent to users by means of invisible user interfaces, ubiquitous connectivity, and intelligent services. In this way, the program hoped to link the real world and the virtual world. The core research of this program focused on user interfaces, network infrastructure, and dispersed services [Po02].
- **Endeavour**: The Endeavor project was conducted at the University of California, relied on a variety of IT devices such as MEMS sensors, PDAs, and cameras, and had the goal of establishing standards and prototypes for widely applicable information processing environments capable of large-scale self-organization. This project began in 1999 and was collaboration between news agencies, manufacturers, and others. Technologies used in this project included MEMS, expandable computing structures, network oriented OS, user interfaces, data management systems, and so on [En99].
- **Smart Kindergarten**: Smart Kindergarten was a research project designed to examine how children learned in the physical space of a kindergarten using ubiquitous

computing and sensor-based wireless networks. This project began in 2000 under the joint cooperation of the computer engineering department, electrical engineering department, and educational information sciences department at UCLA. In the Smart Kindergarten research, wireless recognition technology was used to assess in real time the names and locations of children and toys. The project also used sensor technologies, interaction features, action sensing, and context awareness technology for tracking dynamic changes, and data-mining and Jini-based technologies for analyzing and deducing situations as they were transmitted by sensors in real time [SK02].

- **Smart Medical Home**: Smart Medical Home was implemented by Rochester University in five rooms and consisted of infrared sensors, computers, bio-sensors, video cameras, and so on. One core component of Smart Medical Home, named Smart Mirror, had the ability to monitor changes in skin and detect the onset of cancer. Smart Medical Home's Personal Medical Advisor (PMA) System provided a natural conversation interface. Smart Band-Aid contained an embedded chip that continuously monitored the recovery state of wounds and information collected by these sensors installed in various places was conveyed to the Personal Medical Advisor System as well as a doctor. When this happened, patients were able to manage the transmission of their data making it possible for doctors, nurses, and attendants receiving the data to write prescriptions or make home visits as the situation required [SMH98].

European Union

- **Smart Its**: Smart Its was a project jointly coordinated by ETH Zurich (Swiss Federal Institute of Technology), Germany's TeleCooperation Office, and the VTT Technical Research Institute of Finland. In this project, internal devices known as Smart Its were inserted into objects creating information artifacts capable of detection, recognition, computing, and wireless communication. By communicating with each other, these intelligent artifacts constituted a new environment capable of cooperative situation recognition and action. This project developed wireless recognition technology based on RFID which attached labels to the interactions between objects. It also conducted research on Bluetooth-based wireless communication technology, location and safety, and the interaction between smart objects and the environment. This project also developed Media Cup by loading Smart Its into ordinary coffee mugs capable of recognizing, processing, and transferring information about both the cup and even the user [BG03].
- **Paper++**: Kings College and HP, Germany's Anitra, ETH, France's Argo Wiggings, and others participated in a research project to create Paper++, an electronic teaching aid more useful than conventional paper aids in which were embedded sensors and location-based devices. The augmented math textbook developed through this research was designed so that when a smart pen touched a graph or picture in the book, related information and animations would appear on a device connected to the smart pen [NS05].

- **Grocer**: The Grocer project, initiated by the University of Navarra in Spain, loaded micro-processors into each product in a market and allowed consumers to transcend the limitations of space and purchase products using mobile devices or communication equipment. Grocer was implemented using Bluetooth, WAP, RFID, and other similar communications technologies [Gr02].
- **2WEAR**: The 2WEAR project was research jointly conducted by ICSForth, Nokia, ETH, and MA System. This project was carried out on the premise that computers of the future would be comprised of a variety of devices that are worn or carried about. If a person took a picture with a camera having 2WEAR capability, then the camera would be linked to GPS and a clock, the picture would be recorded along with the location and time of where and when it was taken, and if the camera's memory was full, the picture would automatically be saved to a wristwatch or MP3 player. Also, when a user lost their way when on vacation, the computers they were wearing would search for nearby road direction boards and other such devices in their immediate vicinity, which would then connect them to yet other devices that could instruct them where they were and how to proceed [2W01].

Japan

- **Goopas service**: Goopas Service was jointly developed by Omron and Tokyo Metro and is a service that provides information used to automatically examine subway tickets. Users of this service pre-register simple information about themselves and their station of interest and then receive exclusive permission to board. Afterwards, the user is automatically allowed to pass through the ticket gate of the corresponding station. In addition, event information matching the tastes of users in the area is transmitted to them by cell phone four times a day [Hi02].
- **eHII (Matsushita)**: The eHII project was begun by Matsushita in 1995. HII refers to information-based devices in the home such as AV, information devices, and home electronics that connect families with social infrastructure and services such as broadcasts, communication, public services, and so on. eHII went on display in April 2001 and introduced a convenient and ideal image of family life in which the daily life spaces were connected to internal information devices and the external network, from kitchen to bathroom, from the living room to the bedroom [BBBR04].
- **MY parent's Concierge**: A service fit for the age of the aging, My Parent's Concierge created a ubiquitous computing environment that attached various sensors on the bed of an aging parent including a doll positioned on the bed to which was also attached a sensor. In the event that the senior citizen did not trigger sensors during the day, the system would automatically contact the senior's children and health services in the parent's neighborhood [Hi02].
- **TRON (The Real Time Operating System Nucleus)**: Tron was first launched in 1984 by *Professor Ken Sakamura* and investigated intelligent and regionally distributed systems in Japan's first attempt to unify the software specifications for a variety of internal kernels. In the process, *Professor Ken* developed the TRON chip and proposed domain-specific specifications. The TRON intelligent house applies the

TRON system, deploying over 1000 computers in a house of 330 square meters, to achieve a ubiquitous computing living environment [Ye00].

2.6.2 Security Framework

Today, organizations and businesses apply Information Technology (IT) in order to efficiently manage their assets. In the process, Enterprise Architecture (EA) was developed and applied in order to simplify the derivation, development, management, maintenance, and repair of resources and the interoperability between each resource. In addition to the Enterprise field, the field of Information Security is also being applied.

In the field of security, the security requirements of products or serves are derived systematically. Security architecture is developed in order to develop, manage, maintain and repair products and solutions, and the various methodologies and procedures for developing this architecture constitute the security framework. Sherwood Applied Business Security Architecture (SABSA) is a representative framework for enterprise information security, and is currently a being used and applied in the field of information security as a framework for enterprises and organizations such as the Open Group Architecture Framework (TOGAF).

As this paper focuses primarily on security frameworks, I will briefly describe enterprise architecture and then explain SABSA in greater detail.

- **The Zachman Framework**: The Zachman Framework was proposed by *John Zachman* in 1987 and is a framework for enterprise architecture. *John Zachman* defined an interface integrating all of the components of a system in order to handle the ever increasing size and complexity of information systems. He also noted the need for a logical control structure. *Zachman* presented three categories of information for a given system, namely the what (data), how (process), and where (network), as well a method for distinguishing between the three at five levels of specificity. Then in 1992, *Zachman* thee additional pieces of information, Who (People), When (Time), and Why (Purpose) were added to the original three and together these six are still being used up to the present [Za87].
- **Technical Architecture Framework for Information Management (TAFIM)**: In order to describe DoDAF, we need to discuss Enterprise Architecture and a few other topics. When the Gulf War broke out in 1991, it was discovered that the weapons systems developed over the decades by the Army, Navy, and Air Force did not actually work together in war time. Shortly after the Gulf War in 1992, the Department of Defense began developing TAFIM to solve this problem. TAFIM was developed as the DoD’s Technical Architecture but rather than detailed system architecture, it more closely resembled a Technical Reference Model systematizing the requirements that must be satisfied in the development process such as services, standards, components, and form. Following the development of TAFIM, the DoD realized that in order to reliably communicate information between all sensors, signal processing and command centers, attack weapons and support activities, there was a need for standardization between all systems. In response to this need, the DoD continued to develop TAFIM and in 1997 instituted standards known as the Joint Technical Architecture (JTA) for technical standard specifications and information

support in war-time. While TAFIM developed the JTA, C4ISR, and DoDAF, it also played a role of promoting the need for Enterprise Architecture to the U.S. government. Additionally, TAFIM opened these technologies to the public through the Open Group and was the base upon which The Open Group Architectural Framework (TOGAF) v1.0, introduced in 1995, was developed [SLL10].

- **Federal Enterprise Architecture Framework (FEAF)**: As each U.S. government institute created its respective Information Technology Architecture (ITA), the need for common guidelines was raised. Accordingly federal government's Chief Information Officer (CIO) Council developed FEAF based on the Zachman Framework and developed methods known as "A Practical Guide to the Federal Enterprise Architecture" based on the EAP proposed by *Dr. Steven H. Spewak.*
- **Department of Defense Architecture Framework (DoDAF)**: In 1996, the DoD developed the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture Framework (C4ISR-AF) and proposed a system design scheme for greater compatibility between systems, projects, and services. After undergoing several revisions, C4ISR-AF later evolved into DoDAF. Along each step of the way, from TAFIM to C4ISR-AF and now DoDAF, much interest has been focused on integrating the technology of each sophisticated weapons system. Since the goal has been to standardize information technology architecture that include weapons systems, the DoD's architecture has developed more from the point of view of ITA rather than EA. DoDAF consists of a total of four views which include the Operational View (OV), Systems View (SV), Technical View (TV) and a main view to oversee the entire architecture, All View (AV). Operational View describes the tasks, activities along with the flow of information relevant for accomplishing DoD missions and consists of a total of nine products. Systems View lays out all information assets and systems supporting the Operational View and consists of a total of thirteen products. Technical View consists of two products related to technology standards [SE08].
- **The Open Group Architecture Framework (TOGAF)**: TOGAF is currently being developed and managed by Open Group as a framework for developing Enterprise Architecture (EA). TOGAF Version 1, developed in 1995, was based on TAFIM and developed with the transfer of technology from DoDAF, which was developed by the DoD. Architecture Description Method (ADM), Technical Reference Model (TRM), and Standard Information Base (SIB) have all been provided as important components of TOGAF. In 2001, TOGAF Version 7 was developed from an architecture point of view and differs from Version 8 which specifically elucidates business from an architecture standpoint, applications, information systems, and architecture from a technology standpoint. In recent years, TOGAF Version 9 was released which is now being applied to Model Driven Architecture [TOG09].
- **Sherwood Applied Business Security Architecture (SABSA)**: SABSA was first proposed by the John Sherwood in 1996 [Sh96]. SABSA consisted of three layers, namely a Logical Architecture for representing security services, a Physical

Architecture for representing security mechanisms, and an Operational Architecture for security management.

Table 2.4 The Layer of SABSA Model

View	Architecture
The Business View	Contextual Architecture
The Architect's View	Conceptual Architecture
The Designer's View	Logical Architecture
The Builder's View	Physical Architecture
The Tradesman's View	Component Architecture
The Facilities Manager's View	Operational Architecture

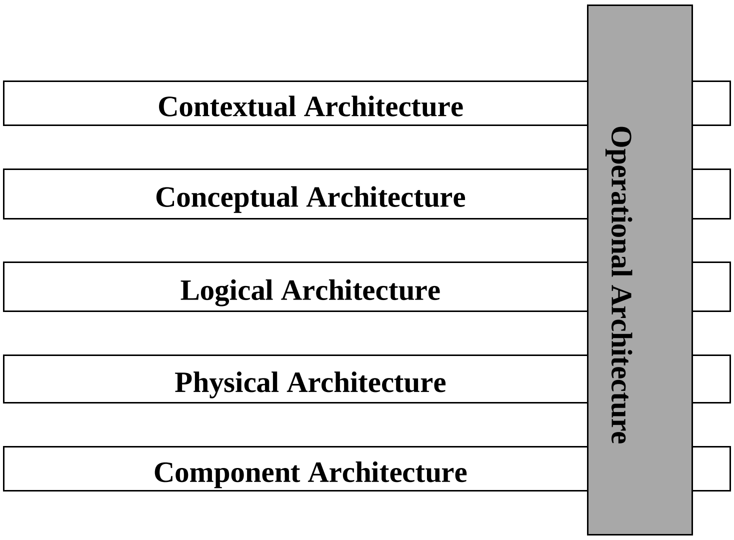


Figure 2.3 SABSA Model

Sherwood added two additional upper layers, a Contextual Architecture and a Conceptional Architecture, which added a business point of view, and added a Component Architecture below, presenting architecture of six layers overall. Each respective layer can be expressed in terms of each user's point of view, including process specification, design, development, and use.

SABSA matrix is a 6x6 matrix whose row values are the six architectural elements and whose column values are the answers to the questions used in the framework presented by *Zachman*.

Table 2.5 The SABSA Matrix for Security Architecture Development

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

SABSA's Development Process is developed sequentially as in Figure 2.4, however the Operational Architecture is simultaneously defined in the process of defining the Local, Physical, and Component Architecture.

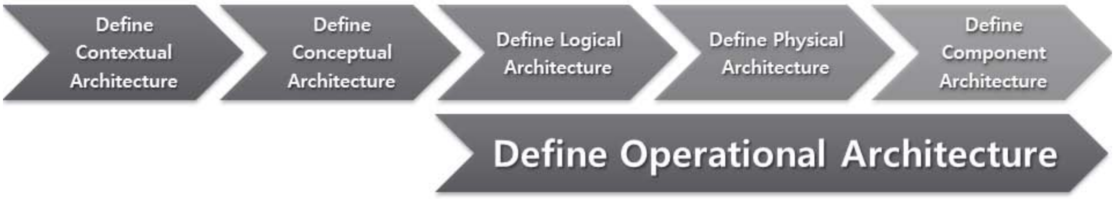

Define Contextual Architecture
Define Conceptual Architecture
Define Logical Architecture
Define Physical Architecture
Define Component Architecture
Define Operational Architecture

Figure 2.4 SABSA Development Process

The following describes the SABSA life cycle. In the Strategy and Concept phase, the Conceptual and Contextual Architecture are defined. The Design phase includes the Logical, Physical, and Operational Architecture. After the Implement and Manage and Measure phases, the cycle returns to the Strategy and Concept phase.

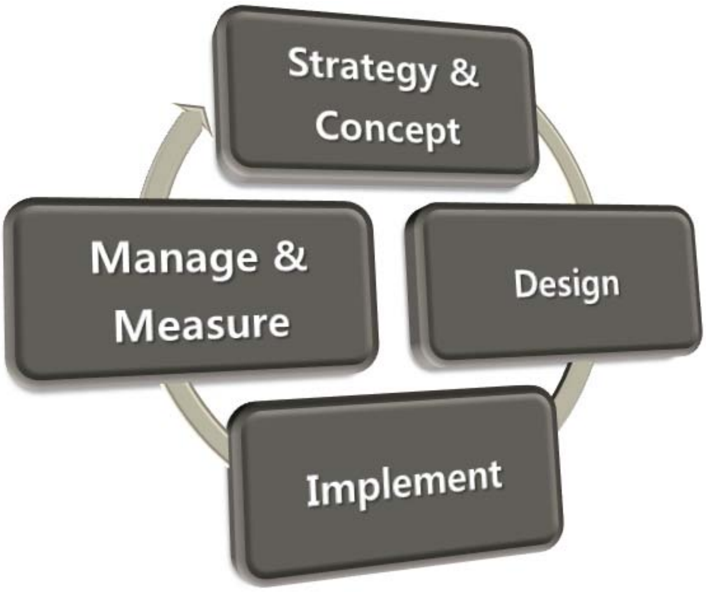


Figure 2.5 SABSA Life Cycle

The process was developed improved to correspond to needs such as management of an agency list, information assurance, governance, and maintenance, and may be used freely by any one in an open manner. With SABSA, it is possible to analyze the risk-based effects of costs and benefits and by using the architecture that has been developed to protect businesses' primary assests it is possible to strengthen an institution's reputation, keep customer's trust, and maintain business relationships, which all contribute to revitalizing business and adding value [SCL05].

Chapter 3. HUC-HISF

In this chapter, I define a hybrid intelligent security framework for H-Ubi Comp(HUC-HISF) that provides secure and intelligent services including core technologies such as WSN/RFID, context awareness, information fusion, authentication, authorization and access control, and surveillance.

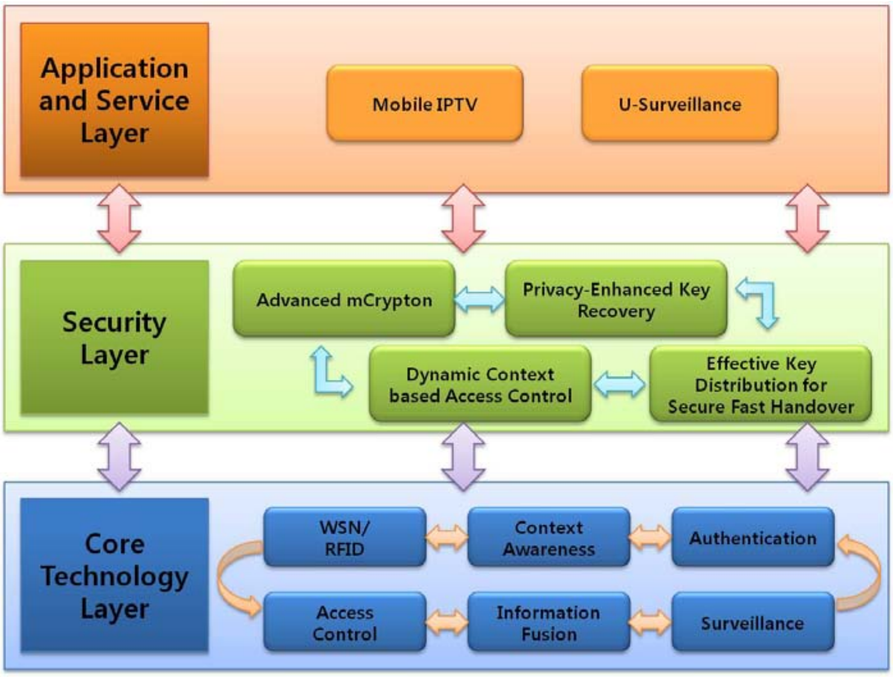


Figure 3.1 HUC-HISF

3.1 Core Technology Layer

The Core Technology Layer consists of technologies for network communication in a ubiquitous computing environment. These technologies include wireless sensor networks (WSN)/radio frequency identification (RFID), context awareness, authentication, access control, surveillance, information fusion, and so on.

In a sensor network, a large number of small-scale sensor nodes are deployed in a designated location or area. Recognition data is collected about the surrounding objects or environment and the network uses this information to activate applications and services. When wireless network interfaces are used to implement a sensor network, this is referred to as a wireless sensor network (WSN). The purpose of a WSN is to construct an environment wherein communication between objects is possible. It accomplishes this by infusing objects with computing and network communications abilities.

WSN have the following properties. One, sensor nodes must not malfunction on account of insufficient power, physical damage, or environment disruption factors. Two, sensor network protocols must be efficient and operate without regard to the scale of the network. Unlike in ad-hoc networks, this is particularly important as the number of nodes demanded may increase indefinitely, depending on the application. Lastly, as each sensor node has a limited amount of power, the WSN must minimize the use of power.

RFID is the next generation of recognition technology and uses wireless radio and an IC chip to manage information about a variety of objects including food, animals, and objects. RFID are often referred to as smart tags or electronic labels because they store information about all processes, from production to sales, on an internal microchip which may then be tracked on a wireless frequency.

RFID systems consist of three components including an RFID tag, antenna, and RFID reader. The reader uses its antenna to request information from the RFID tag by radio. Also using the antenna, the RFID tag sends a radio message to the reader containing the requested information. A computer then interprets and analyzes the data received by the reader.

Access control is a function that allows or refuses specified uses access to certain resources. Generally, it applies to all non-authenticated users as well and includes the comprehensive management of access including the connection IP of the system being protected, connection time, date, day, and category of client.

Context awareness detects contextual changes and either provides appropriate information and services to users or changes the system state directly. In order for the computer to comprehend contextual changes, the context must first be defined. Contextual information includes things such as identity location, state, and so on.

Table 3.1 Some example of Context

Context	Description
Identity	object identifier
Location	2D location information, direction, altitude, relationships between objects
States	Characteristic properties of the object
Time	In most cases, temporal context increases the value of historical information when used to recognize periods or encounter different contexts; in certain cases it simply means confirming the order of a sequence or confirming a cause-effect relationship

Authentication confirms who a user is, typically through confirming a user’s account and password. Other methods include smart card, retinal scan, voice recognition, fingerprint recognition, and so on.

3.2 Security Layer

The Security Layer consists of security technologies that provide secure, H-Ubi Comp services. In this thesis, I propose some security methods and a cryptographic algorithm that will improve the security of such services.

If we categorize information as a kind of asset, then cryptography can be defined as a means created to protect information assets from attack. The following three demands must be satisfied in order to safely protect information. First, it must be kept safe from those not authorized to access it (confidentiality). Second, it must be protected from data tampering (integrity), and third, authorized users must be able to access it when necessary (availability). Cryptographic algorithms are used to guarantee confidentiality. Cryptographic algorithms may largely be divided into symmetric key ciphers and asymmetric key ciphers. Symmetric key ciphers are cryptographic algorithms that use a single key to encrypt the data, one block at a time. The block size of a single block is fixed to be the length of the key. Examples of this category of cryptographic algorithm included Advanced Encryption Standard (AES), Data Encryption Standard (DES), SEED, Camellia, and so on. One the other hand, asymmetric key ciphers are also called public key cryptography. These encryption algorithms encrypt and decrypt plain text with a pair of keys. Examples of this encryption method include Rivest, Shamir, and Adelman (RSA) which uses prime-number factorization, Elliptic Curve Cryptography (ECC) which uses elliptic curves, and LUC which uses the Lucas series.

Generally in asymmetric key cryptography or public key cryptography, no key exchange procedure is necessary because keys are publically available. However, secure key exchange is a critical aspect of symmetric key cryptography, or block cryptography. Key exchange is especially an issue in the event that the private key is long. The technology for a user or agency establishing a private key and transmitting it to another user is called key distribution.

Key recovery refers to the bypassing of regular procedures and urgent decryption of encrypted data. Ciphers may also be decrypted into plain text in the event the decryption key is lost or when the connection with the person who has the key is severed. There are several methods of key recovery, but the most widely used entrusts a decryption key or some equivalent key with a trusted third party. While key recovery methods increase convenience for the user, many avoid this for fear that it comprises the security of the cipher.

In Chapters 4 and 5, I present light-weight encryption algorithms, key distribution/recovery methods, and dynamic access control mechanisms for H-Ubi Comp environments.

3.3 Application and Service Layer

Several types of applications and services are found in the Application and Service Layer. This thesis applies HUC-HISF to two in particular, surveillance services and mobile IPTV services, and simulates the results. Accordingly, I provide the following description of these two services ahead of presenting the content of this thesis.

The details of my proposed enhancements to these two services may be found in the Application and Service Layer section of Chapter 7.

3.3.1 Surveillance

As the Air Force Research Laboratory researched their surveillance system, they placed less emphasis on the nature of the dangerous activities that people do and more on understanding why they do certain things. The US Department of Homeland Security is conducting the Hostile Intent Project. In this project, DHS is researching a system that distinguishes changes in emotion or whether or not a terrorist is trying to hide something based on minute changes in facial expression that are difficult for the naked eye to discern. In an attempt to conceal his emotions, a terrorist may actually make an unnatural expression or act unnaturally. The research being conducted by the DHS attempts to discover these factors using a surveillance system.

Such surveillance systems take several forms. Recently, computer network technology has been grafted onto surveillance systems allowing high quality images to be transmitted over a network from any location and over any distance. The advantages of this technology are that it makes possible real-time monitoring, recording and replay of images from anywhere in the world.

These systems are also able to digitize camera imagery and search for previously defined patterns, analyze the position and patterns of objects, activate defense and quarantine systems, or notify security administrators in the event of an intrusion or accident. As these systems are based on attributes in image data, they typically store image data making it easier to quickly search for context and efficiently manage data. These systems are called intelligent surveillance systems.

The following describes the advantages of surveillance systems to which have been applied the aforementioned two technologies.

- The video transmission cable, power, and control cables can all be combined into one.
- As the video feed is digitalized and compressed, long distance transmission and high volume storage of data is possible.
- As the technologies can be applied without any change in output devices, no additional equipment is necessary.
- Searching and long-term storage is convenient since the data is saved.
- Also, because the data is saved in a digital format, it is more free of background noise and interference than conventional CCTV.

Just like conventional CCTV, these surveillance systems may be applied to the security objective of protecting from intrusion and theft. They may also be applied for the purposes of accident prevention, safety management, regulation compliance, and guarding from facilities damage.

3.3.2 Mobile IPTV

Television service providers transmit video services to users through IP networks. IPTV is a TV service made more advanced than conventional TV by computer networking technology, specifically IP. IPTV offers the following advantages.

- High quality audio and video reception creates a high quality viewing experience
- Unlike conventional TV which simply received audio and video signals and displayed them on the television screen, information is now sent and received in both directions, allowing, for example, a user to search for information about the product he is currently viewing.
- In addition to real-time broadcasts, viewers can view saved Video-On-Demand (VOD) whenever they want.

With mobile IPTV, users can connect to their home TV using a cell phone, notebook, or smart phone, stream audio and video from their TV, and freely watch whatever broadcasts, video files, MP3 files, or any media they own, anywhere, any time.

Table 3.2 displays the requirements of mobile IPTV [LKCRL11].

Table 3.2 Requirements for mobile IPTV

context	requirements
Service	• Defines multimedia content, codecs, and meta data that takes into consideration the mobile environment • Supports a variety of protocols • Supports user and terminal mobility
Terminal	• Detects link properties in a wireless region • Provides service according to the performance of the receiving terminal • Provides a multi-interface
Network	• Guarantees that transmitters are authenticated and that content received is appropriate • Manages user profiles • Supports seamless service by following the terminal as it moves
Quality of Service (QoS)	• Network QofS technology for processing per-class, per-flow traffic • End-to-end signaling that reflects changes in bandwidth and terminal performance • Quality assessment functionality
Security	• Security service for service access control • Security for content backup; management of data distribution and tracking • Terminal security such as management of software downloads

Chapter 4. Advanced mCrypton: Light-weight Crypto Algorithm for HUC-HISF

Wireless mesh networking plays an important role in the next-generation wireless communication systems and is attracting significant interest as a low-cost networking platform to support ubiquitous broadband access in the context of home networking, enterprise networking and so on. As wireless mesh networks become more ubiquitous, the concerns for designing devices and applications suitable for such environment are also increasing. However as ubiquitous computing technology requires low-cost, low-power, and lightweight platforms, existing cryptographic algorithms can hardly be implemented under such resource constraints. Thus, the most promising candidate for security in such applications must be compact and efficient cryptographic algorithms.

The block cipher mCrypton [LK05], a light-weight version of Crypton [Li99], was designed with these constraints in low-cost ubiquitous computing devices such as RFID tags or sensors in wireless sensor networks in mind. Extremely efficient in resource usage and power consumption, mCrypton can be directly integrated into hardware or implemented in the software run on tiny processors embedded in low-cost products. mCryton is a 64-bit block cipher with 12 rounds and variable key sizes of 64 bits, 96 bits and 128 bits. mCrypton is known to be strongly resistant against differential and linear attacks.

In this chapter, I show that 8-round mCrypton with 128-bit key is vulnerable to related-key rectangle attacks. First, I describe how to construct two related-key truncated differentials on which the 7-round related-key rectangle distinguisher is based and then I exploit it to attack 8-round mCrypton. This attack requires 2^{46} dada and 2^{46} time complexities, which is faster than exhaustive search. This is the first known cryptanalysis for mCrypton. My result shows that real applications employing 8-round mCrypton may be broken due to the insecurity of the underlying block cipher.

Related work. There has been no security analysis of mCrypton published in the literature, prior to my cryptanalytic results. However, the related-key rectangle attack that has been used to analyze mCrypton in this chapter is well known to be a powerful cryptanalytic tool for block ciphers. The first introduction of this kind of attack was published in ACISP 2004 to conduct a security analysis of SHACAL-1 [KKHLH04]. Since its introduction, it has been used to analyze popular block ciphers AES [BDKR05, HKLP05, KHP07] and KASUMI [BDKA05] as well as many earlier block ciphers [DKK06, KKLLS04, LKHSL08, Lu09, LU08, LKKDR06, LKKDD06, LLK06, Wa07]. Recently, variants of this kind of attack, namely the related-key boomerang attack and related-key amplified boomerang attack[1], have been applied to several block ciphers including AES [BDKR05, GL08] and MISTY [LKHLSHL08].

Organization of the chapter. This chapter is organized as follows. In Section 4.1 and Section 4.2, I offer a brief description of mCrypton and related-key rectangle attacks,

[1] Note that the related-key amplified boomerang and rectangle attacks are both chosen plaintext attacks, while the related-key boomerang attack is a chosen plaintext and adaptive chosen ciphertext attack.

respectively. I present a related-key rectangle attack on 8-round mCrypton in Section 4.3. I conclude this chapter in Section 4.4

4.1 Description of mCrypton

In this section, I introduce notations used in this chapter and briefly describe mCrypton.

4.1.1 Notations

The following notation will be used throughout this chapter.

- A 64-bit data consists of sixteen 4-bit nibbles $\{a_0, a_1, \ldots, a_{15}\}$ and is internally represented as a *4×4* nibble array as follows :

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} A_r[0] \\ A_r[1] \\ A_r[2] \\ A_r[3] \end{pmatrix} = \begin{pmatrix} A_c[0] & A_c[1] & A_c[2] & A_c[3] \end{pmatrix} \tag{4.1}$$

  where $A_r[i]$ and $A_c[i]$ are the *i*-th row and column of *A*, respectively.
- A^t : transposition of an array *A*.
- $f \circ g$: composition of functions *f* and *g*.
- $X^{<<k}$: left rotation of a 16-bit word *X* by *k*-bit positions.
- $\cdot$, $\oplus$: bit-wise logical operations for AND and XOR, respectively.

4.1.2 mCrypton

mCrypton encrypts data blocks of 64 bits with 64, 96 or 128-bit key by iterating a round function 12 times. The round function of mCrypton consists of four basic steps as follows:

- **Nonlinear Substitution** γ . This step consists of nibble-wise substitutions on a $4 \time 4$ array using four 4-bit S-boxes, S_i, ($0 \le i \le 3$).

Table 4.1 S-boxes, Si ($0 \le i \le 3$)

S_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_0	4	15	3	8	13	10	12	0	11	5	7	14	2	6	1	9
S_1	1	12	7	10	6	13	5	3	15	11	2	0	8	4	9	14
S_2	7	14	12	2	0	9	13	10	3	15	5	8	6	4	11	1
S_3	11	0	10	7	13	6	4	2	12	14	3	9	1	5	15	8

For a 4-nibble word $a = (a_0, a_1, a_2, a_3)$ from the *i*-th row (or column), $\gamma_i(a)$ is operated as follows:

$$\gamma_i(a) = (S_i(a_0), S_{i+1}(a_1), S_{i+2}(a_2), S_{i+3}(a_3)) \tag{4.2}$$

Thus, γ can be defined for 4×4 data array *A* by

$$\begin{aligned} \gamma(A) &= (\gamma_0(A_c[0]), \gamma_1(A_c[1]), \gamma_2(A_c[2]), \gamma_3(A_c[3])) \\ &= (\gamma_0(A_r[0]), \gamma_1(A_r[1]), \gamma_2(A_r[2]), \gamma_3(A_r[3]))^t \end{aligned} \tag{4.3}$$

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \xrightarrow{\gamma} \begin{pmatrix} S_0(a_0) & S_1(a_1) & S_2(a_2) & S_3(a_3) \\ S_1(a_4) & S_2(a_5) & S_3(a_6) & S_0(a_7) \\ S_2(a_8) & S_3(a_9) & S_0(a_{10}) & S_1(a_{11}) \\ S_3(a_{12}) & S_0(a_{13}) & S_1(a_{14}) & S_2(a_{15}) \end{pmatrix}$$

Note that $S_2 = S_0^{-1}$, $S_3 = S_1^{-1}$, and $\gamma_i(a) = \gamma_0(a^{16-4i})^{4i}$.

- **Bit Permutation** (π). This step mixes each column of a 4×4 array A using column permutation π_i for each column *I* ($0 \le i \le 3$):

$$\pi(A) = (\pi_0(A_c[0])\pi_1(A_c[1])\pi_2(A_c[2])\pi_3(A_c[3])) \tag{4.4}$$

Each π_i is defined by

$$b = \pi_i(a) \Leftrightarrow b_j = \bigoplus_{k=0}^{3}(m_{i+j+k \ mod \ 4} \bullet a_k) \tag{4.5}$$

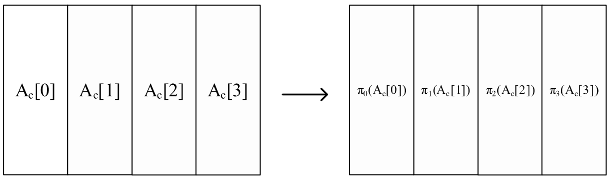


Figure 4.1 The column-wise bit permutation π

where a column $a = (a_0, a_1, a_2, a_3)^t$, a column $b = (b_0, b_1, b_2, b_3)^t$, $m_0 = 1110_2$, $m_1 = 1101_2$, $m_2 = 1011_2$, and $m_3 = 0111_2$. Note that π is an involution permutation, i.e., $\pi = \pi^{-1}$.

- **Column-to-Row Transposition** τ. It moves the nibble at the (*i*,*j*)-th position to the (*j*,*i*)-th position, i.e., $B = \tau(A) \Leftrightarrow b_{ji} = a_{ij}$. So, $\tau^{-1} = \tau$.
- **Key Addition** σ. $B = \sigma_K(A)$ is defined by $B_r[i] = A_r[i] \oplus K[i]$ $(0 \le i \le 3)$ where $K = (K[0], K[1], K[2], K[3])$ is a round key.

Each round function of mCrypton applies the γ, π, τ and σ steps in order and is defined for round key K_i by

$$\rho_{K_i} = \sigma_{K_i} \circ \tau \circ \pi \circ \gamma \tag{4.6}$$

So, the encryption transformation E_K of mCrypton under master key, *K*, consists of an initial key addition, σ_0, ρ repeated twelve times, and a final output transformation, E_K, defined as

$$E_K = \phi \circ \rho_{K_{12}} \circ \rho_{K_{11}} \circ \ldots \circ \rho_{K_2} \circ \rho_{K_1} \circ \sigma_{K_0} \tag{4.7}$$

where $\phi = \tau \circ \pi \circ \tau$. Note that the output transformation, π, can be incorporated into the final round as $\phi \circ \rho_{K_{12}} = \tau \circ \pi \circ \tau \circ (\sigma_{K_{12}} \circ \tau \circ \pi \circ \gamma) = \sigma_{K_{eq}} \circ \tau \circ \gamma$ where $K_{eq} = \phi(K_{12})$ is a equivalent key.

Key Scheduling. mCrypton supports three key sizes : 64 bits, 96 bits and 128 bits.

In this section, however, I focus on the 128-bit key version of the mCrypton that is composed of 12 rounds. It consists of two stages: round key generation through nonlinear S-box transformation in which the key variables update through simple rotations (word-wise rotation and bitwise rotation within word).

Let $K=\{K[i]\}_i^7=(K[0],K[1]\cdots K[7])$ be the master key, where *K*[*i*] represents the *i*-th 16-bit key word in *K*. Let *C*[*i*] be the round constant for round *i*. Each round constant *C*[*i*] consists of four identical nibbles, i.e., $C[i]=0xc_ic_ic_ic_i$, where c_i is generated by x_i in $GF(2^4)$ defined by the irreducible polynomial $f(x)=x^4+x+1$, that is, $c_0=1, c_1=2, \cdots, c_4=3, c_5=6, \cdots$, etc. Let $U=U[i]_{i=0}^7$ be a key register for state update in the encryption key schedule.

To generate round keys, the key register *U* is first initialized with *K* and then encryption round keys are computed for round $r=0,1,\cdots,12$ as :

$$T \leftarrow S(U[0])\oplus C[r],\ T_i \leftarrow T \bullet Mi(0\le i\le 3) \tag{4.8}$$

$$K_r \leftarrow (U[1]\oplus T_0, U[2]\oplus T_1, U[3]\oplus T_2, U[4]\oplus T_3) \tag{4.9}$$

$$U \leftarrow (U[5],U[6],U[7],U[0]^{\square 3},U[1],U[2],U[3],U[4]^{\square 8}) \tag{4.10}$$

where the S-box operation on a word in the key schedule is performed nibble-wise with the same S-box S_0, M_0 = 0xf000, M_1 = 0x0f00, M_2 = 0x00f0, and M_3 = 0x000f.

4.2 The Related-Key Rectangle Attack

In 2004 the related-key rectangle attack was first introduced by Kim et al. to analyze the SHA-1 based block cipher SHACAL-1 [KKHLH04]. Since then, it has been widely used as a cryptanalytic tool to evaluate the security of block ciphers such as AES [BDKR05, HKLP05, KHP07] and KASUMI [BDKA05]. In this section, I describe how to make the related-key rectangle distinguisher used in the attack.

I assume that an *n*-bit block cipher $E:\{0,1\}^k\times\{0,1\}^n\rightarrow\{0,1\}^n$ is divided into $E=E^1\circ E^0$, denoted $E_K=E_K^1(E_K^0(P))$, where *P* is an *n*-bit plaintext, *K* is a *k*-bit secret key, and E^0, E^1 and *E* are all permutations on *n* bits for each *k*-bit secret key. The related-key rectangle attack exploits various related-key differentials to make its distinguisher:

- related-key differentials $\alpha\rightarrow\beta$ for E^0 with probability p_β, i.e.,

$$Pr_{X,K}[E_K^0(X)\oplus E^0_{K\oplus\Delta K^*}(X\oplus\alpha)=\beta]=p_\beta, \tag{4.11}$$

- related-key differentials $\gamma\rightarrow\delta$ for E^1 with probability q_γ, i.e.,

$$Pr_{X,K}[E_K^1(X)\oplus E^1_{K\oplus\Delta K'}(X\oplus\gamma)=\delta]=q_\gamma, \tag{4.12}$$

where ΔK^* and $\Delta K'$ are non-zero key differences chosen by the attacker. If $\hat{p}\cdot\hat{q}>2^{-n/2}$ where $\hat{p}=\sqrt{\sum_\beta p_\beta^2}$, $\hat{q}=\sqrt{\sum_\gamma q_\gamma^2}$, the attacker can make a related-key rectangle distinguisher as follows:

1. Collect *m* pairs of (P,P^*) with difference α and *m* pairs of (P',P'^*) with difference α, where P, P^*, P' and P'^* are encrypted with the keys *K*, K^*, *K'* and K'^*, respectively, resulting in their ciphertexts C, C^*, C' and C'^* (here, key relations are $K^*=K\oplus\Delta K^*$, $K'=K\oplus\Delta K'$ and $K'^*=K\oplus\Delta K^*\oplus\Delta K'$).
2. Compute the number of ciphertext quartets satisfying

$$C \oplus C' = C^* \oplus C'^* = \delta . \tag{4.13}$$

In Step 1, about $m \cdot p_\beta$ pairs of (P, P^*) and $m \cdot p_\beta$ pairs of (P', P'^*) will satisfy the related-key differentials $\alpha \to \beta$ for *E*^{0} under the key difference ΔK^*. Thus, I have about $m^2 \cdot p_\beta^2$ quartets satisfying the related-key differentials for *E*^{0}. Moreover, I get $E_K^0(P) \oplus E_{K'}^0(P') = \gamma$ with probability 2^{-n} under the assumption that the intermediate encrypted values are uniformly distributed over all possible values. Once I have $E_K^0(P) \oplus E_{K^*}^0(P^*) = E_{K'}^0(P') \oplus E_{K'^*}^0(P'^*) = \beta$ (with probability p_β^2) and $E_K^0(P) \oplus E_{K'}^0(P') = \gamma$ (with probability 2^{-n}), it holds that $E_{K^*}^0(P^*) \oplus E_{K'^*}^0(P'^*) = \gamma$ with probability 1. Since each of the pairs $(E_K^0(P), E_{K'}^0(P'))$ and $(E_{K^*}^0(P^*), E_{K'^*}^0(P'^*))$ satisfies the related-key differentials $\gamma \to \delta$ for *E*^{1} with probability q_γ, for each β and γ about $m^2 \cdot p_\beta^2 \cdot q_\gamma^2 \cdot 2^{-n}$ quartets are expected to satisfy Eq. (4.13). Therefore, the expected number of right quartets (satisfying Eq. (4.13)) is about

$$\sum_{\beta,\gamma} m^2 \cdot p_\beta^2 \cdot q_\gamma^2 \cdot 2^{-n} = m^2 \cdot 2^{-n} \cdot \hat{p}^2 \cdot \hat{q}^2 . \tag{4.14}$$

On the other hand, for a random cipher the expected number of right quartets is about $m^2 \cdot 2^{-2n}$, as it requires a *2n*-bit filtration. Thus, $\hat{p} \cdot \hat{q} > 2^{-n/2}$ must hold for the related-key rectangle distinguisher to work.

4.3 Related-Key Rectangle Attack on 8-Round mCrypton

In this section, I first describe a 7-round related-key rectangle distinguisher of mCrypton and then exploit it to attack an 8-round mCrypton with 128-bit key.

The following notation is used throughout my attack.

- $K_0, K_0^*, K_{0'}, K_{0'}^*$: whitening keys generated from master keys K, K^*, K', K'^*, respectively.
- $K_i, K_i^*, K_{i'}, K_{i'}^*$: subkeys of round *i* generated from master keys K, K^*, K', K'^* , respectively.
- *a*: a fixed nonzero nibble value.
- *b*: output difference of S-box for fixed input difference *a*.
- *: a variable and unknown nibble.
- $\Delta K^*, \Delta K', \Delta P^*, \Delta I'$: particular differences described in Figs. 4.2 and 4.3.
- $\Delta T, \Delta O$: particular difference set described in Figure. 4.3.
- $E_K(\cdot)$: 8-round mCrypton encryption with key *K*.
- $E_K^0(\cdot)$: 4-round mCrypton encryption from round 1 to round 4 with key *K*.
- $E_K^1(\cdot)$: 3-round mCrypton encryption from round 5 to round 7 with key *K*.

4.3.1 7-Round Related-Key Rectangle Distinguisher

Figures. 4.2 and 4.3 show my two related-key truncated differentials with probability 1 to form my 7-round related-key rectangle distinguisher. If the master key difference is ΔK^* (resp., $\Delta K'$), then the subkey difference in rounds 1-4 (resp., 5-7) is $\Delta K_0^*, \Delta K_1^*$, ΔK_2^*, ΔK_3^* and ΔK_4^* (resp., $\Delta K_5'$, $\Delta K_6'$ and $\Delta K_7'$) described in Figure. 4.2 (resp., Figure. 4.3).

Our first 4-round differential on *E*^{0}. Let K, K^*, K' and K'^* be four keys with difference $\Delta K^* = K \oplus K^* = K' \oplus K'^*$ and P, P^*, P' and P'^* be four plaintexts with difference $\Delta P^* = P \oplus P^* = P' \oplus P'^*$, where the plaintexts P, P^*, P' and P'^* are encrypted under E^0_K, $E^0_{K^*}$, $E^0_{K'}$ and $E^0_{K'^*}$, respectively. Then (P, P^*) and (P', P'^*) both follow the 4-round related-key truncated differential described in Figure. 4.2.

ΔP^*

Figure 4.2 The first related-key truncated differential for rounds 1-4 (*E*^{0}) of mCrypton

Our second 3-round differential on *E*^{1}. A similar argument can be applied to my second related-key truncated differential for *E*^{1}. Let K, K^*, K' and K'^* be four keys with difference $\Delta K' = K \oplus K' = K^* \oplus K'^*$ (in order to satisfy the two key differences ΔK^* and $\Delta K'$ I need to set $K^* = K \oplus \Delta K^*$, $K' = K \oplus \Delta K'$ and $K'^* = K \oplus \Delta K^* \oplus \Delta K'$).

If $E^0_K(P) \oplus E^0_{K'}(P') = E^0_{K^*}(P^*) \oplus E^0_{K'^*}(P'^*) = \Delta I'$, then $(E^0_K(P), E^0_{K'}(P'))$ and $(E^0_{K^*}(P^*), E^0_{K'^*}(P'^*))$ both follow the 3-round related-key truncated differential described in Figure. 4.3. Note that the output difference of this 3-round differential is one of the elements in ΔT. In Figure.4.3, *b* is an unknown variable which can be one of *7* elements since the *b* is the output difference of the S-box for a given input difference *a*.

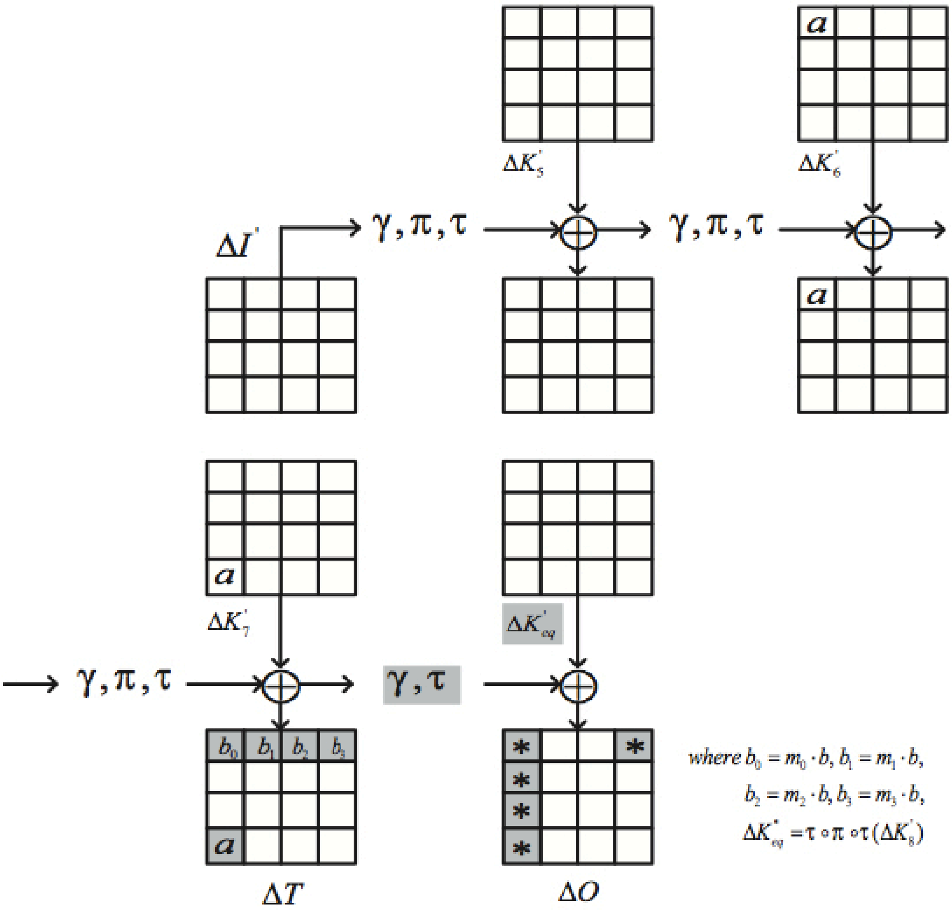


Figure 4.3 The second related key truncated differential for rounds 5-7 (E^1) of mCrypton

Our 7-round rectangle on $E^1 \circ E^0$. As stated above, these two related-key truncated differentials allow us to make a 7-round related-key rectangle distinguisher that has a relatively high probability. In order to compute the probability of this distinguisher I need the following two assumptions A_1 and A_2.

- A_1 : The key quartet (K, K^*, K', K'^*) is related as follows;

$$K \oplus K^* = K' \oplus K'^* = \Delta K^* = (\mathbf{0}, \mathbf{0}, \mathbf{0}, \alpha, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}), \qquad (4.15)$$

$$K \oplus K' = K^* \oplus K'^* = \Delta K' = (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \alpha'); \qquad (4.16)$$

where $\mathbf{0} = (0_4, 0_4, 0_4, 0_4)$, $\alpha = (a, 0_4, 0_4, 0_4)$, $\alpha' = (a_L, a_R, 0_4, 0_4) \in \{0,1\}^{16}$, $a = (a_1, a_2, a_3, a_4)$, $a_L = (0, 0, 0, a_1)$, $a = (a_2, a_3, a_4, 0)$, $0_4 = (0, 0, 0, 0) \in \{0,1\}^4$.

- A_2 : A plaintext quartet (P, P^*, P', P'^*) is related as follows;

$$P \oplus P^* = P' \oplus P'^* = \Delta P^* = (\mathbf{0}, \mathbf{0}, \alpha, \mathbf{0})^T \qquad (4.17)$$

Let I, I^*, I' and I'^* be $E^0_K(P)$, $E^0_{K^*}(P^*)$, $E^0_{K'}(P')$ and $E^0_{K'^*}(P'^*)$, respectively. Then the probability that $I \oplus I^*$ is equal to $I' \oplus I'^*$ is about $(2^{-16} \cdot 2^{-2})^2 \cdot \cdot 2^{16} + (2^{-16} \cdot 2^{-3})^2 \cdot 6 \cdot 2^{16} = \frac{3}{2} \cdot 2^{-22}$.

This is due to the differentials that the active S-box with input difference *a* and the other four active S-boxes can produce. Since the π and τ are linear layers, the π and τ of the last round can be ignored in computing the probability (see Figure. 4.3). Thus $\hat{p} = \sqrt{\frac{3}{2} \cdot 2^{-22}}$.

In order to concatenate the first related-key truncated differential to the second one, I need to compute the probability that $I \oplus I'$ is equal to $I^* \oplus I'^*$ as $\Delta I'$: under the assumption that the intermediate encrypted values are uniformly distributed over all possible values, the probability that $I \oplus I' = I^* \oplus I'^* = \Delta I'$ is 2^{-64} under the condition that $I \oplus I^* = I' \oplus I'^*$. This leads to the probability that

$$I \oplus I^* = I' \oplus I'^* \text{ and } I \oplus I' = I^* \oplus I'^* = \Delta I' \tag{4.18}$$

is $\frac{3}{2} \cdot 2^{-22} \cdot 2^{-64} = \frac{3}{2} \cdot 2^{-86}$, and thus $E^1_K(I) \oplus E^1_{K'}(I')$ and $E^1_{K^*}(I^*) \oplus E^1_{K'^*}(I'^*)$are in the difference set ΔT with probability $\frac{3}{2} \cdot 2^{-86}$ (note that my second related-key truncated differential for E^1 is 1, leading to $\hat{q} = 1$). On the other hand, the same statement can be applied to a random cipher with probability $(2^{-64} \cdot 7)^2 \approx 2^{-123}$, as the number of elements in ΔT is *7*. The quartet (P, P^*, P', P'^*) satisfying (4.18) is called a right quartet.

4.3.2 Key Recovery Attack on 8 Rounds mCrypton

Using the 7-round related-key rectangle distinguisher my 8-round attack recovers 5 bytes of each subkey for $K_{eq}, K^*_{eq}, K_{eq'}, K^*_{eq'}$ whose nibble positions are marked as * on ΔO depicted in Figure. 4.3, where $K_{eq} = \phi(K_8)$, $K^*_{eq} = \phi(K^*_8)$, $K_{eq'} = \phi(K_{8'})$, and $K_{eq'} = \phi(K_{8'})$ (recall that $\phi = \tau \circ \pi \circ \tau$). Since the keys K, K^*, K' and K'^* are related, the number of possible key quartets is 2^{40}. In order to understand the relations of the round keys of round 8, refer to Figure. 4.4.

The basic idea of my attack is as follows. Let (P, P^*, P', P'^*) be right quartet, (C, C^*, C', C'^*) be the corresponding ciphertext quartet and $D_k(\cdot)$ be a partial one round decryption with *k*, where *k* is a 5-byte key candidate of round 8. I guess a 5-byte key quartet (k, k^*, k', k'^*) and check that $D_k(C) \oplus D_{k'}(C') \in \Delta T^5$ and $D_{k^*}(C^*) \oplus D_{k'^*}(C'^*) \in \Delta T^5$, where ΔT^5 is a set of 5 gray nibbles described in ΔT of Figure. 4.3. If the number of ciphertext quartets passing the above test is more than an appropriate threshold, I consider the guessed key quartet as the right one.

Attack algorithm.

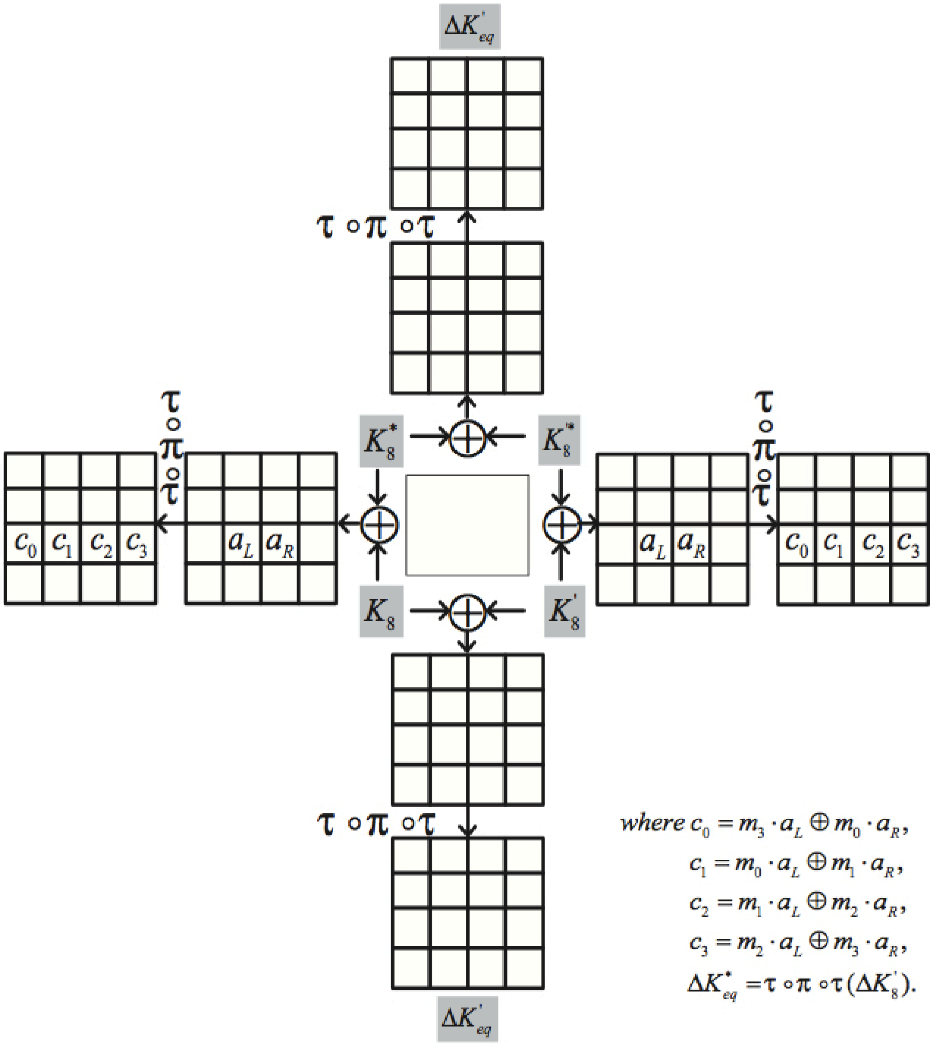
Input: Two pools of 2^{44} plaintext pairs.

Output: 5-byte key quartet of round 8.

---

1. Collect 2^{44} plaintext pairs (P_i, P^*_i) and 2^{44} plaintext pairs (P'_j, P'^*_j) with $P_i \oplus P^*_i = P'_j \oplus P'^*_j = \Delta P^*$. Encrypt the P_i, P^*_i, P'_j , P'^*_j with the keys K, K^*, K' and K'^{*}, respectively, to obtain their ciphertexts C_i, C^*_i, C'_j and C'^*_j . Keep all the obtained ciphertexts in a table.

2. Check that $C_i \oplus C'_j \in \Delta O$ and $C^*_i \oplus C'^*_j \in \Delta O$ for all *i,j*. Discard all the ciphertext quartets that do not satisfy this test.
3. Guess a 5-byte key quartet (k, k^*, k', k'^*) for round 8.
   3.1. For all ciphertext quartets $(C_i, C^*_i, C'_j, C'^*_j)$ passing the test of Step 2, check that $D_k(C_i) \oplus D_{k'}(C'_j) \in \Delta T^5$ and $D_{k^*}(C^*_i) \oplus D_{k'^*}(C'^*_j) \in \Delta T^5$.
   3.2. If the number of quartets $(C_i, C^*_i, C'_j, C'^*_j)$ passing Step 3.1 is greater than or equal to 3, output the guessed key quartet (k, k^*, k', k'^*) as the right key quartet of round 8. Otherwise, repeat Step 3.



$\Delta K'_{eq}$
$\tau \circ \pi \circ \tau$
K^*_8
K'^*_8
K_8
K'_8
c_0 c_1 c_2 c_3
a_L a_R
a_L a_R
c_0 c_1 c_2 c_3
$\tau \circ \pi \circ \tau$
$\tau \circ \pi \circ \tau$
$\tau \circ \pi \circ \tau$
where $c_0 = m_3 \cdot a_L \oplus m_0 \cdot a_R$,
$c_1 = m_0 \cdot a_L \oplus m_1 \cdot a_R$,
$c_2 = m_1 \cdot a_L \oplus m_2 \cdot a_R$,
$c_3 = m_2 \cdot a_L \oplus m_3 \cdot a_R$,
$\Delta K^*_{eq} = \tau \circ \pi \circ \tau(\Delta K'_8)$.
$\Delta K'_{eq}$

Figure 4.4 Differential Property of 4 related keys for rounds 1-8 of mCrypton

Security analysis. Since the attack requires two pools of 2^{44} plaintext pairs and memory space for their ciphertext pairs, the data complexity of this attack is 2^{46} related-key chosen plaintexts and the memory complexity is $5 \cdot 2^{48} (= 2^{46} \cdot 20)$ bytes.

Step 2 requires 2^{44} searches of 2^{44} ciphertext pairs, which can be done efficiently by sorting the ciphertext pairs, $(C_{j'}, C^*_{j'})$'s by $C_{j'}$'s. In Step 2, the test requires a 88-bit filtration (this is due to the fact that $C_i \oplus C'_j \in \Delta O$ and $C^*_i \oplus C'^*_j \in \Delta O$ with probability $2^{-88} (= 2^{-11 \cdot 4 \cdot 2})$ for a wrong quartet $(C_i, C^*_i, C_{j'}, C^*_{j'})$), and thus the expected number of ciphertext quartets passing the test of Step 2 is about $7(\approx 2^{88} \cdot (\frac{3}{2} \cdot 2^{-86} + 2^{-88}))$ (here, $2^{88} \cdot \frac{3}{2} \cdot 2^{-86} = 6$ ciphertext quartets passing the test are expected to be right quartets due to my 7-round related-key rectangle distinguisher). Using this expected number of quartets I can estimate the time complexity of Step 3, i.e., Step 3 requires about $2^{41} (\approx 2^{40} \cdot 7 \cdot 4 \cdot \frac{1}{8} \cdot \frac{1}{2})$ 8-round mCrypton encryptions on average. Hence, the time complexity of this attack is dominated by Step 1, and thus this attack requires about 2^{46} 8-round mCrypton encryptions.

The success rate of the attack is computed as follows. The probability that for the right key quartet there exist at least 3 quartets passing the test of Step 3.1 is about 0.94 $(\approx \sum_{i=3}^{2^{88}} \binom{2^{88}}{i} (\frac{3}{2} \cdot 2^{-86})^i (1 - \frac{3}{2} \cdot 2^{-86})^{2^{88}-i})$, while the probability that a wrong key is outputted by the attack algorithm is $2^{-67} (\approx 2^{40} \cdot \sum_{i=3}^{2^{88}} \binom{2^{88}}{i} (2^{-123})^i (1 - 2^{-123})^{2^{88}-i})$. Therefore, the success rate of this attack is about $0.94 (\approx 0.94 \cdot (1 - 2^{-67}))$.

4.4 Summary

mCrypton was designed for security in resource-constrained applications, such as low-cost RFID tags and sensors in USN. It is based on the structure of Crypton with some improvements in software and hardware efficiency under resource-restricted environments. In this chapter, however, I have analyzed the security of 8-round mCrypton with a 128-bit key against a related-key rectangle attack. According to my result, this attack requires *2^{46}* data and time complexity of equal magnitude, *2^{46}*. As the first known cryptanalytic result on mCrypton, it is worthwhile to apply this attack to other block ciphers and to study simple key scheduling algorithms which may be resistant to this kind of attack.

Chapter 5. Security Protocol Issues for HUC-HISF

In this chapter, I discuss security protocol issues for HUC-HISF. First, I propose a session key distribution mechanism for fast secure handover in wireless mobile networks. The proposed mechanism is based on the stream control transmission protocol wherein a mobile node actively changes its IP address without a loss of connection. When a mobile node moves between different access routers, the required session key at a new access router is distributed through the tunnel previously established between the previous access router and the new access router. Due to the reduced key distribution time, the mobile node achieves a secure and seamless handover. The provided performance analysis offered in this chapter demonstrates how the proposed mechanism reduces signaling costs relative to existing mobility protocols. In addition, the proposed mechanism reduces handover latency such that the reduced amount of packet loss stabilizes handover performance for real-time applications.

Second, I propose both a security-enhanced KR protocol and construct a privacy-enhanced KR protocol based on that security-enhanced KR protocol in order to protect users' location privacy. In mobile communication environments, Wireless Authentication and Key Establishment (WAKE) protocols are essential for secure information transmission. KR protocols, including WAKE protocols, can enable an authorized third party to gain access to encrypted message data under certain lawful circumstances. However, due to the limited resources of mobile hardware, it is not easy to construct KR protocols for mobile communication environments which are both secure and strongly preserve privacy.

Third, I import software products with network security features such as intrusion detection systems (IDS) and a firewall in order to solve the security problems that occur in the networks such as the Internet. In this chapter, I have designed and constructed a general simulation environment for a network security model composed of multiple IDSs and a firewall, which coordinate by means of a contract net protocol (CNP) for the effective detection of an intrusion. CNP, the methodology for efficient integration of computer systems in heterogeneous environments such as distributed systems, is essentially a collection of agents that cooperate to resolve a problem. In the network security model, each model of the simulation environment is hierarchically designed by discrete event system specification (DEVS) formalism. The purpose of this simulation is to evaluate the characteristics and performance of CNP architecture in order to shorten the inference cycle phases of the intrusion detection expert system.

The remainder of this chapter is structured as follows. Section 5.1.1 provides an overview of SCTP and its enhanced handover procedure and then Section 5.1.2 introduces the proposed fast session key distribution mechanism. Section 5.2.1 briefly introduces KR systems and Section 5.2.2 describes previous KR systems used in the WAKE protocol of the ASPeCT project. I propose a security-enhanced KR-WAKE protocol in Section 5.2.3, and a second protocol guaranteeing location privacy of mobile users as well as security in Section 5.2.4. Section 5.3.1 presents results of the about network system modeling that was constructed by network simulation. Section 5.3.2 describes the coordination of the contract net protocol. Finally, I conclude this chapter in Section 5.4.

5.1 Effective Key Pre-Distribution for Fast and Secure Handover

As mobile technologies provide advanced access service to the Internet, security issues for mobile networks have increased dramatically. Several mobility protocols have been proposed. For instance, as an IP layer protocol, Mobile IPv6 has been introduced to allow a mobile node to move around the Internet without a loss of connection [JPA04]. Since the costs of mobility support for Mobile IPv6 are high, other IP based mobility protocols such as Fast Mobile IPv6 and Hierarchical Mobile IPv6 have been introduced [Ko05, SCMB05]. Moreover, some mobility protocols that extend the transport layer for supporting mobile networks have recently been introduced. Apart from various mobility protocols, security mechanisms for mobility protocols have also been introduced. Unfortunately, however, most of these new protocols have merely applied those security mechanisms used in legacy networks which do not well reflect the properties of mobile networks.

From the perspective of seamless handover technology, the main issue is how to reduce handover latency as a mobile node moves among different networks. Mobile IPv6 is a fundamental protocol. In other words, Mobile IPv6 results in long handover latency when the mobile node attaches to another network. This problem is accentuated in the case of latency sensitive services such as multimedia streaming services, voice services, etc. To address such unacceptable latency, extensions of Mobile IPv6 have been proposed. Among them, the fast handover mechanism defined in [Ko05] promises reduced handover latency and packet loss via the tunnel established between access routers. The main feature of this mechanism is the packet-forwarding tunnel. When the mobile node receives a wireless link-layer signal from the new access router, the mobile node generates the new address and then informs the previous (current) access router that it will attach to the new access router. The previous access router makes a tunnel for packet forwarding with the new access router. Accordingly, the mobile node can attach to the new access router with reduced handover latency and packet loss. As a transport layer mobility protocol, stream control transmission protocol (SCTP) provides the dynamic address configuration for mobile nodes. The mobile node can add and delete its communication address with its corresponding node by using SCTP. This feature provides a simple way to change the mobile node's communication address and is easily extended to the fast handover procedure.

For several years, some methods have been proposed to provide secure mobile communication on IPv6 networks. However, current security mechanisms for secure mobile communications do not reflect the properties of mobile networks. For example, in [KC04], a fast session key distribution mechanism introduced to reduce the handover latency, the mobile node receives previously used session key from the previous access router as the mobile node moves to the new access router. The mechanism obviously reduces the authentication and handover latency due to the reduced key distribution time, however it exposes the session key to a spoofing attack.

In this chapter, I propose an effective session key distribution mechanism that reflects the properties of mobile networks. In the proposed mechanism, SCTP is used to establish its communication session with corresponding nodes. In addition, the session key is securely distributed when a mobile node moves to a new access router. The mobile node establishes its secure communication session with the new access router based on the pre-distributed session key.

5.1.1 Stream control transmission protocol for handover managements

Stream control transmission protocol (SCTP) is a reliable transport layer protocol that operates on top of connectionless IP protocol. SCTP provides end-to-end multi-sessions [SXMSSTRKZP00, SSO02, St07]. In other words, SCTP allows more than one active address for both the data source and destination. In addition, these addresses can be added and deleted dynamically while maintaining sessions. Note that this dynamic address configuration was originally developed as a backup feature that provides fault tolerance manners in the event that one communication path link fails. In SCTP based communication, each address of the mobile node is considered as a path for data transmission to the corresponding node. Actually, only one address, called the primary address, is used in data transmission even though other addresses are available. This allows another address to be used by the dynamic address configuration as defined in [SXTMK07]. This feature provides a concise handover management scenario 2. As shown in Figure 5.1, a dynamic address configuration procedure consists of three steps [St07, SXTMK07]. First, the mobile node sends an ADD-IP Address Configuration (ASCONF) message including a new address to its corresponding node when the mobile node obtains the new address. Then, the corresponding node adds the included address in the ASCONF message to its communication address pool for the mobile node. As a result, the ASCONF ACK message is sent to the mobile node. When the mobile node needs to change the new address to the primary address to communicate with the corresponding node, the mobile node sends the ASCONF message including the newly set primary address. As the corresponding node receives this message, it recognizes that the communication address with the mobile node needs to be changed. The corresponding node updates its communication address. Accordingly, packets sent to the mobile node have the new primary address set as their destination address. In the case that the mobile node does not need to maintain the old address, the mobile node sends the ASCONF message along with the old address to its corresponding node and the corresponding node deletes the old address.

[2] Handover refers to a mobile node changing its wireless address as its actual location changes, e.g. as it moves to another access network.

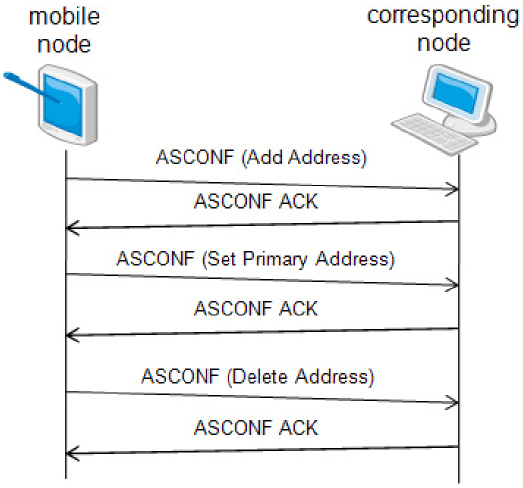


Figure 5.1 Dynamic address configuration procedure in SCTP

Studies that use the dynamic address configuration for handover management have recently been published recently. In [KCL04], the authors have introduced a soft handover mechanism based on SCTP. The mechanism uses the dynamic address configuration when a mobile node informs its new address to the corresponding node. As the corresponding node recognizes the new address, it uses this address as a primary address for communicating with the mobile node. This simple mechanism reduces the complexity of handover management compared to Mobile IPv6. Note that a mobile node operating on Mobile IPv6 has to send its new location to all corresponding nodes by sending binding update messages and these procedures are all known to be high cost procedures. Thus, the SCTP based handover mechanism introduced in [KCL04] results in reductions of handover latency and cost. In [HT07], the authors have focused on the multi-path transmission feature of SCTP and adopted it to improve handover performance. They have concluded that multi-path transmission helps to reduce packet re-transmission and re-ordering problems. Other studies on handover performance demonstrate that SCTP based handover mechanisms provide obvious improvements in performance compared to Mobile IPv6 [HNH05, ZS07]; however, these mechanisms have not addressed the packet loss problem. For instance, packets sent to a previous address will be lost as the mobile node changes its primary address from the previous one to new one. Moreover, security issues have not been considered in such SCTP-based handover mechanisms. One major security issue in mobile networks is session key distribution for a mobile node. Due to its mobile nature, session keys for mobile nodes must be distributed from the key distribution server (KDS) every time that the mobile node moves to another access network. Accordingly, seamless handover (providing low handover latency) and secure communication (providing authentication materials) for mobile nodes ought to be considered simultaneously. The AAA (Authentication, Authorization, and Accounting) architecture is currently believed to provide and control effective network access control mechanisms in wireless mobile networks. Thus I propose implementing KDS within the AAA server that manages all network access control for mobile nodes in its domain [LCGJM07, KKG07].

In order to address both of seamless handover and secure communication in wireless mobile networks, I propose an effective session key distribution mechanism. The proposed mechanism prevents packet loss issues, which previous SCTP-based mechanisms have not considered [KCL04, HT07]. Moreover, the proposed mechanism also enables the mobile node to actively obtain a session key through a tunnel established between access routers as the mobile node moves from one to the next.[3]

5.1.2 Effective session key distribution mechanism

In this section, I present an effective session key distribution mechanism that provides low handover latency and cost. In the proposed mechanism, a mobile node uses signaling defined in SCTP to establish its communication session with the corresponding nodes [SXTMK07]after which a tunnel is established between the previous and new access routers in order for the previous router to distribute the session key to the next [Ko05].

5.1.2.1 Signaling for establishing communication session

As the mobile node receives the wireless link-layer signaling from a new access router, the mobile node sends a Router Solicitation for Proxy Advertisement (RtSolPr) message to its current access router as defined in [Ko05]. As a result, the mobile node receives the Proxy Router Advertisement message from the current access router. The mobile node obtains a new address that will be used in the new access router and then generates the new care-of address (CoA) based on the new address obtained from the PrRtAdv message. This newly generated CoA is sent to the corresponding node. In other words, the mobile node actively sends the ASCONF message including both the new CoA and setting primary address information to its corresponding node to inform it that henceforth the mobile node will use this address as a communication session address. Accordingly, the mobile node can immediately begin to receive data packets sent from the corresponding node as soon as the mobile node connects to the new access router.

Figure 5.2 shows the proposed handover procedure where the mobile node actively establishes its communication session with the corresponding node by sending the ASCONF message. In the following steps, I describe the proposed handover procedure in detail.

[3] When the mobile node changes its location by handover, the mobile node has to obtain its new session key to perform its security association with the new access router.

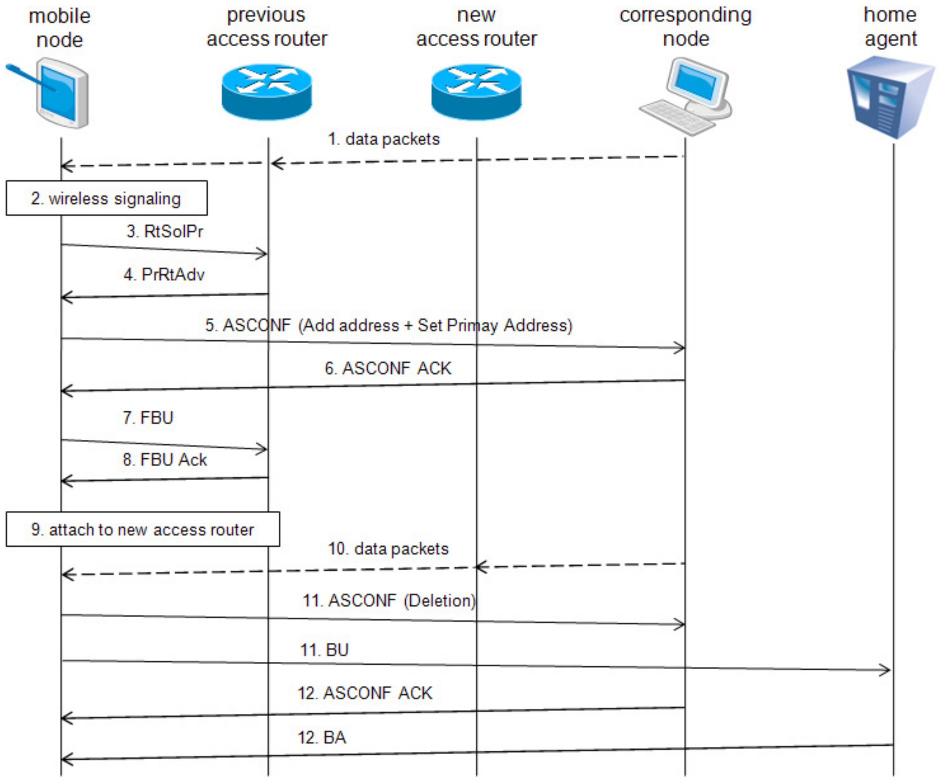


Figure 5.2 Proposed handover procedure

1. The data packets sent from the corresponding node to the mobile node are delivered to the current mobile node's address through the previous (current) access router.
2. The mobile node receives the wireless link-layer signals from the new access router as the mobile node moves toward to the new access router.
3. The mobile node sends the RtSolPr message to the previous access router to obtain the new address that will be used for generating the new CoA address.
4. The previous access router replies with the PrRtAdv message including the new address for the mobile node.
5. The mobile node sends the ASCONF message including the new CoA indicating the primary address to the corresponding node.
6. The corresponding node replies with the ASCONF ACK message upon changing its communication session address with the mobile node.
7. Prior to connecting to the new access router, the mobile node sends the Fast Binding Update (FBU) message to the previous access router as defined in [Ko05].
8. Subsequently, the previous access router sends the FBU Ack message back to the mobile node. The previous access router on receiving the FBU message acknowledges that the mobile node has moved to the new access router. Accordingly, the previous access router can send the session key for the mobile node used within the previous access network. Note that the detailed session key distribution procedure is described in the following sub-section.

9. The mobile node connects to the new access router because the ASCONF ACK sent from the corresponding node confirms that the corresponding node now knows where the mobile node has moved.
10. Data packets sent from the corresponding node to the mobile node are delivered to the new mobile node's address through the new access router.
11. Now connected to the new access router, the mobile node sends messages to both its home agent and corresponding node. The first one is the binding update (BU) message as described in [JPA04] and the second one is the ASCONF message indicating the deletion of the old address. Note that this deletion for the old address is optional.
12. The mobile node receives the replies (BA message and ASCONF ACK message) sent respectively from its home agent and corresponding node in response to the BU message and ASCONF message .

Through the described handover procedure, the mobile node obtains its new CofA and promptly preserves its communication session as it moves from one access router to the next.

5.1.2.2 Key distribution

In the previous sub-section, I described the proposed handover procedure. Here, I concentrate on key distribution for the mobile node. As a mobile node accesses a new router, it must establish a new session key in order to protect its communication session. Standard protocols in the past have required the mobile node to request a session key with every movement. Accordingly, as the mobile node moves to a new network, it needs to obtain a session key from the KDS. Note that in my proposed scheme, I apply the AAA architecture to the task of network control, [LCGJM07, KKG07], and embed the KDS within this control architecture. A key distribution procedure that does not reflect the properties of mobile networks causes long authentication latency thus increasing handover latency. In the proposed mechanism, the mobile node obtains the session used key in the previous access network when it moves to the new access network.

In the proposed key distribution procedure, the previous access router recognizes the movement of mobile node based on the FBU message. When the previous access router receives the FBU message, the previous access router forwards the session key to the new access router through the tunnel established between them. The mobile node can then use this session key forwarded from the previous access router to the new access network. Accordingly, the mobile node does not need to request a new session key from the KDS. The reduced session key distribution procedure is more effective when the mobile node frequently moves across different access networks and the distance increases between the mobile node and the KDS.

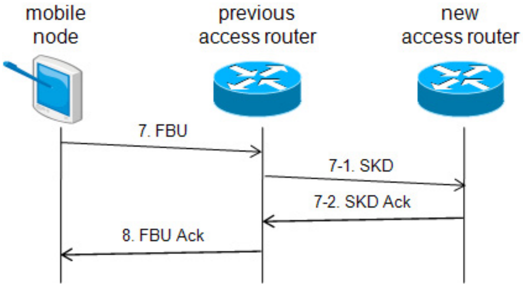


Figure 5.3 Fast key distribution procedure

Figure 5.3 shows the proposed fast key distribution procedure. As the previous access router receives the FBU message sent from the mobile node, it sends its session key, which has been used for protecting communication session with the mobile node, to the new access router by sending the session key distribution (SKD) message. Once the new access router obtains the session key it can then use this session key when the mobile node attaches to its access network. As described in [KC04], an attacker can perform a spoofing attack if the distribution of the session key does not support the confidentiality. Accordingly, the SKD and SKD Ack messages are encrypted between the access routers using a long-term pre-shared key. Note that the access routers are connected by wired network infrastructures and they normally have enough computation power for encryption and decryption.

5.2 Privacy-Enhanced Key Recovery

Currently, I live in the Third Generation (3G) mobile communication environments, such as CDMA2000[OP98, Bu97] and W-CDMA (UMTS)[Bl99]. These cutting edge technologies have changed my life styles and have also prompted much interest in the field of mobile security. These environments offer nice advantages such as video calling, wide data bandwidth, global roaming, but on the downside, my location can easily be traced without my knowledge or permission. In other words, while there are advantages, there are also many security issues.

One such security issue is related to the adoption of Key Recovery (KR) schemes. For the purposes of social security and national security, national governments allow legal eavesdropping on a criminal suspect under a judge-issued warrant. KR is a cryptography mechanism that allows authorized people (users, officers of an organization, and government officials), under certain conditions, to decrypt encrypted messages with the help of information supplied by trusted parties who hold special data related key recovery. And these special data-recovery keys are not normally the same as those used to encrypt and decrypt the data, but rather provide means of determining the data encryption/decryption keys [DB96]. Thus national governments have shown much interest in the application of key recovery and especially the lawful interception of encrypted communication messages for investigating serious crimes and for national security in mobile communication environments.

In this section, I focus on enhancing the security and privacy of KR scheme in mobile communication environments. Normally mobile communication systems are composed of four entities, including mobile users, network operators (NO’s), value-added service providers (VASP's), and service providers (SP's). Mobile communication systems typically provide fundamental security features, such as confidentiality on the air interface, anonymity of user, and mutual authentication between mobile users and NO's/VASP's. In fact, a mobile user's location is often traced for VASP accounting purposes. However, in general I want to protect my location information as tracking a user's location or retrieving a user's location history without any approval would be a serious invasion of privacy.

Horn and *Preneel* proposed the Wireless Authentication and Key Establishment (WAKE) protocol for mutual authentication between a mobile user and a VASP [HP98] in the research project, Advanced Security for Personal Communications Technologies (ASPeCT) [ACT97] in 1998. In the following years, *Rantos* and *Mitchell* proposed a modified WAKE protocol which includes a Key Recovery (KR) feature [RM99]. They modified the user-to-VASP interface of [HP98] to provide a KR capability. In 2000, *Nieto et al.* reported some security flaws in *Rantos* and *Mitchell*'s protocol and proposed a modified KR enhanced WAKE protocol [NPBD00]. In the following year, *Kim* and *Lee* also improved security and efficiency for the protocol of *Nieto et al.* [KL01]. In *Kim* and *Lee*'s proposed scheme, I found a serious problem related to the public KR information (KRI) validation process on the VASP side. In hits section I offer the example of a *single rogue user attack* on *Kim* and *Lee*'s protocol and then introduce a solution to that protocol.

5.2.1 Definitions

Since the Escrow Encryption Standard (EES) was published in 1993, many researchers have studied KR systems. I first describe the following terminologies as in [NPBD00, KL01] for explaining KR systems.

- **Key Recovery Agent (KRA).** A trusted third party that performs KR in response to an authorized request.
- **Key Recovery Information (KRI).** An assortment of data that is needed by the KRA in order to complete a KR request, e.g. a session key encrypted under the KRA's public key.
- **Key Recovery Requestor (KRR).** An authorized entity that requests KR from the KRA. The KRR would usually be a LEA (Law Enforcement Agency) in possession of a valid warrant.
- **Interception Agent (IA).** An entity that acts in response to an authorized request for interception of a target identity by filtering out the communications traffic corresponding to the target identity. This function would usually be performed by NO's who act as a collector of KRI's[ETSI97, ETSI96].

5.2.2 Related Work

In this section, I introduce some protocols [HP98, RM99, NPBD00, KL01] and commonly used notation and definitions from [NPBD00, KL01] to describe these protocols.

5.2.2.1 ASPeCT Project's WAKE Protocol [HP98]

The ASPeCT Project introduced the WAKE protocol for the UMTS environment and this protocol is the first authentication and key establishment protocol developed for wireless communications. The simplified protocol is described in Figure 5.4. A detailed description can be found in [HP98, ACT97]. In fact, the protocol shown in figure 5.4 is one of two variants of the ASPeCT protocol for user-to-VASP interface, which is called the B-variant protocol. Another variant, the so-called C-variant protocol, is an extended version of the B-variant protocol and is expanded to include on-line trusted third parties (TTPs). For brevity I describe the B-variant and mainly consider key recovery within this protocol; however the same solutions can be applied to the C-variant protocol. I used the following notations to describe WAKE protocol.

Table 5.1 Notations for WAKE Protocol

Notation	Description
A	the identity of the user
B	the identity of the VASP
TTP_A	the identity of the TTP that A trusts
g	a generator of a finite group
r_A	a random nonce chosen by A
r_B	a random nonce chosen by B
K_{AB}	a secret session key established between A and B
K_A^{-1}	A's private signature key
A_{Cert}	public key certificate of A that is signed by TTP_A
B_{Cert}	public key certificate of B that is signed by TTP_A
b	the private key component of the public-private key-agreement key pair of B
g^b	the public key component of the public-private key-agreement key pair of B
$\{m\}K_A^{-1}$	the message m signed by A with his private signature key K_A^{-1}
$\{m\}K_{AB}$	the symmetric encryption of a message m using the session key K_{AB}
h,h_1,h_2,h_3	one-way hash functions

Initial Setup:

$$K_{AB} = h_1(r_B, g^{br_A})$$

WAKE Protocol:

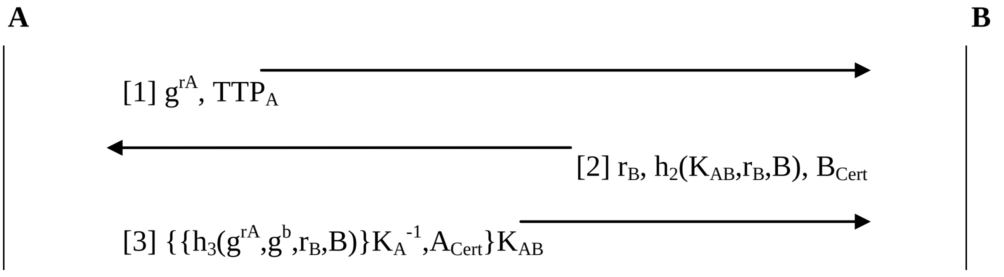

A
B
[1] g^{rA}, TTP_A
[2] r_B, $h_2(K_{AB},r_B,B)$, B_{Cert}
[3] $\{\{h_3(g^{rA},g^b,r_B,B)\}K_A^{-1},A_{Cert}\}K_{AB}$

Figure 5.4 The ASPeCT WAKE protocol

5.2.2.2 WAKE KR Protocol of *Rantos* and *Mitchell* [RM99]

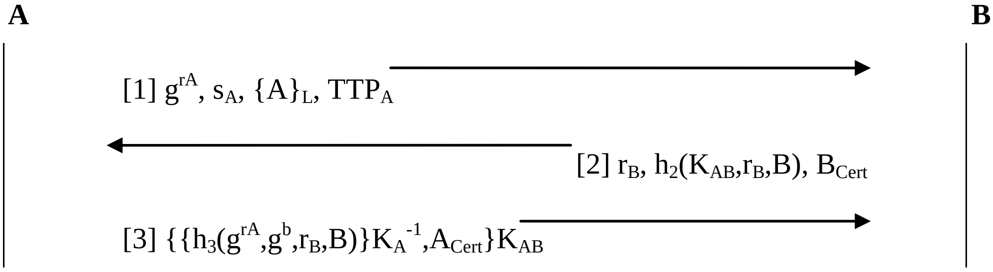
Rantos and *Mitchell* proposed adding a key recovery feature to the ASPeCT WAKE protocol. The enhanced WAKE KR Protocol is described in figure 5.5.

Initial Setup:

$$K_{AB} = h_1(r_B,g^{brA})$$

$$A: r_A=f(w_A,s_A),\ L=(g^{xA})^{rA}$$

WAKE Protocol:



$[1]\ g^{rA}, s_A, \{A\}_L, TTP_A$

$[2]\ r_B, h_2(K_{AB},r_B,B), B_{Cert}$

$[3]\ \{\{h_3(g^{rA},g^b,r_B,B)\}K_A^{-1},A_{Cert}\}K_{AB}$

Figure 5.5 WAKE KR protocol

Rantos and *Mitchell* slightly modified the method of computing A’s random nonce, r_A as shown below;

$$r_A = f(w_A, s_A) \tag{5.1}$$

where f is a one-way function, s_A is a one-time random seed, and w_A is a secret value shared between A and KRA_A.

5.2.2.3 Modified WAKE KR Protocol of Nieto et al. [NPBD00]

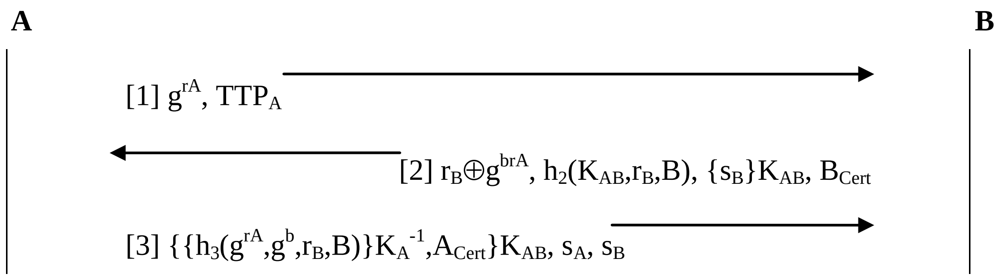
This protocol, proposed by *Nieto et al.*, resolves some security flaws inherent in *Rantos* and *Mitchell*’s WAKE KR protocol. They presented that the inclusion of $\{A\}_L$ in Token 1 was unnecessary. They also described how an impersonation attack could be mounted on the WAKE KR protocol in the case that w_A was a temporary secret. Furthermore, A cannot be sure whether the protocol tokens are being exchanged with B or KRA_B, since both B and KRA_B know b. Thus they proposed the modified WAKE KR protocol as shown in figure 5.6.

Initial Setup:

$$K_{AB} = h_1(r_B,g^{brA})$$

$$A: s_A=(w_A h(g^{rA})+r_A) \bmod q\ /\ B: r_B=f_B(w_B,s_B)$$

WAKE Protocol:



[1] g^{rA}, TTP_A

[2] $r_B \oplus g^{brA}$, $h_2(K_{AB}, r_B, B)$, $\{s_B\}K_{AB}$, B_{Cert}

[3] $\{\{h_3(g^{rA}, g^b, r_B, B)\}K_A^{-1}, A_{Cert}\}K_{AB}$, s_A, s_B

Figure 5.6 Modified WAKE KR protocol

5.2.2.4 Improved WAKE KR Protocol of Kim and Lee [KL01]

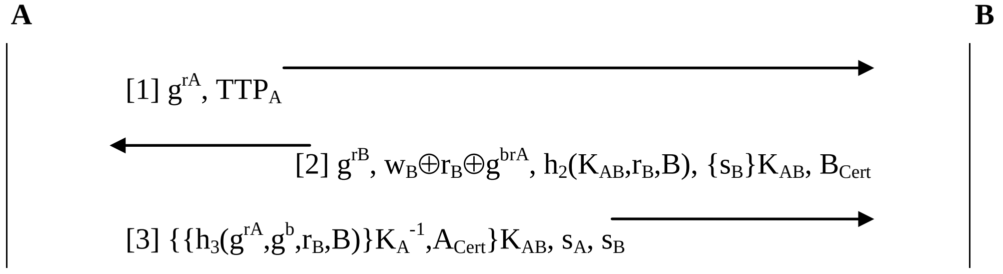
This protocol, which was proposed by *Kim* and *Lee*, improves the security of *Nieto et al.*'s modified KR enhanced protocol by adding the public KRI validation property in domain B. They noticed that in the event that B authenticates to A, a *public KRI validation property* cannot be applied in B's domain in the modified WAKE KR protocol. They also pointed out that the insertion of s_A, s_B, and $\{s_B\}K_{AB}$ may incur transmission and computation overhead, thus they modified it. The improved WAKE KR protocol of *Kim* and *Lee* is described in Figure 5.7.

Initial Setup:

$$K_{AB} = h_1(g^{brA+rB})$$

$$A\colon s_A=(w_A h(g^{rA})+r_A) \bmod q \;/\; B\colon s_B=(w_B h(g^{rB})+r_B) \bmod q$$

WAKE Protocol:



[1] g^{rA}, TTP_A

[2] g^{rB}, $w_B \oplus r_B \oplus g^{brA}$, $h_2(K_{AB}, r_B, B)$, $\{s_B\}K_{AB}$, B_{Cert}

[3] $\{\{h_3(g^{rA}, g^b, r_B, B)\}K_A^{-1}, A_{Cert}\}K_{AB}$, s_A, s_B

Figure 5.7 Improved WAKE KR protocol

In the description of the protocol, I use the following notations according to *Kim* and *Lee*'s paper [KL01]: p is a large prime, q is a prime with q|(p-1), and g is an element in the multiplicative group Z^*_p of order q. All operations are performed modulo p, except where otherwise noted. The KR mechanism consists of three stages as follows.

KRI Generation Phase:

Each entity A and B generates w_A and w_B respectively, and also shares them with KRA_A and KRA_B respectively. The value $\phi_A= g^{wA}$ and $\phi_B= g^{wB}$ are made publicly available. User A selects a random integer, r_A, computes $\mu_A=g^{rA}$, and calculates s_A as

$$s_A=(w_A h(g^{rA})+r_A) \bmod q. \tag{5.2}$$

Similarly the VASP B generates r_B, μ_B, and s_B.

KR Phase:

In A's domain, KRA_A first computes r_A as

$$r_A= s_A-w_A h(\mu_A) \bmod q, \tag{5.3}$$

and KRA_A computes $(g^b)^{rA}$ and $K_{AB} = h_1(g^{brA}g^{rB})$.

In B's domain, KRA_B first computes r_B as

$$r_B= s_B-w_B h(\mu_B) \bmod q, \tag{5.4}$$

and KRA_B computes g^{brA} from $w_B\oplus r_B\oplus g^{brA}$. Then KRA_B computes $K_{AB} = h_1(g^{rB}g^{brA})$.

Public KRI Validation Phase:

Given the public data μ_A, s_A, and A, a third-party monitor, V, can verify the integrity of the KRI fields generated by A by doing the following:

- obtain authentic public value ϕ_A
- compute $c'=h(\mu_A) \bmod q$
- conclude that the validation process is successful if and only if $g^{sA}=\phi^{c'A}\mu_A$

In B's case, the same procedure is applied.

5.2.2.4.1 Problem with the Improved WAKE KR Protocol

I found a security hole in the public KRI validation phase particularly in VASP B's domain of the improved WAKE KR protocol above. In the worst case scenario, a *single rogue user attack* is possible on B. In Token 2, if B sends a bogus value $w_B\oplus r'_B\oplus g^{brA}$ instead of $w_B\oplus r_B\oplus g^{brA}$ to user A, KRA_B may recover a fabricated session key K_{AB}(see Figure 4). For example, during the KR phase, KRA_B first computes r_B from $r_B=s_B-w_B h(\mu_B) \bmod q$ and then obtains $r_B\oplus r'_B\oplus g^{brA}$ rather than g^{brA} as

$$r_B\oplus r'_B\oplus g^{brA} =(w_B\oplus r_B)\oplus(w_B\oplus r'_B\oplus g^{brA}), \tag{5.5}$$

from $w_B \oplus r'_B \oplus g^{brA}$ using w_B , which he knows. Next, KRA_B may recover session key K_{AB}, $h_1((r_B \oplus r'_B \oplus g^{brA})g^{rB})$ instead of $h_1(g^{brA+rB})$. This attack is possible due to the false public KRI validation check. In B's domain, a third-party monitor, V, checks whether B sends a correct s_B and g^{rB} from $g^{sB} = \phi^{c'B}\mu_B$ using ϕ_B and c' which he knows. Consequently, that the problem lies in the fact that V does not check whether the r_B sent by B is correct

5.2.3 Security-Enhanced KR Protocol

First I propose a new WAKE KR protocol that improves on the previous protocols described in Section 5.2.2. In particular, I improve on *Kim* and *Lee*'s protocol by modifying the public KRI validation check in domain B.

5.2.3.1 Protocol Overview

As already seen in Section 5.2.2.4, *Kim* and *Lee*'s protocol has the problem that it does not provide a correct public KRI validation check in B's domain. However if I slightly modify the protocol, I can resolve this problem. The proposed protocol is described in Figure 5.8.

Initial Setup:

$$K_{AB} = h_1(w_B \oplus r_B, g^{brA})$$

$$A: s_A = (w_A h(g^{rA}) + r_A) \bmod q \ / \ B: s_B = (w_B h(w_B \oplus r_B) + r_B) \bmod q$$

WAKE Protocol:

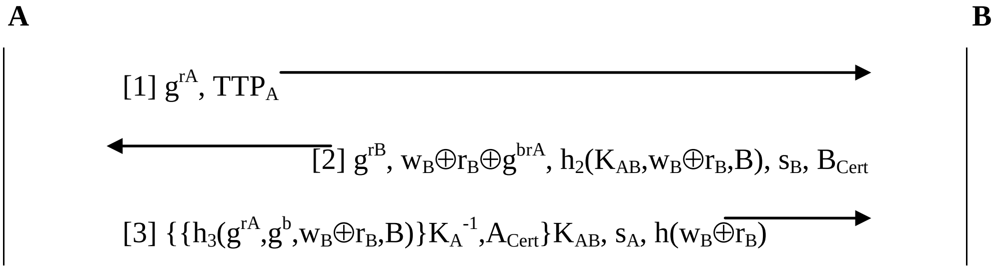

A
B
[1] g^{rA}, TTP_A
[2] g^{rB}, $w_B \oplus r_B \oplus g^{brA}$, $h_2(K_{AB}, w_B \oplus r_B, B)$, s_B, B_{Cert}
[3] $\{\{h_3(g^{rA}, g^b, w_B \oplus r_B, B)\}K_A^{-1}, A_{Cert}\}K_{AB}$, s_A, $h(w_B \oplus r_B)$

Figure 5.8 The proposed security-enhanced WAKE KR Protocol

KRI Generation Phase:

Each entity A and B generates w_A and w_B respectively, and also shares them with KRA_A and KRA_B respectively. The values $\phi_A = g^{wA}$ and $\phi_B = g^{wB}$ are made publicly available. The user A selects a random integer, r_A, computes $\mu_A = g^{rA}$, $c_A = h(g^{rA}) \bmod q$, and calculates s_A as

$$s_A = (w_A h(g^{rA}) + r_A) \bmod q. \tag{5.6}$$

The VASP B similarly generates r_B and μ_B except $c_B = h(w_B \oplus r_B) \bmod q$, and calculates s_B as

$$s_B = (w_B h(w_B \oplus r_B) + r_B) \bmod q, \tag{5.7}$$

where h is a one-way and collision free hash function.

KR Phase:

In A’s domain, KRA_A first computes r_A as

$$r_A= s_A-w_Ah(\mu_A) \bmod q. \qquad (5.8)$$

KRA_A computes $(g^b)^{rA}$ and calculates $w_B\oplus r_B$ from $w_B\oplus r_B\oplus g^{brA}$ and $K_{AB} = h_1(w_B\oplus r_B, g^{brA})$.

In B’s domain, KRA_B first computes r_B as

$$r_B= s_B-w_Bh(w_B\oplus r_B) \bmod q. \qquad (5.9)$$

KRA_B computes g^{brA} from $w_B\oplus r_B\oplus g^{brA}$. Then KRA_B computes $K_{AB} = h_1(w_B\oplus r_B, g^{brA})$.

Public KRI Validation Phase:

Given the public data μ_A, s_A, and A, a monitoring third party V can check the integrity of the KRI fields generated by A by doing the following:

- obtain authentic public value ϕ_A
- compute $c'_A=h(\mu_A) \bmod q$
- resolve the validation process as successful if and only if $g^{sA}=\phi^{c'A}\mu_A$

However, in B’s case, other procedure is applied.

Given the public data μ_B, s_B, $h(w_B\oplus r_B)$, and B, a monitoring third party V can check the integrity of the KRI fields generated by A, by doing the following:

- obtain authentic public value ϕ_B
- compute $c'_B=h(w_B\oplus r_B) \bmod q$
- resolve the validation process as successful if and only if $gs_B=\phi c'_B\mu_B$

5.2.4 Privacy-Enhanced KR Protocol

In this section, I propose a new protocol for ensuring mobile users’ location privacy based on the proposed security-enhanced WAKE KR protocol in the previous section. Location privacy [AMSW97, FJKP95] is an important requirement as the location information of mobile users should be untraceable to unauthorized parties, including the network operators in mobile communications. In relation to this, some solutions, including temporary pseudonym (TP) methods [KFJP96, KRJ98, KYPK05, BM07], MIXes [PPW91] and so on, have been proposed until now. Among these solutions, TP method is based on the concept of trusted devices (TD) which confidentially store sensitive data (authentication keys, location information etc.) [KRJ98, KYPK05]. The basic idea of the TP method is using protecting mobile users’ real identity for protecting their location information. To this end, users would be assigned pseudonyms, or pseudo mobile subscriber identities (PMSI). As long as one of the users who is registered under a pseudonym is currently at a certain place, attackers cannot link the user’s real identity with the user’s present location.

5.2.4.1 Protocol Overview

I show the privacy-enhanced WAKE KR protocol using the above TP method, especially Kim et al.'s TP method [KYPK05]. Some additional notations used in this method and subsequent protocol descriptions are shown as follows;

Table 5.2 Notations for privacy-enhanced WAKE KR protocol

Notation	Description
TD_A	A's trusted device (TD), which is similar to TTP and binds the key to the identity (for simplicity, I did not include this in my protocol). However, TD_A can be connected and used only by user A for secure external computation and storing.
$PMSI_A$	the pseudonym identity of a mobile user A
K_A^{-1}, K_A	the signature key and verification key of A
K_{TDA}^{-1}	the signature key of TD_A
K_{ATD}	the shared secret key between A and TD_A

Initial Setup:

$$K_{AB} = h_1(w_B \oplus r_B,\ g^{brA})$$

$$\text{A: } s_A=(w_A h(g^{rA})+r_A) \bmod q \ /\ \text{B: } s_B=(w_B h(w_B \oplus r_B)+r_B) \bmod q$$

WAKE Protocol:

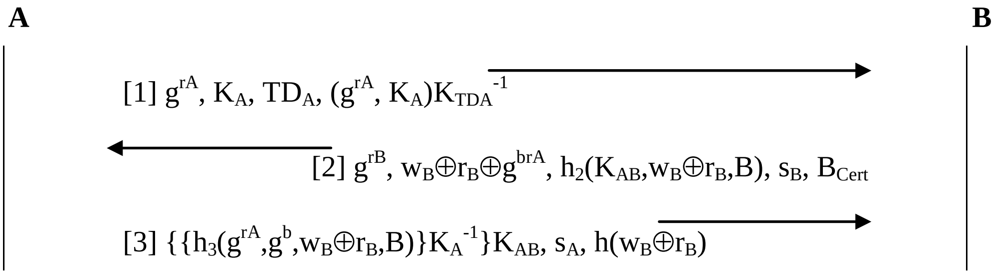

A
B
[1] g^{rA}, K_A, TD_A, $(g^{rA}, K_A)K_{TDA}^{-1}$
[2] g^{rB}, $w_B \oplus r_B \oplus g^{brA}$, $h_2(K_{AB}, w_B \oplus r_B, B)$, s_B, B_{Cert}
[3] $\{\{h_3(g^{rA}, g^b, w_B \oplus r_B, B)\}K_A^{-1}\}K_{AB}$, s_A, $h(w_B \oplus r_B)$

Figure 5.9 The proposed privacy-enhanced WAKE KR Protocol

KRI Generation Phase:

Each entity A and B generates w_A and w_B, and shares with KRA_A and KRA_B respectively. The value $\phi_A= g^{wA}$ and $\phi_B= g^{wB}$ are made publicly available. User A selects a random integer, r_A, computes $\mu_A=g^{rA}$, $c_A=h(g^{rA})$ mod q, and calculates s_A as

$$s_A=(w_A h(g^{rA})+r_A) \bmod q. \qquad (5.10)$$

User A additionally performs the following:

$$A \rightarrow TD: (PMSI_A, g^{rA})K_{ATD} \tag{5.11}$$

$$A \leftarrow TD: \{TD_A, g^{rA}, K_A, K_A^{-1}, (g^{rA}, K_A)K_{TDA}^{-1}\}K_{ATD} \tag{5.12}$$

Similarly B generates r_B, μ_B, $c_B=h(w_B \oplus r_B) \bmod q$, and calculates s_B as

$$s_B=(w_B h(w_B \oplus r_B)+r_B) \bmod q, \tag{5.13}$$

where h is a one-way, collision free hash function.

The following two phases are the same as the above protocol (see Section 5.2.4.1)

5.3 Security Simulation Model based on Contract Network Protocol

Given the recent growth of the Internet, intrusion incidents are becoming common events of life. Some of these incidents are simply out of innocuous curiosity. Some, however, are due to malicious attempts to compromise the availability of the information system or the integrity and privacy of the information itself. Despite the best efforts of the protocol designers, implementers, and system administrators, it is prudent to assume that attacks will occur and some, unfortunately, will succeed. Therefore, it is vitally important to develop means to automatically detect and respond to these attacks in real-time in order to maintain critical information services [JGSWWCW00]. I have designed and constructed the general simulation environment of network security model composed of multiple IDSs [Ba00, Am99] and a firewall [ZCC00, MSK99], coordinated by CNP [YHHMW98, Pa87], for the effective detection of the intrusion. Intrusion detection systems monitor system activities to identify unauthorized use, misuse, or abuse of computer and network systems. A firewall plays a vital role in network security, restricting access between the external and internal networks.

A network-based multiple IDSs, based on the theory of distributed systems, reduces system overloading by distributing jobs to agents and reduces detection time by selecting the best agent to detect an intrusion. Security models are made to coordinate in the multiple IDSs architecture for detection performance enhancement. Most of all, the effective allocation of tasks and coordination of agents is the most critical issue for achieving high performance in an agent-based cooperative design [SSM99]. Agents, as a new technology of distributed artificial intelligence (DAI), have become a new important issue of AI research as evidenced by the large volume of publications [HZZ99, BG98].

To allow effective coordination and control of tasks, CNP allocates agents to the tasks. In this approach, agents coordinate through contracts to accomplish a goal. Contracting involves an exchange of information among agents, an evaluation of the information, and a final agreement based on mutual selection. In other words, CNP selects the best agent to serve jobs by bidding and then the selected agent performs the jobs.

Three different types of modeling and simulation have been conducted. First, a rule-based expert system [Wi93, Ja99] is applied to an IDS model for detecting intrusions. Second, a CNP model is constructed with multiple IDSs. Using the model, the distributed IDSs and firewall are coordinated for better intrusion detection. Lastly, a model is constructed with multiple IDs and a CNP that exploits the rete algorithm for further speeding up the process of intrusion detection activities. The above models are defined by DEVS formalism [ZPK00, SC03], a well-grounded means of expressing discrete event models.

5.3.1 Network System Modeling

5.3.1.1 Target Network Structure

Figure 5.10 shows the structure of the target network that has three subnets: subnet_49, subnet_50 and subnet_53. The types of component models in the network are IDS, Firewall, Router and Gateway models. Each subnet has a Unix server, Linux server, Windows NT server, and etc. The IDS is loaded within each host and cooperates with other IDSs in detecting intrusions. These models are constructed based on DEVS formalism. DEVS formalism, developed by Zeigler, is a theoretical, well-grounded means of expressing hierarchical, modular discrete-event models.

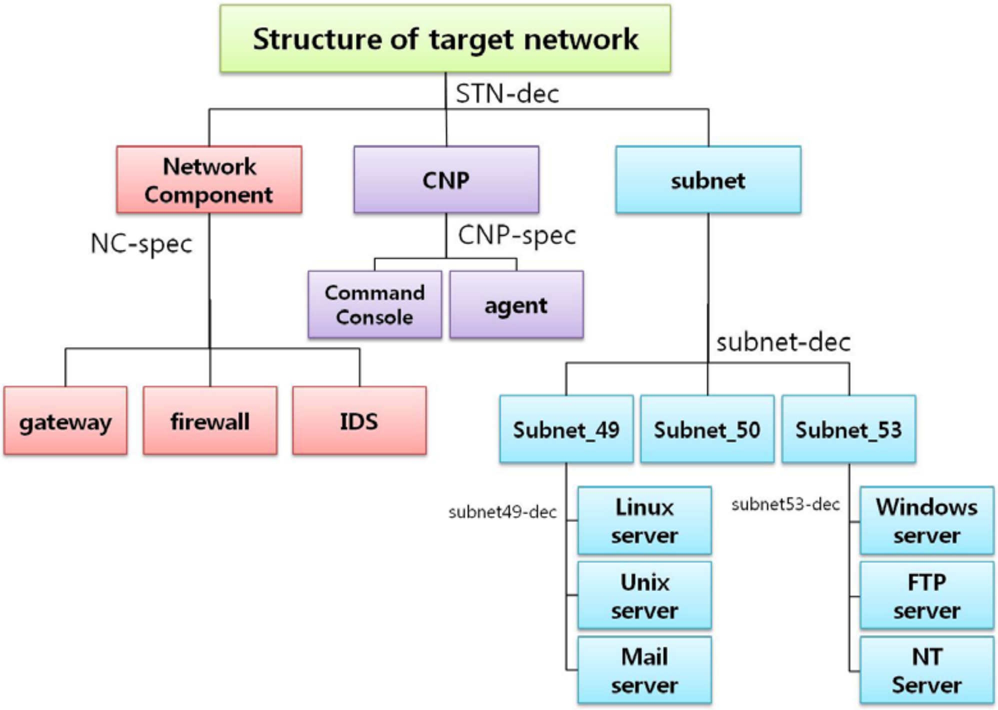


Figure 5.10 Structure of target network

5.3.1.2 Command Console Model

The contract net protocol was originally proposed as a tool for communication and control in a distributed problem solver. It provides a mechanism for agents to communicate and negotiate to solve distributed problems via contracts. A contract is a set of tasks to be accomplished. Agents announce tasks that they need and make bids to perform tasks announced by other agents. Next, agents evaluate bids and award contracts. Contract net protocol is essentially a collection of nodes that cooperates to resolve a problem.

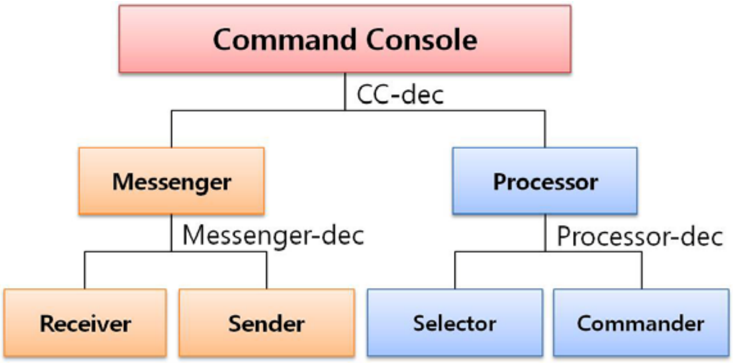


Figure 5.11 Structure of the Command Console mode

The Command Console model, which controls all IDSs models and the firewall model in the CNP, is comprised of two models, the Messenger model and the Process model. Messenger model is composed of a Receiver and a Sender model and manages the communication of messages. The Receiver model receives messages from IDSs and other network components. The Sender model sends the messages formed in the Selector or Commander model to a certain IDSs or IDSs by means of unicast, multicast, or broadcast. The Selector model in the Process model selects an intrusion detection system with bids collected from all IDSs. The Commander model determines the message types that regulate IDSs and the firewall according to the state of the Inner Network.

5.3.1.3 ID Model

Figure 5.12 shows the structure of the ID model. The ID model is divided into a Detector model, a Response_Generator model, and a Logger model.

The Detector model is composed of a Pattern_matcher and an Analyzer model. The Pattern_matcher model is a rule-based expert system that detects intrusions through a pattern matching procedure that compares packet data to rules. The Analyzer model is a statistical detection engine that detects intrusions by analyzing system logs and audits. The Response_Generator model determines responses according to the detection results of the Detector model and sends a message. The Logger model records all information of the detection procedure in the log file.

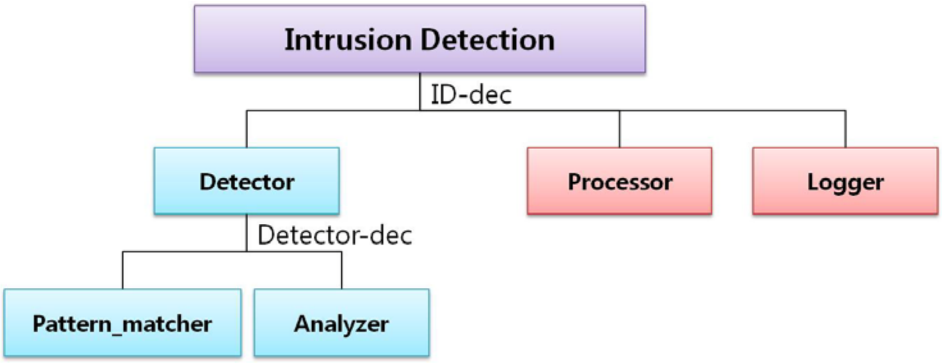


Figure 5.12 Structure of IDE model

The Detector model detects intrusions through state transitions. Figure 5.13 displays the state transition diagram of the Detector model. When packet data enters the input port, the state transition begins with an initial, or Passive state and transits to the Intrusion state that is a goal which may only be reached through the Vulnerable and Active attack states. When the Detector model reaches the Intrusion state, the intrusion is detected by the model. If the Detector model fails to detect an intrusion or if IDS overloading exceeds a predefined threshold value, the state transits to the Failed state and the Detector model requests another IDS to detect the intrusion [Pr01].

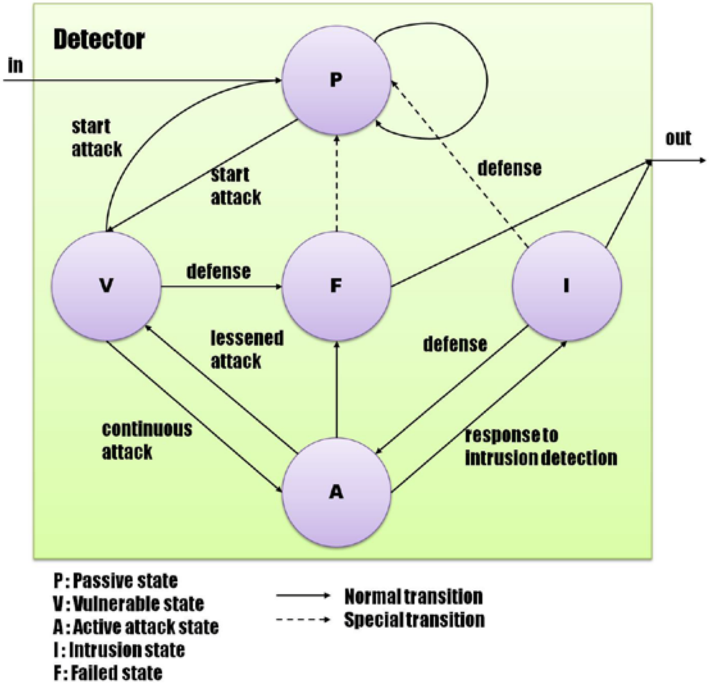


Figure 5.13 State transition diagram of detector model

A single event signature can be identified by analyzing a packet that contains one or more abnormal flags in the packet's header information. If the Detector model detects an intrusion, the state of Detector model transitions from the Passive state to the Intrusion state. Multiple event signatures can be defined by analyzing many packets as with a Denial of Service (DoS) attack. If the Detector model detects an intrusion by analyzing packets, the state of the Detector model transitions from the Passive state to the Intrusion state via the Vulnerable and Active attack states.

5.3.1.4 Firewall Model

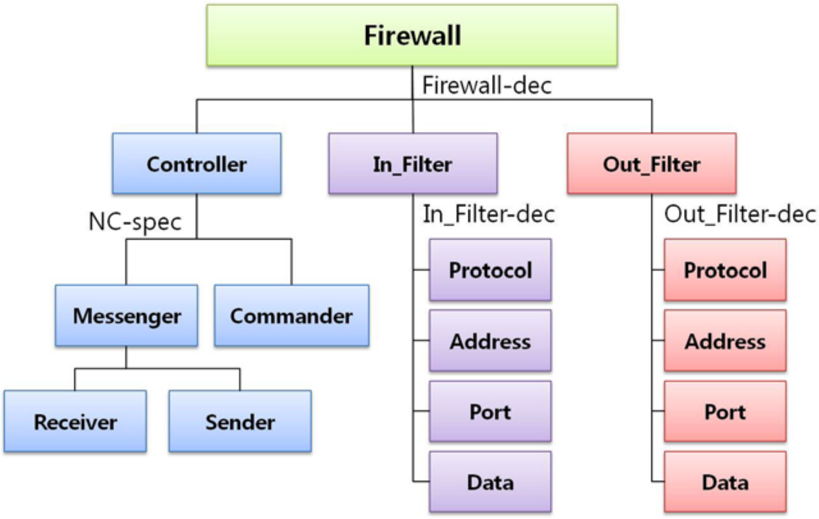


Figure 5.14 Structure of a Firewall model

Firewall models basically carry out the filtering of ingress and egress packets. If an IDS detects an intrusion, the Firewall model blocks the packets related to the intrusion and responds according to policies. Firewall models filter packets attempting to access the Command Console from an external network.

Figure 5.14 shows the structure of a Firewall model that has Controller, In_Filter, and Out_Filter models. The Controller model deals with all messages from the Command Console model. It is decomposed into Messenger and Commander models. The Messenger model manages all messages that come from the Command Console, In_Filter, and Out_Filter. The Commander model determines all activities of the Firewall model. The In_Filter model filters packets which pass from the external network to the internal network using four models: Protocol, Address, Port, and Data models. The Protocol model filters the protocol information found in packet headers and the Address model filters IP addresses. The Port model filters port information and the Data model carries out filtering with packet data. The Out_Filter model filters packets that pass from the internal network to external networks and has the same sub-model as the In_Filter model.

5.3.2 Coordination of CNP

5.3.2.1 Coordination in the Contract Net Protocol

When a simulation begins and packets enter the internal network, the Command Console sends a bid message to all IDS agents. After receiving a bid message, each agent makes a bid and sends a bid_data message. The Command Console selects an IDS agent to detect the intrusion using a selection algorithm with bid_data and then sends an award message to the selected IDS agent. After receiving the award message, the selected agent prepares to detect intrusions and waits for packet_data messages. The Command Console copies packet data to a packet_data message and sends it. The selected IDS agent detects intrusions according to packet_data. If the state of the Detector model becomes the Failed state, the agent sends an announcement message to the Command Console, which upon receiving it, repeats the coordination cycle. If the Detector model detects an intrusion, the agent sends an intrusion message to the Command Console followed by an intrusion_data message. The Command Console then forwards the intrusion and intrusion_data messages to the Firewall which in turn sends broadcast and broadcast_data messages, which include intrusion data, to all agents. The Command Console and IDS agent repeat this cycle.

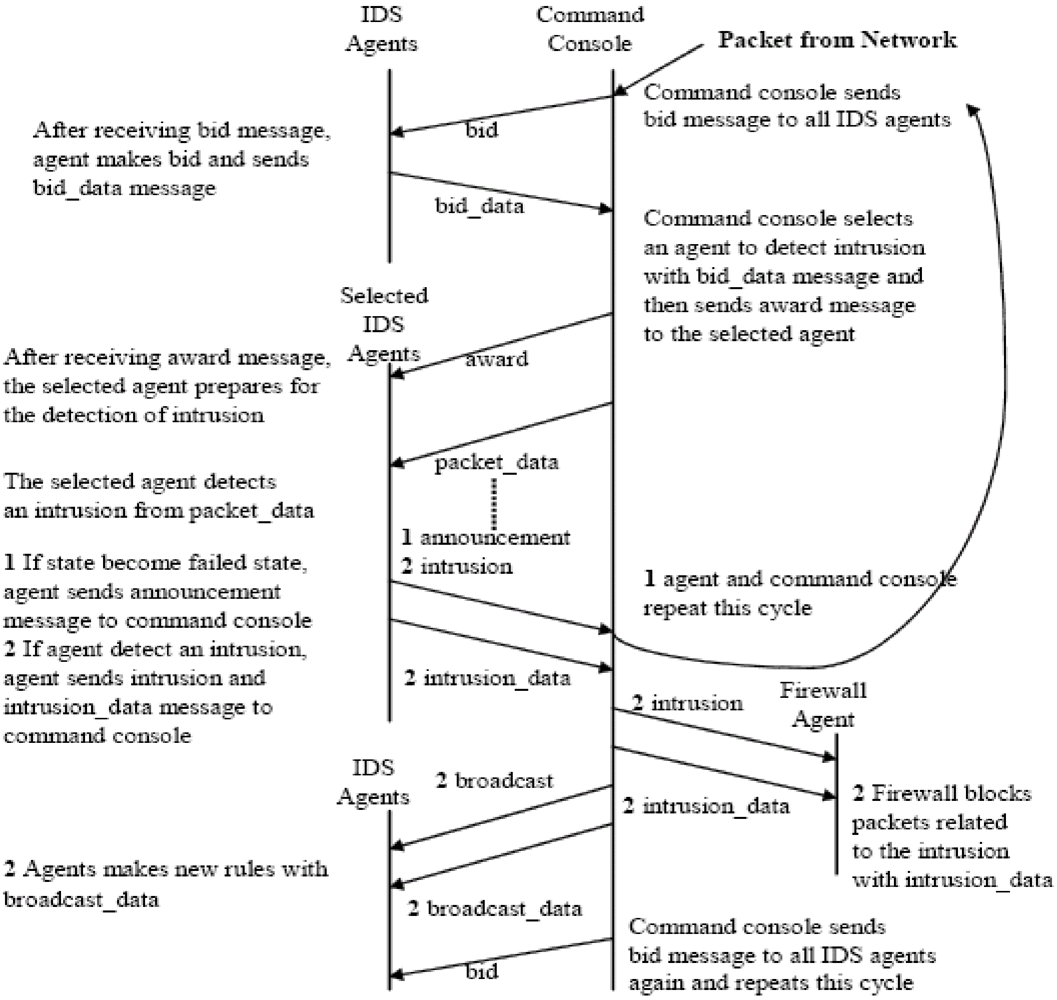

IDS Agents
Command Console
Packet from Network
Command console sends bid message to all IDS agents
After receiving bid message, agent makes bid and sends bid_data message
bid
bid_data
Command console selects an agent to detect intrusion with bid_data message and then sends award message to the selected agent
Selected IDS Agents
After receiving award message, the selected agent prepares for the detection of intrusion
award
packet_data
The selected agent detects an intrusion from packet_data
1 announcement
2 intrusion
1 If state become failed state, agent sends announcement message to command console
2 If agent detect an intrusion, agent sends intrusion and intrusion_data message to command console
1 agent and command console repeat this cycle
2 intrusion_data
2 intrusion
Firewall Agent
IDS Agents
2 broadcast
2 intrusion_data
2 Firewall blocks packets related to the intrusion with intrusion_data
2 Agents makes new rules with broadcast_data
2 broadcast_data
Command console sends bid message to all IDS agents again and repeats this cycle
bid

Figure 5.15 Coordination cycle of CNP

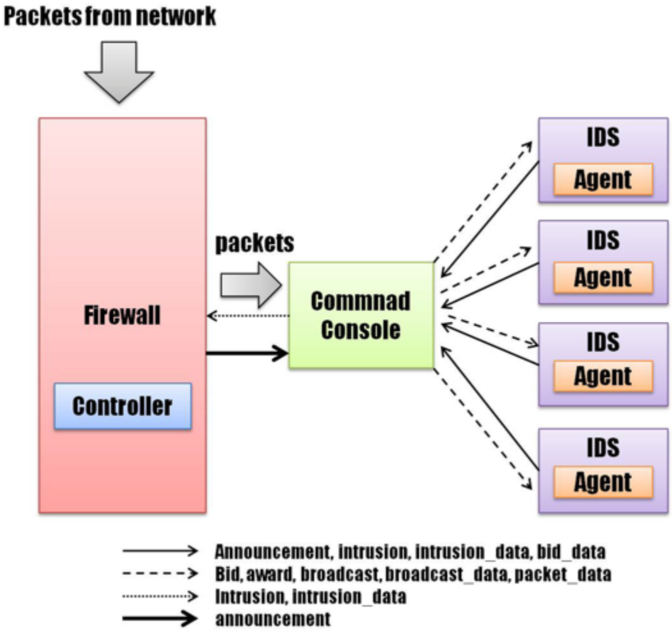

Packets from network
Firewall
Controller
packets
Commnad Console
IDS
Agent
IDS
Agent
IDS
Agent
IDS
Agent
Announcement, intrusion, intrusion_data, bid_data
Bid, award, broadcast, broadcast_data, packet_data
Intrusion, intrusion_data
announcement

Figure 5.16 Coordination structure of CNP

Figure 5.15 sequentially represents the coordination cycle among the IDS, Command Console, and Firewall models. The Command Console sends a bid message to all IDS agents for intrusion data acquisition. IDS agents that receive the bid message immediately respond to the Command Console with a bid_data message. The Command Console selects an almost adaptive IDS agent and then sends an award message to selected IDS agents. The selected IDS agent sends intrusion information to the Command Console which then uses these data.

Figure 5.16 shows the coordination structure of CNP and the flow of messages. The Command Console is a centralized entity and controls the coordination between the IDSs and the Firewall in the CNP. Coordination is actually achieved through the exchange of messages between the Command Console, IDS Agent models, and the Controller model of the Firewall.

5.3.2.2 Coordination Messages

The Command Console, IDS, and Firewall models have Messenger models that play the role of exchanging messages. A Message is divided into a control message and a data message. It is distinguished by msg_type field. Table 5.3 presents the types of messages.

Table 5.3 Types of messages

	Message Number	msg_type
Control Messages	0	Broadcast
	1	Announcement
	2	Bid
	3	Award
	4	Intrusion
Data Messages	5	broadcast_data
	6	bid_data
	7	packet_data
	8	intrusion_data

The Msg_content field is composed of an agent_name field used to search for the address of and agent and the data field includes actual information as depicted in Figure 5.17. Because the Command Console has a mapping table that maps agent_name to the address of an agent, it can receive or send messages to all agents.

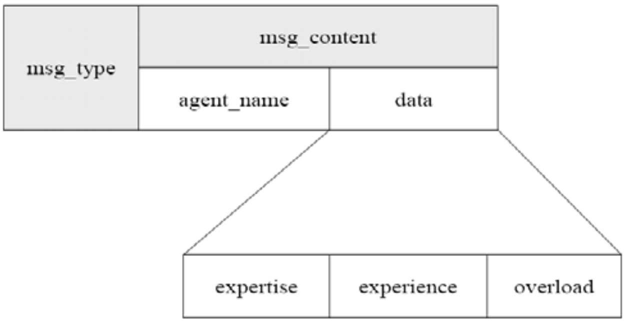


Figure 5.17 Structure of bid_data

The Control message is used for the Command Console to control IDSs and the Firewall. Bid messages announce that all IDS agents should send bids to the Command Console. Award messages reports that an agent has been selected as the IDS agent for intrusion detection. Intrusion messages inform the Command Console that an intrusion has been detected and also makes the Firewall respond to the intrusion. The Announcement message informs the Command Console that all agents repeat the coordination cycle when a state switches to Failed state. Broadcast messages report to all IDS agents that the Command Console has broadcasted detection information.

There are four types of data messages: bid_data, intrusion_data, packet_data, and broadcast_data messages. Bid_data messages provide information requested for agent selection. Packet_data messages contain packet data extracted from real packets. Broadcast_data messages include detection information. The data field of bid_data messages, used for agent selection during the bidding procedure, is composed of expertise, experience, and loading.

5.3.2.3 Agent Selection Algorithm

Each agent sends a bid_data message to the Command Console if the value of the overload field is not greater than the threshold value of the system overload. The Selector of the Command Console makes a list of bids and enters agent bids into the list. First, the Selector model sorts the list by expertise, in descending order, and then selects the agent that has the greatest value of expertise. If the bid numbers are greater than two, the Selector model deletes all bids from the list except those bids having the greatest value of expertise, and then re-sorts the list by experience, in descending order. The Selector model chooses an agent that has the greatest value of experience. If the bid number is greater than two, the Selector deletes all remaining bids from the list except those possessing the greatest value of experience and sorts the list yet again, by loading. and in ascending order. Finally the Selector selects the best agent, the first element on the list, and the selected agent begins to detect intrusions. Table 5.4 depicts the selection algorithm representing the selection routine.

Table 5.4 Selection Algorithm

```
Let bidi be bids
Set bid_list = empty set
Let bid_list = (bid1,bid2,..., bid n) be a list of bids
for i = 1 to n
    if loading of bidi >= threshold value
        Delete bidi from bid_list
Sort bid_list by expertise in descending order
if the number of bid including the greatest value of expertise >= 2 then
{
    Delete bids from bid_list except bids including the greatest value of expertise
    Sort bid_list including bids of the same expertise by experience in descending order
    if the number of bid including the greatest value of experience >= 2 then
    {
        Delete bids from bid_list except bids including the greatest value of experience
        Sort bid_list including bids of the same experience by loading in ascending order
    }
}
Select Agent from bid_list(the first element)
```

5.4 Summary

In this chapter, I discussed security protocol issues for the HUC-HISF.

First, I proposed an effective session key distribution mechanism. In this mechanism, a mobile node obtains its session key from the previous access router and performs an SCTP based location update for corresponding nodes. Accordingly, the proposed mechanism provides reduced signaling costs and handover latency. The presented performance analysis and its numerical results confirm that the proposed mechanism outperforms existing mobility protocols such as Mobile IPv6 and Fast Mobile IPv6 in terms of signaling costs and handover latency. In this thesis, I consider a mobile node-initiated handover so that the proposed mechanism can be extended to the case of network-initiated handovers. In future work, I plan to extend the proposed session key distribution mechanism to network-initiated handover cases.

Second, I proposed a number of WAKE protocols having a key recovery feature. I described a security hole arising in the public KRI validation phase, specifically within the VASP domain of *Kim* and *Lee*'s protocol. In response to this weakness, I designed a new security-enhanced key recovery protocol over the WAKE protocol and demonstrated how this enhanced protocol retains the efficiency of *Kim* and *Lee*'s protocol. I then proposed a new privacy-enhanced key recovery protocol, which can strongly protect users' location privacy.

Third, I selected several indicators for this simulation and constructed the a DEVS-based network security simulation environment and applied the CNP for coordination between IDSs and a Firewall. I also evaluated the performance of IDESs applying a rete pattern matching algorithm. Through simulation, I confirmed that multiple IDSs coordinated by the CNP performs more effectively in the detection of intrusions than a single IDS and can protect the network in advance by cooperating with the firewall. The application of the rete algorithm absolutely improves the efficiency of multiple IDSs with CNP. In the future, it will be necessary to construct a general network security simulation environment that is able to perform various security simulations and develop more effective algorithms that may be applied to the inference cycle of expert systems that detect various intrusions.

Chapter 6. DH-RBAC: Dynamic Human-context Role Based Access Control

In this chapter, I describe DH-RBAC which is the core elements on this thesis. To have a better understanding, I describe the formal definition of context and its expression, and definition and architecture of DH-RBAC. In addition, I discuss DH-RBAC operations through examples.

6.1 Definition of the Context and Expression

In this section, I describe the formal definition of context used in DH-RBAC and related expressions based on [CFZA02, FSGKC01, HW04, ZP04] - context type, context constraint, access control policy, resource access.

Definition.1 Context Type

A Context Type (CT) is defined as a property related to every participant in an application when it is running. The context type may be a definite property such as temporal or spatial information. In addition, context type can be used to describe an abstract concept.

Based on context type, every application has its own Context Set (CS), which is defined as a set of context types:

$$CS = \{CT1, CT2 \ldots CTn\},\ 1 \le i \le n \tag{6.1}$$

In order to make this abstract concept of context type usable when decisions of access control need to be made, it is necessary to have each context type evaluated by some Context Implementation. A context implementation (CI) of context type is defined as a function with n context types that return an object of type CT.

$$CI\colon CT1 \times CT2\ \ldots \times\ CTn \rightarrow CT,\ n \ge 0 \tag{6.2}$$

Definition. 2 Context Constraint

I define a context constraint as a regular expression. Based on this format, our access control is able to specify any complex context related constraint to describe all kinds of security requirements.

$$\mathit{Context\ Constraint} = \bigcup_{j=1}^{i} \mathrm{Cond}_j\ ,\ \mathit{Cond} = \bigcap_{i=1}^{j} \mathrm{SubCond}_i \tag{6.3}$$

$$\text{SubCond:= <CT> <OP> <VALUE>}, \tag{6.4}$$

Where CT∈CS; OP is a logical operator in the set {≥, < , ≤, ≠, =} and VALUE is a specific value of CT. Suppose I have a context set CS = {Time, Location, Security Class}, and I have a partial security rule such as “patient data can be accessed from and within the hospital between 09:00 and 17:00 with a security class of a password, otherwise a higher security class is required.” If “in” is a human-centric logical operator and “hospital” is a valid value of context type as location, then this rule could be expressed as

$$\textit{Context Constraint: = (Time >= 09:00} \cap \textit{Time < 17:00} \cap \tag{6.5}$$

$$\textit{Location in hospital} \cap \textit{SecClass>= H(PW))} \cup \textit{(SecClass > H(PW))} \tag{6.6}$$

Definition. 3 Access Control Policy

I define an access control policy (ACP) as a triple, ACP = (S, P, CC).

S is the subject in this policy, which could be a human or a role.

P is the target permission in this policy, which is defined as a pair <K,O>, where K is an operation kind defined in {READ, WRITE, DELETE, MODIFY} and O is a resource object.

CC is a context constraint in this policy. If CC is empty then this policy returns to simple RBAC.

Definition. 4 Resource Access

I define resource access as a triple, RA = (U, P, RC).

U is a human who issues this resource access in human set.

P is the permission that this human wants to acquire.

RC is Runtime Context which is a set of values for every Context Type in the Context Set. That is, RC = {V1 of CT1, V2 of CT2, …, Vn of CTn}, where = {CT1, CT2 … CTn} is the context set of the application.

A resource access RA (U, P, RC) is granted only if there exists an access control policy ACP (S, P′, CC), such that U ∈ S, P = P′, and CC evaluates to true under RC.

6.2 Formal Definition of the DH-RBAC and its Architecture

DH-RBAC executes context constraint process by using context information such as temporal and spatial information when permission – role assignment (PA) is established. DH-RBAC model indludes basic characteristics of RBAC like Least Privilege, Role Hierarchy, SoD, and Cardinalities concepts.

Table 6.1 Formal Definition of DH-RBAC

U, R, P, S, C represent the finite set of humans, roles, permissions, sessions, and context information respectively within the system

PA ⊆ P x R represents the finite set of permission to role assignments. This is a many-to-many relationship.

UA ⊆ U x R represents the finite set of human to role assignments. This is a many-to-many relationship.

human: S → U, a function that maps a session si to a human.

RH ⊆ R x R is a partial order on R, called the role hierarchy or role dominance relation, also written as ≥, where r1 > r2, only if all permissions of r2 are also permission of r1 are human of r2.

For RBAC 0: $S \rightarrow 2R$, a function that maps a session si to a set of roles, where roles(si) $\subseteq$ {r | (human(si), r) $\in$ UA}, and each session si has the permissions $\cup$r $\in$ roles si) {p | (p, r) $\in$ PA}.

For RBAC1, roles: $S \rightarrow 2R$, is modified from RBAC0 to require roles(si) $\subseteq$ {r | ($\exists$r'$\geq$ r) [(human(si), r') $\in$ UA]} and each session si has the permissions $\cup$r $\in$ roles(si) {p | ($\exists$r' $\leq$ r)[(p, r') $\in$ PA]}.

For Context Constraints (CC), DRBAC adds context constraints in the form of restrictive functions that operate on basic RBAC components to meet the specific needs of the protection policies of an organization and factor of dynamic environments. Constraints in DRBAC include SoD (Separation of Duties) and Cardinalities including concepts of the RBAC 2. In addition, It includes context such as environments, time, location, etc.

CCA $\subseteq$ CC x R represents the finite set of CC to role assignments. This is a many-to-many relationship.

DH-RBAC assigns the essential role among sub-roles to the human. Human-role assignment (UA) relationship and the rights which are assigned to other sub-roles are assigned to the human by inheritance relationship of the sub-role level when a human makes an essential role active. Table 6.1 presents formal definition of DH-RBAC and Figure 6.1 depicts DH-RBAC architecture.

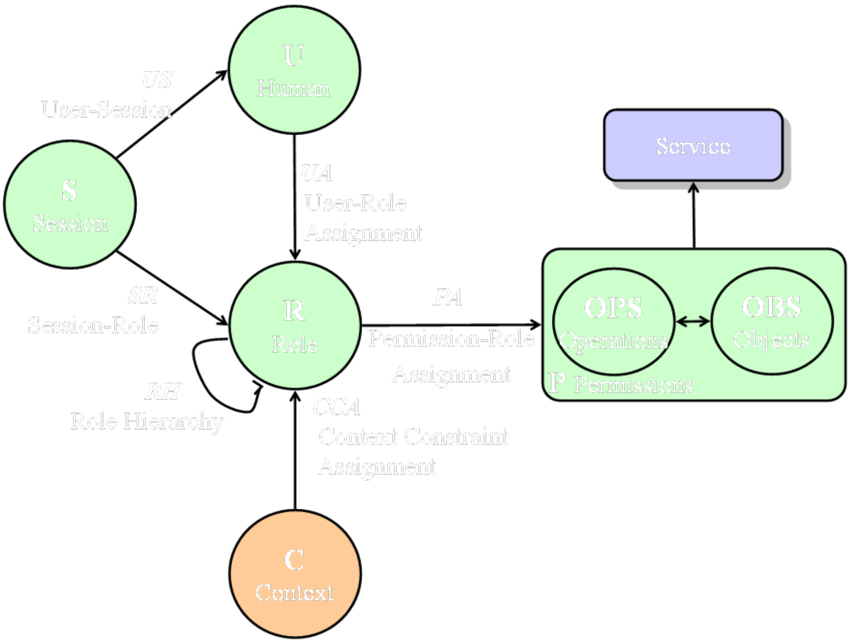


Figure 6.1 DH-RBAC Architecture

6.3 DH-RBAC Operation

Before I explain DH-RBAC operations, I need to remind of the prerequisite - All subjects can communicate freely each others through WSN module - assumed in chapter 1. In addition, the WSN module must be embodied with context agent module to be able to process the context information real-timely.

The role set in DH-RBAC model is divided into role subset and is assigned to human. Furthermore, it is set each role which owned privilege having access to resource, and is assigned as one permission subset from the permission.

I describe DH-RBAC operation by giving a medical scenario example which controls access to patient information document by member of hospital.

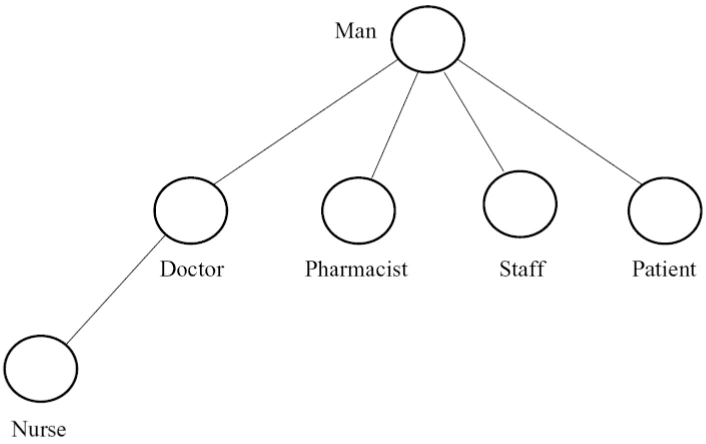


Figure 6.2 Role Hierarchy in Hospital

The hospital is comprised with various subject's roles which are related to their tasks. For example, I can classify those tasks like doctor's role, nurse's role, pharmacist's role, staff's role and patient's role as depicted in Figure 6.2.

Moreover, the patient information document consist s of personal information, medical record, prescription, and administration record shown in Figure 6.3.

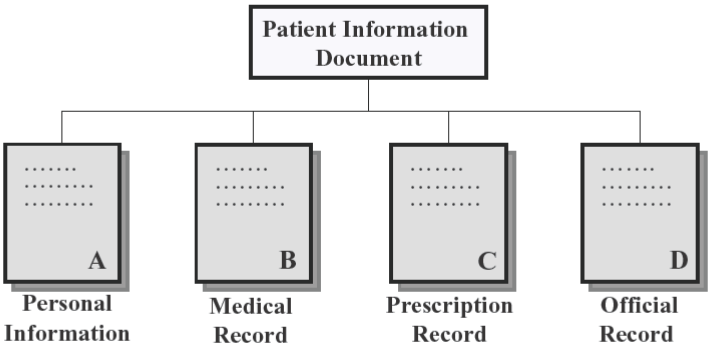


Figure 6.3 Patient Information Document Construction in Hospital

The access to patient information documents is not complicate in those days, any member of hospital can access to this information by using only human class through human authentication. However, critical matters including individual's privacy exposures will be occurred if the access information having higher class of subject is exposed to malicious party.

In this chapter, I present an access control mechanism by using temporal and spatial context information to patient information document. In addition, I assume Read (R), Write (W), Delete (D) and Modify (M) as permissions having access to patient information documents, and express these rights as P1, P2, P3 and P4 respectively.

To apply temporal and spatial context information to our proposed access control model, I divide the time in T1 and T2. T1 means doctor's regular working time from 09:00 to 17:00, and T2 as the other time. Moreover, for the spatial context information, I classify location as three spaces - inner medical office, outer medical office in hospital, and the other place, and I note as L1, L2 and L3 respectively.

In this section, I describe the access control process applying doctor's temporal and spatial context information. In addition, I can specify the access control based on temporal and spatial context information to patient information document as following Table 6.2.

Table 6.2 Example of an access control to patient information document based on temporal and spatial information

Subject	Role	Object	Time	Location	Permission
Kim	Doctor	A	T1, T2	L1, L2	R
		B	T1	L1	R, W, D, M
				L2	R, W
			T2	L1	R, W
				L2	R
		C	T1, T2	L1, L2	R
		D	T1, T2	L1, L2	R
	Nurse	A	-	L1, L2	R
		B	T1,T2	L1,L2	R
		C	T1	L2	R
	. . .	. . .	. . .	. . .	. . .

First of all, let's take a look an access control mechanism using temporal context information. Doctor role is activated when *Dr. Kim* pretend to access to patient information document form 09:00 to 17:00 (T=T1). In addition, regarding to the personal information (object=A), only the permission R (P=P1) is assigned regardless of time. Permissions R, W, D, M (P=P1, P2, P3 and P4) about the medical record (object=B) are assigned for the regular working time (T=T1). In contrast, permission R or W (P=P1 or P=P2) is assigned for the non-regular working time (T=T2). Furthermore, for the prescription record (object=C), the permission R (P=P1) is assigned regardless of time. (Figure 6.4 and Figure 6.5)

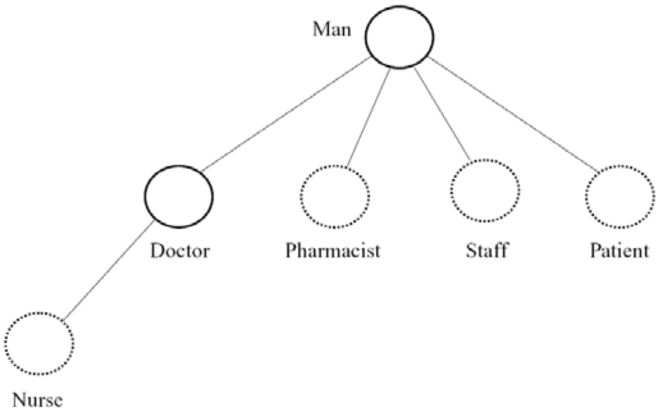


Figure 6.4 Role Activation as Doctor in Hospital

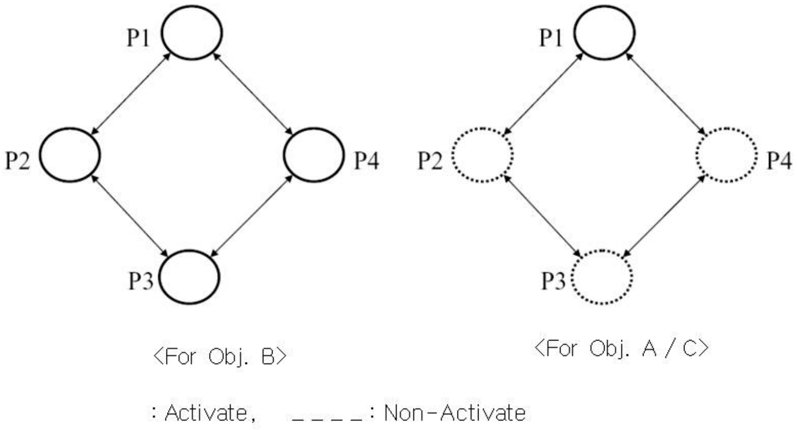


Figure 6.5 Permission Assignment for Object A, B, and C considering Temporal context

However, when *Dr. Kim* pretends to access to patient information document at doctor non-regular working time (T=T2), even if doctor role is activated like in Figure 6.4, the permission to each object might be changed like in Figure 6.6.

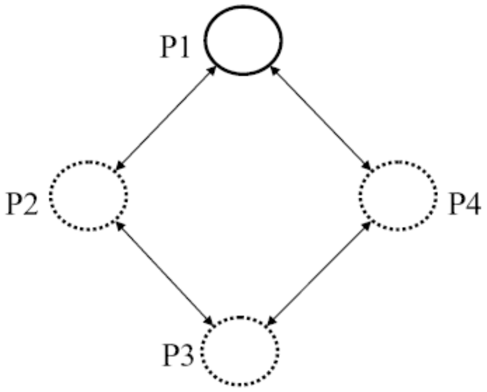
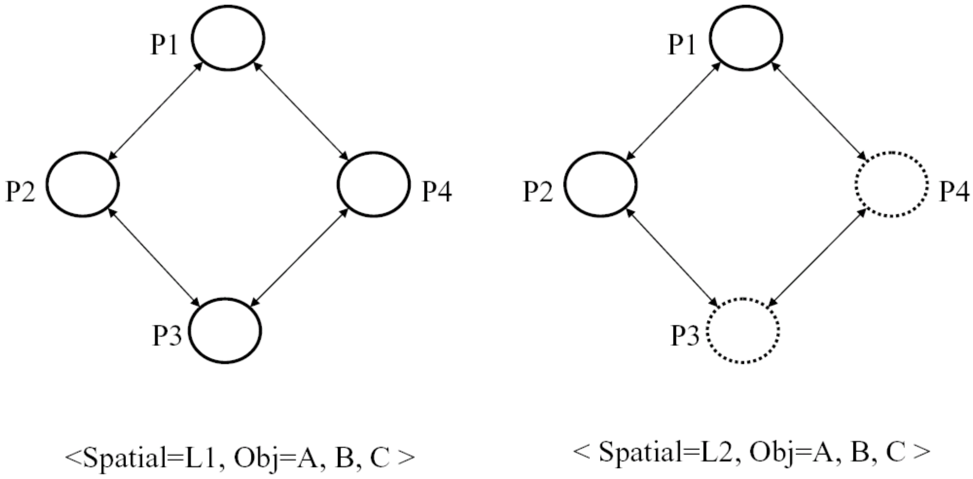


Figure 6.6 Permission Assignment for Object A, B, and C considering Temporal Context

That mean is, only the access permissions R (P=P1) to personal information, medical record and prescription record (object = A, B, C) are assigned. Permission assignments having access to patient information documents will be set in this way for other roles depicted in Figure 6.2. In this section, I consider only doctor role.

The following is an example of access control mechanism using spatial context information. *Dr. Kim* want to access to patient information document when he is in his medical office (Spatial = L1) the access permissions for R, W, D, M (P=P1, P2, P3, P4) to personal information, medical record and prescription record are assigned. In addition, when he is in the hospital (Spatial = L2), only the permissions R, W (P=P1, P2) are assigned. In that case he is outside the hospital (Spatial = L3), permissions are not assigned (Refer to Figure 6.7).



<Spatial=L1, Obj=A, B, C >

< Spatial=L2, Obj=A, B, C >

Figure 6.7 Permission Assignment for Object A, B, and C considering Spatial Context

Finally, I discuss an access control mechanism considering both temporal and spatial context information.

I express access control status as following notation;

$$\{\textit{For x, Context kinds, Can-access, P=Py}\} \tag{6.7}$$

It means that subject can access object x by permission Py under condition of the context kinds.

Let us take a look examples. The permission R is assigned to *Dr. Kim* wherever he is in hospital. I can express like {For Obj=A , Context: (Temporal=T1, T2) ∪ (Spatial =L1, L2), Can-access: P=P1}. In contrast, the permissions R, W, D, M to medical records are assigned at regular work time and only in medical office. Permissions R, W are assigned when he is at the outer medical office in hospital and regular working time. I can express as {For Obj=B, Context: (Temporal=T1) ∩ (Spatial =L1), Can -access: P=P1, P2, P3, P4} ∪ {For Obj=B, Context: (Temporal=T1) ∩ (Spatial =L2), Can -access: P=P1, P2} (Refer to Figure 6.8). For the prescription record, only permission R is assigned inner medical office or in hospital regardless of time and I can express like {For Obj=C, Context: (Temporal=T1, T2) ∪ (Spatial =L1, L2), Can-access: P=P1}.

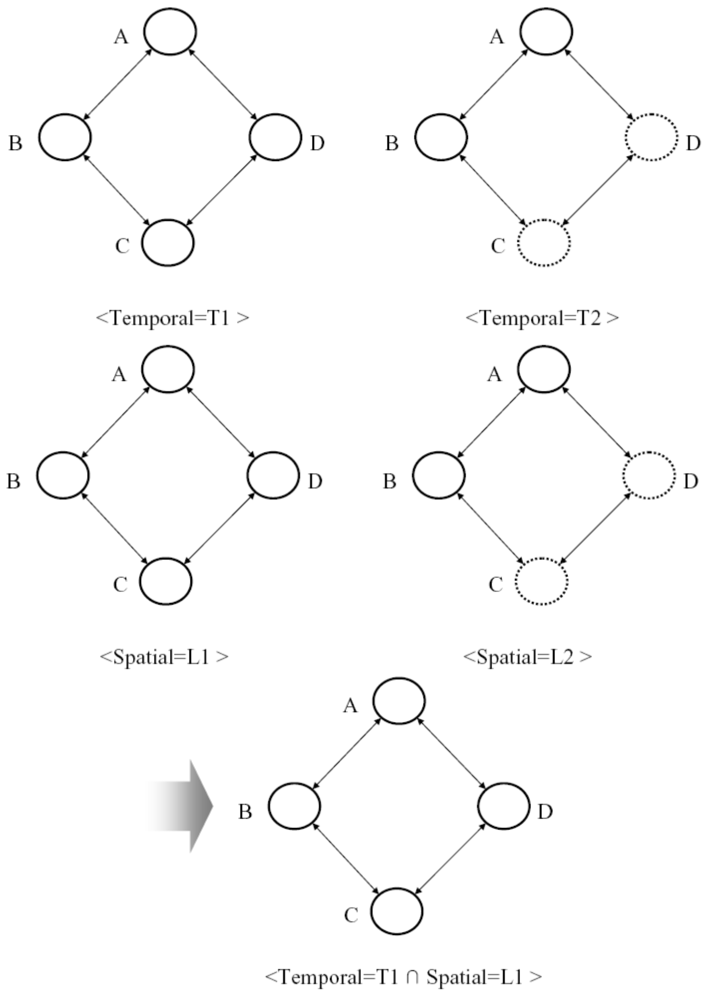


Figure 6.8 Permission Assignment for Object considering Spatial and Temporal Context

That is to say, if I consider only temporal context, *Dr. Kim* can have to access to object A or B or C or D with permission P1 or P2, P3, P3 depend on temporal context. In addition, if I consider only spatial context, *Dr. Kim* can do too. However, If I consider temporal and spatial context, *Dr. Kim* can have to access to the only object B with permission P1, P2, P3, P4 (Refer to Figure 6.8).

Table 6.3 shows some parts of permission definition in DH-RBAC which is accessible to patient information document as XML format.

Table 6.3 Some parts of permission definition in DH-RBAC by XML format

```
<Rule RuleId="AllowAll" Effect="Permit">
   <Subject>
       <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
      DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
         <AttributeValue>Doctor</AttributeValue>
      </Attribute>
   </Subject>
   <Resource>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      DataType="&xml;string">
         <AttributeValue> Patient Information Document </AttributeValue>
      </Attribute>
   </Resource>
   <Action>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="&xml;string">
         <AttributeValue>Read</AttributeValue>
      </Attribute>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
       DataType="&xml;string">
         <AttributeValue>Write</AttributeValue>
      </Attribute>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="&xml;string">
         <AttributeValue>Delete</AttributeValue>
      </Attribute>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="&xml;string">
         <AttributeValue>Modify</AttributeValue>
      </Attribute>
   </Action>
</Rule>
```

Doctor has permissions - Read, Write, Delete, Modify to Patient Information Document Resource. If both Doctor and Nurse have permission READ to resource, I can add Nurse to the Object element and activate Read at the Action element.

6.4 Summary of the DH-RBAC

In this chapter, context constraint based RBAC was described. The main idea is providing expendability and security applying the temporal and spatial context information to Role Based Access Control model.

In addition, I presented the formal definitions for context type, context constraint, access control policy and resource access, etc. Furthermore, I presented the formal definition for DH-RBAC and its architecture, and detailed example scenarios to give better understanding for the proposed DH-RBAC model.

DH-RBAC model is core technology related to secure and intelligent ubiquitous services supporting dynamic access control in smart home. Moreover, DH-RBAC model will be extended to H-Ubi Comp environment, and I expect to be applied various applications.

Chapter 7. Service and Application using HUC-HISF

In this chapter, I discuss services and applications using the HUC-HISF. H-Ubi Comp has emerged as an exciting new paradigm for providing intelligent computing and communications at any time and in any place. But, in order to take advantage of such services, it is important that intelligent security frameworks be suitable for H-Ubi Comp. In this chapter, I propose a privacy and access control scheme for surveillance, a core security technology for ubiquitous hybrid intelligent security framework. In this scheme, device information and signature information can be added to the image data obtained by the image capturing device to maintain the security of the image data and use the image data as digital evidence when a specific incident occurs.

Also, in today's modern society, the rapid development of IT and distribution of the Internet and computers across super-high speed networks have led us to a cultural turning point as a u-knowledge-based society. This change has led to an environment where digital materials have rapidly increased and communication infra has expanded, thus allowing image and sound information to be shared through IP networks as the demand for integrated services increases. In providing IPTV through IP networks, IPTV may result in illegal control, illegal content distribution, service theft, access of unapproved users, sniffing, tapping, DoS attacks, War Dialing attacks, man-in-the-middle attacks, Rogue Device attacks, or harmful software infection and all manner of security vulnerabilities. As such various Iaknesses exist, this study researches AAA, a subscriber authenticated technology, to provide more secure and efficient mobile IPTV services for the next generation mobile IPTV subscribers.

The remainder of this chapter is organized as follows. In section 7.1.1, I describe security requirements for H-Ubi Comp surveillance for H-Ubi Comp. In section 7.1.2, I discuss the proposed USF-PAS including its architecture and flow. I describe a case scenario based on USF-PAS in section 4. Section 7.2.1 presents an overview of IPTV and AAA, security threats to IPTV and security requirements. Section 7.2.2 analyzes existing IPTV security technologies, CAS and DRM. Section 7.2.4 presents secure subscriber authentication technologies for mobile IPTV services.

7.1 U-Surveillance Service

H-Ubi Comp has emerged as an exciting new paradigm that includes pervasive, grid, and P2P computing for intelligent computing and communications at anytime and in any place. As environments expand into my everyday lives and the majority of security applications are designed and developed for ubiquitous environments, ubiquitous services may be offered anywhere, anytime and for any device. However, in order to take advantage of such services, it is important that intelligent security frameworks be suitable for UC [NSM05, CSE05, WADMV05].

Nowadays most services rely on authentication applications based on identity information. A number of authentication mechanisms may have been developed and implemented in various applications for heterogeneous features and environments. In real life, each entity using a service is likely to move from one space to another. Each space may opt to adopt an authentication mechanism for identifying the entity but this varies from application to application. When an entity moves to a specific space where there is no applied authentication mechanisms, but the provided service needs the identity information about the entity, then I have no secure method for providing the services.

I define USF, a Ubiquitous Hybrid Intelligent Security Framework (USF) that provides us with secure and intelligent services including core technologies: WSN / RFID, context awareness, information fusion, authentication, authorization and access control, surveillance, and so on [Pa08] (Refer to figure 7.1).

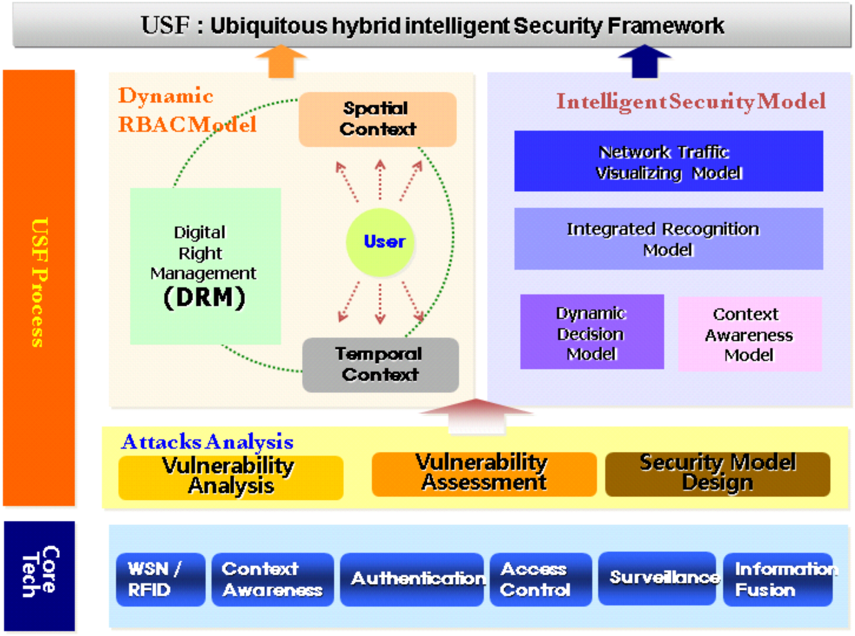


Figure 7.1 Ubiquitous Hybrid Intelligent Security Framework (USF)

Surveillance ensures that I monitor and keep track of objects of interest, which applies to a number of security deployments including home networks, USN, etc. Home networks are new IT technology environments enhancing the convenience and safety of people's lives. A home network infrastructure provides a variety of home network services regardless of device, time, and place. This can be done by connecting home devices based on various kinds of communication networks, such as mobile communication, Internet, and sensor networks [ZCC05]. Recently, home networks have expanded into ubiquitous computing environments as boundaries between networks and systems grow more obscure. However, as surveillance systems are connected to the Internet and consist of heterogeneous network protocols, they are exposed to various cyber attacks over the Internet, including hacking, malicious codes, worms, viruses, DoS attacks and eavesdropping [SK06].

Sensor-data fusion from multiple cameras is a potential problem with many applications. The work in multisource fusion can be divided into two categories based on camera configurations: spatially non-overlapping and spatially overlapping. [SG00] attempts to fuse data from several non-overlapping cameras using a Bayesian reasoning approach. Since there might be significant gaps between each camera's field of view, the precision of prediction may suffer. Most fusion algorithms assume an overlapping camera configuration and concentrate on fusing local coordinate frames of multiple cameras onto one global coordinate system. The DETER project [KTB06] 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 section, I use a two-level hierarchy of Kalman filters for trajectory tracking and data fusion from multiple cameras. The advantage of my 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 prediction-correction paradigm. The quantities of the 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 [BHAE02].

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 [YHTFTSTS05, PM01].

In this section, I are interested in summarizing the trajectory of a vehicle, and hence only its position, not its orientation, is needed. I have thus employed the traditional Kalman filter for the purpose of efficient tracking. 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 [MPTH01]

7.1.1 Security Requirements in Surveillance for H-Ubi Comp

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 for surveillance system security and enforcement points, legacy security modules can be easily deployed without the complicated task of integrating them as each of them performs its' own security function. However, this results in making the surveillance system more complicated and messy to manage. Also, because of inconsistency among the separated security modules, it may result in unexpected security holes. Thus I need a specific way to enforce security policies and manage inconsistency among them. A surveillance device is located at the border of each space and filters accesses based on rules with the help of security modules, enforcing authentication, authorization, and security policies.

- **Authentication and Privacy**: Authentication is supposed to be the 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 the system and verify the identity information by means of a trusted mechanism. General authentication mechanisms include ID/password-based authentication mechanism, Certificate-based authentication mechanisms, authentication mechanisms, and mechanisms using biometric information. Surveillance devices offer authentication mechanisms. A user may choose one mechanism that he or she prefers. When most surveillance systems are deployed, an application server is responsible for authenticating users and devices.

- **Authorization and Access Control**: The purpose of authorization is to control access and restrict privilege and access rights to resources even though the entity has been authenticated successfully. A few authorization mechanisms that are generally used include DAC (Discretionary Access Control), MAC (Mandatory Access Control), and RBAC (Role-based Access Control). The RBAC mechanism for authorizing surveillance system is suitable for many systems and guarantees extensibility and flexibility. RBAC mechanisms use role components between subjects and resources, creating the possibility of indirect authorization relationships.
- **Security Policy Manger**: Security policy managers should generate and manage security policies specialized for their surveillance system which includes an authentication policy, an authorization policy, and other types of security policies. Considering the features of surveillance systems, they must be easy enough for users not familiar with IT.
- **Other Security Polices**: Security policies should be a set of single rules consisting of conditions and actions. Whenever a condition is satisfied, an action is performed. The key issue is how to construct conditions. Elements to be contained in conditions include time (date, day, duration), event (sensor, user-triggering, state), and log(statistics). In addition, relationships (interaction, union) among above elements and supporting recursive structures should be defined. Building complex conditions should be possible. Times and events are the basic elements of conditions and can be used generally. On the other hand, log-based conditions control access by statistical information.

7.1.2 USF-PAS

[Assumptions]

These are some assumptions for USF-PAS in this chapter:

1. Surveillance camera is based on a Kalman Filter and HMM.
2. Each space is monitored by at least a single surveillance device.
3. Each surveillance device has functions for collaborating with other
4. surveillance devices and relaying each entity’s identity information.
5. Legacy authentication applications may communicate with other
6. surveillance devices for send/receiving identity information.

7.1.2.1 USF-PAS Architecture

USF-PAS includes three main components, an image capturing device, a surveillance device, and a surveillance management server (Refer to Figure 7.2).

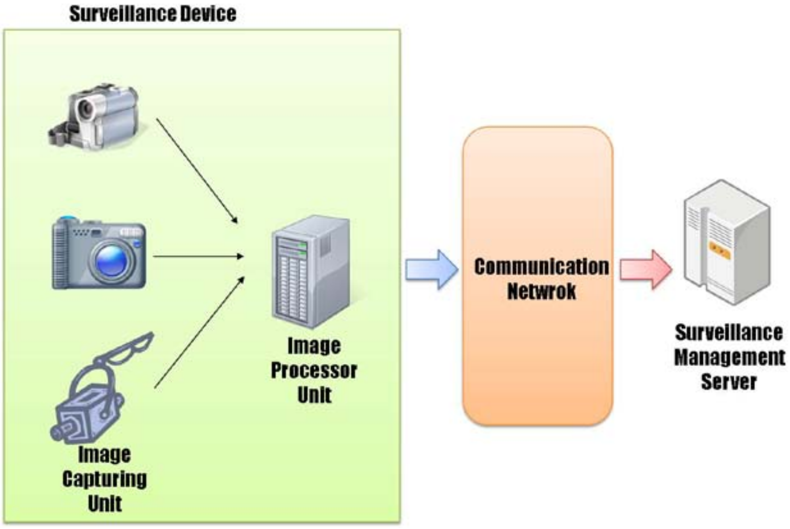


Figure 7.2 USF-PAS Architecture

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.

7.1.2.2 USF-PAS Flows

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

- **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 7.3).

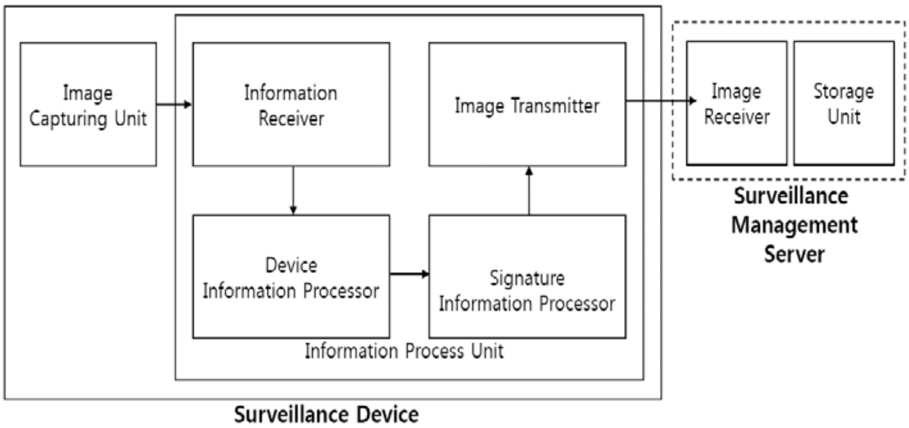


Figure 7.3 Flow of USF-PAS (Device-side Signature)

- **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 7.4).

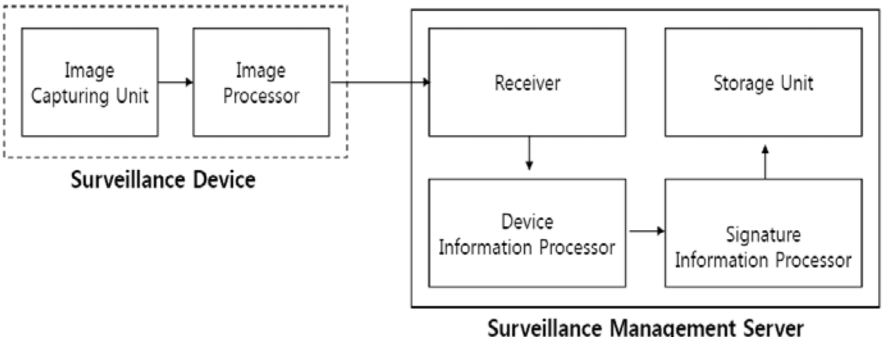


Image Capturing Unit
Image Processor
Surveillance Device
Receiver
Storage Unit
Device Information Processor
Signature Information Processor
Surveillance Management Server

Figure 7.4 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.

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.

- **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.

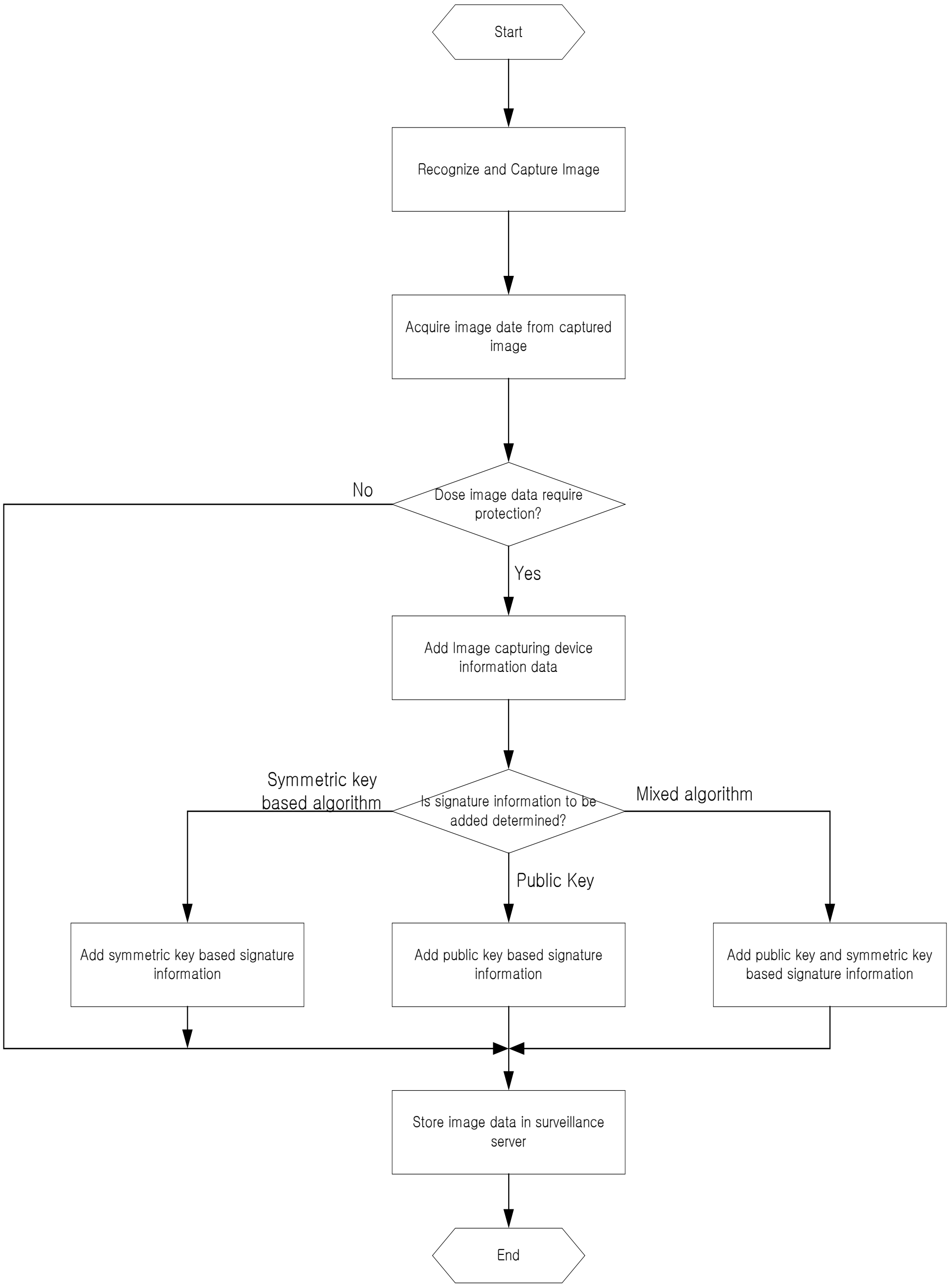

Start
Recognize and Capture Image
Acquire image date from captured image
Dose image data require protection?
No
Yes
Add Image capturing device information data
Is signature information to be added determined?
Symmetric key based algorithm
Public Key
Mixed algorithm
Add symmetric key based signature information
Add public key based signature information
Add public key and symmetric key based signature information
Store image data in surveillance server
End

Figure 7.5 Whole flow of USF-PAS

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, I couldn't guarantee that an entity can be authenticated in every space. Figure 7.6 shows the ubiquitous environment for moving entity of multiple spaces [KLHK08].

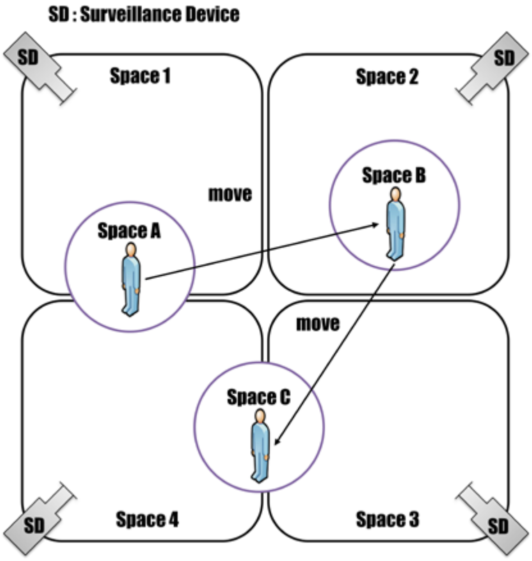


Figure 7.6 Entity's movement through multiple spaces in ubiquitous environment

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.

- **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 [LKSL06].

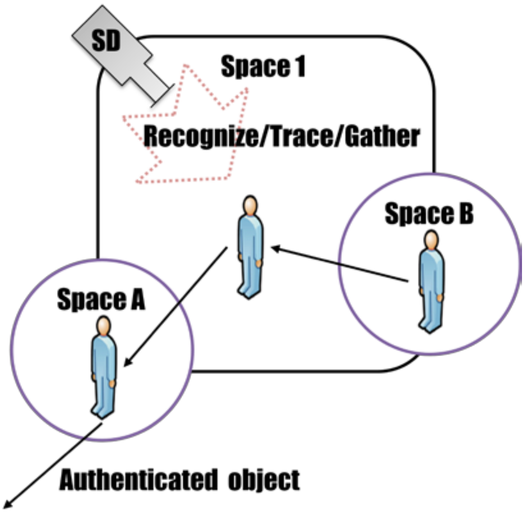


Figure 7.7 Identity relay using surveillance device

Figure 7.7 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.

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’ s possible to identify an entity according to the application environment. But in general applications, I 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.

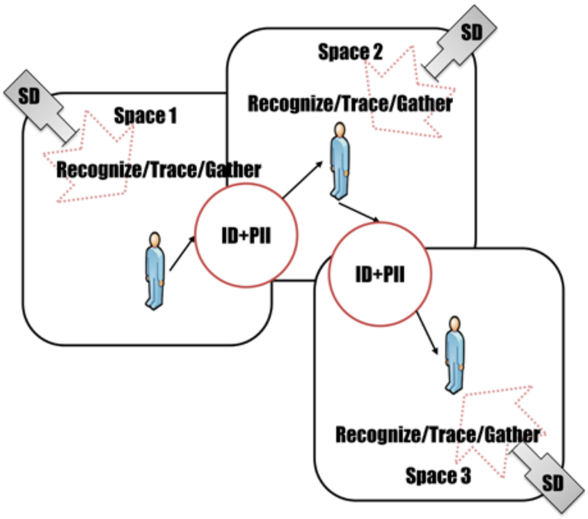


Figure 7.8 Hand-overs through multiple not-authenticated spaces

7.1.3 Analysis of USF-PAS

In this section, the analysis for security and efficiency of USF-PAS is discussed. For the case of security, I analyze USF-PAS based on the security requirements presented in section 7.1.1. In addition, I compare two cases - the applied security requirements and non- the applied security requirements from the aspect of the efficiency of USF-PAS.

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

- **Authentication and Privacy:** In this system, I 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 an 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 my USF-PAS, I use a Drag-and-Drop mechanism to establish the security policy, so anyone can handle it if he has been authenticated successfully.

Second, I explain efficiency of USF-PAC. I verify efficiency at the number of selection by comparing case of non-applied security requirements (A) with case of applied security requirements (B) when I use surveillance system of USF-PAS. As the following at the simulation graph [Figure 7.9], 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.

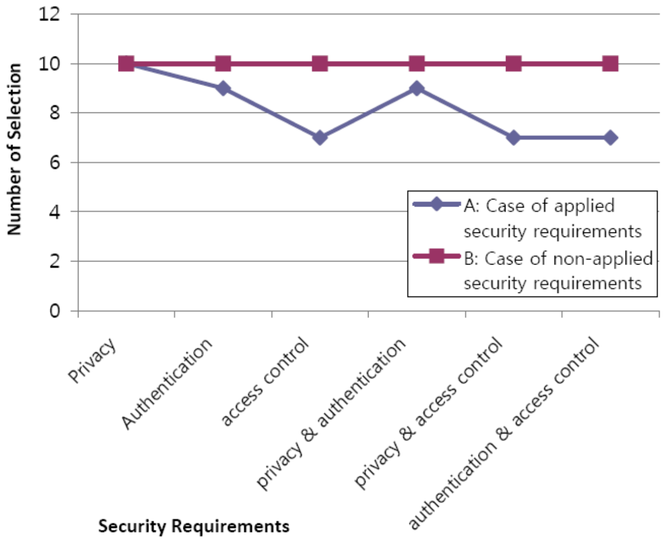


Figure 7.9 Hand-overs through multiple not-authenticated spaces

7.2 Mobile IPTV Service

IT technology is advancing into ubiquitous environments such as the Internet and mobile devices develop. Such a change will provide users with various services, the demand for which will rapidly increase as users want services even while using mobile devices. The scale of the domestic market for these services in the next generation of telecommunication will be great as the use of services via mobile devices is expected to be centered on ubiquitous environments.

However, in spite of the possibilities for advancing and diversifying services, the wireless environment has many risks and weaknesses compared to existing wired networks. For example, wireless environment for mobile devices are vulnerable to sniffing, tapping, DoS (Denial of Service) attacks, man-in-the-middle attacks, Rogue Device attacks, harmful software infection, as well as the risks of existing wireless environments. In other words, receiving IPTV(Internet Protocol Television) via IP network exposes IPTV to other security vulnerabilities such as illegal control, illegal content distribution, service theft, access by unapproved users, sniffing, tapping, DoS attacks, War Dialing attacks, man-in-the-middle attacks, Rogue Device attacks, harmful software infection, etc. [XDZHG07, LP07]. Given such various weaknesses, this study researches applications of subscriber authentication technology, specifically of AAA (Authentication, Authorization, and Accounting) mechanisms for mobile IPTV services.

7.2.1 Background

This section presents an overview of bilinear pairing and AAA, and analyzes security threats and security requirements with regard to existing IPTV.

7.2.1.1 AAA

The AAA (Authentication, Authorization, and Accounting) standard devised by the IETF working group is applicable to the Diameter protocol. An AAA protocol has been established for next-generation roaming environments without restricting the existing RADIUS (Remote Authentication Dial In User Service) protocol. For this protocol standard, a formal working group was formed in December 1998, and the applicable AAA protocol was named Diameter. The basic structure of the Diameter protocol is divided into transmission protocols that include SCTP (Stream Control Transmission Protocol), a base protocol that includes accounting functions, and various high level application protocols.

With the extension of IP-based Internet, there is an increase in demand for accessing the network through wireless mobile environments. Indeed multiple service environments may coexist in the same wireless environment including QoS (Quality of Service) provisions, pre-payment cards, and others. In order to satisfy user requirements, wired and wireless businesses must provide secure and high level services for legitimate users. The AAA protocol is an essential element for such secure network access, mobile service, user authentication, authorization and account processing. In 1991, the AAA protocol was proposed with the Radius protocol by the Livingston Company, and provides an AAA service for the SLIP (Serial Line Internet Protocol) or PPP (Point-to-Point Protocol) linkage service. However, at present, service networks are gradually evolving into open-types and networks are evolving into a series of multiple domain environments. Therefore, the IETF (Internet Engineering Task Force) AAA working group is focused on the standardization of the Diameter protocol that provides AAA services appropriate for roaming environments. In the case of domestic environments, within the recent mobile Internet business domain, relevant businesses are quickly working on providing Mobile IPv4 and Mobile IPv6 services. For such mobile environments, AAA services must be applied between domains. For practical services in actual environments, there is a need for technological development in accordance with existing standards, however, technological development must also include mutual operation tests to determine if interworking is possible between products and standard adaptability tests. Between domestic standardization organizations and foreign standardization organizations, once the Diameter protocol standard is completed and the mobile Internet environment is standardized, the use of the Diameter protocol will expand rapidly, and the market is expected to grow more rapidly [PC97, PBPC03, KI02, KLCYKLY05, VCFGGBLHS00, CLGZA03].

7.2.1.2 Security Technology of IPTV

As representative IPTV security technologies, I present overviews of CAS and DRM and analyze their characteristics, advantages and disadvantages.

7.2.1.3 CAS

CAS (Conditional Access System) has been used as the basic system for controlling users' access to charged broadcasting services since the time of analogue broadcasting. Access conditions of CAS control include a subscription fee payment, receiving regions, receiving grades, etc. Thus, in principle CAS aims to protect the business and profits of charged broadcasting service providers.

Two standards were established from CAS, DVB (Digital Video Broadcasting) CAS in Europe, and ATSC (advanced Television Systems Committee) CAS in USA. Additionally, OpenCable CAS is the standard for digital cable TV in USA and is based on ATSC CAS. Although CAS standards exist, the details regarding specific representations of CAS have yet to be defined. The coexistence of many CASs may be possible, but the compatibility of different kinds of CASs is not guaranteed. The authority given to users who apply for certain broadcasting services is called Entitlement, and CAS controls access so that only qualified users can receive services. The items applied may be certain programs, or a set of TV channels.

CAS has grown in reliability as a content security solution and a growing number of broadcasting service providers have applied it to their existing services. However the condition of IPTV service is somewhat different because the current versions of CAS are based on the structure suitable for one-way broadcasting. CAS is a polling type system, not a Request / Response structure, and has the fundamental problem of wasting transporting streams. EMM (Entitlement Management Message) transmits information to qualified users via broadcasting media. Considering that with broadcasting all users share the same single bandwidth medium, committing every set-top box to the sole purpose of tracking EMM signals is a significant waste of bandwidth. The CAS standard adopts separate hardware such as smart cards and POD (Point Of Deployment) modules, and the necessity of such hardware generally results in an increase in service charges thus increasing the burden of subscribers. In addition to the inner problems of CAS, the fact that CAS is an access controlling solution for transmitting content channels causes difficulties to such functions as pure VOD (Video On Demand) and PVR (Private Video Recording) under the environment of an IP network. In this regard, the POD module structure defines content protection functions to some extent, but in the end, the basic problems are not solved since they only project the transmitting channel.

As for storage of hard disk content, an advanced service of IPTV, illegal copy prevention and access controls have yet to be provided. Management of security keys for consistently managing saved contents and payments and authority control of various services such as VOD should be first issue dealt with relation to IPTV service security [LP07, WRL06].

7.2.1.4 DRM

DRM (Digital Right Management) is a technology used to manage the intellectual property of digital contents in an Internet-based environment. To prevent illegal copying, data encryption of digital contents and licensing for certified users and terminals are required for controlling contents. Licensing includes content authority and decryption keys. Only when requirements for use are met is decryption executed. By protecting the whole process through Tamper Resistant technology, illegal leakage of contents by hackers is prevented.

Since DRM is a technology developed for Internet and PC based content distribution, it is suitable for IPTV service. Originally, it aimed to prevent the illegal copy of online contents, and thus CAS functions are only suitable for DRM as they are for IPTV services. . Not only are various payment methods available such as subscriptions, PPV (Pay per View), VOD, Usage Metering, Prepay, and Post Pay, but the cost-saving effects of excluding POD modules or Smart Cards are also outstanding as well. The modification and upgrade of security related modules mounted in a set-top box, key management, and authority of saved contents are easily implemented because of the basic structure of DRM. In existing broadcasting systems, leakage through intermediate distribution channels was always possible, but DRM enables End-to-End Content Protection from the content provider and end user, which is one of the most outstanding advantages. However, when there is no path available to return the issued license, DRM requires an ECM (Entitlement Control Message)/EMM [XDZHG07, LP07].

7.2.2 Bilinear Pairing

Bilinear pairing is a problem in discrete mathematics about ellipses that was simplified by reducing it to a discrete logarithm in a finite field. It was originally proposed as a map that attacks a conventional crypto-system. Recently, an encryption map for information protection has been used, instead of an attack map, so, that Bilinear Pairing is equivalent to a Bilinear Map. The following terms are used as stated in this paragraph and this theory is defined below [Sh84].

Characteristics that satisfy an Admissible Bilinear Map are as follows.

- Bilinear: Define a map $\hat{e} = G_1 \times G_1 \rightarrow G_2$ as bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ where all $P, Q \in G_1$, and all $a, b \in Z$.
- Non-degenerate: The map does not relate all pairs in $G_1 \times G_1$ to the identity in G_2. Observe that since G_1, G_2 are groups of prime order, this implies that if P is a generator of G_1, then $\hat{e}(P, P)$ is a generator of G_2.
- Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

Based on the bilinear premise, the following definition was constructed.

$$\begin{aligned}\hat{e}(aP, bQ) &= \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b \\ &= \hat{e}(P, Q)^{ab} = \hat{e}(abP, b) = \hat{e}(P, abQ)\end{aligned} \tag{7.1}$$

From this premise, for ellipses, the D-H (Diffie-Hellman) decision problem can be easily solved via the following equation.

$$\hat{e}(aP, bQ) = \hat{e}(cP, P) \Rightarrow ab = c \tag{7.2}$$

Therefore, the following is the basis for resolving the difficulties of the bilinear premise that is used as an encryption tool by many encryption protocols. When elements G_1, P, aP, bP, cP (BDHP, Bilinear Diffie-Hellman Problem) are given, this refers to $\hat{e}(P,P)^{abc}$ calculation problem. This problem can be solved if the ellipse curve discrete mathematics problem can be solved. For example, a can be calculated from aP, then $\hat{e}(P,P)^{abc}$ can be calculated through $\hat{e}(bP,cP)^{a}$

7.2.3 Security Threats and Requirements

IPTV is a brand-new service combining the Internet and broadcasting. All security risks that existed with conventional Internet and broadcasting services remain, some of them for broadcasters as well as some for subscribers.

7.2.3.1 Security threats

- Security threats in IPTV include the following: exposure of personal information: there are possibilities that personal information be exposed through illegal access by a third party such as identification information and payment related information that could result in monetary losses to subscribers.
- Masquerade: a malicious third party may be disguised as a legal subscriber through a communication channel that is not secure, and receive authentication and services. Thus, security should be secured to prevent such illegal access.
- Session hijacking: session hijacking is a form of attack that detours an authentication procedure to a server or a system. First, an attacker blocks the user from accessing a session in such ways as a DoS attack, and then hijacks the session with a server in order to acquire access authority without log-on. Not only sessions but also all information exchanged between the server and user could be tapped through hijacking [KLCYKLY05].
- Data tapping: Since the data transmitted via a communication channel may be exposed to an attacker, the possibilities for analyzing confidential information even when a third party acquires data should be removed to prevent a tapping attack.

7.2.3.2 Security requirements

Basically, the following security requirements should be taken into consideration:

- Confidentiality: the data used in communication should be recognizable only by legitimate users. Attackers must be prevented from noticing the source of data, destination, time, length, traffic characteristics of communication channels, etc. Confidentiality is secured through encryption preventing information analysis.
- Integrity: Data saved in an information system or transmitted through a network must be protected from falsification. When the data are falsified, deleted, or altered, the fact should be confirmable. Such ways as electronic signature are used to notice illegal modification of transmitted data.
- Authentication: it is vital to secure confidentiality in authentication services. The source of messages and electronic documents transmitted by a user, and whether the identification is false should be confirmable.

- Access control: Access authority over all reading and modification of resources should be clearly confirmed so as to prevent any unauthorized access. The access control level could be strengthened by utilizing invasion prevention systems in networks and access control functions in operating systems.

7.2.4 Related Work

This section describes the existing Kerberos authentication procedure, mobile commerce schemes, as well as their characteristics and advantages/disadvantages.

7.2.4.1 Kerberos

Kerberos uses a centralized authentication server and its encryption method uses symmetric encryption for authentication. Thus for a user to gain access he must be granted a ticket-granting ticket issued from the authentication server and a service-granting ticket from the ticket granting server. The user should remember a password agreed in advance for accessing each Kerberos component. The current Kerberos protocol, version 5, has been upgraded from version 4and has been standardized to comply with ETF RFC 4120 [NYHR05]. The Kerberos protocol has a weak point, however, in that its granting server does not preserve the user's anonymity and privacy when distributing the session key. Thus the message information is exposed and vulnerable to interception when being relayed between the user and the service provider's server.

7.2.4.2 Authentication Mechanism for Anonymity and Privacy Assurance

Using the EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) authentication method and the Symmetric-Key Key Establishment scheme, this research designed a more efficient authentication mechanism for the various online activities users enjoy. The suggested mechanism offers SSO (Single-Sign On) service, a service ensuring anonymity and privacy for the user and reliable authentication for the content provider. Upon a user's receiving authentication through the AAA server, content providers affiliated with the authentication server can continuously use the service without a separate login process. . It secures anonymity to the user and exchanges the session key for secure data transport between the user and content provider, without requiring the user to further engage with the authentication server. It secures the user privacy while guaranteeing content providers secure exchange of different session keys [LCY05].

7.2.4.3 AAA Mechanism

Wireless LAN is rapidly becoming a crucial component in next-generation mobile communication. Despite its success, there are many user privacy and access control issues such as authentication problems, accounting, billing problems. Especially in the field of accounting, research about packet accounting based on the IP alone is insufficient, thus, several ISPs (Internet Service Provider)'s adopted a fixed-sum accounting system. This thesis presents a packet accounting model within the AAA mechanism that is compatible with international standards of mobile commerce and the verification results [KLPSJ02]. However, the disadvantage is that payment confirmation and recharge must proceed via separate processes, thereby increasing the possibility of overhead communication between the home authentication server and the billing server.

7.2.4.4 User Authentication for IPTV Service

The goal of the proposed system is to provide an opportunity to use a flexible, user-centric authentication mechanism through Java Card applets in the IPTV application server and 3G Wideband Code Division Multiple Access (W-CDMA) networks. When a viewer watching IPTV is successfully authenticated, an authentication token allows the subscriber to conveniently use services that are adaptable to personal preference anywhere at anytime. In addition, this thesis presents analysis verifying the effectiveness and security of the proposed method. The main purpose of this research is to present a novel approach using Java Card to provide IPTV viewers with authentication, authorization and personalized services. In this thesis, the main focus is the design and development of architecture for IPTV viewer authentication, designed for use on the current popular 3G systems. Furthermore, identity management through Java Card provides users with more personalized services and control over who can view or use their private information *[*PLYLK08].

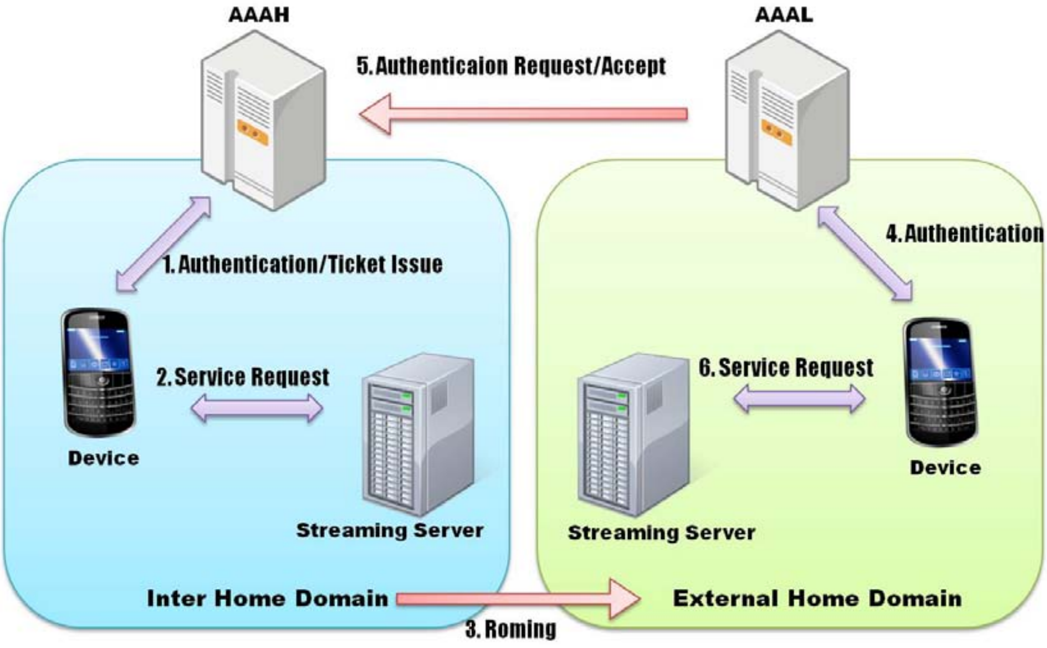


Figure 7.10 Whole flowchart for IPTV

7.2.5 Subscriber Authentication Technology for Mobile IPTV Service Offer

With regard to subscriber authentication technologies supporting mobile IPTV services, Figure 7.10 describes how in a home network environment, the device receives authentication from the home authentication server, receives the authorization ticket, presents the authorization ticket to the home network service, and receives IPTV services. In addition, when the device uses IPTV services by another service provider, the authorization ticket issued by the inner home domain of the foreign home is provided, authentication given, and services presented.

7.2.5.1 Notations

I use the following notations for Mobile IPTV service in this section.

Table 7.1 Notations for Mobile IPTV

Notation	Description
*	Objects (D : Device, $AAAH$: Home Network Authentication Server, $AAAL$: Foreign Network Authentication Server, $Streaming\ Server$: IPTV Streaming Server)
ID_*	Identification of *
OTP	One-time password
g	Generator with order $n-1$ in Z_n^*
$h(\ )$	One-way hash function
CT	Synchronization counter value
e	$G_1 \times G_1 \rightarrow G_2$ Bilinear Map
$E_*[\ ]$	Encryption with key of *
$Sign_*$	Signature of *
KS	Shared symmetric key between D and $AAAH$
$service\_key$	Shared service key between $AAAH$ and $Streaming\ Server$
KU_*	ID-based public key of *
KR_*	ID-based private key of *

7.2.5.2 Proposed Protocol

The proposed protocol is comprised of two phases, IPTV device authentication and authorization issuance phase in the home network, and the IPTV device authentication phase in foreign networks. It is supposed that a shared symmetric key will have been distributed between the device and home network prior to the time of authentication.

7.2.5.3 IPTV device authentication and authorization ticket issueance phase.

When the device requests the home network authentication server to present authentication, the authentication server issues the proper authorization ticket, and transmits the authorization ticket and ID to the streaming server. The device presents the authorization ticket to mobile IPTV services at the time of use.

Step 1. IPTV device generates OTP after XOR operation and hash of the serial number and symmetric key, and generates an ID based on a private key/public key pair. To request the authentication, the device's ID, home authentication server ID, OTP and counter are all encrypted by symmetric keys and transmitted.

$$OTP = h(PIN \oplus KS \oplus CT) \tag{7.3}$$

$$KU_D = ID_D \tag{7.4}$$

$$KR_D = ID_D \bullet g^{OTP} \tag{7.5}$$

$$ID_D,\ ID_{AAAH},\ E_{KS}[OTP, CT] \tag{7.6}$$

Step 2. The home network authentication server generates an OTP based on the values transmitted, saves it in the database, and compares them with the OTP sent by the device requesting authentication. Upon completion of authentication, the private key/public key pair are generated based on the ID of the home network authentication server, the authorization values and authorization ticket are generated and encrypted through the device public key, and finally transmitted.

$$OTP' = h(PIN \oplus KS \oplus CT) \tag{7.7}$$

$$OTP \stackrel{?}{=} OTP' \tag{7.8}$$

$$KU_{AAAH} = ID_{AAAH} \tag{7.9}$$

Step 3. The device certifies the values transmitted by the home network authentication server, specifically the acquired private key, home network authentication server ID, and symmetric key, by means of an Admissible Bilinear Map.

$$Authorization\ Value' = e(KR_{AAAH}, KS \bullet ID_D) \tag{7.10}$$

$$Authorization\ Value \stackrel{?}{=} Authorization\ Value' \tag{7.11}$$

Step 4. The home network authentication server encrypts the device ID and authorization ticket through the service key shared with the streaming server, signs them, and then broadcasts them.

Step 5. The device presents the ticket to the home network service the home network service certifies the ticket, and then provides the device with services.

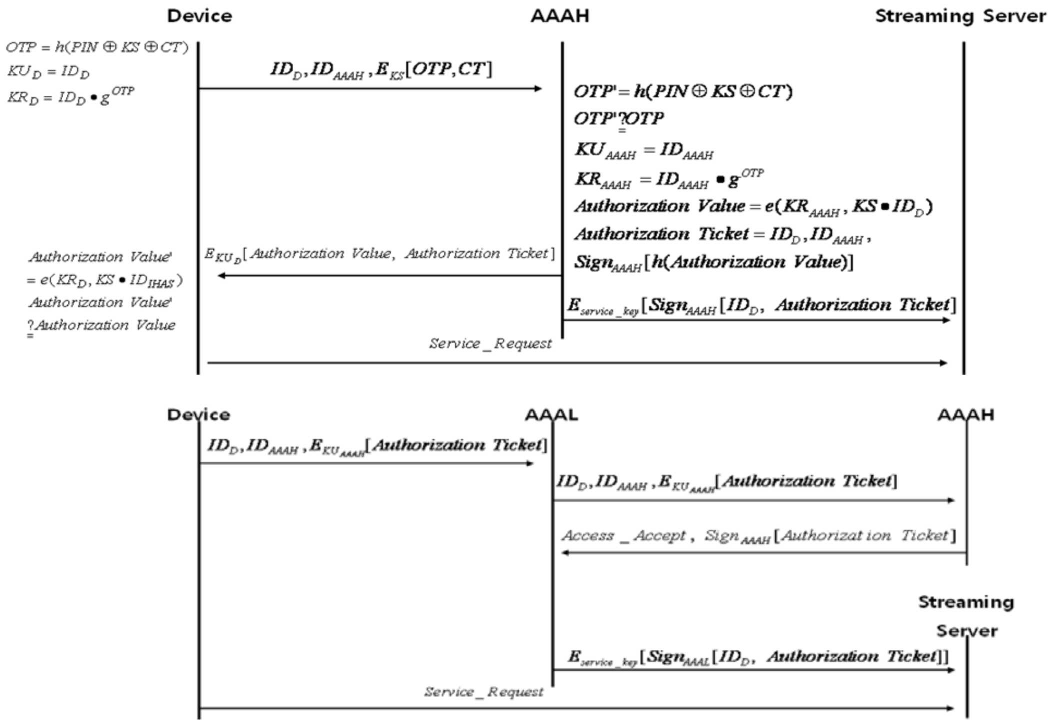

Device
AAAH
Streaming Server
OTP = h(PIN ⊕ KS ⊕ CT)
KU_D = ID_D
KR_D = ID_D • g^OTP
ID_D, ID_AAAH, E_KS[OTP, CT]
OTP' = h(PIN ⊕ KS ⊕ CT)
OTP' ?= OTP
KU_AAAH = ID_AAAH
KR_AAAH = ID_AAAH • g^OTP
Authorization Value = e(KR_AAAH, KS • ID_D)
Authorization Ticket = ID_D, ID_AAAH, Sign_AAAH[h(Authorization Value)]
E_KU_D[Authorization Value, Authorization Ticket]
Authorization Value' = e(KR_D, KS • ID_IHAS)
Authorization Value' ?= Authorization Value
E_service_key[Sign_AAAH[ID_D, Authorization Ticket]
Service_Request
Device
AAAL
AAAH
ID_D, ID_AAAH, E_KU_AAAH[Authorization Ticket]
ID_D, ID_AAAH, E_KU_AAAH[Authorization Ticket]
Access_Accept, Sign_AAAH[Authorization Ticket]
Streaming Server
E_service_key[Sign_AAAL[ID_D, Authorization Ticket]]
Service_Request

Figure 7.11 IPTV device authentication phase protocol in foreign network

7.2.5.4 IPTV device authentication phase in foreign network.

In this step, for the device to move to a foreign network and use mobile IPTV services, the foreign network authentication server is given an authorization ticket issued by the home network authentication server for authentication and providing services.

Step 1. The device encrypts the authorization ticket issued by the home network authentication server by means of the public key of the home network authentication server, and transmits it to the foreign network authentication server along with the ID.

$$ID_D, ID_{AAAH}, E_{KU_D}[Authorization\ \ Ticket] \tag{7.12}$$

Step 2. The foreign network authentication server transmits the values from the device to the home network authentication server; the home network authentication server certifies the authorization ticket, signs the authorization ticket authorizing the use of services, and then transmits it to the foreign network authentication server. The foreign network authentication server broadcasts the ticket to the foreign streaming server.

$$E_{KU_{AAAH}}[Authorization\ \ Tiucket] \tag{7.13}$$

$$Access\_Accept, Sign_{AAAH}[Authorization\ \ Ticket] \tag{7.14}$$

$$E_{Service\ key_{AAAH-Stream\ ing\ Server}}[Sign_{AAAL}[ID_D, Authorization\ \ Ticket] \tag{7.15}$$

Step 3. The device presents the ticket to the foreign streaming server, the streaming server certifies it, and presents services to the device.

7.2.6 Analysis

The proposed methods are analyzed according to the general security requirements in Section 7.2.4, security requirements against attacks, and security requirements in different networks. Table 7.1 presents the results of these analyses.

7.2.6.1 Security Threats Analysis

- Personal information security exposure: Personal information of users may be exposed to illegal access or hacking by a third party, which can cause monetary loss. Thus, to prevent leakage of personal information, data on a transmitting channel should be encrypted, and the authentication and authorization information should be managed in the form of a ticket to minimize the disclosure of personal information.
- Masquerade: A third party may disguise himself as a legal user, and receive authentication or services. Thus, OTP is used, and the information encrypted through an ID based on public key/private key pairs to protect it from masquerade.
- Session hijacking: Attackers may acquire access without proper procedures by snapping sessions on the communication channel. They also may steal the session through hijacking and even tap all information exchanged between the server and user. Thus, the time limit for sessions is set through a counter-based OTP, and the authentication values are not exposed even when the session is stolen, thereby preventing any risk of hijacking.
- Data tapping: Since the data transmitted through communication channels may be exposed to attackers, in order to prevent any tapping attack, the secret values should be resistant to analysis even in the event that the data is acquired by a third party.. In forming the secrete values, data integrity and confidentiality are secured through hash values.

7.2.6.2 Security Requirements Analysis

- Confidentiality: The data used in communication must be readable only by legal users. The proposed method is the public key/private key pair (,) based on the symmetric key) and ID shared between the device and home network authentication server. In each step, encryption secures confidentiality.
- Integrity: Any falsification and destruction of data transmitted through networks or saved in information systems should be prevented. The proposed method uses hash values to secure data integrity.
- Authentication: The falsehood of a user should be certifiable. The proposed method uses synchronization OTP (), and certifies an Admissible Bilinear Map based on authorization values () and authorization tickets that certify the use of specific services.
- Access control: It is necessary to classify the domains of authority to access such as reading and modifying information resources so as to prevent any attempts at unapproved access. Any device without authentication cannot be given an authorization ticket as well as foreign network access and services.

Table 7.2 Analysis of proposed scheme

	Kerberos	Authentication Mechanism for Anonymity and Privacy Assurance	Mobile Commerce AAA Mechanism	User Authentication for IPTV Service	Proposed scheme
Confidentiality	Symmetric key	Public key and symmetric key	Symmetric key	Symmetric key and PKI	Symmetric key and ID-based public key
Integrity	Non offer	Implicit integrity offer	Hash function	Timestamp and Keyed-hash	OTP and authentication
Authentication	Shared password	EAP-TLS	Challenge-response	Java Card	Using OTP and Ticket
Access control	Unauthorized device is not accessed				
Personal information security exposure	•	•	•	USIM	Ticket
Masquerade	•	•	•	USIM	Signature
Session hijacking	Nonce	Timestamp and lifetime	Nonce and sequence	Timestamp	Counter-based OTP and Authorization Value
Data tapping	Secure				
Efficiency	Delay of ticket issue	Non offer roaming	Overhead of authentication server and roaming problems	Extension offers but non offer efficiency	Fast roaming authentication and reduced home authentication server

7.3 Summary

In this chapter, I discussed services and applications using HUC-HISF. In ubiquitous computing environments, there are so many heterogeneous applications in 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 processes be performed without one's knowledge. However, nearly all existing authentication mechanisms request users' intervention and help. Thus I proposed a new model making it possible for a user to access any distributed service protected by heterogeneous applications and being authenticated only once at the initial stage. The centralized UIDM manages the object identifier that is universally unique. In addition, I proposed a novel privacy and access control scheme for my ubiquitous hybrid intelligent security framework using a surveillance system based on Kalman filter and HMM. Fortunately, in the near future spaces that are not covered by authentication applications can be managed by surveillance systems using surveillance devices. This means that an entity’s ID can be relayed to the next application following the movement of the entity.

As IT develops rapidly and the Internet and computers are widely distributed, thereby speeding up the expansion of digital materials and communication infrastructure, image and voice information shared over IP network connections, and the demand for integrated services is increasing. In addition, the demand is increasing for next-generation mobile IP networks that provide mobility among users. However, a number of problems are expected in terms of security on the other side of activation of IPTV services, and security threats will increase in these mobile environments. Thus, the development of security technologies is of great importance in order to ensure that mobile IPTV services are safe and efficient. This study also investigates subscriber authentication technologies, specifically the AAA mechanism, which provide safe and efficient IPTV services over mobile devices. For subscriber authentication, a method was used involving counters based on OTP and authorization tickets based on Admissible Bilinear MAP, and even when the service channel is changed from a home network to a foreign network, the mobile IPTV services are consistently guarded by means of authorization tickets. However, my protocol is not considered STB and standardized. In the future, there should be ways to evaluate services and their compatibility with IPTV standards through performance evaluations. Future studies will conform security protocols to STB standards and enhance compatibility.

Chapter 8. Simulation and Analysis of HUC-HISF

In this chapter, I present simulations and analyses of HUC-HISF. Section 8.1 demonstrates the key recovery attack on 8-round mCrypton and related security analyses. Section 8.2 shows the analysis of effective key distribution for my secure, fast handover model. I analyze the proposed mechanism in relation to existing mechanisms in terms of signaling costs and handover latency. Then I show the improved performance of my proposed mechanism compared to existing mechanisms. Section 8.3 summarizes the analysis of my privacy-enhanced key recovery model, and Section 8.4 analyzes a security simulation model based on the contract network protocol.

8.1 Advanced mCrypton

I show Key Recovery Attack on 8 Rounds mCrypton. Using the 7-round related-key rectangle distinguisher my 8-round attack recovers 5 bytes of each subkey for $K_{eq}, K^*_{eq}, K_{eq'}, K^*_{eq'}$ whose nibble positions are marked as * on ΔO depicted in Figure. 5.3, where $K_{eq} = \phi(K_8)$, $K^*_{eq} = \phi(K^*_8)$, $K_{eq'} = \phi(K_{8'})$, and $K_{eq'} = \phi(K_{8'})$ (recall that $\phi = \tau \circ \pi \circ \tau$). Since the keys K, K^*, K' and K'^* are related, the number of possible key quartets is 2^{40}. In order to understand the relations of the round keys of round 8, refer to Figure. 5.4.

The basic idea of my attack is as follows. Let (P, P^*, P', P'^*) be right quartet, (C, C^*, C', C'^*) be the corresponding ciphertext quartet and $D_k(\cdot)$ be a partial one round decryption with *k*, where *k* is a 5-byte key candidate of round 8. I guess a 5-byte key quartet (k, k^*, k', k'^*) and check that $D_k(C) \oplus D_{k'}(C') \in \Delta T^5$ and $D_{k^*}(C^*) \oplus D_{k'^*}(C'^*) \in \Delta T^5$, where ΔT^5 is a set of 5 gray nibbles described in ΔT of Figure. 5.3. If the number of ciphertext quartets passing the above test is more than an appropriate threshold, I consider the guessed key quartet as the right one.

Attack algorithm.

Input: Two pools of 2^{44} plaintext pairs.

Output: 5-byte key quartet of round 8.

1. Collect 2^{44} plaintext pairs (P_i, P^*_i) and 2^{44} plaintext pairs (P'_j, P'^*_j) with $P_i \oplus P^*_i = P'_j \oplus P'^*_j = \Delta P^*$. Encrypt the P_i, P^*_i, P'_j, P'^*_j with the keys K, K^*, K' and K'^{*}, respectively, to obtain their ciphertexts C_i, C^*_i, C'_j and C'^*_j. Keep all the obtained ciphertexts in a table.
2. Check that $C_i \oplus C'_j \in \Delta O$ and $C^*_i \oplus C'^*_j \in \Delta O$ for all *i,j*. Discard all the ciphertext quartets that do not satisfy this test.
3. Guess a 5-byte key quartet (k, k^*, k', k'^*) for round 8.

   3-1. For all ciphertext quartets (C_i, C^*_i, C'_j, C'^*_j) passing the test of Step 2, check that $D_k(C_i) \oplus D_{k'}(C'_j) \in \Delta T^5$ and $D_{k^*}(C^*_i) \oplus D_{k'^*}(C'^*_j) \in \Delta T^5$.

   3-2. If the number of quartets $(C_i, C^*_i, C'_j, C'^*_j)$ passing Step 3.1 is greater than or equal to 3, output the guessed key quartet (k, k^*, k', k'^*) as the right key quartet of round 8. Otherwise, go to Step 3.

Security analysis. Since the attack requires two pools of 2^{44} plaintext pairs and memory space for their ciphertext pairs, the data complexity of this attack is 2^{46} related-key chosen plaintexts and the memory complexity is $5\cdot2^{48} (= 2^{46}\cdot20)$ bytes.

Step 2 requires 2^{44} searches of 2^{44} ciphertext pairs, which can be done efficiently by sorting the ciphertext pairs, $(C_{j'}, C^*_{j'})$'s by $C_{j'}$'s. In Step 2, the test requires a 88-bit filtration (this is due to the fact that $C_i \oplus C'_j \in \Delta O$ and $C^*_i \oplus C'^*_j \in \Delta O$ with probability $2^{-88} (= 2^{-11\cdot4\cdot2})$ for a wrong quartet $(C_i, C^*_i, C_{j'}, C^*_{j'})$), and thus the expected number of ciphertext quartets passing the test of Step 2 is about $7(\approx 2^{88}\cdot(\frac{3}{2}\cdot2^{-86} + 2^{-88}))$ (here, $2^{88}\cdot\frac{3}{2}\cdot2^{-86} = 6$ ciphertext quartets passing the test are expected to be right quartets due to my 7-round related-key rectangle distinguisher). Using this expected number of quartets I can estimate the time complexity of Step 3, i.e., Step 3 requires about $2^{41}(\approx 2^{40}\cdot7\cdot4\cdot\frac{1}{8}\cdot\frac{1}{2})$ 8-round mCrypton encryptions on average. Hence, the time complexity of this attack is dominated by Step 1, and thus this attack requires about 2^{46} 8-round mCrypton encryptions.

The success rate of the attack is computed as follows. The probability that for the right key quartet there exist at least 3 quartets passing the test of Step 3.1 is about 0.94 $(\approx \sum_{i=3}^{2^{88}} \binom{2^{88}}{i} (\frac{3}{2}\cdot2^{-86})^i (1-\frac{3}{2}\cdot2^{-86})^{2^{88}-i})$, while the probability that a wrong key is outputted by the attack algorithm is $2^{-67}(\approx 2^{40}\cdot\sum_{i=3}^{2^{88}} \binom{2^{88}}{i} (2^{-123})^i (1-2^{-123})^{2^{88}-i})$. Therefore, the success rate of this attack is about $0.94(\approx 0.94\cdot(1-2^{-67}))$.

8.2 Effective Key Distribution for Secure Fast Handover

8.2.1 Performance analysis

In this section, I analyze the proposed mechanism with Mobile IPv6 and Fast Mobile IPv6 in terms of signaling cost and handover latency. Signaling cost represents the cost for the establishment of handovers between different access networks. On the other hand, handover latency refers to the time duration from the time a mobile node switches over in the link-layer to the time a binding update is received by the home agent or a corresponding node. In conducting my performance analysis, I make the following assumptions.

- The data session arrival for the mobile node is exponentially distributed with its mean session holding time $T_s = \mu_s^{-1}$.
- The mobility rate, λ_m, is obtained as the ratio between the velocity of mobile node and the coverage.
- The domain occupancy time of the mobile node is exponentially distributed with its mean occupancy time λ_m^{-1}.

8.2.1.1 Timing diagram

I here present the timing diagrams for each protocol mechanism. The handover timing diagram consists of the link switching latency, t_L, the IP connectivity latency, t_I, the session key distribution latency, t_K, and the location update latency, t_U [KP01, KK04]. Link switching latency refers to the link-layer handover latency. IP connectivity latency represents the time required for detecting the move and configuring the address. Session key distribution latency includes authentication latency, $t_{K\text{-}auth}$ and session key acquisition latency, $t_{K\text{-}acq}$. The location update latency is the time incurred for binding updates.

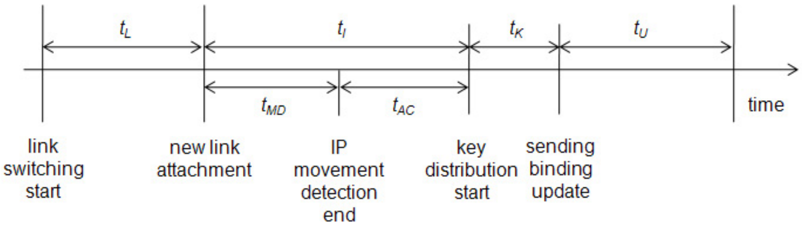


Figure 8.1 Timing diagram for Mobile IPv6

Figure 8.1 shows the timing diagram for Mobile IPv6. The mobile node attaches to the new link as it finishes switching links. Then, the mobile node obtains its care-of address after movement detection and address configuration. Accordingly, IP connectivity latency is the sum of the movement detection latency, t_{MD}, and the address configuration latency, t_{AC}. Then, the mobile node is authenticated based on its pre-shared key. Subsequently, the mobile node obtains the session key that will be used in the new access network. Finally, the mobile node sends its binding update message to its home agent and corresponding nodes to inform them of its new location information.

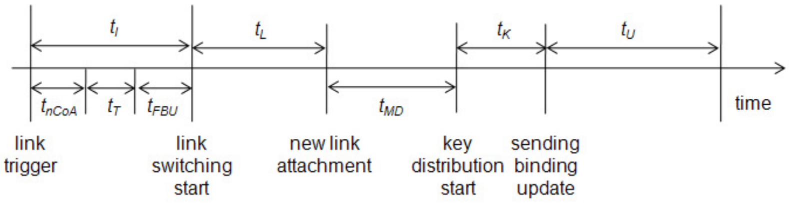


Figure 8.2 Timing diagram for Fast Mobile IPv6

Figure 8.2 shows the timing diagram for Fast Mobile IPv6. In Fast Mobile IPv6, the mobile node previously obtains its care-of address for the new access network. In other words, the address configuration is completed before its link-layer handover takes place. Let t_{nCoA} and t_T be the latency for acquiring a new care-of address and for establishing tunneling between the previous access router and the new access router, respectively. Assume that t_{FBU} is the latency for the FBU. As the mobile node attaches to the new access network, it needs to perform the duplicated address detection t_{MD}. Then, the authentication procedure for the mobile node is performed and the mobile node obtains its session key. Fast Mobile IPv6 reduces handover latency due to early address configuration for the newly accessed network. However, its authentication and session key acquisition procedures are performed after the mobile node attaches to the new access network. Accordingly, the session key distribution latency, t_K , cannot be reduced, e.g., t_K for Fast Mobile IPv6 is the same as that of Mobile IPv6.

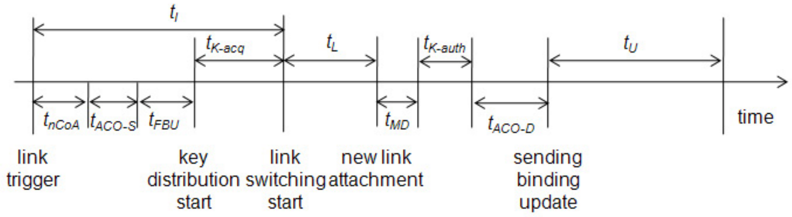


Figure 8.3 Timing diagram for the proposed mechanism

In the proposed mechanism, the session key acquisition procedure is performed before the mobile node attaches to the new access network. In addition, the mobile node establishes new communication sessions for corresponding nodes in previous access networks using SCTP ASCONF messages. Let $t_{ACO\text{-}S}$ and $t_{ACO\text{-}D}$ be the latencies for ASCONF (Set) and ASCONF (Deletion), respectively. Then, t_I, which is performed in the previous access network, is the sum of t_{nCoA}, $t_{ACO\text{-}S}$, t_{FBU}, and $t_{K\text{-}ACQ}$. Accordingly, the proposed mechanism needs to perform three procedures, authentication, ASCONF (Deletion), and sending a binding update for its home agent procedures -- in order to access the new network.

8.2.1.2 Signaling cost

In this sub-section, I present the signaling cost for the proposed mechanism compared to Mobile IPv6 and Fast Mobile IPv6. Similar to [KK04], the signaling cost includes the processing cost at each communication involved node and the transmission cost at each communication path. I assume that the home agent and corresponding node are connected to its network through the wired link. In addition, the transmission cost is proportional to the distance between the communication source and destination. Let δ be the proportionality constant. Then, I also assume the transmission cost over the wireless link is ρ times higher than the case of the wired link. For example, $T_{NAR\text{-}HA}$ is calculated as $l_{NAR-HA}\delta$, where $l_{NAR\text{-}HA}$ is the hop distance between the new access router and the home agent. Let A_γ and K_δ be the authentication cost and the session key acquisition cost, respectively. I assume that all protocols have A_γ as the same cost. I now denote the signaling costs of the proposed mechanism, Mobile IPv6, and Fast Mobile IPv6 as C_{pro}, C_{mip}, and C_{fast}, respectively. Then, the signaling cost for Mobile IPv6, C_{mip}, is expressed as follows.

$$\begin{aligned} C_{mip} &= 3T_{MN-NAR} + T_{NAR-HA} + A_\gamma + K_\delta \\ &\quad + P_{HA} + \kappa(T_{MN-NAR} + T_{NAR-CN} + P_{CN}) \end{aligned} \tag{8.1}$$

where κ is the number of corresponding nodes for the mobile node. $T_{MN\text{-}NAR}$ is calculated as $l_{MN-NAR}\rho\delta$, where $l_{MN\text{-}NAR}$ is the hop distance between the mobile node and the new access router. Because the mobile node is connected to the access routers through its wireless interface, $l_{MN\text{-}NAR}$ and $l_{MN\text{-}PAR}$ are assumed to be 1. Other transmission costs are calculated in the similar way. In Eq. (8.1), the session key acquisition cost, K_δ, can be expressed as $2(T_{MN-NAR} + T_{NAR-HA})$ if I assume the KDC is co-located to the home agent.

For the signaling cost of Fast Mobile IPv6, C_{fast}, I consider the transmission costs incurred between the mobile node and the access routers as follows.

$$\begin{aligned} C_{fast} &= 4T_{MN-PAR} + 3T_{PAR-NAR} + 4T_{MN-NAR} \\ &+T_{NAR-HA} + 3P_{PAR} + 2P_{NAR} + A_{\gamma} + K_{\delta} \\ &+P_{HA} + \kappa(T_{MN-NAR} + T_{NAR-CN} + P_{CN}) \end{aligned} \tag{8.2}$$

where K_{δ} is the same to that of Eq. (8.1) because the mobile node in Fast Mobile IPv6 needs to obtains its session key from the KDC for every movements.

For the signaling cost of the proposed mechanism, C_{pro}, I additionally consider the transmission costs incurred between the mobile node and corresponding node as follows.

$$\begin{aligned} C_{pro} &= 2T_{MN-PAR} + T_{MN-NAR} + T_{NAR-HA} \\ &+P_{HA} + A_{\gamma} + K_{\delta} \\ &+ \kappa(T_{MN-NAR} + T_{NAR-CN} + P_{CN}) \end{aligned} \tag{8.3}$$

where K_{δ} is calculated as $T_{PAR-NAR} + T_{MN-NAR}$, because the session key is delivered from the previous access router, not connecting to the KDC located in the home agent.

8.2.1.3 Handover latency

Based on the presented timing diagrams in Section 8.2.1.1, I calculate the handover latency for each protocol. In this thesis, I only focus the network layer handover latency so that the link switching latency, t_L, is assumed to be the same for each protocol. I denote the handover latencies of the proposed mechanism, Mobile IPv6, and Fast Mobile IPv6 as L_{pro}, L_{mip}, and L_{fast}, respectively. Then, the handover latency for Mobile IPv6, L_{mip}, is as follows.

$$L_{mip} = t_I + t_K + t_U \tag{8.4}$$

where t_I is calculated as the sum of t_{MD} and t_{AC}. In [JPA04], the movement detection is the half of the average time between the unsolicited router advertisement messages. Then, t_{MD} is simply calculated as

$$\frac{MinRtrAdvInterval + MaxRtrAdvInterval}{4} \tag{8.5}$$

where *MinRtrAdvInterval* and *MaxRtrAdvInterval* are the minimal value in milliseconds for the router advertisement message and the maximum value in milliseconds for the router advertisement message, respectively. Let *RetransTimer* and *DupAddrDetectTransmits* be the retransmission timer and the number of consecutive Neighbor Solicitation messages sent while performing duplicate address detection on a tentative address. As described in [TN98, HCH06], t_{AC} is simply calculated as $RetransTimer \cdot DupAddrDetectTransmits$.

As the mobile node attaches to the new access network, $t_K = t_{K-auth} + t_{K-acq}$ is occurred for authentication and session key acquisition. I assume that the authentication latency for each protocol is the same. Let B_{wl} and B_{wd} be the wireless bandwidth and the wired bandwidth, respectively. Also, I define σ_{wl} and σ_{wd} as wireless link latency and wired link latency, respectively. Then, $t_{K\text{-}acq}$ for Mobile IPv6 is calculated as

$$t_{K-acq} = 2\Big((\frac{M_k}{B_{wl}} + \sigma_{wl}) + l_{NAR-HA} (\frac{M_k}{B_{wd}} + \sigma_{wd}) \Big) \tag{8.6}$$

where M_k is the session key message size in where the request and reply messages are assumed to be the same size. Let $t_{U\text{-}h}$ and $t_{U\text{-}c}$ be the locate update latencies for the home agent and corresponding host, respectively. t_U is consists of two parts. Thus, I define t_U as $max(t_{U-h}, t_{U-c})$. Then, similar to Eq. (8.6), $t_{U\text{-}h}$ and $t_{U\text{-}c}$ for Mobile IPv6 are calculated as

$$\begin{aligned} t_{U-h} &= (\frac{M_b}{B_{wl}} + \sigma_{wl}) + l_{NAR-HA} (\frac{M_b}{B_{wd}} + \sigma_{wd}) \\ t_{U-c} &= (\frac{M_b}{B_{wl}} + \sigma_{wl}) + l_{NAR-CN} (\frac{M_b}{B_{wd}} + \sigma_{wd}) \end{aligned} \tag{8.7}$$

where M_b is the binding update message size. Note that Mobile IPv6 standard document does not require the mobile node to receive the binding acknowledge message [JPA04].

The mobile node in Fast Mobile IPv6 performs its address configuration procedure before starting the link-layer switching. Accordingly, the handover latency for Fast Mobile IPv6, L_{fast}, is expressed as follows.

$$L_{fast} = t_{MD} + t_K + t_U \tag{8.8}$$

t_{AC} is simply omitted compared to that of Mobile IPv6. For the latencies of t_K and t_U, I can calculate them in the same ways as shown in Eqs. (8.6) and (8.7).

In the proposed mechanism, the address configuration and location update for the corresponding node is completed before the mobile node attaches to the new access network. In addition, the session key acquisition is also performed in the previous access network. Therefore, the handover latency for Fast Mobile IPv6, L_{pro}, is expressed as follows.

$$L_{pro} = t_{MD} + t_{K-auth} + t_{U-h} \tag{8.9}$$

where $t_{U\text{-}h}$ is calculated as the same way in Eq. (8.8).

8.2.2 Evaluation results

In this section, I compare the performance evaluation results of the proposed mechanism to Mobile IPv6 and Fast Mobile IPv6. The presented evaluation results are based on the signaling cost and handover latency models presented in the previous section. In order to perform the numerical evaluation, I first set the evaluation parameter values as shown in Table 8.1. The defined parameter values are common values and widely used in the literature.

Table 8.1 Evaluation parameters [JPA04, KK04, TN98, HCH06]

Notation	Description	Default Value
l_{MN-PAR}	The hop distance between the mobile node and the previous access router	1
l_{MN-NAR}	The hop distance between the mobile node and the new access router	1

$l_{PAR-NAR}$	The hop distance between the previous access router and the new access router	3
l_{NAR-HA}	The hop distance between the new access router and the home agent	7
l_{NAR-CN}	The hop distance between the new access router and the corresponding node	5
l_{PAR-CN}	The hop distance between the previous access router and the corresponding node	5
P_{PAR}	The processing cost at the previous access router	5
P_{NAR}	The processing cost at the new access router	5
P_{HA}	The processing cost at the home agent	10
P_{CN}	The processing cost at the corresponding node	5
A_{γ}	& The authentication cost for the mobile node	10
δ	The proportionality constant for the transmission cost	0.1
ρ	The additional wireless link cost	2
κ	The number of corresponding node for the mobile node	5
MinRtrAdvInterval	The minimal value for the router advertisement message	30ms
MaxRtrAdvInterval	The maximum value for the router advertisement message	70ms
RetransTimer	The retransmission timer	1000ms
RetransTimer	The number of message sent during address duplication detection	1
t_{K-auth}	The authentication time for the mobile node	0.5ms
M_k	The session key request/reply message size	50bytes
M_b	The binding update message size	72bytes
M_d	The data packet size	100bytes

8.2.2.1 Impact of mobile node velocity on signaling cost

In this sub-section, I provide the evaluation results on signaling cost. For the mobility rate, λ_m, I vary the speed from 10 km/h to 120 km/h and consider two types of network coverage. In other words, I use the network coverage for 3GPP (7.5 km) and network coverage for WLAN (1 km).

Figure 8.4 shows the impact of mobile node speed on signaling cost for wide network, i.e., 3GPP coverage. First, I can see that at high speeds the mobile node incurs high signaling costs due to its increased movement between different access networks. Similar to previous results for handover performance, the results presented in Figure 8.4 show that Fast Mobile IPv6 incurs high costs to support its fast handover mechanism. Especially, the additional required messages that enable the mobile node to configure the new care-of address cost more in signaling than Mobile IPv6. However, the proposed mechanism consumes signaling costs similar to Mobile IPv6. This is because the proposed mechanism uses SCTP based address configuration and provides reduced session key acquisition latency. Note that the mobile node in the proposed mechanism obtains its session key from the previous access router, whereas the mobile node in other protocols obtains the session key from the KDC.

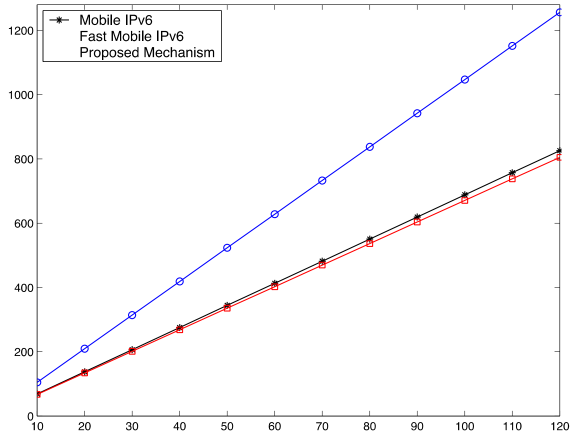


Figure 8.4 Impact of mobile node velocity on signaling costs for wide network coverage

Figure 8.5 Impact of mobile node velocity on signaling cost for small network coverage

When narrow network coverage is available to the mobile node, it moves frequently between different access networks. Such small network coverage increases the mobility rate, λ_m, and mobility rate increases the signaling cost for all protocols. Figure 8.5 shows the impact of mobile node speed on signaling costs for small networks, i.e., WLAN. Similar to the results in Figure 8.4, Fast Mobile IPv6 incurs a higher cost than others and the proposed mechanism outperforms all other protocols as well.

8.2.2.2 Impact of hop distance between the mobile node and KDC on session key distribution latency

Figure 8.6 displays the results of session key distribution latency when varying the hop distance between the mobile node and the KDC. From the analysis of timing diagrams presented in Section 8.2.1.1, I are well aware that the hop distance between the mobile node and the KDC is one performance factor contributing to session key distribution latency as well as the total handover latency. As shown in Figure 8.6, the proposed mechanism provides a lower session key distribution latency than others. In addition, the latency of other protocols is increased as the hop distance between the mobile node and the KDC is increased. In the proposed mechanism, the mobile node obtains its session key from the previous access router so that the proposed mechanism is not affected by the hop distance. The impact of hop distance between the mobile node and KDC appears to be a more important factor when the KDC is located in the AAA server. This is because the AAA server is usually located far way from the access router for mobile nodes.

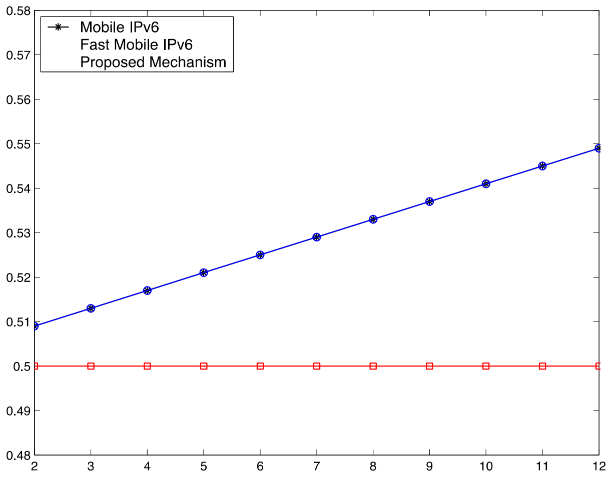


Figure 8.6 Impact of hop distance between the mobile node and the KDC on session key distribution latency

8.2.2.3 Impact of mobile node velocity on packet loss

Based on the handover latency for each protocol, I estimate the amount of packet loss. Let us assume that the corresponding node sends data packets at λ_s kbps. Then, the amount of packet loss can be calculated as follows.

$$P_L = \frac{L}{P_T} \tag{8.10}$$

where L is the handover latency and P_T is the packet time which can be expressed as M_d / λ_s [RASC07]. To estimate packet loss, I set λ_s as 64 kbps and then I vary the velocity of mobile node from 10 km/h to 120 km/h. Figure 8.7 shows the amount of packet loss for wide network coverage. The mobile node with Mobile IPv6 losses much more than others and the amount of packet loss is increased as the velocity increases. Fast Mobile IPv6 shows low packet loss due to its reduced handover latency. While the proposed mechanism exhibited low packet loss similar to Fast Mobile IPv6, it still outperformed Fast Mobile IPv6 because Fast Mobile IPv6 and Mobile IPv6 must obtain the session key from the KDC for every movement. This delay in key acquisition accounts for the increased handover latency and increased packet loss.

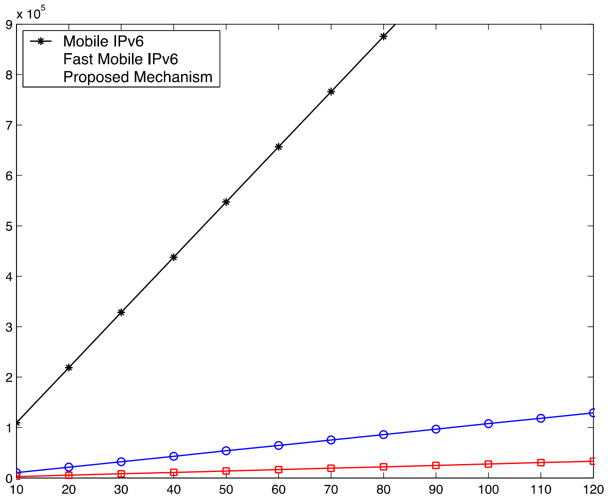


Figure 8.7 Impact of mobile node velocity on packet loss for wide network coverage

Figure 8.8 Impact of mobile node velocity on packet loss for small network coverage

In Figure 8.8, the packet loss for the case of small network coverage is shown and these results are similar to that of Figure 8.7. Due to the reduced network coverage, the mobile node moves frequently, thus the number of movements is also increased. From the result of Figure 8.8, I can see that Mobile IPv6 does not provide acceptable support for real-time applications. In order to support such real-time applications, I need to deploy mobility protocols that support fast handover such as Fast Mobile IPv6 and the proposed mechanism.

8.3 Privacy-Enhanced Key Recovery

8.3.1 Analysis of the proposed Security-Enhanced KR Protocol

In B’s domain, if B sends a bogus value $w_B \square r'_B \square g^{brA}$ instead of $w_B \square r_B \square g^{brA}$, A may generate $h(w_B \square r'_B)$ and send it to B. In this case, a monitoring third party V can prove validity as follows.

First V obtains public value $\square_B$ and computes

$$c'_B=h(w_B \square r'_B) \bmod q. \tag{8.11}$$

Therefore,

$$g^{sB} \square \square^{c'B} \square_B. \tag{8.12}$$

In my protocol, I used $w_B \square r_B$ instead of r_B when computing session key, K_{AB}. Only B knows w_B , and KRA_B and r_B is newly generated by B every session. Therefore, the security of $w_B \square r_B$ depends on random number, r_B.

The user A can generate session key, K_{AB} as follows. He calculates $(g^b)^{rA}$ and then computes $w_B \square r_B$ from $w_B \square r_B \square g^{brA}$ using $(g^b)^{rA}$. Therefore,

$$K_{AB}= h_1(w_B \square r_B, g^{brA}). \tag{8.13}$$

B can generate session key, K_{AB} as follows. She calcu7lates $(g^{rA})^b$ and then computes $w_B \square r_B$, using w_B and r_B , which he knows. Therefore,

$$K_{AB}= h_1(w_B \square r_B, g^{rAb}). \tag{8.14}$$

I used s_B instead of $\{s_B\}K_{AB}$ in Token 2. Even if a monitoring third party V knows s_B, it cannot fabricate session key K_{AB}. This is because he cannot obtain $h(w_B \square r_B)$ or r_B from s_B, w_B, and g^{rB} , which he knows, until Token 2 is passed.

Furthermore, the security of my protocol can be reduced to that of the non-interactive proof of possession of $\log_g \square$ implemented in *Schnorr*’s signature scheme [SC90] as in *Nieto et al.*’s proposal [NPBD00].

Now I compare existing protocols and my proposed security-enhanced protocol in terms of computational overhead. In Table 8.2, I present the number of modular exponentiation in A’s and B’s side. The number within the bracket refers to the number of the required online modular exponentiation when pre-computation is allowed. My protocol supports public KRI validation on both A’s and B’s side and my session key computation, including only simple exclusive-OR operations, is more efficient than *Kim* and *Lee*’s protocol which multiplies g^{brA} by g^{rB} to obtain $h_1(g^{brA}g^{rB})$.

Table 8.2 Comparison of WAKE Protocols

Protocols	Modular operation		Additional transmission overhead	Public validation	KRI
	A’ side	B’s side			
ASPeCT WAKE	2(1)	1(1)			
KR enhanced	3(1)	1(1)	s_A, $\{A\}_L$ or $\{A,r_A\}_L$	None	

Modified enhanced KR	2(1)	1(1)	$\{s_B\}K_{AB}$, s_A, s_B	A
Improved enhanced KR	2(1)	2(1)	g^{rB}, $\{s_B\}K_{AB}$, s_A, s_B	A
Proposed protocol	2(1)	2(1)	$h(w_B \oplus r_B)$, $\{s_B\}K_{AB}$, s_A, s_B	A, B

8.3.2 Analysis of the proposed Privacy-Enhanced KR Protocol

In this protocol, I protect the location privacy of user A by adding $(g^{rA}, K_A)K_{TDA}^{-1}$ in Token 1 for the authentication of A to B instead of eliminating certificate of A, A_{Cert} in Token 3. Here, the K_A in Token 3 is A’s temporary verification key, which is generated by TD_A for communication with B. The TD_A can bind the key of A to the identity of A, but it can be connected and used by only user A for secure external computation and storing. Generally, the TD_A is located in A’s house and shares public key pairs with A. For more detailed information regarding the TP method, please see the paper [KRJ98] and [KYPK05].

This feature guarantees that there would be no information revealing A’s true identity among any of the communication tokens. Therefore, even network operators and authorized third parties cannot get any user specific information from the network. Ultimately, this privacy-enhanced protocol guarantees wireless authentication, key establishment, key recovery, and privacy protection.

8.4 Security Simulation Model based on Contract Network Protocol

The increase of network utilization and the weekly increase in the number of critical application layer exploits means that NIDS designers must find ways to speed up their attack analysis techniques when monitoring a fully-saturated network and maintaining a good false positive to false negative ratio. To evaluate the simulation results, I have selected the intrusion detection time and the false positive error ratio as performance indices. The intrusion detection time represents the time that elapses while detecting an intrusion. The false positive error ratio is the ratio that regards no intrusion as an intrusion [Pr01]. I executed the simulation for a single IDS, multiple IDSs with CNP, and multiple IDSs with CNP & Rete algorithm. Figure 8.9 presents the difference of intrusion detection time as the detection threshold value of the DOS jolt attack is increased. According to the results of the simulation, the detection of multiple IDSs with CNP is faster than that of the single IDS and the detection time of multiple IDSs with CNP & Rete is fastest of them all. Simulation results show that the proposed system (multiple IDSs with CNP & Rete) delivers a superior performance over previous schemes by more than one performance indexes. In Scenario 1, the single IDS is attacked by the external attacker. In Scenario 2, the multiple IDSs with CNP are attacked and in Scenario 3, the multiple IDSs with CNP &Rete is the object of attack.

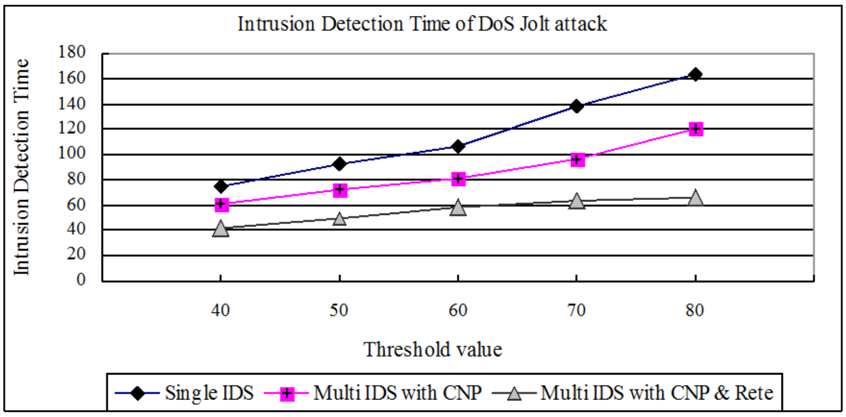


Figure 8.9 Intrusion detection time of jolt attack

Figure 8.10 shows the difference in the false positive error ratio as the detection threshold value of the DOS jolt attack is increased. Multiple IDSs with CNP are superior to a single IDS and the application of the rete algorithm to multiple IDSs with CNP reduces the false positive error ratio. As the detection threshold value increases, the false positive error ratio decreases.

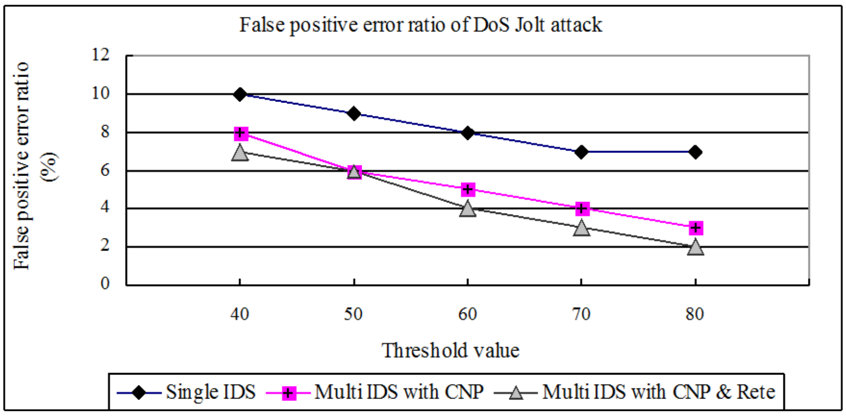


Figure 8.10 False positive error ratio of jolt attack

Figure 8.11 presents the intrusion detection time of DDOS trinoo attacks as the number of detection rules is increased. Detection by multiple IDSs with CNP is faster than that by a single IDS. yjr performance of multiple IDSs with CNP & Rete is yet faster and exhibits a nearly fixed detection time.

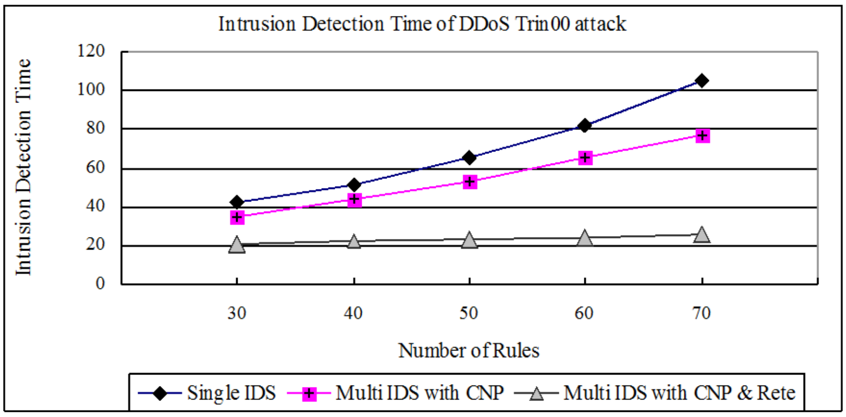


Figure 8.11 Intrusion detection time of trinoo attack

Figure 8.12 shows the false positive error ratio for the DDOS trinoo attacks as the number of detection rules is increased. Multiple IDSs with CNP & Rete has the lowest false positive error ratio and is hardly influenced by the number of detection rules.

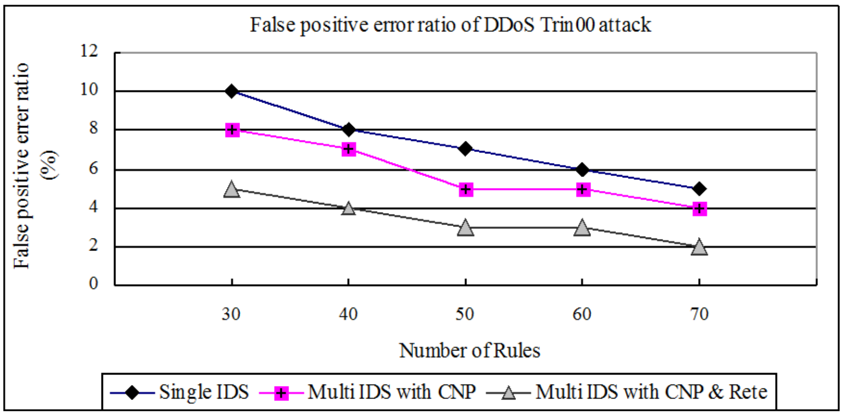


Figure 8.12 False positive error ratio of trinoo attack

Chapter 9. Conclusion

New computing paradigms such as ubiquitous computing and human-centric computing are up and coming due to rapid advances in computing power and network development. Such paradigm changes offer convenient and delightful, human-centered services. However, the ubiquitous and human-centric computing environments have been integrated; there exists a much greater likelihood of exposure to security threats compared to ordinary computing environments. And there are additional threats not present in traditional computing environments; such threats include tampering, signal interference, and battery consumption attacks. Especially in one of most human closed network environment, the ubiquitous computing environment of the human-centered network is compromised by an attack, which could be network information derived from an individual's privacy can cause problems. Than a typical network environment comprised of a human-centered environments in ubiquitous environment is larger than in recent years expanded by service extension.

In particular environment U-health system for the health of the individual person's, the individual's profile in the center of the system have to configured, also that should be prepare a human-centric services, however in your personally identifiable information, including personal health information, the details of the disclosure, number of frequency health problems, any health insurance available, and any u-health system is used information, are used for any purpose whether can still be pirated and illegal market selling. In addition, sensor network system is one of human centered environment in ubiquitous computing area. Sensor networks is principal of information collecting in the individual's human-centered computing, human-centered information. Because of this, personal information about living in an environment, where temperature, humidity, and any location information, which also collects the most ubiquitous model, is presented in a smart home or ubiquitous environment.

This is also theft to be, the individual pattern of living, any habit that the person have, the current home and whether or not, if the person is home than where stay in the house, and where stay at that time, where all the information about the acquisition, which the theft occurred, it makes another big problem occurring.

In recent years, human-centered computing environment will develop reaches and clearly. As a representative of the reason, Smart Home and Smart Car system will be mostly important system and role based on Smart Grid as Human-Centric Service or system. In modern society, the electrical energy is the most important energy, energy conservation developed by the ultimate purpose of human-centric networks for large-scale energy that can be. So, we need intelligent and dynamic security frameworks for secure and flexible human-centric ubiquitous computing environments.

In addition, human-centered computing environment to take place in the center of the diversity of individuals, depending on the required profile, and more than profiling to provide services to individuals close to the basic information is available. This human-oriented, close to the human complex network computing technologies in the current configuration, it should be safe, and a variety of attacks that can occur in the future it is clear that the purpose be.

In this chapter, I summarize and briefly describe contribution of this thesis. In the introduction, this thesis described the overview, scope, aim, method, contribution and outline of this study. I described previous part which described a variety of today's network, it can occur in human-centered computing environment to be considered a sufficient security problems. And the thesis briefly mentioned the problem statements and motivation for a secure and H-Ubi Comp. In Chapter 2, the thesis discussed the background and related works of secure and H-Ubi Comp. I summarized most important existing human-centered computing environment research especially recent research on human-centered computing. One of them, large-scaled collaboration is critical issues of human-centered computing environment, the actual practices applied by checking the current implemented system such as Amazon automatic answering system on FAQ pages. Based on these summarized and analysis and the importance of human-centered computing environment, a report composed which part should be implement of effective and optimized security techniques.

In Chapter 3, I proposed the HUC-HISF. To offer security for a human-centered computing environment described above, the development of a wide variety of computing environments and the resulting human-centered computing environment has suggestions for a secure composing.

In Chapter 4, I presented cryptanalytic result on mCrypton, it is worthwhile to apply this attack to other block ciphers and to study simple key scheduling algorithms which may be resistant to this kind of attack. In addition, for many types of attacks, how to composing the method proposed to prevent and detection as effectively explained.

In Chapter 5, I described an effective session key distribution mechanism and a number of WAKE protocols having a key recovery feature. In Chapter 6, I proposed dynamic human-context access control mechanism. In Chapter 7, the thesis presented U-Surveillance service and Mobile IPTV service using HUC-HISF. In Chapter 8, to show the differentiated properties of HUC-HISF, the proposed schemes were analyzed by the aspects of performance, aspects of security among system requirements for the HUC-HISF.

This thesis presented an intelligent and dynamic security framework considering human aspects for human-centric ubiquitous computing. The proposed HUC-HISF provides a light-weight cryptography algorithm for security in resource-constrained applications, such as low-cost RFID tags and sensors in USN. It has the structure with some improvements in software and hardware efficiency under resource-restricted environments – such as ubiquitous mobile devices. In addition, I proposed improved security protocols for the HUC-HISF and discussed surveillance service and mobile IPTV service for applying HUC-HISF.

To realize a more secure and dynamic human-centric ubiquitous computing environments, I need to expand our researches. As a further extended future study, the ubiquitous environmental and human-centric computing environments with extended smart grid, smart home environment, to apply to the security module. Also, specific architecture framework components for detailed studies should be preceded by the component definition. In addition, all modern computing environments are composed of human-centered environments, more close to human the technology, human to interact with humans must be based on the fact that the technology will become clear, the security technology must also be followed part is obvious. In future research can be applied to today's smart environments and will be define the detailed technology and security architecture will offer configurations.

Finally, I will develop our researches by combining them with other important issues in converged IT environments.

References

[2W01] 2WEAR, 2001, Available from http://2wear.ics.forth.gr/

[Ab10] Aborn, J.A., et al., "Presence Detection for Cellular and Internet Protocol Telephony", US Patent, Aplication No.: 11/183,379, Filing date: 18th July, 2005, Date of Patent, October, 2010.

[Ab11] Abhijan Bhattacharyya, On the Potential of Using Conventional Mobile Communication Technology for Human Context Awareness in Ubiquitous Computing, CCIS 190, pp. 242-249, Springer-Verlag, 2011.

[ACDGM08] Agichtein, E., Castillo, C., Donato, D., Gionis, A., Mishne, G., "Finding high-quality content in social media", In: WSDM, pp. 183-194. ACM, New York, 2008.

[ACT97] ACTS AC095, ASPeCT Deliverable D02, "Initial Report on Security Requirements", AC095/ATEA/W21/DS/P/02/B, 1997, Available from http://www.esat.kuleuven.ac.be/cosic /aspect/

[Ag07] Agrawal, A., et al., WS-BPEL Extension for People (BPEL4People), V1.0, 2007.

[Ah06] Von Ahn, L., "Games with a purpose", IEEE Comput. 39(6), pp. 92-94, 2006.

[AHEA06] Adams, M., ter Hofstede, A.H.M., Edmond, D., Aalst, W.M.P.V.D., "Worklets: a service-oriented implementation of dynamic flexibility in workflows", In: OTM Conferences (1), pp. 291-308, 2006.

[Am07] Amend, M., et al., Web Services Human Task (WS-HumanTask), Version 1.0, 2007.

[Am99] Amoroso, E., Intrusion Detection - An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response, Intrusion.Net Books, 1999.

[AMSW97] B. Askwith, M. Merabti, Q. Shi, and K. Whiteley, "Achieving User Privacy in Mobile Networks", 13th Annual Computer Security Applications Conference, 1997.

[AS11] Ahmed Al-Vahed, Haddad Shhavi, "An overview of modern cryptography", World Applied Programming, Vol. 1, No. 1, pp. 3-8, 2011

[Au00] Aura, Carnegie Mellon , 2000, Available from http://www.cs.cmu.edu/~aura/

[Ba00] Base, R., Intrusion Detection, Macmillan Technical Publishing, 2000.

[BBBR04] D. Bouwhuis, P. De Bra, A. Van Bronswijk, M. Rauterberg, "Benchmark Report Ambient Intelligence Research Focus at the Technische Universiteit Eindhoven", AmI task force group: Benchmarking, 2004.

[BBS99] E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials", Advances in Cryptology - EUROCRYPT 1999, LNCS 1592, pp. 12-23, Springer-Verlag, 1999.

[BDK01] E. Biham, O. Dunkelman and N. Keller, "The Rectangle Attack - Rectangling the Serpent", Advances in Cryptology - EUROCRYPT 2001, LNCS 2045, pp. 340-357, Springer-Verlag, 2001.

[BDK03] E. Biham, O. Dunkelman and N. Keller, "Rectangle Attacks on 49-Round SHACAL-1", FSE 2003, LNCS 2887, pp. 22-35, Springer-Verlag, 2003.

[BDKA05] E. Biham, O. Dunkelman, N. Keller, "A Related-Key Rectangle Attack on the Full KASUMI", Advances in Cryptology - ASIACRYPT 2005, LNCS 3788, pp. 443-461, Springer-Verlag, 2005.

[BDKR05] E. Biham, O. Dunkelman, N. Keller, "Related-Key Boomerang and Rectangle Attacks", Advances in Cryptology - EUROCRYPT 2005, LNCS 3494, pp. 507-525, Springer-Verlag, 2005.

[BE02] M. Blunden and A. Escott, "Related Key Attacks on Reduced Round KASUMI", FSE 2001, LNCS 2355, pp. 277-285, Springer-Verlag, 2002.

[BG03] Michael Beigl, Hans Gellersen, "Smart-Its: An Embedded Platform for Smart Objects", Smart Objects Conference, 2003.

[BG98] Bond, A.H., and L. Gasser, Distributed Artificial Intelligence, Morgan Kaufmann, 1998.

[BHAE02] 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.

[Bi93] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys", Advances in Cryptology - EUROCRYPT 1993, LNCS 765, pp. 398-409, Springer-Verlag, 1993.

[Bl99] U. Black, "Third Generation Mobile Systems (TGMSs)", Second Generation Mobile & Wireless Networks, Prentice Hall, 1999.

[BM07] Bowen, C.L. Martin, T.L., "Preserving User Location Privacy Based on Web Queries and LBS Responses", Information Assurance and Security Workshop, 2007. IAW'07, pp. 175-182, 2007.

[BMKS00] Barry Brumitt, Brian Meyers, John Krumm, Amanda Kern, Steven Shafer, "EasyLiving: Technologies for Intelligent Environments", Handheld and Ubiqitous Computing, 2nd International Symposium, pp. 12-29, 2000.

[BMW98] Page, L., Brin, S., Motwani, R., Winograd, T., The PageRank citation ranking: bringing order to the Web, Tech. rep., Stanford Digital Library Technologies Project, 1998.

[BPD09] Breslin, J., Passant, A., Decker, S., "Social web applications in enterprise. Soc", Semantic Web 48, pp. 251-267, 2009.

[BPW04] Balthazard, P.A., Potter, R.E.,Warren, J., "Expertise extraversion and group interaction styles as performance indicators in virtual teams: how do perceptions of it's performance get formed", DATA BASE 35(1), pp. 41-64, 2004.

[BS90] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology - CRYPTO 1990, LNCS 537, pp. 2-21, Springer-Verlag, 1990.

[Bu97] K. Buhanal et al., "IMT-2000: Service Providers Perspective", IEEE Personal Communications, 1997.

[CFZA02] Michael J. Covington, Prahlad Fogla, Zhiruan Zhan and Mustaque Ahamad, " A Context-Aware Secrutiy Architecture for Emerging Application", ACSAC'02, 2002

[CGRZ04] Sadie Creese, Michael Goldsmith, Bill Roscoe, and Irfan Zakiuddin, "Research Directions for Trust and Security in Human-Centric Computing", SPPC-04: Workshop on Security and Privacy in Pervasive Computing, pp. 1-7, 2004

[CLGZA03] Pat R. Calhoun, John Loughney, Erik Guttman, Glen Zorn, and Jari Arkko, "Diameter Base Protocol," RFC 3588, 2003.

[CNFG96] Cugola, G., Nitto, E.D., Fuggetta, A., Ghezzi, C., "A framework for formalizing inconsistencies and deviations in human-centered systems", ACM Trans. Softw. Eng. Methodol. 5(3), pp. 191-230, 1996.

[Co00] Cool Town, HP, 2000, Available from http://www.cooltown.hp.com

[CSE05] 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.

[DB96] D. Denning and D. Branstad, "A Taxonomy for Key Escrow Encryption Systems", Communications of the ACM, Vol. 39, pp 34-40, 1996.

[DECZ03] Dom, B., Eiron, I., Cozzi, A., Zhang, Y., "Graph-based ranking algorithms for e-mail expertise analysis", In: DMKD, pp. 42-48. ACM, New York, 2003.

[DKK06] O. Dunkelman, N. Keller, J. Kim, "Related-Key Rectangle Attack on the Full SHACAL-1", SAC 2006, LNCS 4356, pp. 28-44, Springer-Verlag, 2006.

[Du04] Dustdar, S., "Caramba a process-aware collaboration system supporting ad hoc and collaborative processes in virtual teams", Distrib. Parallel Databases 15(1), pp. 45-66, 2004.

[EK10] Easley, D., Kleinberg, J., "Networks, Crowds, and Markets: Reasoning About a Highly Connected World", Cambridge University Press, Cambridge, 2010.

[En99] Endeavour, Berkley, 1999, Available from http://endeavour.cs.berkeley.edu/

[ETSI96] ETSI TC-STAG, "Security Techniques Advisory Group (STAG); Definition of User Requirements for Lawful Interception of Telecomunications: Requirements of the Law Enforcement Agencies", ETR 331, 1996.

[ETSI97] ETSI TC Security, "Specification for Trusted Third Party Service: Part1 Key Management and Key Escrow/Recovery", DEN/SEC-003001x, Draft Version 1.0(edition2), 1997.

[FJKP95] H. Federrath, A. Jerichow, D. Kesdogan, and A. Pfitzmann, "Security in Public Mobile Communication Networks", Proceedings of the IFIP TC6 International Workshop on Personal Wireless Communications, pp. 105-116, 1995.

[FSGKC01]DF Ferraiolo, R. Sandhu, S. Gavrila, DR Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control", ACM Transactions aon Information and System Security (TISSEC), pp. 224-274, 2001.

[GL08] M. Gorski and S. Lucks, " New Related-Key Boomerang Attacks on AES", Progress in Cryptology - Indocrypt 2008, LNCS 5365, pp. 266-278, Springer-Verlag, 2008.

[GPSS04] Garlan, D., Poladian, V., Schmerl, B.R., Sousa, J.P., "Task-based self-adaptation", In:WOSS, pp. 54-57, 2004.

[Gr02] The Grocer Project, 2002, Available from
http://www.disappearing-computer.net/projects/GROCER.html

[GRS05] Gentry, C., Ramzan, Z., Stubblebine, S., "Secure distributed human computation", In: EC'05, pp. 155-164. ACM, New York, 2005.

[Ha02] Haveliwala, T.H., "Topic-sensitive pagerank", In: WWW, pp. 517-526. ACM, New York, 2002.

[HCH06] Y. Han, J. Choi, and S. Hwang, "Reactive Handover Optimization in IPv6-Based Mobile Networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 9, pp. 1758-1772, 2006.

[Hi02] Hisao Nakajima, "Marketing strategy in the Era of ubiquitous networks", NRI Papers No.44, 2002.

[HKLP05] S. Hong, J. Kim, S. Lee and B. Preneel, " Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192", FSE 2005, LNCS 3557, pp. 368-383, Springer-Verlag, 2005.

[HNH05] A. Hasswa, N. Nasser, and H. Hassanein, "Performance Evaluation of a Transport Layer Solution for Seamless Vertical Mobility", In Proc. of International Conference on Wireless Networks, Communications and Mobile Computing, pp. 576-581, 2005.

[HP98] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems", Computer Security-ESORICS'98, LNCS 1485, pp. 277-293, Springer-Verlag, 1998.

[HT07] C.-M. Huang and C.-H. Tsai, "The handover control mechanism for multi-path transmission using Stream Control Transmission Protocol (SCTP)", Computer Communications, vol. 30, no. 17, pp. 3239-3256, 2007.

[HW04] Junzhe Hu and Alfred C. Weaver, "A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications", Pervasive Security, Privacy and Trust (PSPT2004), 2004.

[HWRB05] Hammerle, S., Wimmer, M., Radig, B., Beetz, M., "Sensor-based Situated, Individualized, and Personalized Interaction in Smart Environments", In: Workshop on Situierung, Individualisierung, and Personalisierung, Informatik 2005, Bonn, Germany, 2005.

[HZZ99] Hu, S., L. Zhang, and Y. Zhong, Theories, "Technology and Application of Multi-Agent Systems", Computer Science, Vol. 26, No.9, pp. 20-24, 1999.

[IEEE11] IEEE Engineering & Technology, "World News", Engineering & Technology, Vol. 6, Issue 5, pp. 6-7, 2011

[IRK02] Ivanov, B., Ruser, H., Kellner, M., "Presence detection and person identification in Smart Homes", In: International Conference on Sensors and Systems. State Technical University, Saint-Petersburg, 2002.

[Ja99] Jacson, P., Expert systems, ADDISON WESLEY, 1999.

[JD04] G. Jakimoski and Y. Desmedt, "Related-Key Differential Cryptanalysis of 192-bit Key AES Variants", SAC 2003, LNCS 3006, pp. 208-221, Springer-Verlag, 2004.

[JGSWWCW00] Jou, Y.F. , F. Gong, C. Sargor, X. Wu, S.F. Wu, H.C. Chang, and F. Wang, "Design and implementation of a scalable intrusion detection system for the protection of network infrastructure", In Proceeding of DARPA Information Survivability Conference and Exposition, Volume: 2 , pp. 100-111, 2000.

[JLSHL07] K. Jeong, C. Lee, J. Sung, S. Hong and J. Lim, " Related-key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128", ACISP 2007, LNCS 4586, pp. 143-157, Springer-Verlag, 2007.

[JPA04] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, 2004.

[JW03] Jeh, G., Widom, J., "Scaling personalized web search", In: WWW, pp. 271-279. ACM, New York, 2003.

[KAV02] Kumar, A., Aalst, W.M.P.V.D., Verbeek, E., "Dynamic work distribution in workflow management systems: How to balance quality and performance", J. Manag. Inf. Syst. 18(3), pp. 157-193, 2002.

[KC04] H. G. Kim and D. H. Choi, "Session Key Exchange Based on Dynamic Security Association for Mobile IP Fast Handoff", LNCS 3043, pp. 1151-1158, Springer-Verlag, 2004.

[KCL04] S. J. Koh, M. J. Chang, and M. Lee, "mSCTP for Soft Handover in Transport Layer", IEEE Communications Letters, vol. 8., no. 3, pp. 189-191, 2004.

[KFJP96] D. Kesdogan. H. Federrath, A. Jericow, and A. Pfizmann, "Location Management Strategies increasing Privacy in Mobile Communication Systems", 12th IFIP International Conference on Information Security(IFIP/SEC'96), 1996.

[KGD01] Kosorukoff, A., Goldberg, D.E., "Genetic algorithms for social innovation and creativity", Tech. rep., University of Illinois at Urbana-Champaign, 2001.

[KHLLK04] Y. Ko, S. Hong, W. Lee, S. Lee and J. Kang, "Related Key Differential Attacks on 26 Rounds of XTEA and Full Rounds of GOST", FSE 2004, LNCS 3017, pp. 299-316, Springer-Verlag, 2004.

[KHP07] J. Kim, S. Hong and B. Preneel, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256", FSE 2007, LNCS 4593, pp. 225-241, Springer-Verlag, 2007.

[Ki01] Bong-Ju Kim, "Next Generation Authentication Protocol DIAMETER AAA Technical Trend." TTA, 2001.

[Ki02] Dong-Hyun Kim, "A Study of Ticket based AAA Service for Mobile IP," The Graduate School Yonsei University, 2002.

[Ki06] J. Kim, "Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms", Katholieke Universiteit Leuven \& Korea University, Ph.D. Dissertation, 2006.

[KK04] G. Kim and C. Kim, "Low-Latency Non-predictive Handover Scheme in Mobile IPv6 Environments", LNCS 3060, pp. 451-465, Springer-Verlag, 2004.

[KKG07] G. Karopoulos, G. Kambourakis, and S. Gritzalis, "Survey of secure handoff optimization schemes for multimedia services over all-IP wireless heterogeneous networks", IEEE Communications Surveys & Tutorials, vol. 9, no. 3, pp. 18-28, 2007.

[KKHLH04] J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, "The Related-Key Rectangle Attack - Application to SHACAL-1", ACISP 2004, LNCS 3108, pp. 123-136, Springer-Verlag, 2004.

[KKLLS04] J. Kim, G. Kim, S. Lee, J. Lim and J. Song, "Related-Key Attacks on Reduced-Rounds of SHACAL-2", Progress in Cryptology - Indocrypt 2004, LNCS 3348, pp. 175-190, Springer-Verlag, 2004.

[KKS02] J. Kelsey, T. Kohno and B. Schneier, " Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent", FSE 2001, LNCS 1978, pp. 75-93, Springer-Verlag, 2002.

[KL01] C. H. Kim and P. J. Lee, "New Key Recovery in WAKE Protocol", Public Key Cryptography-PKC 2001, LNCS 1403, pp. 325-338, 2001.

[Kl99] Kleinberg, J.M., "Authoritative sources in a hyperlinked environment", J. ACM 46(5), pp. 604-632, 1999.

[KLCYKLY05] HyunGon Kim, ByungGil Lee, DooHo Choi, SangKeun Yoo, Marie Kim, Haedong Lee, HuiJong Yu, "On the International Standardization of AAA Technology," ETRI Journal, Vol.20, No.1, pp. 123-129, 2005.

[KLHK08] Geon Woo Kim, Deok-Gyu Lee, Jong Wook Han, Sang Wook Kim, "Intelligent Security for Inter-space Surveillance Applications," MUE 2008, pp. 419-422, 2008.

[KLPSJ02] Gwanyeon Kim, Chinu Lee, Sehyun Park, Ohyoung Song, and Byungho Jung, "A Study on Mobile Commerce AAA Mechanism for Wireless LAN," HSI 2003, pp. 719-724, 2002.

[Kn96] L.R. Knudsen, "Trucated and Higher Order Differentials", FSE 1996, LNCS 1039, pp. 196-211, Springer-Verlag, 1996.

[Ko05] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, 2005.

[KP01] R. Koodli and C. E. Perkins, "Fast Handover and Context Relocation in Mobile Networks", ACM SIGCOMM Computer Communication Review, vol. 31, pp. 37-47, 2001.

[KRJ98] D. Kesdogan, P. Reichl, and K. Junghartchen, "Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks", ESORICS’98, LNCS 1485, pp. 295-312, Springer-Verlag, 1998.

[KSW96] J. Kelsey, B. Schneier and D. Wagner, "Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES", Advances in Cryptology - CRYPTO 1996, LNCS 1109, pp. 237-251, Springer-Verlag, 1996.

[KSW97] J. Kelsey, B. Schneir and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA", ICICS 1997, LNCS 1334, pp. 233-246, Springer-Verlag, 1997.

[KTB06] 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, pp. 35-43, 2006.

[KYPK05] S. S. Kim, S.-S. Yeo, H.-J. Park, S. K. Kim, "A New Scheme for the Location Information Protection in Mobile Communication Environments", MMM-ACNS 2005, LNCS 3685, pp. 436-441, Springer-Verlag, 2005.

[LCGJM07] G. Lopez, O. Canovas, A. F. Gomez, J. D. Jimenez, and R. Marin, "A network access control approach based on the AAA architecture and authorization attributes", Journal of Network and Computer Applications, vol. 30, no. 3, pp. 900-919, 2007.

[LCY05] Dong-Myung Lee, Hyo-Min Choi, Okyeon Yi, "Design of Authentication Mechanism for Anonymity And Privacy assurance," Proceedings of the 24rd KIPS Autumn Conference, pp. 941-944, 2005.

[Le08] Tom Lee, Presence Detection via the iphone and wifi, 2008, Available from http://echodittolabs.org

[Li99] C. Lim, "Crypton, A Revised Version of CRYPTON: CRYPTON v1.0", FSE 1999, LNCS 1636, pp. 31-45, Springer-Verlag, 1999.

[LK05] C. Lim and T. Korkishko, "mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors", WISA 2005, LNCS 3786, pp. 243-258, Springer-Verlag, 2005.

[LKCRL11] S.H. Lim, Y.I. Kim, C.H. Cho, W. Ryu, H.J. Lee, "Mobile IPTV Technical Trends and development Strategy", ETRI Electronics and Telecommunications Trends, Vol. 26, Issue 4, pp. 43-56, 2011.

[LKHLSHL08] E. Lee, J. Kim, D. Hong, C. Lee, J. Sung, S. Hong and J. Lim, "Weak-Key Classes of 7-Round MISTY 1 and 2 for Related-Key Amplified Boomerang Attacks", IEICE Transactions, vol. 91-A(2), pp. 642-649, 2008.

[LKHSL05] C. Lee, J. Kim, S. Hong, J. Sung and S. Lee, "Related Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b", MYCRYPT 2005, LNCS 3715, pp. 245-263, Springer-Verlag, 2005.

[LKHSL08] C. Lee, J. Kim, S. Hong, J. Sung and S. Lee, " Security Analysis of the Full-Round DDO-64 Block Cipher", Journal of Systems and Software, vol. 81(1), pp. 2328-2335, 2008.

[LKKDD06] J. Lu, J. Kim, N. Keller and O. Dunkelman, "Differential and Related-Key Rectangle Attacks on Reduced-Round SHACAL-1", Progress in Cryptology - Indocrypt 2006, LNCS 4329, pp. 17-31, Springer-Verlag, 2006.

[LKKDR06] J. Lu, J. Kim, N. Keller and O. Dunkelman, "Related-Key Rectangle Attack on 42-Round SHACAL-2", ISC 2006, LNCS 4176, pp. 85-100, Springer-Verlag, 2006.

[LKSHLM05] C. Lee, J. Kim, J. Sung, S. Hong, S. Lee, and D. Moon, "Related-Key Differential Attacks on Cobra-H64 and Cobra-H128", CCC 2005, LNCS 3796, pp. 201-219, Springer-Verlag, 2005.

[LKSL06] 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, pp.326-335, 2006.

[LLK06] J. Lu, C. Lee, J. Kim, "Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b", SCN 2006, LNCS 4116, pp. 95-110, Springer-Verlag, 2006.

[LP07] Chul-Soo Lee, Seok-Cheon Park, "IPTV Content Protection Technology: CAS and DRM," KISA Research paper, 2007.

[Lu08] J. Lu, and J. Kim, "Attacking 44 Rounds of the SHACAL-2 Block Cipher using Related-Key Rectangle Cryptanalysis", IEICE Transactions, vol. 91-A(9), pp. 2588-2596, 2008.

[Lu09] J. Lu, "Related-Key Rectangle Attack on 36 Rounds of the XTEA Block Cipher", International Journal of Information Security 8(1), 2009.

[MGMTM06] Moody, P., Gruen, D., Muller, M.J., Tang, J., Moran, T.P., "Business activity patterns: a new model for collaborative business applications", IBM Syst. J. 45(4), pp. 683-694, 2006.

[MMNV05] Maestre, I.M., Machuca, M., Navarro, A., Velasco, J.R., "A practical aproach to user location awareness in smart home environments using Bluetooth home environments using Bluetooth", In: (Un enfoque practico para la localizacion de usuarios mediante Bluetooth en entornos domoticos), 1st Iberoamerican Congress on Ubiquitous Computing, CICU 2005

[MPS08] Mendling, J., Ploesser, K., Strembeck, M., "Specifying separation of duty constraints in bpel4people processes", In: Business Information Systems. LNBIP, pp. 273-284. Springer, Berlin, 2008.

[MPTH01] Morellas V, Pavlidis I, Tsiamyrtzis P, Harp S, "Urban surveillance systems: from the laboratory to the commercial world", Proc IEEE 89(10), pp.1478-1497, 2001.

[MSK99] Mclure, S., J. Scambray, and G. Kurtz, Hacking Exposed: Network Security Secrets and Solutions, McGraw-Hill, 1999.

[MTRSO10] Mustafa Ergen, Tushar Shah, Rafi Assilian, Singaraselvan Singaraselvan, Oguz Oktay, "Method and System for SMS Based Ticket Numbering Service Over Femto Cell", US Patent, Aplication No.: 12/814,934, Filing date: 14th June, 2010, Date of Patent: 16th, December, 2010.

[NIST94] NIST, "Escrow Encryption Standard (EES)", Federal Information Processing Standard Publication (FIPS PUB) 185, 1994.

[NPBD00] J. Nieto, D. Park, C. Boyd, and E. Dawson, "Key Recovery in Third Generation Wireless Communication Systems", Public Key Cryptography-PKC 2000, LNCS 1751, pp. 223-237, Springer-Verlag, 2000.

[NS05] Moira Norrie, Beat Signer, "Overlaying Paper Maps with Digital Information Services for Tourists",Conference on Information Technology and Travel and Tourism, 2005

[NSM05] Newton, E.M., Sweeny, L., Malin, B., "Preserving Privacy by De-Identifying Face Images", IEEE Trans. Knowledge and Data Engineering 17(2), pp. 232-243, 2005.

[NYHR05] Clifford Neuman, Tom Yu, Sam Hartman, and Kenneth Raeburn, "The Kerberos Network Authentication Service," RFC 4120, 2005.

[OP98] T. Ojanpera and R. Prasad, "IMT-2000 Applications", Wideband CDMA for Third Generation Mobile Communication, T. Ojanpera and R. Prasad (ed.) Artech House Publishers, pp. 65-76, 1998.

[Ox00] Oxygen, MIT, 2000, Available from http://oxygen.lcs.mit.edu/

[Pa08] Jong Hyuk Park, "Study on Ubiquitous Hybrid Intelligent Security Framework Model", Technical Report, 2008.

[Pa87] Parunak, V.D., "Manufacturing Experience with the Contract Net, Research Notes in Artificial Intelligence", Distributed Artificial Intelligence, Vol. 1, pp. 285-310, 1987.

[PBPC03] Jung-Min Park, Eum-Hui Bae, Hye-Jin Pyeon, and Kijoon Chae, "A Ticket-Based AAA Security Mechanism in Mobile IP Network," ICCSA, pp. 210-219, 2003.

[PC00] Pentland, A., Choudhury, T., "Personalizing Smart Environments: Face Recognition for Human Interaction", IEEE Computer, Special issue on Biometrics, 2000.

[PC97] Bhrat Patel and Jon Crowcroft, "Ticket based service access for the mobile user," In Third annual ACM/IEEE internaional conference on Mobile computing and networking, pp. 223-233, 1997.

[PD05] Panteli, N., Davison, R., "The role of subgroups in the communication patterns of global virtual teams", IEEE Trans. Prof. Commun. 48(2), pp. 191-200, 2005.

[Pe10] Petrie, C., "Plenty of room outside the firm", Internet Comput. 14, pp. 92-96, 2010.

[PLYLK08] Youn-Kyoung Park, Sun-Hee Lim, Okyeon Yi, Sangjin Lee, Soo-Hyung Kim, "User Authentication Mechanism using Java Card for Personalized IPTV Services," International Conference on Convergence and Hybrid Information Technology 2008, pp. 618-626, 2008.

[PM01] Pavlidis I, Morellas V, Two examples of indoor and outdoor surveillance systems: motivation, design, and testing. In: Proc. 2nd Europeanworkshop on advanced video-based surveillance, 2001.

[Po02] Portolano, University of Washington 2002, Available from http://portolano.cs.washington.edu/

[PPW91] A. Pfitzmann, B. Pfitzmann, and M. Waidner, "ISDN-MIXes Untraceable Communication with Very Small Bandwidth Overhead", 7th IFIP International Conference on Informatin Security(IFIP/SEC'91), 1991.

[Pr01] P. E. Proctor, Practical Intrusion Detection Handbook, Prentice-Hall Inc., 2001.

[PW98] B. Pfitzmann and M. Waidner, "How to Break Fraud-Detectable Key Recovery", Operating Systems Review, 21, pp. 23-28, 1998.

[RA07] Russell, N., Aalst, W.M.P.V.D., Evaluation of the bpel4people and ws-humantask extensions to ws-bpel 2.0 the workflow resource patterns. Tech. rep., BPM Center Brisbane/Eindhoven, 2007.

[RASC07] R. Rajavelsamy, S. Anand, O. Song, and S. Choi, "A novel scheme for mobility management in heterogeneous wireless networks", Wireless Personal Communications, vol. 43, no. 3, pp. 997-1018, 2007.

[RM99] K. Rantos and C. Mitchell, "Key Recovery in ASPeCT Authentication and Initialization of Payment Protocol", Proceedings of ACTS Mobile Summit, Sorrento, Italy, 1999.

[RSM04] Raducanu, B., Subramanian, S., Markopoulos, P., "Human Presence Detection by Smart Devices" In: Proc. of 4th International ICSC Symposium on Engineering of Intelligent Systems, Island of Madeira, Portugal, 2004.

[SA05] Shetty, J., Adibi, J., "Discovering important nodes through graph entropy the case of enron email database", In: LinkKDD, pp. 74-81. ACM, New York, 2005.

[Sc03] Andrew Schwarz, "What is Human-Centric Computing", ISRC Future Technology Topic Brief, University of Huston, 2003.

[Sch11] Daniel Schall, "A human-centric runtime framework for mixed service-oriented systems", Distrib Parallel Databases, Springer, 2011.

[SC03] Seo, H.S., and T.H. Cho, "Simulation Model Design of Security System based on Policy-Based Framework", Simulation Transactions of The Society for Modeling and Simulation International, vol. 79, no. 9, pp. 515-527, 2003.

[Sc09] Schall, D., "Human interactions in mixed systems architecture, protocols, and algorithms", PhD thesis, Vienna University of Technology, 2009.

[Sc90] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards", CRYPTO’89, LNCS 330, pp. 239-251, Springer-Verlag, 1990.

[SCL05] John Sherwood, Adnrew Clark, David Lynas, "Enterprise Security Architecture: A Business-Driven Approach", CMP, 2005.

[SCMB05] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, 2005.

[SD01] Smart Dust, California Berkeley, 2001, Available from http://robotics.eecs.berkeley.edu/~pister/SmartDust/

[SE08] Jeffrey W. Seifert, "Federal Enterprise Architecture and E-Government: Issues for Information Technology Management", CRS Report for congress, 2008

[SFV05] Siegemund, F., Floerkemeier, C., Vogt, H., "The value of handhelds in smart environments", In: Personal and Ubiquitous Computing, vol. 9(2), March, 2005.

[SG00] Stauffer, C., Grimson,W.E.L., "Learning Patterns of Activity using Real-Time Tracking", IEEE Trans. Pattern Analysis and Machine Intelligence 22, pp. 747-757, 2000.

[Sh84] Adi Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO'84, pp. 47-53, 1984.

[Sh96] John Sherwood, "SALSA: A method for developing the enterprise security architecture and strategy", Computers & Security, Vol. 15, Issue 6, pp. 501-506, 1996.

[SK02] Smart Kindergarten, UCLA, 2002, Available from http://nesl.ee.ucla.edu/projects/smartkg/

[SK06] 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), pp. 2660-2668, 2006.

[SKBMCR98] Steve Shafer, John Krumm, Barry Brumitt, Brian Meyers, Mary Czerwinski, Daniel Robbins, "The New EasyLiving Project at Microsoft Research", Joint DARPA/NIST Smart Spaces Workshop, 1998.

[SLL10] Samuel Sambasivam, Sheldon Liang, Roger Liao, "NATIS: Novel Architecture Framework for Algorithmic Trading Information Systems - Automated Stock Trading via Electronic Communication Networks", Conference on Information Systems Applied Research, 2010.

[SMH98] Smart Medical Home,1998, University of Rochester, Available from http://www.urmc.rochester.edu/future-health/validation/smart-home.cfm

[SPCB07] Su, Q., Pavlov, D., Chow, J.H., Baker, W.C., "Internet-scale collection of human-reviewed data", In: WWW ’07, pp. 231-240. ACM, New York, 2007.

[SPD06] Sharifi, M., Payne, T., David, E., "Public display advertising based on Bluetooth device presence", In: Proceedings of the Workshop Mobile Interaction with the Real World, MIRW 2006, 2006.

[SR94] Smart Room,MIT, 1994, Available from http://vismod.media.mit.edu/vismod/demos/smartroom/

[SS08] Smart Space, NIST, 2008, Available from http://www.nist.gov/smartspace/

[SSM99] Sim, K.M., S. K. Shiu, and B. L. Martin, "Simulation of a Multi-agent Protocol for Task Allocation in Cooperative Design", IEEE SMC '99 Conference Proceedings, Vol. 3, pp. 95-100, 1999.

[SSO02] J. Stone, R. Stewart, and D. Otis, "Stream Control Transmission Protocol (SCTP) Checksum Change", RFC 3309, 2002.

[St02] Frank Stajano, "Security for Ubiquitous Computing", Wiley, 2002

[St07] R. Stewart, "Stream Control Transmission Protocol", RFC 4960, 2007.

[STD08] Schall, D., Truong, H.L., Dustdar, S., "Unifying human and software services in Web-scale collaborations", IEEE Internet Comput. 12(3), pp. 62-68, 2008.

[SXMSSTRKZP00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, 2000.

[SXTMK07] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, M. Kozuka, "Stream Control Transmission Protocol Dynamic Address Reconfiguration", RFC 5061, 2007.

[TN98] S. Thomoson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, 1998.

[TOG09] The Open Group, "TOGAF Version 9 Enterprise Edition: A Pocket Guide (Togaf Series)", 2009.

[TPBE07] Thomas, J., Paci, F., Bertino, E., Eugster, P., "User tasks and access control over Web services", In: ICWS’07, pp. 60-69. IEEE, New York, 2007.

[VCFGGBLHS00] John Vollbrecht, Pat calhoun, Stephen Farrell, Leon Gommans, George Gross, Betty de Bruihjn, Cess Laat, Matt Holdrege and David Spence, "AAA Authorization Framework," RFC 2904, 2000.

[VMNLVPM05] Velasco, J.R., Maestre, I.M., Navarro, A., Lopez, M.A., Vicente, A.J., de la Hoz, E., Paricio, A., Machuca, M., "Location aware services and interfaces in smart homes using multiagent systems", In: Juan, R. (ed.) Proceedings of Int. Conferecence on Pervasive Systems and Computing (PSC 2005), Las Vegas, 2005.

[Wa07] G. Wang, "Related-Key Rectangle Attack on 43-Round SHACAL-2", ISPEC 2007, LNCS 4464, pp. 33-42, Springer-Verlag, 2007.

[Wa99] D. Wagner, " The Boomerang Attack", FSE 1999, LNCS 1636, pp. 156-170, Springer-Verlag, 1999.

[WADMV05] Wickramasuriya, J., Alhazzazi, M., Datt, M., Mehrotra, S., Venkatasubramanian, N., "Privacy-Protecting Video Surveillance", In: Proc. SPIE International Symposium on Electronic Imaging, vol. 5671, pp. 64-75, 2005.

[We91] Mark Weiser, "The computer for the 21st century", Scientific American, pp. 94-104, 1991

[WHFG92] Want, R., Hopper, A., Falcao, V., Gibbons, J., "The Active Badge Location System", ACM Transactions on Information Systems 10(1), 1992.

[Wi93] Winston, P.H., Artificial Intelligence Third Edition, ADDISON WESLEY, 1993.

[WRL06] Je-Hak Woo, Chang-Hyun Roh, Wan-Bok Lee, "IPTV Content Protection Technology: CAS and DRM," KOCON Vol. 6, No. 8, pp. 157-164, 2006.

[xAP08] xAP Blue V0.1 Brings Bluetooth Presence Detection, 2008, Available from http://www.automatedhome.co.uk

[XDZHG07] Yang Xiao, Xiaojiang Du, Jingyuan Zhang, Fei Hu, Sghaier Guizani, "Internet Protocol Television: The Killer Application for the Next-Generation Internet," IEEE Communication Magazine, pp. 126-134, 2007.

[YAA08] Yang, J., Adamic, L., Ackerman, M., "Competing to share expertise: the taskcn knowledge sharing community", In: Int. Conf. on Weblogs and Social Media, 2008.

[Ye00] Ramesh Yerraballi, "Real-Time Operating Systems: An Ongoing Review", IEEE Real-Time Systems Symposium (RTSSWIP00), 2000.

[YHHMW98] Yang, J., R. Havaldar, V. Honavar, L. Miller, and Johny Wong, "Coordination of Distributed Knowledge Networks Using Contract Net Protocol", In Proceedings of Information Technology Conference, pp. 71-74, 1998.

[YHTFTSTS05] 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.

[Za87] JA Zachman, "A framework for information systems architecture", IBM systems journal, pp. 276-292, 1987.

[ZAA07] Zhang, J., Ackerman, M.S., Adamic, L., "Expertise networks in online communities: structure and algorithms", In: WWW, pp. 221-230. ACM, New York, 2007.

[ZCC00] Zwicky, E.D., S. Cooper, and D. B. Chapman, Building Internet Firewalls second edition, O'reilly & Associates, 2000.

[ZCC05] Zhang, W., Cheung, S.S., Chen, M., "Hiding Privacy Information in Video Surveillance System", In: ICIP2005. Proc. IEEE International Conference on Image Processing, pp. 868-871, 2005.

[Zi04] Andrew W. Zinn, "The use of integrated architectures to support agent based simulation: an initial investigation", Department of the Air Force Air University, 2004.

[ZP04] Guangsen Zhang, Manish Parashar, "Context-aware dynamic access control for pervasive applications, Proc. of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), Western Multi-Conference (WMC), 2004.

[ZPK00] Zeigler, B.P., H. Praehofer, and T.G. Kim, Theory of modeling and simulation: Integrating discrete event and continuous complex dynamic system, San Diego: Academic Press, 2000.

[ZS07] S. Zeadally and F. Siddiqui, "An Empirical Analysis of Handoff Performance for SIP, Mobile IP, and SCTP Protocols", Wireless Personal Communications, vol. 43, no. 2, pp. 589-603, 2007.