A Ticket based Authentication Scheme for Group Communication

Soobok Shin¹, Hongjin Yeh¹, Kangseok Kim²¹

¹ Graduate School of Information and Communications, Ajou University, Suwon, Korea
² Department of Knowledge Information Security, Ajou University, Suwon, Korea
{watermel, hjyeh, kangskim}@ajou.ac.kr

Abstract. With the advent of new generation of mobile access devices such as smartphone and tablet PC, there is coming a need for ubiquitous collaboration which allows people to access information systems independent of their access device and their physical capabilities and to communicate with other people in anytime and in anywhere. As the number of collaborators with a large number of disparate access devices increases in ubiquitous collaboration environment, the difficulties for protecting secured resources from unauthorized users as well as unsecured access devices will increase since the resources can be compromised by inadequately secured human and devices. In this paper we present an effective authentication scheme for secure and authorized end-to-end delivery mechanism of messages between entities (publishers and subscribers) for ubiquitous collaboration.

Keywords: Ubiquitous Collaboration, Authentication Scheme, Mobile Device

1 Introduction

In collaboration systems, a group of users generally work sharing collaborative applications and resources in their workgroups. The cooperation on the resources shared among them may hence produce new results on the shared resources. On the contrary, security is about restricting unauthorized access to resources and thus it is essential that security of collaboration environments as well as of collaborative applications running on them is ensured while providing openness only to users that are authorized to access them. Therefore, difficulties to deal with the conflicting goals of allowing and restricting accesses for resources among a group of users may happen in collaboration environment.

The study in [2, 4] presented a user authentication scheme using a ticket in mobile networks. Also the study in [1] presented a ticket based single sign on protocol among application systems. The benefit of the authentication using a ticket is that an authentication mechanism is based on the ticket given to a service server without the need of re-authentication. In heterogeneous networked environments including battery powered mobile devices, an authentication scheme should be lightweight. Therefore

¹ Author to whom correspondence should be addressed; E-Mails: kangskim@ajou.ac.kr
in this paper we present an effective authentication scheme to overcome limitations of mobile devices (with high network latency and low computing performance) in ubiquitous computing environment.

2 Authentication scheme for ubiquitous collaboration

In this section we present an authentication scheme for secure and authorized end-to-end delivery mechanism of messages between entities (publishers and subscribers) in our messaging system.

2.1 Overall authentication procedure

A conference manager (CM) manages information related to all the conferences. The manager resides on web server running on tomcat. The manager is responsible for user’s registration, issuing a ticket to entities, and managing revocation lists. The issued ticket is specified with a secret number for a participant, a set of sessions, a right information in the sessions, and a lifetime of the ticket. After a subscriber is registered, she transmits a join request message and her ticket to a chairperson (CP). The CP authenticates the subscriber through the ticket.

2.2 Proposed authentication scheme

The proposed scheme is divided into two phases. The first phase is for registration / ticket issue as shown in Fig. 1. The second is authentication / session joining phase through the ticket as shown in Fig. 2.

**Fig. 1.** Protocol for registration and ticket issue, where $E_k(M)$ means encryption of message $M$ using key $k$ and $D_k(M)$ means decryption of message $M$ using key $k$.

### 2.2.1 Registration and ticket issue phase

A user registers to CM for joining a conference and gets a ticket and group session keys issued from CM. The group session keys are generated from key management center (KMC [3]). A user $u_i$ transmits registration / ticket request message. CM generates $x_i$ (secret number), $P_i$ (information about registration), $K_i$ (group session keys) and the ticket $Ticket_i = (x_i, P_i, life-time)$ and transmits $Ticket_i$ and $K_i$ encrypted by $k_{login}$ to $u_i$. Also CM transmits
$x_i$ encrypted by group key to related CPs. CPs decrypt the message received from CM and add $x_i$ in session / presence list.

2.2.2 Authentication and session joining phase. The participant submits the ticket issued from CM to a CP for joining a session. After a participant who wants to join a session $t$ generates a time-stamp $T_i$ and encrypts her ticket and the time-stamp by a group key $k_t$ of the session $t$, she transmits the encrypted message to $CP_t$. The $CP_t$ decrypts the message using $k_t$ and verifies $T_i, x_i$ and life-time. Also $CP_t$ computes a filter function $F_i(P_i)$ and verifies the value. Finally the $CP_t$ publishes a joining message of the new subscriber to other existing subscribers and then they update their session / presence list.

![Diagram of protocol for authentication and joining a session](image)

**Fig. 2.** Protocol for authentication and joining a session where $CP_t$ means a chairperson of session $t$, Mem$^t$ means a member of session $t$, $T_i$ means time stamp generated by $u_i$ and $F_i$ means filter function of session $t$.

3 Summary and future work

In this paper, we proposed an authentication scheme for users joining a conference with disparate access devices. In our proposed authentication mechanism, a user can join all sessions by a ticket which is issued by conference manager and the computation for authentication is not complex because the length of ticket is fixed. Thus, our proposed scheme is effective even as mobile devices are involved for group communication. In future work we will analyze the security and the performance of our proposed scheme. Also, we will show the practical evaluation of the proposed scheme.

**Acknowledgments.** This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA (Korea Internet Security Agency).

**References**