http://dx.doi.org/10.14400/JDC.2014.12.2.335

P2P 기반의 모바일 상거래를 위한 동적 그룹 인증

윤성현*
백석대학교 정보통신학부*

The Dynamic Group Authentication for P2P based Mobile Commerce

Sunghyun Yun*
Div. of Information & Communication Engineering, Baekseok University*

요 약 사용자 스마트폰에서 네트워크 비디오를 실시간으로 재생하려면, 서버가 비디오 콘텐츠를 스트리밍 방식으로 전송해야 한다. 일반적으로 상거래 서버는 유료 가입자 인증과 콘텐츠 분배를 담당한다. 단점은 사용자들의 서비스 요구가 급증하면 서버의 과부하, 전송 대역폭의 제한으로 고객에게 돌아가는 서비스 품질이 저하된다는 것이다. P2P 프로토콜은 콘텐츠를 보유한 사용자가 서버 역할을 분담하기 때문에 수요가 집중될 수록 서비스 품질이 좋아진다. 하지만 P2P 프로토콜은 분산된 서버를 제어할 수 없기 때문에 불법 콘텐츠 분배가 가능하여 상거래 용도로 적합하지 않다. 본 논문에서는 P2P 기반의 모바일 상거래에 적합한 동적 그룹 인증 기법을 제안한다. 제안한 기법은 공통키 생성, 공통키 업데이트, 그룹 서명 및 검증 프로토콜로 구성된다. 그룹을 구성하는 시더의 가입과 탈퇴를 반영할 수 있고, 하이브리드 P2P 기반의 상거래 모델에 적용되어 상거래 서비스는 중앙 서버가 담당하고 콘텐츠는 P2P 기반으로 분배할 수 있다.

주제어 : 동적 그룹 인증, 하이브리드 P2P, 서버 과부하, 그룹 서명, 키 업데이트

Abstract To play the networked video contents in a client's mobile device in real time, the contents should be delivered to it by the contents server with streaming technology. Generally, in a server-client based commerce model, the server is in charge of both the authentication of the paid customer and distribution of the contents. The drawback of it is that if the customers' requests go on growing rapidly, the service quality would be degraded results from the problems of overloaded server or restricted network bandwidth. On the contrary, in P2P based networks, more and more the demand for service increasing, the service quality is upgraded since a customer can act as a server. But, in the P2P based network, there are too many servers to manage, it's possible to distribute illegal contents because the P2P protocol cannot control distributed servers. Thus, it's not suitable for commercial purposes. In this paper, the dymanic group authentication scheme is proposed which is suited to P2P based applications. The proposed scheme consists of group based key generation, key update, signature generation and verification protocols. It can control the seeder's state whether the seeder is joining or leaving the network, and it can be applied to hybrid P2P based commerce model where sales transactions are covered by the index server and the contents are distributed by the P2P protocol.

Key Words : Dynamic Group Authentication, Hybrid P2P, Server Overload, Group Signature, Key Update

Received 10 January 2014, Revised 10 February 2014
Accepted 20 February 2014
Corresponding Author: Sunghyun Yun(Baekseok University)
Email: shcrpt@gmail.com

ISSN: 1738-1916

1. 서론

스마트폰과 광대역 유무선 통신망의 보급으로 실시간 비디오 콘텐츠 서비스에 대한 사용자들의 수요가 급증하고 있다. 실시간 서비스는 콘텐츠를 다운로드 받으면서 동시에 재생할 수 있는 것으로 비디오 스트리밍 기술에 기반을 둔다. 일반적으로 비디오 스트리밍 서비스는 콘텐츠 및 회원 관리가 용이한 클라이언트-서버 기반으로 구축된다[1].

비디오 콘텐츠는 다른 종류의 콘텐츠보다 용량이 크고 네트워크 대역폭을 많이 요구한다. 따라서 많은 사용자들이 특정 콘텐츠에 몰리면 스트리밍 서버에 과부하가 걸리고, 그 결과로 비디오 콘텐츠가 지연되거나 드롭되어 유료 회원에게 제공되는 서비스 품질이 저하된다[2].

P2P 프로토콜은 피어(클라이언트)가 서버 역할도 함께 하는 분산 네트워크 기술로 피어 간의 직접 연결로 콘텐츠를 공유한다. 특정 콘텐츠에 대한 사용자 수요가 급증하면 이를 제공하는 서버 수도 함께 증가되어 서비스 품질이 향상된다[3].

피어간의 연결로 콘텐츠를 검색할 경우에 많은 시더가 존재하는 콘텐츠는 쉽게 찾을 수 있지만, 그렇지 않은 경우에는 검색에 시간이 많이 걸리고 못 찾게 되는 경우도 많다. 따라서 콘텐츠 검색은 구글, 네이버 등과 같이 중앙 서버에서 주기적으로 수집하여 구축한 대용량 데이터베이스를 이용하는 것이 보다 효과적이다.

Hybrid P2P는 상기한 P2P 기반 검색의 단점을 보완하기 위하여, 콘텐츠 검색은 서버를 이용하고 파일 전송은 P2P 기반으로 처리하는 방식이다. 피어 간의 질의로 콘텐츠를 탐색하는 것 보다는 구글과 같은 인덱스 서버를 이용하는 것이 보다 빠르고 정확하며, 콘텐츠 분배는 P2P 방식을 이용하는 것이 자원을 효율적으로 사용할 수 있어 경제적이다[3].

본 논문에서는 P2P 기반의 상거래에 적합한 동적 그룹 인증 기법을 제안한다. P2P 기반 모델을 판매와 분배 파트로 구분하여, 인덱스 서버는 주문, 결제로 구성되는 판매 트랜잭션을 관리하고, 콘텐츠는 P2P 기반으로 분배한다. 트래커는 해당 콘텐츠를 보유한 시더를 찾아서 그룹으로 만들고 이를 인증함으로써 콘텐츠에 대한 불법 접근 및 유통을 제어한다.

트래커는 서버 정책에 의하여 정적으로 할당되고 임의로 가입 및 탈퇴하는 시더를 직접 관리한다. 판매자 서버와 트래커 그룹은 PKI 기반으로 인증하여 법적 구속력을 확보함으로써 콘텐츠를 보유한 시더 그룹이 트래커에 종속되도록 한다.

시더는 임의적 가입과 탈퇴가 가능하기 때문에 실시간으로 시더 그룹을 업데이트 및 인증할 수 있어야 한다. 구성원들의 상태가 수시로 변하는 환경에서는 PKI 인증서 도용 및 노출의 위험이 크고 이를 이용한 가장 공격이 가능하다. 바이오메트릭 데이터는 사용자 신체의 일부이며 고유 정보이기 때문에 그 자체로 법적 구속력이 있고 대리 인증이 어려워 가장 공격의 위험을 최소화할 수 있다. 따라서 시더 그룹과 같이 동적인 상태를 반영해야 하는 환경에는 바이오메트릭 기반 인증이 보다 더 적합하다.

2 장에서는 P2P 네트워크의 시더 인증을 위해서 바이오메트릭 인증이 왜 필요한지 설명한다. 3 장에서는 제안한 동적 그룹 인증 기법을 기술하고 4 장에서 안전성 분석을 한다. 5 장에서 결론 및 향후 연구과제를 제시한다.

2. 연구의 필요성

P2P 네트워크에서 피어는 콘텐츠의 공급자이며 소비자가 될 수 있다. 시더는 공유 콘텐츠의 전부 또는 일부를 가지고 있는 피어를 의미하고, 트래커는 시더와 피어를 연결해주는 서버로 시더의 위치 정보를 피어에게 알려주고 실제 콘텐츠 분배는 피어와 시더간의 일대일 연결로 이루어진다[3].

서버 클라이언트 모델에서 서버는 자신이 모든 것을 관리하기 때문에 다양한 정책 수립 및 제공이 가능하다. 따라서 특정 상거래 모델에 맞는 맞춤형 서버를 제공할 수 있다. 이에 반하여 P2P 기반 모델은 콘텐츠를 제공하는 시더(서버)가 산재되어 있기 때문에 효율적인 콘텐츠 분배는 가능하지만 다양한 상거래 모델에 맞는 정책 설정이 어렵다.

트래커 서버의 역할은 콘텐츠를 보유한 시더를 피어에게 연결해 주는 것이다. 시더는 가입과 탈퇴가 자유롭고 대규모이며 분산되어 있기 때문에 개별 인증이 불가능하고 콘텐츠 불법 유통을 제어하기 힘들다.

Unstructured 방식은 순수 P2P 프로토콜로 피어 간의 질의로만 시더를 찾아서 콘텐츠를 공유한다. 피어가 요청한 콘텐츠가 희귀한 경우에는 이를 보유한 시더를 찾기가

쉽지 않다[4].

Structured 방식에서 트래커 서버는 DHT(Distributed Hash Table)를 이용하여 콘텐츠를 보유한 시더를 관리한다. DHT는 시더의 위치와 식별 정보를 이진트리 형식으로 구조화하여 저장한 테이블이다. 따라서 희귀한 콘텐츠를 질의해도 DHT를 이용하여 해당 콘텐츠를 보유한 시더를 신속히 찾아낼 수 있다. 하지만 피어와 시더가 수시로 가입 및 탈퇴하는 P2P의 동적인 특성 때문에 DHT 테이블을 관리하는 것이 쉽지 않으며, 동적 성향이 높아지면 DHT 테이블에 대한 신뢰도가 떨어지게 된다[4].

하이브리드 P2P 방식은 P2P와 클라이언트-서버 방식의 장점을 결합한 것으로, 콘텐츠 탐색을 위해서 인덱스 서버의 기능을 이용하고 연결된 피어와 시더들 같의 콘텐츠 전송은 P2P 방식으로 진행한다[5].

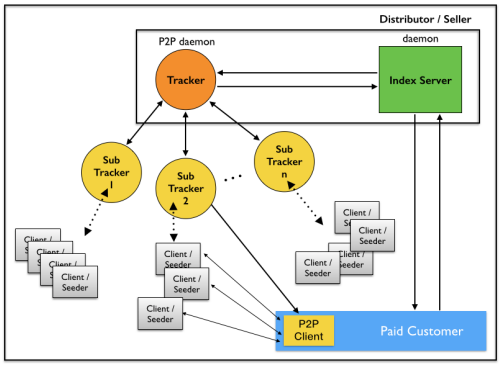
안전한 모바일 상거래를 위해서 거래 내용에 대한 법적 구속력 확보는 필수적이다. P2P 기반 모델에서 유료 콘텐츠를 구매한 피어는 콘텐츠 분배를 담당하는 서버 역할을 동시에 수행해야 한다. 불법 콘텐츠 유통을 차단하려면 분배 권한이 있는 시더만 콘텐츠를 분배할 수 있어야 한다.

하이브리드 P2P 방식에서는 서버 정책 수립이 가능하기 때문에 시더 네트워크를 콘텐츠 별로 그루핑하여 관리하는 것이 가능하다. 서버와 트래커는 상거래 서버 구축 및 운용 단계에서 정적 구성이 가능하기 때문에 PKI 기반으로 인증 트리를 구성할 수 있다. 시더 그룹은 가입 및 탈퇴가 자치적으로 이루어지는 동적 그룹이기 때문에 인증서 노출의 위험이 적은 바이오메트릭 기반의 인증 및 서명이 적합하다. 시더 그룹 멤버의 자격을 유료 가입한 회원으로 국한하면 P2P 기반의 네트워크에서 시더 제어가 가능하다.

바이오메트릭 서명에서 사용자는 자신의 바이오메트릭 템플릿을 이용하여 바이오메트릭 키를 생성한다. 서명 생성 및 검증은 일반 서명 기법과 동일하다[6]. PKI 기반의 공개키는 항상 인증 센터의 도움을 받아야 본인의 키 임을 입증할 수 있다. 바이오메트릭 키는 제 3자의 도움 없이 본인이 직접 자기 자신의 것임을 입증할 수 있다. 바이오메트릭 서명의 이러한 특성은 가입 및 탈퇴가 자발적으로 발생하는 동적 P2P 네트워크에서 시더를 인증하는 용도로 적합하다.

3. P2P 시더 그룹 인증

P2P 기반 상거래에 적합한 바이오메트릭 기반의 동적 그룹 인증 기법을 제안한다. 제안한 기법은 공통키 생성, 공통키 업데이트, 그룹 서명 및 검증 프로토콜로 구성된다.



[Fig. 1] Hybrid P2P based business model

그림 1은 하이브리드 P2P 기반의 모바일 상거래 모델을 보여준다. 피어(구매자)는 상거래 서버에서 콘텐츠를 구매하고, 트래커는 해당 콘텐츠를 보유한 시더를 찾아서 시더 그룹을 만든다. 시더는 상거래 서버에 가입된 회원으로 콘텐츠 제공의 법적 권한을 갖는다. 트래커는 피어의 콘텐츠 요청 메시지를 시더 그룹으로 전송한다. 공통키 생성은 시더간에 순차적으로 수행되고, 서명 생성은 독립적으로 진행된다. 공통키 업데이트 프로토콜은 시더의 가입 및 탈퇴에 따른 그룹의 상태를 반영한다. 시더는 자신의 바이오메트릭 키를 이용하여 콘텐츠 요청 메시지에 서명하고 해당 콘텐츠를 피어에게 제공한다.

3.1 시더 그룹 공통키 생성

가정 1. 시더는 자신의 바이오메트릭 템플릿을 서버에 등록하고, X.1088 표준에 명시된 바이오메트릭 키 생성 절차를 따라서 공개키와 개인키 쌍을 생성한다[7]. 바이오메트릭 템플릿은 원본이 아닌 변형된 형태로 등록되며 도용 시 재등록이 가능하다[8].

정의 1. GF(p)는 암호학적으로 안전한 유한체이고 g는 위수 p-1을 갖는 생성자이다[9].

가정 2. 서버, 트래커, 시더의 공개키 및 개인키는 다음과 같다. 법 p는 큰 소수로 2^{512} 보다 크고, g는 생성자로 p 보다 작다.

Nodes	Private key	Public key
Server	$sk_C < p$	$pk_C \equiv g^{sk_C} \bmod p$
Tracker	$sk_T < p$	$pk_T \equiv g^{sk_T} \bmod p$
Seeder	$sk_S < p$	$pk_S \equiv g^{sk_S} \bmod p$

가정 3. 트래커는 동일한 콘텐츠를 보유한 n 개의 시더를 찾아서 그룹을 만들고 시더들 간의 순서 리스트를 생성한다. 트래커는 시더 리스트를 자신의 개인키로 서명하고 이를 서버에 등록한다.

$list_S = [S_1 \| S_2 \| \cdots \| S_n]$

$Tracker's\ Signature = ER_{sk_T}(list_S)$

$list_S$: ordered list of seeders

S_i: i−th seeder

(1) S_1 (첫 번째 시더)

단계 1: 트래커는 구매자 정보, 콘텐츠 정보, 저작자 정보 등으로 구성된 주문 데이터를 해쉬한다. 순서 리스트의 첫 번째인 S_1에게 주문 데이터와 함께 공통키 생성을 요청한다.

$h_C = H(\text{order}_C)$

$\text{order}_C = [\text{Buyer} \| \text{Contents} \| \text{Author} \| \cdots]$

H: hash function, order_C: customer's order

단계 2: S_1은 p−1과 서로소인 임의의 난수 k_1을 선택하여 R_1과 G_1을 생성하고 자신의 공개키로 PK_1을 만든다. S_1은 S_2에게 (R_1, G_1, PK_1)을 전송한다.

$$R_1 \equiv h_C^{k_1} \bmod p,\ G_1 \equiv g^{k_1} \bmod p,\ PK_1 = pk_1$$

(2) S_i (i = [2..n])

단계 1: S_i는 S_{i-1}로부터 (R_{i-1}, G_{i-1}, PK_{i-1})을 수신한다.

$$R_{i-1} \equiv R_{i-2}^{k_{i-1}} \equiv h_C^{\prod_{j=1}^{i-1} k_j} \bmod p$$

$$G_{i-1} \equiv G_{i-2}^{k_{i-1}} \equiv g^{\prod_{j=1}^{i-1} k_j} \bmod p$$

$$PK_{i-1} \equiv PK_{i-2}^{sk_{i-1}} \equiv g^{\prod_{j=1}^{i-1} sk_j} \bmod p$$

단계 2: S_i는 p−1과 서로소인 임의의 난수 k_i를 선택하여 R_i와 G_i를 생성하고 자신의 개인키로 PK_i를 만든다. S_i는 S_{i+1}에게 (R_i, G_i, PK_i)를 전송한다.

$$R_i \equiv R_{i-1}^{k_i} \equiv h_C^{\prod_{j=1}^{i} k_j} \bmod p$$

$$G_i \equiv G_{i-1}^{k_i} \equiv g^{\prod_{j=1}^{i} k_j} \bmod p$$

$$PK_i \equiv PK_{i-1}^{sk_i} \equiv g^{\prod_{j=1}^{i} sk_j} \bmod p$$

단계 3: S_i가 시더 리스트의 마지막이 아니면 단계 1과 2를 반복한다. 마지막 순번의 시더 S_n은 그룹 공통키 (R, G, PK)를 시더 그룹과 트래커에게 전송한다.

$$R \equiv R_{n-1}^{k_n} \equiv h_C^{\prod_{j=1}^{n} k_j} \bmod p$$

$$G \equiv G_{n-1}^{k_n} \equiv g^{\prod_{j=1}^{n} k_j} \bmod p$$

$$PK \equiv PK_{n-1}^{sk_n} \equiv g^{\prod_{j=1}^{n} sk_j} \bmod p$$

3.2 공통키 업데이트

시더 그룹에 새로운 시더가 추가되거나 또는 기존 시더가 삭제될 경우에 다음과 같이 공통키를 업데이트 한다.

(1) 새로운 시더 S_{n+1}의 가입

단계 1: 트래커는 새로 가입한 시더 S_{n+1}에게 (R, G, PK)를 전송한다.

단계 2: S_{n+1}은 p−1과 서로소인 임의의 난수 k_{n+1}을 선택하여 R과 G를 업데이트 하고 자신의 개인키로 PK를 수정한다. S_{n+1}은 (R, G, PK)를 시더 그룹과 트래커에게 전송한다.

$$R \equiv R_n^{k_{n+1}} \equiv h_C^{\prod_{j=1}^{n+1} k_j} \bmod p$$

$$G \equiv G_n^{k_{n+1}} \equiv g^{\prod_{j=1}^{n+1} k_j} \bmod p$$

$$PK \equiv PK_n^{sk_{n+1}} \equiv g^{\prod_{j=1}^{n+1} sk_j} \mod p$$

단계 3: 트래커는 시더 리스트에 S_{n+1}을 추가하고 자신의 개인키로 서명한다. 새로운 시더 그룹에 대한 공통키 (R, G, PK)와 서명된 시더 리스트를 서버에 등록한다.

$$list_S = [S_1 \| S_2 \| \cdots \| S_n \| S_{n+1}]$$

(2) 기존 시더 S_b의 탈퇴 ($S_b \in \{S_1, S_2, \cdots, S_n\}$)

단계 1: 트래커는 탈퇴할 시더 S_b에게 (R, G, PK)를 전송한다.

단계 2: S_b는 k_b를 이용하여 R과 G를 업데이트 하고 자신의 개인키로 PK를 수정한다. S_b는 (R, G, PK)를 시더 그룹과 트래커에게 전송한다. k_b와 sk_b는 p-1과 서로소이기 때문에 법 p-1에 대한 모듈라 곱셈의 역이 존재한다[10].

$$R \equiv R^{k_b^{-1}} \equiv h_C^{(\prod_{j=1}^{n} k_j) \cdot k_b^{-1}} \mod p$$

$$G \equiv G^{k_b^{-1}} \equiv g^{(\prod_{j=1}^{n} k_j) \cdot k_b^{-1}} \mod p$$

$$PK \equiv PK^{sk_b^{-1}} \equiv g^{(\prod_{j=1}^{n} sk_j) \cdot sk_b^{-1}} \mod p$$

단계 3: 트래커는 시더 리스트에서 S_b를 삭제하고 순서를 업데이트 한다. 트래커는 시더 리스트를 서명하고 새로운 공통키 (R, G, PK)와 함께 서버에 등록한다.

$$list_S = [S_1 \| S_2 \| \cdots \| S_{n-1}]$$

3.3 그룹 서명 생성

단계 1: 시더 리스트에 있는 각 시더는 주문 데이터에 서명하고 $sign_i$를 트래커에게 전송한다. k_i와 p-1은 서로소이므로 $sign_i$에 대한 유일한 해가 존재한다[10].

$$k_i \cdot sign_i \equiv sk_i \cdot R - k_i \cdot h_C \mod p-1$$

단계 2: 트래커는 $sign_i$를 조합하여 그룹서명 SIGN을 생성한다. 트래커는 ($order_C$, h_C, R, G, PK, SIGN)으로 구성된 서명 패키지를 만들어 서버에 등록하고 시더그룹에게 배포한다.

$$SIGN \equiv \prod_{j=1}^{n} (h_C + sign_j) \mod p$$

3.4 그룹 서명 검증

단계 1: 시더 리스트의 각 시더는 주문 데이터를 해쉬하여 해쉬 값이 일치하는 지 확인한다. 일치하면 단계 2로 그렇지 않으면 검증 프로토콜을 종료한다.

$$h_C = H(order_C)$$

단계 2: 각 시더는 다음 검증식을 통하여 그룹서명을 검증한다. 검증식을 만족하면 구매자의 연결 요청을 수락하고 콘텐츠를 전송한다. 그렇지 않으면 연결 요청을 거부한다.

$$G^{SIGN} \equiv PK^{R^n} \mod p$$

4. 안전성 분석

정리 1. 시더 그룹은 그룹 서명에 대해서 부인할 수 없으며 인증된 그룹만 콘텐츠 분배에 참여할 수 있다.

(증명) 3.1절의 공통키 생성 과정에서 각 시더는 자신만이 알고 있는 난수 k_i와 개인키를 이용하여 (R, G, PK) 생성에 참여한다. 시더가 보유한 난수 k_i와 개인키를 공개된 (R_i, G_i, pk_i)로부터 유추하는 것은 다음과 같이 이산 대수 문제가 된다.

$$\prod_{j=1}^{i} k_j \equiv \log_{h_C} R_i \mod p, \quad \prod_{j=1}^{i} k_j \equiv \log_{h_C} G_i \mod p$$

$$sk_i \equiv \log_g pk_i \mod p$$

정의 1에서 GF(p)는 암호학적으로 안전한 유한체이므로 이산 대수 문제를 푸는 것은 계산상 불가능하다[10].

3.4절의 검증식은 다음과 같이 증명된다.

$$G^{SIGN} \equiv g^{(\prod_{j=1}^{n} k_j) \cdot SIGN} \equiv g^{\prod_{j=1}^{n} k_j \cdot (h_C + sign_j)} \mod p$$

$$PK^{R^n} \equiv g^{(\prod_{j=1}^{n} sk_j) \cdot R^n} \equiv g^{\prod_{j=1}^{n} sk_j \cdot R} \mod p$$

$$\prod_{j=1}^{n} k_j \cdot (h_C + sign_j) \equiv \prod_{j=1}^{n} sk_j \cdot R \mod p-1$$

$$\therefore G^{SIGN} \equiv PK^{R^n} \mod p$$

가정 1에서 시더의 개인키는 바이오메트릭 키로 법적 구속력을 갖는다. 따라서 인증된 그룹만 콘텐츠 분배에 참여할 수 있고 그룹 서명에 대해서 부인할 수 없다. Q.E.D.

정리 2. 제안한 공통키 업데이트 프로토콜은 시더의 가입과 탈퇴로 구성원이 변하는 동적 그룹을 인증한다.
(증명) 업데이트 이전과 이후의 공통키 값을 이용하여 비밀정보를 유추할 수 없음을 증명한다. 먼저 시더가 추가된 경우에 대해서 살펴본다. 업데이트된 공통키 값을 R′, G′, PK′으로 하고 이전 값을 R, G, PK로 한다.

$$R' \equiv h_C^{\prod_{j=1}^{n+1} k_j} \bmod p, \quad R \equiv h_C^{\prod_{j=1}^{n} k_j} \bmod p$$

$$G' \equiv g^{\prod_{j=1}^{n+1} k_j} \bmod p, \quad G \equiv g^{\prod_{j=1}^{n} k_j} \bmod p$$

$$PK' \equiv g^{\prod_{j=1}^{n+1} sk_j} \bmod p, \quad PK \equiv g^{\prod_{j=1}^{n} sk_j} \bmod p$$

R′과 R을 이용하여 새로운 시더가 보유한 k_{n+1} 값을 구하려면 다음과 같은 이산 대수 문제가 된다. 정의 1로부터 GF(p) 상에서의 이산 대수 문제는 계산상 불가능하다 [10].

$$\prod_{j=1}^{n+1} k_j \equiv \log_{h_C} R' \bmod p, \quad \prod_{j=1}^{n} k_j \equiv \log_{h_C} R \bmod p$$

기존 시더들이 모두 공모하여 R′ 값에서 k_i 값을 제거하여도, 새로 가입한 시더의 k_{n+1} 값을 유추하려면 다음 식을 풀어야 한다.

$$R' \equiv R^{\prod_{j=1}^{n} k_j^{-1}} \equiv h_C^{(\prod_{j=1}^{n+1} k_j) \cdot (\prod_{j=1}^{n} k_j)} \equiv h_C^{k_{n+1}} \bmod p$$

$$k_{n+1} \equiv \log_{h_C} R' \bmod p$$

새로 가입한 시더의 k_{n+1} 값을 찾는 것은 GF(p) 상에서의 이산 대수 문제가 된다. 따라서 업데이트 이후의 R′과 이전의 R은 동일한 안전성을 갖는다.
(G′, G, PK′, PK)도 같은 방식으로 증명이 가능하다. 시더 탈퇴로 업데이트 된 공통키의 안전성은 본 증명과 동일한 방식으로 증명된다. Q.E.D.

5. 결론

본 논문에서는 P2P 기반의 상거래를 위한 동적 그룹 인증 기법을 제안하였다. 제안한 방법은 그룹 공통키 생성, 그룹 서명 및 검증 프로토콜로 구성된다. 공통키 업데이트 프로토콜은 시더의 가입과 탈퇴로 변화하는 그룹 상태를 반영하며 이에 대한 안전성을 증명하였다. 시더 그룹은 바이오메트릭 기반의 그룹 서명에 참여함으로써 콘텐츠 유통에 대한 법적 구속력을 갖게 된다. 따라서 P2P 기반 상거래에서 안전하고 효율적으로 콘텐츠 분배를 분산화할 수 있다.

본 연구에서 제안한 시더 탈퇴 프로토콜은 시더가 공통키에 있는 자신의 정보를 제거해야만 가능하다. 시더는 통제받지 않는 자치적인 특성을 갖기 때문에 탈퇴 프로세스에 참여하지 않을 수도 있다. 따라서 시더의 도움 없이 탈퇴 프로토콜을 업데이트 할 수 있는 방법이 추가로 연구되어야 한다.

REFERENCES

[1] Streaming media, http://en.wikipedia.org/wiki/Streaming_ media

[2] E. Setton, B. Girod, Peer-to-Peer Video Streaming, Springer, e-ISBN-13:978-0-387-74115-4, 2007.

[3] Q. H. Vu, M. Lupu, B. C. Ooi, Peer-to-Peer Computing, Principles and Applications, Springer, DOI 10.1007/978-3-642-03514-2, 2010.

[4] E. Buyukkaya, M. Abdallah, G. Simon, A survey of peer-to-peer overlay approaches for networked virtual environments, Peer-to-Peer Networking and Applications, Springer, http://dx.doi.org/10.1007/s12083-013-0231-5, pp. 1-25, 2013.

[5] V. Darlagiannis, Hybrid Peer-to-Peer Systems, Peer-to-Peer Systems and Applications, Springer, ISBN 9783540291923, 2005.

[6] P. Janbandhu, M. Siyal, Novel biometric digital signatures for Internet-based applications, Information Management & Computer Security, Vol. 9, No. 5, pp. 205-212, 2001.

[7] ITU-T X.1088, A Framework for biometric digital key generation, ITU-T, 2008.

[8] N. K. Ratha, J. H. Connell, R. M. Bolle, Enhancing security and privacy in biometric-based authentication systems, IBM Systems Journal, Vol. 40, No. 3, pp. 614 - 634, 2001.

[9] W. Diffie, M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976.

[10] D. M. Burton, Elementary Number Theory, McGraw-Hill Science/Engineering/Math, 2010.

윤 성 현(Yun, Sung Hyun)

- 1992년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1994년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : 모바일 보안, 바이오메트릭 인증, DRM, 전자투표
- E-Mail : shcrpt@gmail.com