낙관적 다자간 계약서 서명 프로토콜 라운드의 하한

(Lower bound on the Number of Rounds for Optimistic Multi-party Contract Signing Protocol)

주 홍 돈 † 장 직 현 ††
(Hongdon Joo) (Jik Hyun Chang)

요 약 네트워크의 성장은 전자상거래의 중요성을 증대시켰다. 그리고 공정교환 프로토콜은 전자상거래의 중요한 부분을 차지하므로 공정교환 프로토콜에 관련된 많은 연구들이 이루어졌다. 계약서 서명 프로토콜은 공정 교환 프로토콜의 일부로서 많은 연구가 이루어졌지만 대부분은 양자간 프로토콜에 집중되었다. 그리고 다자간의 계약서 서명 프로토콜에 대한 연구는 부족하였다. Baum-Waidner가 제시한 다자간 계약서 서명 프로토콜이 지금까지 알려진 가장 적은 수의 라운드를 가지는 비동기방식의 낙관적인 다자간의 계약서 서명 프로토콜이다[4]. 하지만, 낙관적인 다자간의 계약서 서명 프로토콜이 필요로 하는 라운드 수의 하한은 알려지지 않았다. 본 논문에서는 낙관적인 다자간의 계약서 서명 프로토콜이 필요한 라운드 수의 밀착 하한을 제시한다.

키워드 : 암호 프로토콜, 계약서 서명 프로토콜, 하한

Abstract The growth of networks increase the importance of electronic commerces. Since the fair exchange protocol is an important part of electronic commerces, a number of researches have been done in relation to the fair exchange protocol. As the contract signing protocol is a part of fair exchange protocol, many protocols have been proposed, but most of them were focused on two-party protocol. Only a few were on the multi-party contract signing protocol. So far the optimistic multi-party contract signing protocol presented by Baum-Waidner has the least number of rounds in asynchronous network[4]. But, the lower bound on the number of rounds required by any optimistic multi-party contract signing protocol has been not known. In this paper, we present a tight lower bound on the number of rounds for optimistic multi-party contract signing protocol.

Key words : Cryptographic Protocol, Contract Signing Protocol, Lower Bound

1. 서 론

인터넷의 발달로 네트워크를 통한 전자상거래의 필요성이 증대되었으며, 이에 따라 전자상거래에 기반이 되는 공정 교환 프로토콜에 대한 많은 연구가 이루어 졌다. 그중에서 계약서 서명 프로토콜은 n명이 계약서에 서명을 하려고 할 때, 최대 n-1 명의 부정직한 참가자가 있더라도, 모든 정직한 참가자들이 모두 서명된 계약서를 얻거나 또는 아무도 서명이 된 계약서를 얻지 못하는 프로토콜이다. 여기서 부정직한 참가자들이란 프로토콜에서 주어진 명세대로 행동을 하지 않은 참가자들을 의미한다. 이러한 계약서 서명 프로토콜은 공정 교환 프로토콜의 기반이 되는 프로토콜로 여러 가지 효율적인 방법들이 제시되었다[1-5]. 물론, 다자간의 계약서 서명 프로토콜을 포함하여 공정 교환 프로토콜은 낙관적 프로토콜이 아니라면 신뢰기관인 TTP(Trusted Third Party)로 전송하는 그리고 TTP가 다시 재분배하는 2개의 기본적인 단계를 통해서 프로토콜을 완료할 수 있다. 하지만, 이러한 프로토콜은 TTP에게 너무 많은 작업이 집중이 되는 문제점을 가진다.

최초의 낙관적인 다자간의 계약서 서명 프로토콜은 Asokan, Baum-Waidner와 Schunter이 낙관적인 경우 2개의 페이즈(phase)와 최악의 경우 TTP와 연동하는 2

· 본 연구는 2003년도 서강대학교 교내연구비 지원으로 수행되었음
† 학생회원 : 삼성전자 TN 통신연구소 연구원
narziss@sogang.ac.kr
†† 종신회원 : 서강대학교 컴퓨터학과 교수
jchang@alglab.sogang.ac.kr
논문접수 : 2005년 2월 1일
심사완료 : 2005년 6월 10일

개의 페이즈를 가지는 동기방식의 프로토콜을 제시하였다[1]. 하지만, 인터넷과 같이 동기방식으로 동작하기 어려운 네트워크를 위해서 비동기 방식의 프로토콜에 대한 개발이 요구되었다. 최초로 제시된 비동기방식의 낙관적인 프로토콜은 Garay와 MacKenzie에 의하여 제시되었으며, 참가자의 수가 n이면 $O(n^2)$의 라운드를 가지는 프로토콜이다[2]. 이어서 Baum-Waidner와 Waidner는 O(t)(t는 부정직한 참가자의 최대 수)의 라운드를 가지는 프로토콜을 제시하였다[3]. 이어서 Baum-Waidner는 라운드의 수를 줄인 프로토콜을 제시하였다[4]. 또, 부정직한 참가자가 최대 n-1명인 경우에 비동기방식의 다자간의 계약서 서명.프로토콜의 라운드 수의 하한은 Garay와 MacKenzie에 의하여 n으로 제시되었지만[2], 부정직한 참가자의 수가 $t(1\leq t<n-1)$인 경우에 다자간의 계약서 서명 프로토콜의 라운드 수의 하한은 알려져 있지 않았으며 Baum-Waidner는 이를 미해결 문제로 제시하였다[4]. 뿐만 아니라, Garay와 MacKenzie에 의하여 제시된 다자간의 계약서 서명 프로토콜의 라운드 수의 하한은 밀착하한이 아니다.

본 논문은 다자간 계약서 서명 프로토콜의 라운드 수의 하한에 대한 연구로, 기존의 비동기 방식에서 부정직한 참가자가 최대 n-1인 경우 Garay와 Mackenzie에 의하여 n으로 제시된 데 이어, 부정직한 참가자의 수 t가 $1\leq t<n-1$ 인 경우 다자간의 계약서 서명 프로톡로의 라운드 수의 하한뿐만 아니라, 부정직한 참가자의 수가 n-1명인 경우, 기존의 n보다 더 작은 하한을 제시하고 이를 증명하였다.

Baum-Waidner의 프로토콜은 기존의 다자간의 계약서 서명 프로토콜에서 필요한 라운드의 수를 $n\geq 2t+1$ 인 경우에는 O(t)에서 O(1)으로 감소시켰고 $n<2t+1$인 경우에는 라운드의 수가 O(t)에 비하여 서서히 증감함을 보였다. 하지만, Baum-Waidner의 프로토콜이 최소의 라운드를 가지는지는 알려지지 않았다.

본 논문에서는 한명 이상의 부정직한 참가자가 존재할 때 필요한 라운드 수의 하한을 2 라운드(모든 참가자가 프로토콜에 참가하는 경우)와 3 라운드(일부참가자가 프로토콜에 참가하지 않을 수 있는 경우)로 나누어 증명하였고, 부정직한 참가자들의 최대 수에 따라 필요한 라운드 수의 하한을 $\lfloor n/(n-t)\rfloor+\lceil n/(n-t)\rceil-1$(모든 참가자가 프로토콜에 참가하는 경우)와 $\lfloor n/(n-t)\rfloor+\lceil n/(n-t)\rceil$(일부 참가자가 프로토콜에 참가하지 않을 수 있는 경우)로 제시하고 증명하였다. 그리고 제시된 라운드 수의 하한은 Baum-Waidner에 의하여 제시된 프로토콜과 같은 수의 라운드를 가지므로 밀착하한이다.

2. 모델

모델에 대한 정의를 하기 전에, 본 논문에서 고려하는 프로토콜은 낙관적인 다자간 계약서 서명 프로토콜이므로 이를 정의한다.

정의 1. 낙관적인 다자간 계약서 서명 프로토콜 : n명의 참가자와 신뢰할 수 있는 기관인 TTP이 참여하는 프로토콜로서, 계약서 M이 있을 때, 모든 참가자들이 M에 대한 서명된 계약서를 얻고자하는 프로토콜이다. 그리고 모든 참가자들이 정직하게 프로토콜을 수행한다면 TTP의 참여 없이 프로토콜을 완료할 수 있다. □

위의 프로토콜을 구성하는 요소에 대한 모델은 다음과 같이 정의한다. 이는 Baum-Waidner와 Waidner가 제시한 모델과 유사하다[3].

서명된 계약서 : 적어도 한 번의 모든 참가자들의 서명을 포함하며, 어느 누구라도 TTP와 같은 외부의 참여 없이 서명된 계약서임을 검증할 수 있다. 그리고 서명된 계약서는 취소시킬 수 없다.

참가자 : $\{P_1,...,P_n\}$의 n명으로 구성되며 프로토콜 중간에 추가되거나 제외되지 않는다. 최대 $t(0<t<n)$ 명의 참가자가 부정직한 참가자이다. 부정직한 참가자는 프로토콜의 명세대로 행동을 하지 않는 참가자를 말한다.

TTP(Trusted Third Party) : 신뢰할 수 있는 기관으로 참가자가 요구하는 경우에 프로토콜에 참여할 수 있다. 또, TTP는 부정직한 참가자 수의 최대 값 t를 알고 있다. 그리고 TTP는 서버처럼 메시지를 받을 때만 응답을 하고, 능동적으로 프로토콜에 참여하지는 않는다.

네트워크 : TTP로부터 각 참가자들로 보내지는 메시지들과 참가자들로부터 TTP로 보내는 모든 메시지는 언제인지는 모르지만 반드시 전달된다. 하지만, 참가자들 사이의 메시지들은 제거되거나, 또는, 순서대로 전달되지 않을 수도 있다.

공격자 : 공격자는 참가자들 사이의 모든 메시지를 읽고, 추가하고, 또는, 삭제할 수 있다. 그리고 TTP와 참가자들 사이의 모든 메시지도 읽고, 필요한 메시지를 삽입할 수 있다. 그리고 공격자는 부정직한 참가자들을 제어할 수 있다.

정의 2. 안전한 비동기방식의 낙관적인 다자간 계약서 서명 프로토콜 : 위의 네트워크 모델에서 동작하는 낙관적인 다자간 계약서 서명 프로토콜로서 다음의 4개의 성질에 만족한다.

완전성(Completeness) : 모든 참가자가 프로토콜을 올바르게 수행한다면, 프로토콜을 완료할 수 있다.

건전성(Soundness) : 참가자가 계약서에 대한 자신의 서명을 다른 참가자들에게 전송하지 않는 한, 어떠한 참가자도 서명된 계약서를 얻을 수 없다.

공정성(Fairness) : 한명의 정직한 참가자라도 서명

된 계약서를 얻지 못한다면 어떠한 참가자도 서명된 계약서를 얻지 못한다.

종료에 대한 보장 : 정직한 참가자들은 프로토콜이 종료되는 것을 확신할 수 있어야 한다. □

프로토콜에서 사용되는 메시지들은 3가지로 구별한다. TTP로 전송하는 요청메시지, TTP로부터 받는 응답메시지, 그리고 참가자들끼리 메시지 송수신에 사용하는 라운드 별 메시지로 구별한다.

라운드 메시지(round message) : 참가자들 간의 메시지 송수신에 사용하는 메시지이다.

요청메시지(resolve message) : 참가자가 TTP로 보내는 모든 메시지를 요청메시지라 한다. 참가자들은 요청메시지를 보낼 때, 자신이 지금까지 받은 모든 라운드 메시지를 포함하여 요청메시지를 TTP로 전송할 수 있다.

응답메시지(result message) : TTP가 참가자에게 요청메시지의 응답으로 보내는 메시지이다. 프로토콜이 중지 또는 완료됨을 알려준다. 단, 완료된 경우 서명된 계약서를 전송해야 한다. 그리고 서명된 계약서는 참가자들로부터 받은 요청메시지들로부터 만들 수 있어야 한다. 그렇지 않다면 중지메시지를 보낼 수밖에 없다.

본 논문에서는 Baum-Waidner가 제시한 프로토콜이 요구하는 라운드의 수가 비동기 방식의 낙관적인 다자간 계약서 서명 프로토콜의 라운드 수의 하한임을 증명하고자 하므로 라운드에 대하여 좀 더 상세하게 살펴보자.

참가자별 라운드 : 메시지의 크기나 메시지를 보내는 참가자의 수와 관계없이 하나의 라운드에 메시지를 송수신할 수 있다. 그러나 로컬 또는 이전 라운드까지 수신한 메시지들을 이용한 메시지만을 송신할 수 있다.

그러면, 프로토콜의 라운드는 어떻게 설정할 수 있을까? 참가자별 라운드로부터 프로토콜의 라운드를 간단하게 결정할 수 있을 것 같지만, 다음의 3명의 참가자가 있는 프로토콜의 예를 살펴보면 그렇지 않음을 알 수 있다. 만약, P_1이 P_2에게 서명을 전송하고 P_2가 다시 P_3에게 서명을 전송하고, 다시 P_3이 P_1로 서명을 전송하는 프로토콜을 생각하면 참가자들은 많아야 2개의 라운드에 참여하지만, 프로토콜의 전체 라운드는 3이 되므로, 단순하게 프로토콜의 라운드를 결정할 수 없음을 알 수 있다.

프로토콜의 라운드를 결정하기 위해서 다음과 같은 방향 그래프를 정의하였다.

방향 그래프 G=(N,E)는 노드의 집합 N과 에지의 집합 E로 구성된다.

노드의 집합 N : n명의 참가자 $\{P_1,...,P_n\}$가 프로토콜에 참여하고, 각각의 참가자 P_i가 R_i번의 라운드에 참가한다면 $N=\{(P_i,j)|\ i=1,...,n \text{ and } j=1,...,R_i\}$으로 구성된다.

에지의 집합 E : 방향을 가지는 에지들의 집합으로, 예를 들어 참가자 P_i가 자신의 라운드 3에서 P_j의 참가자의 라운드 2에게 메시지를 송신한다면 에지 $<(P_i,3),(P_j,2)>$가 E에 포함된다.

그러면, **방향 그래프의 경로의 최대 길이가 프로토콜에 필요한 라운드**가 된다. 그리고 프로토콜 라운드는 다음과 같이 정의할 수 있다.

프로토콜 라운드 : 각 노드에서 자신까지의 경로 중 최대 길이이다.

그리고 앞으로 논문에서 사용되는 라운드는 프로토콜 라운드를 의미한다.

예를 들면 P_1과 P_3이 메시지 m에 대한 각자의 서명을 P_2에게 전송하고, P_2는 수신된 메시지에 자신의 서명을 하여 P_1,P_3에게 전송하고, P_1과 P_3은 다시 받은 메시지에 자신들의 서명을 하여 P_2에게 전송한다면 다음과 같은 방향 그래프를 구성할 수 있다.

$G=(\{(P_1,1),(P_1,2),(P_2,1),(P_2,2),(P_3,1),(P_3,2)\},$
$\{<(P_1,1),(P_2,1)>,<(P_3,1),(P_2,1)>,...\})$

다음의 그림 1은 위의 그래프를 나타낸 것으로 그림에서 라운드는 프로토콜 라운드를 의미한다. 프로토콜 라운드 $(P_1,1)$는 1, 프로토콜 라운드 $(P_2,1)$는 2이고 프로토콜 라운드 $(P_3,1)$는 1이다.

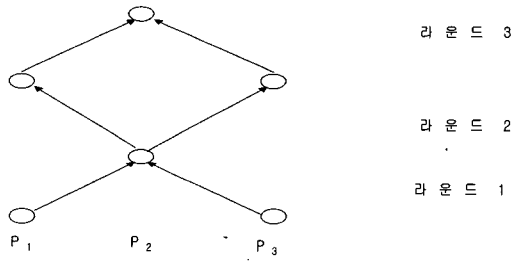

그림 1 라운드의 예제

이어서 그래프 G에서 참가자별로 next 함수를 정의한다.

참가자 P_i의 next(R) : min {프로토콜 라운드 (R'') | $e_j=<(P_k,R'),(P_i,R'')> \in E$ for $1\le k\ne i\le n$ 그리고 프로토콜 라운드(R'')>R}

즉, next(R)는 참가자 Pi가 다른 참가자들에게 메시지를 수신하는 다음 라운드이다. 단, next(0)는 프로토콜에서 참가자가 처음으로 다른 참가자들로부터 메시지를 수신하는 라운드를 의미하고, ∞값을 가지는 경우에는 더 이상 프로토콜에서 해당 참가자가 메시지를 수신하지 않는다는 것을 의미한다. 그러므로 그림 1과 같은 경우에는 P_1에 대하여 next(0)=2, next(1)=2, next(2)=∞

이고, P_2에 대하여 next(0)=1,next(1)=2, next(2)=3, next(3)=∞이고, P_3에 대하여 next(0)=2, next(1)=2, next(2)=∞가 된다.

3. 중요한 관찰

본장에서는 안전한 계약서 서명 프로토콜을 위한 몇 가지 중요한 관찰에 대하여 살펴본다. 앞으로 특별히 혼동되는 경우를 제외하고 "비동기방식의 낙관적인 다자간의 계약서 서명 프로토콜"은 "계약서 서명 프로토콜"이라고 줄여서 쓴다.

먼저, 프로토콜에 대하여 살펴보기 전에 메시지들에 대하여 간단하게 살펴보자. 안전한 계약서 서명 프로토콜에서 요청메시지, 응답메시지 그리고 라운드 메시지들은 프로토콜이 완료되기 전에 메시지를 만든 참가자의 확인이 가능하여야 한다. 그렇지 않다면, 부정직한 참가자 또는 공격자 등이 메시지를 임의로 만들 수 있으므로 건전성을 위배할 수 있다. 디지털 서명을 사용하면 간단하게 메시지를 만든 참가자의 확인이 가능하지만, 프로토콜의 완료 이전에 메시지를 만든 참가자의 확인이 가능하다면 어떠한 방법을 사용하더라도 제한하지 않는다. 이제 프로토콜에서 사용되는 메시지들은 해당 메시지를 만든 참가자들의 확인을 할 수 있다고 가정한다.

보조정리 1. 안전한 계약서 서명 프로토콜에서 TTP는 부정직한 참가자로 확인할 수 없는 참가자 n-t명으로부터 요청메시지를 받으면 항상 응답메시지를 전송해야 한다.

증명. 우리가 고려하는 모델에서 TTP는 서버와 같이 동작하므로, TTP는 응답메시지를 보내는 때는 참가자들로부터 요청메시지를 받았을 경우이다. 그런데, n-t명을 제외하면 나머지는 모두 부정직한 참가자일 수 있고, 그들은 TTP에게 요청메시지를 전송하지 않을 수 있다. 그러므로 TTP가 n-t명을 초과하는 참가자들로부터 요청메시지를 받을 때까지 기다렸다가 요청메시지를 보낸 참가자들에게 응답메시지를 보낸다면, 정직한 참가자들에게 프로토콜 종료를 보장할 수 없다. □

Baum-Waidner는 참가자들이 프로토콜에 참가하지 않을 수 있는 경우와 모든 참가자들이 항상 프로토콜에 참여하는 경우로 구분하여 계약서 서명 프로토콜을 제시하였다[4]. 그런 구분에 따라서 몇 가지 성질들을 살펴본다.

보조정리 2. 안전한 계약서 서명 프로토콜에서, 일부 참가자가 프로토콜에 참여하지 않을 수 있는 경우, 참가자가 다른 참가자로부터 메시지를 받지 못하고, 요청메시지를 TTP에게 전송한다면 TTP는 즉시 중지메시지를 전송해야 한다.

증명. 서명된 계약서는 모든 참가자들의 서명을 적어도 한번 포함하여야 한다. 그리고 TTP는 서명된 계약서를 참가자들로부터 받은 요청메시지들의 내용으로만 만들 수 있다. 즉, 요청메시지에 모든 참가자들의 서명이 포함되지 않았으면 서명된 계약서를 만들 수 없다. 더욱이 프로토콜에 일부 참가자들이 참여하지 않을 수 있다면, TTP로 요청메시지를 전송한 참가자들 제외하면 아무도 프로토콜에 참가하고 있지 않을 수 있으므로, 정직한 참가자들에게 프로토콜 종료에 대한 보장을 하려면 요청메시지를 받는 즉시 응답메시지를 전송해야 한다. 그리고 서명된 계약서를 보낼 수 없으므로 응답메시지는 중지메시지가 될 수밖에 없다. □

그러면, 일부 참가자들이 프로토콜에 참여하지 않을 수 있는 경우에 모든 참가자들의 서명을 포함하지 못하고 요청메시지를 보낸 참가자에게 TTP는 보조정리 2에 의하여 항상 중지메시지를 전송할 것이다. 그리고 모든 참가자들이 항상 프로토콜에 참여하는 경우에도 n-t명의 참가자들로부터 요청메시지를 받으면 보조정리 1에 의하여 응답메시지를 전송해야 하는데, 만약 TTP가 수신된 요청메시지로부터 모든 참가자들의 서명을 얻을 수 없다면 중지메시지를 전송해야 할 것이다. 이제는 TTP가 일부 참가자들에게 이미 중지메시지를 전송한 후에 다른 참가자들로부터 요청메시지를 받았을 경우에 대하여 생각해보자.

보조정리 3. 안전한 계약서 서명 프로토콜에서 TTP가 부정직한 참가자로 결정을 할 수 없는 참가자들에게 이미 중지메시지를 전송했다면, 나머지 참가자들에게도 중지메시지를 전송해야 한다.

증명. 부정직한 참가자로 결정할 수 없는 참가자들로부터 요청메시지를 받고 일부에게 중지 메시지를 전송하고, 또 일부에게 서명된 계약서를 전송한다면 프로토콜의 공정성에 위배될 수 있다. 즉, 이미 중지메시지를 받은 참가자들이 정직한 참가자들이고, 나머지 참가자들이 부정직한 참가자인 경우 공정성에 위배된다. □

이제 TTP가 어떻게 부정직한 참가자들을 결정할 수 있는가를 생각해보자. TTP는 참가자들로부터 네트워크를 감시하지 않으므로 참가자들로부터 요청메시지를 받는 것을 제외하면 어떠한 정보도 얻을 수 없다. 그리고 공격자에 의하여 메시지의 수정 또는 삭제가 가능하므로, 잘못된 메시지의 수신 또는 받지 못한 메시지로 인하여 해당 메시지를 송신한 참가자를 부정직한 참가자로 결정할 수 없다. 그러므로 TTP가 부정직한 참가자로 결정하려면, 해당 참가자가 자신이 수신한 메시지를 수신하지 못한 것으로 가장하여 TTP에게 요청메시지를 보낸 것을 확신할 수 있을 때뿐이다. 그래서 TTP로 라운드 R에서 요청메시지를 보낸 참가자를 부정직한 참가

자로 결정하려면, 그 참가자가 라운드 R+1 이후에 프로토콜에 참여한 것을 다른 참가자들이 보낸 요청메시지로부터 보일 수 있을 때 뿐이다.

4. 계약서 서명 프로토콜에 필요한 라운드

모든 참가자들이 항상 프로토콜에 참여하는 경우와 참가자가 프로토콜에 참여하지 않을 수도 있는 경우로 구분하여 안전한 다자간 계약서 서명이 요구하는 라운드 수의 하한을 제시한다. 그것은 Baum-Waidner에 의하여 제시된 프로토콜과 같은 수의 라운드를 가지므로 밀착하한이다. 다음의 표 1에서는 라운드 수의 하한을 나타낸다. 단, TTP와 통신하는 라운드의 수는 포함하지 않았다.

또, 참가자들은 다른 참가자들로부터 마지막 메시지를 받으면 서명된 계약서를 얻을 수 있다고 가정한다. 만약, 서명된 계약서를 얻은 이후에 다른 참가자들로부터 메시지를 수신하는 라운드가 존재한다면, 이를 프로토콜에서 제외하여도 동일한 기능을 하는 라운드 수가 증가하지 않는 프로토콜이 존재하므로, 이런 가정을 하고 프로토콜의 라운드의 하한을 구하는 것은 일반성을 잃지 않는다.

간단하게 생각하면 모든 참가자들이 서로 계약서에 자신들의 서명을 하여 다른 참가자들에게 전송을 한다면, 1개의 라운드로 계약서 서명 프로토콜을 구성할 수 있을 것 같지만, 부정직한 참가자가 존재하므로 이는 불가능하다. 정리1은 이에 대한 증명이다.

정리 1. 안전한 계약서 서명 프로토콜은 1개의 라운드로 구성될 수 없다.

증명. 하나의 라운드로 구성된 계약서 서명 프로토콜 **P**가 있다고 하자. **P**가 안전한 계약서 서명 프로토콜이 될 수 없음을 보인다.

먼저, 공격자는 정직한 참가자들이 메시지를 받지 못하게 하고, 나머지 참가자들은 메시지를 수신할 수 있도록 한다. 그러면 정직한 참가자들을 제외한 나머지 참가자들은 서명된 계약서를 얻을 수 있다. 하지만, 정직한 참가자들은 서명된 계약서를 얻지 못한다. 그리고 정직한 참가자들이 TTP로 요청메시지를 송신하여도 부정직한 참가자들의 서명을 포함할 수 없으므로, TTP는 서명된 계약서를 전송할 수 없다. 그러므로 **P**는 안전한 계약서 서명 프로토콜이 아니다. □

모든 참가자가 항상 프로토콜에 참여하는 경우 부정직한 참가자의 수 t가 $n \geq 2t+1$인 경우 2개의 라운드로 구성되는 안전한 계약서 서명 프로토콜을 Baum-Waidner에 의하여 제시되었다[4]. 하지만 일부 참가자들이 참가하지 않을 수 있는 경우에는 3개의 라운드를 가지는 프로토콜을 제시하였는데[4], 정리 2에서는 2개의 라운드를 가진 안전한 계약서 서명 프로토콜이 존재하지 않음은 증명한다.

정리 2. 일부 참가자가 프로토콜에 참여하지 않을 수 있는 경우, 안전한 계약서 서명 프로토콜은 적어도 3개의 라운드가 필요하다.

증명. 2개의 라운드로 구성된 계약서 서명 프로토콜을 **P**라고 하자. 이제 **P**가 안전한 계약서 서명 프로토콜이 아님을 보인다. **P**에서 참가자들은 2개의 라운드에서 모두 메시지를 수신하거나, 또는 라운드 1또는 라운드 2에서만 메시지를 수신할 것이다.

먼저, 라운드 1에서만 다른 참가자로부터 메시지의 수신을 하는 참가자가 있다고 하자. 그러면 그를 공격자라 하자. 그러면, 공격자는 다른 참가자들의 메시지의 수신을 막아도 자신은 서명된 계약서를 얻을 수 있다. 하지만 다른 참가자들은 라운드 1에서 서명된 계약서를 받지 못한다. 그리고 서명된 계약서를 받지 못한 참가자들이 TTP로 요청메시지를 전송하더라도 적어도 공격자의 서명을 요청메시지에 포함할 수 없으므로 TTP는 서명된 계약서를 전송할 수 없다.

이제 두 번째 라운드에서만 메시지 수신을 하는 참가자들과 2개의 라운드에서 모두 메시지 수신을 하는 참가자들만 있다고 하자. 그러면 임의의 참가자를 공격자로 선정하여, 라운드 1에서 TTP에게 요청메시지를 전송한다. 그러면 TTP는 보조정리 2에 의하여 중지메시지를 공격자에게 전송할 것이다. 하지만, 라운드 1에서 다른 참가자들에게 정상적으로 메시지를 전송한다. 그러면, 모든 참가자들은 라운드 1에 메시지를 받았으므로 라운드 2에 메시지를 전송할 것이다. 이제 공격자는 정직한 참가자들이 라운드 2에서 메시지를 수신하지 못하도록 막는다. 그러면, 공격자는 서명된 계약서를 얻지만, 정직한 참가자들은 서명된 계약서를 얻을 수 없다. 뿐만 아니라, 정직한 참가자들은 요청메시지를 TTP로 전송하여도, TTP는 공격자를 부정직한 참가자로 결정할 수 없으므로 요청메시지를 보낸 참가자들에게 중지메시지를 전송해야 한다. 그러므로 **P**는 안전한 계약서 서명 프로토콜이 아니다. □

표 1 라운드의 수(t (0<t<n):공격자의 최대 수, n: 프로토콜에 참가자)

	모든 참가자는 항상 프로토콜에 참여	모든 참가자의 참여여부 불투명
0<t<n-1	$\lfloor n/(n-t) \rfloor + \lceil n/(n-t) \rceil - 1$	$\lfloor n/(n-t) \rfloor + \lceil n/(n-t) \rceil$
t=n-1	t+2	

지금까지 한명이상의 부정직한 참가자가 존재한다면, 모든 참가자가 항상 프로토콜에 참여하는 경우에는 정리 1에 의하여 2개의 라운드, 그리고 참가자가 프로토콜에 참여하지 않을 수 있는 경우에는 정리 2에 의하여 3개의 라운드가 적어도 필요함을 알았다. 이제, 부정직한 참가자들의 최대 수 t(0<t<n)에 따라서 필요한 라운드 수의 하한을 구한다. 정리 3, 4와 5에서 제시된 하한은 Baum-Waidner가 제시한 프로토콜과 동일한 라운드를 가지므로 밀착하한이다[4].

정리 3. 모든 참가자가 프로토콜에 항상 참여하는 경우, 안전한 계약서 서명 프로토콜은 적어도 $\lfloor n/(n-t) \rfloor + \lceil n/(n-t) \rceil - 1$개의 라운드가 필요하다(단 n은 프로토콜 참가자의 수, t(0<t<n-1)는 부정직한 참가자의 최대 수).

증명. 모든 참가자가 프로토콜에 항상 참여하는 경우에는 적어도 2개의 라운드가 필요함을 정리 1에서 증명하였다. 그런데, n>2t이면 $\lfloor n/(n-t) \rfloor + \lceil n/(n-t) \rceil - 1 = 2$이므로 $n \le 2t$인 즉, $\lfloor n/(n-t) \rfloor + \lceil n/(n-t) \rceil - 1 > 2$인 경우만 고려한다.

그러면, R(>2)에 대하여 라운드 $R(< \lfloor n/(n-t) \rfloor + \lceil n/(n-t) \rceil - 1)$에 완료할 수 있는 계약서 서명 프로토콜을 **P**가 존재한다고 하자. 이제 공정성에 위배되는 상태를 만들 수 있는 시나리오를 제시하여 **P**가 안전한 계약서 서명 프로토콜이 될 수 없음을 보인다. 다음은 공정성에 위배되는 상황을 만드는 시나리오이다.

1. 집합 $T=\{P_i | i=1..n\}$ 속하는 모든 참가자들에 대하여 next(0)를 구한다.
2. next(0)가 가장 작은 n-t명의 참가자를 선택하여, 자신의 next(0)에 해당하는 라운드에 TTP로 요청메시지를 송신한다. 요청메시지를 전송할 때 해당 라운드에서 다른 참가자들로부터 어떠한 메시지를 받지 못한 것으로 가장하여 요청메시지를 TTP로 전송한다. 그러면, 요청메시지를 보낸 참가자들은 모두 TTP로부터 중지메시지를 받는다. 그리고 이들의 집합을 T_1이라고 한다.
3. T_1에서 next(0)가 가장 큰 값을 R_1이라고 하고 $next(0)=R_1$인 참가자들의 집합을 S_1이라고 한다(이는 중지메시지를 받을 참가자들 중에 적어도 1명 이상의 참가자를 포함하여 n-t명의 부정직한 참가자로 결정할 수 없는 참가자가 TTP로 요청메시지를 보낸 상태를 만들기 위해서이다.).
4. $T=T-T_1$; i=1
5. $R_i < R-1$ 이면 다음 5.1-5.5를 반복한다.
5.1 T에 속한 모든 참가자들의 $next(R_i)$를 구한다.
5.2 $next(R_i)=\infty$인 P_j가 존재한다면 공정성에 위배되는 시나리오를 구성한다. 라운드 R_i 이후에도 P_j를 제외하고 메시지를 수신하는 n-t명의 참가자를 선택하여 라운드 R_i 이후에 메시지 수신을 막는다. 그러면, n-t명의 참가자들이 정직한 참가자라면 그들이 서명된 계약서를 얻지 못하여 공정성에 위배된다.
5.3 $next(R_i)=\infty$인 P_j가 존재하지 않는다면, $next(R_i)$가 작은 순서로 $n-t-|S_i|$의 참가자를 T로부터 선택하여, 각 참가자들의 $next(R_i)$에 해당하는 라운드에 TTP로 요청메시지를 보낸다. 그러면 그들은 모두 TTP로부터 중지메시지를 받는다. 그리고 그들을 T_{i+1}로 설정한다.
5.4 T_{i+1}에서 $next(R_i)$가 가장 큰 값을 R_{i+1}이라고 하고 $next(R_i)=R_{i+1}$인 참가자들의 집합을 S_{i+1}이라고 한다.
5.5 $T=T-T_{i+1}$;i=i+1;
6. 아직 요청메시지를 보내지 않은 참가자들 중에서 n-t명의 참가자들을 선택하여 라운드 R_{i+1}부터 공격자가 이들이 메시지 수신하는 것을 막는다. 그러면, 그들은 서명된 계약서를 얻지 못하므로, 그들이 정직한 참가자인 경우 공정성에 위배된다.

먼저 단계 1에서 모든 참가자들의 next(0)를 구하는 것은 항상 가능하다. 즉, 프로토콜이 수행시마다 메시지를 송수신하는 참가자들이 변경될 수 있는 프로토콜이라고 하더라도, 비동기방식의 프로토콜이라면, 참가자들이 라운드 1에서 메시지를 송신하지 않는다면, 다른 참가자들로부터 임의의 라운드에서 메시지를 수신하여야 그 다음 라운드를 진행할 수 있기 때문이다. 같은 이유로 단계 5.1에서 T에 있는 모든 참가자들의 $next(R_i)$를 구하는 것도 항상 가능하다.

프로토콜 **P**에서 모든 참가자들은 적어도 한번 이상 다른 참가자들로부터 메시지를 수신하여야 하므로 단계 2에서 n-t명의 참가자를 선택은 가능하다. 그리고 참가자들이 어떠한 메시지의 수신도 못한 상태로 TTP로 요청메시지를 전송하였으므로, TTP는 그들을 부정직한 참가자들로 결정할 수 없다. 그리고 n-t명으로부터 요청메시지를 받았으므로 보조정리 1에 의하여 중지메시지를 전송할 것이다.

이제 시나리오에서 증명이 필요한 곳은 단계 5.2, 단계 5.3과 단계 6이다.

먼저 단계 5.2에서 $|T|>n-t$ 이상이라면 이들은 적어도 라운드 R_i 이후에 메시지를 수신하는 라운드를 가지고 있으므로 P_j를 제외하더라도 라운드 R_i 이후에 메시지를 수신하는 라운드를 가지는 n-t명의 참가자들을 선택할 수 있다. 그러면, P_j는 서명된 계약서를 얻지만, P_j를 제외한 나머지 참가자들은 서명된 계약서를 참가자들과의 통신으로는 얻을 수 없다. 또, TTP로 요청메시지를 보내더라도 실제로 라운드 R_i 이후에 메시지의 수신을 하지 못하였으므로, TTP는 라운드 R_i부터 요청메시지를 보낸 참가자들을 부정직한 참가자로 결정할 수

없다. 그러므로 TTP는 보조정리 3에 의하여 중지메시지만을 전송할 수 있다. 그러므로 선택한 n-t명의 참가자들이 정직한 참가자인 경우 공정성에 위배되는 상황을 만들 수 있다.

다음으로 단계 5.3에서 $n-t-|S_i|$명의 참가자를 선택할 수 있다면 TTP는 라운드 R_i에 요청메시지를 보낸 참가자들과 자신의 라운드 next(R_i)에 요청메시지를 보낸 참가자들을 부정직한 참가자로 결정할 수 없고, 또, 부정직한 참가자로 결정할 수 없는 참가자의 수가 n-t명이상이므로 보조정리 1에 의하여 요청메시지를 보낸 $n-t-|S_i|$명의 참가자들에게 응답을 하여야 하는데, 부정직한 참가자로 결정할 수 없는 $|S_i|$명의 참가자들에게 이미 중지메시지를 전송했으므로, 보조정리 3에 의하여 이들에게도 중지 메시지를 전송해야만 한다.

이제 단계 5.2에서 $|T|>n-t$ 그리고 단계 5.3에서는 $n-t-|S_i|$을 항상 선택할 수 있음을 증명하면 단계 5.2와 단계 5.3의 수행이 올바르게 됨의 증명이 완료된다. 그런데, T_{i+1}을 선택할 때, 이전라운드에서 요청메시지를 보낸 참가자를 포함하여 n-t명의 참가자들을 선택한다. 그리고 T_1에서 n-t명을 선택한다. 그러므로 T_1에서 선택한 참가자들이 같은 라운드에 있다면 하나의 라운드에서 최대 n-t명이 선택될 수 있다. 그리고 나머지 라운드에서는 모든 연속된 2개의 라운드는 T_i와 T_{i+1}로 구분되든지 아니면 동일한 T_i에 속하는 것과 관계없이 최대 n-t명의 참가자들이 선택된다. 그러므로 라운드 $2\lfloor t/(n-t)\rfloor-1$까지 선택할 수 있는 최대 참가자의 수는 $(n-t)\lfloor t/(n-t)\rfloor$가 된다. 그런데, $\lfloor t/(n-t)\rfloor=\lceil t/(n-t)\rceil$이면 $\lfloor t/(n-t)\rfloor+\lceil t/(n-t)\rceil=2\lfloor t/(n-t)\rfloor$이고 $\lfloor t/(n-t)\rfloor\neq\lceil t/(n-t)\rceil$이면 $t-(n-t)\lfloor t/(n-t)\rfloor>0$이므로 라운드 $\lfloor t/(n-t)\rfloor+\lceil t/(n-t)\rceil-1\leq W-1$까지는 최대 t명의 참가자들로 선택할 수 있으므로 $|T|>n-t$이고, $n-t-|S_i|$명의 참가자의 선택을 할 수 있다.

그리고 위에서 알 수 있듯이 단계 6에서는 $|T|\geq n-t$이다. 그들 중에서 n-t명을 선택하여 라운드 R_i+1 이후에 메시지 수신을 하지 못하도록 한다면, 단계 5.2와 동일하게 공정성에 위배되는 상황을 만들 수 있다.

그러므로 **P**는 안전한 계약서 서명 프로토콜이 아니다. □

일부 참가자들이 프로토콜에 참여하지 않을 수 있는 경우에는 모든 참가자들이 항상 프로토콜에 참여하는 경우와는 달리 단 한명의 참가자라도 TTP에게 요청메시지를 보낸 다면 즉시 응답을 보내야 하는 것이다. 즉, 모든 참가자들이 항상 프로토콜에 참여하는 경우에는 n-t명의 참가자들로부터 요청메시지를 받을 때까지 기다렸다가 응답을 할 수 있지만 일부 참가자들이 프로토콜에 참여할 수 없는 경우에는 이는 불가능하다. 그래서 일부참가자들이 프로토콜에 참여하지 않을 수 있는 경우에는 모든 참가자들이 항상 프로토콜에 참여하는 경우에 비하여 1개의 라운드가 추가되었다.

정리 4 : 일부 참가자가 프로토콜에 참여하지 않을 수 있는 경우 안전한 계약서 서명 프로토콜은 적어도 $\lfloor n/(n-t)\rfloor+\lceil n/(n-t)\rceil$ 라운드가 필요하다. (단, n은 프로토콜 참가자의 수, $t(0<t<n-1)$는 부정직한 참가자의 최대 수)

증명. 참가자가 프로토콜에 참여하지 않을 수 있는 경우에는 적어도 3개의 라운드가 필요함은 정리 2에서 증명하였다. 그런데, $n>2t$이면 $\lfloor n/(n-t)\rfloor+\lceil n/(n-t)\rceil=3$이므로 $n\leq 2t$인 경우인 $\lfloor n/(n-t)\rfloor+\lceil n/(n-t)\rceil>3$만 고려한다.

그러면 $R(>3)$에 대하여 라운드 $R(<\lfloor n/(n-t)\rfloor+\lceil n/(n-t)\rceil)$에 완료할 수 있는 계약서 서명 프로토콜을 **P**가 존재한다고 하자. **P**가 안전한 계약서 서명 프로토콜이 될 수 없음은 정리 3의 시나리오에서 단계 2를 단 한명의 참가자만을 선택하는 것으로 변형하면, 계약서 서명프로토콜 **P**는 안전한 계약서 서명프로토콜이 아님을 증명할 수 있다. □

이제 부정직한 참가자의 최대 수가 n-1인 경우에 대하여 생각해보자. 위의 정리 3과 4에서 부정직한 참가자들은 $n-t-|S_i|$명이 요청메시지를 TTP로 전송하였다. 하지만, n-t=1인 경우 $n-t-|S_i|=0$ 또는 1이 되는데, 0인 경우를 제외하면 t명의 부정직한 참가자로 최대 라운드 t까지 TTP로 요청메시지를 보내는 참가자를 선택할 수 있을 것이다. 그리고 다음 라운드에서 정직한 참가자는 메시지를 수신하지 못하도록 한다면, TTP는 적어도 정직한 참가자를 포함하여 2명의 참가자가 부정직한 참가자인지 결정할 수 없으므로, t+1개 이하의 라운드를 가지는 계약서 서명 프로토콜은 안전한 계약서 서명 프로토콜을 완성할 수 없다.

정리 5. 안전한 계약서 서명 프로토콜은 부정직한 참가자의 최대 값이 t= n-1이면 적어도 t+2 라운드가 필요하다(단, n은 프로토콜 참가자의 수, t는 부정직한 참가자의 최대 수). □

5. 결론 및 향후 연구 방향

계약서 서명 프로토콜은 공정교환 프로토콜의 기반이 되는 프로토콜이며, 공정교환 프로토콜은 전자상거래의 기본 프로토콜이다. 다자간 계약서 서명프로토콜은 양자간의 프로토콜을 일반화한 프로토콜이다. 또, 인터넷처럼 동기 모드로 동작하기 어려운 환경을 위하여, 비동기 방식의 프로토콜의 개발은 필수적이다. 하지만, 비동기 방식의 낙관적인 다자간의 계약서 서명 프로토콜의 라운드 수의 하한은 알려져 있지 않았다. 그래서 본 논문

에서는 라운드 수의 하한을 제시하고 증명하였다. 그리고 이는 Baum-Waidner에 의하여 제시된 프로토콜이 가지는 라운드 수와 동일하므로 밀착하한이다[4]. 더욱이 비동기방식의 낙관적인 다자간 공정교환 프로토콜은 비동기방식의 낙관적인 다자간의 서명 프로토콜을 포함하므로, 다자간의 공정교환 프로토콜의 라운드의 하한 역시 동일하다. 향후에는 라운드 수뿐만 아니라 계약서 서명 프로토콜에서 요구되는 전체 메시지 크기의 하한에 대한 연구도 또한 필요하다.

참 고 문 헌

[1] N. Asokan, B. Baum-Waidner and M. Schunter, M. Waidner, "Optimistic Synchronous Multi-Party Contract Signing," IBM Research Reports RZ 3089(#93125), Zurish, 1998.

[2] J.Garay and P.MacKenzie, "Abuse-free Multi-party Contract Signing," DISC '99(LNCS 1693), Springer-Verlag, pp.151-165, 1999.

[3] B. Baum-Waidner and M.Waidner, "Round-optimal and Abuse-free Optimistic Multi-Party Contract Signing," ICALP 2000(LNCS 1853), pp.524-535, 2000.

[4] B. Baum-Waidner, "Optimistic Asynchronous Multi-Party Contract Signing with Reduced Number of Rounds," ICALP 2001(LNCS 2076), pp.898-917, 2001.

[5] N. Asokan, V.Shoup and M. Waidner, "Optimistic Protocols for Fair Exchange," CCS '97, Zurich, pp.6-17, 1997.

주 홍 돈

1992년 2월 서강대학교 학사. 1994년 2월 서강대학교 석사. 1999년 9월~현재 서강대학교 박사과정. 1994년 2월~1999년 5월 삼성전자. 2001년 7월~2002년 10월 KISA. 2005년 3월~현재 삼성전자 TN 통신연구소 근무. 관심분야는 암호프로토콜, 보안 프로토콜, 인터넷 프로토콜

장 직 현

1972년 2월 서울대학교 수학과 학사 1977년 8월 서울대학교 수학과 석사 1986년 8월 미네소타대학 전산학과 박사. 1986년 9월~현재 서강대학교 컴퓨터학과 교수. 관심분야는 알고리즘 설계와 분석, 암호알고리즘