이동성을 보장하는 상호 공정 계약 프로토콜

장경아, 이병래, 김태윤
고려대학교 컴퓨터학과
e-mail : gypsy93@netlab.korea.ac.kr

Mutual Fair Contracts Protocol for Mobility of Subject

Kyung-Ah Chang, Byung-Rae Lee, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

이동 주체의 전자 상거래 참여는 계약 문서나 결제 정보 교환 서비스에 대해 사용자 실체에 대한 증명과 교환 메시지의 사후 검증 수단을 요구하고 있다. 본 논문에서는 이동 주체의 이동성에 따른 한계적 계산 능력 및 대역폭 사용을 고려하여 부분적으로 제 3 의 신뢰 기관(Trusted Third Party, *TTP*)의 효율적인 참여 구조를 수용한 상호 공정 계약 프로토콜을 제안하였다.
본 논문에서는 기존 공정 계약 프로토콜에 대한 연구를 상거래 주체에 대한 이동성을 지원하기 위해 상호 공정 계약 프로토콜로 확장하였다. 제안한 프로토콜은 이동성에 대한 한계적 능력에 대해 해당 *TTP* 와 공개키를 기반으로 거래 주체간의 상호 인증을 수행하도록 하였으며, 이러한 초기화를 수행한 이후 상거래 주체는 해당 인증 결과를 기반으로 주체간 상호 메시지 교환을 위한 공정 계약 프로토콜을 수행하도록 하였다. 또한 사전에 동의한 계약 과정 이외의 예외 상황 발생시 부분적 TTP 의 참여를 허용하여 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다.

1. 서 론

인터넷과 결합된 전자 상거래는 거래 주체간에 전자 매체를 이용하여 상품이나 서비스 및 지불 정보를 교환한다. 기존 사용자 접근 통제 및 시스템 이용 기록 관리 등의 보안 서비스와는 달리, 전자 상거래에서는 불안전한 네트워크 구조로 인하여 거래 내용, 신용카드 정보, 관련 비밀 번호 등 주요 정보들의 노출을 방지하기 위해 사용자 실체에 대한 증명과 교환 메시지의 사후 검증 수단을 요구하고 있다.

최근 이동 에이전트 구조에 기반한 거래 주체들의 참여가 증가하면서 이에 따른 안전성 및 이동성에 대한 많은 연구가 진행 중이다. 구조적으로 이동 에이전트는 위치 정보에 대한 투명성을 보장하여야 하며 다양한 전자 상거래 구조를 수용하면서 동시에 각 시스템 영역 고유의 운영 정책을 반영할 수 있어야 한다 [2, 3]. 또한, 암호화 정책을 기반으로 무선 링크에 대한 도청 방지 및 송신 호스트의 인증으로 타호스트로의 위장 방지 서비스 등을 제공하여야 한다.

본 연구에서는 이동 주체의 이동성에 따른 한계적 계산 능력 및 대역폭 사용을 고려하여 부분적으로 제 3 의 신뢰 기관(Trusted Third Party, *TTP*)의 효율적인 참여 구조를 수용한 상호 공정 계약 프로토콜을 제안하고자 한다. 이 프로토콜은 이동성에 대한 한계적 능력에 대해 해당 네트워크의 *TTP* 와 공개키를 기반으로 거래 주체간의 상호 인증을 수행하도록 하였으며, 상거래 주체는 해당 인증 결과를 전달 받은 후에야 상호 교환을 위한 공정 계약 프로토콜을 수행할 수 있도록 하였다. 또한 공정 계약 프로토콜에서 역시 이동 주체의 특성을 고려하여 예외 상황에 대한 처리는 해당 네트워크의 *TTP* 가 일시적으로 참여하여 수행하도록 한 후 그 결과를 상거래 주체에게 통보하도록 하였다.

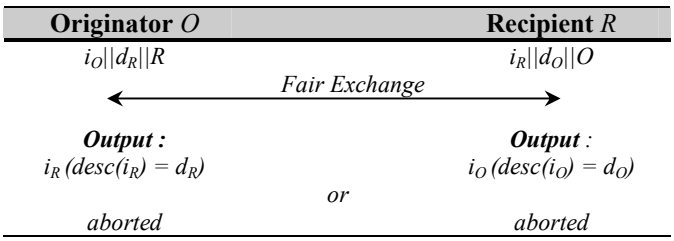
본 연구의 구성은 다음과 같다. 2 장에서 전자 상거래를 지원하기 위한 상호 교환 서비스의 요구 사항 분석 및 공개키를 기반으로 한 상거래 주체간 상호 인증 구조를 살펴본다. 3 장에서 해당 네트워크 *TTP* 의 부분적 참여를 온라인 구조를 수용하여 주체간 상호 인증 수행 및 이후 인증된 결과 정보를 통보 받은 주체의 공정 계약 프로토콜 수행시 예외 경우에 대한 수행을 보장하는 공정 계약 프로토콜을 제안한다. 마지막으로 4 장에서 결론을 내리고 향후 과제를 제시한다.

2. 전자 상거래 지원 상호 교환 서비스

2.1 상호 교환 서비스

전자 상거래의 계약 문서나 결제 정보 교환에 대한 상호 교환 서비스는 논리적 동시성 보장을 가정하였으나 네트워크 환경에서 양자간의 메시지 교환시 동시성을 보장한다는 것은 불가능하므로 제 3 의 신뢰기관을 설치하여 그 센터가 메시지를 중개하도록 구성하였다. 후자의 경우 이러한 공정 상호 교환 서비스는 온라인 제 3 기관 프로토콜(third party protocol)이라 하고, 전자의 경우 신뢰도가 통신 라운드를 통해 점차 증가되는 단계적 상호 교환 프로토콜(gradual exchange protocol)이라 한다.

그러나, 제 3 기관 해결책은 제 3 기관으로의 병목 위험이 단점으로 지적되었으며 단계적 상호 교환 해결책은 고가의 통신 오버헤드 때문에 현실적이지 못하다는 단점으로 일반적인 경우 아래의 <그림 1>과 같이 미리 정의된 예외 경우에서만 제 3 기관을 이용하는 최적화 기법이 제안되었다.



<그림 1> 공정 상호 교환 프로토콜

<그림 1>은 공정 상호 교환 프로토콜의 개요를 나타내고 있다. 상호 교환 프로토콜의 공정성은 *desc()*로 지원되며 *desc()*는 입력에 대해 상호 교환될 아이템을 연산 함수이다. 입력 i_R 에 대해 참여자 O 는 d_R 과 상호 교환되기를 기대하고 있다. 전자 상거래에서 *desc("payment")*는 지불 정보를 입력할 경우, 참여자는 지불 정보의 환율, 지불자 정보, 가치 등의 기대 값을 연산할 것이다.

서비스 초기 참가자 양측은 <그림 1>과 같이 공정 상호 교환 프로토콜에서 사용될 대상과 예외 경우에서 이용하게 될 제 3 기관에 대해 동의하도록 한다. 서비스 초기 참여자는 상대가 응답 해주기를 기대하며 그의 아이템을 전송하게 된다. 만약 다른 참여자가 기대한 아이템에 대한 응답을 회수하게 되면 프로토콜을 성공적으로 종료하게 된다. 그렇지 않은 경우 송신자는 공정 상호 교환 여부를 판단하기 위해 제 3 기관에게 접속한다. 이러한 방식을 최적화 공정 상호 교환 프로토콜(optimistic fair exchange protocol)이라고 한다. 이러한 공정 상호 교환 서비스는 아래와 같이 정리할 수 있다.

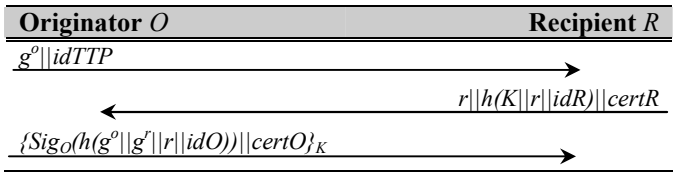
- 사용자 O 와 R 이 미리 약속된 과정을 수행하고 도중에 상호 교환을 포기하지 않는다면 프로토콜이 완료되었을 때, O 는 $i_R\,(desc(i_R) = d_R)$을 보유하게 된다.
- 프로토콜이 완료되었을 때 O 가 i_R 을 보유하고 있는 경우, R 이 i_O 에 관한 추가적 정보를 유추할 수 없는 경우, O 가 중재자에게 R 이 O 로부터 더 이상의 간섭 없이 i_O 를 받았다는 것을 입증할 수 있는 경우 본 프로토콜 수행은 공정성을 보장한다고 한다.
- 상호 교환이 성립된 후 O 는 R 로부터 생성된 아이템. i_R 를 통해 정보 기원(origin)을, R 이 받은 i_O 를 통해 부인 방지를 검증할 수 있다.

2.2 전자 상거래 지원 상호 인증 구조

전자 상거래 구조에서 임의의 이동 주체가 자신이 등록되어 있는 홈 에이전트에서 외부 에이전트로 이동하는 경우, 이동 주체와 외부 에이전트, 외부 에이전트와 홈 에이전트간의 인증이 이루어진 후 이동 주체는 서비스를 시작한다. 그러나, 이동 주체가 빈번하게 이동할 경우 이와 비례하여 인증이 수행되어야 하므로 이동 주체만의 컴퓨팅 능력으로는 한계가 있다. 또한 일반적으로 이동 주체에 대한 한계적 계산 능력은 비밀키 암호 방식 이상을 채택하기 어렵다.

본 논문에서 고려하고 있는 이동 주체에 대한 환경은 이동 주체가 외부 에이전트 시스템에 도착해서 계약 프로토콜 수행을 결정하도록 한다. 실제 계약 프로토콜은 이동 주체의 홈 에이전트와 외부 에이전트 사이간에 인증이 수행된 다음 실행 된다. 이동 주체는 홈 에이전트로부터 인증 결과를 통보 받은 후 해당 상대 주체와 계약 프로토콜을 실행하게 된다.

이동 주체의 한계적인 컴퓨팅 능력을 고려하였을 때, *TTP* 의 부분적 프로토콜 수행은 효율적이다. 또한 홈 에이전트와 이동 주체는 세션키를 공유하므로, 이동 주체는 프로토콜의 종료후, 단지 결과를 통보 받기만 하면 된다.



<그림 2> 기본 인증 프로토콜

본 논문에서 제안하는 공정 상호 계약 프로토콜의 기본 인증 구조는 O 가 난수 o 를 생성하여 공개키 동의 키(public key agreement key) g^o 와 함께 메시지를 교환하고자 하는 R 의 해당 인증 기관 정보 *id_caR* 를 R 에게 전송하면서 시작된다. <그림 2>은 기본 인증 프로토콜 구조를 나타내고 있다.

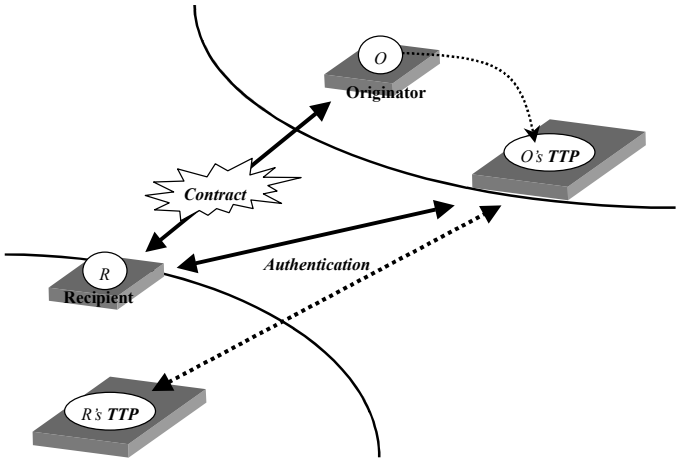
이 메시지로는 R 은 아직 통신 대상을 파악할 수 없으나 난수 r 을 생성하여 전송 받은 정보를 $(g^o)^r$ 로 연산하여 세션키 K 를 생성하여 해쉬화(h)한 후 R 의 인증서 *certR* 와 함께 전송한다. O 는 *certR* 를 통해 R 의 공개키 정보 등을 파악할 수 있으며 자신의 신분 정보 *idO* 와 함께 인증서 *certO* 를 자신의 공개키로 서명

한 후 다시 *K* 로 암호화하여 전송하게 된다. 이후 *R* 은 *certO* 를 통해 *O* 의 서명을 검증하게 되고 이 정보는 차후 서비스에 반영하도록 하며 양측은 상호간의 인증서를 교환하므로써 인증 수행시 양측 *TTP* 의 참여를 가정하고 있다.

3. 이동성을 보장하는 상호 공정 계약 프로토콜

3.1 제안한 상호 공정 계약 프로토콜 개요

본 연구에서 제안하는 프로토콜은 전자 상거래 이동 주체 상호간의 인증 및 공정 계약 과정으로 구성된다. 온라인 *TTP* 의 부분적 참여를 구조를 기반으로 상호 인증 및 공정 계약 과정에서 이동 주체의 컴퓨팅 능력 및 대역폭에 대한 오버헤드에 대한 대단위 계산의 효율성을 증가시킨다.



<그림 3> 제안한 온라인 *TTP* 참여 기반 구조

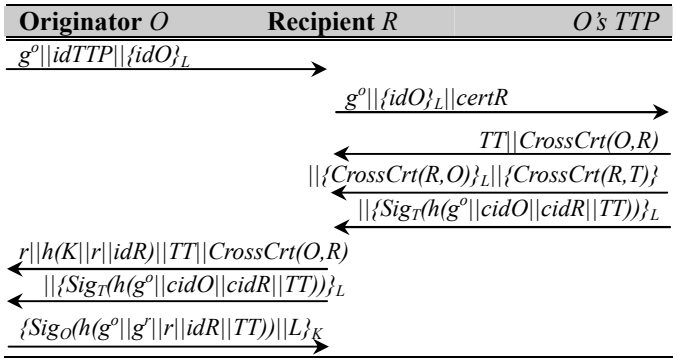
전자 상거래에 참여하고 있는 *Originator*(*O*)와 *Recipient*(*R*)는 각각 다른 *TTP* 에 등록되어 있는 주체로서 거래를 수행하기 전 주체간 상호 인증 프로토콜을 수행하므로써 초기화하도록 한다. 양측 상거래 주체 *O* 와 *R* 중 대해 이동성에 대한 지원은 각 주체의 *TTP* 에 참여를 구성하며 본 논문에서는 이동성에 대한 가정으로 *O's TTP* 를 해당 프로토콜에 함께 구성하였다. 상호간 인증된 주체는 해당 *TTP* 에 범용 인증서(*CrossCrt*)를 보유하게 되어 이것은 *TTP* 의 범주를 확장 가능하게 하며, 이후 상호 공정 계약 프로토콜 수행시 상대 주체의 서명 검증 수단으로 사용한다.

또한 상호 공정 계약 프로토콜 수행시 사전에 계약 문서 형태에 동의하도록 하였으며, 양측 참여 주체만으로 구성된 양자간 프로토콜 수행하게 된다. 그러나, 의도하지 않았던 예외 경우시 양측은 *O's TTP* 과 *Abort* 와 *Resolve* 프로토콜을 수행할 수 있으며 제안한 프로토콜은 부분적 온라인 *TTP* 의 참여구조를 지원하고 있다.

3.2 주체간 상호 인증 프로토콜

주체간 상호 인증 프로토콜은 참여자 *O* 와 *R* 이 상대방의 인증서 검증을 위해 해당 *TTP* 의 공개키 보유 및 해당 *TTP* 에 자신의 공개키에 대한 인증서 식별 정보(*cidO*, *cidR*)를 인지하고 있음을 가정한다. <그림 4>는 제안한 상호 인증 프로토콜을 나타내고 있다.

상호 인증 프로토콜은 외부 영역의 이동 주체 *O* 가 R 에게 자신의 네트워크 *TTP* 식별 정보 및 *TTP* 과의 공유 비밀키 *L* 로 암호화된 자신의 신분 정보를 전송한다.



<그림 4> 제안한 상호 인증 프로토콜

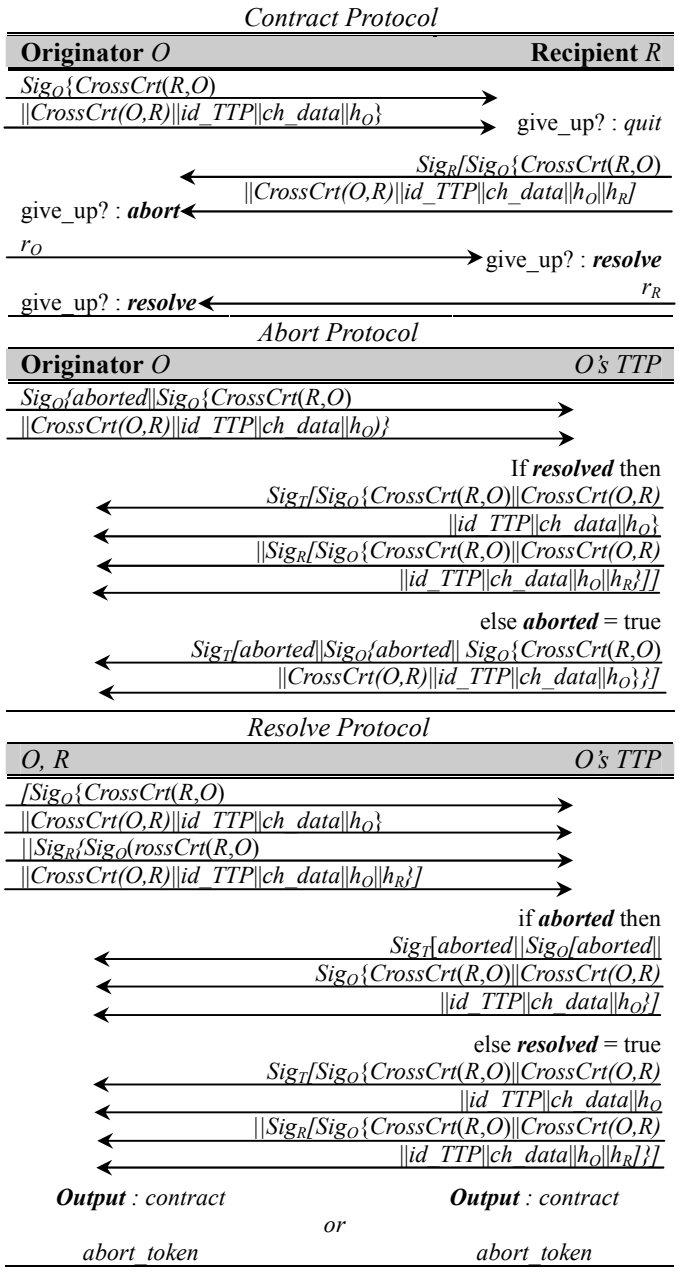
이 메시지를 *R* 은 자신의 인증서(*certR*)와 함께 *O's TTP* 에게 전달(forwarding)한다. 이때 *O's TTP* 는 $\{idO\}_L$ 를 복호화하여 현재 유용한 사용자인지를 확인하고 *R* 의 인증서 적합성 역시 검증하여 이동 주체에 대한 상호 인증을 수행하도록 한다.

만약 *O's TTP* 에 *O* 와 *R* 의 인증서에 대한 정보가 부족할 경우, *O's TTP* 는 *O* 에게 문의하는 한편, *certR* 의 발행 *TTP* 와 접속하여 *R* 이 전송한 인증서의 적합성 여부 및 신분 정보를 검증한다. 인증서의 유용성이 검증된 경우, *O's TTP* 는 타임스탬프 *TT* 와 *O* 에 대한 범용 인증서(*CrossCrt*)들과 검증된 인증서에 대한 고유 식별 정보 *cidO, cidR* 를 서명하여 암호화한 후 *R* 에게 전송한다. *CrossCrt* 는 *TTP* 가 외부 네트워크에 존재하고 온라인으로 접속이 불가능할 경우에 대비하여 해당 네트워크의 *TTP* 가 그 인증서에 서명하여 일반 인증서를 확장한 형태이다. *CrossCrt(O, R)*의 경우, *R* 의 인증서(*certR*)에 대해 *O's TTP* 가 서명하여 확장한 인증서로, *CrossCrt(R, O)*의 경우, *O* 의 인증서(*certO*)에 대해 *R's TTP* 가 서명하여 확장한 인증서로, *CrossCrt(R, T)*의 경우, *O's TTP* 의 인증서(*certT*)에 대해 *R's TTP* 가 서명하여 확장한 인증서 형태이며 각 참여자의 서명을 검증 수단으로 사용된다.

마지막으로 *O* 가 받은 메시지의 서명을 검증하여 올바르다고 판단되었다면 *O* 는 *R* 에게 비밀키 *L* 을 포함한 메시지를 세션키 *K* 로 암호화하여 전송한다. R 은 비밀키 *L* 을 사용하여 *O* 의 마지막 전송 단계 이후 *TTP* 로부터 받은 메시지를 복호화하고 그 서명을 검증할 수 있다.

3.3 온라인 상호 공정 계약 프로토콜

양자간 상호 공정 계약 프로토콜에 대해 양측은 계약 문서 형식에 동의하도록 한다. 유용한 계약 문서 구성은 각 계약 문서 인자에 대해 부인 방지 토큰을 구성하여 사후 검증 수단으로 사용하도록 하였다. 일반적으로 *O* 와 *R* 은 상대 주체가 먼저 계약서에 동의한 부인 방지 토큰들과 함께 종료되기를 기대다. 공정 계약 프로토콜은 양측 참여자가 모두 유용한 계약 수행 완료로서 종료하거나 양측 모두 종료 불가 결과를 얻게 된다.



<그림 5> 제안한 상호 공정 계약 프로토콜

본 연구에서 제안한 공정 상호 계약 프로토콜은 *Contract*, *Abort*, *Resolve* 프로토콜로 구성하였다. 정상적인 계약 수행시 양자간 프로토콜로 구성된 *Contract* 프로토콜만 실행되며, 상거래 참여 주체 *O* 와 *R* 이 프로토콜 수행에 오류가 있다는 결정으로 강제적 종료를 실행하고자 할 때 *O's TTP* 를 참여하도록 하여 온라인 구조로서 이동 주체의 지역적 수행에 있어 상대 주체의 정당성 여부를 판단하여 프로토콜의 계속 여부를 결정하도록 하였다.

<그림 5>는 제안한 상호 공정 계약 프로토콜을 나타내고 있다. 상호 공정 계약 프로토콜의 수행 과정을 정리하면 다음과 같다.

1. *O* 와 *R* 은 이미 계약서에 동의하였고 서명 검증 키로서 사전 초기화 단계에서 생성된 *CrossCrt(R,O)*와 *CrossCrt(O,R)*을 사용하며, 계약 내용에 대한 *ch_data* 와 난수 r_O 을 단방향 해쉬 함수를 사용하여 해쉬화 된 h_O 를 함께 전송한다. h_O 는 r_O 에 대한 공개 위임 수단으로 사용되며 수정될 수 없다.
2. *R* 이 프로토콜 *quit* 을 결정하는 경우, 프로토콜의 수행은 종료된다. 이때 *R* 은 규정 시간 내에 메시지를 전송 받지 못한 경우에만 철회를 결정할 것이다. 본 연구는 이동 주체를 대상으로 가정하고 있으므로 프로토콜 전반에 걸친 동기적 시각을 요구하지 않는다.
3. *O* 가 프로토콜 *abort* 를 결정하는 경우, *id_TTP* 의 해당 *O's TTP* 와 함께 *abort* 프로토콜을 실행한다. 이때 *O* 는 규정 시간 내에 *R* 의 메시지를 회수하지 못할 경우 철회한다.
4. *R* 이 프로토콜 give_up 을 결정하는 경우, *id_TTP* 의 해당 *O's TTP* 와 함께 *resolve* 프로토콜을 실행한다. 전형적으로 *R* 은 h_O 의 난수 r_O 를 시간내에 회수하지 못할 경우 철회한다.
5. *O* 가 프로토콜 give_up 을 결정하는 경우, *id_TTP* 의 해당 *O's TTP* 와 함께 *resolve* 프로토콜을 실행한다. R 의 경우와 마찬가지로 h_R 의 난수 r_R 를 시간내에 회수하지 못할 경우 철회한다

abort 프로토콜은 *O* 에 의해 프로토콜을 실패하였을 경우 사용하며 *O's TTP* 는 차후에 프로토콜을 해결하지 않을 것이다. *resolve* 프로토콜은 *O* 또는 *R* 에 의해 완료된 프로토콜 종료를 강제하기 위하여 사용된다. 상호 교환이 이미 실패하였다는 결정이 내려지면 *O's TTP* 는 단순히 *abort_token* 을 리턴한다.

상호 공정 계약 프로토코의 양측은 교환되는 서명된 메시지에 대하여 범용 인증서를 통해 서명의 공정성을 검증할 수 있으며 상거래 주체에 대한 이동성에 대해 전달(forwarding) 기법 기반으로 공정성에 대한 *TTP* 의 지원으로 상대 프로토콜과의 연결을 종료하지 않은 상태에서 해당 메시지의 검증을 수행할 수 있도록 구성하였으며 이동 주체의 계산량을 고려하여 각 메시지에 대한 연산은 사전 상호 인증 프로토콜에서 연산된 *CrossCrt* 의 사용 등을 재사용하여 효율성을 지원하였다.

4. 결론 및 향후 과제

인터넷과 결합된 전자 상거래는 기존 사용자 접근 통제 및 시스템 이용 기록 관리 등의 보안 서비스와는 달리, 거래 내용, 신용카드 정보, 관련 비밀 번호 등 주요 정보들의 노출을 방지하기 위해 사용자 실체에 대한 증명과 교환 메시지의 사후 검증 수단을 요구하고 있다.

최근 이동 에이전트 구조에 기반한 거래 주체들의 참여가 증가하고 있으나 암호화 정책을 기반으로 무선 링크에 대한 도청 방지 및 송신 호스트의 인증으로 타호스트로의 위장 방지 서비스 등을 제공하면서 동시에 시스템 측면의 투명성 등의 여러 요구 사항이 제기되고 있다.

본 연구에서는 이동 주체의 이동성에 따른 한계적 계산 능력 및 대역폭 사용을 고려하여 부분적으로 제 3 의 신뢰 기관(Trusted Third Party, *TTP*)의 효율적인 참여 구조를 수용한 상호 공정 계약 프로토콜을 제안하였다. 이 프로토콜은 이동성에 대한 한계적 능력에 대해 해당 *TTP* 와 공개키를 기반으로 거래 주체간의 상호 인증을 수행하도록 하였으며, 이러한 초기화를 수행한 이후 상거래 주체는 해당 인증 결과를 기반으로 주체간 상호 메시지 교환을 위한 공정 계약 프로토콜을 수행하도록 하였다. 또한 공정 계약 프로토콜에서 역시 이동 주체의 특성을 고려하여 예외 상황에 대한 처리는 해당 *TTP* 의 일시적 참여 구조로서 프로토콜을 수행하도록 하였으며 그 결과를 상호 공정 계약 결과에 대해 반영하도록 하였다.

본 논문에서는 기존 공정 계약 프로토콜에 대한 연구를 상거래 주체에 대한 이동성을 지원하기 위해 상호 공정 계약 프로토콜로 확장하였다. 또한 초기 상호 인증 프로토콜을 수행하므로 이동 주체 기반 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다. 향후 본 논문에서 제안한 상호 공정 계약 프로토콜의 실질적인 검증을 통한 비동기적 통신 메커니즘에 대한 연구 및 정형 검증 등의 방법을 통해 안정성 분석이 진행되어야 할 것이다.

참 고 문 헌

[1] Matthias and Schunter, Michael Waidner, “Architecture and Design of a Secure Electronic Marketplace,” *Proceedings JENC 8*, Sep 1997.

[2] W. Ford, and M. Baum, Secure Electronic Commerce, Prentice Hall, 1996.

[3] OMG, Mobile Agent System Interoperability Facilities Specification, 1998.

[4] N. Asokan and Victor Shoup, “Optimistic fair exchange of digital signatures”, *Advances in Cryptology – EUROCRYPT ’98, Springer-Verlag*, 1998.

[5] N. Asokan, Victor Shoup, Michael Waidner, “Asynchronous protocols for optimistic fair exchange”, Research Report RZ 2976(#93022), IBM Research, 1997.

[6] M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest, “A fair protocol for signing contracts”, *IEEE Transactions on Information Theory*, Vol. 36 No.1, pp.40-46, 1990.

[7] Holger Burk, Andresas Pfitzmann, “Value exchange systems enabling security and unobservability”, Computers & Security, Vol. 9 No. 8, pp.715-721, 1990.

[8] Benjamin Cox, J. D. Tygar, Marvin Sirbu, “NetBill security and transaction protocol”, *USENIX Workshop on Electronic Commerce*, USENIX, 1995.

[9] Reboert H. Deng, Li Gong, Aurel A. Lazar, Weiguo Wang, “Practical protocols for certified electronic mail”, *Journal of Network and System Managemnet*, Vol. 4 No. 3, 1996.

[10] Mattew K. Franklin, Michael K. Reiter, “Fair Exchange with a semi-trusted third party”, *ACM Conference on Computer and Communications Security*, pp1-7, 1997.

[11] N. Asokan, M. Schunter, M. Waidner, “Optimistic protocols for fair exchange”, *ACM Conference on Computer and Communications Security*, pp. 8-17, 1997.