# 모바일 전자상거래 프로토콜의 정형명세 및 분석

노정현[0*], 김일곤*, 최진구**, 김현석*, 최진영*

*고려대학교 컴퓨터학과
{jhnoh[0], igkim, hskim, choi}@formal.korea.ac.kr,

**KT 컨버전스 연구소
jinchoi@kt.co.kr

# Formal Specification and Analysis of Mobile E-commerce Protocol

Jung Hyun Noh[0*], Il-Gon Kim*, Hyun-Seok Kim*, Jin-Young Choi*,
*Dept of Computer Science & Engineering, Korea University

Jin-Ghoo Choi**
**KT Convergence Laboratory

요 약

무선 인터넷을 이용한 전자상거래가 증가함에 따라 모바일 환경에서 전자상거래를 보다 안전하고 효율적으로 사용할 수 있도록 SET/A (Secure Electronic Transaction Agent) 프로토콜이 제안되었다. 본 논문에서는 키 노출에 따른 보안 취약점을 분석이 아닌 프로토콜의 행위적 관점에서 SET/A를 정형명세하고 무선망 접속 불량이나 에이전트 동작 실패와 같은 오류 상황에 의해 교착 상태에 빠지지 않는지 정형 검증하였다. 그 결과 SET/A가 교착 상태에 빠질 수 있음을 확인하였고 확장된 SET/A 프로토콜을 제안하고 검증하였다.

## 1. 서론

IT 산업의 발달로 인터넷 이용자가 폭발적으로 늘어남에 따라 인터넷을 통한 전자상거래 시장이 급속히 성장하고 있다. 전자상거래 시장은 최근 들어 다양한 형태로 변화하고 있는데, 이 중 대표적인 것이 핸드폰이나 PDA를 이용한 무선 인터넷 환경에서의 전자상거래이다. 그러나, 무선 환경은 낮은 주파수 대역폭, 제한된 단말기 연산능력, 높은 통신 비용 등의 제약을 감안해야 하므로, 유선망에서 사용되던 것보다 훨씬 효율적이고 실용적인 전자 지불 방식이 요구되고 있다.

유선 인터넷 환경의 전자상거래에서 안전한 지급 결제를 실현하기 위해 VISA, MasterCard 사에 의해 SET (Secure Electronic Transaction) 프로토콜이 제안되었다. SET은 고객, 상인, 인증기관, 지불 결제 사업자 사이의 상호 인증, 거래 정보 기밀성, 데이터 무결성을 보장하지만, 프로토콜의 구조가 복잡하여 무선 환경에서는 적합하지 않았다. 이러한 문제점을 해결하기 위해 SET 프로토콜에 모바일 에이전트의 개념을 첨가한 SET/A 프로토콜이 제안되었다 [2]. 모바일 에이전트란 사용자가 원하는 작업을 자신의 컴퓨터가 아닌 다른 컴퓨터에서 수행할 수 있도록 도와주는 프로그램으로서, SET/A에서는 거래에 필요한 고객 정보를 가지고 상인의 서버로 이동하여 거래를 수행한 후 처리 결과를 가지고 돌아오는 기능을 담당한다. 이러한 방식은 고객의 입장에서 무선망 사용에 따른 통신 비용과 단말기의 연산량을 줄여주는 장점을 갖는다.

정형 기법을 통한 분석은 다양한 분야에서 사용되며 효과적인 것으로 평가 받고 있으며 거래의 기밀성, 데이터의 무결성, 신뢰성과 같은 다양한 속성을 분석하여 프로토콜의 안전성을 높이는데 크게 기여하고 있다. 대부분의 연구들이 키 노출에 의한 보안 취약점을 분석하는데 중점을 두었으나 [3]에서는 키의 관점이 아닌 전자상거래 행위적인 관점에서 전자상거래 프로토콜을 명세하고 전자 지갑의 기능을 검증하는 연구를 처음 시도하였다. 이밖에, 프로세스 알제브라 언어인 CSP (Communicating Sequential Processes)와 모델 체킹 도구인 FDR (Failure-Divergence Refinement)을 이용한 연구도 다수 찾아볼 수 있다 [4][5].

본 논문에서는 프로세스 알제브라 언어인 LOTOS (Language Of Temporal Ordering Specification)를 이용하여 행위적 관점에서 SET/A 프로토콜을 명세하고 CADP (Construction and Analysis of Distributed Processes) 모델 체킹 도구를 이용하여 교착 상태 속성을 검증하였다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 SET/A 프로토콜과 LOTOS, CADP에 대해 간단히 소개하고, 3장에서 SET/A를 LOTOS로 명세한 후 교착 상태에 빠지는 경우가 있는지 CADP에 의해 검증한다. 검증 결과 SET/A는 오류 상황(failure)에서 교착상태에 빠질 수 있음을 발견하고 이를 해결하기 위해 확장된 SET/A 프로토콜을 제안한다. 마지막으로 4장에서 결론과 향후 연구 방향을 언급하며 끝을 맺는다.

## 2. SET/A, LOTOS 및 CADP

### 2.1 SET/A

SET/A는 무선 환경에서 전자상거래를 보다 효율적으로 수행하기 위한 프로토콜으로서 SET 프로토콜에 모바일 에이전트 개념을 넣어 확장한 것이다. 모바일 에이전트는 고객으로부터 거래에 필요한 정보를 넘겨받은 후 네트워크를 통해 상인의 서버로 이동한 후 그곳에서 거래에 필요한 과정을 직접 수행하며 거래가 종료되면 처리 결과를 가지고 고객의 단말기로 돌아온다. 이러한 방식에 의해 고객은 통신 비용의 절감과 함께 단말기의 연산 부담을 줄일 수 있는 장점이 있다. 그림 1은 SET/A 프로토콜의 동작을 나타낸 것으로서, 고객, 모바일 에이전트, 상인, 지불 결제 사업자의 상호 작용을 나타내고 있다. 그림에서, 고객은 C, 모바일 에이전트는 Ag, 상인은 M, 그리고 지불 결제 사업자는 PG (Payment Gateway)로 표시하였다.

먼저, 고객은 모바일 단말을 이용하여 인터넷 쇼핑몰을 검색한 후 구입할 물품을 선택한다. 다음으로 모바일 에이전트를 생성하여 구입 절차에 필요한 구입 요청서, 고객 인증서, 구매 정보와 결제 정보를 만들 수 있는 데이터 등을 에이전트에게 건네준다 (STEP1). 모바일 에이전트는 그 정보를 가지고 상인의 서버로 이동하여 구입 절차의 초기화를 실행한다 (STEP2). 이때부터 상인과 에이전트 사이의 작업은 무선망을 경유하지 않고 상인의 서버 내부에서 직접 수행된다. 상인은 에이전트에게 상인 인증서, 지불 결제 사업자의 인증서와 유일한 거래 식별자를 넘겨준다 (STEP3). 정보를 건네 받은 모바일 에이전트는 고객의 인증서, 구매 정보, 암호화된 결제 정보, 전자 봉투, 이중 서명 (Dual Signature) 등을 상인에게 제공한다 (STEP4). 상인은 구매 정보와 이중 서명을 확인 하고 암호화된 결제 정보, 전자 봉투 등을 지불 결제 사업자에게 전송한다 (STEP5). 지불 결제 사업자가 이 요청에 대해 허가를 하면 (STEP6) 상인은 에이전트에게 상인 인증서, 구매 응답을 보내고 상품을 배달한다 (STEP7). 응답을 받은 에이전트는 네트워크를 경유하여 고객의 단말기로 돌아와 처리 결과를 알려준다 (STEP8).

STEP1. C → Ag: Dispatch Response
STEP2. Ag → M: Initiate Request
STEP3. M → Ag: Initiate Response
STEP4. Ag → M: Purchase Request
STEP5. M → PG: Authorization and Capture Request
STEP6. PG → M: Authorization and Capture Response
STEP7. M → Ag: Purchase Response
STEP8. Ag → C: Dispatch Response

그림 1. SET/A 프로토콜의 지불 과정

### 2.2 LOTOS

LOTOS는 통신 프로토콜과 분산 시스템 등을 명세하기 위해 ISO에서 개발한 정형 명세 언어로서, 프로세스 알제브라 언어인 CCS (Calculus of Communication System), CSP (Communication Sequential Processes)로 표현된 Basic LOTOS와 추상적인 데이터 타입 언어인 ACT ONE으로 표현된 Full LOTOS의 두 부분으로 구성되어 있다. Basic LOTOS는 프로세스의 행위를 모델링 할 수 있으며, Full LOTOS는 데이터 구조와 값을 표현할 수 있다 [6].

### 2.3 CADP

CADP는 통신 프로토콜과 분산 시스템 등을 디자인하고 검증하기 위해 VASY와 INRIA Rhone-Alpes에서 만들어진 통합 도구로서 CAESAR.ADT, CAESAR, ALDEBARAN 등의 세분화된 도구들로 이루어져 있다 [7]. CAESAR.ADT와 CAESAR는 LOTOS의 행위 부분과 데이터 부분을 컴파일 하여 LTS (Labeled Transition System)또는 C 코드로 바꾸어주는 역할을 하며, ALDEBARAN은 LTS 표현을 다양한 동치 관계를 통해 검증할 수 있는 기능을 제공한다

## 3 SET/A 프로토콜의 명세 및 검증

### 3.1 SET/A 명세

그림 2는 SET/A를 LOTOS로 명세한 것으로서, 프로토콜 참여자인 고객, 모바일 에이전트, 상인, 지불 결제 사업자를 프로세스로 표현하고, 각 프로세스가 주고 받는 메시지들의 중간에 채널 프로세스를 두었다. 참여자 프로세스들 사이와 채널 프로세스들 사이는 병렬적 (||| 기호로 표기)으로 명세하였고, 참여자 프로세스와 채널 프로세스 사이는 동기적 (|[]| 기호로 표기)으로 움직이게 하였다. 본 논문에서는 지면상의 이유로 LOTOS 코드의 주요 부분만을 명시한다.

```
Specification SETA_protocol [c_out_ag, c_in_ag, ag_in_c,
ag_out_c, ag_out_m1, ag_in_m1, ag_out_m2, ag_in_m2, m_in_ag1,
m_out_ag1, m_in_ag2, m_out_ag2, pg_in_m, pg_out_m, m_out_pg,
m_in_pg] : noexit
behaviour
(
   (
      CUSTOMER [c_out_ag, c_in_ag]
      |||
      MOBILE_AGENT [ag_in_c, ag_out_c, ag_out_m1, ag_in_m1,
ag_out_m2, ag_in_m2]
      |||
      MERCHANT [m_in_ag1, m_out_ag1, m_in_ag2, m_out_ag2,
m_out_pg, m_in_pg]
      |||
      PAY_GW [pg_in_m, pg_out_m]
   )
   |[c_out_ag, c_in_ag, ag_in_c, ag_out_c, ag_out_m1, ag_in_m1,
ag_out_m2, ag_in_m2, m_in_ag1, m_out_ag1, m_in_ag2, m_out_pg,
m_in_pg, m_out_ag2, pg_in_m, pg_out_m]|
   (
      C_Ag[c_out_ag, ag_in_c]
      |||
      Ag_C [ag_out_c, c_in_ag]
      |||
      Ag_M1 [ag_out_m1, m_in_ag1]
      |||
      M_Ag1 [m_out_ag1, ag_in_m1]
      |||
      Ag_M2 [ag_out_m2, m_in_ag2]
      |||
      M_Ag2 [m_out_ag2, ag_in_m2]
      |||
      M_PG [m_out_pg, pg_in_m]
      |||
      PG_M [pg_out_m, m_in_pg]
   )
)
where  (* 이하 생략 *)
```

그림 2. SET/A 프로토콜의 LOTOS 명세

### 3.2 SET/A 검증

SET/A는 무선 환경에서 에이전트의 동작으로 거래가 이루어 지는 프로토콜이다. 즉, 불안정한 무선 통신 환경과 에이전트 프로그램의 버그 등 기존의 환경보다 안전성이 떨어질 수 밖에 없다. 그림 3은 무선망의 접속 불량과 에이전트의 동작 실패 등과 같은 오류 상황이 발생할 때 SET/A가 교착 상태에 빠질 수 있음을 보여주고 있으며 그림 4는 그림 3에서의 오른쪽 창의 결과를 보여주고 있다. 교착 상태의 속성은 도구에서 기본적으로 분석할 수 있게 제공해주고 있다.

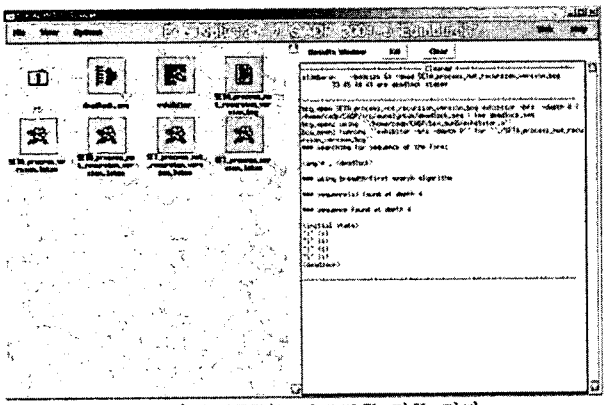

그림 3. SET/A 프로토콜 검증 결과

```
39. 45. 48. 49 are deadlock states
----------------------------------------------------
*** searching for sequence of the form:
<any>* . <deadlock>
*** using breadth-first search algorithm
*** sequence(s) found at depth 4
*** sequence found at depth 4
<initial state>
"i" (i)
"i" (i)
"i" (i)
"i" (i)
<deadlock>
```

그림 4. SET/A 프로토콜 검증 결과

### 3.3 확장된 SET/A

위의 문제를 해결하기 위해 SET/A의 명세 부분에 다음의 두 가지를 추가하였다. 첫째, 고객이 모바일 에이전트로부터 응답을 받지 못 한 경우 직접 상인에게 결과에 대한 질의를 요구한다. 이 방법은 [8]에 제안된 방법이며, 본 논문에서는 추가적으로 두 번째 방법을 제안하였다. 어떠한 이유로든 거래가 실패하여 장시간 응답 또는 요청이 오지 않을 경우 각 프로세스마다 타임 아웃을 넣어 응답 또는 요청을 재전송할 수 있게 설계하였다. 확장된 SET/A 프로토콜의 검증 결과는 교착 상태가 발생하지 않음을 확인할 수 있다. 그림 5와 6은 확장된 SET/A의 명세의 일부분과 검증 결과를 보여주고 있다. 본 논문에서는 지면상 이유로 확장된 SET/A의 명세는 생략한다.

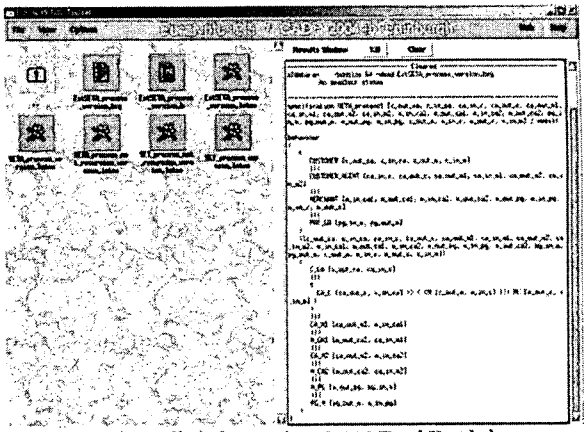

그림 5. 확장된 SET/A 프로토콜 검증 결과

```
No deadlock states
----------------------------------------------------
```

그림 6. 확장된 SET/A 프로토콜 검증 결과

### 4. 결론

본 논문에서는 전자상거래의 행위적인 측면에서 SET/A 프로토콜을 명세하고 무선망 접속 불량, 에이전트 동작 실패 등의 오류 상황에서 교착 상태에 빠지지 않는지 검증하였다. 검증 결과로부터 SET/A 프로토콜이 교착 상태에 빠질 수 있음을 확인하고 이를 해결하기 위해 확장된 SET/A 프로토콜을 제안하였다.

향후, 물품에 대한 공정한 거래를 지원하도록 SET/A 프로토콜을 확장한 후, 정형기법을 이용하여 명세하고 검증할 것이다.

### 5. 참고문헌


[1] VISA INTERNATIONAL and MASTERCARD INTERNATIONAL, "Secure Electronic Transaction (SET) Specification," Version 1.0, May 1997.

[2] A. Romao and M.M. da Silva, "An agent-based secure internet payment system for mobile computing," In Proceedings of TREC '98, LNCS 1402, pages 80-93, 1998.

[3] S. Stepney, D. Cooper, and J. Woodcock, "An Electronic Purse : Specification, Refinement, and Proof," Technical Report RPG-126, 2000.

[4] N. Heintze, J.D. Tygar, J. Wing, and H.C. Wong, "Model Checking electronic commerce protocols," In Proceedings of the Second USENIX Workshop on Electronic Commerce, pages 147-164, 1996.

[5] G. Lowe and B. Roscoe, "Using CSP to detect errors in the TMN protocol," IEEE Transactions on Software Engineering, 23(10) :659-669, 1997.

[6] T. Bolognesi and E. Brinksma, "Introduction to the ISO Specification Language LOTOS," Computer Networks and ISDN Systems, vol. 14(1), pages 25-59, 1987.

[7] H. Garavel, F. Lang and R. Mateescu, "An Overview of CADP 2001," European Association for Software Science and Technology (EASST) Newsletter volume 4, pages 13-24, August 2002.

[8] V. S. Lam and J. Padget, ""Formal Specification and Verification of the SET/A Protocol with an Integrated Approach," CEC, pages 229-235, July, 2004.