情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

프라이버시 보호 및 부인방지를 제공하는 택배 시스템 제안*

최 민 석,† 조 관 태, 이 동 훈‡
고려대학교 정보보호대학원

Privacy Protection and Non-repudiation Mechanisms for Parcel Service*

Min Seok Choi,† Kwantae Cho, Dong Hoon Lee‡
Graduate School for Information Security, Korea University

요 약

최근 택배산업의 성장과 물량이 급격히 증가하면서 피해 사례가 계속해서 늘어나고 있다. 현재 택배서비스 이용 시 피해가 발생한 경우 책임소재 입증불가 및 사업자의 책임회피로 택배 이용 고객들은 피해보상을 제대로 받지 못하고 있다. 특히 운송물 분실 시 택배사업자와 수하인 또는 대리인의 책임소재를 입증할 수 있는 증거자료가 부족하기 때문에 책임이 불명확하고 책임소재 파악을 위하여 많은 시간이 소요된다. 이를 사전에 방지하기 위해서 관련된 증거를 생성, 수집, 유지, 활용, 입증 등이 반드시 필요하다. 본 논문에서는 택배 운송장에서 발신자 정보와 수신자 정보를 암호화 및 코드화하여 개인정보를 보호한다. 또한, 피해 사례 발생 시, 정의된 발신 코드 및 수신 코드를 이용하여 발신・배송・수신에 대한 명확하고 신속한 책임 소재 파악이 가능하도록, 효율적이고 안전한 부인방지 프로토콜을 제안한다.

ABSTRACT

As delivery services market has grown the damage cases are also continuously increased. When using delivery services, Customers would not be compensated in any way. Perhaps worse, losing a cargo would create a great deal of trouble. Because the lack of evidence, they takes a lot of time to clarify who is responsible. To prevent these things, we must create, collect, maintain and confirm. In this paper, we introduce new delivery system with a trusted third party for non-repudiation services. Moreover, in damage case, we show that the proposed system is efficient and provide non-repudiation. Using sending and receiving codes, the proposed system identifies a responsible subject with quickness and clearness.

Keywords: Privacy, Non-repudiation, Parcel service, The distribution industry, Personal information

I. 서 론

국내 택배산업은 CATV 홈쇼핑과 전자상거래의 발전 등에 힘입어 2005년 택배물량이 5억 7천만 개에 불과하던 것이 2011년도에는 14억 6천만 개로 크게 증가했다[1]. 택배물량이 증가하면서 택배서비스 피해 사례도 급격히 증가하고 있지만, 피해를 예방하기 위한 법률적 또는 기술적 방안이 부족하다. 현재 택배서비스 피해 발생 시 피해 구제절차가 복잡하고 증거자료 부족 등으로 많은 시간과 비용이 소요되고 있으며, 대부분의 피해자들은 제대로 된 피해보상을 받지 못하고 있다. 공정거래위원회 표준약관 제10026호에

접수일(2012년 09월 13일), 게재확정일(2012년 11월 26일)
* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음.
† 주저자, koreacms@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

서는 운송물의 멸실, 훼손과 같은 사고 발생 시 손해배상 금액을 운송장에 기재된 운송물의 가액을 기준으로 산정한다고 명시되어 있다[2]. 하지만 현재 운송장에는 대부분 운송물의 가액이 기재되어 있지 않고 있어 손해배상 금액 산정에 어려움이 있다[3]. 또한, 개인정보보호에 대한 인식이 높아지면서 기업뿐만 아니라 국가적 차원에서도 많은 노력을 하고 있지만 대부분 온라인 기반에서의 개인정보보호로 오프라인에서의 개인정보보호에 대해서는 그 노력이 상대적으로 많이 부족하다. 현재 운송장에는 고객의 주소, 이름(또는 상호) 및 전화번호 등의 개인정보가 그대로 노출되어 있거나, 고객의 성명과 전화번호와 같은 정보는 일부분 마스킹 처리 하고 있다. 이러한 이유로 운송장을 폐기할 때 각별히 신경을 써야 하는 실정이다[4-5]. 최근 운송장을 이용한 사회공학적 공격사례와 보이스피싱이 빈번하게 발생하고 있으며, 매년 그 피해액도 증가하고 있다[6]. 오픈마켓과 소셜커머스 등 전자 상거래 증가와 함께 운송장에 적힌 정보를 악용한 범죄가 잦아지고 있으며 그 유형도 보이스피싱에서 물품 가로채기, 상해, 성범죄에 이르기까지 갈수록 고도화·세분화 되고 있다[7,8].

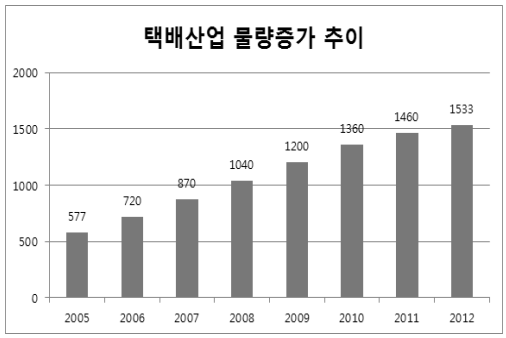
본 논문에서는 위와 같은 문제를 해결하기 위해 신뢰된 제3의 기관(TTP: Trusted Third Party)을 이용하여 발신자 정보를 수신자의 일회용 비밀키로 암호화하고, 수신자 정보를 배송기관의 비밀키로 암호화하는 방법을 이용하여 운송장에서 발신자와 수신자의 정보를 보호하는 프로토콜을 제안한다. 공개키 기반(PKI)의 인증서와 신뢰된 제3의 기관에 의해 생성된 부인방지 토큰을 이용하여 발신, 수신, 배송에 대한 부인방지 메커니즘을 제공한다[9]. 신뢰된 제3의 기관은 고객의 개인정보를 보호하기 위하여 개인정보를 암호화하고, 암호화된 정보를 다시 코드화하여 운송장을 생성한다. 그리고 수집된 증거자료를 활용하여 발신, 수신, 배송에 대한 부인방지 서비스를 제공하고 사고 및 분쟁발생 시 증거자료를 제공하는 역할을 담당한다.

본 논문의 구성은 2장에서 현재 물류 운송서비스 현황과 문제점을 분석하고, 3장에서는 현재 운송업계에서 고객의 개인정보를 보호하기 위해 개발된 기술을 소개한다. 4장에서는 보안 요구사항과 제안하는 서비스 시나리오와 프로토콜을 자세하게 설명한다. 5장에서 제안하는 프로토콜에 대한 안전성 및 효율성을 분석하고, 6장에서 본 논문의 결론을 내린다.

II. 물류 운송서비스 현황과 문제점

2.1 물류 운송서비스 현황

국내 택배산업은 CATV 홈쇼핑과 전자상거래의 발전 등에 힘입어 2005년 택배물량이 5억 7천만 개에 불과하던 것이 2011년도에는 14억 6천만 개로 크게 증가하였으며, 2012년도에는 15억 3천만 개로 예상되고 있다. 시장규모로는 3조 3,100억 원대에 이르며, 대한민국 국민이 5,000만 명이라고 가정할 때 1인당 1년 동안 약 26건의 택배를 이용하는 것이다.



〔그림 1〕 택배산업 물량증가 추이 (단위: 백만 개)

현재 택배산업은 더욱 신속하고, 저렴한 비용으로 택배 물량을 운송하기 위해 많은 노력과 투자를 하고 있다. 대표적으로 허브터미널 운영과, 종합정보시스템 구축 및 인터넷 예약 서비스 등이 있으며, 최근에는 모바일을 활용한 서비스가 제공되고 있다. 택배시스템의 주요 업무는 크게 배송품 집하와 배송이다. 배송품 집하 업무는 해당 지역의 담당 배송사원이 개인이나 기업 또는 수탁점을 방문하여 운송장을 발급하고 배송품을 인수하는 업무를 말하며, 배송 업무는 영업소에서 배송품을 도착지 또는 배달지 별로 분류하고 터미널로 운송하여 최종적으로 수하인에게 배송품을 인계하는 업무를 말한다. 현재 가장 많이 사용되고 있는 배송품 접수 방법으로는 고객이 택배사업자에게 직접 전화를 하여 접수하는 방법이다. 그리고 인터넷 사용이 보편화되고 전자상거래에 친숙한 세대가 소비의 주체로 떠오르면서 인터넷을 이용한 택배 접수도 지속해서 증가 하고 있다. 현재 택배 시스템에서 배송물의 구분과 업무 프로세스 전산화를 위하여 1차원 또는 2차원 바코드를 사용하고 있다[10]. 하지만 사용되고 있는 바코드는 정보의 양이 한정적이라는 문제점과 각

〔표 1〕 개인정보보호법 주요 내용

조항	주요 내용
제17조(개인정보의 제공) 제1항 제2호	정보주체 동의 없이 개인정보를 제3자에게 제공하지 말 것
제59조(금지행위) 제1호	영리 또는 부정한 목적과 수단으로 개인정보를 취득하지 말 것
제3조(개인정보 보호 원칙) 제6항	사생활 침해 우려 정보를 다루지 말 것
제59조(금지행위) 제2호	업무상 알게 된 개인정보를 누설하지 말 것
제59조(금지행위) 제3호	타인 개인정보를 훼손, 멸실, 유출하지 말 것
제25조(영상정보처리기기의 설치·운영 제한) 제5항	영상정보처리기기를 설치목적에 맞게 사용할 것
제24조(고유식별정보의 처리 제한) 제3항	안전성 확보 조치 없이 개인정보를 분실, 도난, 유출하지 말 것
제36조(개인정보의 정정·삭제) 제2항	정정, 삭제에 필요한 조치 없이 개인정보를 계속 이용하지 말 것
제37조(개인정보의 처리정지 등) 제2항	개인정보처리 정지요구를 무시하고 계속 이용하거나 제3자에게 제공하지 말 것

각의 택배사업자별로 요구하는 역할과 코드화된 정보가 서로 다르므로 통합적으로 관리할 수 없다.

2.2 물류 운송서비스 문제점

2011년 3월 29일 자로 공포된 개인정보보호법은 일정 기간 계도기간을 거쳐 지난 2012년 3월 30일부터 본격적인 시행에 들어갔다. 이번에 개정된 개인정보보호법의 주요 내용은 〔표 1〕과 같다〔11〕.

택배업체에서는 이번 개인정보보호법 시행과는 큰 관련이 없어 보이지만 일반 고객들을 대상으로 한 택배업체들의 경우 개인정보보호법을 준수해야만 한다〔12〕. 그러나 지금껏 택배업체들은 이러한 개인정보보호에 대해 둔감하게 반응해왔으며, 택배상자에 부착된 운송장을 통해 개인정보가 유출된 사건이 발생한 후 이를 방지하고자 노력한 사례들은 있지만, 전체 취합된 개인정보유출 방지를 위한 노력은 다소 미흡하다. 해당 배송사원들이 수거한 택배운송장을 종이상자에 담아 영업소 구석에 장기간 보관하는 사례가 많았으며, 배송을 위해 스캔 받은 운송장 개인정보들이 아무런 잠금장치도 없는 컴퓨터 상에 보관하는 업체들도 있다. 만약 누군가가 악의적으로 이러한 개인정보를 유출하고자 했다면 손쉽게 유출이 가능한 구조로 운영되고 있는 현실이다〔13〕. 또한, 기존에는 고객이 상품을 주문하면 바로 고객의 정보를 택배회사에 제공하였지만, 앞으로는 이러한 절차에 대해 고객에게 통지해야 하며 고객의 개인정보를 제3자(택배회사)에게 제공하기 위해 반듯이 동의를 얻어야 한다. 기존에는 배송업무를 처리하는 과정에서 발생한 개인정보유출 사고의 대다수는 택배업체들의 잘못으로 처리되는 경우가 많았으나 이제는 개인정보를 맡긴 수탁자가 손해배상을 해야만 한다.

현재 물류 운송시스템의 또 다른 문제점으로 배송업무 중 사고나 피해 발생 시 증거자료가 부족하여 피해보상을 받는데 소요되는 시간이 오래 걸린다는 점과 분실 시 그 책임이 불분명하다는 문제점이 있다.

〔표 2〕 택배 사고 현황

(단위: 건)

구분	파손, 훼손	분실	계약 위반	기타	계
2008년	86	69	3	4	168
2009년	80	42	5	1	130
2010년	108	92	3	12	220
2011년	130	94	3	17	240

한국소비자원에 따르면 택배 사고(분실·파손·계약위반 등)는 지난 2008년 168건에서 지난해 244건으로 약 45%가량 증가했다〔14〕. 또한, 경기도 소비자정보센터가 도내 소비자 1,097명과 12개 사업자를 대상으로 택배서비스 이용 및 운용실태 설문조사를 시행한 결과, 응답자의 28.2%가 택배서비스 피해를 경험했다고 답했다. 피해내용은 '물품 파손'과 '물품 분실'이 가장 많았고 그 중 68.6%는 피해보상을 받지 못했다고 응답했다. 피해보상을 받지 못한 이유로는 '책임소재 입증불가' 41.2%, '사업자의 책임회피' 36.9% 등이었다. 택배서비스 이용 시 가장 불편한 점으로는 '부재중 처리 미흡'으로 조사되었으며, 개선되길 바라는 점으로는 '안전배송'에 관한 의견이 가장 많았다〔15〕. 현재 택배 서비스에서는 수신 또는 배송에 대한 부인방지 서비스를 완벽하게 제공하지 못하고 있으며, 기존의 수취인 서명 또는 대리인 서명만으로는 사고발생 시 증거자료로 활용하기에는 부족한 면이 있다.

III. 관련 연구

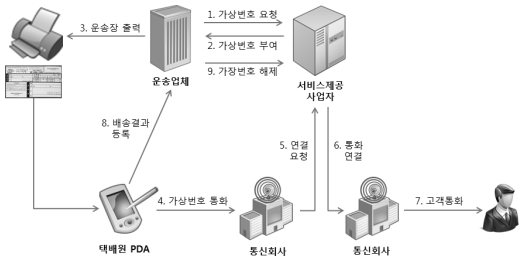
지금까지의 택배 서비스에서 고객의 배송품과 개인정보를 보호하기 위해 여러 기술이 제안되었다. 이 장에서는 고객의 배송품과 개인정보를 보호하기 위한 기술 중 코팅처리 기술과 가상번호 서비스에 대한 소개, 마지막으로 암호화된 바코드 운송장에 대해 자세히 알아본다.

3.1 코팅처리 기술

수기 운송장은 보통 3~4장으로 이루어져 고객이 송수하인의 주소, 전화번호 등을 기재하면 감압복사지를 통해 중첩된 여러 장에 모든 정보가 함께 인쇄된다. 그러기 때문에 상자를 폐기 시, 개인정보 노출 가능성이 매우 높다. 그래서 개발된 운송장은 배송품에 붙이는 마지막 장의 전화번호 기재란을 코팅 처리해 정보를 제한적으로 인쇄시켜 정보 노출을 방지하는 기술이다[16].

3.2 가상번호 서비스

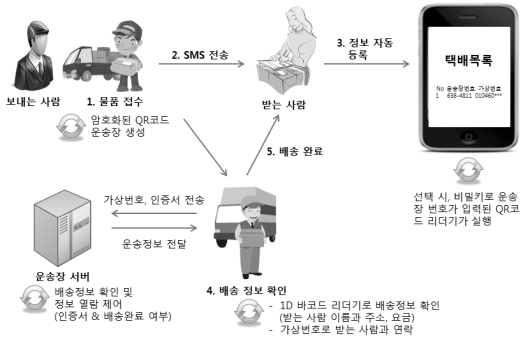
가상번호 서비스는 해당 고객의 전화번호 대신 암호화 프로그램에 의해 생성된 가상의 전화번호를 사용하는 것이다. 제3자는 고객의 진짜 전화번호를 알지 못한 생태에서도 가상번호를 통해 고객과 직접 통화할 수 있다. 또한, 배송이 완료된 뒤에는 그 번호가 자동 해지되기 때문 운송장이 노출되더라도 고객의 전화번호는 보호할 수 있다[17].



[그림 2] 가상번호(안심번호) 서비스

3.3 암호화된 바코드 운송장

운송장 자체를 키 교환 방식으로 암호화하여 QR 코드 기반의 바코드 운송장을 생성한다. 암호화에 사용된 키는 운송업체와 물품 수령자만 알고 있는 정보이며, 운송장 조회 시 사용되기도 한다. 운송장의 모든 정보가 암호화되었기 때문에 제3자는 운송장에 대한 정보를 알 수 없다[18].



[그림 3] 암호화된 바코드 운송장

IV. 제안하는 서비스

본 장에서는 논문에서 제안하는 암호화된 QR코드[19]를 이용하여 운송장에서 고객의 개인정보를 보호한다. 또한, 기존의 택배 서비스에서 배송업무 중 사고나 피해가 발생했을 경우 증거자료 부족과 부인방지 서비스를 제공하지 않아 피해보상을 받는데 오랜 시간이 소요되는 문제점과 분실 시 그 책임이 불분명하다는 문제점을 해결하기 위하여 신뢰된 제3의 기관을 활용한다. 단, 신뢰된 제3의 기관은 현실적으로 타당성이 없으므로, 증거자료를 생성 및 저장하는 역할과 피해 발생 시 증거자료를 제공하는 역할을 담당한다.

4.1 용어표기

[표 3] 용어표기

용어	정의
A	발신 실체를 구분하는 식별자, 발신자
B	수신 실체를 구분하는 식별자, 수신자
DA	배송 기관(delivery authority)
TTP	신뢰된 제3의 기관, 부인방지 토큰을 생성, 발신, 수신 Code를 생성
S_info	발신자 정보(이름, 주소, 전화번호)
R_info	수신자 정보(이름, 주소, 전화번호)
D_info	배송자 정보(이름, 배송기관, 전화번호)
P_info	물품 정보(발송 물품, 수량, 가격)
s_key	발신자의 개인키(PKI 기반)
s`_key	발신자의 공개키(PKI 기반)

ttp_key	TTP 비밀키(TTP만 소유)
d_key	배송자 또는 배송기관의 비밀키(TTP와 키공유)
r_key	수신자 일회용 비밀키(TTP와 키공유)
R_token	수신부인방지 토큰(S_info, SN, TD 정보를 ttp_key를 이용하여 MAC 생성)
D_token	배송부인방지 토큰(R_info, SN, TD 정보를 ttp_key를 이용하여 MAC 생성)
S_code	발신 코드(P_info, SN, R_token 정보를 r_key로 암호화한 코드)
R_code	수신 코드(R_info, SN, D_token 정보를 d_key로 암호화한 코드)
D_code	배송기관 코드 정보(Number or Character)
TD	서비스 요청 시간 정보
SN	운송장 번호
MD	메시지 다이제스트(Message Digest), 메시지 평문의 Hash 값
SD	개인키로 전자서명된 값(Signed Data)
GPS_info	위치정보(위도, 경도, 시간)
PON	검증 및 처리 결과 값('완료' 또는 '실패')

4.2 제안하는 시스템 모델

4.2.1 전제 조건

고객의 개인정보를 보호하면서 부인방지서비스 제공하기 위해서는 다음과 같은 전제 조건을 만족해야 한다.

1) 운송장 암호화 및 부인방지 서비스를 제공하기 위하여 TTP의 존재가 필수적이고, 일반적으로 Online TTP를 사용한다.
2) 배송자의 단말기는 QR코드를 스캔할 수 있어야 하며, GPS 정보수신과 무선통신이 가능해야 한다.
3) 발신자, 배송자 또는 배송기관, 수신자는 동일한 TTP를 신뢰한다.
4) 발신자는 발신자의 개인키(s_key)를 소유하고 있으며, TTP는 발신자의 공개키(s'_key)를 소유하고 있다.
5) TTP는 자신의 키(ttp_key)를 소유하고 있으며, 배송자 또는 배송기관의 비밀키(d_key)를 안전하게 공유한다.
6) 수신자는 SMS 또는 e-Mail을 수신할 수 있는 단말기(예를 들어, 모바일폰)를 소유하고 있다.
7) TTP는 수신자의 일회용 비밀키(r_key)를 생성하고 수신자에게 안전하게 분배한다.

4.2.2 보안 요구사항

현재 택배 서비스 이용 시 운송장에 기재되어 있는 고객의 개인정보는 손쉽게 유출될 수 있다는 단점을 해결하기 위하여 도입된 바코드 운송장은 고객의 정보를 암호화하여 더욱 안전한 서비스를 제공해야 한다. 이러한 부분을 해결하기 위한 보안 요구사항으로는 다음과 같다.

1) TTP는 안전한 인증과 부인방지에 대한 증거자료를 수집 및 보관해야 한다.
2) 인가되지 않은 제3자는 운송장에서 어떠한 정보도 얻을 수 없어야 한다.
3) 서비스 요청 시 운송장 정보에 대해서 무결성 검증과 발신자 인증을 해야 한다.
4) 배송자가 수신자 정보를 요구 시 먼저 배송자를 인증 후 수신자 정보를 제공해야 한다.
5) 배송품을 수신자에게 인계 시 정확한 수신자인지를 인증해야 한다.
6) TTP가 생성하는 어떠한 정보도 제3자가 생성할 수 없어야 한다.
7) 발신자, 수신자, 배송기관이 동일한 경우 생성되는 토큰 및 바코드는 서로 상이해야 한다.
8) 택배 사고 발생 시 배송자는 본인이 업무를 충실히 이행하였음을 입증할 수 있어야 한다.
9) 발신자는 배송품을 발신한 것에 대한 부인방지가 가능해야 한다.
10) 배송자는 배송품을 전달한 것에 대한 부인방지가 가능해야 한다.
11) 수신자는 배송품을 수신한 것에 대한 부인 방지가 가능해야 한다.

4.2.3 제안 프로토콜

1) 서비스 요청: 인터넷을 통한 택배 서비스 요청 시 S_info, R_info, 배송기관 선택, P_info를 입력하고 입력된 값에 무결성 검증을 위한 MD 생성, 발신 부인방지를 위해 전자서명(SD) 후 TTP에 관련 정보를 전송한다.

- $Send(M, SD)$
  $M = S\_info \| R\_info \| D\_code \| P\_info$
  $MD = HASH(M)$
  $SD = SIGN_{s\_key}(MD)$

2) 검증 및 코드 생성: 전송받은 데이터(M', SD')에 무결성 검증과 발신자 검증을 거친 후, TTP는

SN을 생성하고, R_token과 D_token을 생성하여 S_code, R_code를 생성한다.

- $Verify(SD)$
  $M' = S\_info \| R\_info \| D\_code \| P\_info$
  $MD = HASH(M')$
  $MD' = VERIFY_{s'\_key}(SD')$
  $IF(MD = MD') => Success$
- $ELSE => Failure$
- $Gen(SN, Tokens, Code)$
  $SN = RAND()$
  $R\_token = MAC_{ttp\_key}(S\_info \| SN \| TD)$
  $D\_token = MAC_{ttp\_key}(R\_info \| SN \| TD)$
  $S\_code = ENC_{r\_key}(P\_info \| SN \| R\_token)$
  $R\_code = ENC_{d\_key}(R\_info \| SN \| D\_token)$

3) 코드 전송: TTP는 발신자가 선택한 배송기관에 S_info와 생성된 바코드 운송장, SN을 전송한다.

- $Send(M, Codes, SN)$

4) 서비스 접수 완료 통지: TTP는 발신자에게 서비스가 정상적으로 완료 되었다는 것을 SMS 또는 e-Mail 등으로 통지한다.

- $Send(M, SN, PON)$

5) 코드 출력 및 물품 접수: 배송기관은 TTP에서 전송받은 바코드 운송장을 출력하고 배송자를 직접 찾아가 배송품을 접수한다.

- $Print(Code, SN), Recipt$

6) 배송품 접수 완료 통지 및 검증: 배송자가 발신자로부터 배송품을 인계받았을 때 배송품에 바코드 운송장을 부착하고, 배송자의 단말기로 R_code를 스캔한다. 스캔 시 배송자의 인증을 위해 d_key를 입력하여 R_code를 복호화한다. 배송자 단말기는 복호화된 D'_token과 SN을 현재 위치정보(GPS_info), D_info와 함께 TTP에 자동으로 전송한다. TTP는 전송받은 SN으로 2) 검증 및 코드 생성에서 생성한 D_token과 전송받은 D'_token을 비교하여 TTP가 생성한 부인방지 토큰인지를 검증한다.

- $R\_info \| SN \| D'\_token = DEC_{d\_key}(R\_code)$
- $Send(D'\_token, GPS, SN, D\_info)$
- $IF(D\_token = D'\_token) => Success$
  $ELSE => Failure$

7) 배송 정보 전송: TTP는 수신자에게 물품정보와 TTP가 생성한 일회용 비밀키(r_key), 배송자 정보를 SMS, e-Mail 등으로 통지한다.

- $Send(S\_info, r\_key, SN, P\_info)$

8) 배송 완료 및 서명 요청: 배송자가 배송품을 수신자에게 인계할 시 발신코드를 배송자 단말기로 스캔한다. 스캔 시 수신자 인증을 위해 수신자의 서명(r_key 입력)을 요청한다.

- $Delivery, Request(r\_key)$

9) 서명: 수신자는 TTP에서 전송받은 r_key를 배송자 단말기에 입력한다.

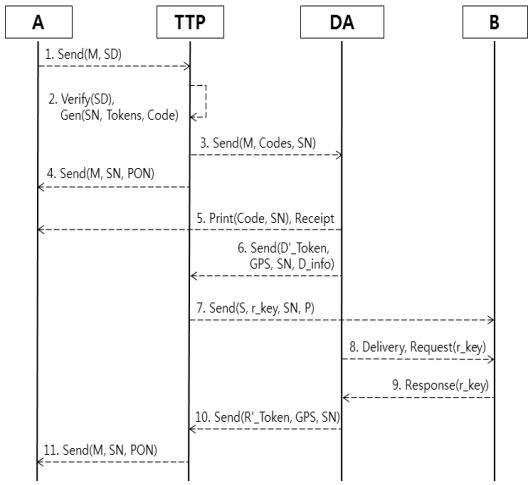
- $Response(r\_key)$

10) 서명 검증 및 완료 통지: 배송자 단말기는 수신자가 입력한 r_key로 S_code를 복호화한 후 R'_token과 SN을 현재 위치정보(GPS_info)와 함께 TTP에 자동으로 전송한다. TTP는 전송받은 SN으로 2) 검증 및 코드 생성에서 생성한 R_token과 전송받은 R'_token을 비교하여 TTP가 생성한 부인방지 토큰인지를 검증한다. 검증 후 배송자는 수신자에게 배송품을 인계한다.

- $P\_info \| SN \| R'\_token = DEC_{r\_key}(S\_code)$
- $Send(R'\_token, GPS, SN)$
- $IF(R\_token = R'\_token) => Success$
  $ELSE => Failure$

11) 배송 완료 통지: TTP는 배송이 완료되었음을 발신자에게 통지한다.

- $Send(M, SN, PON)$



〔그림 4〕 제안 프로토콜

V. 분석

5.1 안전성 분석

본 논문 4.2.2절에서 제시한 보안 요구사항을 바탕으로 안전성을 검토한 결과는 〔표 4〕와 같다.

5.2 효율성 분석

현재 택배 서비스와 논문에서 제안하는 택배 서비스를 발신자, 수신자, 배송기관 및 배송자 관점에서 각각 효율성을 분석한다. 본 절에서 의미하는 효율성은 가용성을 의미한다. 가용성이란, 발신자, 수신자, 배송자가 제안한 택배시스템을 큰 불편 없이 이용할

〔표 4〕 안전성 분석

보안 요구사항	분석 결과
TTP는 안전한 인증과 부인방지에 대한 증거 자료를 수집 및 보관해야 한다.	TTP는 발신자가 서비스 요청 시 발신자 정보, 수신자 정보, 배송자 정보, 물품 정보를 저장하고 각각의 정보를 이용하여 부인방지토큰을 생성 후 부인방지토큰을 포함하는 발신코드와 수신코드를 생성하고, 그 증거 자료를 저장하고 보관하고 있기 때문에 보안 요구사항 1)에 만족한다.
인가되지 않은 제3자는 운송장에서 어떠한 정보도 얻을 수 없어야 한다.	운송장의 발신 코드는 수신자의 일회용 비밀키로 수신 코드는 배송자의 비밀키로 암호화되어 있기 때문에 안전하며, 운송장 정보를 이용한 운송장 조회 시 수신자의 일회용 비밀키가 필요하므로 보안 요구사항 2)에 만족 한다.
서비스 요청 시 운송장 정보에 대해서 무결성 검증과 발신자 인증을 해야 한다.	TTP는 발신자가 서비스 요청 시 발신자의 공개키를 이용하여 공개키 기반 전자서명 검증으로 메시지에 대한 무결성 검증과 발신자 인증이 가능하므로 보안 요구사항 3)에 만족한다.
배송자가 수신자 정보를 요구 시 먼저 배송자를 인증 후 수신자 정보를 제공해야 한다.	배송자는 암호화 및 코드화되어 있는 수신자의 정보를 확인하기 위해서 배송자 비밀키를 입력하여 인증을 수행해야만 수신자 정보를 확인할 수 있으므로 보안 요구사항 4)에 만족한다.
배송품을 수신자에게 인계 시 정확한 수신자인지를 인증해야 한다.	배송자가 배송품을 수신자에게 인계 시 배송자는 수신자의 일회용 비밀키를 요구하며, 수신자는 배송자의 단말기에 TTP에서 생성한 동일한 일회용 비밀키를 입력해야만 배송품 인계가 가능하므로 보안 요구사항 5)에 만족한다.
TTP가 생성하는 어떠한 정보도 제3자가 생성할 수 없어야 한다.	TTP가 생성하는 정보 중 외부로 유출되는 정보는 운송장 정보를 제외하고 모두 암호화되어 있으며, 특히 부인방지토큰은 오로지 TTP의 비밀키로 생성할 수 있으므로 보안 요구사항 6)에 만족한다.
발신자, 수신자, 배송기관이 동일한 경우 생성되는 토큰 및 바코드는 서로 상이해야 한다.	TTP가 부인방지토큰 생성 시 서비스 요청 시간 정보(TD)를 이용하여 토큰을 생성하기 때문에 발신자, 수신자, 배송기관이 동일할 지라도 서비스 요청 시간 정보가 1/1000초라도 다르다면 토큰 및 바코드 정보는 서로 상이하므로 보안 요구사항 7)에 만족한다.
택배 사고 발생 시 배송자는 본인이 업무를 충실히 이행하였음을 입증할 수 있어야 한다.	배송자는 배송자 단말기의 GPS 모듈을 이용해서 배송자가 직접 발신자로부터 배송품 접수 시 위치정보를 TTP에 전송하고 수신자에게 배송품을 인계 시 위치 정보를 TTP에 전송하기 때문에 배송자가 배송에 관한 업무를 충실히 하였음을 입증 할 수 있으므로 보안 요구사항 8)에 만족한다.
발신자는 배송품을 발신한 것에 대한 부인방지가 가능해야 한다.	발신자가 서비스 요청 시 TTP는 요청에 대하여 PKI 기반 전자서명을 발신자에게 요청한다. TTP는 발신자의 전자서명을 검증하고 관련 정보를 저장함으로서 발신부인방지가 가능하며, 이는 보안 요구사항 9)에 만족한다〔20〕.
배송자는 배송품을 전달한 것에 대한 부인방지가 가능해야 한다.	TTP는 배송부인방지 토큰을 생성하여 운송장의 수신코드에 배송기관 비밀키로 암호화 하여 저장 한다. 배송자가 발신자에게 배송품을 접수하게 되면, 배송자는 수신코드를 스캔한다. 이때 배송자의 단말기는 암호화된 수신코드를 배송기관의 비밀키로 복호화 하고 배송부인방지 토큰을 TTP로 전송하여 배송부인방지가 가능하며, 이는 보안 요구사항 10)에 만족한다.
수신자는 배송품을 수신한 것에 대한 부인 방지가 가능해야 한다.	TTP는 수신부인방지 토큰을 생성하여 운송장의 발신코드에 수신자의 일회용 비밀키로 암호화 하여 저장한다. 배송자가 수신자에게 배송품을 인계할 때, 배송자의 단말기로 발신코드를 스캔 하고 수신자에게 일회용 비밀키 입력을 요청한다. 수신자가 일회용 비밀키를 입력하게 되면 배송자의 단말기는 암호화된 발신코드를 복호화 하고 수신부인방지 토큰을 TTP로 전송하여 수신부인방지가 가능하며, 이는 보안 요구사항 11)에 만족한다〔21〕.

수 있는 정도를 의미한다. 안전성이 아무리 높다 하더라도 절차에 시간이 오래 걸려 이용자들이 커다란 불편을 느낀다면, 제안한 택배 시스템은 낮은 가용성으로 인해 이용되지 않을 것이다. 본 논문에서 제안하는 택배 시스템은 기존 택배 시스템과 비교하면 안정성을 크게 향상시켰으며, 분쟁 발생 시, 평균 한 달이 소요되는 피해구제 업무 절차에서 택배사와 고객(발신자와 수신자) 사이에서 책임소재를 분명히 결정할 수 있도록 수집된 증거자료를 바탕으로 시간과 비용을 단축시킬 수 있다. 하지만 추가적인 절차를 요구하기 때문에, 기존 택배 시스템과 비교하면 가용성은 분명히 떨어질 것이다. 본 절에서는 제안한 택배 시스템이 가용성을 떨어뜨린다 할지라도, 그 정도가 작으며, 또한 이용자들(발신자, 수신자, 배송자) 입장에서 정확하고 신속한 분쟁처리가 이루어지기 때문에, 전체적인 가용성은 증가한다는 것을 보여준다.

5.2.1 발신자

발신자는 기존의 택배 서비스에서 인터넷을 통한 택배 신청 서비스와 유사하지만, 서비스 신청 시 발신자의 공인인증서를 이용한 전자서명을 통해서만 신청할 수 있다는 점이 다르다. 발신자는 자신이 직접 발신자 정보와 수신자 정보를 입력한 후에 공인인증서로 전자서명을 함으로써 추후 분쟁 발생 시 증거 자료로 활용하여 원활한 처리가 가능하다.

5.2.2 수신자

수신자는 기존의 택배 서비스와 제안하는 택배 서비스의 가장 큰 차이점은 TTP에서 일회용 비밀키를 수신받고 물품을 수취할 때 비밀키로 수신자 확인을 거쳐야 한다는 점이다. 이는 하나의 절차가 추가됨으로써 기존의 택배 서비스보다 가용성은 떨어질 수 있지만, 배송품 분실 및 오 배송을 예방하는 효율성을 보장한다. 만약 수신자가 부득이한 사정으로 자신이 직접 배송품을 수취하지 못할 경우 대리인에게 일회용 비밀키를 사전에 알려 줌으로서 배송품 위탁이 가능하다. 단, 배송품이 다수일 경우 일일이 일회용 비밀키를 확인하고 입력해야 하는 불편함은 있을 수 있지만 사고 발생 시 수집된 증거자료를 통하여 기존 택배 서비스보다 정확하고 신속하게 피해보상 및 분쟁처리가 가능하다.

5.2.3 배송기관

배송기관은 수신자가 배송품을 수취하였음에도 불구하고 수취하지 않았다고 부인 할 때 명확한 증거자료를 제시할 수 있으며, 제3자가 악의적으로 배송품을 수취하려 해도 수신자의 일회용 비밀키를 알 수 없으므로, 배송품 도난 또는 분실을 예방할 수 있다. 단점으로는 현재의 운송장으로 쉽게 확인이 가능했던 고객의 정보를 단말기를 통해서 수신자 정보 코드를 판독하고 배송기관 또는 배송자의 비밀키를 입력해야만 확인할 수 있다는 점이다. 하지만 배송자가 단말기에 배송기관 또는 배송자의 비밀키를 안전하게 저장하고 있다고 가정을 하게 되면, 수신자 정보 코드를 스캔하였을 때 일일이 비밀키를 입력하지 않아도 배송정보를 확인할 수 있다. 또한, 발신자로부터 택배 물품 접수 시 배송기관의 중앙 서버에서 운송장 번호를 이용해 수신자 정보와 1:1로 매핑 하여 배송자에게 관련 리스트를 제공하고, 배송업무가 끝난 후 안전하게 파기된다면 불편함을 다소 해소 될 수 있다.

VI. 결 론

사회적으로 큰 이슈가 되고 있는 개인정보보호는 온라인상에서는 활발히 그 연구가 진행되고 있지만, 오프라인상에서의 연구는 미흡하다. 오프라인에서 우편이나 택배 운송장의 고객정보를 보호하기 위한 연구와 배송사고 발생 시 택배회사와 고객의 충돌을 최소화하고 신속한 처리를 위해 발신, 수신, 배송에 관한 부인방지 연구가 필요하다.

본 논문은 택배 운송장에서 발신자 정보를 수신자의 일회용 비밀키로 암호화하고 수신자 정보를 배송기관의 비밀키로 암호화하여 고객의 개인정보를 보호하는 방법과 부인방지 서비스제공을 위해 신뢰된 제3의 기관을 제안하였다. 신뢰된 제3의 기관은 부인방지 토큰을 생성하고 저장함으로써, 사고 및 분쟁 발생 시 증거자료를 활용하여 신속한 처리와 피해보상이 가능하다.

참고문헌

〔1〕 KLN, "물류시장 2011/2012 회고와 전망-택배산업," http://www.klnews.co.kr/news/articleView.html?idxno=102910, 2011년 12월.

〔2〕 공정거래위원회 택배 표준약관 제10026호, 2008년

1월.
〔3〕 서울경제, "사고뭉치 택배 믿고 맡기겠나," http://economy.hankooki.com/lpage/industry/201204/e20120409164839120180.htm, 2012년 4월.
〔4〕 아시아투데이, "택배상자의 개인정보, 그들에겐 황금어장," http://www.asiatoday.co.kr/news/view.asp?seq=604808, 2012년 3월.
〔5〕 경제투데이, "버려진 택배박스 통해 개인정보 '술술' 샌다," http://www.eto.co.kr/news/outview.asp?Code=20120119161053640&ts=165010, 2012년 1월.
〔6〕 금융감독원, "2012년 상반기 보이스피싱 피해현황 및 향후 대응방향," 금융감독원 보도자료, 2012년 8월.
〔7〕 아시아투데이, "무심코 버린 택배상자, 부메랑이 되어 날아온다," http://www.asiatoday.co.kr/news/view.asp?seq=604809, 2012년 3월.
〔8〕 이동휘, 최경호, 이동춘, 김귀남, 박상민 "사회공학 기법을 이용한 피싱 공격 분석 및 대응기술," 정보·보안 논문지 6(4), pp. 171-177, 2006년 12월.
〔9〕 서문석, 이병천, 백준상, 김광조, 김상정, 이경구 "부인방지 표준 메커니즘의 분석," 한국정보보호센터, 2010년 8월.
〔10〕 문성철 "미국의 지능형우편 도입 현황 및 시사점," 정보통신정책 20(11), pp. 38-58, 2008년 6월.
〔11〕 개인정보보호법, 법률 제10465호, 2011년 3월.
〔12〕 KLN, "안전한 물품 배송 위해 개인정보보호 수칙 마련," http://www.klnews.co.kr/news/articleView.html?idxno=104805, 2012년 8월.
〔13〕 KLN, "개인정보보호에 둔감했던 택배업계 발등에 불 떨어져," http://www.klnews.co.kr/news/articleView.html?idxno=103889, 2012년 4월.
〔14〕 한국소비자원, "2011년 소비자 택배 피해유형," 한국소비자원 보도자료 2012년 4월.
〔15〕 아시아투데이, "소비자 28.2%, 택배서비스 이용 피해 경험," http://www.asiatoday.co.kr/news/view.asp?seq=566780, 2011년 12월.
〔16〕 보안뉴스, "개인정보 유출 방지 택배운송장 등장," http://www.boannews.com/media/view.asp?idx=14867&kind=1, 2009년 3월.
〔17〕 보안뉴스, "현대택배, 고객 전화번호 암호화," http://www.boannews.com/media/view.asp?idx=14672&kind=1, 2009년 3월.
〔18〕 김석현, 김승현, 진승헌 "개인정보를 암호화한 바코드 운송장," 한국정보처리학회논문집 18(1), pp. 836-839, 2011년 05월.
〔19〕 DENSO Korea SALES CORPORATION, "QRcode manual," in The advantage of QRcode, Ver.1007, 2010.
〔20〕 ISO/IEC FCD 13888-3. Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques, Nov. 2008.
〔21〕 ISO/IEC FCD 13888-2. Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques, Oct. 2009.

〈著者紹介〉

최 민 석 (Min Seok Choi) 학생회원
2009년 8월: 서원대학교 컴퓨터공학과 졸업
2011년 2월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 부인방지, 소프트웨어 공학

조 관 태 (Cho, Kwantae) 학생회원
2005년 2월: 고려대학교 컴퓨터학과(학사)
2005년 3월~2008년 2월: 고려대학교 정보보호대학원(공학석사)
2008년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 WSN 보안, 기기간 보안 통신, 차량간 보안 통신, 키 교환

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과(학사)
1987년 12월: Oklahoma University 전산학 대학원(공학석사)
1992년 5월: Oklahoma University 전산학 대학원(공학박사)
1992년 8월: 단국대학교 전자계산학과 전임강사
1993년 3월 ~ 1997년 2월: 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월: 고려대학교 전산학과 부교수
2001년 2월 ~ 현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술