Journal of Korea Multimedia Society Vol. 18, No. 6, June 2015(pp. 710-722)
http://dx.doi.org/10.9717/kmms.2015.18.6.710

RFID 태그의 소유권 이전 프로토콜을 기반으로 한 위조 방지 메카니즘

이 재 동†

Anti-Counterfeiting Mechanism Based on RFID Tag Ownership Transfer Protocol

Jae-Dong Lee†

ABSTRACT

Counterfeit products have been a major concern in global market. With the emergence of RFID systems, to detect counterfeit products in supply chain is relatively easy. Many anti-counterfeiting techniques for products attached by RFID tag are proposed. Most of the previous anti-counterfeiting techniques are not considering the distribution of the counterfeit from a customer to a customer. Using the ownership transfer protocols we can prevent the counterfeit from being distributed on the supply chain as well as between the customers and the customers. The ownership transfer protocols must be modified for anti-counterfeiting because of the usage of the protocol. In this paper, we modify the ownership transfer protocol proposed by G. Kapoor and S. Piramuthu[1] to be able to detect the counterfeit and track and trace the products in the supply chain. Our proposed protocol consists of three phases: the products delivery phase, the products takeover phase, and the products sale phase. We show that our protocol is anti-counterfeiting as well as secure against the security attacks.

Key words: RFID Security, Ownership Transfer Protocol, Anti-Counterfeiting

1. 서 론

위조품(counterfeit products)은 현재의 상업에서 매우 중요한 위협 중의 하나이다. ICC(International Chamber of Commerce)의 CIB(Counterfeiting Intelligence Bureau)는 위조품이 세계 무역의 5%에서 7%에 이른다고 추산하고 있다[2]. 위조품은 시계, 의복, 의약품 등의 고가의 작은 제품에서부터 자동차, 오토바이, 자전거 등의 고가의 큰 제품에 이르기까지 전 제품에 퍼져 있다. 위조품을 막기 위해 홀로그램, 워터마크, 마이크로 프린팅, 형광잉크 등을 사용하고 있다. RFID(Radio Frequency IDentification) 기술이 발전함에 따라, 제품에 RFID 태그를 부착함으로써 멀리 떨어진 거리에서 제품들을 인식할 수 있고, 공급망(supply chain)에서 제품이 유통되는 경로를 추적할 수 있을 뿐만 아니라 제품의 위조 여부를 파악할 수 있다.

RFID 태그가 부착된 제품들의 위조 방지 및 탐지를 위한 많은 연구가 이루어졌다[3-12]. 이들 연구들을 몇 개의 부류로 분류하면 다음과 같다. 첫째, 유통경로 추적(track and trace)에 기반을 둔 방법이다[3, 4,5,6]. 이 방법에서는 태그가 부착된 제품들이 유통노드(예를 들어, 생산자, 도매상, 소매상 등)를 따라 이동할 때마다 유통노드(distribution node)에 있는

※ Corresponding Author : Jae-Dong Lee, Address: (631-701) Kyungnamdaehak-ro 7, Masanhappo-gu, Changwon-si, Gyeongsangnam-do, Korea, TEL : +82-55-249-2214, FAX : +82-55-248-2554, E-mail : jdlee@kyungnam.ac.kr

Receipt date : Mar. 9, 2015, Revision date : Mar. 26, 2015
Approval date : Apr. 20, 2015

† Dept. of Computer Science and Engineering, Kyungnam University

RFID 리더(reader)에 의하여 엑세스되고 리더는 이 제품들의 위치를 서버에 전달한다. 서버는 각 제품들의 위치와 관련 정보들을 수정한다. 위조된 태그(즉, 제품)는 수상한 사용 패턴(예를 들어, 같은 태그가 다른 두 지역에 존재)을 보일 것이다. 이런 현상을 이용하여 위조품을 찾을 수 있다. 이 방법은 서버와 리더 간의 통신량이 많고 프라이버시(privacy) 문제가 발생한다[7]. 두 번째 방법은 암호화에 기반을 두고 있다[7,8,9]. 모든 태그는 유일한 ID와 비밀키를 가진다. 리더와 태그의 통신에는 비밀키로 생성된 암호화된 메시지가 사용되며, 태그(제품)의 진위 여부는 리더에 의해 이루어진다. 태그가 올바른 비밀키를 가지고 있지 않으면 전송된 메시지를 풀 수 없기 때문에 올바른 응답 메시지를 보내 수 없다. 따라서, 위조된 제품으로 판별하게 된다. 이 방법은 암호화의 방식에 따라 대칭 암호화 기법과 공개키 기반 암호화 기법[7,8,9]으로 나뉠 수 있으며, 리더가 위조를 판별하기 위해 서버의 도움을 받는지 여부에 따라 온라인[9], 오프라인[8], 그리고 준-오프라인(semi-offline) 방식[7]으로 나뉜다. 이 방식의 문제점은 태그가 암호화를 처리할 수 있는 능력을 가져야 함으로 태그의 비용이 비싸진다. 또한, 공급망 관리(예를 들어, 유통 경로 추적 등)를 위해서는 별도의 메카니즘이 필요하다. 세 번째 방법은 공급망에서의 올바른 유통 경로에 기반을 둔 방법이다[10,11]. 공급망에서 제품이 유통노드를 거칠 때, 태그에는 거쳐간 유통노드 관련 정보가 저장된다. 리더에는 공급망에서의 모든 올바른 유통노드의 경로들이 미리 저장되어 있다. 리더가 태그에 저장된 거쳐온 유통노드의 정보를 엑세스하여 올바른 경로를 거쳐온 제품은 진품으로, 그렇지 않은 제품은 위조품으로 판별한다. 이 방법의 가장 큰 문제점은 각 제품이 거쳐야 될 올바른 경로를 사전에 설정하여 리더에게 제공해야 하는 점이다. 유통노드가 바뀌면 다시 모든 올바른 경로를 재설정해야 한다. 네 번째 방법은 태그의 소유권 이전 프로토콜(ownership transfer protocol)을 이용한 것이다. 유통노드 간에 태그의 소유권을 안전하게 이전할 수 있으면 위조품이 소비자에게 전달될 수 없음을 기반으로 한 방법이다. 이런 연구는 C.L. Chen 등이 공개키 기반으로 제안하였다[12]. 하지만, C.L. Chen 등이 제안한 프로토콜은 소유권 이전 과정에서 태그 ID, 전자서명 등의 정보가 노출되어 위조된 태그를 만들 수 있는 보안상의 문제점이 노출되었으며, 또한, 이 프로토콜은 소매상과 소비자 간의 소유권 이전만을 다루고 있다.

위에서 언급한 네 그룹의 위조 방지 및 탐지 방법들을 위조품의 유통 범위 측면에서 분석하면, 첫 번째와 세 번째 그룹의 방법들은 유통망 내에서만 위조품이 유통되지 않도록 하는 반면, 두 번째 그룹은 소비자가 제품을 구입할 시에만 위조품을 판별토록 한다. 네 번째 방법은 소매상과 소비자 간에 제품이 전달될 때 위조품인지를 판별한다.

본 논문에서는 유통망 내에서 뿐만 아니라 소비자와 소비자 간의 제품 전달 과정에서도 위조품이 유통되지 못하게 하려고 한다. 이를 위해서, 공장에서부터 제품의 최종 소비자에게 전달되는 과정마다, 즉, 제품의 소유권이 이전되는 과정마다 진품이 전달될 수 있도록 하기 위해 RFID 태그의 소유권 이전 프로토콜을 사용할 수 있다. 소유권 이전 프로토콜은 태그가 부착된 제품을 현 소유주에서 새 소유주에게로 안전하게 제품을 이전할 수 있는 프로토콜이다. 이 프로토콜을 이용하면 유통노드에서 유통노드로 진품을 안전하게 유통시킬 수 있으며, 소비자가 가진 제품을 다른 소비자에게 이전할 때도 진품 여부를 판단하여 안전하게 이전할 수 있다. 소유권 이전 프로토콜에 대한 많은 연구가 진행되었다[1,12-18]. 기존의 프로토콜들은 공개키 암호화를 사용하는 방법[12], 대칭키를 사용하는 방법[1,13,14,17], 그리고 해시함수를 사용하는 방법[15,16,18] 등이 있다. 이 프로토콜들은 소유권 이전을 위해 현 소유주와 새 소유주가 한 곳에서 동시에 태그를 접근하여 소유권 이전이 이루어진다. 공급망에서 제품이 유통되는 과정은 제품을 인도할 유통노드와 제품을 인수할 유통노드가 대부분 멀리 떨어져 있어 한 장소에서 동시에 태그를 접근하여 제품을 인도 및 인수할 수 없다. 즉, 소유권 이전 프로토콜을 그대로 공급망에 사용할 수 없다. 이와 같은 특성 때문에 소유권 이전 프로토콜을 위조 방지를 위해 공급망에 사용하기 위해서는 수정이 필요하다. 본 논문에서는 대칭키 암호화를 사용한 비교적 간단한 G. Kapoor와 S. Piramuthu가 제안한 소유권 이전 프로토콜[1]을 공급망에서 제품의 유통 경로 추적과 위조 방지를 할 수 있도록 수정하였다. 우리가 제시한 프로토콜은 크게 3개의 단계로 이루어진다. 제품을 인도하는 유통노드에서 수행

되는 제품 인도 단계, 제품을 인수할 유통노드에서 수행될 제품 인수 단계, 그리고 소매점에서 소비자에게 제품을 판매할 때 수행되는 제품 판매 단계이다. 이 프로토콜은 위조 방지를 비롯한 여러 보안 공격에 안전함을 보였다. 다른 여러 소유권 이전 프로토콜들도 우리가 수정한 방식과 유사하게 수정함으로써 위조 방지를 위해 활용할 수 있다.

본 논문의 기여(contribution)는 다음과 같이 정리할 수 있다. 첫째, 공급망 내에서 뿐만 아니라 소비자와 소비자 간에도 유통되는 제품의 유통 경로 추적과 위조 방지를 할 수 있는 보안 공격에 안전한 프로토콜을 제시하였다. 둘째, 태그의 능력에 맞는 기존 소유권 이전 프로토콜을 공급망에서의 위조 방지 프로토콜로 수정하는 방법을 보였다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 위조 방지 프로토콜을 기술하기 위한 표기법과 보안 요구 조건을 기술하고, 3장에서는 위조 방지 프로토콜을 제시하고, 4장에서는 제시한 프로토콜이 보안 공격에 안전함을 보인다. 5장에서는 결론과 향후연구에 대한 방향을 제시한다.

2. 표기법 및 보안 요구 조건

본 절에서는 공급망(supply chain), 표기법 및 가정, 보안 요구 조건 등을 기술한다.

2.1 표기법 및 가정

제품은 Fig. 1처럼 생산공장에서 생산되어 물류창고을 거쳐 여러 도매상에 보급되고, 여러 도매상을 거쳐 소매상에 전달되어 소비자에게 판매된다. 이런 물류의 흐름 속에 배송을 담당하는 배송업자도 포함될 수 있다. 제품의 성질에 따라 생산공장에서 물류창고, 도매상, 소매상을 거쳐 소비자에게 판매되는 유통구조를 가질 수도 있고, 생산공장에서 1개 이상의 물류창고와 1개 이상의 도매상을 거쳐 소매상에서 소비자에게 판매되는 유통구조를 가질 수도 있으며, 또한 제품이 생산공장, 물류창고, 도매상 및 소매상으로 전달되는 과정에 배송업자가 관여할 수도 있다. 본 논문에서는 생산 공장, 물류 창고, 배송업자, 도매상, 소매상 등을 '유통노드' 라고 부른다.

생산되는 모든 제품에는 RFID 태그가 부착되어 있으며, 각 유통노드에 RFID 리더를 두어 태그들을 엑세스한다. 또한, RFID 태그와 리더에 대한 모든 정보를 저장하고 유통과정에서 소유권 이전 및 진품 판정을 위해 리더와 통신하는 서버(또는 TTP (Trusted Third Party Server))를 둔다. 대부분의 RFID 시스템처럼 태그와의 통신은 리더를 통해서 이루어지므로 서버와 태그 간의 통신 시, 서버는 리더를 통해 태그와 통신한다. 또한, 리더와 서버 사이의 통신은 안전한 통신 채널을 사용하고 태그와 리더 사이의 통신은 노출된(안전하지 않는) 것으로 가정한다. 그리고, 태그와 리더 사이의 통신을 위해서는 상호 인증이 이루어져야 한다.

본 논문에서 제시하는 프로토콜을 위한 표기법은 Table 1과 같다.

2.2 보안 요구 조건

제품에 부착된 RFID 태그에는 소유자 정보 및 접근 제어를 위한 데이터가 저장되어 있으므로 공급망에서 위조 방지를 위해 아래의 보안 및 프라이버시 요구사항을 만족시켜야 한다.

- 새 소유자 프라이버시(New owner privacy): 태그의 소유권이 새 유통노드에게로 이전 되었을 때, 단지 새 유통노드만이 태그를 식별하고 태그 내의 정보를 접근할 수 있다. 이전 유통노드는 그 태그에 대해 더 이상 접근할 수 없다.
- 전 소유자 프라이버시(Old owner privacy): 태그의 소유권이 새 유통노드에게 이전되었을 때, 새 유통노드는 전 유통노드와 태그 사이의 과거 활동을 추적할 수 없다.

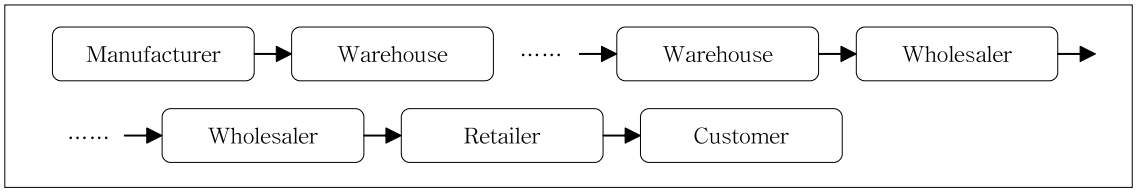

Fig. 1. The supply chain.

Table 1. The meaning of the notation

Notation	Meaning
R_O	RFID reader of the distribution node O
Tag_i	ith RFID tag(i is the product number or EPC)
r_O	shared secret key between reader R_O and server
t_i	shared secret key between tag Tag_i and server
c_u	shared secret key between customer c and server
s	secret key
f_k	keyed(with key k) encryption function
N_J	random nonce generated by J
H_k	keyed(with key k) hash fuction
h	hash function
$\oplus$	exclusive OR
$\|\|$	concatenation

• 권한 복구(Authorization recovery): RFID 태그가 붙은 제품에 대한 반품 또는 애프터 서비스(after-sales service)와 같은 상황에서, 현재의 유통노드는 전 유통노드가 태그 내의 정보를 접근할 권한을 잠시 동안 가지도록 태그의 소유권을 잠시 이전할 필요가 있다.

• 서비스 거부 공격에 안전(Resistance to Denial of Service (DoS) attack): DoS 공격 을 막기 위해서 태그와 서버가 공유하고 있는 비밀정보에 대한 동기화 메커니즘이 요구된다.

• 재생 공격에 안전(Resistance to replay attack): 공격자가 리더와 태그 사이의 통신 메시지를 도청하여 리더나 태그를 속이기 위해 도청한 메시지를 사용할 수 없도록 한다.

• 중간자 공격에 안전(Resistance to man-in-middle attack): 공격자가 태그와 리더 사이에서 가짜 메시지 또는 수정한 메시지를 사용하여 원하는 일을 할 수 없도록 한다.

• 위조 방지(Anti-Counterfeiting): 공급망에 위조된 태그를 부착한 제품이 유통되지 않도록 해야 한다.

3. 공급망에서의 위조 방지 프로토콜

3.1 초기단계

서버에는 Table 2와 같은 4개의 테이블이 필요하다. 태그 테이블(Tag Table)에는 태그번호(tag number, i), 공유 비밀키(shared secret key, t_i), 비밀키(secret key, s), 새 비밀키(new secret key, s'), 제품의 소유 유통노드(distribution node의 owner 필드),

Table 2. Tables in server

(a) Tag Table

tag number	shared secret key	secret key	new secret key	distribution node		others info.
				owner	delivery	

(b) Reader Table

reader	shared secret key	distribution node	others info.

(c) Customer Table

user name	password	shared secret key	others info.

(d) Distribution Node Table

distribution node	related information

제품이 다른 유통노드로 전달 중이면 전달될 유통노드(distribution node의 delivery 필드) 및 기타 정보로 구성된다. 리더 테이블(Reader Table)에는 리더(reader, R_O), 서버와 리더 간에 공유하는 비밀키(shared secret key, r_O), 이 리더를 소유하고 있는 유통노드(distribution node) 및 기타 필요한 정보가 저장 된다. 소비자 테이블(Customer Table)에는 소비자가 물건을 구입할 때 본인이 직접 진품임을 확인하기 위해 사용자명(user name), *password*, 공유 비밀키(shared secret key) 및 필요한 정보가 저장된다. 유통노드 테이블(Distribution Node Table)은 모든 유통노드에 대한 정보가 저장된다.

제품이 생산되면 제품에 부착되는 태그에는 제품번호(i), 서버와 공유하는 공유 비밀키(t_i)와 비밀키(s)를 생성하여 저장하고, 서버의 태그 테이블에 저장한다. 태그 테이블의 owner 필드를 생산공장으로 설정한다. 또한, 서버는 제품의 비밀키를 생산공장의 리더에게 전송하여 생산공장의 리더가 태그를 접근할 수 있도록 한다. 다른 유통노드의 리더는 제품의 인도/인수 과정에서 비밀키를 획득하여 태그를 접근한다.

리더가 태그에 접근하기 위해 리더와 태그 간의 상호인증이 필요하다. 본 연구에서는 G. Kapoor와 S. Piramuthu가 제시한 Fig. 2의 프로토콜[1]을 사용한다.

리더 R_O와 Tag_i는 비밀키 s를 가지고 있다. 상호인증 과정은 다음과 같다.

(1) 리더가 난수 N_{R_O}를 생성하여 Tag_i에게 인증을 요구한다.

(2) Tag_i는 난수 N_T를 생성하여 리더로부터 받은 난수 N_{R_O}를 $(N_T \oplus s)$를 키로 사용하여 해시값을 만들어 전송한다.

(3) 리더는 자신의 비밀키 s를 사용하여 해시값을 구하여 비교한다. 같으면 태그를 인증한다. 그리고, 새로운 난수 N_{R_O}'를 생성하고, $(N_T \oplus s)$를 키로 사용하여 $(N_{R_O}' \oplus s)$를 암호화한 메시지를 전송한다. 여기서, op는 필요한 연산(읽기, 쓰기, 갱신 등)을 나타낸다.

(4) 이 메시지를 받은 태그는 자신이 가지고 있는 비밀키(s)를 이용하여 이 메시지를 해독 하여 리더를 인증한다. 마지막으로 ACK 메시지로 $H_s(N_{R_O}')$ 를 전송한다.

태그의 비밀키가 2개인 경우(비밀키 s와 새 비밀키 s'), 리더와 태그의 상호 인증 시 어떤 비밀키를 사용하더라도 태그의 접근이 가능하다. 이런 상황은 다음에 설명하는 위조 방지 프로토콜에서 자주 발생한다.

3.2 제품 인도 단계

R_O 리더를 가진 유통노드에서 R_d 리더를 가진 유통노드로 제품을 전달한다고 하자(본 논문에서는 유통노드의 이름 대신 그 노드의 리더명을 사용한다. 이 리더명이 전달되면 서버가 유통노드를 알 수 있으므로 리더명과 유통노드는 같은 의미를 나타낸다.). 제품을 전달하기 위해 두 단계를 거친다. 먼저, 제품을 인도하는 유통노드에서 처리되는 제품 인도 단계와 제품을 인수하는 유통노드에서 처리되는 제품 인수 단계이다. 제품 인도 단계는 Fig. 3의 과정을 거친다.

제품인도 단계는 Fig. 3과 같이 아래의 단계로 처리된다.

(1) 제품을 인도할 유통노드의 리더가 물품인도요구(*Delivery Request*)메시지를 서버로 전송한다.

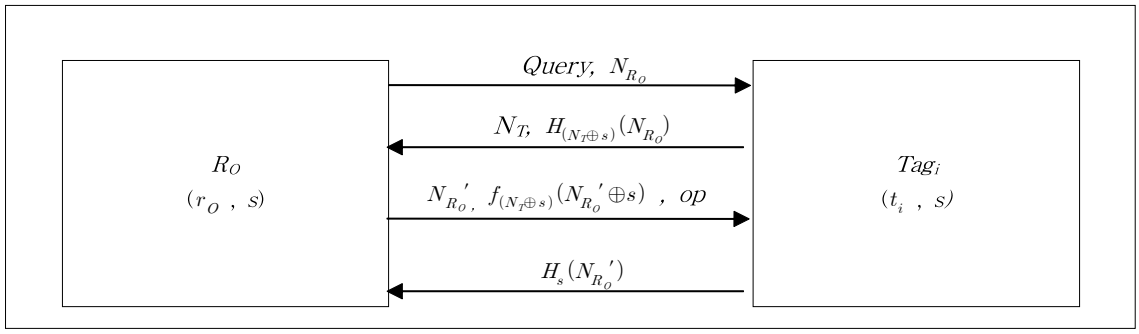

Fig. 2. The authentication protocol.

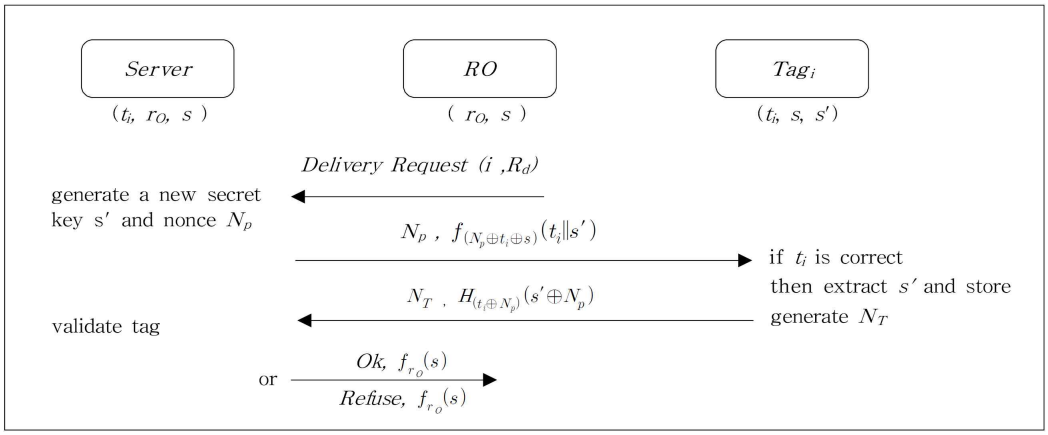

Fig. 3. The products delivery phase.

이 메시지에는 태그번호(i)와 전달될 유통노드(R_d)가 포함되어 있다. 태그번호는 앞에서 언급 한 리더와 태그의 상호인증을 통해 리더가 태그로부터 읽은 값이다.

(2) 요구를 받은 서버는 새로운 키 s′와 난수 N_p를 생성한 후, ($t_i||s'$)를 ($N_p \oplus t_i \oplus s$)로 암호화한 값과 N_p를 Tag_i로 전송한다.

(3) 태그는 t_i가 올바르면 s를 추출하여 저장한 후, 난수 N_T를 생성하여 N_T와 해시값 $H_{(t_i \oplus N_T)}(s' \oplus N_p)$를 서버로 전송한다. t_i가 틀린 값이면 무시한다.

(4) 서버는 전송된 해시값을 확인 후, 올바른 값이면 태그를 인증하고 리더(R_O)에게 제품 인도를 허락하는 메시지 (Ok, $f_{r_O}(s)$)를 전송한다. 만약 잘못된 값이거나 정해진 시간 내에 메시지를 받지 못하면 (2)번 작업, 즉, (N_p, $f_{(N_p \oplus t_i \oplus s)}(t_i||s')$)메시지를 재전송한다. 정해진 횟수만큼 재전송 후에도 잘못된 값이거나 메시지를 받지 못하면 R_O에게 제품 인도 거절 메시지 ($Refuse$, $f_{r_O}(s)$)를 보낸다.

(5) R_O는 허락 메시지를 받으면 제품을 R_d 유통노드로 배송한다. 만약, 거절 메시지를 받으면 2가지 경우를 고려해야 된다. 먼저, 통신상의 문제, 즉, 통신상태 불량 또는 침입자의 공격(DoS 공격 등)이고, 두 번째는 제품의 진위문제이다. R_O는 첫 번째 문제를 해결한 후, 제품 인도 단계를 다시 요청한다. 정해진 횟수만큼의 반복 요청에도 불구하고 계속 거절되면 제품이 위조된 것으로 판단하여 반송처리 한다.

서버는 제품 인도 단계가 성공적으로 수행되면 태그 테이블의 새 비밀번호 필드에 s′, 유통노드의 delivery 필드에 R_d를 저장한다.

3.3 제품 인수 단계

제품이 R_d로 전달되면 유통노드 R_d에서 제품 인수 단계를 수행한다. 제품 인수 단계는 Fig. 4와 같이 아래의 단계로 처리된다.

(1) 제품을 인수할 유통노드의 리더 R_d가 서버에게 인수요청($TakeOver\ Request$)메시지 를 보낸다.

(2) 서버는 R_d로 인도될 제품의 태그를 태그 테이블의 유통노드의 delivery 필드를 통해 찾는다. 찾은 태그의 비밀키(s')을 R_d로 전달하기 위해 난수 N_P'을 생성하고 (N_P', $f_{(r_d \oplus N_P')}(s' \oplus r_d)$) 메시지를 R_d로 전송한다.

(3) R_d는 비밀키(s')을 추출하여 태그를 액세스하기 위해 난수 NR_d를 생성한다.

(4) 태그의 소유주를 R_d로 바꾸기 위해 (N_{R_d}, $f_{s'}(N_{R_d})$) 메시지를 태그로 전송한다. 태그는 암호화된 N_{R_d}를 풀어 보내온 N_{R_d}와 일치하면 비밀키(s)를 s'으로 변경한다. 즉, 이 태그 의 소유주를 비밀키(s')를 알고 있는 R_d로 변경한다. 만약 값이 일치하지 않으면 아무런 작업도 않는다.

(5) 값이 일치하여 s를 변경시킨 후, R_d에 응답메시지 (N_T', $H_{(N_T' \oplus s')}(N_{R_d} \oplus s')$)를 전송한다.

(6) R_d는 응답 메시지의 해시값을 계산하여 일치하면 태그의 비밀키 s를 새 비밀키 s'으로 설정한 후, 제품 인수가 완료되었음을 서버에게 (Ok, $H_{r_d}(s' \oplus N_p')$) 메시지로 알린다. 서버는 제품 인수가 완료됨에 따른

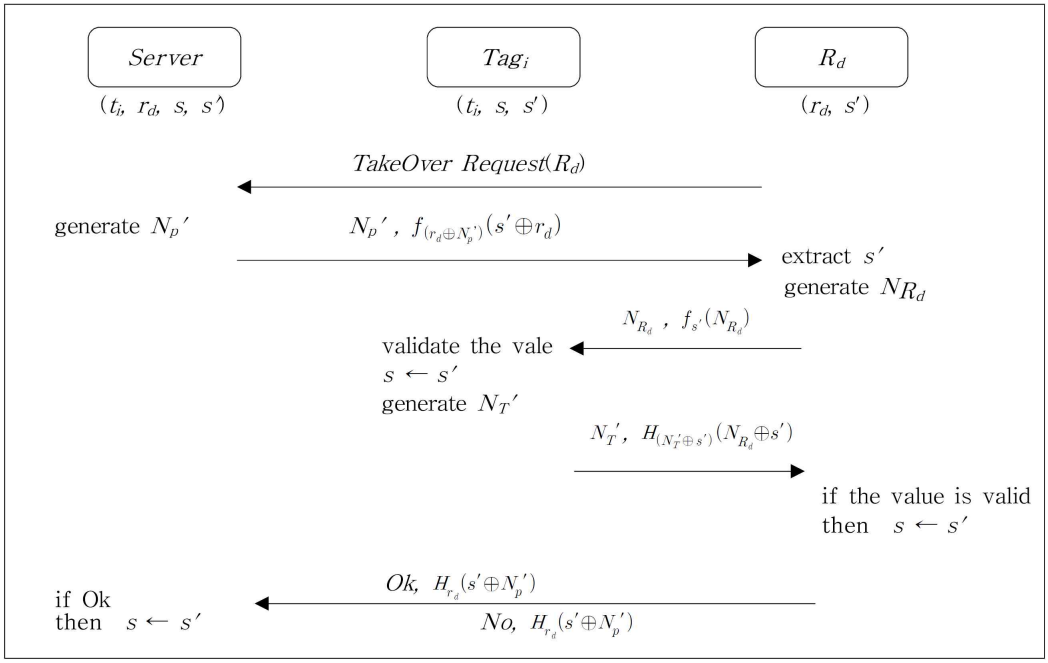

Fig. 4. The products takeover phase.

테이블 수정 작업을 한다. 예를 들어, 비밀키 s를 s'으로 바꾸고, 태그의 owner 필드를 수정한다. 만약, R_d가 받은 응답메시지의 해시값이 일치하지 않거나, 정해진 시간 내에 응답 메시지가 오지 않으면 (4)번 작업 (즉, $(N_{R_d},\ f_s'(N_{R_d}))$ 메시지 전송)을 다시 한다. 정해진 횟수만큼 반복해도 올바른 응답메시지가 오지 않으면 2가지 경우를 고려해야 한다. 첫째, 통신상의 문제, 즉, 통신 상태 불량 또는 침입자의 공격(DoS 공격 등)이고, 두 번째는 제품의 진위 문제이다. R_d는 첫 번째 문제를 해결한 후, 다시 (4)번 작업을 요청한다. 정해진 횟수만큼 반복해도 올바른 메시지를 받지 못하면 제품이 위조된 것으로 판단하고 서버에게 인수거절을 나타내는 메시지 $(No,\ H_{r_d}(s' \oplus N_p'))$을 전송한다. 서버는 제품이 위조된 것으로 판단하여 반품처리토록 한다.

R_d가 인수할 제품이 n개이면, (2)번 작업에서 서버에서 R_d로 보내는 메시지 $(N_P',\ f_{(r_d \oplus N_p')}(s' \oplus r_d))$ 대신에 $(N_P',\ f_{(r_d \oplus N_p')}((s_1' \oplus r_d) \| (s_2' \oplus r_d) \| \cdots \| (s_n' \oplus r_d)))$ 메시지를 전송하면 R_d는 n개의 비밀키를 추출하여 각각 제품의 인수 작업을 처리 할 수 있다.

3.4 제품 판매 단계

제품들은 여러 유통노드를 거쳐 소매점에 도착한다. 각 유통노드를 거칠 때 마다 3.2절과 3.3절의 제품 인도와 인수 과정을 거치게 된다. 이렇게 전달된 제품이 소매점에서 소비자에게 판매된다. 소비자가 제품을 구매할 때 제품이 진품인지 확인해야 하며, 제품을 구입한 후 제품에 대한 소유권을 가져야 한다. 이를 위한 제품 판매 단계는 앞에서 설명한 제품 인도 과정과 인수 과정을 적절히 조합한 구조로 Fig. 5와 같이 아래의 단계로 처리된다.

(1) 제품을 구입할 소비자는 자신을 서버에 등록한다. 이 때, 사용자명과 *password*가 제공되고, 이 *password*를 사용하여 서버와 소비자가 공유할 비밀키 c_u를 해시함수 *h(password)*로 구한 다. 사용자명, *password*와 공유 비밀키를 소비자 테이블에 저장한다.

(2) 소매상(소매상의 리더)은 제품 판매 요청(*Sale Request*)메시지를 서버로 전송한다. 이 메시지에는 태그번호(i)와 소매상(R_l)이 포함되어 있다.

(3) 요구를 받은 서버는 새로운 키 s′와 난수 N_p를 생성한 후, $(t_i \| s')$를 $(N_p \oplus t_i \oplus s)$로 암호화한 값과 N_p를 Tag_i로 전송한다.

(4) 태그는 t_i가 올바르면 s를 추출하여 저장한 후, 난수 N_T를 생성하여 N_T와 해시값 $H_{(t_i \oplus N_T)}(s' \oplus N_p)$를 서버로 전송한다. t_i가 틀린 값이면 무시한다.

(5) 서버는 전송된 해시값을 확인 후, 올바른 값이면 태그를 인증하고 소비자에게 태그의 비밀키(s')을 전달하기 위해 난수 N_P'을 생성하고 (N_P', $f_{(c_u \oplus N_p')}(s' \oplus c_u)$) 메시지를 전송 한다. 만약 잘못된 값이거나 정해진 시간 내에 메시지를 받지 못하면 (3)번 작업, 즉, (N_p, $f_{(N_p \oplus t_i \oplus s)}(t_i \| s')$)메시지를 재전송한다. 정해진 횟수만큼 재전송 후에도 잘못된 값이거나 메시지를 받지 못하면 2가지 경우를 고려해야 된다. 먼저, 통신상의 문제, 즉, 통신상태 불량 또는 침입자의 공격(DoS 공격 등)이고, 두 번째는 제품의 진위문제이다. 소매상은 첫 번째 문제를 해결한 후, (2)번 단계, 즉, 제품판매요청을 다시 요청한다. 정해진 횟수만큼의 반복 요청에도 불구하고 계속 거절되면 제품이 위조된 것으로 판단하여 반송처리토록 한다.

(6) 소비자는 (N_P', $f_{(c_u \oplus N_p')}(s' \oplus c_u)$) 메시지로부터 비밀키($s'$)을 추출하여 태그를 액세스 하기 위해 난수 N_C를 생성한다.

(7) 태그의 소유주를 소비자로 바꾸기 위해 (N_C, $f_{s'}(N_C)$) 메시지를 태그로 전송한다. 태 그는 암호화된 N_C를 풀어 보내온 N_C와 일치하면 비밀키(s)를 s'으로 변경한다. 즉, 이 태그의 소유주를 비밀키(s')를 알고 있는 소비자로 변경한다. 만약 값이 일치하지 않으면 아무런 작업도 않는다.

(8) 값이 일치하면, 태그는 s를 변경시킨 후, 소비자에게 응답메시지(N_T', $H_{(N_T' \oplus s')}(N_C \oplus s')$) 를 전송한다.

(9) 소비자는 응답 메시지의 해시값을 계산하여 일치하면 태그의 비밀키 s를 새 비밀키 s'으로 설정한 후, 제품 구입이 완료되었음을 서버에게 (Ok, $H_{c_u}(s' \oplus N_p')$)메시지로 알린다. 서버는 제품 판매가 완료됨에 따른 테이블 수정작업을 한다. 예를 들어, 비밀키 s를 s'으로 바꾸고, 태그의 owner 필드를 사용자명으로 수정한다. 만약, 소비자가 받은 응답메시지의 해시값이 일치하지 않거나, 정해진 시간 내에 응답 메시지가 오지 않으면 (7)번 작업, 즉, (N_C, $f_{s'}(N_C)$) 메시지 전송을 다시 한다. 정해진 횟수만큼 반복해도 올바른 응답메시지가 오지 않으면 2가지 경우를 고려해야 한다. 첫째, 통신상의 문제, 즉 통신 상태 불량 또는 침입자의 공격(DoS 공격 등)이고, 두 번째는 제품의 진위 문제이다. 소비자는 첫 번째 문제를 해결한 후, 다시 (7)번 작업을 다시 요청한다. 정해진 횟수만큼 반복해도 올바른 메시지를 받지 못하면 제품이 위조된 것으로 판단하고 서버에게 위조를 알리기 위한 메시지 (NO, $H_{c_u}(s' \oplus N_p')$)을 전송한다. 서버는 제품이 위조된 것으로 판단하여 반품처리토록 한다.

3.5 소비자 간의 소유권 이전

소비자에게서 다른 소비자로 소유권 이전이 필요할 때, 제품의 진품 여부 확인과 제품(즉, 태그)의 소유권 이전 작업이 필요하다. 이를 위해, 두 소비자는 서버에 등록을 해야 한다. 이전할 소비자를 U_1, 이전받을 소비자를 U_2라 하자. 소유권 이전 작업은 두 소비자가 같은 장소에 있는 경우와 멀리 떨어진 장소에 있는 경우에 따라 다른 방법을 사용한다. 같은 장소에 있는 경우는 Fig. 5의 제품 판매 단계와 같은 방법으로, 멀리 떨어진 경우는 Fig. 3의 제품 인도 작업과 Fig. 4의 제품 인수 작업과 같은 방법으로 이루어진다.

먼저, 같은 장소에 있는 경우는 제품 판매 단계에서 소매상 대신 U_1로, 소비자 대신 U_2로 설정한다. U_1과 서버의 공유키는 c_{u_1}로, 비밀키는 s로 하고, U_2와 서버의 공유키는 c_{u_2}로 하여 U_1이 서버에 소유권 이전 요구를 함으로써 이루어진다. 이후의 과정은 제품 판매 단계와 같다.

두 소비자가 멀리 떨어진 경우는 제품 인도 단계에서 R_O 대신 U_1로 하고, U_1과 서버의 공유키는 c_{u_1}로, 비밀키는 s로 하여 U_1이 서버에게 소유권 이전 요구를 한다. 이후의 과정은 제품 인도 단계와 같다. 제품이 U_2에게 도착하면 U_2는 소유권을 이전을 받기 위해 제품 인수 단계에서 R_d 대신 U_2로, U_2와 서버의 공유키는 c_{u_2}로 하여 U_2가 서버에게 소유권 인수 요구를 한다. 이후의 과정은 제품 인수 단계와 같다.

이렇게 두 소비자 간의 소유권을 이전하기 위해서는 소비자는 서버가 인증하는 RFID 리더가 있는 곳(예를 들어, 소매점)으로 가서 소유권 이전 작업을 해야 한다. 이는 태그와의 통신 시, 서버가 인증하는 리더와 통신을 해야 올바른 작업을 수행할 수 있기 때문이다. RFID 태그 대신 NFC 태그를 사용한다면 사용자의 스마트폰에서 작업이 가능하다.

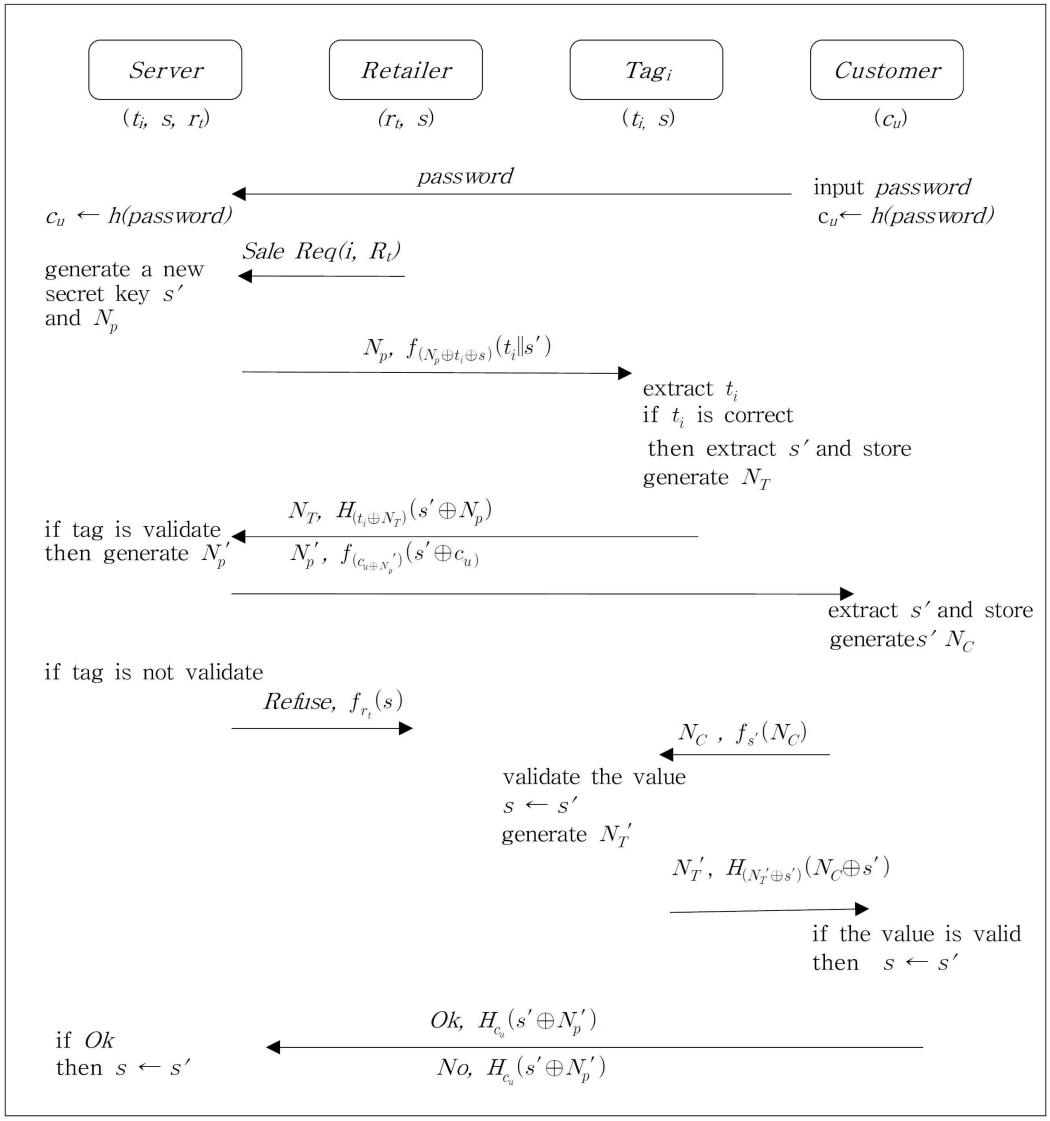

Fig. 5. The products sale phase.

4. 보안 요구 조건 분석

본 장에서는 3장에서 제안한 위조 방지 프로토콜이 2.2절에서 기술한 보안 요구 조건을 만족하는지를 분석하고 이 프로토콜과 관련된 기타사항들을 언급한다.

4.1 보안 요구 조건 분석

3.1절에서 언급한 상호 인증 프로토콜은 보안에 안전하다[1]. 여기서는 우리가 제시한 위조 방지 프로토콜에 대한 보안 분석만 한다.

• 새 소유주 프라이버시(New owner privacy): 제품 인도 단계에서 제품을 인도할 유통노드가 서버에게 제품 인도 요구를 하면 새 비밀키 s'를 생성하여 Tag_i에게 전송한다. 이 새 비밀키는 제품을 인도할 유통노드는 알 수 없다. 제품이 인도되어 제품 인수 단계에서 제품을 인수할 유통노드는 인수요청을 서버에게 요구한다. 서버는 이전에 생성해 둔 비밀키 s'를 제품을 인수할 유통노드에게 보내고, 서버와 Tag_i의 비밀키를 s'으로 설정한다. 이렇게 함으로서

제품을 인도한 유통노드는 더 이상 Tag_i를 접근할 수 없고, 인수한 유통노드만이 Tag_i를 접근할 수 있다. 제품 판매 단계에서도 마찬가지로 소매상이 소비자에게 물건을 판매할 때, Tag_i의 비밀키를 새 비밀키로 변경함으로서 소매상은 더 이상 Tag_i에 접근할 수 없고 단지 소비자만이 Tag_i에 접근할 수 있다. 그러므로 새 소유주 프라이버시가 보호된다.

• 전 소유주 프라이버시(Old owner privacy): 제품을 인수할 유통노드(또는 소비자)는 서버로부터 변경된 비밀키 s'만을 받는다. 따라서, 제품을 인수한 유통노드(또는 소비자)는 제품을 인도한 유통노드와 Tag_i 사이의 트랜잭션들을 추적할 수 없기 때문에 제품을 인도한 유통노드의 프라이버시를 보호할 수 있다.

• 권한 복구(Authorization recovery): 제품을 인도한 유통노드에게 권한을 복구시키기 위해 다음과 같은 절차로 처리 가능하다. 먼저, 제품을 인수한 유통노드(또는 소비자)가 서버에게 권한 복구 요청을 한다. 서버는 제품을 인도한 유통노드에게 태그를 접근할 수 있는 비밀키(s)를 전송한다. 제품을 인도한 유통노드는 이 비밀키로 태그를 접근할 수 있다. 사용이 끝나면, 제품을 인도한 유통노드는 서버에게 사용이 끝났음을 알린 후, 3장에서 제시한 제품 인도 단계와 제품 인수 단계(또는 제품 판매 단계)를 사용하여 소유권을 기존의 유통노드(또는 소비자)에게 넘길 수 있다.

• 서비스 거부 공격에 안전(Resistance to Denial of Service (DoS) attack): 제품 인도 작업, 제품 인수 작업 및 제품 판매 단계에서 DoS공격이 가능하다. 먼저, 제품 인도 작업에서의 공격을 알아보자. 이 단계에서의 공격은 두 가지가 있을 수 있다. 첫째, 서버에서 Tag_i로 전송되는 메시지 $(N_p,\ f_{(N_p \oplus t_i \oplus s)}(t_i \| s'))$의 전송이 이루어지지 않도록 하는 공격과 둘째, Tag_i에서 서버로 전송되는 메시지$(N_T,\ H_{(t_i \oplus N_p)}(s' \oplus N_p))$의 전송이 이루어지지 않도록 하는 공격이다. 3.2절의 제품 인도 단계 (4)와 (5)에서 언급했듯이 서버는 정해진 시간 내에 메시지를 받지 못하면 (2)번 작업, 즉, $(N_p,\ f_{(N_p \oplus t_i \oplus s)}(t_i \| s'))$메시지를 재전송한다. 정해진 횟수만큼 재전송 후에도 메시지를 받지 못하면 R_O에게 제품 인도 거절 메시지를 보낸다. R_O가 거절 메시지를 받으면 통신상의 문제, 즉, 통신상태 불량 또는 침입자의 공격(DoS 공격 등)을 해결한 후, 제품 인도 단계를 다시 요청한다. 정해진 횟수 만큼의 반복 요청에도 불구하고 계속 거절되면 제품이 위조된 것으로 판단하여 반송처리토록 한다. 다음으로, 제품 인수 작업에서의 공격을 알아보자. 이 단계에서의 공격 역시 두 가지가 있을 수 있다. 첫째, R_d에서 Tag_i에 전송되는 메시지 $(N_{R_d},\ f_{s'}(N_{R_d}))$의 전송이 이루어지지 않도록 하는 공격과 둘째, Tag_i에서 R_d로 전송되는 메시지 $(N_T',\ H_{(N_T' \oplus s')}(N_{R_d} \oplus s'))$의 전송이 이루어지지 않도록 하는 공격이다. 3.3절의 제품 인수 단계 (6)에서 언급했듯이, R_d는 정해진 시간 내에 응답 메시지가 오지 않으면 (4)번 작업 (즉, $(N_{R_d},\ f_s'(N_{R_d}))$ 메시지 전송)을 다시 한다. 정해진 횟수만큼 반복해도 올바른 응답메시지가 오지 않으면 통신 상태 불량 또는 침입자의 공격(DoS 공격 등)을 해결한 후, 다시 (4)번 작업을 요청한다. 정해진 횟수만큼 반복해도 올바른 메시지를 받지 못하면 제품이 위조된 것으로 판단하고 서버에게 인수거절을 나타내는 메시지 $(No,\ H_{r_d}(s' \oplus N_p'))$을 전송한다. 서버는 제품이 위조된 것으로 판단하여 반품처리토록 한다. 마지막으로, 제품 판매 단계에서의 공격을 알아보자. 이 단계에서의 공격은 네 가지가 있을 수 있다. 첫째, 서버에서 Tag_i로 전송되는 메시지 $(N_p,\ f_{(N_p \oplus t_i \oplus s)}(t_i \| s'))$의 전송이 이루어지지 않도록 하는 공격, 둘째, Tag_i에서 서버로 전송되는 메시지$(N_T,\ H_{(t_i \oplus N_p)}(s' \oplus N_p))$의 전송이 이루어지지 않도록 하는 공격, 셋째, 소비자에서 Tag_i에 전송되는 메시지 $(N_C,\ f_{s'}(N_C))$의 전송이 이루어지지 않도록 하는 공격, 넷째, Tag_i에서 소비자로 전송되는 메시지 $(N_T',\ H_{(N_T' \oplus s')}(N_C \oplus s'))$의 전송이 이루어지지 않도록 하는 공격이다. 첫 번째와 두 번째 공격은 제품 인도 단계에서와 같은 방식으로 처리되고, 세 번째와 네 번째 공격은 제품 인수 단계에서와 같은 방법으로 처리된다. DoS 공격으로 반품된 제품들은 진위 확인을 거친 후, 진품이면 다시 유통될 수 있다. 따라서, 위조 방지 프로토콜은 서비스 거부 공격에 안전하다.

• 재생 공격에 안전(Resistance to replay attack): 위조 방지 프로토콜에서 도청할 수 있는 메시지는 8개이다. 제품 인도 작업에서 서버에서 Tag_i로 전송되는 메시지 $(N_p,\ f_{(N_p \oplus t_i \oplus s)}(t_i \| s'))$와 Tag_i에서 서버로 전송되는 메시지$(N_T,\ H_{(t_i \oplus N_p)}(s' \oplus N_p))$, 제품 인수 작업에서 R_d에서 Tag_i에 전송되는 메시지 $(N_{R_d},\ f_{s'}(N_{R_d}))$와 Tag_i에서 R_d로 전송되는 메시지 $(N_T',$

$H_{(N_T'\oplus s')}(N_{R_d}\oplus s')$), 제품 판매 단계에서 서버에서 Tag_i로 전송되는 메시지 (N_p, $f_{(N_p\oplus t_i\oplus s)}(t_i\|s')$), Tag_i에서 서버로 전송되는 메시지(N_T, $H_{(t_i\oplus N_p)}(s'\oplus N_p)$), 소비자에서 Tag_i에 전송되는 메시지 (N_C, $f_{s'}(N_C)$)와 Tag_i에서 소비자로 전송되는 메시지 (N_T', $H_{(N_T'\oplus s')}(N_C\oplus s')$) 등이다. 공격자는 이들 메시지들을 도청하여 재생 공격에 사용할 수 있다. 하지만, 도청한 메시지의 전송은 리더와 태그 사이에서 발생함으로 3.1절에서 언급한 상호 인증 프로토콜로 리더와 태그 사이에 상호 인증이 이루어져야 한다. 상호 인증을 위해서는 비밀키 s를 알아야 하지만 공격자는 비밀키 s를 알 수 없으므로 도청한 메시지를 송신할 수 없다. 따라서, 위조 방지 프로토콜은 재생 공격에 안전하다.

• 중간자 공격에 안전(Resistance to man-in-middle attack): 공격자들은 서버, 리더와 태그 사이에 전송된 메시지를 도청하여 이 메시지를 수정하여 사용할 수 있다. 위조 방지 프로토콜에서는 메시지의 수정이 불가능하도록 암호화를 사용하며, 수정되었는지를 쉽게 판별하기 위해 키를 사용한 해시함수를 사용한다. 공격자들이 도청한 메시지를 수정하여 서버, 리더 및 태그에 보냈을 때 수신자는 쉽게 이 메시지의 진위를 알 수 있다. 그 이유는 공격자들이 비밀키(s)와 서버와 태그 간의 공유키(t_i)를 알 수 없어 암호화한 메시지를 풀 수 없을뿐더러 해시함수의 값을 유추할 수 없기 때문이다. 따라서, 위조 방지 프로토콜은 중간자 공격에 안전하다.

• 위조 방지(Anti-Counterfeiting): 위조 방지 프로토콜에서 위조품을 만들기 위해서는 태그에 저장된 비밀키를 알아야 한다. 비밀키를 알기 위해서는 암호화된 메시지를 풀거나 해시함수 값에서 키를 유추해야 한다. 하지만 이는 암호학적으로 유추가 어렵다. 따라서, 유통망 상에 위조품이 유통될 수 없다. 다만, 제품 인도를 하는 유통노드나 제품 인수를 하는 유통노드가 의도적으로 태그의 비밀키를 유출시켜 이 비밀키를 가진 태그가 부착된 위조품을 만들어 유통시킬 수 있다. 하지만, 위조 방지 프로토콜의 제품 판매 단계에서 위조품임을 알 수 있다. 제품 판매 단계의 (3)에서 서버에서 태그로 (N_p, $f_{(N_p\oplus t_i\oplus s)}(t_i\|s')$) 메시지를 보내면 위조된 태그는 t_i를 알 수 없어 암호화된 메시지를 풀 수 없다. 따라서, 제품 판매 단계의 (4)에서 태그에서 서버로 보내는 (N_T, $H_{(t_i\oplus N_T)}(s'\oplus N_p)$) 메시지가 올바른 값을 가질 수가 없으므로 서버는 이 제품을 위조로 판명하게 된다.

4.2 기타 사항

본 논문에서 제시한 위조 방지 프로토콜에서 태그를 물리적으로 복사하거나 제품에 부착된 태그를 강제로 제거하여 다른 제품에 부착하면 위조 여부를 판별할 수 없다. PUF(Physical Unclonable Functions) 태그[19,20]를 사용함으로써 이와 같은 공격을 막을 수 있다.

제품의 특성 상, 제품에 부착된 태그와 리더의 거리가 가까워도 문제가 없는 경우에는 모든 태그를 NFC(Near Field Communication) 태그로 대체하여 우리가 제시한 위조 방지 프로토콜을 사용할 수 있다. 대부분의 스마트폰에는 NFC 리더가 있으므로 유통노드 뿐만 아니라 소비자는 각자의 스마트폰을 이용하여 태그를 접근하고 서버와 통신함으로써 어디에서든 위조 방지 프로토콜을 수행할 수 있다. 이렇게 되면 소비자가 다른 소비자에게 소유권을 이전하기 위해 RFID 리더가 있는 곳으로 갈 필요가 없어진다.

4. 결 론

위조품은 현재의 상업에서 매우 중요한 위협 중의 하나이다. RFID 기술이 발전함에 따라, 제품에 RFID 태그를 부착함으로써 멀리 떨어진 거리에서 제품들을 인식할 수 있고, 공급망에서 제품이 유통되는 경로를 추적할 수 있을 뿐만 아니라 제품의 위조 여부를 파악할 수 있다.

RFID 태그가 부착된 제품들의 위조 방지 및 탐지를 위한 많은 연구가 이루어졌다. 이들 연구들은 유통 경로 추적에 기반으로 하는 방법, 암호화에 기반을 둔 방법, 공급망에서의 올바른 유통 경로에 기반을 둔 방법, 그리고, 태그의 소유권 이전 프로토콜을 이용한 방법 등이다. 기존의 위조 방지 방법들은 대부분 공급망에서 위조품이 유통되지 않도록 한다. 하지만, 소비자에서 소비자로 제품이 유통될 때는 위조를 판별할 수가 없다. 소유권 이전 프로토콜을 사용하면 유통망 뿐만 아니라 소비자에서 소비자로 제품이 유통될 때도 위조를 판별할 수 있다. 소유권 이전

프로토콜을 이용하면 유통노드에서 유통노드로 진품을 안전하게 유통시킬 수 있으며, 소비자가 가진 제품을 다른 소비자에게 이전할 때도 진품 여부를 판단하여 안전하게 이전할 수 있다. 하지만, 기존 소유권 이전 프로토콜들은 소유권 이전을 위해 현 소유주와 새 소유주가 한 곳에서 동시에 태그를 접근하여 소유권 이전이 이루어진다. 공급망에서 제품이 유통되는 과정은 제품을 인도할 유통노드와 제품을 인수할 유통노드가 대부분 멀리 떨어져 있어 한 장소에서 동시에 태그를 접근하여 제품을 인도 및 인수할 수 없다. 즉, 소유권 이전 프로토콜을 그대로 공급망에 사용할 수 없다. 이와 같은 특성 때문에 소유권 이전 프로토콜을 공급망에 사용하기 위해서는 수정이 필요하다.

본 논문에서는 대칭키 암호화를 사용한 비교적 간단한 G. Kapoor와 S. Piramuthu가 제안한 소유권 이전 프로토콜[1]을 공급망에서 제품의 유통 경로 추적과 위조 방지를 할 수 있도록 수정하였다. 우리가 제시한 프로토콜은 크게 3개의 단계로 이루어진다. 제품을 인도하는 유통노드에서 수행되는 제품 인도 단계, 제품을 인수할 유통노드에서 수행될 제품 인수 단계, 그리고 소매점에서 소비자에게 제품을 판매할 때 수행되는 제품 판매 단계이다. 이 프로토콜은 위조 방지를 비롯한 여러 보안 공격에 안전함을 보였다. 다른 여러 소유권 이전 프로토콜들도 본 논문에서 수정한 방식과 유사하게 수정함으로써 위조 방지를 위해 활용할 수 있다.

제품의 특성 상, 제품에 부착된 태그와 리더의 거리가 가까워도 문제가 없는 경우에는 모든 태그를 NFC 태그로 대체하여 우리가 제시한 위조 방지 프로토콜을 사용할 수 있다. 대부분의 스마트폰에는 NFC 리더가 있으므로 유통노드 뿐만 아니라 소비자는 각자의 스마트폰을 이용하여 태그를 접근하고 서버와 통신함으로써 어디에서든 위조 방지 프로토콜을 수행할 수 있다. 이렇게 되면 소비자가 다른 소비자에게 소유권을 이전하기 위해 RFID 리더가 있는 곳으로 갈 필요가 없어진다.

REFERENCE

[1] G. Kapoor and S. Piramuthu, "Single RFID Tag Ownership Transfer Protocols," *IEEE Transactions on Systems, Man, and Cybernetics,* Vol. 42, No. 2, pp. 164-173, 2012.

[2] OECD, *The Economic Impact of Counterfeiting and Privacy*, Organisation for Economic Co-operation and Development, 2008.

[3] S.H. Choi and C.H. Poon, "An RFID-based Anti-counterfeiting System," *IAENG International Journal of Computer Science*, Vol. 35, No. 1, pp. 1-12, 2008.

[4] M. Cerlinca, C. Turcu, T. Cerlinca, R. Prodan, and V. Popa, "Anti-counterfeiting ISO 15693 RFID Solutions Involving Authentication and Traceability using Symmetric and Asymmetric Cryptography," *Proceedings of the 11th International Conference on Development and Application Systems*, pp. 175-178, 2012.

[5] H.H. Cheung and S.H. Choi, "Implementation Issues in RFID-based Anti-counterfeiting Systems," *Computers in Industry*, Vol. 62, No. 7, pp. 708-718, 2011.

[6] M.P. Schapranow, A. Zeier, F. Leupold, and T. Schubotz, "Securing EPCglobal Object Name Service-Privacy Enhancements for Anti-counterfeiting," *Proceedings of Second Intelligent Systems, Modelling and Simulation*, pp. 332-337, 2011.

[7] A. Arbit, Y. Oren, and A. Wool, "Toward Practical Public key Anti-Counterfeiting for Low-Cost EPC Tags," *Proceeding of International IEEE Conference on RFID*, pp. 184-191, 2011.

[8] M.Q. Saeed, Z. Bilal, and C.D. Walter, "An NFC Based Consumer-level Counterfeit Detection FrameWork," *Proceeding of 11th Annual Conference on Privacy, Security and Trust*, pp. 135-142, 2013.

[9] C.L. Chen, Y.Y. Chen, T.F. Shih, and T.M. Kuo, "An RFID Authentication and Anti-counterfeiting Transaction Protocol," *Proceedings of International Symposium on Computer, Consumer and Control*, pp. 419-422, 2012.

[10] E.O. Blass, K. Elkhiyaoui, and R. Molva,

"Tracker: Security and Privacy for RFID-based Supply Chains," *Procceding of 18th Annual Network and Distributed System Security Symposium*, pp. 455-472, 2011.

[11] K. Elkhiyaoui, E.O. Blass, and R. Molva, "CHECKER: On-site Checking in RFID-based Supply Chains," *Proceedings of the fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks,* pp. 173-184, 2012.

[12] C.L. Chen, Y.Y. Chen, Y.C. Huang, C.S. Liu, C.I. Lin, and T.F. Shih, "Anti-counterfeiting Ownership Transfer Protocol for Low Cost RFID System," *The World Scientific and Engineering Academy and Society Transactions on Computers*, Vol. 7, Issue 8, pp. 1149-1158, 2008.

[13] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An Effcient and Secure RFID Security Method with Ownership Transfer," *Proceeding of International Conference on Computational Intelligence and Security*, pp. 1090-1095, 2006.

[14] S. Fouladgar and H. Afifi, "An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags," *Proceeding of The First International EURASIP Workshop on RFID Technology*, pp. 59-62, 2007.

[15] S. Song, "RFID Tag Ownership Transfer," *Workshop on RFID Security*, 2008.

[16] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight Mutual Authentication and Ownership Transfer for RFID Systems," *IEEE INFOCOM*, pp. 251-255, 2010.

[17] J. Satio, K. Imamoto, and K. Sakurai, "Reassignment Scheme of an RFID Tag's Key for Owner Transfer," *Lecture Notes in Computer Science*, Vol. 3823, pp. 1303-1312, 2005.

[18] J.D. Lee, "RFID Tag Ownership Transfer Protocol using Lightweight Computing Operators," *Journal of Korea Multimedia Society*, Vol. 16, No. 12, pp. 1413-1426, 2013.

[19] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," *Proceedings of the IEEE International Conference on RFID*, pp. 58-64, 2008.

[20] P. Tuyls and L. Batina, "RFID-Tags for Anti-Counterfeiting," *Topics in Cryptology - CT-RSA 2006, Lecture Notes in Computer Science*, Vol. 3860, pp. 115-131, 2006.

이 재 동

1983년 2월 서울대학교 계산통계학과 이학사
1985년 2월 서울대학교 전산과학전공 이학석사
1995년 2월 서울대학교 전산과학전공 이학박사

1986년~현재 경남대학교 컴퓨터공학과 교수
관심분야: 실시간 시스템, 임베디드 시스템, 컴퓨터 보안