IoV 환경에서의 RFID 기반 적응형 차량 인증 프로토콜의 취약점 연구

김동현, 김현민, 손채윤, 오민규, 이창의, 박요한*

계명대학교, *계명대학교

laders23@naver.com, c3man161@gmail.com, sonchaeyun0604@gmail.com, alsrb4719@gmail.com, rhlijh7410@gmail.com, *yhpark@kmu.ac.kr

Security Analysis of An Adaptive, Lightweight, Secure and Efficient RFID-Based Scheme for IoV

Kim Dong Hyeon, Kim Hyeon Min, Son Chae Yun, Oh Min Gyu, Lee Chang Ui, Park Yo Han*

Keimyung Univ., *Keimyung Univ.

요 약

본 논문은 차량 인터넷 환경에서 RFID(Radio Frequency IDentification)를 통해 근처 RSU(Road Side Unit)과의 통신을 통해 빠른 인증을 진행한다. 차량 인터넷 환경은 빠른 이동성과 제한된 연산 한계 등의 문제를 가지고 있으므로 안전하면서도 빠르고 가벼운 인증 프로토콜의 연구가 필요하다. 2023년 Gong 등은 차량 인터넷 환경에서 안전한 RFID 기반의 적응형 경량 인증 프로토콜을 제안하였다. 본 논문에서는 Gong 등이 제안한 인증 프로토콜의 문제점을 분석하고, 이에 대한 대응방안을 제시하였다.

Ⅰ. 서 론

본 논문에서는 무선 통신 및 IoT 기술의 발전으로 인해 차량 인터넷에 RFID 기술이 보편화되어 개인 데이터 보안과 식별 및 추적 정확성을 높이는데 기여했다[1]. 차량 인터넷 환경에서는 교통이 혼잡할 때 한 곳에 오랜 시간 동안 머무르는 경향이 있다. 그 결과 RSU와 차량은 빈번한 상호 인증을 수행하게 되며, 이로 인해 상당한 양의 계산 및 통신 오버헤드가 발생할 수 있다. 따라서 최근 경량화되고, 안전한 RFID 기술에 대한 연구가 진행되고 있다[2]. 2023년에 Gong[3] 등은 교통 혼잡 시나리오에 대한 경량 RFID 보안 고속 인증 프로토콜을 제안했다. 본 논문에서는 Gong 등이 제안한 스키마가 고정된 키 값을 사용함으로부터 발생하는 임시 키 노출 공격, 장기 비밀성, 내부자 공격 등에 취약하다는 것을 발견했고 이에 대한 대응 방안을 제시한다.

Ⅱ. 본론

본 논문에서는 Gong 등의 인증 및 키 합의 프로토콜에 대해서 소개하고 보안 취약점을 분석한다.

2.1 Gong 등의 인증 및 키 합의 프로토콜

차량 인터넷 환경에서의 RFID 인증 프로토콜을 위해 Gong 등은 초기화 단계, 태그 등록 단계, 리더 등록 단계, 빠른 상호 인증 단계, 소유권 이전 단계로 나뉜다.

2.1.1 초기화 단계

초기화 단계에서 인증 기관은 큰 소수인 d를 엣지서버의 비밀 키로 생성한다. 이후 G를 기저점으로 사용하는 타원곡선에서 공개키인 $Q = dG$를 계산한다.

2.1.2 등록 단계

태그와 리더는 클라우드에 등록을 진행하며 등록과정은 그림1, 그림 2와 같다.

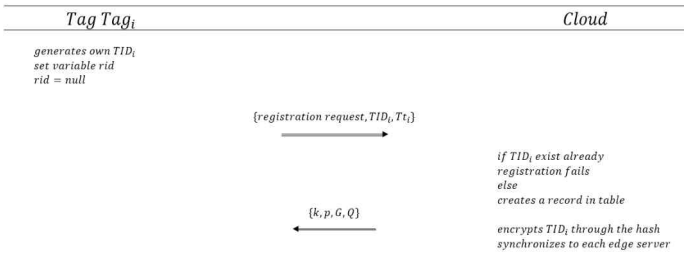

그림 1. 태그 등록 단계

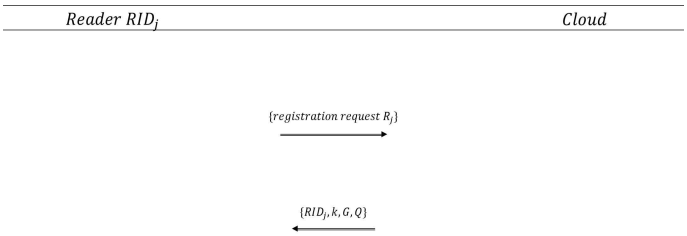

그림 2. 리더 등록 단계

2.1.3 인증 단계

정상적으로 클라우드에 등록된 태그는 자신의 근처에 있는 리더와 인증을 진행하는 경우 그림3과 같이 인증을 진행한다. 만약 리더가 태그의 통신 범위 밖에 있는 경우 그림 4와 같이 인증을 진행한다.

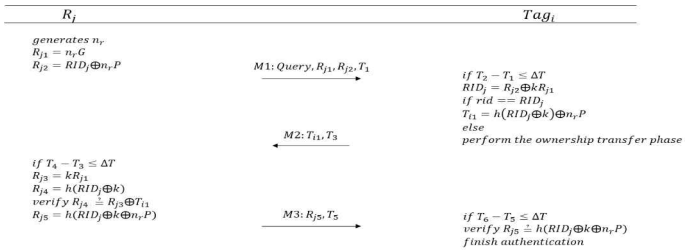

그림 3. 리더와 태그 간 빠른 상호 인증 단계

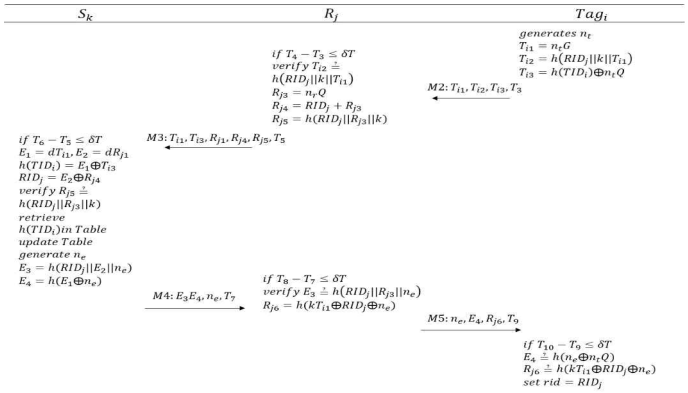

그림 4. 소유권 이전 단계

2.2 Gong 등의 인증 스킴의 문제점

본 논문에서는 Dolev-Yao(DY) 모델[4]을 사용하여 보안 취약점을 분석하였다. 공격자는 공개채널로 송수신되는 메시지를 도청, 삭제, 삽입, 수정할 수 있다. DY 모델은 키 교환 프로토콜의 분석에 널리 사용되는 모델이다.

2.2.1 내부자 공격을 통한 태그 사칭 공격

1단계 : 공격자는 정당한 사용자로 등록을 시도한다.

2단계 : 공격자는 등록 과정에서 비밀 파라미터인 $\{k\}$를 얻을 수 있다.

3단계 : k를 기반으로 공격자는 빠른 인증 단계의 검증 과정에 필요한 파라미터 값을 추출 및 계산할 수 있다.

3.1 공개 채널을 통해 전송되는 $\{R_{j1}, R_{j2}\}$을 통해 RID_j를 추출한다.

3.2 공개 채널에서 전송되는 M_2의 $\{T_{i1}\}$을 통해 $\{T_{i1} \oplus h(RID_j \oplus k) = n_r P\}$를 추출한다.

3.3 공개 채널에서 전송되는 M_3 의 $\{R_{j5}, T_5\}$를 탈취한 다음, 해당 값을 통해 다른 태그의 정보를 가지고 검증과정을 성공적으로 통과할 수 있다.

따라서, 내부자 공격을 통한 태그 사칭 공격이 가능하다.

2.2.2 정확성 문제

Gong 등이 제안한 스킴은 정확성 문제가 있다.

a. 소유권 이전 단계에서 리더측 $\{RID_j\}$와 클라우드 측 $\{RID_j\}$를 같은지 확인하는 과정에서 $RID_j = E_2 \oplus R_{j4}$와 $n_r Q \oplus (RID_j + n_r Q)$의 동일 유무를 확인하는데, $RID_j \neq n_r Q \oplus RID_j$라는 결과에 의해 검증될 수 없기 때문에 다음 단계로 넘어갈 수 없다.

b. 소유권 이전 단계에서 리더측 $\{R_j\}$를 검증하기 위해 R_{j6}를 전송 후, 태그측에서 해당 값을 검증할 때, $R_{j6} = h(k T_{i1} \oplus RID_j \oplus n_e)$와 $R_{j6} = h(k T_{i1} \oplus TID_i \oplus n_e)$는 $RID_j \neq TID_j$라는 결과에 의해 검증에 실패하게 되고, 다음 단계로 넘어갈 수 없다.

따라서 Gong 등이 제안한 스킴은 정확성에 문제가 있다.

Ⅲ. 결론

본 논문에서는 Gong 등이 제안한 경량 RFID 기반 고속 인증 프로토콜이 임시 비밀 누출 공격 및 내부자 공격과 장기 비밀성에 취약하고 안전성을 보장하기 못함을 보였다. 이와 같은 취약점을 보완하기 위하여 k 값에 랜덤 넘버 값을 연산하여 계산하는 대응 방안을 제시한다. 따라서 공격자는 k 값을 알 수 없으며 사용자의 정보는 안전할 수 있다. 위와 같은 대응 방안을 통하여 k와 같은 키의 안전성 및 태그의 프라이버시를 보장하는 RFID 기반 고속 인증 프로토콜이 제안 가능하다.

ACKNOWLEDGMENT

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2021R1I1A3059551.

참 고 문 헌

[1] Cao, B.; Gu, Y.; Lv, Z.; Yang, S.; Zhao, J.; Li, Y. RFID reader anticollision based on distributed parallel particle swarm optimization. IEEE Internet Things J. 2020, 8, 3099 - 3107.

[2] Lee, Y.K.; Sakiyama, K.; Batina, L.; Verbauwhede, I. Elliptic-curve-based security processor for RFID. IEEE Trans. Comput. 2008, 57, 1514 - 1527.

[3] Gong, Y.; Li, K.; Xiao, L.; Cai, J.; Xiao, J.; Liang, W.; Khan, M.K. VASERP: An Adaptive, Lightweight, Secure, and Efficient RFID-Based Authentication Scheme for IoV. Sensors 2023, 23, 5198.

[4] DOLEV, Danny; YAO, Andrew. On the security of public key protocols.*IEEE Transactions on information theory*, 1983, 29.2: 198-208.