[10-60] RFID 태그 보안을 위한 Randomized Tree Walking 알고리즘의 개선

최원준, 노병희, 유승화
아주대학교 정보 통신 전문 대학원
macgebi@nownuri.net bhroh@ajou.ac.kr swyoo@ajou.ac.kr

A Modified Randomized Tree Walking Scheme for RFID Tag Security

Wonjoon Choi, Byeong-hee Roh, and S.W. Yoo
Graduate School of Information and Computer Science, Ajou University

요약

RFID 시스템에서 사물의 유일한 식별번호를 가지고 있는 RFID 태그는 스스로의 파워를 갖고 있지 않으며 작은 크기, 낮은 가격을 목표로 하기 때문에 연산 능력이 매우 미약하다. 또한 태그로부터 정보를 수집하는 리더가 발생시키는 전파에 포함되어 있는 에너지를 이용하여, 태그가 자신의 정보를 출력하기 때문에, 태그의 전파는 크기가 약하고, 도달 거리가 짧다. 이런 특성을 이용하여 태그로부터 리더로 전달되는 무선 경로인 backward 채널은 도청의 가능성이 거의 없다는 가정하에 대부분의 태그 보안 방법은 리더로부터 태그로 정보를 전달하는 forward 채널을 보호하는데 초점을 맞추고 있다. 하지만, 실제로 태그와 가까이에 있는 불법적인 리더는 정보를 불법적으로 수집할 수 있다. 본 논문에서 우리는 Randomized Tree Walking의 개선 방법을 제안한다. 이 방법은 자신의 정체를 드러내지 않고, 정상적인 리더와 태그간의 통신을 엿들음으로써 불법적으로 정보를 수집하는 리더를 방해한다. 우리는 개선된 방법으로 보호되는 정보의 양을 분석하고, 태그의 추가적인 변경 없이 리더의 동작만을 변경시킴으로써 정보가 보호됨을 보인다.

1. 서론

RFID 태그에 저장되어 있는 유일한 일련번호를 무선으로 파악할 수 있는 '비접촉식 정보 교환'이라는 RFID 시스템의 특성을 이용하여, 물류시스템, 도서관 관리 시스템, 박물관의 정보 시스템이 보다 지능화, 자동화, 효율화되고 있다. 또한, 대형 마트, 도서관, 각종 신분 인식 시스템 등 이미 삶의 깊숙하게 들어와 있다.

현재 주로 개발, 사용하고 있는 RFID 태그는 눈에 보이지 않을 정도로 작은 크기를 갖고 사물의 외향에 영향을 주지 않고 부착될 수 있으며, 제조 비용의 목표를 매우 낮게 책정함으로써 필요한 모든 사물에 부착할 수 있도록 구상되고 있다. 이런 제약에 따라 RFID 태그는 연산 능력과 저장능력이 매우 미약하며, 통신에 필요한 전력은 리더로부터 발생된 전파에 내재되어 있는 에너지에 의존한다.

다른 통신 시스템과 마찬가지로 RFID역시 정보 보호를 위한 기술의 개발과 적용이 필요하다. 통신의 보호를 위한 기술은 이미 기존에 많은 것들이 나와있다. 무선의 경우, 매체가 공개되어 있기 때문에 보다 많은 주의가 필요하며, 불법적인 도청 및 변조를 견뎌내기 위한 암호화와 인증 기법이 일반적으로 쓰인다. 하지만 RFID 태그는 앞에서 말한 바와 같이 가격과 크기의 제약으로 인해, 컴퓨팅 파워가 약하다는 약점을 갖고 있으므로, 이런 방법은 적합하지 않다. 이런 약점을 극복하기 위해 태그와 리더간의 통신 알고리즘인 tree-walking 알고리즘의 특성을 이용하여 Silent-Tree-Walking Singulation 알고리즘[],