# Ad Hoc 네트워크에서 사용자 노드의 인증을 위한 키 관리 기법 연구동향 분석

*황치범 **최진영
*고려대학교 컴퓨터과학기술대학원 정보통신학과
*hwangcb72@korea.ac.kr

# A Study of key management technique for user's node Authentication in Ad Hoc Networks

*Chibum Hwang **Jinyoung Choi
Dept. of Computer Science & Technology, Korea University

## 요 약

Ad Hoc 네트워크에서는 기존의 인프라에서 지원하는 Public key infrastructure 또는 Third party key management service를 자주 사용하지 못하는 환경에서 사용되는 네트워크 구조로 여러 유형의 보안 문제가 발생할 수 있다. 특히 무선 연결에 따른 보안 취약점과 중앙 통제를 위한 고정된 제어 장치가 없어 인증과 키 관리가 문제가 되고 있다. 따라서 본 논문에서는 Ad Hoc 네트워크 환경에서의 인증을 위한 키 생성 및 키 합의 프로토콜 기법의 여러 가지 연구동향과 연구에 기반 한 프로토콜 분석 및 단점에 관하여 살펴보도록 한다.

## 1. 서론

최근 인터넷의 급격한 성장에 힘입어 인터넷을 이동 중에도 이용하고자 하는 노력이 빠르게 개발됨으로 이동 컴퓨팅에 대한 응용 범위와 사용량이 크게 증가하였다. 또한, 기지국이나 인프라를 구축되지 못한 상황에서도 통신하기 위한 연구가 활발히 전개되고 있다. 이를 일컬어 Infrastructureless 네트워크에 기반 한 Ad Hoc 네트워크라 한다.

Ad Hoc 네트워크는 무선 이동 호스트 장치들의 집합으로 인프라 기반이 없는 환경에서 다른 Ad Hoc 장치들과 통신할 수 있어야 한다. 따라서 여러 이동 단말 사이에서 데이터를 전달할 수 있어야 하는데, 이를 위해 각 이동 단말들은 유선망의 라우터 기능을 수행해야 한다. 또한, Ad Hoc 네트워크의 노드는 이동성을 가지고 있기 때문에 시간의 흐름에 따라 네트워크 위상이 동적으로 변하며, 배터리 유지에 따른 데이터 전송 반경의 제한되는 단점과 낮은 대역폭과 높은 에러율을 고려하여야 한다.

이 Ad Hoc 네트워크 환경에서는 인프라 기반구조를 지원하기 곤란하므로 이에 따른 취약점이 보안에 많은 문제점을 발생시킬 수 있다. 노드들은 중앙의 통제가 없이 분산된 작업을 수행하므로 인증과 키 합의 및 키분배에 기존의 방법과는 다른 방법이 필요하므로, 본 연구에서는 Ad Hoc 네트워크 환경에 필요한 키 관리기법에 대하여 여러 가지 연구 동향을 분석하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 인증을 위한 여러 가지 고려사항을 분석하였고, 3장에서는 네트워크를 안전하게 보호하기 위한 키 관리 기법의 여러 가지 연구들을 기술하고, 마지막으로 4장에서는 결론을 맺는다.

## 2. Ad Hoc 네트워크의 인증을 위한 고려사항 분석

Ad Hoc 네트워크에서 보안 메커니즘을 위해 사용자 노드들에 대해 인증하는 것은 매우 중요한 문제이다. 고려사항 중, 첫 번째 이슈는 키 설정(establishment)이다. 이는 가장 중요하고 복잡한 이슈로, 키 설정은 키 전송