[5A-15]

무선 Ad-hoc 기반 인증 메커니즘 설계

*이철승, *민혜란, *박종철, *홍성표, **이광, ***김충원, ***이준
*조선대학교 대학원 컴퓨터공학과
**청주과학대 컴퓨터과학과
***조선대학교 전자정보공과대학 컴퓨터공학과
*e-mail : cheolseung@hotmail.com

Design of Authentication Mechanism based on Mobile Ad-hoc

*Cheolseung Lee, *Hyeran Min, *Jongcheul Park, *Seongpyo Hong,
**Kwang Lee, ***Choongwoon Kim, ***Joon Lee
*Dept. of Computer Engineering Graduate School. Chosun University
**Dept. of Computer Science. Chongju National College
***Dept. of Computer Engineering. Chosun University

요 약

본 논문은 무선 이동 Ad-hoc 망에서 신뢰성 있는 사용자 인증문제를 해결한다.

Ad-hoc 망은 기존의 무선망과는 달리 고정 노드가 없이 망 전체가 이동 무선 노드들로 구성된 망이다. 따라서 Ad-hoc 망을 이용하면 선로 설치가 어려운 곳이나, 임시적으로 망을 구성해야 할 경우 또는 응급시에 신속하고도 유연하게 통신망을 구축할수 있다. 하지만 각 노드들이 이동하기 때문에 끊임없는 망의 변화가 생겨나며 중앙 관리 체제가 없기 때문에 노드들은 규제할 수 있는 방법이 없다. 이런 상황에서 가장 중요한 것은 효과적인 통신경로 설정과 적법한 사용자 인증문제가 시급한 실정이다. 본 논문은 Ad-hoc 망에서 DSR 라우팅 프로토콜을 이용하여 경로설정 및 경로유지를 하며, 무선망의 보안구조 및 보안요소, 기존 인증시스템과 관련된 각종 암호 관련기술을 살펴본후, KerberosV5 인증 프로토콜을 사용하여, 적법한 Ad-hoc 망의 인증메커니즘을 설계한다.

I. 서론

무선통신 기술의 지속적인 발전과 대중화와 함께 무선인터넷 이라는 새로운 서비스를 만들어 냈으며, 기존의 유선인터넷 환경의 다양한 멀티콘텐츠를 수용하기 위한 노력으로 이어졌다. 그러나 유선 인터넷 과 무선 인터넷은 다루는 트래픽의 특성이 매우 상이한 특징을 가지고 있어, 여러 가지 기술적인 차이점을 가지게 되었다.

Ad-hoc 망은 기존의 무선망과는 달리 고정 노드가 없이 망 전체가 이동 무선 노드들로 구성된 망이다. 따라서 Ad-hoc 망을 이용하면 선로 설치가 어려운 곳이나 임시적으로 망을 구성해야 할 경우 또는 응급시에 신속하고도 유연하게 통신망을 구축할 수 있다. 하지만 각 노드들이 이동하기 때문에 끊임없는 망의 변화가 생겨나며 중앙 관리 체제가 없기 때문에 노드들은 규제할 수 있는 방법이 없다. 이런 상황에서 가장 중요한 것은 효과적인 통신경로 설정과 적법한 사용자 인증문제가 시급한 실정이다.

본 논문은 Ad-hoc 망에서 효과적으로 통신 경로 설정 및 경로 유지를 위한 DSR 라우팅 프로토콜을 이용하여 무선망의 보안구조 및 보안요소, 기존 인증시스템과 관련된 각종 암호 관련 기술을 살펴본후, Ad-hoc 망의 KerberosV5 인증 프로토콜을 사용하여 사용자 인증을 위해 서버 클라이언트가 지니는 설계상의 문제점과 취약점을 찾아 대안을 제공한다.

II. 인증 시스템 기반 기술

2.1 Ad-hoc

Ad-hoc 망은 데이터전송에 필요한 고정된 네트워크 기반 시설이나, 중앙 통제 요소가 없이 동적으로 구성된 노드들이 라우터로서의 기능을 제공하는 네트워크를 말한다.

유선 망에서는 Link-State, Distance-Vector 와 같은 효율적인 라우팅 프로토콜을 많이 사용하지만, 빈번하게 변화하는 Ad-hoc 망에서는 적용하기가 힘들다.

또한 이동 노드의 제한된 대역폭과 저 전력을 효율적으로 사용하기 위해서 라우팅 오버헤드를 줄여야 하는 제약 조건을 가지며, Ad-hoc 망에서의 라우팅 프로토콜은 크게 Tablen-driven 방식과 On-demand 방식으로 분류할 수 있다. Table-driven 방식은 각각의 노드가 망전체 노드에 대한 라우팅 정보를 유지하고 이용하여, 라우팅을 수행하며, On-demand 방식은 망 내의 모든 노드에 대한 전체 경로를 항상 유지하는 것이 아니라 전송할 데이터가 발생했을 때에 경로를 획득하고 실제 경로에 대한 정보만을 유지하는 방식이다[1].

아래의 그림 1 은 Ad-hoc 망의 Table-driven 방식과, On-demand 방식에서 사용하는 프로토콜을 보이고