[5C-51]

이동 Ad-hoc 네트워크에서의 안전한 키 관리 알고리즘

김진철, *오영환
한전 KDN㈜, *광운대학교
kjc@kdn.com *yhoh@gwu.ac.kr

A secure key management algorithm for Mobile Ad-hoc Networks

Jincheol Kim, *Youngwhan Oh,
KDN, *Kwangwoon University

요 약

MANET(Mobile Ad-hoc Network)은 이동 노드들의 무선 통신을 위한 새로운 패러다임으로서, 통신 인프라가 없는 환경에서 이동 노드들만으로 구성된 자율적이고 수평적인 네트워크이다. 대부분의 MANET 연구들은 안전한 통신 환경을 가정하고, 네트워크에 참여하는 모든 이동 노드들이 서로 신뢰함으로써 보안을 고려하지 않고 진행하였다. 본 논문에서는 MANET 상의 보안을 제공하기 위한 보안 요소들을 분석하고, 새로운 키 알고리즘을 제안하였다. 제안한 알고리즘은 인증 기능을 이동 노드들에게 분산시키고, 핸드셰이크 절차를 통하여 안전한 정보 송수신이 이루어 지도록 하였다. 또한 제안한 키 관리 알고리즘이 보안 요소들에 부합되는지 분석하였다.

I. 서론

MANET(Mobile Ad-hoc Network)은 이동 노드들의 무선 통신을 위한 새로운 패러다임으로서, 통신 인프라가 없는 환경에서 이동 노드들만으로 구성된 자율적이고 수평적인 네트워크이다. [1] 대부분의 무선 네트워크 시스템은 고정된 기지국에 의한 중앙관리와 유선 기반 네트워크가 요구된다. 그러나 유선 기반 네트워크를 설치하기 어려운 산간 지방 또는 빙하 지역 같은 오지나 홍수, 전쟁 등의 재난으로 유선 기반 네트워크가 파괴된 지역에서의 신속한 통신 복구를 위해서는 유선 기반 네트워크가 필요없는 자체 통신 네트워크를 구성할 필요성이 대두되었다. [2] 최근 이러한 연구가 IETF (Internet Engineering Task Force)의 MANET (Mobile Ad-hoc Network) 워킹그룹 중심으로 멀티 홉(Multi-hop)으로 구성된 이동 노드들이 통신하기 위하여 필요한 Ad-hoc 라우팅 프로토콜을 연구 개발하고 있다.

MANET 은 통신 인프라가 없는 환경에서 무선 채널을 공유할 수 있는 편리한 통신 방식이지만, 다음과 같은 어려움들이 필연적으로 해결되어야 한다. 첫째, 이동 노드들이 일정한 속도를 가지고 끊임없이 이동함으로 인하여 빈번하게 변하는 네트워크 토폴로지에 빠르게 적응 가능하고, 잦은 라우팅 재설정 요구 과정에서도 높은 데이터 전송 효율을 가질 수 있고, 확장성이 보장되는 라우팅 프로토콜이 필요하다. 둘째, CA(Certificate Authority)를 통하여 인증서를 받는 보안 인프라가 없는 환경에서 모든 이동 노드들이 언제든지 공격을 받을 수 있는 위험성이 내포되어 있으므로 이를 해결할 수 있는 안전한 통신 방안이 강구되어야 한다.

지금까지 대부분의 MANET 연구들은 안전한 통신 환경을 가정하고, 네트워크에 참여하는 모든 이동 노드들이 서로 신뢰함으로써 보안을 고려하지 않고 진행하였다. 본 논문은 먼저 MANET 상에서 발생할 수 있는 보안 공격 유형을 살펴보고, 새로운 키 관리 알고리즘을 제안하고자 한다. 제안하는 키 관리 알고리즘은 CA 의 기능을 이동 노드들에게 분산시킴으로써 안전한 인증 과정이 수행할 수 있도록 하고, 데이터 전송시 핸드셰이크 절차를 통하여 안전한 데이터 송수신 과정을 수행할 수 있도록 하였다. MANET 에 제안한 키 관리 알고리즘을 적용하면 도청이나 DoS (Denial of Service) 공격에 취약한 MANET 의 보안을 향상시킬 수 있다.

II. MANET 의 보안 요소

MANET 에 보안을 제공하기 위해서, 다음과 같은 요소들을 고려해야 하며, 각각에 대한 정의는 다음과 같다. [1]

1) 유효성 (Availability): DoS 공격에 대해 네트워크 서비스의 survivability 를 어느 정도 확신시켜 줄 수 있는지를 의미한다. Dos 공격은 MANET 의 어느 통신 계층에서도 발생할 수 있다. DoS 공격의 예를 들면, 물리적 계층(Physical layer)과 MAC 계층에서는, 공격자가 jamming 기술을 사용해서 물리적인 채널에서의 통신을 방해할 수 있다. 네트워크 계층 공격자는 라우팅 프로토콜을 파괴할 수 있다. 또한, 상위 계층 공격자는 는 키 관리 서비스와 같은 보안 프레임워크에 필수적인 서비스를 공격할 수 있다.

2) 기밀성 (Confidentiality): 정보가 인증받지 못한 이동 노드들에게 유출되지 않도록 하는 것을 의미한다. 이 정보에는, 데이터 정보뿐만 아니라, 라우팅 정보도 해당된다. 라우팅 정보는 공격자가 라우팅 과정을 공격