논문 2010-47TC-7-19

# 무선 메쉬 네트워크를 위한 데이터 송신 인증 기술

## ( Data Origin Authentication Scheme for Wireless Mesh Networks )

강 남 희*

( Namhi Kang )

요 약

무선 메쉬 네트워크는 자가 구성 및 자가 관리가 가능한 애드혹 네트워크의 유비쿼터스 특성을 반영한 접속 기술이다. 본 논문에서는 무선 메쉬 네트워크에서 경로상의 노드들이 매 홉 단위로 전달 받은 데이터의 송신을 인증할 수 있고 무결성을 검증할 수 있는 방안을 제안한다. 제안하는 방식에서는 무선 메쉬 네트워크의 통신 인프라를 구성하는 노드와 데이터의 송신, 수신 및 릴레이 역할을 수행하는 무선 애드혹 네트워크의 사용자 노드를 구분하여 서로 다른 인증 기술을 적용한다. 즉, 무선 백본을 형성하는 경로 상에서 적용되는 홉 기반 인증 방안과 애드혹 네트워크의 경로 상에 위치한 노드들 간의 홉 단위 인증 방안이 다르게 적용된다. 이를 통해 기존에 제안되었던 MANET의 데이터 인증 방안에 비해 보안 설정 및 유지의 복잡도가 적고 백본을 구성하는 구간에서 빠르게 인증이 수행되기 때문에 송신에서 수신까지의 데이터 전달 지연이 적은 장점이 있다.

Abstract

Wireless mesh network, which is an access network technology, adopts ubiquitous features of ad-hoc network that includes capabilities of self-configuration and self-management. This paper proposes a scheme which enables nodes along route in wireless mesh network to authenticate data and verify data integrity. The scheme distinguishes infra-node, which is a network device used to form mesh network, and user node in ad-hoc network, which operates functions as a sender, receiver or relayer, to deploy different authentication scheme. That is, hop-based authentication scheme along route forming wireless backbone differs from authentication scheme for user nodes in route over MANET. The proposed scheme is less complex than previously proposed schemes from the repects of security setup procedures and managements. In addition, the scheme is able to reduce transmission delay from a source to a destination owing to fast authentication over wireless backbone.

**Keywords**: Data Origin Authentication, Wireless Mesh Networks, MANET Security, One-way Hash

## I. 서 론

전통적인 인터넷 접속 기술은 사전에 설정된 통신 인프라의 물리적 통신조건에 따라 통신이 가능한 영역이 제한되며 통신을 개시하기 위한 수동적인 설정이 필요하다. 유비쿼터스 환경이 실현되기 위해서는 통신 인프라에 의존 없이 언제 어디서나 통신이 가능해야 한다. 유비쿼터스 네트워크의 특성은 무선 이동 애드혹 네트워크 (MANET: Mobile Ad hoc Networks)의 속성과 잘 융합된다. MANET은 사전에 구축된 네트워크 인프라가 없더라도 무선 이동 노드들이 협업하여 자가 구성(self-configured)할 수 있는 네트워크이다[1].

MANET에 관련된 초기 연구는 군사 작전이나 재난 등의 특수한 상황에서도 네트워킹을 지원해주기 위한 대처 방안으로 연구되었지만 최근 보다 일반적인 목적을 갖는 응용으로 확산되고 있다. 특히, 무선 메쉬 네트워크(WMN: Wireless Mesh Network)는 MANET의 자가 구성 기능 및 릴레이 기능을 기반으로 저비용으로 네트워크를 구축할 수 있도록 해 준다[2].

* 정회원-교신저자, 덕성여자대학교 디지털미디어학과
(Digital Media Department, Duksung Women's University)

※ 본 연구는 덕성여자대학교 2009년도 교내연구비 지원에 의해 수행되었음

접수일자: 2010년3월26일, 수정완료일: 2010년7월14일

MANET이 다양한 영역에서 사용되고 각광 받기 시작하면서 MANET에서 발생할 수 있는 다양한 보안 위협과 이를 대처할 수 있는 방안들도 제안되고 있다. 특히, 노드의 이동성으로 인해 네트워크 경로의 단절과 재설정이 빈번하게 요구되는 MANET의 특성으로 인해 안전한 경로 설정 방안들이 많이 제안되었다[3].

네트워크를 자가 구성하는 노드들의 협업을 통해 데이터가 전달되는 MANET에서 악의적 경로설정에 따른 피해는 심각할 수 있다. 즉, MANET을 구성하는 내부 노드들이나 외부 네트워크에 존재할 수 있는 악의적인 노드들에의해 위조된 경로가 설정된다면 전달되는 모든 데이터들이 위조 경로를 통해 전달될 것이고 이를 통한 다양한 공격들이 가능하다. 또한, 악의적인 순환 경로를 설정하여 데이터를 전달할 수 없게 하거나, 경로를 유지하는 중간 노드들의 자원을 고갈시키는 래빗공격도 가능하다.

기존에 제안되어 있는 안전한 경로설정 방안들의 문제점은 경로 설정을 위해 전달되는 제어 메시지의 인증만을 고려하고 있다는 것이다. 즉, 경로 설정 이후 전달되는 데이터의 인증 방안은 제공하지 못한다. 또한, 오버헤드로 인해 제안된 방안들을 모든 데이터의 인증 방안으로 확장 적용하기는 어렵다[4].

이를 해결하기위해 LHAP[5], LAP[6], HEAP[4] 등의 메시지 송신 인증 기술들이 제안되었다. 이 기술들은 MANET에서 제어메시지와 데이터 메시지를 구분하지 않고 경로 상의 노드들 간에 홉 단위로 데이터 송신을 검증할 수 있는 방안을 제공해준다. 그러나 [8]의 방식처럼 무선 접속 네트워크의 확장성과 다양한 서비스를 제공할 수 있도록 제안된 준인프라 구조의 MANET이나 WMN에 직접 적용하기는 어렵다.

WMN를 구성하는 WMR(Wireless Mesh Router)은 데이터 송신이나 수신의 역할이 아닌 데이터 릴레이 역할을 하는 백본의 구성요소이다. 이러한 네트워크 장치의 경우 네트워크 구성자나 관리자가 사전에 비밀키를 안전하게 저장할 수 있고, 다양한 키분배 프로토콜을 이용하여 세션키를 공유할 수 있다. 이러한 특성을 기반으로 본 논문에서는 WMN에 적합한 인증 시스템을 제안한다. 제안하는 방식에서는 무선 백본을 경유하는 홉 기반 인증 방안과 MANET의 인증 방안을 분리하여 적용한다. 이를 통해 인증 시스템의 복잡성이 감소되고 종단 사이의 전달 지연이 감소된다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 본 논문이 사용하려는 네트워크의 모델 및 제안 방식의 핵심 방안인 단방향 인증 기술을 설명한다. Ⅲ장에서는 MANET에서 데이터 인증을 제공하기위해 제안된 기술들을 살펴본다. Ⅳ장에서 제안되는 인증 기술을 설명하고 Ⅴ장을 통해 안정성 및 성능을 분석한다.

## Ⅱ. 연구 배경

### 1. 시스템 모델

WMN은 자체 구성된 MANET에 유연 (flexible) 하고 비용 효율적인 방법으로 유선 인프라를 확장할 수 있는 방안을 제공해 준다. 그림 1은 각 도메인은 MANET으로 구성하고 도메인 간의 연결을 WMN을 적용하여 확장한 네트워크 구조를 나타낸다.

MANET에서의 라우팅 기술은 proactive, reactive 그리고 두 방안을 통합한 하이브리드 방안으로 구분된다. Proactive 라우팅은 데이터 전달 전에 네트워크의 토폴로지 정보를 모든 노드들이 갖는 방안이다. Reactive 라우팅 방안은 이와 달리 데이터를 전달할 필요가 있을 때만 경로를 설정하는 on-demand 방식이다. 두 방안의 단점은 노드의 이동성으로 인해 빈번하게 변경되는 경로를 재갱신하고 유지하기 위해 요구되는 제어 메시지로 인해 확장성이 떨어지는 것이다. 이를 해결하기위해 [3]에서는 하이브리드 방안을 기반으로 효율성과 신뢰성을 높일 수 있는 구조가 제안되었다. 기본 아이디어는 그림 1에 나타낸 것처럼 네트워크를 작은 도메인으

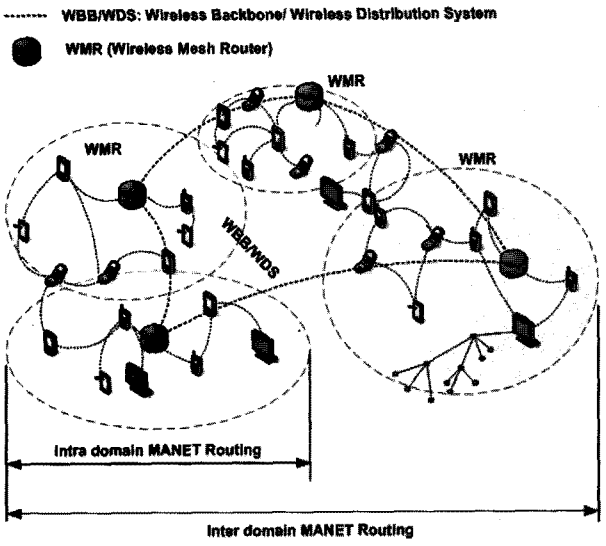


그림 1. 무선 메쉬 네트워크 구조
Fig. 1. Wireless Mesh Network Architecture.

로 구분하고 도메인간의 라우팅 프로토콜과 도메인 사이의 라우팅을 구분하여 적용하는 것이다.

### 2. 단방향 키체인

제안하는 데이터 인증 기술은 보안 해쉬함수를 기본 생성되는 단방향 키체인을 이용한다. 그림 2는 단방향 키체인을 이용한 대표적인 인증 방안인 TESLA[7] 기술의 개념을 나타낸다.

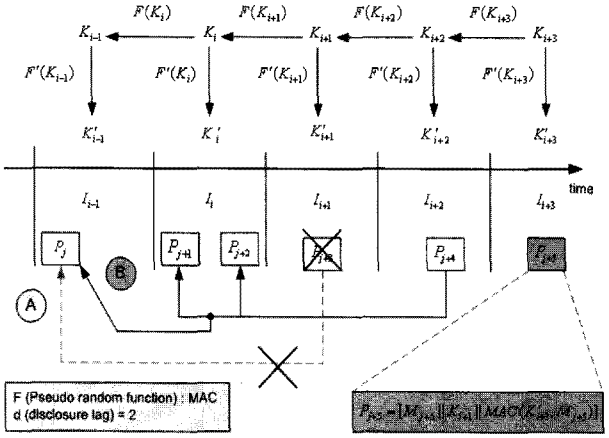


그림 2. 단방향 키체인 기반 인증 기술
Fig. 2. Authentication scheme using one-way key chain.

송신은 정해진 시간 간격동안 유효한 키를 적용한 MAC(Message Authentication Code)을 계산하여 전송하는 패킷의 인증값으로 사용한다. 이때 사용되는 키는 그림 2에 나타낸 것처럼 단방향 키체인을 통해 사전에 생성한다 (i.e., $F(K)$). 각 구간에 사용된 키는 사전에 정해진 약속에 따라 일정 구간 이후에 공개된다 (i.e., d: disclosure lag). 그림에 표시된 예를 설명하면, $I_i$번째 구간에 보내지는 $P_{j+1}$과 $P_{j+2}$ 패킷을 위한 MAC은 $K_i$를 이용하여 생성되고, $K_i$는 $d$의 값으로 정해진 2개의 시간 구간 이후에 전송되는 $P_{j+4}$를 통해 수신단에 노출된다. 따라서 수신자는 전달받은 패킷을 정해진 시간 구간 이후에 인증값의 검증을 수행한다. 보안 해쉬함수의 단방향 계산 특성으로 인해 송신이 MAC 값을 생성했던 키값을 노출하기 전에 공격자가 사용되는 키를 알아내는 것은 계산 상 불가능하다. 즉, $I_i$구간에는 $K_{i-2}$값만 노출되어있고, $K_{i-2}$값으로 $K_i$를 계산할 수 있어야 $P_{j+1}$의 MAC 값을 변경시킬 수 있게 된다.

## Ⅲ. 관련 연구

무선 애드혹 네트워크에서 메시지 송신 인증 방안으로 제안된 기법은 LHAP, LAP, HEAP 기술이 있다. LHAP과 LAP 기술은 TESLA 방식에 적용된 일방향 체인 기술에 기반을 두고 있다.

TESLA는 인프라 기반 네트워크에서 메시지를 전달하고자 하는 종단간의 인증 방안으로 MANET에 직접 적용하기는 어렵다. 데이터 종단에서만 송신을 확인하는 방식은 많은 보안 위협에 노출 될 수 있다[4]. MANET은 네트워크 인프라를 이용하여 종단간에 데이터를 주는 기존의 통신 방식이 아닌 일반 노드들이 협업하여 데이터를 종단까지 릴레이해주는 구조를 갖는다. 즉, MANET은 경로를 구성하는 모든 홉이 일반 노드이므로 홉 기반 인증방안이 요구된다. 또한 TESLA의 보안성은 종단 단말 간의 시간동기 (loosely time synchronization) 여부에 의존하고 있는데 중앙 제어 장비에 의존하지 않는 MANET에서는 모든 노드들이 시간의 동기를 맞춘다는 것은 어려운 문제다.

LHAP는 상기 기술한 TESLA를 MANET에 적용했을 때 발생할 수 있는 문제점을 고려한 애드혹 네트워크에 특화된 홉 기반 데이터 인증 기술이다. 데이터 송신은 사전에 두 개의 키 체인 (즉, TRAFFIC 키와 TESLA 키 체인)을 생성하고, 통신전에 자신의 1홉에 위치한 이웃 노드들과 공개키 기반 인증 방식을 통해 공유한다. 송신이 전달하는 메시지는 식 (1)의 형식을 갖는다.

$$A \rightarrow *: M, K_A^F(i) \quad (1)$$

식 (1)에서 *는 모든 이웃 노드들에게 전송함을 의미하고, $K_A^F(i)$는 TRAFFIC 키 체인을 통해 인증할 수 있는 값이다. 이를 위해 노드 A는 MANET에 JOIN했을 때 인증 과정에서 사용될 검증값으로 식 (2)와 같은 형식의 메시지를 주변 노드들에게 전송한다.

$$Cert_A, Sign_A[A|K_A^T(0)|K_A^F(0)|T_A^T(0)|T_A^F(0)] \quad (2)$$

식 (2)에서 $K_A^T(0)$은 향 후 KEYUPDATE 메시지에서 TRAFFIC 키를 갱신하기 위해 사용되는 TESLA 키 체인의 검증값이고, $T_A^F(0)$와 $T_A^T(0)$는 각 키의 시작 시간을 나타낸다.

LHAP 방식의 문제점은 웜홀(wormhole) 공격과 중

간자(man in the middle) 공격이 가능하다는 것이다. 특히, 전송하는 메시지 자체가 인증값을 생성하는 요소로 작용되지 않으므로 내/외부 공격자의 협업을 통해 웜홀 공격이 쉬워질 수 있다.

LAP 역시 MANET에 특화된 홉 기반 데이터 인증 기술로서 단방향 키 체인을 주요 기반으로 삼고 있다. LHAP와 달리 LAP 방식에서는 전달하는 메시지를 MAC 값을 계산하는 요소로 사용하고 있고 두 개가 아닌 하나의 키체인을 기반으로 동작한다. 메시지 인증을 위해 노드 A가 MANET에 JOIN할 때 식 (3)과 같은 형식의 메시지를 주변 노드에게 전송한다.

$$A \rightarrow *: Cert_A, [A|h_n^A|H_A], Sign_A(A, h_n^A, H_A) \quad (3)$$

여기서 $h_n^A$과 $H_A$는 단방향 키체인의 검증값과 사용될 보안 해쉬함수를 나타낸다. 이 후, 메시지 전송을 요할 경우 노드 A는 다음과 같은 형식으로 데이터를 보낸다. $A \rightarrow B: M, MAC(M, h_i^A)$, 여기서 M은 전송하고자 하는 메시지이고, $h_i^A$는 현재 노드 A가 사용하고 있는 키값으로 아직 노출된 값은 아니다. 따라서 노드 B는 노드 A로부터 KEYUPDATE 메시지를 통해 전송되는 $h_i^A$가 있어야 인증값을 검증하게 된다.

LAP는 TESLA와 같이 일정 시간 후 노출되는 키값을 인증 검증을 위해 사용하여 종단 입장에서 겪는 총 지연이 단점이 된다. 또한 KEYUPDATE 메시지를 받기까지 수신 받은 데이터를 저장하고 있어야 하므로 DoS 공격에 취약하다.

HEAP는 LAHP와 LAP와 달리 HMAC이나 NMAC의 내부 계산방식을 이용하여 홉 단위 인증을 수행한다. 노드들은 MANET에 JOIN 할 때, 모든 노드들이 갖는 그룹키인 $iKey$를 공유해야 하고 1 홉 이웃 노드들과는 개별 비밀키에 해당하는 $oKey$를 공유해야 한다. 공유된 두 키는 식 (4)에 나타낸 것처럼 HMAC을 계산할 때 사용 된다 (즉, inner key와 outer key).

$$HMAC(M, K) = H(oKey|H(iKey|M)) \quad (4)$$

식 (4)의 HMAC 계산 방식에서 알 수 있듯, HEAP 방식에서는 HMAC 계산 시 긴 메시지는 $iKey$ 만으로 연산이 수행되고, 이후 $oKey$로 최종 인증값이 계산되기 때문에 효율적일 수 있다. 그러나 이 방식의 단점은 메시지를 브로드캐스팅 해야 할 경우 (예, 라우팅의 제어메시지 전달) 각 이웃 노드들 별로 인증값을 개별 계산해야 한다는데 있다. 또한 MANET은 일반적으로 노드가 이동하는 환경을 생각해야 한다. 이동성이 잦을 경우 LAHP나 LAP와 달리 HEAP 방식은 모든 이웃 노드들과 키를 공유하기 위해 연산량이 큰 공개키 기반 키 공유 방식을 각각 사용해야 하므로 성능이 저하될 수 있다.

## IV. 제안 기법

WMN에 적용할 수 있는 데이터 인증기술을 그림 3에 나타낸 네트워크 상황을 예로 설명한다. A, B, C 그리고 D는 일반 사용자 노드들로 데이터의 송신, 수신 및 릴레이 노드로 동작한다. WMR1과 WMR2는 무선 메쉬 라우터로 데이터의 송수신 역할이 아닌 데이터 릴레이 기능만을 수행하여 무선 백본을 형성한다. 무선 영역에서의 간섭을 줄이고 백본을 형성하기 위해 WMR간의 통신은 다른 주파 대역을 쓰는 무선 기술로 설정한다. 예로 노드간 통신은 2.4GHz 대역을 쓰는 IEEE 802.11b 기술을 적용하고 WMR 간의 통신은 5GHz를 사용하는 IEEE 802.11a를 적용한다.

기존에 제안되어있는 방안들(즉, LHAP, LAP, HEAP)처럼 제안하는 인증 방안에서도 노드들이 MANET에 JOIN하기 전에 믿을 수 있는 기관 (즉, TCA: Trusted Certificate Authority)으로부터 인증된 공개키 인증서를 사전에 배포 받았다고 가정한다. 또한 많은 연산량이 요구되는 공개키 기반 방식은 보안 설정 단계에서만 사용되고, 패킷 단위의 데이터 송신 인증은 빠르게 계산되는 MAC을 적용하여 수행한다.

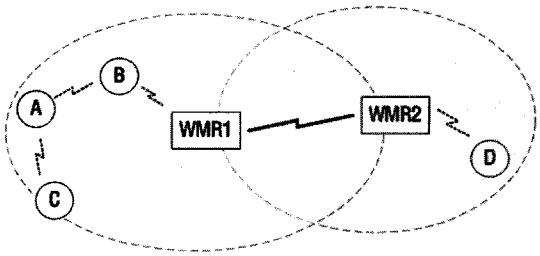


그림 3. 네트워크 시나리오
Fig. 3. Network scenario.

### 1. 일반 노드들의 사전 보안 설정

MANET에 JOIN한 노드 A는 인증 기술을 적용하기 위해 자신의 이웃 노드들에게 사전 보안 설정 요청 단계를 거친다. 노드 A가 주변 노드들에게 브로드캐스팅

$$AK_1 \xrightarrow{H(\bullet)} AK_2 \quad \cdots\cdots \quad \xrightarrow{H(\bullet)} AK_{n-1} \xrightarrow{H(\bullet)} AK_n$$

그림 4. MAC 키 해쉬 체인
Fig. 4. MAC key hash chain.

하는 메시지는 다음과 같다.

$$A \rightarrow *: [SM_A \mid Cert_A \mid Sign_A(SM_A)], \\ where\ SM_A = ID_A \mid MAC(\bullet) \mid H(\bullet) \mid AK_i \mid i \quad (5)$$

식 (5)에서 $Cert_A$와 $Sign_A(SM_A)$는 전송 노드 A의 인증서와 개인키로 서명한 값을 나타낸다. 서명되는 메시지 $SM_A$의 구성 요소들을 왼쪽에서 오른쪽으로 정합(concatenation)된 순으로 나타내면, 자신의 ID, 사용할 MAC 및 해쉬 함수의 종류, 키체인의 인증값, 해쉬 체인에서 인증값의 인덱스이다. 최초에 JOIN하는 노드의 경우 해쉬 체인의 위치는 전체 체인 크기에 해당하는 값이 된다. 즉, 해쉬 체인의 구성 값이 총 $n$개인 경우 $i$는 $n$이 된다. 따라서 노드 A가 초기 설정 단계 이후 사용하는 키값은 $AK_n$을 통해 유효성이 검증될 수 있다. 그림 4는 인증에 사용되는 키 체인을 나타낸다.

그림 4를 통하면 $AK_{n-3}$의 유효성을 검증하기위해 수신자는 $AK_{n-3}$을 3번 해쉬하여, 그 결과가 $AK_n$과 같은지 확인한다. 해쉬 함수의 일방향성으로 인해 공격자는 $AK_n$을 알고 있더라도 $AK_{n-3}$을 유추하기는 계산 상 불가능하다.

노드 A의 사전 설정 요청 메시지는 B와 C가 받게 된다. B를 통해 설명하면, B는 식 (6)에 나타낸 형식의 메시지를 A에게 응답 메시지로 전송한다.

$$B \rightarrow A: [SM_B \mid Cert_B \mid Sign_B(SM_B)] \quad (6)$$

이때 사용되는 $SM_B$의 구성요소는 A가 B에게 준 것과 같은 형식을 따른다. 단, B가 현재 사용하고 있는 키체인의 인증값과 인덱스는 B가 MANET에 JOIN된 초기 상태가 아닌 경우이므로 $n$보다 작은 값이 된다.

## 2. WMR간의 사전 보안 설정

WMN의 백본을 형성하는 WMR은 일반 노드가 아닌 준 인프라로 사용되는 장비로서, 애드혹 네트워킹이 필요할 때 서비스 제공자나 관리자가 통신 지역에 사전 설정한다. 앞서 기술한 것처럼 WMR은 데이터를 생성하거나 최종 데이터 수신자 역할은 수행하지 않는다. 따라서 단일 서비스 제공자에 의해 구성되는 WMN의 경우, 관리자가 사전에 WMR의 안전한 저장영역에 MAC의 계산에 사용되는 비밀키를 저장해 놓을 수 있다. 또한, 네트워크 운영 중 정책에 따라 세션키를 재분배 할 수도 있다.

안전하게 통신 주체 간에 세션키를 분배할 수 있는 방식은 Diffie-Hellman 방식이 제안된 이후 보안이나 성능 특성을 향상 시킬 수 있는 많은 방식들이 제안되어왔다. SSL/TLS, EAP, SAML 등에 적용되고 있는 SRP[9] 프로토콜이나 실시간 데이터 전송 응용을 위해 적용되는 ZRTP[10], MIKEY[11] 프로토콜 등이 사용될 수 있다.

그러나 응급 재난 지역이나 규모가 있는 국제 전시회와 같은 경우 일정 영역 단위로 통신 서비스 제공자가 달라 질 수 있고, 서로 다른 관리자에 의해 해당 영역의 WMR이 설치되고 운영될 수 있다. 그림 3은 이러한 경우의 예를 나타낸 것으로, WMR1과 WMR2의 관리자가 다르고 WMR2가 통신 영역을 확장하기 위해 새롭게 설치되었다고 가정한다. 이 경우 인증키 설정 방안을 설명하면 다음과 같다. WMR2는 통신 영역에 자신을 JOIN하기 위해 WMR1에게 사전 설정 요청 메시지를 식 (7)의 형식으로 전송한다.

$$WMR2 \rightarrow WMR1: [Cert_{MR2} \mid ID \mid nonce \mid \\ Sign_{MR2}(ID \mid nonce)] \quad (7)$$

요청 메시지를 받은 WMR1은 WMR2의 인증서를 기반으로 전송받은 ID와 nonce의 유효성을 서명값인 $Sign_{MR2}(ID \mid nonce)$을 통해 검증한다. 서명 검정 후, WMR1은 WMR2에게 현재 무선백본에서 사용되고 있는 그룹 세션 키 $sGK$를 다음 형식으로 전송해준다.

$$WMR1 \rightarrow WMR2: [SM_{MR1} \mid Enc_{MR2}(sGK) \mid \\ Cert_{MR1} \mid Sign_{MR1}(SM_{MR1})] \quad (8)$$

식 (8)에서 $Enc_{MR2}(sGK)$는 WMR2 인증서를 통해 전달된 WMR2의 공개키로 암호화한 그룹 세션 키를 나타낸다. 따라서 WMR2 이외의 다른 노드는 sGK를 복호화 할 수 없다. $SM_{MR1}$은 다음 식 (9)의 내용을 포함한다.

$$SM_{MR1} = [ID \mid MAC(\bullet) \mid VT \mid nonce] \quad (9)$$

$SM_{MR1}$의 구성 요소들은 WMR1의 식별 ID, 데이터 인증처리에 사용할 MAC 함수, $sGK$의 유효 시간, 그리고 WMR2가 전송했던 nonce 값이다. 전송된 세션키는 유효 시간동안 사용되고 갱신된다. 또한 nonce를

통해 중간자공격에 대처하고 freshness를 보장해 주게 된다.

식 (8)에 나타낸 것처럼, 세션키를 전달하기 위해 수행되는 암호화하고 인증을 위한 서명의 계산은 빈번하게 수행되는 작업이 아니므로 패킷 단위의 데이터 인증 처리의 성능은 저하되지 않는다.

### 3. Trust 관리

제안하는 인증 방안에서 전송되는 데이터의 안전성은 단방향 키 체인에 의존한다. 따라서 패킷을 보낼 경우 키체인 상의 위치인 인덱스값과 키 체인의 인증값이 갱신되어야 안전하고, 해쉬 함수의 연산량을 줄여 데이터 전송 지연을 줄일 수 있다.

일정기간 데이터를 보내지 않는 노드의 경우 MANET에서 이웃 노드들의 상황을 파악하기 위해 일반적으로 사용하는 HELLO 메시지를 확장하여 trust를 관리한다. HELLO 메시지에 포함되는 정보는 다음과 같다.

$$N \rightarrow NB^{*} : [ID_N | AK_t | i(=t)] \quad (10)$$

이를 받은 주변 노드들(i.e., $NB^{*}$)은 자신이 알고 있는 인덱스 값인 $s$와 전송 받은 t 값을 이용하여 전달받은 $AK_t$값을 $s-t$번 해쉬하여 저장된 $AK_s$와 동일한지 확인한다. 검증 결과가 같은 경우 전송받은 키체인의 인증값과 인덱스를 해당노드의 것으로 갱신한다.

LAP와 같은 기존 인증 방안에서는 주기적으로 trust 관리를 위해 KEYUPDATE 메시지를 전송한다. 그러나 제안하는 방식에서는 데이터를 전달할 것이 없는 노드들만 키체인의 인증값을 전송한다. 이유는 제안하는 인증 방식은 준인프라 구조의 WMN을 대상으로 하기 때문이다. WMN에서는 네트워크 성능을 높이기 위해 하나의 WMR가 관리하는 영역에서는 proactive한 MANET 라우팅 프로토콜이 사용되고, 다른 WMR이 관리하는 노드로의 데이터 전달은 reactive한 라우팅 방식을 적용 한다[8]. 이 경우 한 도메인 내부에는 내부 경로 정보를 확인하기 위해 주기적으로 HELLO 메시지가 전송되므로 제안 방식에서는 별도의 KEYUPDATE 메시지 대신 전송되는 HELLO 메시지를 확장 적용하는 것으로 제어 오버헤드를 줄여준다.

### 4. 메시지 인증

MAC은 전송 받은 데이터의 무결성을 검증하기위한 효율적인 보안 프리미티브이다. MAC을 적용한 인증 방식에서 송신자는 수신자와 사전에 공유한 비밀키 $sK$를 이용하여 각 패킷 $P_i$에 인증값으로 계산된 $MAC(P_i, sK)$을 첨부하여 전송한다. 이 방식을 애드혹이나 메쉬네트워크의 일반 송.수신 노드에 변경 없이 적용하는 것은 성능 및 키 분배 문제로 인해 어렵다. 네트워크를 구성하는 노드의 수가 $n$일 경우 모든 노드들은 $n(n-1)/2$의 키를 관리하고, 자신의 키를 $n-1$ 노드들에게 안전하게 분배해야하기 때문이다. 따라서 제안하는 인증 시스템은 MANET을 구성하는 구간과 무선 백본을 구성하는 구간에 다른 방식을 적용하여 메시지 인증을 수행한다.

그림 3에 나타낸 환경에서 노드 A가 노드 D에게 메시지를 전달한다고 가정하면 매 홉 단위로 다음과 같은 메시지 인증이 수행된다. 노드 A는 노드 B에게 식 11과 같은 형식의 패킷을 전송한다.

$$A \rightarrow B : [M_i | i | AK_p | p | MAC(AK_{p+1}, M_i | i | p)] \quad (11)$$

여기서 $i$는 메시지의 일련번호이고 $p$는 노출하는 키 $AK_p$의 키체인 상의 인덱스 값이다. 이를 받은 B는 IEEE 802.11 기반 무선 접속 기술에서 수행하는 ACK 메시지를 식 (12)와 같은 형식으로 확장하여 전송한다.

$$B \rightarrow A : [ACK_i | AK_q | q | MAC(AK_{q+1}, ACK_i | q)] \quad (12)$$

식 (11)과 (12)를 통해 나타낸 것처럼 제안하는 방식에서 인증키의 노출은 다음패킷을 통해 지속적으로 수행한다. 이는 TESLA나 LAP와 같이 수 ms 단위로 기다린 후 노출할 경우 DoS 공격에 취약하기 때문이다. 특히, 저장 공간의 문제보다 실시간 전송의 요구사항이 큰 응용의 경우 기존 방식은 적용하기가 어렵다. 제안하는 방식의 단점은 노드들이 사전에 키체인을 만들고 저장해야 되는 부담이 있다. 그러나 [12]에 제안된 기법을 적용하면 효율을 높일 수 있다.

만약 전달하는 패킷이 마지막인 경우 HELLO 메시지를 통해 전 패킷의 키를 전달해 준다. B와 WMR1의 홉에서도 위의 방식과 동일한 절차로 인증을 수행한다.

WMR1과 WMR2의 인증 방식은 일반 노드의 방식과 달리 사전에 공유된 그룹 세션키를 이용하여 인증값을 생성하게 된다. 또한 단방향 키 체인을 사용하지 않으

므로 데이터가 도착하는 즉시 검증 연산을 수행할 수 있다. 전달되는 패킷의 형식은 다음과 같다.

$$WMR1 \rightarrow WMR2 : [Mi|i|MAC(sGK, Mi|i)] \quad (13)$$

WMR2와 D 간의 메시지 인증은 A와 B의 인증방식과 동일하게 수행된다.

## V. 보안 및 성능 분석

### 1. 보안 분석

기존에 제안된 종단간의 인증 시스템은 (예, TESLA) 통신 인프라가 사전에 구성되어 있는 네트워크를 가정하고 있다. 종래의 네트워크를 구성하는 인프라 장비는 서비스 관리자에 의해 일반 사용자 시스템보다 보안 관점에서 취약성이 적다. 그러나 본 논문에서 제안하는 인증방식은 WMN을 위한 방안이다. WMN은 인프라 장비도 있지만, 일반 사용자 노드들로 구성되는 MANET이 존재한다. 따라서 경로를 구성하는 사용자 노드들을 기존 인프라 장비와 동일하게 취급하여 종단간에만 인증을 수행하는 방식은 적합하지 않다. 따라서 제안 방식과 같이 홉 단위의 인증을 수행하는 방안이 보안 취약성을 줄이게 된다.

본 논문에서 제안하는 인증시스템은 노드가 WMN에 JOIN할 경우 디지털서명을 통해 주변 노드들과 trust 관계를 생성하고, 인증에 사용될 단방향 키체인의 인증키값을 배포한다. 이를 통해 중간공격 및 재전송 공격에 대응할 수 있다. 또한 키체인을 생성하는 보안 해쉬함수의 일방향성으로 인해 공격자가 향 후 사용될 키를 유도하는 것은 계산상 불가능하다.

기존에 제안되었던 LHAP 시스템에서는 전달하는 인증 패킷에 송신을 인증할 수 있는 키만을 추가하여 전송한다. 따라서 전송 받은 키값의 인증은 보장되나 메시지 자체는 인증되지 못하고, 무결성 또한 제공할 수 없다. 본 방식에서는 데이터를 전달할 경우 메시지와 일련번호에 MAC을 계산하여 송신 인증 및 무결성을 제공하고 재전송 공격을 방어할 수 있다.

IEEE 802.11 기반 무선 접속 기술에서 메시지를 받은 수신자는 ACK 메시지를 전달하게 된다. 본 인증 시스템은 ACK 메시지를 받은 송신자가 다음 메시지를 통해 직전 패킷의 인증키를 노출하게 되므로 중간자 혹은 복수의 중간자들이 협업하는 웜홀 공격이 수행되기는 어렵다. 802.11기반 규격에 따라, 메시지가 전달된 후 다른 메시지의 전송보다 ACK 메시지의 전송이 우선시된다. 즉, 무선 구간에서 송신자가 메시지를 전달할 때 다른 데이터를 전달하고자 하는 타 송신노드가 있더라도, 수신자의 ACK 메시지가 먼저 전송된다. 따라서 중간자가 메시지를 가로채더라도 메시지를 위조하기가 어렵다.

### 2. 시스템 성능

MAC을 사용한 인증방식은 디지털서명 기법을 사용하는 방식보다 적은 계산량과 전송해야 하는 인증정보의 양이 적어서 효율적이다. 특히, 전송하고자 하는 데이터를 패킷 단위로 디지털 서명 작업을 하는 것은 효율성을 크게 저하시키는 방식이다. 본 논문에서 제안하는 방식은 초기 설정 단계에서만 디지털서명 기법을 사용하고, 이후 패킷단위 인증자의 계산은 상대적으로 빠른 MAC을 계산하여 전송하는 것으로 계산 및 전송 효율을 높였다.

경로 상에 위치한 전송 노드들의 성능은 MAC 계산을 위해 사용되는 키체인의 크기에 따라 달라진다. 키체인을 구성하는 랜덤 값의 크기가 클수록 노드가 계산해야 하는 양과 계산된 랜덤값을 저장하기위해 요구되는 저장 공간의 크기도 커진다. 키체인을 구성하는 랜덤 값들은 사전에 계산되어 저장된 후 사용하거나, 필요한 시점에 계산하여 사용하는 방식이 있다. 또한 성능을 높이기 위해 두 방식을 섞어서 적용할 수도 있다 [7]. 키체인을 사용하는 암호시스템의 효율성은 [12]에 제안된 방식을 적용할 경우 높아진다. $N$개의 랜덤 값으로 구성된 단방향 키체인을 사용하는 시스템의 경우 $\log(N)$의 저장공간과 $\log(N)$의 계산량이 필요하다. 효율성을 높이기 위한 또 다른 방법은 키가 사용되는 유효시간의 크기를 크게 하여 (즉, 키노출 시간을 크게 함) 하나의 랜덤 키 값으로 복수개의 패킷들의 MAC 계산에 사용하는 것이다. 이 방식의 경우, 데이터 수신단에서 키가 노출되는 시간만큼 도착한 패킷을 보관해야 하는 단점이 있다. 특히, 수신단에서 많은 패킷을 보관한 후 연산을 수행해야하는 방식은 DoS 공격에 취약해진다.

제안한 방식에서는 인증 키 노출 시간을 줄여 홉 단위의 지연값을 줄였다. 또한 인프라 역할을 수행하는 WMR간에는 사전에 공유된 그룹세션키를 사용하여 즉시 인증값을 검증할 수 있도록 하였다. 따라서 기존 제안 방식인 LAP와 LHAP를 WMN에 직접 적용한 경우

보다 종단간의 지연을 크게 줄일 수 있다.

## VI. 결 론

본 논문에서는 준인프라 구조의 MANET이나 무선 메쉬네트워크에 적용할 수 있는 메시지 인증 기술을 제안했다. 제안하는 방식은 공개키 기반 방식보다 계산 및 전송 효율이 우수한 MAC 프리미티브를 사용했다. 또한, 브로드캐스팅을 기본으로 하는 무선 영역에서 안전하게 MAC의 비밀키를 사용할 수 있도록 단방향 키 체인 기술을 기반으로 하고 있다. 제안 방식은 단방향 키 체인을 기반으로 메시지를 인증하는 기존에 제안되었던 방식들의 보안 취약성을 개선했다. 또한, 실시간 데이터를 전송해야 하는 응용에 적합하도록 종단간의 전달 지연시간을 감소시킬 수 있다.

## 참 고 문 헌


[1] IETF MANET (Mobile Ad hoc Networks) Working Group, MANET Charter's page in http://www.ietf.org/html.charters

[2] R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," IEEE Com. Mag., pp. 123-131, Mar. 2005.

[3] Y. Hu, A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy vol.2(3), pp. 28-39, May/June 2004.

[4] R. Akbani, T. Korkmaz, G. Raju, "HEAP: A Packet Authentication Scheme for Mobile Ad hoc Networks," Ad Hoc Networks vol. 6(9), pp. 1134-1150, September 2008.

[5] S. Zhu, S. Xu, S. Setia, Z. Jajodia, "LHAP: a lightweight network access control protocol for ad-hoc networks," Ad Hoc Networks Journal vol.4(5), pp. 567 - 585, May 2006.

[6] B. Lu, U.W. Pooch, "A lightweight authentication protocol for mobile ad hoc networks," International Journal of Information Technology, vol11(2), pp. 119-135, February 2005.

[7] A. Perrig, R. Canetti, J. Tygar, D. Song, "Efficient and Secure Source Authentication for Multicast," in Proc. of the Network and Distributed System Security Symposium (NDSS), pp. 35-46, February 2001.

[8] N. Kang, S. Yoo, Y. Kim, S. Jung, K. Hong, "Heterogeneous Routing Protocol Coordinator for Mobile Ad Hoc Networks," in Proc. of UCS 2006, LNCS 4239, pp. 384-397, October 2006.

[9] T. Wu, "The SRP Authentication and Key Exchange System," IETF RFC 2945, September 2000.

[10] P. Zimmermann, A. Johnston, J. Callas, "ZRTP: Media Path Key Agreement for Secure RTP," IETF Intenet-Draft, January 2010.

[11] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman, "MIKEY: Multimedia Internet KEYing," IETF RFC 3830, August 2004.

[12] D. Coppersmith and M. Jakobsson, "Almost optimal hash sequence traversal," in Proc. of the Fourth Conf. on Financial Cryptography, Lecture Notes in Computer Science, vol. 2357, pp. 102-119, 2003.


### 저 자 소 개


강 남 희(정회원)-교신저자

1999년 숭실대학교 정보통신공학 학사졸업

2001년 숭실대학교 정보통신공학 석사졸업

2005년 Siegen University (독일) 컴퓨터공학 박사

2006년 다산네트웍스 선임연구원

2007년 가톨릭대학교 컴퓨터정보공학부 초빙교수

2009년 덕성여대 컴퓨터공학부 전임강사

<주관심분야 : 유무선통신, 시스템, 인터넷보안>