[UCI]I804:24011-200000235890

2008년 2월
박사학위 논문

MANET 환경에서 강인한 OTP-EKE 인증기법

조선대학교 대학원

컴 퓨 터 공 학 과

이 철 승

MANET 환경에서 강인한 OTP-EKE 인증기법

A Robust OTP-EKE Authentication Scheme in MANET Environments

2008년 2월 일

조선대학교 대학원

컴 퓨 터 공 학 과

이 철 승

MANET 환경에서 강인한 OTP-EKE 인증기법

지도교수 : 이 준

이 논문을 공학 박사 학위신청 논문으로 제출함

2007년 11월 일

조선대학교 대학원

컴 퓨 터 공 학 과

이 철 승

이철승의 박사학위 논문을 인준함.

위원장 조선대학교 교수 나 상 동

위 원 조선대학교 교수 조 범 준

위 원 조선대학교 교수 金 忠 源

위 원 조선대학교 교수 김 판 구

위 원 조선대학교 교수 李 俊

2007년 12월 일

조선대학교 대학원

목 차

List of Titles

표 목 차 ..... *iii*

도 목 차 ..... *iv*

약 어 ..... *vi*

ABSTRACT ..... *viii*

Ⅰ. 서 론 *1*

Ⅱ. *MANET* 보안 환경 및 인증기법 *3*

A. AODV 라우팅 프로토콜 *5*

B. 위협과 공격유형 *10*

C. MAENT 인증기법 *12*

*1. OTP*를 이용한 인증기법 *14*

*2. OTP*를 이용한 인증기법의 문제점 *23*

Ⅲ. 패스워드 기반 키 교환 프로토콜 *26*

A. 패스워드 암호화를 위한 세션키 생성 *27*

B. 세션키를 이용한 인증키 교환 프로토콜 *30*

1. EKE 프로토콜 *32*

2. DH-EKE 프로토콜 *35*

Ⅳ. *OTP-EKE* 인증기법 39
A. OTP-EKE 보안 요구사항 42
B. 안전한 통신 경로 확보를 위한 라우팅 44
1. 라우팅을 위한 해시테이블 생성 46
2. 라우팅 탐색 및 설정 47
3. 라우팅 유지 및 관리 53
C. 인증을 위한 검증 및 키 교환 55
1. SN 등록 및 검증 56
2. 인증키 교환 단계 58

Ⅴ. *OTP-EKE* 인증기법 실험 및 결과분석 63
A. 시뮬레이션 환경 64
1. NS2 시뮬레이터 65
2. MANET 모델 설계 68
B. 시뮬레이션 결과 분석 70
*1. SN*의 검증자 생성 및 전송 71
2. 인증키 교환 72
C. OTP-EKE 인증기법의 안전성 및 효율성 분석 77
1. 안전성 분석 및 검증 77
2. 효율성 분석 81

Ⅵ. 결 론 88
【참 고 문 헌】

표 목 차

List of Tables

표 1. MD5 매개변수 ····· 17
표 2. MANET OTP 인증기법의 특징과 문제점 ····· 25
표 3. 패스워드 기반 키 교환 프로토콜 ····· 31
표 4. EKE 프로토콜에 사용되는 계수 ····· 32
표 5. DH-EKE 프로토콜에 사용되는 계수 ····· 35
표 6. OTP-EKE 인증 기법에 사용되는 계수 ····· 55
표 7. 시뮬레이션 환경 ····· 64
표 8. 원시근 2의 값 ····· 80
표 9. 전송횟수와 연산량 ····· 81

도 목 차

List of Figures

그림 1. MANET의 독립된 구조 ····· 4
그림 2. MANET 라우팅 프로토콜 ····· 6
그림 3. 경로탐색 초기화 ····· 7
그림 4. RREP 경로설정 ····· 8
그림 5. AODV 라우팅 프로토콜 ····· 9
그림 6. MANET 공격유형 ····· 11
그림 7. MANET 환경의 인증기법 ····· 13
그림 8. OTP의 예 ····· 15
그림 9. 해시함수 ····· 16
그림 10. 시간동기 인증기법 ····· 19
그림 11. 시도응답 인증기법 ····· 20
그림 12. OTP S/Key 인증기법 ····· 22
그림 13. Diffie-Hellman 키 교환 ····· 29
그림 14. 패스워드 기반의 EKE 프로토콜 ····· 34
그림 15. 패스워드 기반의 DH-EKE 프로토콜 ····· 38
그림 16. MANET 기반 OTP-EKE 수행절차 ····· 41
그림 17. MANET OTP-EKE 인증 요구사항 ····· 43
그림 18. OTP-EKE 인증기법의 라우팅 단계 ····· 45
그림 19. MN들의 해시테이블 ····· 46
그림 20. *H(RREQ)* 메시지 ····· 47
그림 21. 라우팅 경로탐색 ····· 49
그림 22. *H(RREP)* 메시지 ····· 50
그림 23. *H(AODV)* 경로설정 과정 ····· 51
그림 24. 라우팅 경로설정 ····· 52

그림 25. *H(RRER)* 메시지 ····· 53
그림 26. 라우팅 경로유지 ····· 54
그림 27. 등록 단계 ····· 56
그림 28. 검증 단계 ····· 57
그림 29. SN과 DN사이의 키 교환 ····· 61
그림 30. OTP-EKE 인증절차 ····· 62
그림 31. NS-2.29 구조 ····· 66
그림 32. NS-2.29 클래스 계층구조 ····· 67
그림 33. MANET 모델 설계 ····· 69
그림 34. 실험결과 ····· 70
그림 35. SN과 DN의 해시코드 ····· 75
그림 36. NAM을 이용한 시뮬레이션 실행 ····· 76
그림 37. 시간에 따른 패킷 전달률 ····· 83
그림 38. 악의적인 노드가 있는 경우의 패킷 전달률 ····· 84
그림 39. 시간에 따른 라우팅 오버헤드 ····· 86
그림 40. 악의적인 노드가 있는 경우 라우팅 오버헤드 ····· 87

약 어

Notation	*Description*
AMP	Authentication via Memorable Password
AODV	Ad-hoc On-demand Distance Vector
AP	Access Point
ARP	Address Resolution Protocol
CA	Certificate Authority
CBR	Constant Bit Rate
DES	Data Encryption Standard
DH	Diffie Hellman
DN	Destination Node
DLP	Discrete Logarithm Problem
DOS	Denial of Service
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
EKE	Encrypted Key Exchange
EtoE	End to End
IA	Interface Address
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
LHAP	Lightweight Hop-by-Hop Authentication Protocol
LL	Link Layer
MAC	Message Authentication Code
MAC	Media Access Control
MANET	Mobile Ad-hoc Networks
MD	Message Digest

약 어 (계속)

Notation	*Description*
MN	Mobile Node
NN	Neighbor Node
OLSR	Optimized Link State Routing
OTcl	Object Tool Command Language
OTP	One Time Password
PFS	Perfect Forward Secrecy
PIN	Personal Identification Number
PKG	Private Key Generator
PKI	Public Key Infrastructure
RERR	Route Error
RFC	Request For Comments
RREP	Route Reply
RREQ	Route Request
SHA	Secure Hash Algorithm
SN	Source Node
SPEKE	Secure Password Exponential Key Exchange
SRP	Secure Remote Password
TBRPF	Topology Dissemination Based on Reverse-Path Forwarding
TCL	Tool Command Language
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunication System
WG	Working Group
WLAN	Wireless Local Area Network

ABSTRACT

A Robust OTP-EKE Authentication Scheme in MANET Environments

Lee, Cheol-seung
Advisor : Prof., Lee Joon, Ph. D.
Department of Computer Engineering
Graduate School of Chosun University

Recently demands in construction of the stand-alone networks and interconnection between convergence devices have led an increase in research on IETF MANET working group, Bluetooth, and HomeRF working group and much attention has been paid to the application of MANET as a Ubiquitous network which is growing fast.

With performance both as hosts and routers, easy network configuration, and fast response, mobile nodes participating in MANET are suitable for Embedded computing, but have vulnerable points, such as lack of network scalability and dynamic network topology due to mobility, passive attacks, active attacks, which make continuous security service impossible. MANET has no fixed infrastructure and lack of CA leads to mobile nodes cooperative key distribution and key management, resulting in higher risk of attack by malicious nodes.

Authentication of mobile nodes in IETF MANET working group using Threshold encryption authentication technique, LHAP authentication technique, PKI authentication technique, and One Time Password authentication technique is

available but research is conducted on it on the assumption that it is safe. So, routing security and authentication are not perfect. For perfect MANET setting, very reliable authentication is required which can guarantee security and efficiency through secure routing.

This study analyzes MANET authentication techniques to solve security vulnerabilities and suggests a very reliable OTP-EKE authentication technique providing authentication, confidentiality, integrity, availability and non-repudiation service. OTP-EKE authentication technique consists of routing for securing safe communication path, and verification and key exchange for source node authentication. In routing, hashed AODV is used to protect from counterfeiting messages by malicious nodes in the course of path finding and setting, and disguising misrouted messages as different mobile nodes and inputting them into the network. In verification and key exchange, EtoE session keys are set and safe exchange of session keys are performed through encryption as a verifier of the hashed password for safe packet transmission and data encryption using OTP S/key authentication technique and DH-EKE to verify source node's possession of the password.

The Linux-based NS2 simulator is used for testing the OTP-EKE authentication technique. Stability and efficiency are measured through comparing the authentication mechanisms using OTP S/Key authentication technique performing the AODV routing, DH-EKE authentication technique performing the H(AODV) routing, and the proposed OTP-EKE authentication mechanism.

The result shows that routing messages are protected from counterfeiting and routing may be secured against impersonation and eavesdropping. Security can be achieved against a replay attack, a man-in-the-middle attack, password guessing, Denning-sacco, and a Stolen-verifier attack. For determining efficiency exponent operation, packet delivery fraction and routing overhead are measured. The numbers of message transmission, encryption, and exponent operation are lowered by one

respectively than those of DH-EKE authentication technique. Packet transmission rate can be said to be effective because existing AODV routing protocols and approximate packet transmission rate after 400 seconds are achieved. Measurement of routing overhead shows increase in overhead for path search, resulting from no intervention of malicious nodes. With man-in-the-middle attacks by malicious nodes, the proposed authentication can be more effective than the current mechanism because of the decrease in the routing overhead. Therefore, OTP-EKE authentication mechanism can be said to be a very reliable authentication technique with enhanced security and efficiency.

Ⅰ. 서 론

최근 독립된 네트워크의 구성 및 다양한 컨버전스 디바이스간 상호연결에 대한 요구로 MANET의 연구는 IETF MANET WG[1], Bluetooth[2], HomeRF WG[3]에서 활발하게 진행되고 있으며, 유비쿼터스 컴퓨팅 활용은 많은 주목과 고도의 성장을 보이고 있다[4].

MANET에 참여하는 MN들은 호스트와 라우터 기능을 동시에 수행하여 네트워크 환경설정이 쉽고 빠른 대응력으로 임베디드 컴퓨팅에 적합하지만 MN의 이동성으로 인한 동적 네트워크 토폴로지, 네트워크 확장성 결여 그리고 수동적·능동적 공격에 대한 취약성을 지니고 있어 지속적인 보안 서비스를 관리할 수 없다[5]. 또한 고정된 인프라가 없고 CA의 부재로 네트워크에 참여하는 MN들은 협력적인 키 분배 및 관리를 수행해야 하며 악의적인 노드의 공격 대상이 된다.

IETF MANET WG에서는 MN의 보안 인증을 위해 Threshold 암호화 인증기법[6], 계층적 분산구조 인증기법[7], LHAP 인증기법[8], PKI 인증기법[9] 그리고 OTP를 이용한 인증기법[10] 등이 연구되고 있지만, MANET 인증기법들은 MN들을 신뢰한다는 가정 하에 연구가 되고 있어 네트워크 경로설정을 위한 라우팅 보안과 신뢰할 수 있는 MN 인증기법은 미비한 실정이다[11]. 완전한 MANET 환경을 위해서는 보안 라우팅을 통한 경로설정의 안전성과 효율성이 보장되어야 하며 신뢰할 수 있는 강인한 MN 인증기법이 필요하다.

본 논문은 MANET에서 발생하는 보안의 취약성을 해결하기 위해 MANET 라우팅과 인증기법을 분석하고 인증, 기밀성, 무결성, 가용성 그리고 부인봉쇄 서비스를 제공하는 신뢰성이 강한 OTP-EKE 인증기법을 제안한다.

OTP-EKE 인증기법은 안전한 통신경로 확보를 위한 라우팅 단계와 SN 인증을 위한 검증 및 키 교환 단계로 구성하였다. 라우팅 단계에서는 경로탐색 및 경로설정 시 악의적인 노드가 라우팅 메시지를 위·변조 하거나 적법한 MN으로 위장하는 공격을 방지하기 위해 AODV 라우팅 프로토콜에 OTP를 적용한 해시된 라우팅 프로토콜을 이용하였다. 검증 및 키 교환 단계에서는 SN의 패스워드 검증과 세션키 교환을 통한 인증을 위해 OTP S/Key 인증기법과 패스워드 기반 키 교환 프로토콜인 DH-EKE를 이용하였다. 안전한 패킷전송과 데이터 암호화를 위한 EtoE 세션키를 설정하고 세션키

교환 시 MD5로 해시된 패스워드 검증자로 암호화하여 안전하게 세션키 교환을 한다.

OTP-EKE 인증기법의 실험을 위해 Linux 기반의 NS2 시뮬레이터를 사용하였고 AODV 라우팅을 수행하는 OTP S/Key 인증기법, 해시된 AODV 라우팅을 수행하는 OTP S/Key 인증기법과 DH-EKE를 적용한 인증기법 그리고 OTP-EKE 인증기법을 비교 분석하여 안전성과 효율성을 측정하였다.

안전성 측정결과 해시된 AODV를 통한 라우팅 메시지의 위·변조 및 악의적인 노드의 위장, 도청에 대한 라우팅 안전성과 DLP 연산을 통해 생성된 세션키와 패스워드 검증자를 이용하여 재전송 공격, 중재자 공격, 패스워드 추측 공격, Denning-sacco 공격과 Stolen-verifier 공격에 대한 키 교환 안전성을 확보할 수 있었다.

효율성 측정을 위해 메시지 전송횟수와 연산량, 패킷 전달률 그리고 라우팅 오버헤드를 측정하였다. 메시지 전송횟수와 연산량 측정결과 지수승 연산을 하는 DH-EKE를 이용한 인증기법보다 메시지 전송횟수, 암호화 횟수 그리고 지수승 횟수가 각 1회씩 감소하였고, 패킷 전달률은 AODV 라우팅을 수행하는 OTP S/Key 인증기법과 해시된 AODV 라우팅을 수행하는 OTP-EKE 인증기법이 400초 후에 유사한 패킷 전달률을 확보할 수 있었다. 하지만 5개의 악의적인 노드가 네트워크에 참여시 OTP S/Key 인증기법은 평균 39.3%의 패킷이 악의적인 노드를 통과하는데 반해, OTP-EKE 인증기법은 평균 20% 미만만이 악의적인 노드를 통과하여 안전성과 효율성을 제공하였다. 그리고 악의적인 노드를 네트워크에 참여시켜 경로탐색을 위한 라우팅 오버헤드를 측정한 결과, OTP S/Key 인증기법은 방대한 플로딩으로 OTP-EKE 인증기법보다 라우팅 오버헤드가 증가하여 OTP-EKE 인증기법이 효율적이었다.

OTP-EKE 인증기법은 MANET상의 라우팅 보안과 MN의 인증 보안을 확보하여 안전성과 효율성을 향상시켰으며 완전한 MANET 환경의 신뢰성이 강한 인증기법이라 할 수 있다.

Ⅱ. *MANET* 보안 환경 및 인증기법

MANET[12]은 MN간에 패킷 데이터를 전송하는 네트워크로 전쟁터, 재난상황, 컨퍼런스 및 회의실 등에서 일시적인 네트워크 구성에 적합한 통신기술이다. 초기 군사적인 응용목적으로 연구가 시작된 MANET은 네트워크 인프라가 구축되지 않는 환경에서 백본망과는 완전히 독립된 형태로 존재하거나 AP나 기지국과 같은 인터워킹 되는 형태로 존재할 수 있다.

그림 1과 같은 독립된 구조의 MANET은 MN간의 주소 자동설정[13]을 통해 IA를 설정하고 호스트와 라우터 기능이 통합된 무선 디바이스로 단일 홉 또는 멀티 홉 형태로 구성된다[14]. MANET은 MN의 이동성과 동적 네트워크 토폴로지에 의한 불안전한 링크, 한정된 주파수 대역과 전송거리에 대한 제약 그리고 MN의 증가로 인한 전파간섭으로 많은 보안상 위험에 노출되어 있다. MN의 라우팅 지원을 백본망에 의존할 수 없어 분산된 조건하에 운영을 해야 하며, MN이 서비스를 분배하고 MN간 협력을 제공해야 한다. 그 밖에도 배터리로 인한 전력제한, 보안 라우팅 프로토콜의 부재 및 멀티 홉 무선 인터페이스의 제한으로 유선 네트워크상의 프로토콜을 그대로 사용할 수 없어 침입이나 오동작으로 인한 심각한 위협과 공격유형이 존재한다[15].

MANET의 보안 연구는 라우팅 보안, 악의적인 노드, 침입탐지가 주된 연구이고, 암호화와 같은 링크레벨 보안기술과 네트워크 계층에서 보안을 적용하는 경우 네트워크 제어정보를 교환하기 전에 MN간 인증을 수행하는 방식 등이 주된 주제가 되고 있다.

MANET WG에서는 DOS 공격을 방지하는 독립 IP[16] 라우팅 프로토콜로 RFC 2501[17], RFC 3513[18], RFC 3561[19], RFC 3626[20], RFC 3684[21]를 채택 하였으며 MANET 보안을 강화하기 위해 공개키 기반의 인증기법들과 OTP를 이용한 인증기법이 연구가 되고 있다. MANET 환경을 고려한다면 인증 프로토콜을 사용하면서 발생할 수 있는 MN의 성능저하 문제점을 고려해야 하며 연산과정이 단순하면서도 이동성을 보장해 줄 수 있는 OTP를 이용한 인증기법이 효율적이다.

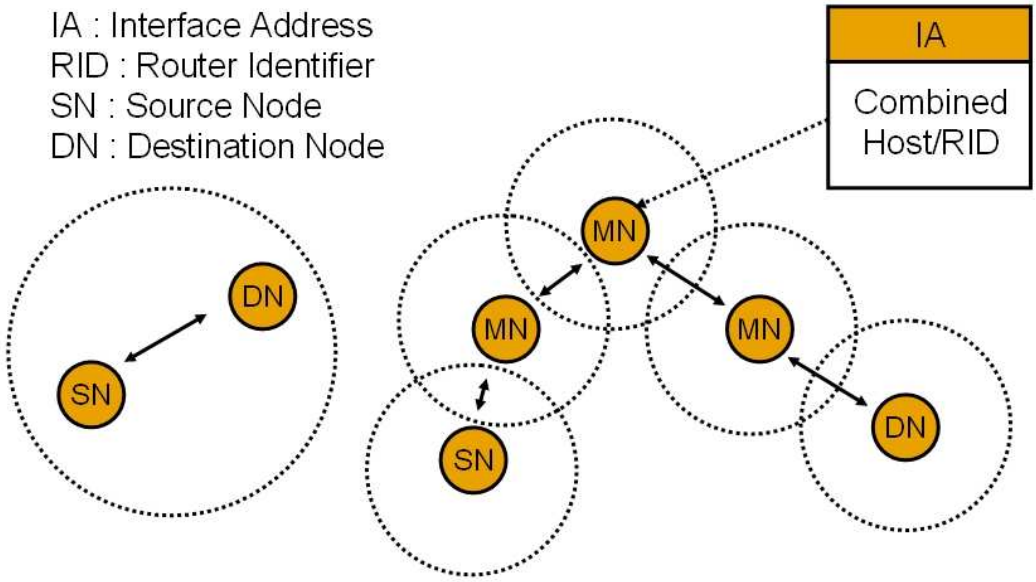


그림 1. MANET의 독립된 구조

Fig. 1. Stand-alone Structure of MANET

A. AODV 라우팅 프로토콜

MANET의 효율적인 경로설정을 위한 라우팅 프로토콜로는 그림 2와 같이 Table-driven 방식, On-demand 방식 그리고 Hybrid 방식으로 나눌 수 있다[22].

Table-driven 방식[23]은 유선 네트워크의 Bellman-ford 방식을 적용한 것으로 주기적인 MN간 경로를 설정해 준다. 각 MN은 도착 가능한 모든 MN의 라우팅 정보를 라우팅 테이블에 상시 유지하여 연결요청이 빠르며, 모든 MN은 주기적으로 라우팅 정보를 플로딩하여 다른 MN의 최신 라우팅 테이블의 정보를 갱신 하도록 유도한다. 또한 Table-driven 방식은 소규모 네트워크에 적합한 장점이 있지만 최신정보 유지로 인한 플로딩 오버헤드가 커지는 단점이 있어 On-demand 방식에 비해 연구 결과가 적은 편이다.

On-demand 방식[24]은 송신할 데이터를 갖는 SN이 DN에 전송요구가 있을 때만 해당 DN의 경로를 탐색, 생성, 유지하는 방식이다. MN의 이동성을 연결 요청시마다 즉시 반영한다는 점에서 보다 정확한 경로설정[25]을 할 수 있고, Table-driven 방식보다 제어 트래픽에 의한 오버헤드를 줄일 수 있어 규모가 큰 네트워크에 적용할 수 있다는 장점이 있다[26]. 하지만 경로탐색을 위한 플로딩 오버헤드가 커지는 단점이 존재한다.

Hybrid 방식[27]은 Table-driven 방식과 On-demand 방식의 장점을 혼합한 방식으로 각 MN이 미리 정의된 영역을 유지하기 위해서는 Table-driven 방식을 사용하고, 외부영역에서는 On-demand 방식을 사용하여 경로설정을 하는 방식을 말한다.

MANET WG는 MN간 통신을 위한 유니캐스트 라우팅 프로토콜에 대한 표준화 작업을 추진하고 있으며 AODV, OLSR, TBRPF, DSR[28]과 관련된 문서를 실험적 RFC[29]로 채택하였다.

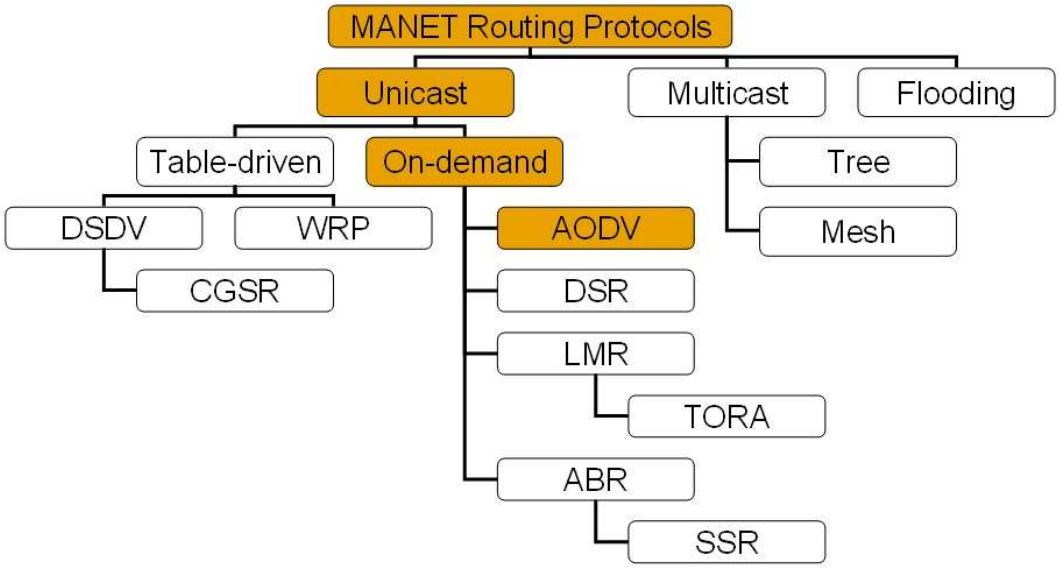


그림 2. MANET의 라우팅 프로토콜

Fig. 2. Routing Protocols of MANET

그림 5와 같은 AODV 라우팅 프로토콜[30]은 유니 캐스트와 멀티 캐스트를 모두 지원하며 DSDV 라우팅 프로토콜 기반으로 DN의 순차번호를 이용하여 라우팅 루프를 방지한다. DSR 라우팅 프로토콜과 유사한 경로탐색 절차를 사용하며 전체경로에 대한 설정을 사전에 유지·관리하지 않는 On-demand 방식으로 불필요한 전송횟수를 줄일 수 있어 전체 네트워크 성능을 향상시킬 수 있다.

SN이 DN까지의 경로설정을 위한 메시지를 전송하고자 할 때 SN이 DN의 경로정보를 가지고 있지 않다면, SN은 경로탐색 과정을 실행하게 되고, SN이 DN의 경로정보를 가지고 있다면 경로설정을 위한 메시지인 RREQ 메시지를 송신한다. RREQ 메시지를 수신한 이웃한 MN들이 DN으로 가는 최신 경로정보를 가지고 있지 않다면, SN은 RREQ 패킷을 재전송하게 된다.

각 MN은 그림 3과 같이 순차번호와 RREQ를 보낼 때마다 증가하는 브로드캐스트 ID를 사용하며 주소 자동설정[31]을 통해 고유의 IP주소와 브로드캐스트 ID를 생성한다. RREQ 패킷을 받은 MN은 DN으로 RREQ를 전달하는 과정에서 자신의 라우팅 테이블에 첫 RREQ 메시지를 보내온 MN의 IP주소를 기록하므로 역방향 경로를 설정할 수 있다.

```
Type = 1 //RREQ
Hop Count = 0
Broadcast ID += 1
Destination IP Address
Destination Sequence Number = Last Destination Sequence Number
Source IP Address
Source Sequence Number = Last Destination Sequence Number + 1
```

그림 3. 경로탐색 초기화

Fig. 3. Setup of Route Discovery

RREQ 패킷이 DN에 도착하거나 N1, N2, N3노드들이 응답할 만큼 최근의 경로 정보를 가지고 있다면, DN은 이웃한 MN을 통해 SN까지 RREP 패킷을 유니캐스트 방식으로 응답하게 되므로, AODV 라우팅 프로토콜은 양방향 특성이 동일한 링크만을 지원한다. RREP 패킷을 수신한 MN들은 순방향 루트정보를 생성하여 저장하며 하나

의 MN이 동일한 RREQ 메시지를 중복으로 수신한 경우 최초로 수신된 것만을 사용한다.

```
Type = 2 //RREP
Hop Count = 1 //Destination Node
Hop Count = Destination Hop + 1 //Intermediate Node
Destination IP Address
Destination Sequence Number = last Destination Sequence Number + 1 //Destination Node
Destination Sequence Number = last Destination Sequence Number //Intermediate Node
Source IP Address
Lifetime = Routing Effective Time
```

그림 4. RREP 경로설정

Fig. 4. RREP Routing Setting

라우팅 경로내의 특정 링크에서 오류가 발생한 경우 MN들은 RERR 패킷을 SN으로 전송하여 루트 재탐색 절차[32]를 시작하게 되고, RERR을 수신한 MN들은 오류가 발생한 링크와 관련된 경로정보를 삭제한다.

AODV 라우팅 프로토콜은 RREQ, RREP 메시지를 통해 다른 라우팅 프로토콜보다 효율성이 우수하지만 이는 보안성을 배제한 것이며 MN간 멀티 홉 통신, 동적 네트워크 토폴로지의 제약성 때문에 MANET 라우팅 프로토콜들은 많은 위협과 공격유형에 노출되어 있다.

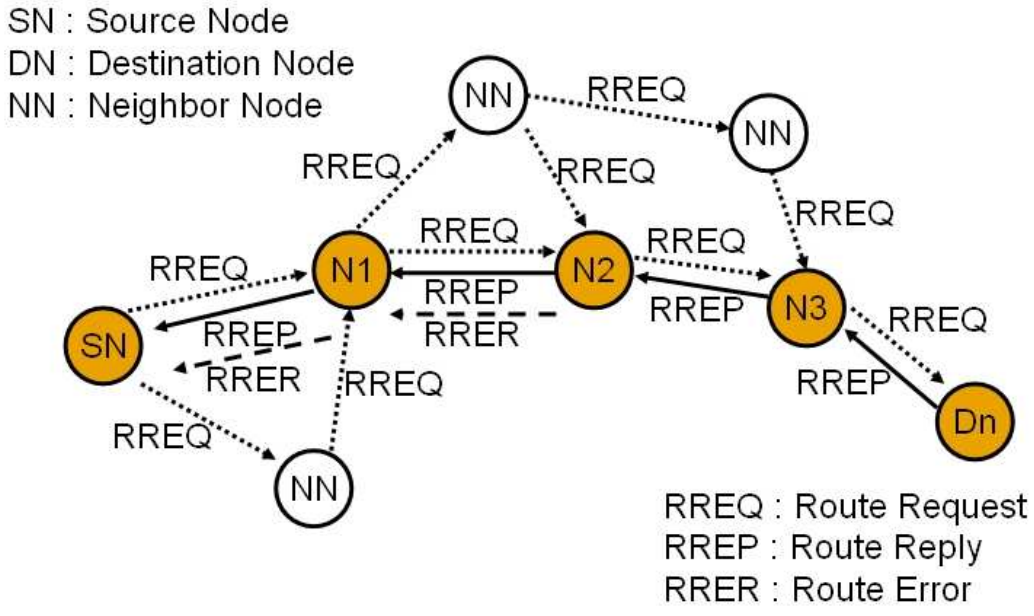


그림 5. AODV 라우팅 프로토콜

Fig. 5. AODV Routing Protocol

B. 위협과 공격유형

MANET은 MN의 이동성과 동적 네트워크 토폴로지에 의한 불안전한 링크, 한정된 주파수 대역, 전송거리와 에너지 제약성 그리고 MN의 증가로 인한 전파간섭으로 악의적인 노드에 대한 물리적 방어가 결핍되어 있다. 또한 데이터의 무결성 및 기밀성 문제, 정적인 보안기법의 제약성과 CA 부재로 다양한 위협과 공격에 노출되어 있다[33].

MANET의 보안상 위협은 외부위협과 내부위협으로 구분하며, 외부위협은 잘못된 라우팅 정보의 삽입을 통한 위협, 이전의 라우팅 정보를 재생하여 악용하는 위협, 라우팅 정보를 변형하여 네트워크에 위험을 가져오는 위협 등으로 분류한다. 외부위협을 통해 악의적인 노드는 네트워크를 분할하거나 극심한 트래픽을 유발하여 전체 네트워크 장애를 발생시키며, 외부위협을 방어하기 위해서는 라우팅 정보를 통해 MN이 악의적인 노드와 타협되어 생성된 것인지 아니면 동적 네트워크 토폴로지 변화로 훼손된 MN인지 구분해야 한다. 내부위협은 훼손된 MN에게서 발생하여 이웃한 MN들에게 잘못된 정보를 제공하고 네트워크 장애를 유발한다. 외부위협과 내부위협을 효과적으로 대처할 수 있는 방법은 충분한 MN을 확보하여 훼손된 MN 주변을 우회할 수 있는 경로를 확보하는 것이다.

그림 6과 같이 MAENT은 SN과 DN사이에 단일 홉 데이터 전송도 가능하지만 멀티 홉을 통해 NN들이 데이터를 전송해주는 역할을 하므로 쉽게 악의적인 노드로부터 수동적 공격 및 능동적 공격을 받을 수 있다. 수동적 공격은 악의적인 노드의 에너지를 절약하기 위한 목적으로 네트워크에서 수행해야할 협동 작업을 하지 않는 공격을 말한다. 라우팅 패킷에 대한 허가되지 않은 “listening″을 수반하며 데이터 도청을 가능하게 한다. 능동적인 공격은 악의적인 노드의 행동이나 MN의 부정행위로 에너지가 소비되는 공격을 말한다. 네트워크에 참여한 악의적인 노드는 패킷을 변조, 위조, 재생, 누락시켜 적법한 MN으로 위장하여 동일한 메시지를 수신하게 하거나 변조된 메시지를 전송하여 MN간의 메시지 흐름을 저하시키며 방해한다. 능동적 공격의 목적은 정보의 충돌을 통해 라우팅 노드를 혼란시켜 패킷을 지연 시키거나 방해하여 패킷이 DN에 도달할 수 없도록 하는데 있다. 또한 악의적인 노드와 타협된 MN들이 정상적으로 동작하는 것처럼 보이나 네트워크의 라우팅 구조를 왜곡시킬 수 있는 잘못된 정보의 생성 및 전송을 통한 복잡성 장애, CA의 부재로 멀티 홉을 통한 MN간 상호 인증문제로 보안상 취약성이 존재하며[34], 신뢰성 있는 MANET 보안 인증기법들이 필요하다.

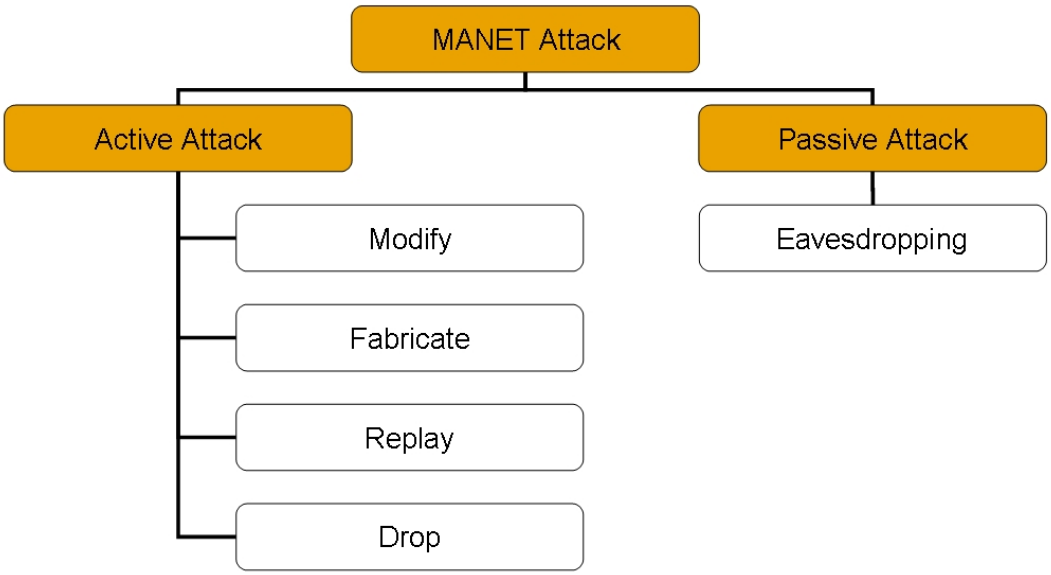


그림 6. MANET 공격유형

Fig. 6. MANET Attack Pattern

C. MANET 인증기법

MANET 보안 시스템의 구축을 위해서는 보안 5요소인 가용성, 인증, 기밀성, 무결성 그리고 부인봉쇄 서비스가 요구되지만 인증 제공이 보안유지를 위한 핵심적 부분이면서도 어려운 측면으로 인식되고 있다. 인증은 MN사이에 데이터를 송·수신하는 적법한 노드를 검증하는 것으로 네트워크 기반의 PKI를 이용한 실체인증과 암호화를 이용한 개인 식별 인증으로 나뉜다. 암호화 기법이 견고하다 할지라도 인증이 제공되지 않는다면 악의적인 노드의 네트워크 참여가 자유롭게 되어 MANET 자원 및 중요한 정보에 대한 접근권한을 얻을 수 있어 더 이상의 보안은 의미가 없다.

그림 7과 같이 MANET 보안을 위해 제안된 인증기법들은 신뢰된 CA의 존재 유·무로 나눌 수 있으며 CA가 존재하는 공개키 기반의 인증기법과 CA가 존재하지 않는 OTP를 이용한 인증기법으로 나뉜다. 공개키 기반의 인증기법으로는 Threshold 암호화를 이용한 인증기법[37], 완전분배 Threshold CA[35], ID기반 Threshold PKG[36], 자기 인증서 발행기법[38]등이 있다. OTP를 이용한 인증기법으로는 시간동기 인증기법, 시도응답 인증기법, OTP S/Key 인증기법 등이 있다. 그 외에도 계층적 분산구조 인증기법, LHAP를 이용한 인증기법, PKI 인증기법 등 다양한 기법들이 제안 되었지만, MN이 호스트와 라우터로 동작한다는 본질적 특성 때문에 기존 인증기법들은 많은 문제점이 존재하며 완전한 MANET 환경의 인증기법이라 할 수 없다.

완전한 MANET 환경의 신뢰성 있는 인증을 위해서는 보안 라우팅 프로토콜과 인증을 위한 암호화기법 그리고 악의적인 노드와 타협된 MN을 고려해야 한다. 인증을 위한 암호화기법 사용은 MN에 많은 부하를 발생시키고, 공개키를 이용한 인증기법들은 네트워크 안전성은 제공하지만 MN의 강력한 계산능력을 요구하므로 독립된 구조의 MANET에는 어울리지 않는다.

MANET 환경과 MN을 고려한다면 해시함수와 세션키 검증자와 같은 연산과정이 단순하면서 보안성을 제공하는 OTP를 이용한 인증기법이 필요하다[39]. 그러나 OTP를 이용한 인증기법 또한 안전한 키 관리나 기밀성 요구를 충족하지 못하기 때문에 많은 문제점이 존재한다.

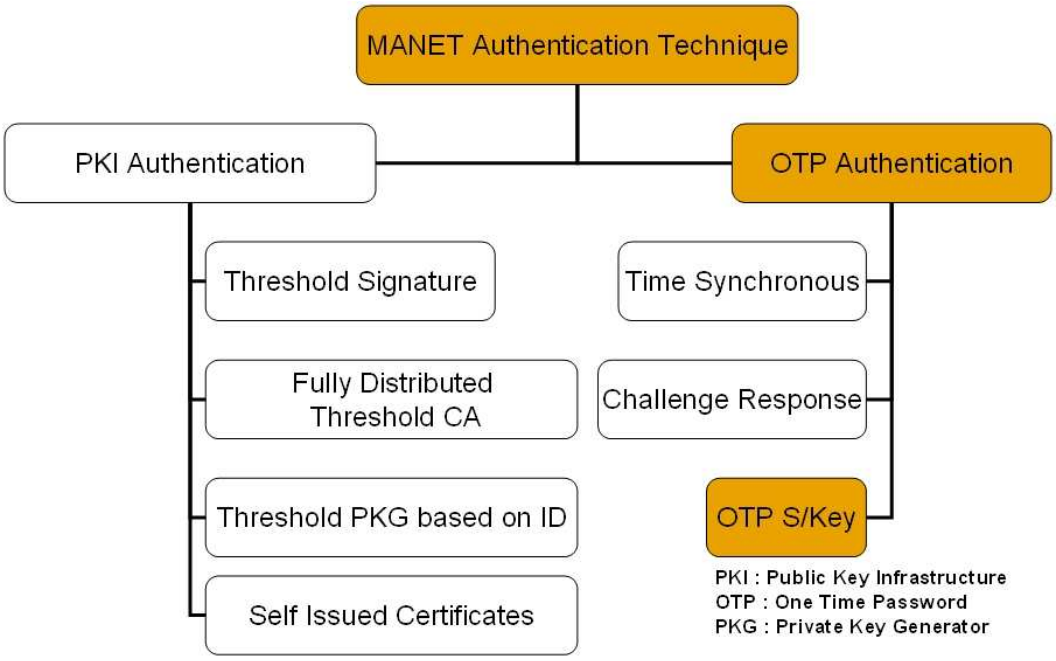


그림 7. MANET 환경의 인증기법

Fig. 7. Authentication Technique in MANET Environment

1. *OTP*를 이용한 인증기법

OTP를 이용한 인증기법은 SN이 인증을 받고자할 경우 암호학적 해시함수의 난수적 특성을 이용하여 매번 다른 형태의 패스워드를 생성한다. 악의적인 노드가 해시된 패스워드를 가로챈다 하더라도 패스워드를 사용할 수 없기 때문에 신뢰성 있는 인증체계를 구성할 수 있다.

OTP를 이용한 인증기법[40]은 한 개의 비트를 서명하기 위해 비밀키로 사용할 임의의 x값을 선택하고 각 비트에 해시함수 $H()$를 적용하여 하나의 공개키 $y = H(x)$를 생성한다. 서명할 메시지의 비트들 중에 비트값이 1인 경우 서명인은 비트값 1에 해당하는 비밀키 x값을 메시지와 함께 전송한다. 이는 서명을 받은 증명인이 자신이 받은 비밀키 x에 대해 부인하거나 서명된 메시지에서 1의 개수를 변경하는 등의 행동을 할 수 있으므로 이를 방지하기 위해, 서명인은 메시지에 포함된 비트 0의 개수를 계산하여 메시지와 함께 서명한다. n비트의 메시지를 서명하는데 비트 0의 개수를 추가하기 위하여 $\log_2 n$비트가 메시지에 추가된다. 그러나 서명될 메시지의 비트값이 0인 경우, 서명인은 메시지에 어떤 값도 전송하지 않는다.

그림 8과 같이 8비트 메시지 “0100 1110”을 서명하려 한다면 8비트의 비트열중 0의 개수를 계산하여 3비트 “100”을 추가하고 “0100 1110 100”과 같은 총 11비트 메시지의 비밀키값 x_2, x_5, x_6, x_7, x_9를 포함시켜 OTP 전자서명을 만들게 된다[41]. 서명인은 8비트 메시지에 OTP 전자서명을 포함하여 수신자에게 전송하고, 수신자는 전송된 8비트 메시지의 0의 개수인 3비트 메시지를 추가한 후 11비트의 메시지에 대한 OTP 전자서명을 생성하여 수신된 OTP 전자서명과 비교한 후 메시지를 검증한다.

OTP를 이용한 인증기법은 메시지 이외에 OTP 전자서명을 추가로 전송해야 하므로 전송량이 조금 늘어나는 반면 메시지가 아무리 길더라도 단 한 번의 서명생성 과정만이 필요하므로 효율적이다. 이처럼 메시지를 해시함수를 이용하여 원래보다 짧은 길이로 바꾼 후 비밀키로 서명한다면 인증에 걸리는 시간을 단축할 수 있고 해시함수의 일방향성에 의해 메시지의 위·변조를 방지하는 무결성을 제공한다. OTP를 이용한 인증기법은 암호학적 해시함수에 근거하여 생성되며 패스워드 유효기간을 1회로 한정하기 때문에 더 이상 오용할 수 없다는 장점을 가지고 있어 시간동기 인증기법, 시도응답 인증기법 그리고 OTP S/Key 인증기법 등에 안전성 및 효율성을 제공하기 위해 사용된다.

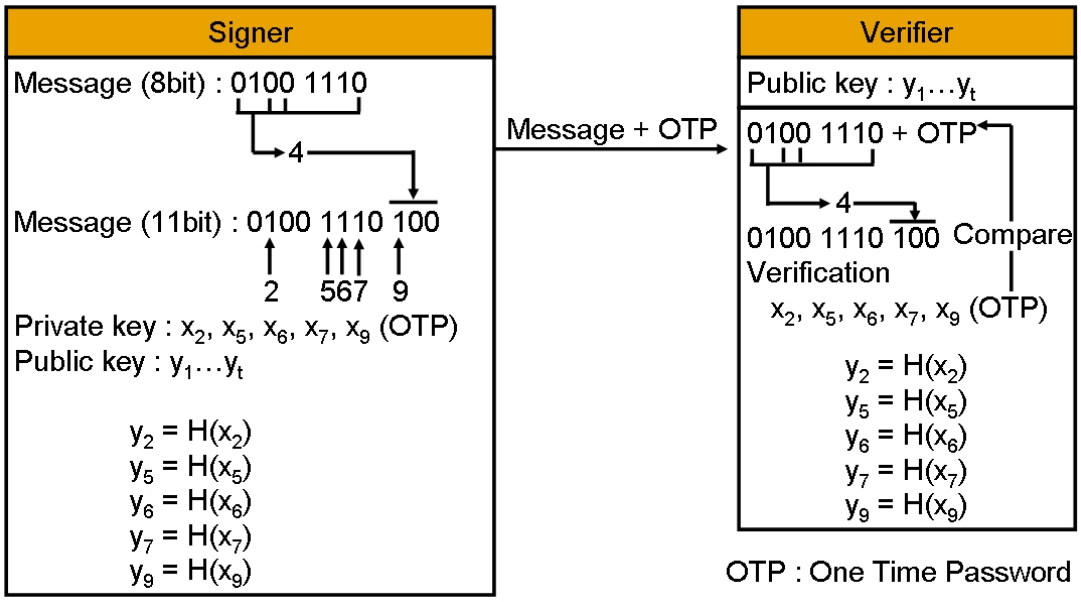


그림 8. OTP의 예

Fig. 8. Example of OTP

1-1. 암호학적 해시함수

암호학적 해시함수는 서로 다른 임의의 가변길이 비트열 입력을 동일한 출력 값이 발생하지 않도록 일정한 길이의 비트열로 압축시키는 함수를 말한다. 해시함수는 $y = H(x)$와 같은 식으로 표현하며, x는 가변길이 비트열이고, y는 해시함수를 통해 생성된 고정길이의 해시코드이다. 가변길이 x에 대해 $H(x)$를 계산하는 것은 쉬우나, 해시코드 $y = H(x)$의 만족하는 x를 찾는 것은 일방향 해시함수의 특성상 불가능하다.

해시함수는 암호화 기법보다 빠른 속도와 데이터의 무결성을 체크하며, 식 (2.1)과 같이 동일한 해시함수 $H()$를 가지는 가변길이 비트열 x_1과 x_2는 충돌회피의 특성을 나타낸다.

$$H(x_1) \neq H(x_2) \qquad (2.1)$$

해시함수는 그림 9와 같이 메시지 M을 일정한 크기의 R비트 단위로 나누어서 메시지 다이제스트를 생성한다. R비트로 나누어진 메시지는 동일한 E_k를 통해 XOR 연산을 수행하는 암호화 블록을 통과하며 최종적으로 $H(M)$을 생성하게 된다.

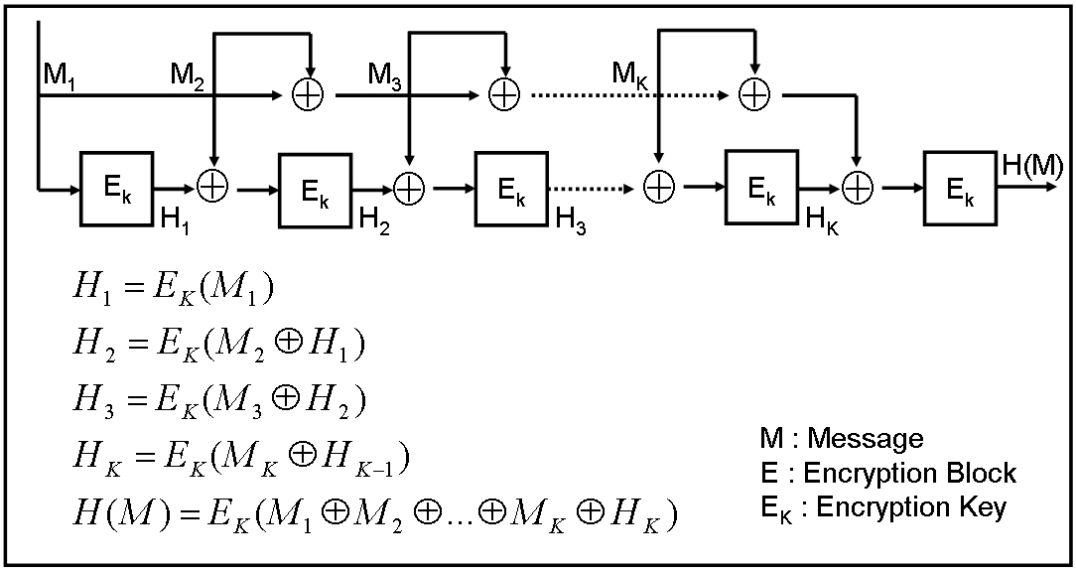


그림 9. 해시함수

Fig. 9. Hash Function

데이터 무결성 유지와 OTP를 이용한 인증기법에서는 많은 해시함수가 제안되었고 Snefru, N-HASH, MD4, MD5, SHA등이 사용되고 있다.

MD5[42]는 MD4를 개선한 것으로 빠른 속도의 소프트웨어 구현을 위해 가변길이의 입력으로부터 식 (2.2)를 이용한 512비트 블록의 최종 결과 값인 128비트 메시지 다이제스트를 생성한다.

$$A \leftarrow B + ((A + g(B, C, D) + X[k] + T[i]) <<< s) \quad (2.2)$$

표 1. MD5 매개변수

Table 1. Parameters in MD5

매개변수	내 용
A, B, C, D	MD5 버퍼, 단계에 따라 상이한 순서로 되어 있음
g	해시함수 F, G, H, I 중의 하나
$<<< s$	s 비트에 의한 32비트 매개변수의 순환 좌 쉬프트
$X[k]$	메시지의 512비트 블록 중에서 k번째 32비트
$T[i]$	행렬 T에서 i번째 32비트
$+$	2^{23} 덧셈

MD5는 OTP를 이용한 인증기법의 암호화된 패스워드 생성에 사용되며 inversion, collision, forgery등 3가지 견고한 방어책이 있어야 한다. inversion는 주어진 해시 값으로부터 메시지를 알아내는 것이고, collision는 두개 이상의 서로 다른 메시지가 같은 해시 값을 갖는 것이다. 그리고 forgery는 비밀키에 대한 지식 없이 MAC을 산출하는 것이다. OTP를 이용한 인증기법에서 MD5는 IEEE 802.11의 무선 디바이스 인증에 표준으로 사용되고 있으며 해시함수를 이용한 암호화된 패스워드 사용으로 MANET 환경의 신뢰성 있는 OTP 인증체계를 구성할 수 있다.

1-2. 시간동기 인증기법

MANET 환경의 시간동기 인증기법[43]은 매 분마다 한 개의 난수인 OTP를 생성하기 위하여 난수생성 알고리즘과 64비트 크기의 비밀키가 필요하다.

그림 10과 같이 각각의 MN에게는 특정한 키가 할당되며 SN의 지능형 토큰과 DN의 Key_DB에 저장된다. SN이 응용 서비스를 받기위해 DN에게 메시지 전송을 시도하면, DN은 4개의 숫자로 이루어진 MN의 식별번호 *PIN*과 시간의 초기값을 64비트 비밀키와 조합한 후 난수생성 알고리즘을 통해 6개의 숫자로 이루어진 난수를 Key_DB에 저장한다.

SN은 토큰 안에 저장된 비밀키와 시간의 초기값을 난수생성 알고리즘을 통해 6개의 숫자로 이루어진 난수를 생성하고 *PIN*과 난수를 DN에게 전송한다. DN은 SN으로부터 전송된 10개의 숫자중 *PIN*을 인덱스로 하여 Key_DB에 이미 저장된 64비트 비밀키를 찾아, 생성된 6개의 난수가 SN으로부터 전송된 난수와 일치하는지를 검사한다. SN에서 전송된 난수와 DN의 Key_DB에 저장된 난수가 동일하다면, DN은 SN에게 서비스에 대한 이용권한을 부여한 후 인증절차를 끝낸다.

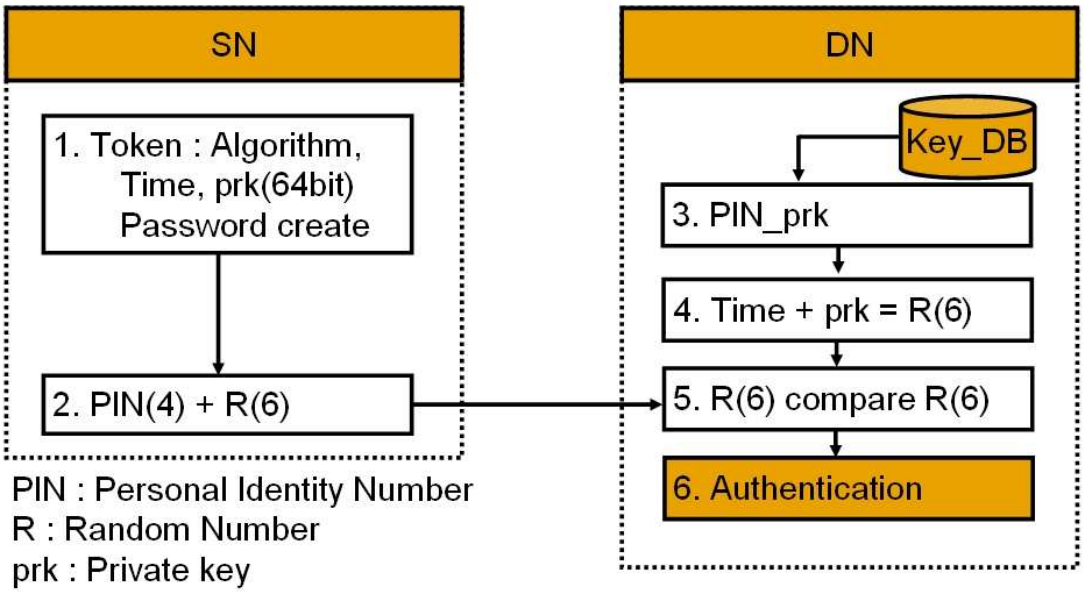


그림 10. 시간동기 인증기법

Fig. 10. Time-synchronous Authentication Technique

1-3. 시도응답 인증기법

MANET 환경의 시도응답 인증기법[44]은 SN의 인증을 위해 기본인증과 다이제스트 인증을 사용하는 방식을 말한다. 기본인증은 패스워드를 평문으로 전송하고 평문 전송을 방지하기 위해 다이제스트 인증방식을 사용한다.

그림 11과 같이 SN이 인증요구와 함께 SN의 PIN을 DN에게 전달하면, DN은 난수를 생성하여 *Challenge* 메시지를 SN에게 전송하고, DN은 SN의 PIN에 해당하는 비밀키를 Key_DB에서 추출하여 DN이 생성한 난수와 함께 DES 암호화를 시작한다. *Challenge* 메시지를 받은 SN은 자신의 비밀키와 DN이 전송한 난수를 이용하여 DES 암호화를 통해 OTP를 생성하여 *Response* 메시지로 DN에게 반환한다. DN은 SN으로부터 *Response*를 받아 동일한 *Challenge*와 SN의 정보를 이용해 OTP를 생성하고 SN으로부터 수신된 *Response*값을 비교하여 일치하는 경우에 SN을 적법한 MN으로 인증하게 된다.

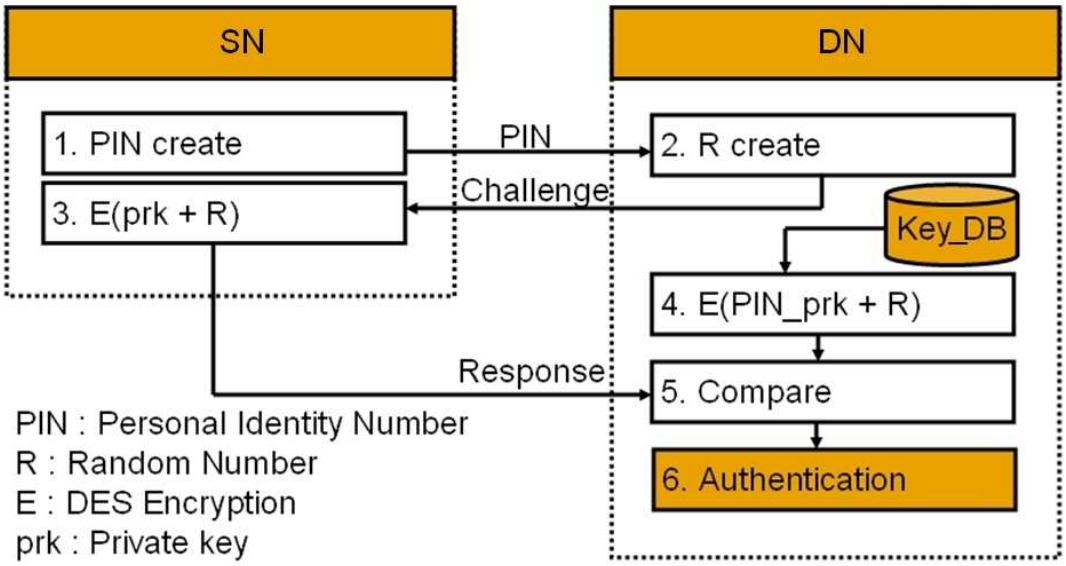


그림 11. 시도응답 인증기법

Fig. 11. Challenge-response Authentication Technique

1-4. OTP S/Key 인증기법

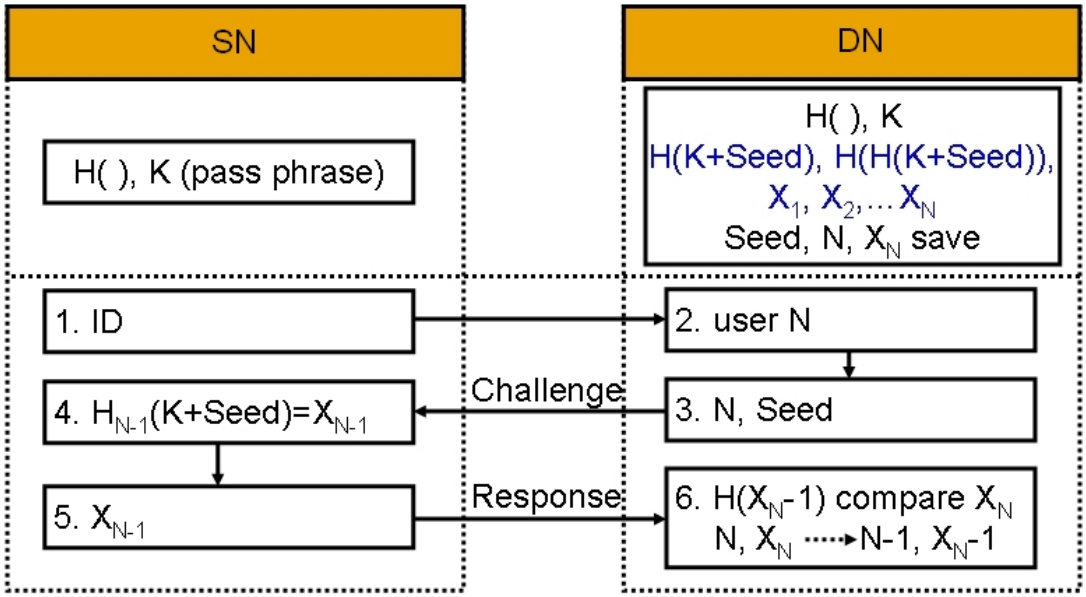
OTP S/Key 인증기법[45]은 MANET에서 OTP를 이용한 MN의 인증에 활발히 사용되고 있는 인증기법이다. OTP는 해시함수를 매번 다르게 적용하여 항상 다른 해시코드를 생성하고 추가계산을 한 후 DN이 저장한 값과 일치여부에 따라 SN을 인증한다. SN은 OTP를 생성하고, DN은 OTP가 검증되어야 하며, OTP의 생성과 검증은 MD4, MD5와 같은 해시함수를 통해 8바이트 입·출력 코드를 생성하므로 악의적인 노드로부터 네트워크상의 도청과 재전송 공격에 안전하다. 또한 OTP S/Key 인증기법은 자동화될 수 있어 어떠한 비밀정보도 MN에 보관하지 않는 장점을 가지고 있다.

그림 12는 SN의 비밀키인 패스-프레이즈 K와 DN에서 생성한 임의의 수 $Seed$를 인증 요청횟수 N만큼 해시함수를 수행하여 OTP를 생성한다. SN은 생성된 OTP를 DN에 전송하고, DN은 이미 전송된 OTP를 한 번 더 해시하여 전송된 OTP의 일치여부에 따라 SN을 인증한다.

SN과 DN사이의 인증 요청회수 N이 4라고 할 경우, DN이 $OTP(1)$을 저장하고 있으면, SN은 $OTP(2)$를 DN에게 전송한다. DN은 SN으로부터 수신한 $OTP(2)$를 한 번 더 해시하여 $H(OTP(2))$를 $OTP(1)$과 비교하여 일치하지 않을 경우, 그 인증요구는 실패로 종료하고 일치할 경우 $OTP(2)$로 대체하여 저장한다. OTP의 사용을 모니터하고 있는 악의적인 노드는 다음 패스워드 $OTP(N+1)$를 생성해낼 수 없을 것이며 첫 세션에서 SN의 비밀키를 알지 못하면 도청이 불가능하게 된다.

OTP S/Key 인증기법은 SN에 의해 수행된 해시함수의 수가 하나씩 줄어들기 때문에 인증 요청횟수 N이 1이 되면, SN은 시스템을 재 초기화해야 한다.

MANET의 OTP S/Key 인증기법의 보안은 SN에게만 알려진 비밀 패스-프레이즈에 전적으로 의존하며, 전체 비밀정보는 어떠한 계산 장치로도 찾아낼 수 없는 형태로 저장된다. 또한 시간동기 인증기법, 시도응답 인증기법에 비해 안전성, 실용성 그리고 간편성이 우수하지만, OTP를 이용한 인증기법들은 여전히 많은 문제점을 지니고 있다.



- SN : OTP created, DN : OTP verification
- 1st pwd (N=4) : OTP(1) = H(H(H(H(K+Seed))))
- 2st pwd (N–1) : OTP(2) = H(H(H(K+Seed)))

그림 12. OTP S/Key 인증기법

Fig. 12. OTP S/Key Authentication Technique

2. *OTP*를 이용한 인증기법의 문제점

시간동기 인증기법의 문제점은 난수를 일치시키기 위해서 시간에 대한 동기가 보장되어야 한다. 어느 지역에서나 시간은 동일할 수가 없고 지역차이 때문에 약간의 시간차이가 발생하게 된다. 그러나 시간에 대한 동기는 그리니치 표준시간을 양쪽 노드에 사용하여 해결 될 수는 있다. 시간동기 인증기법의 가장 큰 문제는 시간편차이다. 토큰이 일회용이 아니고 일반적으로 수년간에 걸쳐 사용되는 장치이기 때문에 하루에 몇 초라도 늦어지거나 빨라진다면 토큰과 DN간의 동기는 보장 될 수 없다. 또한 토큰에서 생성된 난수가 패스워드로 사용되는데, 패스워드는 유효시간이 60초이다. 악의적인 노드가 MANET상의 PIN과 패스워드를 60초안에 추출하여 DN에 접속한다면 적법한 MN으로 인증하게 되고, 짧은 패스워드와 일방적 키 교환은 악의적인 노드의 도청 및 추측 공격을 가능하게 한다.

시도응답 인증기법의 문제점은 여러 번의 시도응답 절차로 인해 처리속도가 느려지는 문제점과 효과적인 키 관리이다. 인증과정에서 송·수신 노드는 동일하게 암호화 및 복호화가 가능해야하고 부인방지 기능이 존재하지 않아 DN의 신뢰성에 대한 단점이 존재하며, 동일한 *Challenge*값이 생성된다면 보안상의 문제점이 발생될 수 있다. 하지만 시간동기 인증기법에 비해 복잡성이 덜하며 안전성이 높다.

MANET의 OTP를 이용한 인증을 위해 활발히 사용되고 있는 OTP S/Key 인증기법은 사전 공격에 대한 문제점, 스푸핑에 대한 문제점, 패스워드 사용횟수의 문제점 그리고 상호인증이 불가능하다.

OTP S/Key 인증기법의 네트워크 중간에 위치한 악의적인 노드는 MN간 패스-프레이즈 사용과 반복횟수 그리고 *Seed*를 평문으로 전송하는 점을 이용하여 *Challenge*와 *Response*를 획득하고 사전의 단어들을 적용한 *Challenge*의 결과와 비교할 수 있는 사전 공격이 가능하다. 또한 SN의 패스워드 선택 시 보안성 검사를 하지 않는다는 단점을 이용하여 정당한 패스워드를 유추하게 되고 *Challenge*와 상관없이 OTP를 생성해 낼 수 있는 사전 공격에 문제점을 지니고 있다. 또한 OTP S/Key 인증기법은 SN만을 인증하므로, 악의적인 노드가 DN으로 위장하는 스푸핑 공격에 문제점을 지니고 있다. 스푸핑 공격은 네트워크 중간에서 악의적인 노드를 설정하여 SN의 ID로 접속을 하고 반복횟수 *N*과 *Seed*를 획득하여 SN으로 전송한다. 악의적인 노드로부터 *N*과 *Seed*를 받은 SN은 적법한 DN으로 착각하여 *Response*를 전달하게 되고, 악의적인 노드는 해

시함수를 통해 다음 횟수의 *Response*를 계산할 수 있는 스푸핑에 대한 문제점을 지니고 있다.

OTP S/Key 인증기법은 SN과 DN사이의 초기화 세션에서 반복횟수 N을 저장하고 매번 SN을 인증한 후 1씩 감소시키므로, N이 1에 도달하게 되면 반복횟수 N을 재설정해야 하는 문제가 발생하게 된다. 초기 설정된 N이 최대 반복횟수가 되고 N회 SN을 인증한 후 반복횟수 N을 재설정해야 한다. 또한 OTP S/Key 인증기법은 SN의 인증 기능만을 제공하므로 SN과 DN간의 안전한 통신을 위해 상호인증이 요구되는 경우에는 사용이 불가능하다. DN은 SN의 *Response*를 통하여 적법한 SN임을 인증할 수 있지만, SN은 *Challenge*를 보낸 DN이 적법한 MN인지를 인증할 방법이 없다. 악의적인 노드가 DN으로 위장했을 경우 SN은 공격대상이 되며 중요한 정보의 누출이나 파괴의 위험에 직면하게 된다. SN과 DN이 상호인증이 된다면 더욱 신뢰성 있는 통신이 가능하게 된다.

표 2는 MANET에서 OTP를 이용한 인증기법들의 특징과 문제점을 보이고 있다. OTP S/Key 인증기법이 시간동기 인증기법, 시도응답 인증기법보다 안전성과 실용성을 제공하지만, OTP S/Key 인증기법은 사전 공격, 스푸핑, 패스워드 사용횟수의 문제점과 인증기법에서 가장 중요한 상호인증이 불가능하다. MANET 보안의 안전성과 상호인증을 위해서는 연산량을 고려한 패스워드 기반의 키 교환 프로토콜을 적용하여 MN간의 신뢰성 있는 인증체계가 필요하다.

표 2. MANET OTP 인증기법의 특징과 문제점

Table 2. Feature and Problem of OTP Authentication Technique in MANET

MANET OTP 인증기법			
구 분	시간동기	시도응답	*OTP S/Key*
적 용	- 휴대용 난수 생성기	- 대칭키, DES	해시함수
특 징	- 시간에 대한 함수값 (난수)생성	- 간단 - 안전	-도청 방지 -간단 -자동화 -알고리즘 비밀 -정보보관 없음
문제점	- 시간동기 - 시간편차 - 패스워드의 유효성	- 시간소요 - 키 관리 - 서버의 신뢰성	- 사전 공격 - 스푸핑 공격
실용성	- 간단 - 시간동기의 문제	- 비교적 안전 - 키 관리와 복잡한 절차	- 간편 - 안전성 양호

Ⅲ. 패스워드 기반 키 교환 프로토콜

패스워드 기반 키 교환 프로토콜[46]은 개방된 네트워크에서 안전하고 효율적인 세션키 교환을 통해 각 노드간 인증을 수행하는 프로토콜로 부가적인 기억장치가 필요하지 않고 노드의 패스워드를 쉽게 선택하여 키 교환을 수행할 수 있는 장점이 있어 많은 관심과 연구가 진행되고 있다. 하지만 패스워드는 정보량적인 측면에서 낮은 엔트로피를 가지고 있기 때문에 패스워드에 대한 추측 공격에 취약하다는 단점이 존재한다. 패스워드 추측 공격에 대한 문제는 안전성을 증가시키기 위해 비밀통신을 원하는 노드간 세션키 설정의 문제와 목적지의 공개키를 획득할 수 있는 문제로 나눌 수 있으며, 키 교환을 위해서는 대칭키 암호화 방식과 비대칭키 암호화 방식을 사용한다.

대칭키 암호화 방식은 사전에 안전한 네트워크를 이용한 송·수신 노드가 미리 비밀키를 공유해야 하므로 개방된 네트워크에 적용하는데 많은 어려움이 있다. 비대칭키 암호화 방식을 사용할 경우는 송·수신 노드의 연산량을 고려해야 하므로 대칭키 암호화 방식과 비대칭키 암호화 방식을 결합한 EKE[47]가 제안되었다.

EKE가 제안된 이후 다양한 암호화 키 교환 기법들이 제안되었으며, IEEE P1363.2[48]에서는 패스워드 기반 키 교환 프로토콜의 연구와 표준화 작업이 진행 중에 있다.

A. 패스워드 암호화를 위한 세션키 생성

송・수신 노드간 논리적 연결을 위한 세션은 네트워크에 참여하는 각 노드들이 서로 통신을 위한 채널을 형성하여 데이터를 송·수신한 후 채널이 종료될 때까지의 시간을 말한다. 네트워크상 송・수신노드사이에 안전한 데이터 전송을 위해서는 효과적인 키 관리와 데이터 암호화를 위한 세션키 생성이 중요하다.

세션키는 형성된 하나의 세션에서만 사용하며 송·수신노드의 메시지를 암호화 복호화 과정을 수행하고 세션이 종료되면 함께 소멸되는 비밀 공유키이다. 안전한 세션키 사용을 위해서는 세션키로부터 네트워크 참여자가 가지고 있는 공유키를 유도할 수 없으며, 전방향 보안을 위해 이미 사용된 세션키는 다음 세션에 사용될 세션키를 유추할 수 없고 역방향 보안이 제공되어야 한다.

세션키는 세션키를 생성하기 위한 프로토콜과, 키 합의 프로토콜 그리고 키 전달 프로토콜로 나누어진다. 세션키 생성 프로토콜은 네트워크에 참여하는 송·수신노드 사이에 안전한 데이터 전송을 위한 키 생성이고, 키 합의 프로토콜은 송·수신노드가 암호화 기법을 이용하여 각자의 비밀키 값을 생성하고 교환하여 하나의 공유키를 생성하는 방식이다. 그리고 키 전달 프로토콜은 송신노드가 임의로 공유키를 생성하여 수신노드에게 전송하는 방식을 말한다. 이처럼 개방형 네트워크상의 송・수신노드 사이에 안전한 데이터 전송과 효과적인 키 관리를 위해서는 세션키 생성이 중요하며, 상용화 될 수 있는 세션키 교환 프로토콜로는 Diffie-Hellman 프로토콜이 존재한다.

Diffie-Hellman 세션키 교환 프로토콜[49]은 공개키 암호화 시스템의 개념을 제안하면서 세션키 교환을 위한 방법으로 송・수신 노드간 안전한 키 교환을 할 수 있도록 정의되었고 메시지 암호화에 사용된다.

Diffie-Hellman 프로토콜 자체는 키 교환에 한정되어 있고, 그 유효성은 지수승 계산을 쉽게 하며, DLP 계산의 어려움에 의존한다. DLP에서 큰 소수 p에 대하여 g의 멱수가 $mod\ p$에 의해 1에서 $(p-1)$까지의 모든 정수의 생성하는 수를 p의 원시근이라 정의한다. g가 큰 소수 p의 원시근이면 그 숫자는 어떤 순열의 형태에서 1에서 $(p-1)$ 사이의 식 (3.1)과 같은 정수로 구성된다.

$$g\ mod\ p,\ g^2\ mod\ p,\ \cdots,\ g^g\ mod\ p \qquad (3.1)$$

식 (3.2)와 같이 어떠한 정수 b와 큰 소수 p의 원시근 g에 대하여 유일한 멱지수 i

를 찾을 수 있다.

$$b = g^{i} \bmod p \qquad (3.2)$$

멱지수 i는 $g \bmod p$에 대한 b의 index라고 불리며 $ind_{g,p}(b)$라고 표기한다. 사전에 공유 값을 가지고 있지 않은 두 노드 A, B사이에서의 키 공유를 위해 사용되며 공개적으로 알려진 큰 소수 p와 p의 원시근인 정수 g를 2개 사용한다.

그림 13은 노드 A와 B사이의 키 교환 단계와 세션키 생성을 보이고 있다. A와 B는 큰 소수 p와 원시근 g를 선택하고 g는 p보다 작은 정수이어야 하며, A는 p보다 작은 랜덤정수 x를 선택하여 B에게 식 (3.3)을 통해 계산된 공개키 X를 전송한다.

$$X = g^{x} \bmod p \qquad (3.3)$$

노드 B는 A와 동일한 방법으로 p보다 작은 랜덤정수 y를 선택하여 A에게 식 (3.4)를 통해 계산된 공개키 Y를 전송한다.

$$Y = g^{y} \bmod p \qquad (3.4)$$

A, B는 x, y를 각각 비밀키로 저장하고 X, Y는 공개키로 사용한다. A는 B로부터 전송된 Y를 자신의 비밀키 x를 이용하여 Y에 지수승하여 식 (3.5)와 같은 세션키 K를 구한다.

$$K = Y^{x} \bmod p = g^{xy} \bmod p \qquad (3.5)$$

B 또한 A로부터 수신한 X값에 B의 비밀키 y를 지수승하여 식 (3.6)과 같이 세션키 K를 구한다.

$$K = X^{y} \bmod p = g^{xy} \bmod p \qquad (3.6)$$

Diffie-Hellman 세션키 교환 프로토콜은 A, B 노드 간에 어떠한 정보도 없이 비밀리에 공유된 세션키를 구할 수 있어 수동적 공격을 막을 수 있다. 악의적인 노드는 A, B 사이에 전송된 데이터를 가지고 X, Y, g, p값은 알 수 있지만, 세션키를 구하기 위해서는 x와 y를 알아야 한다. 악의적인 노드가 x와 y를 구하기 위해서는 DLP를 풀어야 하기 때문에 올바른 세션키를 구할 수 없어 패스워드 기반 인증키 교환 프로토콜에 다양하게 응용되어 사용되고 있다.

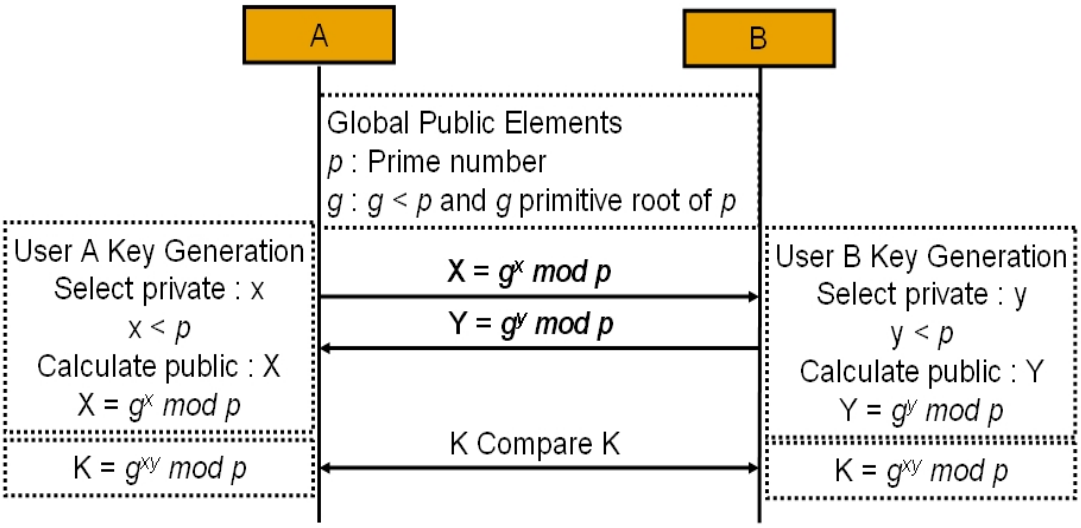


그림 13. Diffie-Hellman 키 교환

Fig. 13. Diffie-Hellman Key Exchange

B. 세션키를 이용한 인증키 교환 프로토콜

세션키를 이용한 인증키 교환 프로토콜은 네트워크에 참여한 노드가 선택한 패스워드를 사용하여 노드의 인증키를 검증하는 방식이다. 인증키는 패스워드 자체를 이용하는 방식들과 패스워드를 인자로 갖는 해시함수를 이용하여 증명자와 검증자가 패스워드에 관해 다른 지식을 소유하게 만드는 방식으로 나눌 수 있다.

증명자는 패스워드 자체이고, 검증자는 패스워드는 알 수 없지만 패스워드로부터 생성될 수 있는 값으로 노드 식별기능을 제공한다. 패스워드 검증자는 노드의 패스워드 P에 해시함수를 적용시켜 $H(P)$를 만들거나 패스워드를 곱셈군의 원시근 g의 지수로 하여 g^P 지수승을 계산하여 만든 값으로 노드를 인증하는데 필요한 정보이다.

검증자는 상대노드가 검증자를 소유하고 있더라도 쉽게 패스워드를 알아내는 것이 불가능하도록 만들어져야 한다. 검증자 기반 방식의 인증 프로토콜은 SN이 자신의 패스워드만을 기억하고, DN은 SN의 패스워드 검증자만을 저장하며, SN이 자신의 패스워드 정보는 알려주지 않으면서 패스워드의 소유자임을 증명하는 프로토콜이다.

표 3과 같이 패스워드 기반 키 교환 프로토콜은 암호화 키 교환방식을 사용하는 프로토콜로 SN과 DN이 상대방을 인증하고 세션키를 설정하려고 할 때, SN과 DN이 세션키의 일부분이 되는 키 재료값을 상대방에게 전송한다. 암호화 키 교환방식에서는 SN과 DN이 미리 알고 있는 패스워드 검증자로 키 재료값을 암호화하여 전송한다. 이처럼 암호화 키 교환방식의 프로토콜은 메시지 위·변조 공격이나, 중재자 공격 등에 안전하며 대칭구조와 비대칭구조의 패스워드 기반 인증키 교환 프로토콜로 구분한다.

표 3. 패스워드 기반 키 교환 프로토콜

Table 3. Key Exchange Protocols based on Password

구 분	대칭 구조	비대칭 구조
정 의	송·수신노드 사이에 같은 값을 이용하여 정당한 노드를 인증	송·수신노드 사이에 각기 다른 값을 이용하여 정당한 노드를 인증
증명방법	패스워드	증명자 : 패스워드 자체 검증자 : 패스워드로 유도된 값
공격형태	SN 위장 공격 DN 위장 공격	DN 위장 공격 전제조건 : DN을 위장하려면 사전 공격 수행해야함
종류	EKE SPEKE	A-EKE, B-EKE, SRP, AuthA[50]
요구조건	SN은 DN을 무조건 신뢰	

1. EKE 프로토콜

패스워드 기반의 EKE 프로토콜[47]은 대칭키 암호화 기법과 공개키 암호화 기법을 이용하여 네트워크상에 참여 노드간 기밀성과 인증기능을 제공한다.

표 4. EKE 프로토콜에 사용되는 계수

Table 4. Parameters Involved in EKE Protocol

계 수	의 미
A, B	참여자 A, B
P	A와 B가 공유한 패스워드
PUK, PRK	공개키, 비밀키
A^{PUK}, A^{PRK}	A의 공개키, A의 비밀키
$E_P(M)$	메시지(M)를 패스워드로 대칭 암호화
A^R, B^R	A의 난수, B의 난수
K	세션키

표 4와 같은 EKE 프로토콜의 계수를 이용한 네트워크 참여자 A와 B가 공유된 패스워드 P를 가지고 있을 경우 공통 세션키 K를 구하기 위한 과정은 다음과 같다.

그림 14와 같이 네트워크 참여자 A는 공개키(A^{PUK})와 개인키(A^{PRK})를 랜덤하게 생성하여, A^{PUK}를 참여자 B와 공유하고 있는 P로 암호화하여 A^{ID}와 함께 식 (3.7)과 같이 B에게 전송한다.

$$A^{ID},\ E_P(A^{PUK}) \qquad (3.7)$$

네트워크 참여자 B는 A로부터 전송된 $E_P(A^{PUK})$를 A와 공유된 P를 이용하여 A^{PUK}를 복호화하고, B는 랜덤한 세션키 K를 생성한다. K는 A^{PUK}로 암호화되고 한번 더 A와 공유된 P로 암호화하여 식 (3.8)과 같은 형태로 A에게 전송한다.

$$E_P(E_A^{PUK}(K)) \qquad (3.8)$$

A는 B로부터 수신한 메시지 $E_P(E_A^{PUK}(K))$를 P로 복호화하고 K값을 구한 후 A의

난수(A^R)를 $Challenge_A$값으로 선택하고, 식 (3.9)와 같이 K로 암호화하여 B에게 전송한다.

$$E_k(A^R) \quad (3.9)$$

B는 A로부터 전송된 메시지 $E_k(A^R)$를 복호화하여 A^R를 얻고, B의 난수(B^R)인 $Challenge_B$값을 선택한 후, 식 (3.10)과 같이 A^R과 B^R을 K로 암호화하여 A에게 전송한다.

$$E_k(A^R,\ B^R) \quad (3.10)$$

A는 B로부터 전송된 $E_k(A^R,\ B^R)$를 복호화하여 A^R과 B^R를 추출하고, $Challenge_A$값인 A^R과 전송된 A^R이 동일하다면 A가 같은 세션키로 공유했음을 확인하고, 식 (3.11)과 같이 B^R를 세션키 K로 암호화하여 B에게 전송한다.

$$E_k(B^R) \quad (3.11)$$

B는 A로부터 전송된 $E_k(B^R)$를 복호화하여 B^R를 추출하고 $Challenge_B$값인 B^R과 전송된 B^R이 동일하다면, B가 같은 세션키를 공유했음을 확인하고 A를 인증한다.

패스워드 기반 EKE 프로토콜은 B가 공유된 P와 A^{PUK}를 사용하여 K를 암호화한 후 A에게 전송하므로 객체인증, 키 신규성, 키 확인이 이루어지지만 키 동의 과정은 이루어 지지 않는다. 네트워크 중간에 위치한 악의적인 노드가 A와 B의 전송 메시지를 알고 있다면 K를 구하기 위해서 패스워드에 대한 사전 공격을 시도하고, 선택한 패스워드가 정당한 것인지를 알기 위해서는 공개키 암호화 기법을 풀어야 한다.

악의적인 노드는 A와 B사이에 공유된 K를 구할 수 없기 때문에 낮은 엔트로피를 가진 패스워드 기반 기법을 높은 엔트로피를 가지는 공개키 암호화 기법을 푸는 문제로 생성하므로 전체 시스템의 안전성을 가진다. 하지만 A의 K를 B에서 생성하여 분배하기 때문에 프로토콜의 흐름상 K가 악의적인 노드에 노출 되었을 경우, 악의적인 노드는 그동안 도청한 정보를 기반으로 A와 B가 공유된 P의 정보나 다음 세션에서 사용될 세션키를 얻고자 하는 Denning-sacco 공격에 취약할 수 있다.

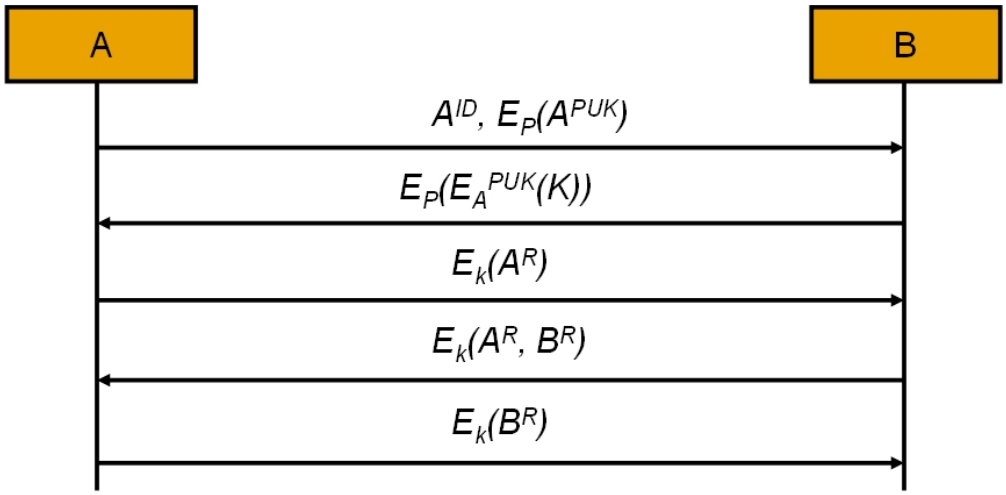


그림 14. 패스워드 기반의 EKE 프로토콜

Fig. 14 EKE Protocol based on Password

2. DH-EKE 프로토콜

패스워드 기반의 DH-EKE 프로토콜[51]은 Diffie-Hellman 키 교환 프로토콜을 사용한 세션키 교환방식으로 객체인증, 키 신규성, 키 확인, 키 동의가 이루어지며 EKE 프로토콜의 Denning-sacco 공격의 취약성을 개선하기 위해 네트워크 참여자 A와 B가 각각 난수를 발생시켜 세션키 K를 생성한다. DH-EKE 프로토콜은 패스워드(P)에 해시함수 $H(P)$를 암호화키로 사용하여 대칭 암호시스템과 Diffie-Hellman 키 교환 프로토콜을 결합한 세션키 분배 프로토콜이다.

표 5. DH-EKE 프로토콜에 사용되는 계수
Table 5. Parameters Involved in DH-EKE Protocol

계 수	의 미
A, B	참여자 A, B
A^{ID}	참여자 A의 ID
P	패스워드
p, g	큰 소수, 원시근
A^R, B^R	참여자 A, B의 난수
$E_P(M)$	M을 패스워드로 대칭 암호화
C_A, N_A	A에 의해 생성된 $Challenge$값과 난수
$E_K(M)$	M을 세션키 K로 대칭 암호화
$Challenge_A$, $Challenge_B$	A와 B의 자신의 검사값

표 5는 DH-EKE 프로토콜에 사용되는 계수이다. 네트워크 참여자 A는 P를 선택하고 B는 해시된 패스워드의 검증자 $H(P)$를 가지고 있으며 전체적인 인증절차는 그림 15와 같다.

A는 자신의 난수 A^R를 선택하고 큰 소수 p의 원시근 g에 A^R을 지수승하여 A^{ID}와

함께 B와 해시함수로 공유된 패스워드 $H(P)$를 이용하여 식 (3.12)와 같은 형태로 암호화한 후 B에게 전송한다.

$$A^{ID}, E_{H(p)}(g^{A^R} \bmod p) \quad (3.12)$$

B는 A로부터 전송된 $A^{ID}, E_{H(p)}(g^{A^R} \bmod p)$를 공유된 패스워드로 복호화하여 A^R을 구한 후 자신의 난수 B^R로 지수승하여 식 (3.13)과 같이 세션키 K를 구한다.

$$K = (g^{A^R})^{B^R} = g^{A^R B^R} \bmod p \quad (3.13)$$

B는 자신의 공개키 g^{B^R}을 공유된 패스워드 $H(P)$로 암호화하고 자신의 검사값 $Challenge_B$를 세션키 K로 암호화하여 식 (3.14)와 같은 형태로 A에게 전송한다.

$$E_{H(P)}(g^{B^R} \bmod p), E_K(Challenge_B) \quad (3.14)$$

A는 B로부터 전송된 메시지 $E_{H(P)}(g^{B^R} \bmod p), E_K(Challenge_B)$를 복호화하여 B의 공개키 g^{B^R}을 생성한 후 A의 개인키 A^R을 지수승하여 세션키 $K = g^{B^R A^R}$를 생성하고 K를 이용하여 $Challenge_B$를 복호화 한다. A는 키 확인을 위해 자신의 검사값 $Challenge_A$와 $Challenge_B$를 식 (3.15)와 같이 K로 암호화하여 B에게 전송한다.

$$E_K(Challenge_A, Challenge_B) \quad (3.15)$$

B는 A로부터 전송된 $E_K(Challenge_A, Challenge_B)$를 K로 복호화하여 B가 가지고 있는 $Challenge_B$와 A로부터 전송된 $Challenge_B$의 일치여부에 따라 A와 동일한 세션키를 공유했음을 확인하고 A를 인증한다. 그리고 $Challenge_A$를 식 (3.16)과 같이 세션키 K로 암호화하여 A에게 전송하고, A는 전송된 $Challenge_A$의 일치여부를 확인한 후 B를 인증한다.

$$E_K(Challenge_A) \quad (3.16)$$

패스워드 기반 DH-EKE 프로토콜은 악의적인 노드가 네트워크 참여자 A, B의 패스워드를 알기 위해서는 Diffie-Hellman의 공개키를 알아야하며, 공개키를 알기 위해

서는 생성된 세션키 K를 알아야하는 문제점을 지니고 있다. K는 신분을 위장한 능동적 공격자도 자신의 전송정보를 이용한 패스워드 추측 공격을 성공적으로 수행할 수 없기 때문에 완전한 PFS를 제공한다[52].

악의적인 노드가 K를 알고 있더라도 A^R, B^R을 모르기 때문에 추측한 패스워드가 A의 패스워드임을 확인할 방법이 없어 Denning-sacco 공격에 안전하다. 하지만 사전에 B가 악의적인 노드에 의해 저장된 A의 패스워드가 노출 되었다면, 악의적인 노드는 A의 패스워드를 이용하여 A로 위장한 후 B에 접속하여 세션키를 공유할 수 있기 때문에 Stolen-verifier 공격에 취약하다.

모든 패스워드 기반 인증키 교환 프로토콜은 패스워드에 대한 사전 공격에 취약하고 Stolen-verifier 공격 때문에 DN을 무조건 신뢰해야 한다. 패스워드 기반 키 교환 프로토콜을 MANET에 이용할 경우 라우팅 보안과 패스워드 추측 공격에 안전해야 하며 상호인증이 제공되는 신뢰성이 강한 OTP를 이용한 키 교환 인증기법이 필요하다.

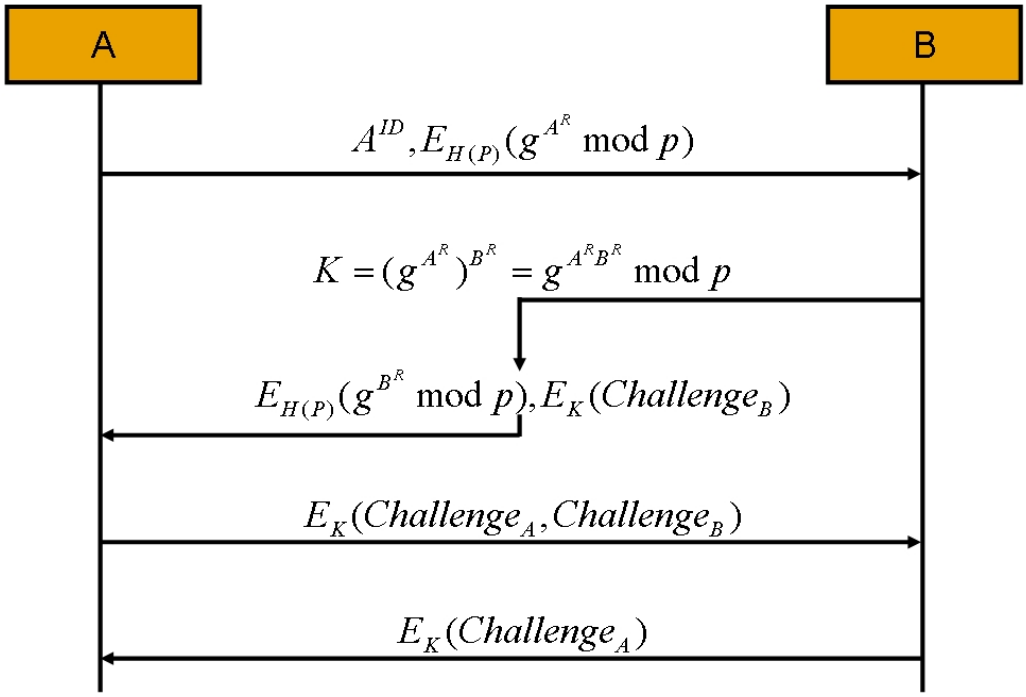


그림 15. 패스워드 기반의 DH-EKE 프로토콜

Fig. 15. DH-EKE Protocol based on Password

Ⅳ. *OTP-EKE* 인증기법

MANET은 MN간에 패킷 데이터를 전송하는 동적 네트워크로 침입이나 오동작으로 인한 심각한 보안상 취약점을 지니고 있다. 네트워크 중간에 훼손된 MN이 발생되면 MN간 신뢰관계는 변하게 되고 신속하게 처리할 수 있는 MANET 보안 환경의 강인한 MN 인증기법이 필요하다.

MANET 보안 환경을 위해 공개키 암호화를 이용한 인증기법, OTP를 이용한 인증기법 등이 연구가 되고 있다. 그러나 공개키 암호화를 이용한 인증기법은 전자서명을 검증하는 과정에서 소요되는 시간이 커진다는 단점을 가지고 있어 시간적 효율성을 보장하기 어렵고, OTP를 이용한 인증기법 또한 안전한 키 관리나 기밀성 문제를 충족하지 못하는 단점이 존재한다.

MANET 환경의 OTP를 이용하는 인증기법 중 가장 활발히 사용되고 있는 OTP S/Key 인증기법은 MN들을 신뢰한다는 가정 하에 연구가 되고 있어, 악의적인 노드가 네트워크에 참여시 사전 공격, 스푸핑, 중재자 공격 그리고 패스워드 추측 공격에 대한 많은 문제점이 존재한다.

본 논문은 MANET 보안 환경을 구축하기 위해 MANET 인증기법의 문제점을 분석하고 경로설정을 위한 라우팅 보안과 OTP S/Key 인증기법의 문제점을 해결할 수 있는 패스워드 기반 키 교환 프로토콜의 적용으로 동적 네트워크 토폴로지에 즉시 대응할 수 있는 신뢰성이 강한 OTP-EKE 인증기법을 제안한다.

그림 16과 같이 OTP-EKE 인증기법은 안전한 통신경로를 확보하는 라우팅 단계와 MN 인증을 위한 검증 및 키 교환 단계로 구성하였다. 라우팅 단계에서는 전자서명이 사용된 공개키 요소의 첫 세트를 반복적으로 MD5에 적용하여 해시테이블을 생성하고 생성된 해시테이블로부터 공개키 요소들의 여러 세트를 유도한다. 각 MN들은 OTP를 포함한 해시된 AODV 라우팅 생성을 통해 기밀성과 무결성을 제공하는 안전한 경로설정을 한다. MN 인증을 위한 검증 및 키 교환 단계에서는 SN과 DN사이의 MD5로 해시된 패스워드 검증자 $H^n(P)$를 등록하는 등록 단계와 세션이 연결될 때 마다 SN과 DN 사이의 세션키를 교환하는 키 교환 단계로 구성하였다. 세션키 설정시 $H^n(P)$ 검증자로 암호화하여 키 교환을 수행하며, $H^n(P)$는 SN과 DN사이의 패스워드를 알 수 없으며 패스워드에서 생성된 $H^n(P)$를 저장하여 패스워드가 직접 노출되는 것을 막을

수 있을 뿐만 아니라 악의적인 노드의 가장 공격을 막을 수 있다.

OTP-EKE 인증기법의 라우팅 단계와 인증 단계의 MD5 사용은 IEEE 802.11의 패스워드 암호화를 이용한 MN인증 체계에 따른 것이며, MD5의 사용으로 악의적인 노드는 패스워드 암호화를 풀기 위해 방대한 전산자원을 감수해야 하며 결국 악의적인 노드는 패스워드 추측 공격을 포기할 수밖에 없다.

OTP-EKE 인증기법은 SN의 강력한 인증을 위해 OTP S/Key 인증기법에 DH-EKE 프로토콜을 개선하고 적용하였다. 그러나 제안 인증기법에 EKE를 적용한다면 DN을 무조건 신뢰한다는 조건하에 수행되어지므로 공개키 CA방법이나 분산 CA방법들과 차이가 없어 완전한 MANET 환경이라 할 수 없다. 제안 인증기법에서는 SN과 DN사이에 안전한 라우팅을 위해 OTP를 적용한 해시된 AODV 라우팅 프로토콜을 이용하여 $H^n(P)$로 암호화된 라우팅 메시지의 변조에 대한 무결성을 확보할 수 있었고, MN의 강력한 인증을 위해 $H^n(P)$ 검증자로 암호화하여 키 교환을 수행하는 공통적인 방식을 적용하였다.

OTP-EKE 인증기법은 MANET상에 해시된 AODV 적용으로 라우팅 보안과 세션키와 DLP 연산을 통한 MN의 인증 보안을 확보하여 안전성과 효율성을 향상시켰으며, 완전한 MANET 환경의 신뢰성이 강한 인증기법이라 할 수 있다.

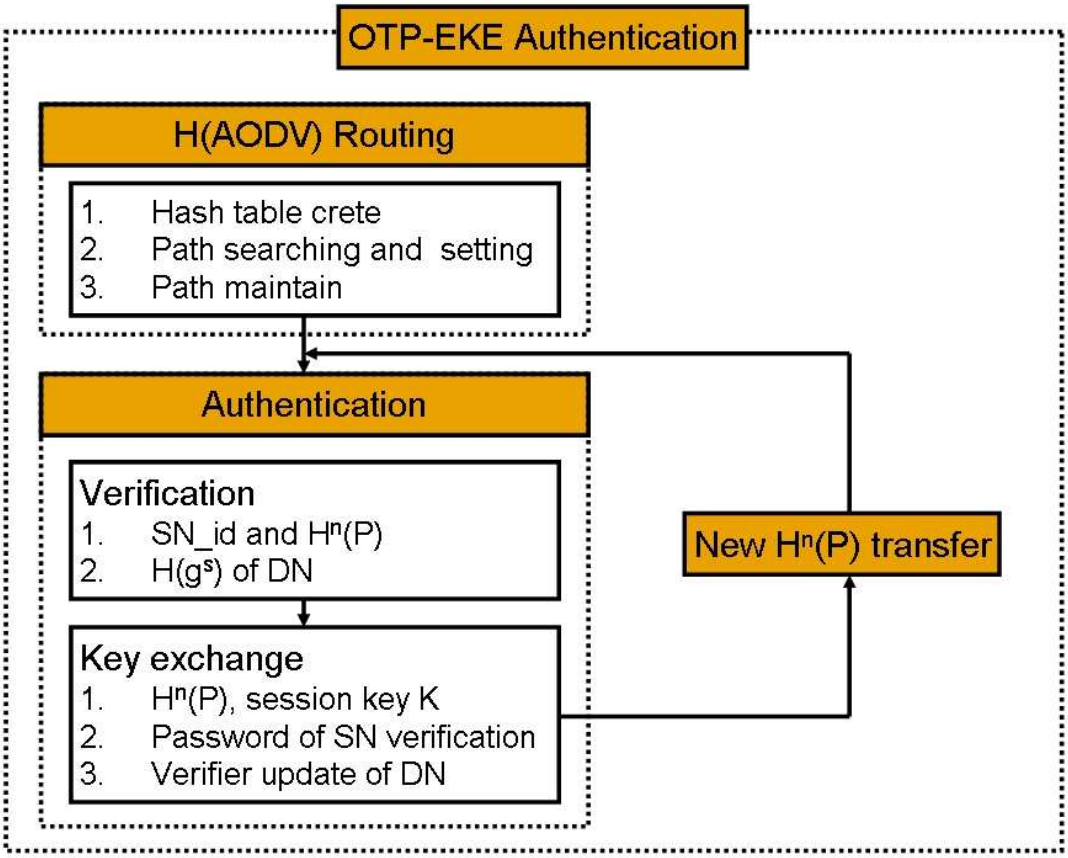


그림 16. MANET 기반 OTP-EKE 수행절차

Fig. 16. OTP-EKE Process based on MANET

A. OTP-EKE 보안 요구사항

MANET 환경에서 패스워드 기반 키 교환 프로토콜을 이용한 인증기법들은 MANET의 보안 특성과 안전성이 유지되어야 한다. OTP-EKE 인증기법에서는 신뢰성 있는 MN의 인증을 위해 경로설정을 위한 라우팅 보안과 인증을 위한 키 교환 보안의 요구조건을 만족하도록 설계하였다.

MANET의 라우팅 프로토콜은 각 MN이 전송된 라우팅 데이터를 전적으로 신뢰하기 힘들다는 원칙적 제한을 가질 수밖에 없다. 이는 MN이 상호협력에 의존하여 라우팅을 수행하기 때문이다. MN은 특정 DN의 라우팅 정보를 받을 경우 신뢰도순으로 순위를 매김 할 수 있어야 하며, 라우팅 경로설정이 정확하지 않을 경우 이를 삭제할 수 있는 기법이 필요하다. 또한 정적 네트워크 토폴로지를 구성할 때에도 각 MN이 주기적으로 라우팅 메시지를 주고받기 때문에 높은 네트워크 오버헤드를 부담해야 한다.

패스워드 기반 키 교환 인증기법에서는 정보량 측면에서 낮은 엔트로피를 갖는 패스워드를 사용하여 인증하고 패스워드를 기반으로 세션키를 설정하기 때문에 추측 공격, 사전 공격 등에 취약할 수 있다[53]. 따라서 이러한 공격들에 대해서 안전성이 유지되어야하며 그 밖에 세션키를 설정하는데 고려해야 하는 보안 특성도 만족해야 한다.

MANET의 라우팅 프로토콜과 인증기법의 연구는 MN을 신뢰한다는 가정 하에 수행되고 있지만, 각 MN들은 패킷 포워딩, 라우팅, 네트워크 관리기능을 수행하므로 부정행위를 할 수 있는 기회가 증가한다[54]. 따라서 OTP-EKE 인증기법에서는 안전한 경로설정을 위한 라우팅 보안과 인증을 위한 키 교환 보안 요구사항을 만족해야 한다.

그림 17은 OTP-EKE 인증기법의 보안 요구사항으로 라우팅 보안과 인증을 위한 키 교환 보안으로 나눈다. 라우팅 보안을 위한 요구사항으로는 악의적인 노드로부터 MN 간 전송되는 라우팅 메시지의 각 필드의 위·변조와 스푸핑에 대한 위장 공격에 안전해야하고, 인증을 위한 키 교환 보안 요구사항으로는 재전송 공격, 중재자 공격, 세션키로부터 패스워드를 유출하는 Denning-sacco 공격, 악의적인 노드가 DN과 세션키를 공유하는 Stolen-verifier 공격 및 PFS에 만족하도록 라우팅 단계와 인증키 교환 단계를 설계한다.

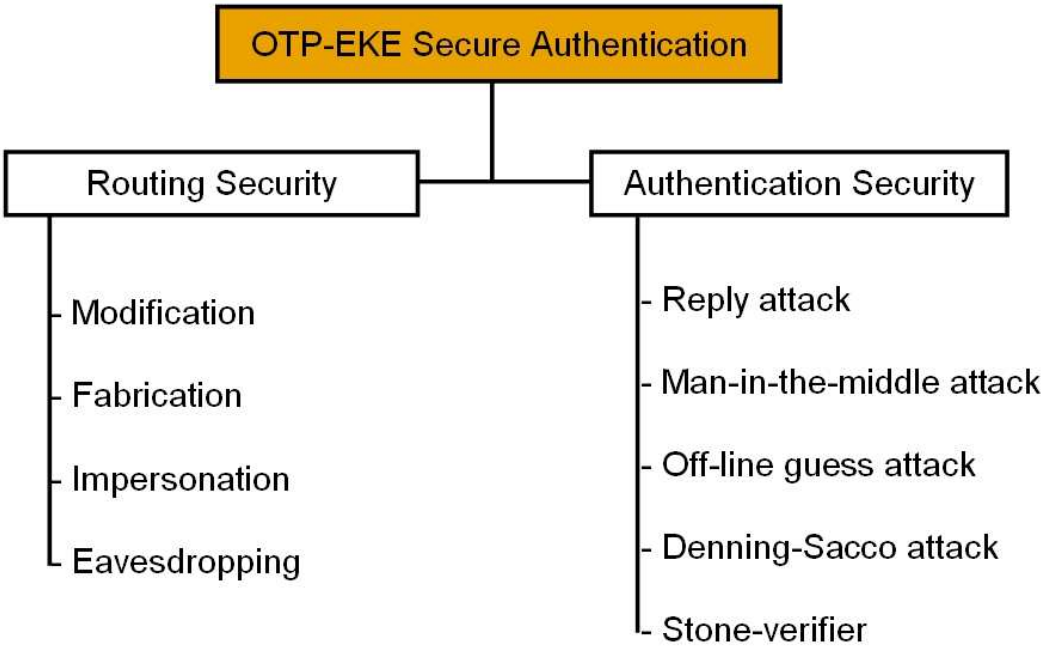


그림 17. MANET OTP-EKE 인증 요구사항

Fig. 17. OTP-EKE Authentication Requirements in MANET

B. 안전한 통신경로 확보를 위한 라우팅

그림 18과 같이 OTP-EKE 인증기법의 안전한 통신경로를 확보하는 라우팅 단계에서는 On-demand 방식의 AODV 라우팅 프로토콜에 OTP를 결합한 해시된 *H(AODV)* 라우팅 프로토콜을 사용한다. MD5 수행으로 생성된 OTP는 라우팅 메시지를 인증하고 악의적인 노드로부터 메시지의 위·변조에 대한 기밀성과 무결성을 제공한다.

라우팅 단계에서는 라우팅 프로토콜이 개시되기 전에 OTP 전자서명에 사용될 키 생성을 위한 해시테이블 생성과정이 수행되며, 해시테이블 생성 후 각 MN은 해시테이블의 해시체인을 통해 경로탐색 및 경로설정을 수행한다. 경로탐색을 위한 RREQ 메시지와 경로설정을 하는 RREP 메시지의 검증을 OTP 전자서명과 동일한 방법으로 수행하여 MN간에 홉 카운터 정보를 보호하였다.

OTP-EKE 인증기법의 안전한 통신경로 확보를 위한 라우팅 단계에서는 OTP 키 생성을 위한 해시테이블을 생성하고, OTP를 적용한 *H(RREQ)*와 *H(RREP)* 메시지를 사용하는 경로탐색 및 경로설정 단계와 경로유지 및 관리 단계로 나눈다.

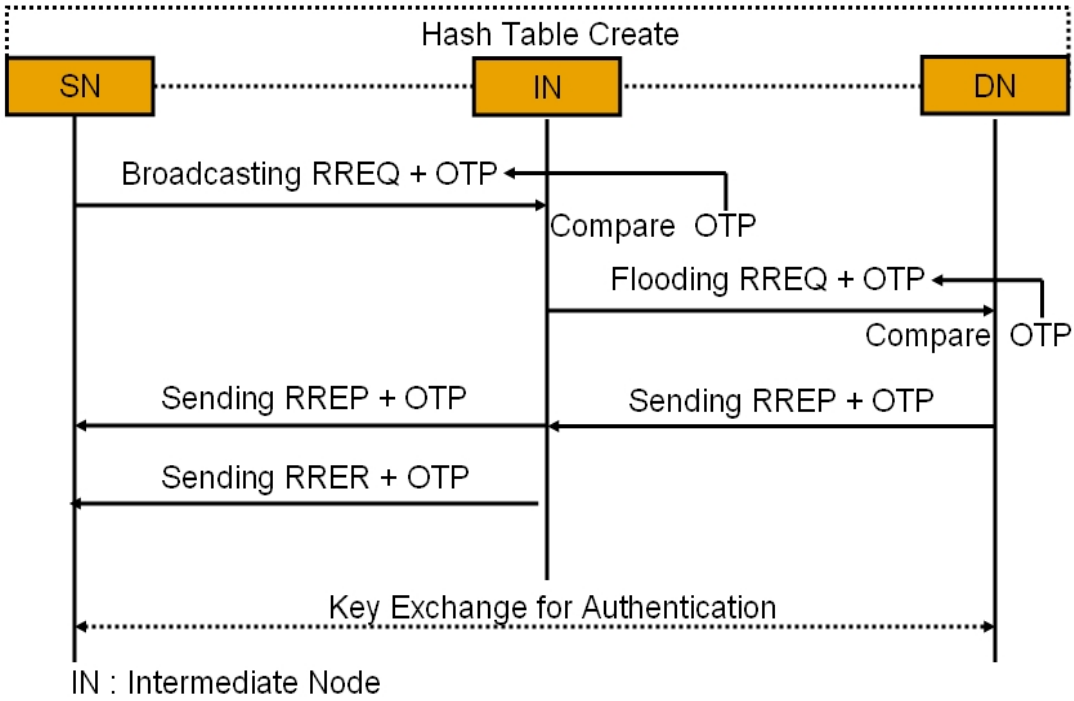


그림 18. OTP-EKE 인증기법의 라우팅 단계

Fig. 18. Routing Step of OTP-EKE Authentication Technique

1. 라우팅을 위한 해시테이블 생성

OTP-EKE 인증기법에서는 라우팅 프로토콜에 개시되기 전에 MN들은 OTP 키 생성을 위한 해시테이블을 생성해야 한다.

그림 19와 같은 해시테이블은 MD5를 사용하며 하나의 비트열 x로부터 해시체인 $h^0(x), h^1(x), \cdots, h^n(x)$을 생성한다. i가 1부터 길이 n일때 $h^0(x)$은 x, $h^1(x)$은 $h^0(x)$에 한번 더 해시한 $h(h^0(x))$이고, $h^i(x)$는 $h(h^{i-1}(x))$이다. 그리고 각 MN들은 n비트인 k개의 메시지를 OTP를 이용하여 해시테이블을 생성한다. 각 MN들은 해시테이블을 생성하기 위해 j가 1부터 길이 n일 때 비밀키 요소인 x_j를 선택하고 n개의 비밀키 요소에 대해 길이가 k인 해시체인을 생성한다. SN은 공개키 기반 암호화 시스템을 사용하여 해시테이블의 k번째의 비밀키로 메시지를 서명하여 전송하고, 이웃한 MN들은 SN으로부터 전송된 $h^k(x_j)$값을 검증한 후 j가 1부터 길이 n인 v_j를 MN의 OTP 공개키 요소로 사용되며, $h^k(x_j)$는 라우팅 단계의 OTP로 사용된다.

0	$h^0(x_1)$	$h^0(x_2)$	$h^0(x_3)$	$\cdots$	$h^0(x_j)$	$\cdots$	$h^0(x_n)$
1	$h^1(x_1)$	$h^1(x_2)$	$h^1(x_3)$	$\cdots$	$h^1(x_j)$	$\cdots$	$h^1(x_n)$
2	$h^2(x_1)$	$h^2(x_2)$	$h^2(x_3)$	$\cdots$	$h^2(x_j)$	$\cdots$	$h^2(x_n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
$k-i$	$h^{k-i}(x_1)$	$h^{k-i}(x_2)$	$h^{k-i}(x_3)$	$\cdots$	$h^{k-i}(x_j)$	$\cdots$	$h^{k-i}(x_n)$
k	$h^k(x_1)$	$h^k(x_2)$	$h^k(x_3)$	$\cdots$	$h^k(x_j)$	$\cdots$	$h^k(x_n)$

그림 19. MN들의 해시테이블

Fig. 19. Hash Table of MNs

2. 라우팅 탐색 및 설정

안전한 통신 경로설정을 위해 SN이 DN까지 라우팅을 하고자 할 때, SN의 라우팅 테이블에 DN까지의 라우팅 정보가 없을 경우 이웃한 MN들로부터 DN까지 라우팅 경로 탐색을 위한 *H(RREQ)* 메시지를 전송하여 경로탐색을 시작한다.

그림 20의 경로탐색을 위한 요청 메시지인 *H(RREQ)*는 Type을 1로 설정하고 브로드캐스드 ID, i번째 홉 카운트, DN의 IP주소, DN의 순차번호, SN의 IP주소, SN의 순차번호, 카운터 그리고 RREQ 패킷의 OTP를 포함한다.

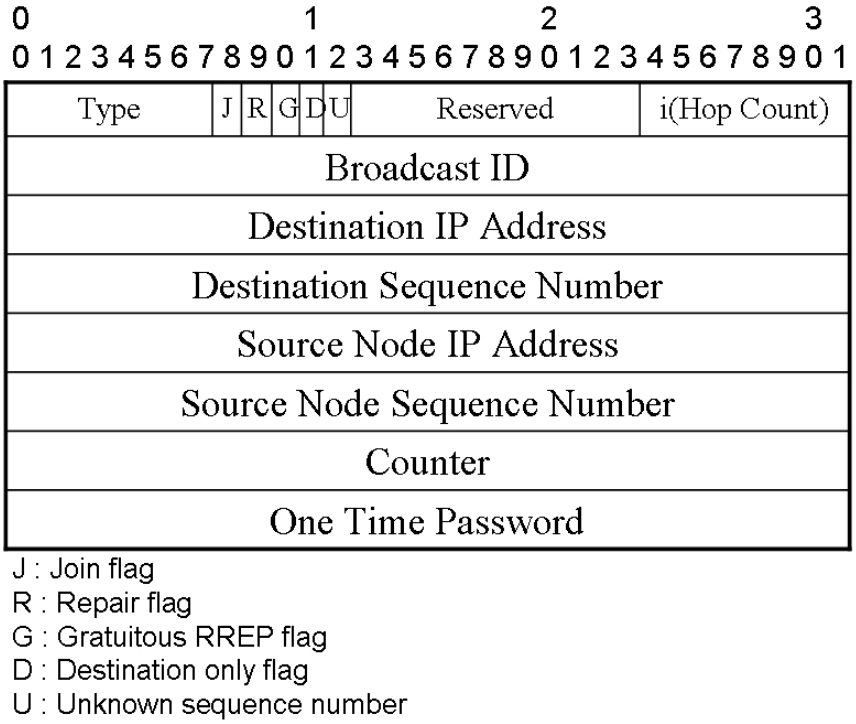


그림 20. *H(RREQ)* 메시지

Fig. 20. *H(RREQ)* Message

그림 21과 같이 SN은 전송하고자 하는 i번째 RREQ 메시지를 서명하기 위해 MD5 (*448 mod 512*)를 적용하여 무결성이 보장된 $H(RREQ_i)$를 생성한다. $H(RREQ_i)$는 SN의 메시지의 각 비트를 서명하기 위해 하나의 비밀키 x와 하나의 공개키 y를 생성하여

서명할 메시지의 추가비트를 구성하기 위해 $\log_2 n$비트가 메시지에 추가된다.

$H(RREQ_i)$에서 0의 비트수를 계산하여 $H(RREQ_i)$에 추가하고 n비트의 비트 스트링 g를 갖게 된다. j번째 비트 스트링 g_j가 1인 모든 j에 대하여 각 MN에서 생성된 해시 테이블의 $(k-i)$번째 행에서 $h^{k-i}(x_j)$ 해시 값을 찾아 $H(RREQ_i)$ 메시지에 추가하여 식 (4.1)과 같은 OTP를 생성하고 $H(RREQ)$ 메시지를 이웃한 MN들에게 전송한다.

$$H(RREQ) = H(RREQi) + h^{k-i}(x_j) \qquad (4.1)$$

$H(RREQ)$ 메시지를 수신한 이웃한 MN은 전자서명 검증을 위해 MD5를 적용하여 $H(RREQ_i)$를 얻고 $\log_2 n$후 메시지의 비트열의 0의 개수를 계산하여 $H(RREQ_i)$에 추가한 후 n비트 스트링 g값을 생성한다. j번째 비트 스트링 $g_j = 1$인 모든 j에 대하여 $h^{i-i'}(r_j) = v_j$ 인지를 체크한다. r_j는 현재 전송된 $H(RREQ)$ 메시지의 OTP이고, v_j는 $H(RREQi')$번째 메시지에 대한 OTP이다. $h^{i-i'}(r_j) = v_j$가 동일하다면 라우팅 정보의 무결성이 보장되었다는 것을 알 수 있으며, $H(RREQ)$를 검증한 MN은 다음 $H(RREQ)$ 메시지 탐색과 검증을 위해 v_j를 r_j값으로 갱신하여 SN에서부터 DN까지 포워딩 절차를 반복 수행한다.

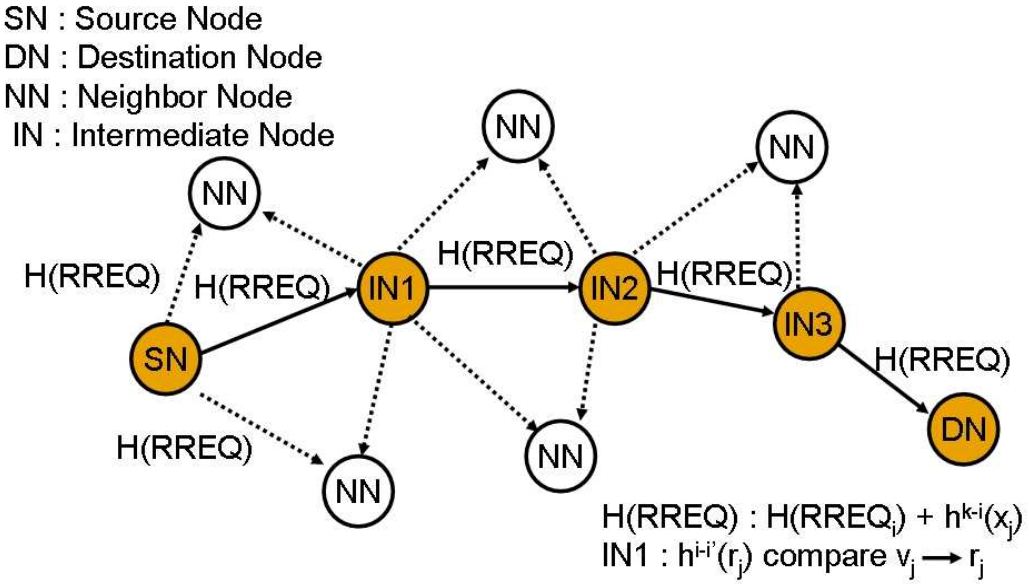


그림 21. 라우팅 경로탐색

Fig. 21. Routing Path Searching

SN으로부터 *H(RREQ)* 메시지를 수신한 DN은 *H(RREQ)*에 대한 응답 메시지인 *H(RREP)*를 생성하여 SN에서 DN까지 생성된 역 경로를 통해 *H(RREP)* 메시지를 전송한다.

그림 22와 같은 *H(RREP)* 메시지는 Type을 2로 설정하고 프리픽스 사이즈, 해당 노드의 홉 카운트, DN의 IP주소, DN의 순차번호, SN의 IP주소, 라이프 타임, 카운터 그리고 RREP 패킷의 OTP를 포함한다.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	R	A	Reserved	Prefix Sz	i(Hop Count)
Destination IP Address					
Destination Sequence Number					
Source Node IP Address					
Lifetime					
Counter					
One Time Password					

R : Repair flag
A : Acknowledgement required

그림 22. *H(RREP)* 메시지

Fig. 22. *H(RREP)* Message

그림 24와 같이 DN의 i번째 *H(RREP)* 메시지는 *H(RREQ)* 메시지와 동일한 무결성을 제공하기 위해 MD5를 적용하여 $H(RREP_i)$를 생성한다. $H(RREP_i)$ 메시지의 추가 비트를 구성하기 위해 $\log_2 n$비트가 메시지에 추가되며 $H(RREP_i)$에서 0의 비트수를 계산하여 $H(RREP_i)$에 추가하고 n비트의 비트 스트링 g를 갖게 된다. j번째 비트 스트링 g_j가 1인 모든 j에 대하여 각 MN에서 생성된 해시테이블의 $(k-i)$번째 행에서 $h^{k-i}(x_j)$ 해시 값을 찾아 *H(REEP)* 메시지에 추가하여 OTP를 생성하고 *H(RREP)* 메시지를 *H(RREQ)*의 역 경로를 통해 이웃한 MN들에게 전송한다.

H(RREP) 메시지를 받은 IN3노드는 전자서명 검증을 위해 MD5를 적용하여 $H(RREP_i)$를 얻고 $\log_2 n$후 메시지의 비트열의 0의 개수를 계산하여 $H(RREP_i)$에 추가한 후 n비트 스트링 g값을 생성한다. j번째 비트 스트링 $g_j = 1$인 모든 j에 대하여 $h^{i-i'}(r_j) = v_j$인지를 체크한다. r_j는 현재 전송된 *H(RREP)* 메시지의 OTP이고, v_j는 $H(RREPi')$번째 메시지에 대한 OTP이다. $h^{i-i'}(r_j) = v_j$가 동일하다면 라우팅 정보가 기밀성과 무결성이 보장되었다는 것을 알 수 있다. *H(RREP)*를 검증한 IN3노드는 다음 *H(RREP)* 메시지 탐색과 검증을 위해 v_j를 r_j값으로 갱신하여 IN3부터 SN까지 포워딩 절차를 반복 수행한다. 이를 통해 악의적인 노드가 다른 MN으로 위장하여 거짓된 라우팅 정보를 유포하거나, *H(RREP)*에 대한 재생 공격을 막을 수 있으며, SN까지 DN이 보낸 *H(RREP)* 메시지가 전송되면 그림 23과 같이 *H(AODV)*를 이용한 안전한 라우팅 경로가 확보된다.

Type = 1 //H(RREQ)
Hop Count = 0
Broadcast ID += 1
Destination IP Address
Destination Sequence Number = Last Destination Sequence Number
Source IP Address
Source Sequence Number = Last Destination Sequence Number + 1
One Time Password

Type = 2 //H(RREP)
Hop Count = 1 //Destination Node
Hop Count = Destination Hop + 1 //Intermediate Node
Destination IP Address
Destination Sequence Number = last Destination Sequence Number + 1 //Destination Node
Destination Sequence Number = last Destination Sequence Number //Intermediate Node
Source IP Address
Lifetime = Routing Effective Time
One Time Password

그림 23. *H(AODV)* 경로설정 과정

Fig. 23. *H(AODV)* Path Setting Process

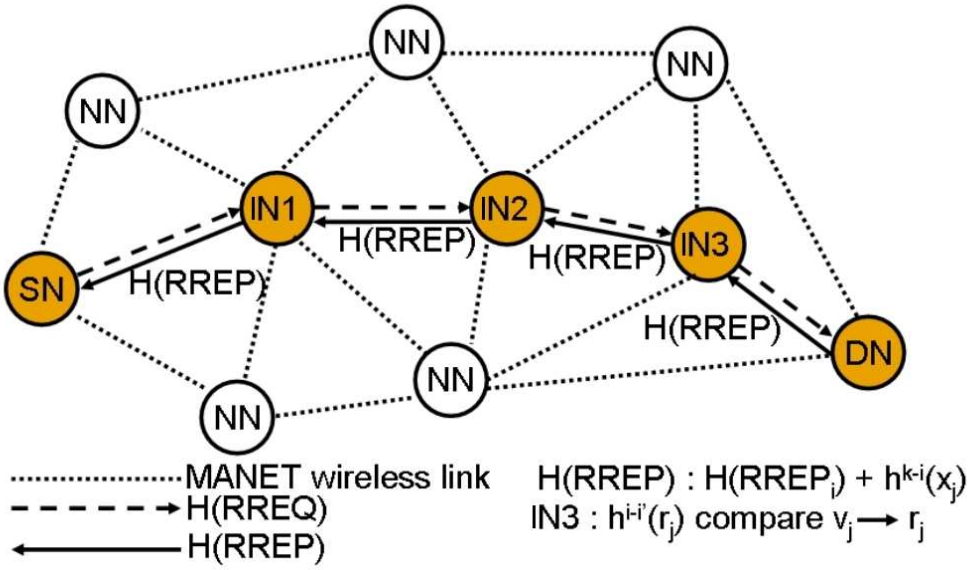


그림 24. 라우팅 경로설정

Fig. 24. Routing Path Setting

3. 라우팅 유지 및 관리

경로설정 이후 각 MN들은 라우팅 경로가 유효한지를 확인하기 위해 이웃한 MN들에게 주기적으로 확인 메시지를 전송한다. MN들은 라이프타임 동안 경로상의 트래픽 발생이 없다면 MN의 라우팅 테이블에 경로가 활동하지 않는다고 체크한다. 그러나 유효하지 않는 경로로부터 데이터가 전달되면, MN은 SN으로 향하는 역 경로를 이용하여 그림 25와 같은 *H(RRER)* 메시지를 생성하여 전송한다. 또한 MN들의 동적 특성으로 인해 경로상의 링크가 끊어진 경우도 *H(RRER)* 메시지를 생성하여 SN에게 전송한다. *H(RRER)* 메시지는 해당 노드의 DestCount, 도착 불가능한 DN의 IP주소, 도착 불가능한 DN의 순차번호, 카운터, *H(RREP)* 패킷의 OTP가 포함된다.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	N	Reserved	DestCount
Unreachable Destination IP Address (1 ~ n)			
Unreachable Destination Sequence Number (1~ n)			
Counter			
One Time Password of H(RREP)			

N : No delete flag

그림 25. *H(RRER)* 메시지

Fig. 25. *H(RRER)* Message

그림 26과 같이 *H(RRER)* 메시지가 SN에 도달할 때 까지 경로 상에 있는 MN들은 *H(RREQ)*와 *H(RREP)* 메시지와 동일하게 서명, 검증하고 다시 자신의 서명을 하여 메시지를 포워딩하는 절차를 반복적으로 수행한다. 악의적인 노드가 경로가 끊어졌다는 거짓된 *H(RRER)* 메시지를 위조하여 발송할 경우 악의적인 노드의 행동을 탐지하는 것은 어렵지만 *H(RRER)* 메시지가 OTP로 서명되어 있기 때문에 악의적인 노드가 다른 적법한 MN으로 위장하여 *H(RRER)* 메시지를 생성하는 공격을 막을 수 있다.

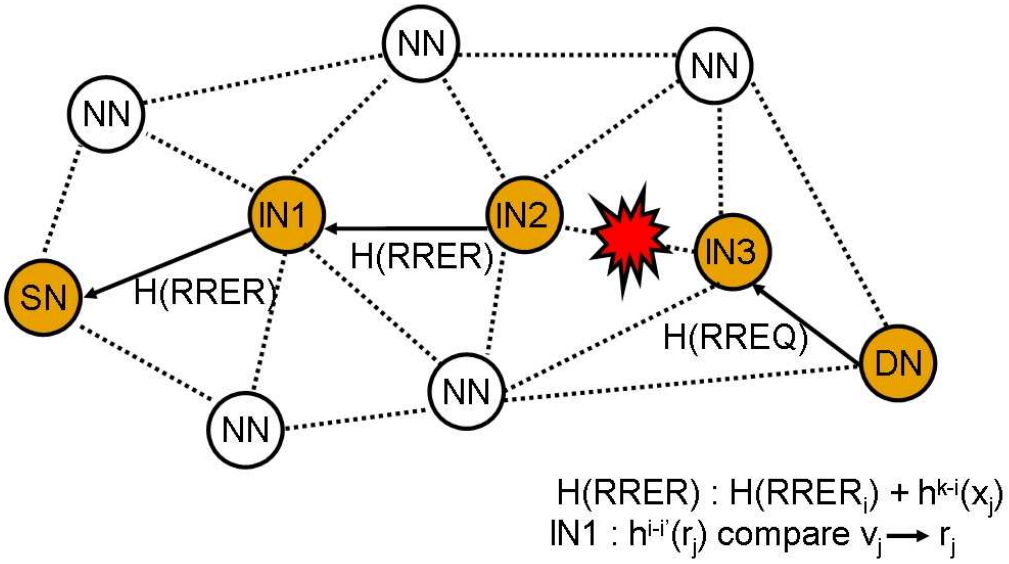


그림 26. 라우팅 경로유지

Fig. 26. Routing Path Maintain

C. 인증을 위한 검증 및 키 교환

OTP-EKE 인증기법의 두 번째 단계인 인증을 위한 검증 및 키 교환 단계에서는 기밀성과 무결성이 제공되는 $H(AODV)$를 이용하여 SN의 정보를 DN에 등록한 후 등록된 정보를 검증하고 세션키를 교환하는 단계로 SN의 등록 및 검증 단계와 인증을 위한 키 교환 단계로 구성된다.

SN의 등록 및 검증 단계에서는 초기화 과정 중 악의적인 노드가 SN의 패스워드를 도청하지 못하도록 MD5를 n번 적용하여 패스워드 검증자 $H^n(P)$를 DN에 전송한다. DN은 패스워드 검증자 $H^n(P)$를 이용하여 OTP S/Key 인증기법과 동일하게 SN을 검증하며 $(n-1)$번째 세션에서 새로운 $H^n(P)$를 설정하는 단계이다.

인증을 위한 키 교환 단계에서는 SN과 DN사이의 세션키를 설정하여 암호화 과정을 수행하는 단계로 MANET의 안전성과 효율성을 제공한다.

표 6. OTP-EKE 인증 기법에 사용되는 계수

Table 6. Parameters Involved in OTP-EKE Authentication Technique

계 수	의 미
$H(AODV)$	해시된 라우팅
SN_id	SN의 ID
$H^n(P)$	패스워드 검증자
$H(g^s)$	SN과 DN의 공개 패스워드
$Sn \in_R [1, p-1]$	SN의 랜덤한 비밀값
g^{Sn}	SN의 키 재료값
$Dn \in_R [1, p-1]$	DN의 랜덤한 비밀값
g^{dn}	DN의 키 재료값
$K=g^{SnDn}$	세션키
$K'=g^{Sns}$	세션 패스워드 검증자
g^s	DN의 장기 공개키
$H(K \| K')$	키 검증 메시지

1. SN 등록 및 검증

SN의 등록 및 검증 단계의 초기화 과정인 등록 단계는 그림 27과 같이 SN과 DN사이에 신뢰성 있는 검증을 위해, SN은 *SN_id*와 해시함수를 *n*번 적용하여 생성된 패스워드 검증자 $H^n(P)$를 안전한 통신경로인 *H(AODV)*를 통해 DN에게 전송한다. DN은 SN으로부터 전송된 *SN_id*와 $H^n(P)$를 패스워드 디렉토리 내에 저장하고 SN과 DN사이에 인증을 위한 공개 패스워드 $H(g^s)$를 *H(AODV)*를 통해 SN에게 전송한다.

등록 단계에서 $H^n(P)$는 MN간 세션시 악의적인 노드가 쉽게 패스워드를 알아내는 것을 불가능하게 한다. SN은 자신의 패스워드만 기억하고, DN은 SN의 패스워드에서 생성된 임의의 값인 $H^n(P)$만 기억하기 때문에 SN의 패스워드가 직접 노출되는 것을 막을 수 있을 뿐만 아니라 악의적인 노드의 가장 공격을 막을 수 있다.

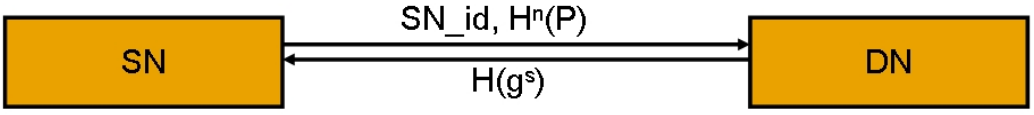


그림 27. 등록 단계

Fig. 27. Registration Step

검증 단계에서는 SN과 DN의 등록과정을 마친 후 $H^n(P)$를 기반으로 SN이 패스워드를 알고 있음을 증명하며 DN의 패스워드 디렉토리에 저장되어 있는 $H^n(P)$를 다음 세션을 위한 검증자로 갱신하는 일을 한다.

$H^n(P)$는 OTP S/key 인증기법과 동일하게 매 세션마다 해시함수가 하나씩 줄어들기 때문에 패스워드를 설정한 후 $i(i \le i < n)$번째 세션에서는 SN의 $H^{n-i+1}(P)$와 DN의 $H^{n-i}(P)$가 패스워드 검증자로 사용된다. 또한 초기에 설정한 패스워드 검증자가 $(n-1)$번째 세션이 진행된 후에는 새롭게 패스워드 검증자를 생성하여 전송한다.

그림 28은 SN과 DN사이의 시간의 흐름에 따른 검증자를 검증하는 단계를 보이고 있다. 첫 세션에서 SN은 등록시킨 $H^n(P)$ 검증자를 통해 DN과 세션을 공유하고 SN의 패스워드 소유를 증명하기 위해 사용될 검증자 $H^{n-1}(P)$를 암호화하여 전송한다.

$H^{n-1}(P)$는 SN이 패스워드를 알고 있다는 것을 증명하며, 중간에 위치한 악의적인

노드가 $H^n(P)$를 알고 있더라도 해시된 $H^{n-1}(P)$를 알지 못하기 때문에 SN의 패스워드를 생성할 수 없다. DN은 SN으로부터 전송된 $H^{n-1}(P)$에 한번 더 해시함수를 적용하여 $H(H^{n-1}(P))$값과 DN의 패스워드 디렉토리 내에 저장되어 있는 $H^n(P)$값이 같은지를 비교한다. $H(H^{n-1}(P))$와 $H^n(P)$값이 같다면 $H^{n-1}(P)$가 정당하게 생성 되어졌으며 동시에 SN의 패스워드 값을 확인할 수 있다.

$H(H^{n-1}(P))$와 $H^n(P)$의 비교 과정이후 DN은 $H^{n-1}(P)$를 디렉토리에 저장하고 (n-1) 번째 통신까지 동일한 방법으로 검증자를 검증한다. 그리고 검증자는 OTP S/Key 특성상 설정된 일정횟수만큼 사용할 수 있는 해시테이블의 해시체인 형태로 표현되며, DN의 검증 단계 이후 SN과 DN은 생성된 검증자를 통해 인증을 위한 키 교환 단계를 수행한다.

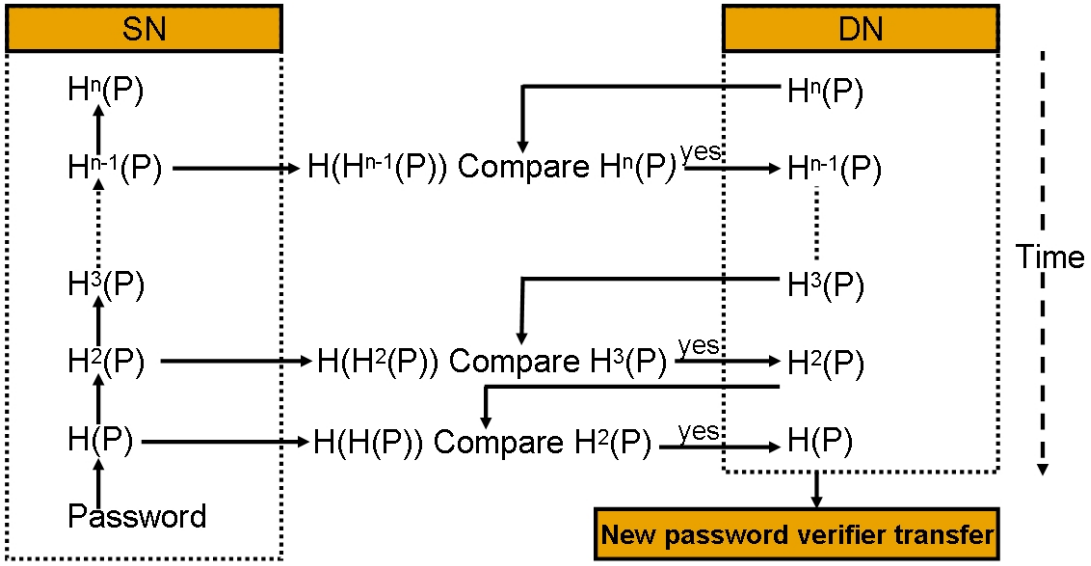


그림 28. 검증 단계

Fig. 28. Verification Step

2. 인증키 교환 단계

인증키 교환 단계에서는 OTP-EKE 인증기법의 초기화 과정인 등록 단계와 검증 단계를 수행한 후 각 MN들의 해시테이블에 $H^n(P)$ 검증자를 저장하고 SN과 DN사이에 암호화를 수행하여 세션키를 생성한다.

SN과 DN사이의 암호화를 위한 i번째 세션의 과정별 수행과정은 그림 29와 같다. SN은 랜덤하게 생성된 비밀값 $Sn \in_R [1, p-1]$과 세션키를 생성하기 위한 키 재료값 g^{Sn}을 계산한다. 악의적인 노드가 g^{Sn}에 위·변조 공격을 수행하는 것을 방지하기 위해 초기화 과정에서 SN과 DN사이에 비밀리에 공유했던 $H^{n-i+1}(P)$로 g^{Sn}를 암호화하여 SN_id와 함께 식 (4.2)와 같은 형태로 DN에게 전송한다.

$$SN_id,\ E(H^{n-i+1}(P),\ g^{Sn}) \qquad (4.2)$$

DN은 SN으로부터 $SN_id,\ E(H^{n-i+1}(P),\ g^{Sn})$를 수신한 후 SN의 암호화된 키 재료값 $E(H^{n-i+1}(P),\ g^{Sn})$를 DN의 패스워드 디렉토리에 저장된 SN의 패스워드 검증자 $H^{n-1}(P)$를 이용하여 식 (4.3)과 같이 복호화한 후 g^{Sn}을 추출한다.

$$D(H^{n-1}(P),\ g^{Sn}) \qquad (4.3)$$

DN은 랜덤하게 생성된 비밀값 $Dn \in_R [1, p-1]$을 선택하여 세션키를 생성하기 위한 키 재료값 g^{dn}를 계산하고, 식 (4.4)와 같이 g^{Sn}에 g^{dn}의 지수승 계산을 하여 세션키 K를 생성한다.

$$K = g^{SnDn} \qquad (4.4)$$

DN은 장기 비밀키 s를 이용하여 다음 세션에 사용될 패스워드 검증자 K'를 식 (4.5)를 이용하여 계산한다.

$$K' = g^{Sns} \qquad (4.5)$$

세션키 K와 패스워드 검증자 K' 생성을 끝낸 DN은 SN과 DN이 공통으로 생성한 키의 값이 서로 동일한지를 검증하기 위해 식 (4.6)과 같은 키 검증 메시지를 생성한다.

$$H(K \| K') \quad (4.6)$$

키 검증 메시지는 MD5를 근거하여 생성되기 때문에 키 값을 정확히 계산하는 SN과 DN만이 키 검증 메시지를 생성해 낼 수 있다. 키 검증 메시지를 생성한 후 DN의 장기 공개키 g^s와 키 재료값 g^{Dn}을 악의적인 노드로부터 위·변조 공격을 방지하기위해 SN과 비밀리에 공유했던 $H^{n-i+1}(P)$를 이용하여 g^{Dn}을 암호화한 후 키 검증 메시지 $H(K \| K')$와 함께 SN으로 식 (4.7)과 같은 형태로 전송한다.

$$E(H^{n-i+1}(P),\ g^{Dn}),\ g^s,\ H(K \| K') \quad (4.7)$$

SN은 DN으로부터 메시지를 수신한 후 $E(H^{n-i+1}(P),\ g^{Dn})$를 자신의 패스워드 검증자로 복호화하고 DN의 장기 공개키 g^s에 해시함수를 적용하여 자신이 가지고 있는 공개 패스워드 $H(g^s)$값과 같은지를 비교한다. DN으로부터 전송된 g^s값과 해시함수를 적용한 SN의 g^s값이 일치하지 않는다면, DN이 올바르지 않은 장기 공개키 값을 전송한 것이므로 SN과 DN사이에 세션을 종료한다. 또한 DN이 장기 비밀키 s를 알고 있음을 검증하기 위해 K'를 사용한다.

OTP-EKE 인증기법의 키 교환 과정에서는 Diffie-Hellman 키 교환 프로토콜의 어려움에 근거하여 장기 비밀키 s를 모르면 SN의 키 재료값 g^{Sn}과 DN의 키 재료값 g^{Dn}를 악의적인 노드가 획득 했을지라도 $K' = g^{Sns}$를 계산하지 못한다. 따라서 DN이 키 검증 메시지를 제대로 생성하여 보냈다면 DN의 장기 비밀키 s를 올바르게 알고 있음을 증명한다.

SN은 랜덤하게 생성된 비밀값 $Sn \in_R [1,\ p-1]$을 이용하여 g^{Sn}과 세션키 $K = g^{SnDn}$ 그리고 $K' = g^{Sns}$를 계산한 후 키 검증 메시지 $H(K \| K')$값을 확인한다. 키 검증 메시지에 대한 검증을 끝낸 후, SN은 다음 세션을 위해 $H^{n-i}(P)$와 세션키 $K = g^{SnDn}$를 해시함수에 적용한 메시지 $H(K)$를 식 (4.8)과 같이 K'로 암호화하여 DN에게 전송한다.

$$E_{K'}(H^{n-i}(P),\ H(K)) \quad (4.8)$$

$K' = g^{Sns}$는 SN의 다음 세션 패스워드 검증자를 DN에게 전송하기 위하여 사용된 인증키이며 SN과 DN만이 생성할 수 있는 값이다. 그러므로 악의적인 노드는 K'를 생성하지 못하기 때문에 다음 세션에 SN의 패스워드 검증자를 암호화하여 전송할 때

K'를 사용한다. DN은 SN으로부터 K'를 이용해 복호화하여 $H(K)$를 확인하고 SN과 세션키 K를 올바르게 공유했음을 확인한다. 또한 수신한 패스워드 검증자 $H^{n-i}(P)$에 해시함수를 한번 더 적용하여 $H(H^{n-i}(P))$값과 $H^{n-i+1}(P)$값이 식 (4.9)처럼 같은 값인지를 비교하여 두 값이 일치한다면, DN은 SN이 패스워드를 올바르게 알고 있다는 사실을 인증하게 된다. SN과 DN이 적법한 인증절차를 수행했다면, DN은 SN의 패스워드 검증자 $H^{n-i}(P)$로 교체하여 디렉토리에 저장한다.

$$H(H^{n-i}(P))\ compare\ H^{n-i+1}(P) \qquad (4.9)$$

OTP-EKE 인증기법의 SN과 DN사이의 인증키 생성과정은 패스워드 검증자 $H^{n}(P)$를 OTP S/Key 인증기법으로 만들기 때문에 설정된 패스워드를 다 사용한 후 새로운 패스워드로 교체하여 검증자를 생성해야 한다. 이는 설정된 패스워드 검증자를 이용하여 마지막 세션에서 프로토콜을 수행할 때 SN과 DN사이의 인증된 세션키로 새로운 패스워드 검증자를 암호화한 후 전송하는 방법으로 수행된다.

제안한 OTP-EKE 인증기법은 악의적인 노드가 세션키 K를 구하기 위해 패스워드에 대한 사전 공격을 시도하는 경우, 악의적인 노드가 선택한 패스워드가 올바른 것인지를 알기 위해서는 공개키 암호화 기법을 풀어야 하고 DLP 어려움을 지니고 있으며 이를 풀기위해서는 높은 엔트로피를 요구하므로, OTP-EKE 인증기법은 MANET 환경의 안전성과 효율성을 제공한다.

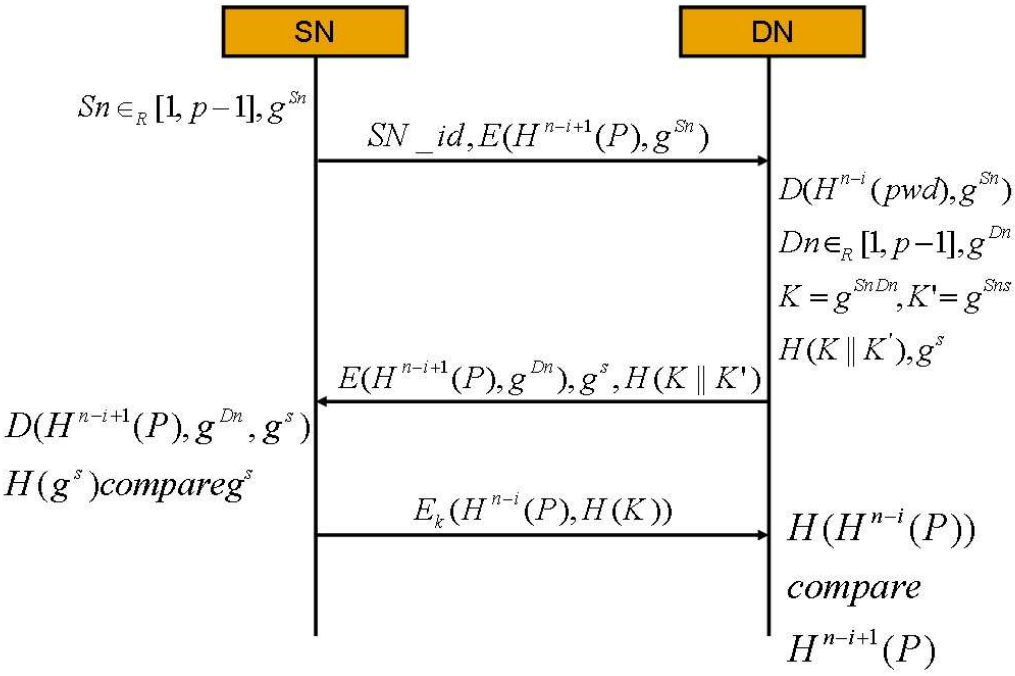


그림 29. SN과 DN사이의 키 교환

Fig. 29. Key Exchange of Between SN and DN

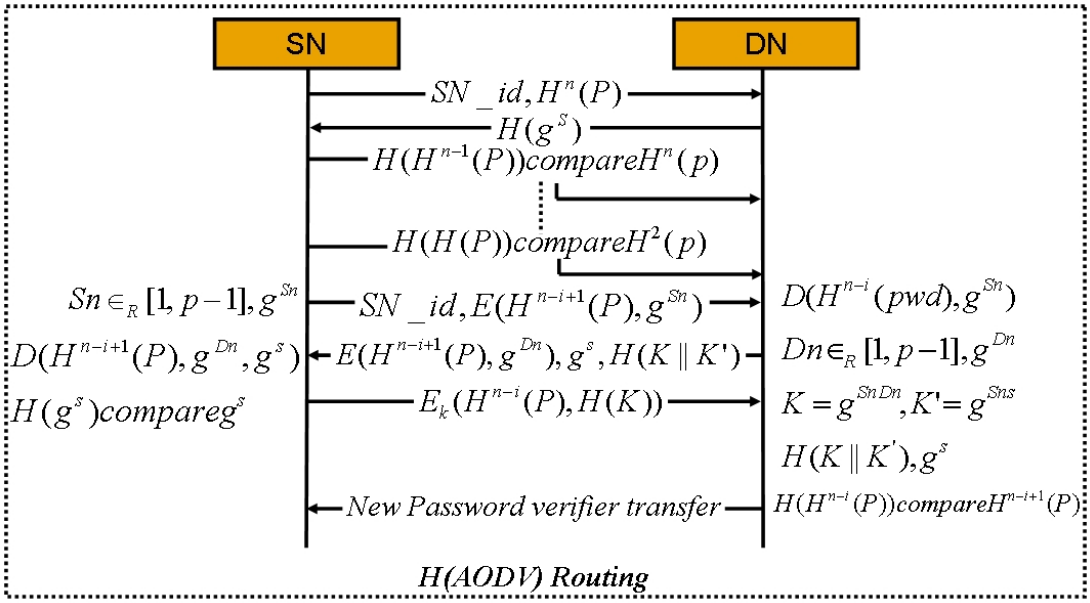


그림 30. OTP-EKE 인증절차

Fig. 30. OTP-EKE Authentication Process

V. *OTP-EKE* 인증기법 실험 및 결과분석

OTP-EKE 인증기법의 실험 및 결과분석을 위해 시뮬레이션을 하여 제안기법의 안전성과 효율성을 비교 평가하였다. 시뮬레이션 환경으로는 유닉스 및 리눅스 환경에서 구동되는 NS2(NS-allinone-2.29)[55]를 사용하여 IEEE 802.11 링크계층과 TDMA에 따라 MANET 환경에 맞도록 설계하였다.

각 MN은 무작위로 선택되었던 NN과 세션을 생성하고 512byte 4개 패킷이 전송되며, 각 MN은 임의의 DN을 향하여 0과 MAX(20m/sec)의 일률적으로 배포되는 스피드로 움직이고, 시뮬레이션 시간은 0~900/sec이다. 또한 오버헤드는 $n/\log_2 n$패킷에 대한 개별인증을 제공하여 패킷에 포함된 오버헤드를 측정하였다.

SN은 데이터를 일정한 크기의 블록으로 등분한 후 각 블록을 서명하는 대신에 각 블록에 대한 고정크기의 해시 값으로 구성된 해시테이블을 생성하여 대표서명을 한다. 그 후 인증된 데이터를 요청하는 DN에게 해시테이블을 먼저 전송하며, DN은 해시테이블을 저장하고 서명을 인증한 후, 전송되는 각 데이터 블록이 DN에 도착하면 미리 전송된 해시테이블의 검증자를 통해 빠르게 인증하도록 하였다.

A. 시뮬레이션 환경

표 7은 MANET 환경에서 OTP-EKE 인증기법의 시뮬레이션을 하기위한 환경과 시스템 현황이다.

표 7. 시뮬레이션 환경

Table 7. Simulation Environment

구 분	모 델
CPU	Pentium4 3.0G
RAM	640MB
OS	Redhat Linux9 Kernel 2.4.20-8smp
Network Simulator	ns-allinone-2.29
Language	C, C++
MANET	1000 × 1000(m^2), 50 nodes
Mobility	Random waypoint, Random drunken, Trace based
Radio Model	Noise Accumulating
Data Link(MAC)	CSMA, IEEE 802.11 and MAC
Network Routing	H(AODV)
Transport	UDP (654 port)
Simulation Time	0~900 sec, Pause Time (5sec)
Packet	4 × 512byte/sec
Application	CBR, FTP, HTTP, and Telnet

1. NS2 시뮬레이터

OTP-EKE 인증기법의 성능평가를 위한 실험도구인 NS2 시뮬레이터는 네트워킹을 연구하기 위하여 개발 되었으며 MANET, WLAN, Mobile-IP, UMTS, 위성 네트워크 등과 같은 무선 네트워크뿐만 아니라 유선 네트워크까지 지원할 수 있는 매우 광범위한 시뮬레이션 도구이다.

NS2 시뮬레이터의 구조상 특징은 그림 31과 같이 이벤트 스케줄러와 IP 기반의 네트워크 컴퍼넌트로 이루어진 Event-Driven 방식을 채택한 시뮬레이터이고, 프로그램 언어는 TCL(tcl8.4.11) 스크립트 언어에 객체지향의 개념을 추가한 OTcl(OTcl-1.11)과 C++이다. C++은 소스코드를 정의하고, OTcl은 MN의 인터페이스와 매개변수 등을 정의 하였으며 TclCL(tclcl-1.17)을 사용하여 OTcl과 C++를 연동시킨다.

그림 32는 NS2 시뮬레이터의 OTcl 클래스 계층구조이며, NS Object는 MANET 컴퍼넌트인 MN, 링크, 큐, 에이전트가 포함된다.

OTcl 클래스의 루트는 TclObject 클래스인 동시에 OTcl 라이브러리 오브젝트의 슈퍼클래스이다. OTcl 라이브러리 오브젝트에는 스케줄러, 네트워크 컴퍼넌트, 타이머 그리고 NAM과 관련된 오브젝트들이 있다. NsObject 클래스는 패킷을 처리하는 네트워크 컴퍼넌트를 포함하는 슈퍼클래스이고 MN이나 링크와 같은 네트워크 오브젝트를 포함하며 Connector 클래스와 Classifier 클래스로 나뉜다.

네트워크 오브젝트는 Connector 클래스에 바탕을 두고 있기 때문에 오직 한 개의 출력용 data path를 가지며, 스위칭 오브젝트는 Classifier 클래스에 바탕을 두고 있기 때문에 여러 개의 출력용 data path를 갖는다.

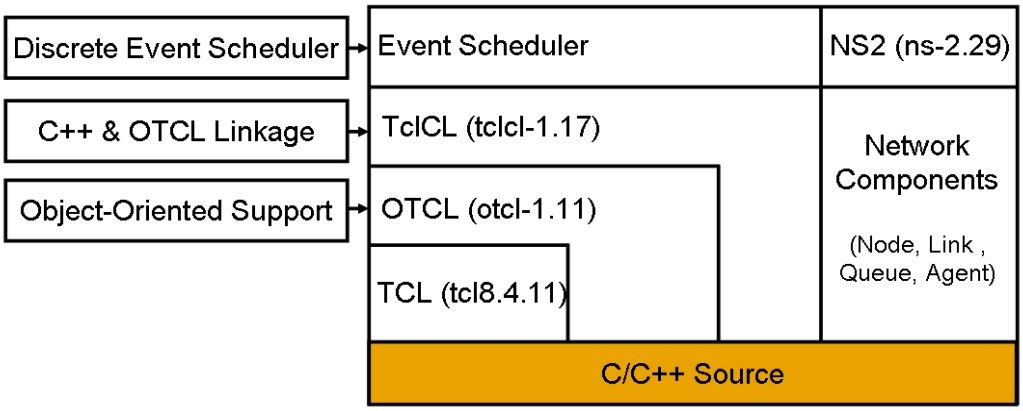


그림 31. NS-2.29 구조

Fig. 31. Architectural View of NS-2.29

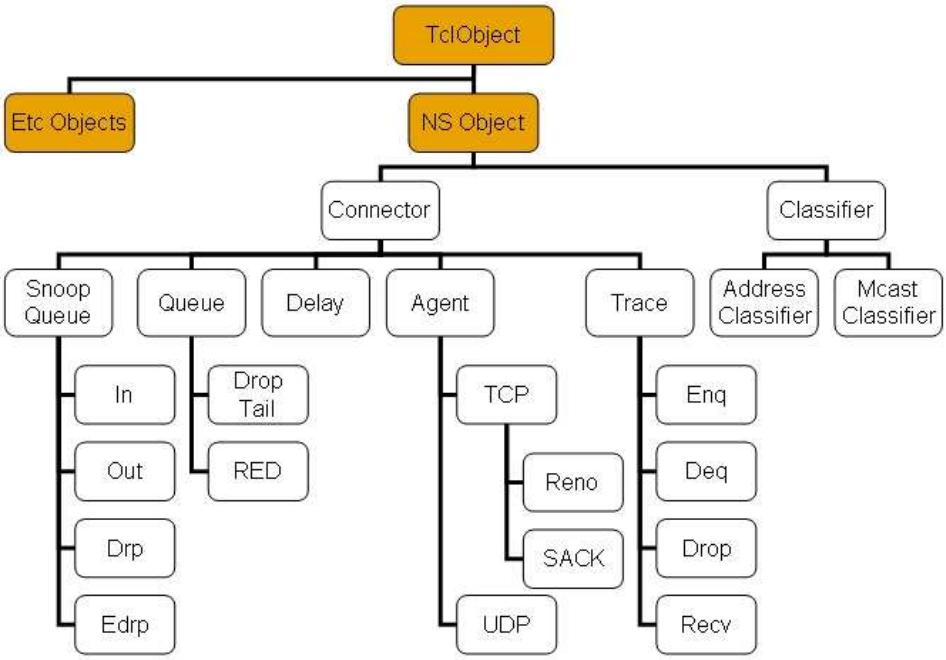


그림 32. NS-2.29 클래스 계층구조

Fig. 32. Class Hierarchy of NS-2.29

2. *MANET* 모델 설계

OTP-EKE 인증기법의 시뮬레이션을 하기위한 첫 작업으로 MANET 모델을 설계하였다.

그림 33과 같이 MANET 모델은 4단계의 과정으로 구성된다. 첫 번째, 동적인 네트워크 토폴로지 생성에서는 MN과 IEEE 802.11의 링크의 특성을 결정하고, MN에서 이용하는 CSMA, MAC 프로토콜 사용으로 MN의 트래픽 에이전트와 애플리케이션 서비스를 결정한다. 두 번째, 트래픽 에이전트는 전송계층에서 이용할 UDP 프로토콜을 결정한다. 세 번째 응용계층 프로토콜에서 전송하는 애플리케이션 서비스를 지정하는 작업으로 CBR, FTP, HTTP 그리고 Telnet과 같은 구체적인 트래픽 타입을 지정해 준다. 마지막 네 번째 과정은 모든 시뮬레이션의 기초가 되는 시뮬레이션 시간을 0~900(sec)로 설정하였다.

OTP-EKE 인증기법의 MANET 모델은 위 4단계의 과정을 적용하여 MN의 객체를 구성하였다. C++ MobileNode 클래스는 부모 클래스인 Node에서 파생 되었으므로, MN은 node 객체에 무선 환경과 MN의 기능이 추가된다. *H(AODV)* 라우팅 프로토콜은 MN이 무선채널을 액세스할 수 있도록 하는 네트워크 스택을 생성하는 방법을 다룬다. 그리고 무선 시뮬레이션을 위한 스택 컴퍼넌트, Trace 지원, Movement나 Traffic 시나리오를 작성한다. MN의 이동과 주기적인 위치갱신 그리고 토폴로지 경계유지 등과 같은 Mobility 특징들은 C++로 구현하였으며, MN과 관련된 네트워크 컴퍼넌트는 OTcl로 구현하였다. MN과 관련된 네트워크 컴퍼넌트는 Classifier, Demux, LL, MAC, Channel등이 있으며, MN의 움직임은 random waypoint를 사용하여 이동할 목적지를 무작위로 선택하고 0~20m/sec의 속도로 목적지를 향해 움직인다. 각 MN은 목적지에 도달한 후 5초 동안 머물다 또 다른 목적지로 이동하도록 하였다. MN의 random waypoint 사용은 실제 MANET에서 MN들의 움직임과 가장 흡사하므로 OTP-EKE 인증기법의 MN의 이동모델로 사용하였다.

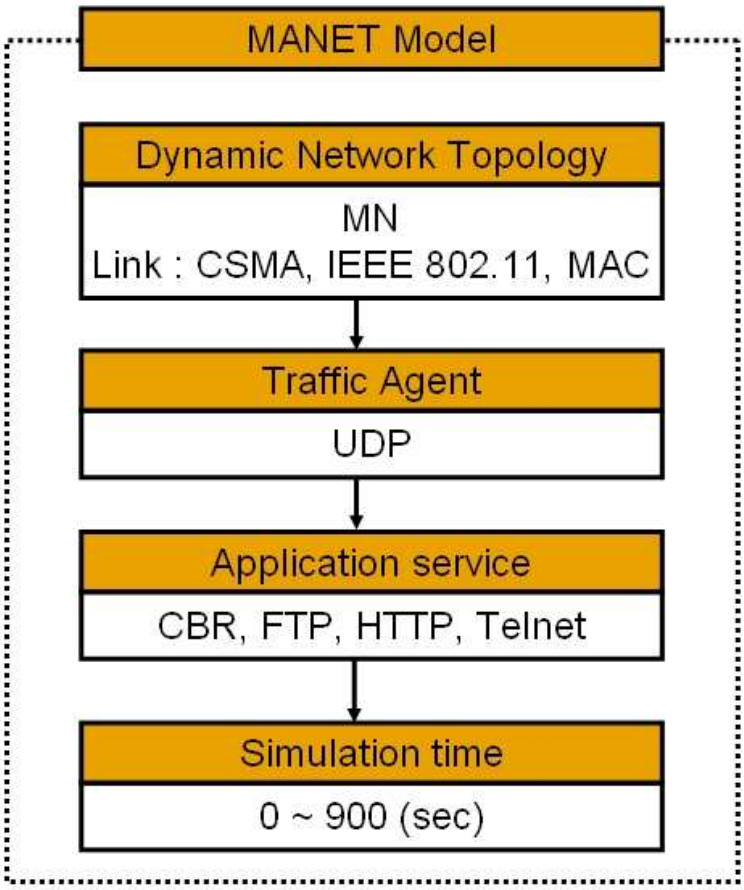


그림 33. MANET 모델 설계

Fig. 33. Design of MANET Model

B. 시뮬레이션 결과 분석

OTP-EKE 인증기법의 초기 패스워드 검증자 생성을 위해 MD5의 수행횟수 n을 4회로 설정하였으며 공통 매개변수인 p, g를 생성하였다.

그림 34의 34-1부터 34-10까지는 128비트 16진수로 출력된 시뮬레이션 결과 값이다. 실험에 사용된 p값과 g값은 임의의 선택된 값이며, p값과 g값을 다르게 부여한다면 측정결과는 달라진다.

SN과 DN사이에 큰 소수 p값을 997로 하고, g는 p의 원시근 중에 하나인 7로 선택하였다. 원시근은 p의 거듭제곱을 했을 경우 [1, p-1]까지를 랜덤하게 생성되고, 실험의 공통 매개변수 p, g는 SN과 DN사이에 세션이 바뀔 때 마다 $Sn \in_R [1, p-1]$ 랜덤하게 생성된다.

p	ec5aa0b7846082a2415f0902f0da88f2
g	07

그림 34-1. p와 g의 실험결과

Fig. 34-1. Simulation Result of p and g

DN은 SN과 DN의 세션에 사용할 장기 비밀키 s를 설정하고 SN과 DN 사이에 장기 공개키 g^s를 생성하며, s는 세션이 끝나도 변하지 않는 값이다.

s	e4da3b7fbbce2345d7772b0674a318d5
g^s	8694959cf2d53e57681d8fdc472468d6

그림 34-2. s와 g^s의 실험결과

Fig. 34-2. Simulation Result of s and g^s

*1. SN*의 검증자 생성 및 전송

SN은 초기 등록 단계에서 자신의 *SN_id*와 MD5를 4회 적용하여 생성된 패스워드 검증자 $H^4(P)$를 *H(AODV)*를 이용한 안전한 통신경로를 통해 DN에게 전송한다.

$H^4(P)$	0f9a156317d5bbd5ee8411643123487c

그림 34-3. $H^4(P)$의 실험결과

Fig. 34-3. Simulation Result of $H^4(P)$

SN의 패스워드는 MD5 16라운드를 한 값으로 128비트에 크기를 가진다. SN은 자신의 패스워드만을 기억하고, DN은 *SN_id*와 $H^4(P)$를 수신한 후 장기 공개키 g^s에 MD5를 1회 적용한 결과 값을 SN에게 전송한다.

$H(g^s)$	a07235a92149d6d0230d3e6d88f1dd89

그림 34-4. $H(g^s)$의 실험결과

Fig. 34-4. Simulation Result of $H(g^s)$

$H^4(P)$ 검증자는 SN과 DN의 첫 세션을 위해 사용되고, $H^4(P)$는 OTP S/Key 인증 기법과 동일하게 매 세션마다 해시함수가 하나씩 줄어들기 때문에 반복횟수 n이 1이 될 경우 새로운 패스워드 검증자를 생성해서 전송한다.

2. 인증키 교환

OTP-EKE 인증기법의 인증키 교환 단계에서는 $H^n(P)$를 기반으로 암호학적인 연산에 사용할 수 있는 공통 세션키 K를 설정하고, SN이 패스워드를 알고 있음을 증명하며, DN내에 저장되어 있는 SN의 $H^n(P)$를 다음 세션을 위한 검증자로 갱신하는 일을 한다. $H^n(P)$는 패스워드의 직접 노출을 막을 수 있을 뿐만 아니라 악의적인 노드의 가장 공격을 막을 수 있다.

SN은 랜덤하게 생성된 비밀값 $Sn \in_R [1, p-1]$을 선택하여 세션키 생성을 위한 키 재료값 g^{Sn}을 $H^4(P)$로 암호화하여 DN에게 전송한다. SN에 의해 생성된 비밀 랜덤키 Sn과 키 재료값 g^{Sn}은 한 세션에서만 사용되는 단기간 키 값으로 128비트 크기의 난수이다.

Sn	45c48cce2e2d7fbdea1afc51c7c6ad26
g^{Sn}	f840d8fb30c54c6e6dce5670c79ef837
$E(H^4(P),g^{Sn})$	9cc8337286822829fe72067d800b6d1a

그림 34-5. Sn와 g^{Sn} 그리고 $E(H^4(P),g^{Sn})$의 실험결과

Fig. 34-5. Simulation Result of Sn, g^{Sn} and $E(H^4(P),g^{Sn})$

DN은 SN으로부터 전송된 암호화된 키 재료값 g^{Sn}을 DN의 패스워드 디렉토리에 저장된 SN의 $H^4(P)$를 이용하여 복호화 한다.

DN은 랜덤하게 생성된 비밀값 $Dn \in_R [1, p-1]$를 선택하여 키 재료값 g^{Dn}을 계산한다. DN에 의해 생성된 비밀 랜덤값 Dn과 g^{Dn}은 한 세션에만 사용된 단기간 키 값으로 128비트 크기의 난수이다.

Dn	c9f0f895fb98ab9159f51fd0297e236d
g^{Dn}	118bd558033a1016fcc82560c65cca5f

그림 34-6. Dn과 g^{Dn}의 실험결과

Fig. 34-6. Simulation Result of Dn and g^{Dn}

DN은 SN으로부터 전송된 키 재료값 g^{Sn}에 DN의 비밀 랜덤값 Dn의 지수승을 계산하여 세션키 $K = g^{SnDn}$를 생성하며 장기 비밀키 s를 이용하여 다음 세션에 사용할 패스워드 검증자 $K' = g^{Sns}$를 계산한다.

K	3c14437d40671d67c816b98e423ffe24
K'	f579861acf6ffb31d6992bd637dbbe3a

그림 34-7. K와 K'의 실험결과

Fig. 34-7. Simulation Result of K and K'

DN은 세션키 K와 패스워드 검증자 K'의 키 값이 서로 동일한지를 검증할 검증메시지 $H(K||K')$와 $E(H^d(P),g^{Dn})$를 생성한다. $E(H^d(P),g^{Dn})$는 SN의 $H^d(P)$를 암호화키로 사용하고, 키 검증 메시지는 MD5를 근거하여 생성되기 때문에 키 값을 정확히 계산하는 SN과 DN에서만이 키 검증 메시지를 정확히 생성해 낼 수 있다.

$E(H^d(P),g^{Dn})$	5754c858e267fde24103d3e18a883738
$H(K\|\|K')$	3c14437d40671d67c816b98e423ffe24 f579861acf6ffb31d6992bd637dbbe3a

그림 34-8. $E(H^d(P),g^{Dn})$와 $H(K||K')$의 실험결과

Fig. 34-8. Simulation Result of $E(H^d(P),g^{Dn})$ and $H(K||K')$

DN은 장기 공개키 g^s와 $E(H^d(P),g^{dn})$를 $H(K||K')$와 함께 SN에게 전송한다. SN은 DN으로부터 전송된 메시지를 자신의 패스워드 검증자로 복호화하고 DN의 장기 공개키 g^s에 해시함수를 적용하여 SN의 $H(g^s)$와 같은 값인지를 비교한다. DN의 g^s에 해시함수를 적용시킨 값과 SN의 $H(g^s)$값이 일치하지 않는다면, DN은 올바르지 않은 장기 공개키 값을 전송한 것이므로 SN과 DN사이의 세션은 종료된다. 또한 DN이 장기 비밀키 s를 알고 있음을 K'를 사용하여 DN이 만든 키 검증 메시지를 통하여 검증한다. 장기 비밀키 s를 모르면 SN의 키 재료값 g^{Sn}과 DN의 키 재료값 g^{Dn}을 악의적인 노드가 획득했을 지라도 $K' = g^{Sns}$를 계산하지 못한다. DN이 K'를 올바르게 생성했다

면 s를 올바르게 알고 있음을 증명한다.

SN은 랜덤하게 생성된 비밀값 $Sn \in_R [1, p-1]$을 이용하여 g^{Sn}과 세션키 $K = g^{SnDn}$와 $K' = g^{Sns}$를 계산한 후 키 검증 메시지 $H(K||K')$값을 확인한다. 키 검증 메시지에 대한 검증을 끝낸 후, SN은 다음 세션을 위해 $H^3(P)$와 $H(K)$를 K'로 암호화하여 DN에게 전송한다.

$H^3(P)$	c8dd7cc459c3cc2fed1fbf26ad836710
$H(K)$	83d5121018497a02ad14fa8f4359fef2
$E_{K'}(H^3(P),H(K))$	74b0c4c4305dd0c5a017af910a716903

그림 34-9. $H^3(P)$와 $H(K)$ 그리고 $E_{K'}(H^3(P),H(K))$의 실험결과

Fig. 34-9. Simulation Result of $H^3(P)$, $H(K)$ and $E_{K'}(H^3(P),H(K))$

K'는 SN과 DN만이 생성할 수 있는 값으로 K'를 다음 세션에 SN의 패스워드 검증자를 암호화하여 전송하는데 사용한다. DN은 K'를 이용하여 $H(K)$를 확인하고 전송된 $H^3(P)$에 한번 더 해시함수를 적용하여 $H(H^3(P))$와 SN에게 보냈던 $H^4(P)$값이 같은지를 비교한다. $H(H^3(P))$와 $H^4(P)$가 일치한다면, DN은 SN이 패스워드를 올바로 알고 있다는 사실을 인증한 후 $H^3(P)$를 DN의 패스워드 디렉토리에 저장하여 패스워드 검증자 값을 갱신한다.

$H(H^3(P))$	0f9a156317d5bbd5ee8411643123487c
$H^4(P)$	0f9a156317d5bbd5ee8411643123487c

그림 34-10. $H(H^3(P))$와 $H^4(P)$의 실험결과

Fig. 34-10. Simulation Result of $H(H^3(P))$ and $H^4(P)$

그림 35. SN과 DN의 해시코드

Fig. 35. Hash Code of SN and DN

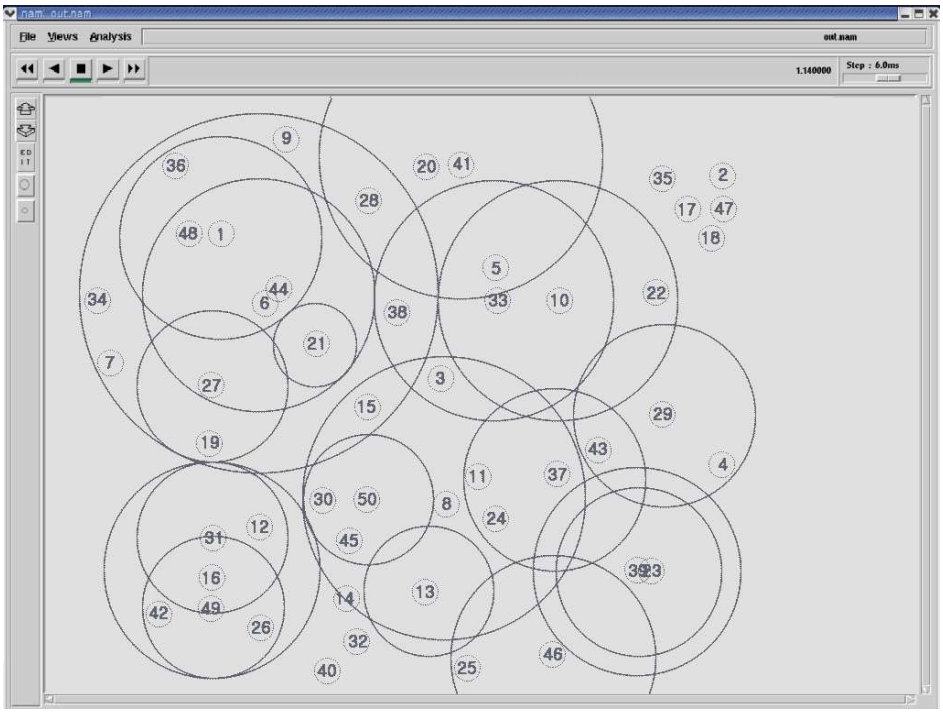


그림 36. NAM을 이용한 시뮬레이션 실행

Fig. 36. Execution of Simulation using NAM

C. OTP-EKE 인증기법의 안전성 및 효율성 분석

본 절에서는 OTP-EKE 인증기법과 MANET 기반 인증기법들의 보안 요구조건에 따라 안전성 분석과 검증 그리고 기존 인증기법과 효율성을 비교 분석하였다.

1. 안전성 분석 및 검증

OTP-EKE 인증기법의 안전성은 경로설정을 위한 라우팅 안전성과 인증을 위한 키 교환 안전성으로 구분하여 분석하고 안전성 검증을 위해 키 교환 단계의 DLP 과정을 통해 검증한다.

1-1. 라우팅 안전성

OTP-EKE 인증기법의 라우팅 단계에서는 라우팅 프로토콜이 개시되기 전에 MD5를 이용한 OTP를 생성하여 각 MN에 해시테이블 형태로 저장된다. MN사이에 경로탐색 메시지와 경로 응답 메시지가 식(5.1)과 식(5.2)를 사용하기 때문에 MN간 홉 카운터와 메시지 필드가 변조되지 않는다. 네트워크 중간에 위치한 악의적인 노드에 의해 라우팅 메시지가 변조 된다면 경로상 이웃한 MN에 의해 변조된 메시지는 탐지가 되며, 전송된 메시지는 삭제가 되어 라우팅 메시지 변조 공격에 대한 무결성을 제공한다.

$$H(RREQ) = H(RREQ_i) + h^{k-i}(x_j) \quad (5.1)$$

$$H(RREP) = H(RREP_i) + h^{k-i}(x_j) \quad (5.2)$$

라우팅 메시지는 네트워크 참여시 자신의 공개키를 다른 MN에게 전송한 MN만이 위조할 수 있어 위조된 메시지를 통한 공격유형을 식별하는 것은 어렵다. 하지만 제안 인증기법은 악의적인 노드가 서명한 공개키를 통해 위조된 라우팅 메시지를 보낸 MN을 알 수 있으므로 추후 라우팅 과정중 악의적인 노드를 제외시킬 수 있다.

OTP-EKE 인증기법에서는 MN들이 자신의 비밀키 값을 가지고 서명을 해야 하므로 경로탐색 과정에서 악의적인 노드들이 적법한 MN으로 위장하여 행동할 수 없다. 또한 경로설정 과정에서도 DN만이 자신의 비밀키 값을 가지고 전자 서명을 할 수 있으므로, 다른 MN이 DN을 대신하여 경로탐색 요청에 응할 수 없다.

악의적인 노드가 경로가 끊어졌다는 거짓된 RRER 메시지를 위조하여 발송할 경우 악의적인 노드의 행동을 탐지하는 것은 어렵지만, 식 (5.3)과 같은 $H(RRER)$ 메시지가 OTP로 서명되어 발송되기 때문에 악의적인 노드가 적법한 MN으로 위장하여 $H(RRER)$ 메시지를 생성하는 공격을 막을 수 있다.

$$H(RRER) = H(RRERi) + h^{k-i}(x_j) \quad (5.3)$$

1-2. 인증을 위한 키 교환 안전성

OTP-EKE 인증기법에서는 동일한 메시지가 연속적으로 전송되지 않고 매 세션마다 식 (5.4)와 식 (5.5)를 이용하여 난수와 $H^n(P)$를 통한 새로운 세션키를 생성한다. 악의적인 노드는 이전 세션의 메시지를 가지고 있을지라도 다음 세션의 난수와 세션키를 생성하지 못하기 때문에 재전송 공격에 안전하다.

$$Sn \in_R [1,\ p-1] \quad (5.4)$$

$$Dn \in_R [1,\ p-1] \quad (5.5)$$

중재자 공격은 Diffie-Hellman 기반의 키 교환 기법을 사용한 인증기법에서 공격대상이 된다. OTP-EKE 인증기법은 Diffie-Hellman 기반의 DH-EKE를 적용했기 때문에 중재자 공격에 취약할 수 있다. 하지만 세션키 K와 세션키 검증자 K' 사용으로 중재자 공격을 방지할 수 있다. 네트워크 중간에 위치한 악의적인 노드는 K와 K'를 알기 위해서는 g^{Sn}, g^{Dn}, g^{s}를 알아야하며, OTP-EKE 인증기법에서는 식 (5.6)과 같이 g^{Sn}, g^{Dn}이 $H^n(P)$로 암호화되기 때문에 악의적인 노드는 K와 K'를 알 수 없다.

악의적인 노드가 g^{Sn}, g^{Dn}을 획득했을지라도 DLP와 MD5 특성상 식 (5.7)를 이용한 K와 식 (5.8)를 이용한 세션키 검증자 K'를 알 수 없으므로 중재자 공격에 안전하다.

$$E(H^{n-i+1}(P),\ g^{Sn}) \quad (5.6)$$

$$K = g^{SnDn} \quad (5.7)$$

$$K' = g^{Sns} \quad (5.8)$$

OTP-EKE 인증기법에서는 SN의 세션키 K 생성이 SN의 공개키를 사용하지 않는 DH-EKE를 모태로 하기 때문에 Denning-sacco 공격을 방어할 수 있으며, K는 SN과 DN사이에 랜덤한 비밀값 $Sn \in_R [1, p-1]$과 $Dn \in_R [1, p-1]$에 의해 세션마다 바뀌게 된다. 악의적인 노드가 이전 세션키를 이용하여 현재 세션키 K를 구하는 것은 DLP를 푸는 공격자만 가능하다. 또한 노출된 K는 패스워드에 대한 정보를 포함하고 있지 않기 때문에 SN의 패스워드 정보를 알 수 없어 Denning-sacco 공격에 안전하다.

오프라인 추측 공격은 악의적인 노드가 MN들에 의해 자주 선택된 패스워드 사전을 가지고 공격하는 것을 말한다. 악의적인 노드가 추측 공격을 통해 패스워드를 알아낸다 하더라도 $H^i(P)$로 암호화된 메시지는 임의의 난수들로 추정가능 문이나 기지평문이 아니기 때문에 사전 공격을 통한 올바른 패스워드를 알아낸다는 것은 불가능하다.

OTP-EKE 인증기법에서 SN의 패스워드가 노출된다 하더라도 세션키의 안전성은 DLP의 어려움과 Diffie-Hellman 어려움에 기반하고 있어 PFS 보안성을 제공하고 Stolen-verifier 공격의 안전성을 제공한다.

1-3. OTP-EKE 인증기법 안전성 검증

OTP-EKE 인증기법의 안전성 검증을 위해 키 교환 단계의 DLP 과정을 설명한다. OTP-EKE 인증기법의 실험에 사용된 원시근 g값을 7로 했을 경우와 동일하게 임의의 소수 p에 대한 g값 7을 고정하고 식 (5.9)와 같이 라운딩한 결과 연속 4회에 해당하는 동일한 정수 a값의 찾을 수 없었다.

$$7^i = a \bmod p \qquad (5.9)$$

식 (5.9)의 i는 반복횟수를 의미하며 4회로 설정한 이유는 OTP-EKE 인증기법의 실험에 사용된 n횟수가 4회이고 안전성을 제공하기 위함이다. 그러나 표 8과 같이 소수가 37, 53, 59에 원시근 g가 2인 경우 4번의 연속적인 라운딩한 정수값이 같기 때문에 p를 알지 못해도 원시근 g에 대한 추측 공격이 가능하게 된다. 원시근 g에 대한 추측 공격을 해결하기 위해서는 p가 16이상인 경우 원시근 2를 사용하면 위험하고, p가 81 이상인 경우 원시근 3, p가 256이상인 경우 원시근 4, 그리고 p가 625이상인 경우 원시근 5를 사용하면, 악의적인 노드로부터 패스워드 추측 공격이 가능하므로 이 값을

사용하지 않는 것을 원칙으로 한다.

OTP-EKE 인증기법의 g^{Sn}은 $mod\ p$값보다 작을 경우 패스워드 추측 공격에 노출되므로 설정한 p값보다 커야한다. 그리고 악의적인 노드가 적법한 DN으로 위장하는 것을 방지하기 위해 SN의 원시근을 큰 값으로 부여해야 한다. OTP-EKE 인증기법은 위와 같은 패스워드 추측 공격, 위장 공격에 해당하는 p와 g값을 사용하지 않고 수행하기 때문에 안전성을 보장할 수 있다.

표 8. 원시근 2의 값

Table 8. Two of Primitive Root

$p = 37,\ g = 2$	$p = 53,\ g = 2$	$p = 59,\ g = 2$
$2^1 = 2 \bmod 37$	$2^1 = 2 \bmod 53$	$2^1 = 2 \bmod 59$
$2^2 = 4 \bmod 37$	$2^2 = 4 \bmod 53$	$2^2 = 4 \bmod 59$
$2^3 = 8 \bmod 37$	$2^3 = 8 \bmod 53$	$2^3 = 8 \bmod 59$
$2^4 = 16 \bmod 37$	$2^4 = 16 \bmod 53$	$2^4 = 16 \bmod 59$
$2^5 = 32 \bmod 37$	$2^5 = 32 \bmod 53$	$2^5 = 32 \bmod 59$

2. 효율성 분석

OTP-EKE 인증기법의 효율성을 분석하기 위해 AODV 라우팅과 해시된 AODV 라우팅을 각각 수행하는 OTP S/Key 인증기법, 해쉬된 AODV 라우팅을 수행하는 DH-EKE를 적용한 인증기법과 OTP-EKE 인증기법을 비교하여 효율성을 측정하고 분석한다. 효율성을 측정하기 위한 항목으로는 전송횟수와 연산량, MN의 패킷 전달률 그리고 라우팅 오버헤드를 측정하였다.

2-1. 전송횟수와 연산량

OTP-EKE 인증기법의 전송횟수와 연산량을 측정하기 위해 지수승 계산을 하는 DH-EKE를 이용한 인증기법이 비교대상으로 사용되었다.

표 9. 전송횟수와 연산량

Table 9. Transmission Count and Operation Quantity

인증기법	전송 횟수	암호화 횟수	지수승 횟수		난수생성 횟수	
			SN	*DN*	*SN*	*DN*
DH-EKE	4	4	3	3	1	1
OTP-EKE	3	3	2	2	1	1

표 9와 같이 DH-EKE를 이용한 인증기법과 OTP-EKE 인증기법의 메시지 전송횟수, 암호화 횟수, SN과 DN의 지수승 횟수 그리고 난수생성 횟수를 측정한 결과, 메시지 전송횟수와 메시지 암호화 횟수는 DH-EKE를 이용한 인증기법이 4회, OTP-EKE 인증기법이 3회 그리고 지수승 횟수는 2회로 각 1회씩 줄여 SN과 DN사이의 키 교환 시간을 줄일 수 있었고, 난수생성 횟수는 DH-EKE와 동일하게 각 1회씩 발생하여 DH-EKE를 이용한 인증기법보다 효율성이 향상 되었다고 할 수 있다.

2-2. 패킷 전달률

OTP-EKE 인증기법의 패킷 전달률을 측정하기 위해 AODV 라우팅을 수행하는 OTP S/Key 인증기법과 해시된 AODV 라우팅을 수행하는 OTP S/Key 인증기법, DH-EKE를 이용한 인증기법을 비교대상으로 하였다. 각 비교대상 인증기법들은 CBR 세션을 처음 시작한 SN이 1초당 512byte 4개의 패킷을 생성하여 DN까지 전송된 데이터 패킷을 계산량, 지연시간 그리고 random waypoint를 사용한 MN의 움직임 (0 ~ 20m/sec)에 따라 측정한 것이다.

$$packet\ delivery\ fraction = \frac{receive_packet}{send_packet} \times 100 \quad \text{———} \quad (5.10)$$

그림 37은 식 (5.10)을 이용하여 트래픽 생성 스크립트(cbrgent.tcl)를 통해 생성된 결과 값이며 정지시간 0초부터 900초 동안의 시뮬레이션 시간에 따른 패킷 전달률을 보이고 있다. 정지시간이 0인 경우 MN은 DN을 향해 이동하게 되고, 정지시간이 시뮬레이션 시간과 동일하면 MN이 시뮬레이션 시간동안 이동하지 않았음을 의미한다.

그림 37에서 해시된 AODV 라우팅을 수행하는 OTP S/Key 인증기법을 H(OTP S/Key), DH-EKE를 이용한 인증기법을 H(DH-EKE) 그리고 OTP-EKE 인증기법을 H(OTP-EKE)라 표현하며, AODV 라우팅 프로토콜에 추가적인 메시지 전송과정 없이 OTP를 삽입한 *H(RREQ)*와 *H(RREP)* 메시지만을 전송한다.

AODV 라우팅을 수행하는 OTP S/Key 인증기법은 0초부터 900초 동안 94%이상의 패킷 전달률을 보이고 있으며, 해시된 AODV 라우팅을 수행하는 각 인증기법 또한 유사한 패킷 전달률을 보이고 있다. 하지만 H(OTP-EKE)의 경우 시뮬레이션 시작시간인 0초에서는 93.0%로 다른 인증기법에 비해 경로를 탐색하기 위한 패킷 전달률은 떨어진다. 하지만 400초 이후에는 패킷 전달률이 점차 증가되는 것을 볼 수 있다.

시뮬레이션 종료시점인 900초에서는 H(OTP-EKE)가 99.8%로 OTP S/Key 인증기법과 0.1%정도의 오차를 보여 데이터 패킷을 송·수신하기 위한 경로를 탐색하고 설정하는 것이 매우 효율적이고 정확하다는 것을 설명해 준다. 하지만 그림 37은 악의적인 노드를 고려하지 않고 측정한 결과이므로 정확한 패킷 전달률이라 할 수 없다.

그림 38은 MANET에 참여한 50개의 노드중 임의의 5개의 노드를 악의적인 노드로

선별하고, 소수 p값을 부여하지 않고 원시근 g값만을 2로 설정하여 패스워드 추측 공격과 사전 공격의 가능성을 부여하여, 900초 동안의 패킷 전달률을 측정한 값이며 OTP S/Key, H(DH-EKE) 그리고 H(OTP-EKE)를 비교대상으로 하였다.

0초부터 900초 동안 전체 데이터 패킷에 대해 악의적인 노드를 거쳐 간 패킷 전달률로 측정값이 작을수록 악의적인 노드의 공격에 안전하고 효율적으로 라우팅을 수행한다는 것을 알 수 있다. OTP S/Key 인증기법은 평균 39.3%의 패킷이 악의적인 노드를 통과하는데 반해, H(DH-EKE)는 평균 23.2% 그리고 H(OTP-EKE)는 평균 20%만이 악의적인 노드를 통과하였다. OTP S/Key 인증기법의 경우 라우팅 과정중 악의적인 노드가 홉 카운터 필드를 0으로 변조하여 공격을 수행한 결과이며, OTP-EKE 인증기법의 소수 p값과 원시근 g값을 알지 못한 상태에서 수행한다면, 패킷 전달률은 비교대상 인증기법보다 안전성과 효율성이 향상 된다고 할 수 있다.

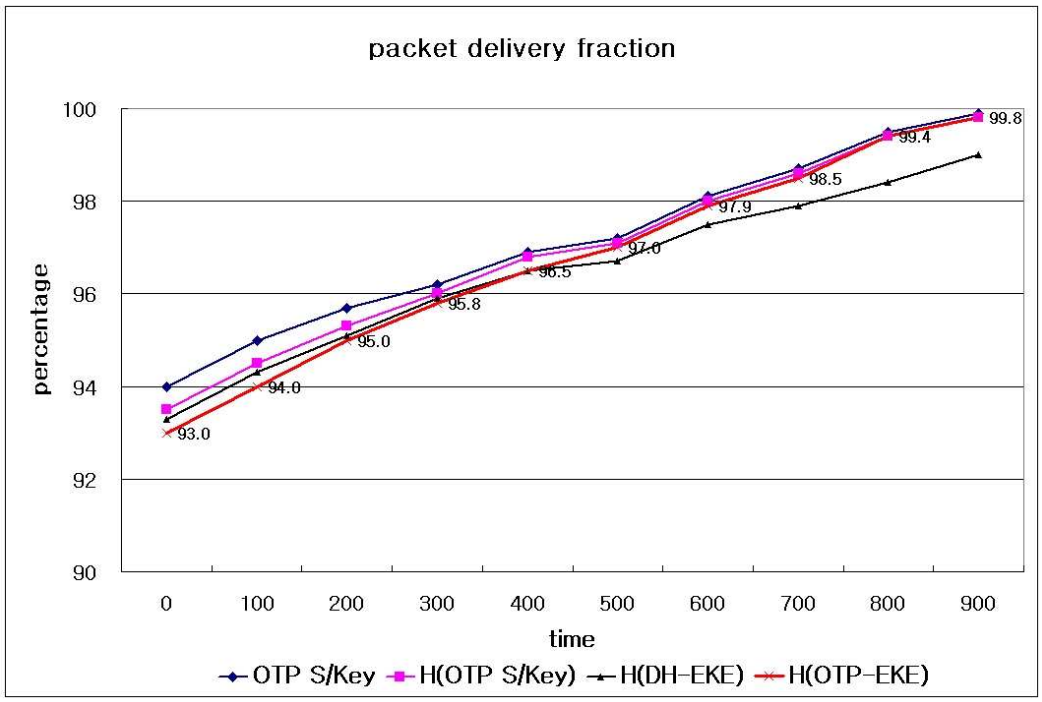


그림 37. 시간에 따른 패킷 전달률

Fig. 37. Packet Delivery Fraction of Time

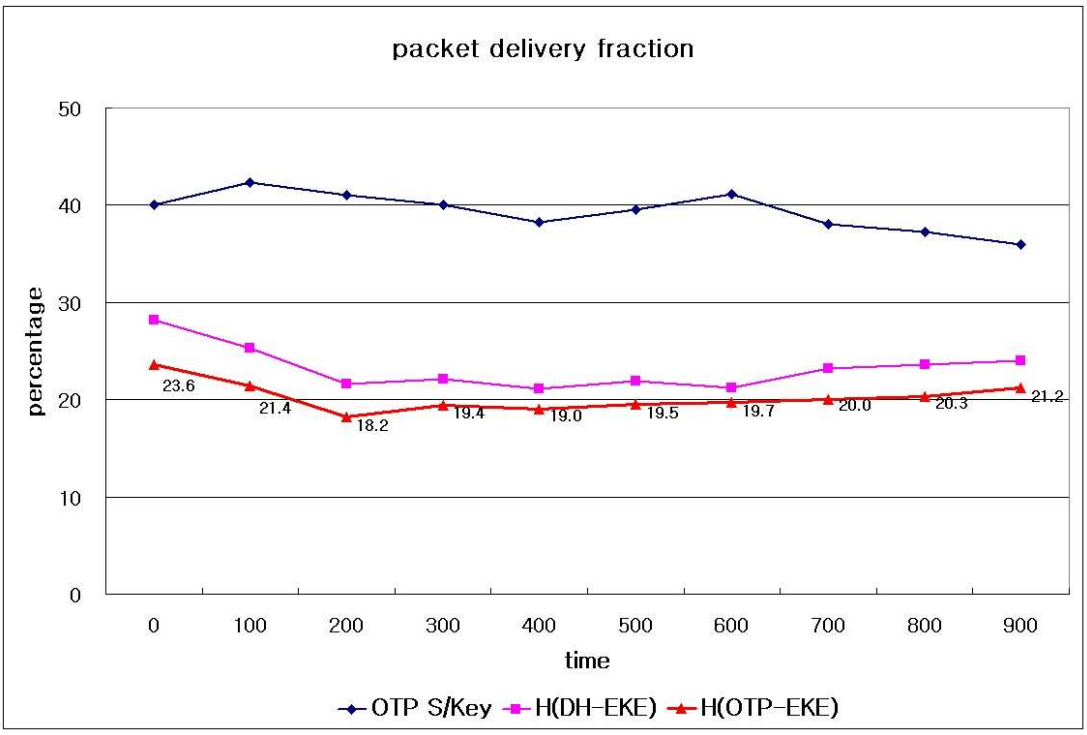


그림 38. 악의적인 노드가 있는 경우의 패킷 전달률

Fig. 38. Packet Delivery Fraction with Malicious Node

2-3. 라우팅 오버헤드

라우팅 오버헤드는 하나의 데이터 패킷이 SN에서 DN까지 전송되는 CBR 세션동안 소요되는 제어 패킷수를 말한다. SN에서 DN까지 데이터를 전송하고자 할 때 사용되는 메시지는 에이전트 레벨, 라우팅 레벨, MAC 레벨에서 발생하며 에이전트 레벨의 메시지는 전송하고자 하는 CBR 데이터, 라우팅 레벨의 메시지는 CBR 데이터를 전송하기 위한 RTR_level 메시지, MAC 레벨의 메시지는 ARP와 같은 주소결정 프로토콜 메시지이며 식 (5.11)을 통해 네트워크에 참여한 50개의 노드 중 30개의 노드를 연결하여 라우팅 오버헤드를 측정하였다.

$$routing\ overhead = \frac{MAC_level_messages + RTR_level_messages}{receive_messages} \quad \text{———} \quad (5.11)$$

그림 39에서는 0초부터 900초 동안의 MN의 라우팅 오버헤드를 보이고 있다. 라우팅 오버헤드는 SN에서 DN까지 전달된 패킷 데이터에 대하여 경로탐색과 설정을 위해 사용된 라우팅 메시지의 패킷수를 나타낸다.

AODV 라우팅을 수행하는 OTP S/Key 인증기법은 경로탐색을 위해 1.71개의 라우팅 패킷을 가지고 있고, H(OTP-EKE)의 경우 H(DH-EKE)보다 암호화 횟수가 적어 2.32개의 라우팅 패킷을 가지고 있지만, H(OTP-EKE)는 *H(RREQ)* 패킷에 OTP를 포함하므로 OTP S/Key 인증기법에 비해 더 큰 라우팅 패킷이 전송되고 있다. 하지만 H(OTP-EKE)의 경우 500초 후에 AODV 라우팅과 유사한 오버헤드를 보이고 있어 효율적이라 할 수 있지만, 이는 악의적인 노드를 고려치 않은 측정결과이다.

그림 40과 같이 MANET에 참여하는 50개의 노드 중 30개의 노드를 연결하고 그 중 5개의 노드를 악의적인 노드로 선별하여 소수 p값을 부여하지 않고 원시근 g값만을 2로 설정하여 시간에 따른 오버헤드를 측정한 결과이다. 시뮬레이션 시간 0초부터 900초 동안 AODV 라우팅을 수행하는 OTP S/Key 인증기법은 50개의 노드를 기준으로 데이터 패킷이 6.4라우팅 패킷을 지니고 있다. OTP S/Key 인증기법의 경우 AODV의 경로 발견의 수는 대부분 방대한 플로딩을 가지고 있기 때문에 연결이 증가할 때 마다 더 많은 라우팅이 필요하게 된다.

H(OTP-EKE)의 경우 악의적인 노드의 개입이 없을 때에는 2.32개의 라우팅 패킷을 가지고 있지만, *g*값을 2로 설정했을 경우 악의적인 노드를 배제한 경로탐색을 실행하므로 2.83개의 라우팅 오버헤드를 보이고 있다. H(DH-EKE)의 경우 H(OTP-EKE)보다 악의적인 노드의 공격 가능성이 높아 3.62개의 패킷을 전달한다. 결과적으로 악의적인 노드의 개입이 없을 경우 0초부터 900초 동안 평균 1.00개의 패킷 오버헤드를 보이며, 30개의 노드 중 5개의 악의적인 노드를 고려했을 경우 1.47개의 패킷으로, 악의적인 노드의 개입이 없는 AODV와 평균 0.83개로 유사한 오버헤드를 보여 결과적으로 보안성이 결여된 AODV보다 안전성과 효율성이 향상 되었다고 할 수 있다.

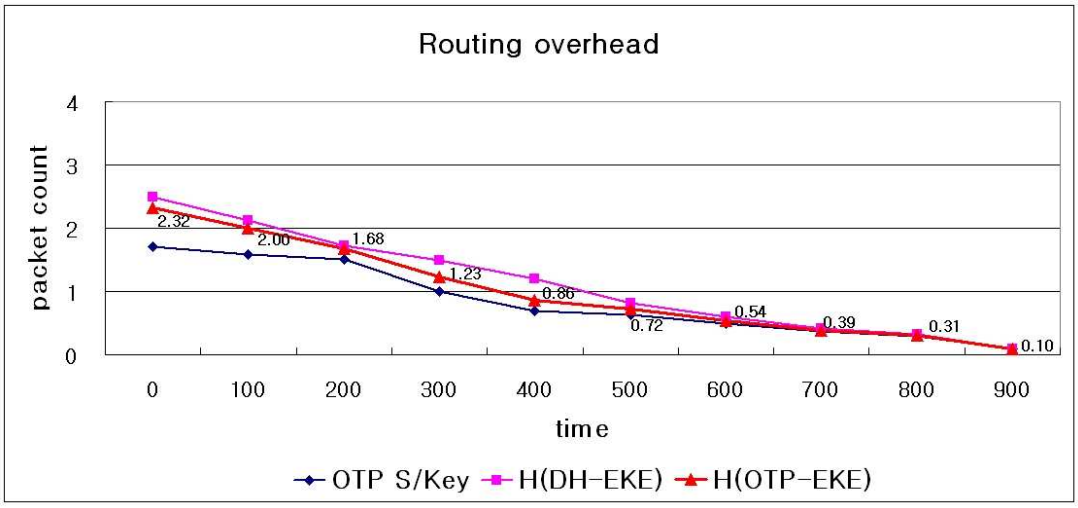


그림 39. 시간에 따른 라우팅 오버헤드

Fig. 39. Routing Overhead of Time

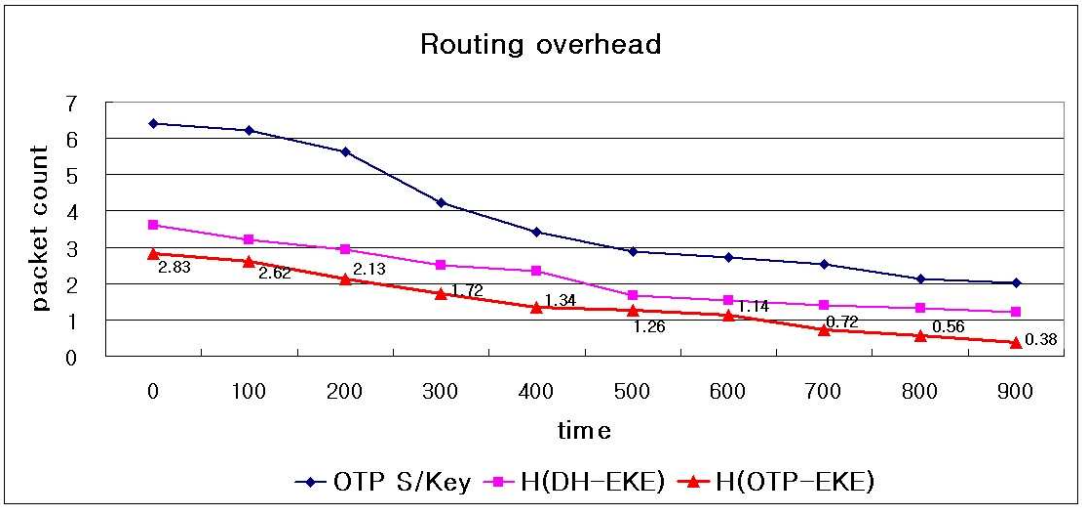


그림 40. 악의적인 노드가 있는 경우 라우팅 오버헤드

Fig. 40. Routing Overhead with Malicious Node

Ⅴ. 결　론

MANET은 기존의 네트워크와 같이 인프라가 구축되지 않는 환경에서 MN들 상호간에 라우팅 수행으로 데이터를 송·수신 할 수 있는 형태의 네트워크를 말한다. 네트워크에 참여하는 각 MN들은 기지국이나 AP의 도움 없이 라우터와 호스트를 동시에 수행하면서 다른 MN을 대신하여 패킷을 전송할 수도 있고, MN 어플리케이션들을 실행할 수도 있어야 한다. 또한 전쟁터나 재난 시와 같이 기반시설을 사용할 수 없는 일시적인 네트워크를 구성해야 하는 경우 MANET은 좋은 대안이 될 수 있다. 하지만 MN의 이동성으로 인한 동적 네트워크 토폴로지로 유선상의 네트워크보다 링크의 불안전성, MN의 물리적 보호의 한계, MN의 연결의 산재성 등 많은 보안상 취약점이 존재한다. MANET은 라우팅 보안과 인증기법의 미비로 악의적인 노드로부터 수동적·능동적 공격에 취약성을 지니고 있어 지속적인 보안 서비스를 관리할 수 없다

본 논문에서는 MANET 인증기법의 라우팅 보안 및 키 교환 프로토콜의 보안 요구사항을 분석하고 이를 만족하는 MANET 환경의 MN간 신뢰성 있는 인증을 제공할 수 있었다. 제안 인증기법은 라우팅 단계와 인증키 교환단계에서 MD5를 적용한 OTP 사용으로 구조가 간단하고, DLP 연산을 통한 안전성을 제공하였고, MANET 환경의 OTP S/Key 인증기법에 패스워드 기반 키 교환 프로토콜인 DH-EKE를 개선하여 안전성과 효율성이 강조 되었다. 또한 해시된 AODV 라우팅 수행으로 라우팅 보안과 키 교환 보안을 확보할 수 있어 기밀성, 무결성, 가용성, 인증, 부인방지 서비스를 제공할 수 있었다. SN과 DN사이 패스워드 검증자를 이용한 암호화, 복호화 수행으로 기밀성을 제공하고, MD5를 이용한 해시된 라우팅으로 무결성을 제공하였다. 암호화를 위한 키 교환 수행능력이 높을수록 가용성은 떨어지고, 암호화가 낮을수록 가용성은 높아지는 상반된 관계를 보이지만, 가용성을 높이게 되면 악의적인 노드의 공격가능성도 높아진다고 할 수 있다. 그리고 부인방지 서비스로는 SN과 DN사이의 해시된 검증자를 이용하여 MN간 서명, 검증을 수행함으로 부인방지 기능을 제공하였다.

OTP-EKE 인증기법의 실험을 위해 NS2를 사용하였으며 안전성과 효율성을 분석하였다. 안전성 분석은 라우팅 안전성과 인증을 위한 키 교환 안전성으로 구분하여 분석하였으며 메시지 위·변조, 악의적인 노드의 위장에 대한 라우팅 안전성과 재전송 공격, 중재자 공격, Denning-sacco 공격, 오프라인 추측 공격 그리고 Stolen-verifier 공

격에 대한 키 교환 안전성을 확보하였다.

효율성 분석을 위해 메시지 전송횟수와 연산량, 패킷 전달률, 그리고 라우팅 오버헤드를 측정하였다. 메시지 전송횟수와 암호화 횟수, 지수승 횟수를 DH-EKE를 이용한 인증기법보다 각 1회씩 줄여 효율성을 제공하였고, 패킷 전달률은 시뮬레이션 시간동안 AODV 라우팅과 유사한 패킷 전달률을 보였으며, 5개의 악의적인 노드를 고려한 패킷 전달률에서는 평균 20%만이 악의적인 노드를 통과하여 안전성과 효율성을 제공하였다. 그리고 라우팅 오버헤드 측정결과 평균 1.47개의 패킷으로 보안성이 결여된 AODV보다 안전성과 효율성이 향상되었다. 따라서 OTP-EKE 인증기법은 완전한 MANET 환경에 강력한 신뢰성을 제공하는 인증기법이라 할 수 있다.

향후 MANET의 성장성을 감안한다면 MANET의 보안 인식은 크게 증가될 것이며 MN의 인증기법은 가장 필요할 것이다. 제안 인증기법은 무선 환경을 구성하는 다양한 컨버전스 디바이스간 인증기법으로 사용될 수 있으며 MN의 연산량을 고려하였다. 무선 환경과 MANET의 시장성을 고려한다면 더욱더 보안성이 강조된 라우팅 프로토콜과 인증기법의 개발이 시급하고, MN의 연산량을 감소시키면서 강력한 보안성을 제공할 수 있는 추가적인 MANET 인증기법이 필요할 것이다. 제안 인증기법의 향후 연구과제로는 시뮬레이션 환경이 아닌 실제 적용 가능한 클라이언트 어플리케이션의 개발로 유비쿼터스 환경에 바로 적용할 수 있는 상용화 연구가 필요할 것이다.

[참 고 문 헌]

[1] IETF, Mobile Ad-Hoc Networks (manet) Charter, IETF MANET Working Group, 2007.
http://www.ietf.org/html.charters/manet-charter.html/

[2] The Bluetooth Special Interest Group, 2007.
http://www.bluetooth.org/apps/content/

[3] The HomeRF Resource Center,
http://www.palowireless.com/homerf/homerf2.asp/

[4] 이철승, 이준, "MANET 기반 원타임 패스워드 키 교환 인증기법", 한국 해양 정보통신학회 논문지, Vol. 11, No. 7, 7, 2007.

[5] B. Kadri, A. M''hamed, M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, Vol. 7, No. 3, March, 2007.

[6] J. Chang, J. Jang, "BECT : A Balanced Energy Consumption Algorithm by Threshold-Tuning for Mobile Ad Hoc Networks", 13th Joint Conference on Communication and Information 2003 (JCCI2003), April, 2003.

[7] Lakshmi Venkatraman, Dharma P. Agrawal, "A Novel Authentication Scheme for Ad Hoc Networks," IEEE Wireless Communications and Networking Conference 2000, Vol. 3, pp. 1268-1273, 2000.

[8] Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil Jajodia, "LHAP : A Lightweight Hop-by-Hop Authentication Protocol For Ad-Hoc Networks", International Workshop on Mobile and Wireless Network(MWN 2003), May, 2003.

[9] Seung Yi, Robin Kravets, "Practical PKI for Ad Hoc Wireless Networks", No. UIUCDCS-R-2002-2273, Technical Report, August, 2001.

[10] L. Lamport, "Construction digital signatures from one-way function", SRI-CLS-98, SRI International, Technical Report, October, 1979.

[11] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Special Issue on Network Security, Vol. 13, No. 6, pp. 24-30, 1999.

[12] Ram Ramanathan, Jason Redi, "A Brief Overview of Ad Hoc Networks :

Challenges and Directions", IEEE Communication Magazine, Vol. 40, pp. 20-22, May, 2002.

[13] J. H Jeong, J. S Park, "Autoconfiguration Technology for IPv6 Ad-hoc Mobile Wireless Network", IPv6 forum Korea, Technical Report 20.

[14] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Jorjeta Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98), pp. 25-30, October, 1998.

[15] T. Camp, J. Boleng, V. Davies, "A survey of mobility models for Ad Hoc network research", Wireless Communications F4 Mobile Computing (WCMC) : Special issue on Mobile Ad Hoc Networking : Research, Trends and Applications", Vol. 2, No. 5, pp. 483-502, 2002.

[16] Albert Young, "Enabling IPv6 in Mobile Ad-Hoc Wireless Networks", IPv6 Summit, Boeing, June, 2004.

[17] Charles E. Perkins, Jari T. Malinen, Ryuji Wakikawa, "IP Address Autoconfiguration for Ad Hoc Networks", IETF Internet Draft : draft-ietf-manet-autoconf-01.txt, 14, November, 2001.
http://www.cs.ucsb.edu/~ebelding/txt/autoconf.txt/

[18] Hinden, R. Hindon, S. Deering, "Internet Protocol Version 6(IPv6) Addressing Architecture", RFC 3513, April, 2003.
http://www.ietf.org/rfc/rfc3513.txt/

[19] Charles E. Perkins, et al., "Ad hoc on demand distance vector routing", IETF Internet Draft : draft-ietf-manet-aodv-13.txt, February, 2003.
http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt/

[20] Thomas Clausen, Philippe Jacquet, "Optimized Link State Routing Protocol", IETF Internet Draft : draft-ietf-manet-olsr-11.txt, July, 2003.
http://hipercom.inria.fr/olsr/draft-ietf-manet-olsr-11.txt/

[21] R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February, 2004.
http://www.ietf.org/rfc/rfc3684.txt/

[22] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing

Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April, 1999.

[23] J. Chang, L. Tassiulas, "Energy Conserving Routing in wireless Ad-hocNetworks", IEEE INFOCOM 2000, pp. 22-31, 2000.

[24] Vincent D. Park, M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", April, 2004.

[25] X. Jia, J. Wu, Y. He, "Mobile Ad-hoc and Sensor Networks", First International Conference MSN 2005 Proceedings, Lecture Notes in Computer Science, Vol. 3794, pp. 164-174. Springer, 2005.

[26] R. Zheng, R. Kravets, "On-demand power management for Ad Hoc networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies 2003 (INFOCOM 2003), Vol. 1, pp. 481-491, March, 2003.

[27] Zygmunt. J. Hass, Marc. r. Pearlman, "The Zone Routing Protocol(ZRP) for Ad-Hoc Network", IETF Internet Draft : draft-ietf--manet-zone-zrp-04.txt, July, 2002.
http://tools.ietf.org/id/draft-ietf-manet-zone-zrp-04.txt/

[28] David B. Johnson, David A. Maltz, Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR)", IETF Internet Draft : draft-ietf-manet-dsr-10.txt, July, 2004.
http://tools.ietf.org/id/draft-ietf-manet-dsr-10.txt/

[29] RFC Index (3601..3700),
http://www.armware.dk/RFC/rfc/index3601.html#3684/

[30] M. S. Corson, J. P. Macker, "Mobile Ad hoc Networking(MANET) : Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January, 1999.
http://www.faqs.org/rfcs/rfc2501.html/

[31] S. H. Seo, H. Lee, J. Lee, J. Ji, J. Song, "CPAA : Certificate based Predictable Address Auto-configuration Mechanism in Mobile Ad-hoc Networks", GESTS International Transactions on Computer Science and Engineering, Vol. 12, No. 1, June, 2005.

[32] Manel Guerrero Zapata, Manel Guerrero, "Secure Ad Hoc On-Demand

Distance Vector (SAODV) Routing", IETF Internet Draft : draft-guerrero-manet-saodv-05.txt, February, 2005.
http://personals.ac.upc.edu/guerrero/papers/draft-guerrero-manet-saodv-05.txt/

[33] C-K Toh, "*Ad Hoc Mobile Wireless Networks Protocols and System*", Prentice Hall, Jan, 2004.

[34] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis, M. Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks", Third IEEE International Conference on Pervasive Computing and Communications, March, 2005.

[35] S. Yi, R. Kravets, "MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks", Proceedings of 2nd Annual PKI Research Workshop Program (PKI 03), 2003.

[36] A. Khalili, J. Katz, W. A. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks", Proceedings of 2003 Symposium on Applications and the Internet Workshops(SAINT 2003 Workshops), 2003.

[37] J. Hubaux, L. Buttyan, S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks", Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), October, 2001.

[38] S. Capkun, L. Buttyan, J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 2, No. 1, pp. 52-64, 2003.

[39] 이철승, 이준, "Ad Hoc 네트워크 기반의 가변 지오캐스팅", 한국 해양 정보통신 학회 논문지, Vol. 10, No. 8, 8, 2006.

[40] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function", CRYPTO'87 Proceedings, Lecture Note in Computer Science, Vol. 293, pp. 369-378, Springer. 1987.

[41] N. Haller, C. Metz, P. Nesser, M. Straw, "A One-Time Password System", RFC 2289, February, 1998.

[42] "The MD5 Message-Digest Algorithm",
ftp://ds.internic.net/rfc/rfc1321.txt/

[43] Kemal BICAKCI, Nazife BAYKAL, "Improving the Security and Flexibility of One-Time Passwords by Signature Chains", Turk J Elec Engine, Vol. 11, No.

3, 2003.

[44] N. Haller, C. Metz, “A One-Time Password System", RFC 1938, May, 1996. http://www.ietf.org/rfc/rfc1938.txt/

[45] N. Haller, “The S/KEY one-time password system", RFC 1760, 1995. ftp://ds.internic.net/rfc/rfc1760.txt/

[46] E. Bresson, O. Chevassut, D. Pointcheval, “Security Proofs for an Ecient Password-Based Key Exchange", Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 241-250, October, 2003.

[47] Steven M. Bellovin, Michael Merrit, “Encrypted key exchange : Password-based protocols secure against dictionary attack", In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 72-84, May, 1992.

[48] Bellare, Jablon, Krawczyk, MacKenzie, Rogaway, Swaminathan, “Proposal for P1363 Study Group on Password-Based Authenticated-Key-Exchange Methods”, February, 2000.

[49] W. Diffie, M. Hellman, “New directions in cryptography", IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976.

[50] Mihir Bellare, Phillip Rogaway, “The AuthA Protocol for Password-Based Authenticated Key Exchange”, Contribution to IEEE P 1363 and its study group looking at new projects, March, 2000.

[51] V. Boyko, P. MacKenzie, S. Patel, “Provably secure password authenticated key exchange using Diffie_Hellman", Advances in Cryptology-Eurocrypt 2000, pp. 14-18, May, 2000.

[52] T. Wu, “The Secure Remote Password Protocol", Internet Society Symposium on Network and Distributed System Security, 1998.

[53] E. Bresson, O. Chevassut, D. Pointcheval, “Security Proofs for an Ecient Password-Based Key Exchange" Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 241-250, October, 2003.

[54] G. Montenegro, C. Castelluccia, “Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address", NDSS′ 02, February, 2002.

[55] 배성수, 한종수, “*네트워크 시뮬레이터*”, 세화, January, 2006.

감사의 글

어느덧 4년간의 박사과정 생활을 마쳐야 할듯합니다. 지난 시간동안은 제 인생에 많은 전환점 이었습니다. 앞만 보고 달려와 놓친 것, 잃은 것도 많았지만, 저에게는 그 이상의 큰 발전과 발돋움에 기간이었으며 이렇게 발전하게 도와주신 주위에 많은 분들께 글로써 감사의 마음을 전합니다.

먼저 항상 부족한 저를 학문에 정진할 수 있도록 격려해 주신 이준 지도교수님께 진심으로 감사드립니다. 그리고 논문이 완성될 때까지 세심한 지도를 해주신 나상동 교수님, 항상 바쁜 일과 중에도 많은 힘이 되어주신 조범준 교수님, 따뜻한 격려와 체계적인 지도를 해주신 김충원 교수님, 논문의 깊이를 일러주신 김판구 교수님과 컴퓨터 공학과의 여러 교수님들의 배려와 가르침에 감사드립니다.

불철주야 학문에 전념하며 힘들고 지칠 때마다 힘이 되어준 시스템 소프트웨어 연구실에 홍성표 박사님, 항상 자상하게 인도해준 신명숙 선생님, 작은 일도 함께한 김국세 선생님, 웃음으로 함께한 안성수 교수님, 이정기 박사님, 선광에게 고마움을 전하며, 그동안 많은 어려움을 극복하도록 도와주신 송기범 박사님, 정성옥 교수님께 감사드립니다. 그리고 석·박사 과정동안 많은 시간을 함께했던 컴퓨터 공학과의 여러 연구실 선·후배님께 고마움을 전합니다.

오늘이 있기까지 33년 동안 못난 아들을 위해 오직 희생과 사랑으로 감싸주신 아버님, 어머님, 언제나 든든한 조언을 해준 누나 그리고 공부하는 큰 사위를 격려해 주신 장인어른, 장모님, 묵묵히 지켜봐준 동서와 처제 그리고 처남에게 진심으로 감사드립니다.

감사의 글을 쓰고 있는 오늘은 제 아내의 생일이기도 합니다. 항상 저에게 힘과 용기로 위로해준 사랑하는 아내 정숙희씨에게 이 논문을 생일선물로 전하고, 잘 놀아주지도 못한 아빠에게 언제나 해맑은 웃음을 안겨준 사랑하는 딸 채윤이에게 진심으로 고마움을 전하며, 사랑하는 제 가족에게 이 논문을 바칩니다.

저작물 이용 허락서

학 과	컴퓨터공학과	학 번	20047376	과 정	석사, (박사)
성 명	한글 : 이 철 승 한문 : 李 哲 丞 영문 : Cheol-seung Lee				
주 소	전라남도 담양군 담양읍 천변리 144번지				
연락처	E-MAIL : cyberec@chosun.ac.kr				
논문제목	한글 : MANET 환경에서 강인한 OTP-EKE 인증기법				
	영문 : A Robust OTP-EKE Authentication Scheme in MANET Environments				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(◯) 반대( )

2007년 12월 일

저작자 : 이 철 승 (서명 또는 인)

조선대학교 총장 귀하