논문 2006-43TC-4-2

MANET 환경에서 Zone Routing Protocol을 이용한 안전한 경로설정 보안 알고리즘 S-ZRP

(Secure routing security algorithm S-ZRP used Zone Routing Protocol in MANET)

서 대 열*, 김 진 철**, 김 경 목**,오 영 환***

(Daeyoul Seo, Jinchul Kim, Kyoung-Mok Kim, and Young-Hwan Oh)

요 약

MANET(Mobile Ad-Hoc Network)은 고정된 기반이 없이 노드간의 자율적이고 독립적인 네트워크를 구성한다. 이러한 네트워크에서 경로설정은 이동성이 많은 단말들이 임시로 망을 구성하기 때문에 망 자체가 유기적으로 자주 변하며, 이로 인해 잦은 연결실패로 인한 불안전한 환경이 조성되어 경로설정을 유지하는데 많은 어려움이 있다. 이를 효과적으로 하기 위하여 ZRP(Zone Routing Protocol) 경로설정 프로토콜이 제안 되었다. 그러나 ZRP는 보안에 관한 요소를 포함하고 있지 않기 때문에, 경로설정을 할 때 DoS(Denial of Service)공격에 취약하며, 또한 키 분배에 관한 메커니즘을 가지고 있지 않기 때문에 경로가 설정되었다고 해도 실제 데이터 전송 시 제 3자에 의하여 공격당하기 쉽다. 이를 보안하기 위해서 ZRP가 경로를 설정할 때 안전하게 경로를 설정할 수 있는 S-ZRP(Secure Zone Routing Protocol) 알고리즘을 제안하였다. 제안한 알고리즘은 경로설정 패킷에 대한 무결성 보장 및 근원지 인증 메커니즘을 통해서 보다 안전하게 전송할 수 있다.

Abstract

An mobile ad hoc network(MANET) is a collection of wireless computers (nodes), communicating among themselves over multi-hop paths, without the help of any infrastructure such as base stations or access points. Prior research in MANET has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. In this paper, we design and evaluate the Secure Zone Routing Protocol(S-ZRP), a secure ad hoc network routing protocol is based on the design of the hash chain. In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and don't use asymmetric cryptographic operations in the protocol. Proposed algorithm can safely send to data through authentication mechanism and integrity about routing establishment.

Keywords : MANET, Hash, ZRP

I. 서 론

지난 수년 동안 통신과 네트워크 분야에 엄청난 발전이 있었으며 무선 환경에서의 이동통신 사용자들 간의 통신서비스는 점점 인기를 얻고 있다. 무선 데이터 통신의 발전은 새로운 분야의 발전 가능성을 제시하고 있으며 그 중 대표적으로 주목받고 있는 분야가 mobile Ah hoc 네트워크(MANET)이다.

MANET은 다음과 같은 몇 가지 특성을 가진다, 첫째, 노드의 이동에 따라 네트워크의 토폴로지가 동적으로 변환한다. 둘째, 이동 노드들은 무선 인터페이스를 사용하여 서로 통신한다. 셋째, 이동 노드들은 제한된 용량의 배터리를 사용하기 때문에 에너지 사용에 대한 제약이 크다[1,2,3].

MANET상의 이동 노드들은 무선 인터페이스를 통

* 학생회원, ** 정회원, *** 종신회원,
광운대학교 전자통신공학과
(Dept. of Electronics and Communications Engineering, Kwangwoon University)
접수일자: 2005년12월30일, 수정완료일: 2006년4월12일

하여, 모든 노드들이 경로설정 기능을 가지고 통신하고 있기 때문에 보안상으로 매우 취약한 단점을 가지고 있다. 특히, 브로드캐스팅 되는 경로설정 제어 메시지는 해킹의 위험이 크다.

이러한 보안적인 문제점을 보완하고자 MANET상에서 이동 노드 간 경로 설정 시 안전한 경로설정을 위한 다양한 경로설정 보안 알고리즘들이 제안되고 있다. 그러나 많은 기존의 경로설정 보안 알고리즘들은 대칭키나 비대칭키 방식을 유선 상에서 동일하게 적용하기 때문에 경로설정 패킷을 전송할 때, 전력이 많이 소비되며 속도가 느려지는 문제점이 있다. 이러한 문제를 해결하기 위해서 본 논문에서는 경로설정 보안 알고리즘에 일방향 해쉬 체인 요소를 사용한다[4,5].

본 논문에서는 ZRP(Zone Routing Protocol)에서 경로 설정 시 안전하게 경로설정을 할 수 있는 경로설정 보안 알고리즘 S-ZRP(Secure Zone Routing Protocol)을 제안하였다. 이 알고리즘은 대칭키나 비대칭키 방식을 사용하지 않고 해쉬함수를 사용해서 전력소비를 줄이고 경로설정 속도를 빠르게 하였다[6,7,8,9,10].

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 ZRP의 구조 및 경로탐색 과정에 관하여 알아보고, Ⅲ장에서는 ZRP(Zone Routing Protocol)경로설정 프로토콜에 일방향 해쉬 함수를 적용한 안전한 경로설정 보안 알고리즘 S-ZRP를 제안하였으며 Ⅳ장에서는 본 논문에서 제안하고 있는 방안의 성능을 평가한 후에 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. Zone Routing Protocol

ZRP(Zone Routing Protocol)은 MANET에서의 테이블 기반 방식(Table Driven)의 프로토콜과 요구 기반방식(On-Demand Driven)의 프로토콜이 혼합된 방식으로 각 프로토콜의 장점만을 적용하여 만들어진 방식이다. 테이블 기반 방식은 어떤 목적지에 대한 경로가 요구될 때 바로 그 목적지에 대한 경로가 제공 될 수 있다는 장점을 가지고 있다. 하지만 망 자체가 계속적으로 변하는 MANET 망의 특성상 테이블 기반 방식을 사용할 경우 필요로 하지도 않는 노드에 대한 경로 유지를 위해 상당양의 제어 패킷의 교환이 일어나게 되며 무선 자원의 심각한 낭비를 초래하게 된다. 요구 기반 방식은 경로설정을 하기 위해서는 경로설정 요구, 경로설정 응답 등의 패킷 등을 망 전체에 전파시켜 경로를 찾으며 이에 따른 지연이 경우에 따라 커질 수 있다.

1. ZRP의 구조

ZRP에서 각 노드는 zone이라는 범위를 가진다. 노드별 zone의 범위는 임의의 홉 수에 따라 정의된다. zone의 노드들은 내부노드, 외부노드와 경계노드로 나뉘게 된다. 내부노드는 정해진 홉 수 보다 작은 홉 수를 가지는 노드를 말하고, 외부노드는 정해진 홉 수 보다 큰 홉 수를 가지는 노드를 말하고, 경계노드는 정해진 홉 수와 같은 홉 수를 가지는 노드를 말한다.

그림 1은 2홉으로 구성된 임의의 노드 S의 zone을 나타내고 있다. 노드 S의 zone은 노드 F를 제외한 노드들이 속하게 된다. 그림에서 보는 바와 같이 둥근 원은 노드 S의 zone의 영역이 된다.

그림 2는 ZRP의 구조를 나타낸다. 각 프로토콜 중에서 IARP(Intra-Zone Routing Protocol)는 테이블 기반 방식이 적용되었고, IERP(Inter-Zone Routing Protocol)은 요구 기반 방식을 따른다. IARP는 임의의 zone에 존재하는 노드들의 경로설정 정보를 유지하는 기능을 가지고, IERP에 의해 유지되는 경로설정 정보를 바탕으로 경로 탐색과 경로 유지를 담당하게 된다. 또한 BRP(BorterCast Resolution Protocol)은 RREQ(Route Request)패킷을 다른 zone에 전이시키고자 할 때 경계노드에게만 RREQ를 보내는 기능을 갖는다.

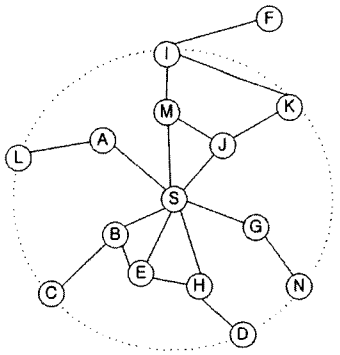


그림 1. 2홉으로 구성된 노드 S의 zone
Fig. 1. Node S's zone consisted of 2 unit of measure.

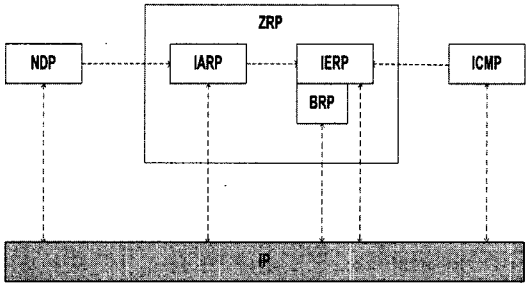


그림 2. Zone Routing Protocol의 구조
Fig. 2. Zone Routing Protocol's structure.

2. ZRP 경로 탐색

경로 탐색 과정을 각 프로토콜별로 살펴보면, 첫 번째 목적노드가 해당 zone 내부에 있는지 외부에 있는 경우인지를 IARP 경로설정 테이블을 통해서 검사를 하게 된다. 내부에 있는 경우에는 RREP(Route Replay)를 소스노드에게 보내고, 외부에 있는 경우에는 IERP를 사용하게 된다. IERP는 경로발견을 위해 기존의 브로드캐스트 기반의 알고리즘을 사용하지 않고 BRP라는 메시지 분산 서비스를 이용하게 된다. BRP는 기존의 이웃 노드에게 무조건 패킷을 브로드캐스트 하지 않고 경로설정 zone의 경계에 위치한 경계노드에게 직접적인 질의(query)를 전달하는 방식이다. 이것을 보더캐스트(bodercast)라고 한다.

Ⅲ. 제안한 S-ZRP 알고리즘

본 논문에서는 ZRP (Zone Routing Protocol)에서 경로 설정 탐색 시 안전하게 경로설정을 할 수 있는 경로설정 보안 알고리즘 S-ZRP(Secure Zone Routing Protocol)을 제안하였다. 이 알고리즘은 대칭키나 비대칭키 방식을 사용하지 않고 해쉬함수를 사용해서 전력소비를 줄이고 경로설정 속도를 빠르게 하였다.

S-ZRP는 크게 두 가지 구조를 가진다. 경로설정 목적지 주소에 따라 zone 내부에서 안전하게 경로설정 업데이트하는 방법과 zone 외부에서 안전하게 경로설정을 맺는 방법이다.

제안하는 알고리즘은 다음과 같은 가정을 한다.

1. 각각의 노드들은 서로 비밀키를 공유하고 있다. 이 비밀키는 네트워크를 구성하기 이전에 미리 각 노드에 저장해 둔다.
2. 키 획득 공격에 노드는 안전하다.
3. 경로설정 메시지가 발생하면 경로설정 메시지의 목적지를 보고 IARP가 관리하는 경로설정 테이블을 통해서 경로설정 메시지가 zone 내부인지 zone 외부 인지를 판단하게 된다.

1. 목적노드가 zone 내부에 있는 경우

본 논문에서는 zone안에서 안전한 경로 설정 업데이트 메시지를 주고받기 위해서 테이블 기반 방식에서 사용되고 있는 경로설정 보안 알고리즘인 SEAD (Secure Efficient Distance Vector Routing)[11,12,13]을 적용하였다.

S-ZRP 알고리즘에서 zone 내에서 안전하게 경로설정 업데이트 메시지를 주고받는 방법은 다음과 같다. 일방향 해쉬 체인 요소를 사용하여서 경로설정 테이블 업데이트 메시지의 sequence number와 목적지 주소와 metric을 인증하는 것이다. 메시지마다 sequence number를 할당함으로써 routing loop를 피할 수 있다. 또한 metric 값에 해쉬 값을 적용함으로써 경로설정 업데이트 메시지의 무결성과 근원지 보장을 할 수 있다. zone 내부에서 경로설정 업데이트 메시지가 발생했을 때 경로설정 업데이트 메시지 인증 알고리즘은 다음과 같다.

※ 표기법

S : 소스노드

D : 목적지 노드

h : 함수 함수

MAC : 메시지 인증 함수

M : HMAC 함수

SN : 경로설정 업데이트 sequnce number

Metric : 증가만하는 경로설정 업데이트 메시지 인증 요소

UpMsg : 경로설정 업데이트 메시지

단계 1. [초기 해쉬 함수 h_0을 발생]

경로설정 메시지가 발생하기 전에 소스에서 해쉬 체인을 만든다.

$$h_0 = MAC_{k_{SD}}(UpMsg, S, D, SN, Metric)$$

$$h_1 = H(h_0), \ldots\ldots\ldots\ldots, h_n = H(h_{n-1})$$

단계 2. [경로설정 업데이트 메시지를 발생]

경로설정 업데이트 메시지는 다음과 같다.

$$< UpMsg, S, D, SN, Metric, h_0 >$$

단계 3. [다음 노드로 경로설정 업데이트 메시지를 보냄]

단계 4. [해쉬 값 인증]

예를 들면, 인증이 된 h_0값이 주어지면 노드들은 $H(H(H(h_{i-3})))$을 계산하고 h_i와 결과 값이 같은지 비교하여 h_{i-3}을 인증한다. 이러한 과정을 통해서 해쉬 값 인증을 수행하고 단계 5를 수행한다.

단계 5. [Metric과 sequence number 비교]

일방향 해쉬 체인으로 얻은 metric, sequence number와 새로운 metric, sequence number와 비교한다.

기존 Metric ≦ 새로운 Metric and

기존 sequence number ≦ 새로운 sequence number

단계 6. [경로설정 업데이트 메시지 인증]

위의 단계에서 성공하면 새로운 경로설정 업데이트 메시지를 인증하고, 위의 단계에서 실패하면 새로운 경로설정 업데이트 메시지를 버린다.

단계 7. [끝냄]

모든 과정을 끝낸다.

그림 3은 위에서 살펴본 과정들을 흐름도로 보여주고 있다. 각각의 노드는 metric을 0으로 하여 각각의 경로설정 업데이트 내 해쉬 체인으로부터 특별한 인증(서명) 요소를 사용한다. 이러한 초기 요소를 기본으로 하여 일방향 해쉬 체인은 노드에 대한 다른 경로설정 업데이트 내 metric상의 lower bound에 대한 인증을 제공한다. 경로설정 업데이트 엔트리 내 sequence number와 metric 값이 일치하는 해쉬 값은 목적지의 현재 sequence number보다 더 큰 sequence number를 가지는 목적지의 주소를 알려주는 메시지를 막는다. 경로에 존재하고 있는 metric은 해쉬 체인의 일방향 특성 때문에 감소되지 않기 때문에 노드는 경로설정 메시지를 받은 것 보다 더 좋은 경로를 알려주지 못한다.

즉, 노드가 경로설정 업데이트를 받았을 때 노드는 받은 업데이트 목록 안에 목적지 주소, sequence number, 그리고 metric 정보의 인증을 확인한다. 그 확인과 함께 최근의 목적지 해쉬 체인으로부터 인증된 해쉬 값을 받은 적 있는지 확인한다. 받은 시간의 정확한 확인을 통해서 받은 정보의 해쉬 값을 계산하고 확실한 해쉬 값을 비교하여 인증하여 받은 경로설정 업데이트의 진위를 확인 한다. 이러한 방법으로 경로설정 패킷에 대한 무결성 및 인증 메커니즘을 통해서 보다 안전하게 전송할 수 있다.

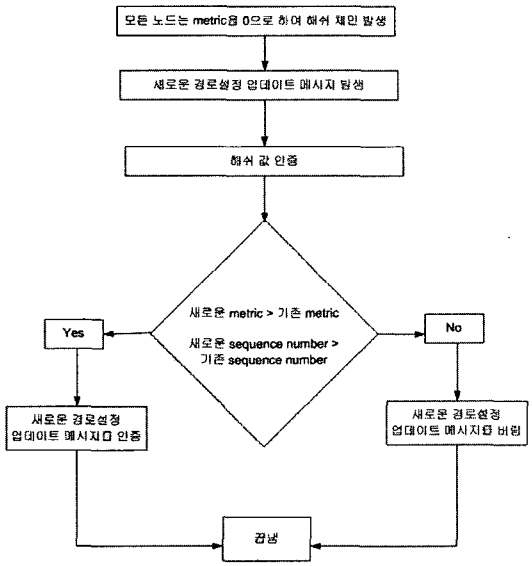


그림 3. zone 내부에서 경로설정 업데이트 인증 해쉬 알고리즘 흐름도

Fig. 3. Path establishment update authentication algorithm flowchart in zone inside.

2. 목적노드가 zone 외부에 있는 경우

목적노드가 zone 외부에 있는 경우에는 IERP를 개시하고 Route Query를 경계노드에게 보더캐스팅(bordercasting)을 하게 된다. 본 논문에서는 zone 외부에서 안전한 경로 설정 메시지를 주고받기 위해서 요구 기반 방식에서 사용되고 있는 경로설정 보안 알고리즘인 Ariadne[14,15]를 적용하였다.

zone 외부에서 경로설정 업데이트 메시지가 발생했을 때 경로설정 메시지 인증 알고리즘은 다음과 같다.

※표기법

S : 소스노드

D : 목적지 노드

h : 해쉬 함수

MAC : 메시지 인증 함수

M : HMAC 함수

id : 노드의 ID

ti : time interval

REQUEST : 경로설정 요청 메시지

REPLY : 경로설정 응답 메시지

단계 1. [초기 해쉬 함수 h_0을 발생]

경로설정 메시지가 발생하기 전에 소스에서 해쉬 함수를 발생한다.

$$h_0 = MAC_{k_{SD}}(REQUEST, S, D, id, ti)$$

단계 2. [경로 설정 요청 메시지를 통해서 다음 노드로 전파]

경로설정 요청 메시지는 다음과 같다.

$$< REQUEST, S, D, id, ti, h_0, (\text{노드}), (\text{노드의 } HMAC) >$$

단계 3. [노드가 경로설정 요청 메시지를 받으면 목적지 주소를 확인]

경로설정 요청 메시지에 목적지 주소가 맞으면 단계 5를 수행하고, 아니면 단계 4를 수행한다.

단계 4. [HMAC 인증 수행]

경로설정 요청 메시지의 목적지 주소가 아니면 다음과 같은 과정을 수행한다.

(단계 4-1) 해쉬 함수 발생

$$h_1 = H[A, h_0]$$

(단계 4-2) HMAC 함수 발생

$$M_A = MAC_{K_{ti}}(REQUEST, S, D, id, ti \\ h_1, (A), ())$$

(단계 4-3) 위의 과정을 거친 경로설정 요청 메시지를 다음 노드로 전파

$$< REQUEST, S, D, id, ti, h_1, (A), (M_A) >$$

(단계 4-4) 단계 3을 수행

단계 5. [소스에 경로설정 응답 메시지를 보냄]

목적지 주소를 찾으면 소스에게 경로설정 응답 메시지를 보낸다. 경로설정 응답 메시지는 다음과 같다.

$$< REPLY, D, S, ti, (\text{거쳐간 노드}), (\text{거쳐간 노드의 } HMAC), M_D >$$

단계 6. [끝냄]

모든 과정을 끝낸다.

그림 4는 위에서 살펴본 과정들을 흐름도로 보여주고 있다.

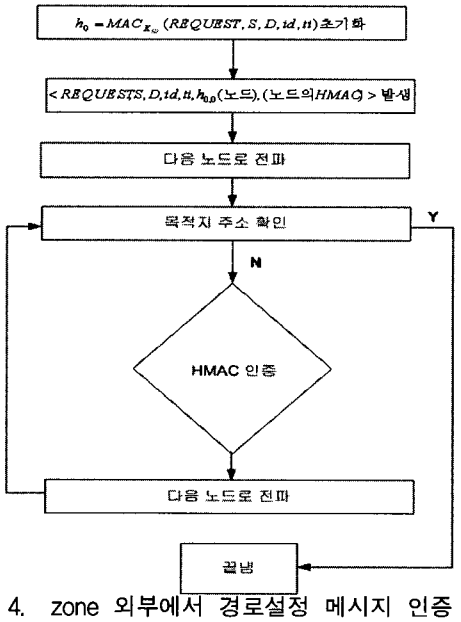


그림 4. zone 외부에서 경로설정 메시지 인증 알고리즘 흐름도

Fig. 4. Path establishment message authentication algorithm flowchart in zone outside.

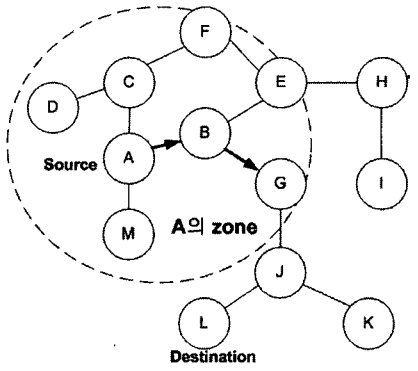


그림 5. zone 외부에서 경로설정 과정(Route Request)

Fig. 5. Path establishment process in zone outside(Route Request).

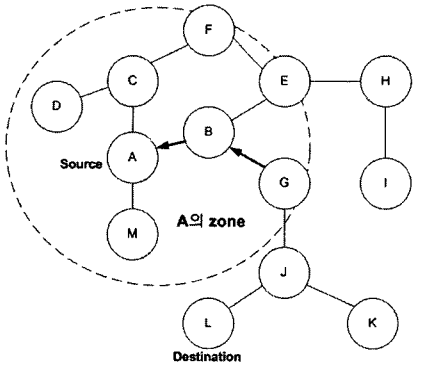


그림 6. zone 외부에서 경로설정 과정(Route Reply)

Fig. 6. Path establishment process in zone outside(Route Reply).

그림 5와 그림 6은 A 노드에서 L 노드까지 경로 설정을 하는 과정을 보여주고 있다. A 노드에서 목적지 주소가 자기 zone 외부에 있기 때문에 IERP를 개시하고 경로설정 요청 메시지를 B 노드에게 보내게 된다. B 노드 역시 L 노드가 자기 zone안에 없기 때문에 경로설정 요청 메시지를 G 노드에게 보내게 된다. G 노드에서 L 노드가 자기 zone안에 있기 때문에 더 이상 경로설정 요청 메시지를 보내지 않고 A 노드에게 Reply를 보내게 된다.

그림 7과 그림 8은 안전한 경로설정 메시지를 주고받는 과정을 보여주고 있다. 출발지 노드 A는 최초 $MAC_{K_{SD}}$(*RouteRequest, source id, destination id, broadcast id, time interval*)로 인증을 하며 $HMAC$은 비워진다.

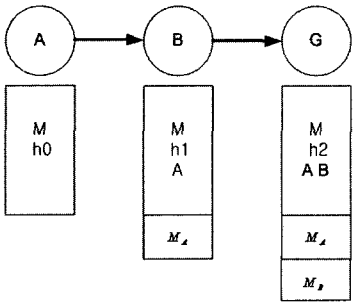
두 번째 노드 B는 원래의 메시지(*RouteQuery, source id, destination id, broadcast id, time interval*)를 전송받아서 A 노드와 B 노드간의 MAC 키를 이용하여 $HMAC$을 형성한다.

B 노드는 *HMAC* 값을 G 노드에 전송한다. B 노드부터 최종 도착지 G 노드까지, 두 번의 인증 절차를 거치게 되는데, *ID* 인증과 *HMAC*키 값에 의한 인증이다. 첫 번째, *ID* 인증은 다음과 같이 해쉬함수를 반복함으로써 이루어진다.

$H(\eta_n \| H(\eta_{n-1} \| \cdots\cdots \| H(\eta_1 \| MAC_{K_{SD}}(Message))))$ 여기서 η는 각 노드의 ID이다.

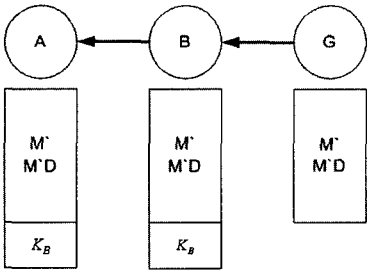
두 번째, *HMAC*값에 의한 인증은 각각의 노드가 이미 알고 있는 *MAC*키에 의해 전체 메시지를 인증하고 *HMAC*에 의한 인증을 반복한다. 이 때, 각 노드는 다음 경로설정을 위한 *HMAC* 값을 *HMAC* 키로 사용하기 위하여 저장한다.

ZRP에서 도착지 노드는 Reply를 전송하면서, Route Request를 전송할 때 받았던 전체 해쉬 값을 출발지 노드로 전송한다. 이러한 해쉬 값은 각 노드의 키 값이 된다. 이러한 출발지 노드와 각 노드간의 키는 멀티캐스팅으로 데이터를 전송하거나, RREP을 전송받을 때, 경로설정을 위한 별도의 키 분배 절차 없이 출발지 노드에 저장된 키를 가지고 경로를 설정한다. Reply 과정은 그림 8과 같다.



$M = < Route\ Request, S, D, id, ti >$
$h0 = MAC_{k_{SD}}(M)$
$h1 = H(A, ho)$
$HM_A = HMAC_{k_A} < M, h1, A >$
$h2 = H(B, h1)$
$HM_B = HMAC_{k_B} < M, h2, A, B, M_A >$

그림 7. 안전한 Route Request 과정
Fig. 7. Secure Route Request process.



$M' =< Reply, D, S, ti, A, B, M_A >\ K_B = M_B$
$M'_D = MAC_{k_{DC}}(M')$

그림 8. 안전한 Route Reply 과정
Fig. 8.= Secure Route Reply process.

Ⅳ. 성능평가

본 논문에서 기존의 Ariadne, SEAD와 S-ZRP 보안의 성능을 평가하기 위해서 시뮬레이션을 통하여 비교 분석하였다. 시뮬레이션은 버클리(Berkeley) 대학의 Network Simulator 2.26(NS-2.26)을 사용하였다. 시뮬레이션을 통하여 각각의 평균 데이터 수신율, 패킷 오버헤드, 경로 설정 탐색 시간을 비교 분석하였다.

1. 시뮬레이션 환경 및 파라미터

실험 환경으로는 무선 ad-hoc 망을 기본으로 하고, 최대 20m/s의 속도의 이동성을 가지는 50개의 노드들이 1500m x 300m의 지역 내에서 이동하게 된다. 50개의 노드 중 20개의 노드가 소스 노드로써 RREQ를 요청하게 되고, 나머지 노드들은 중간 노드 또는 목적 노드의 역할을 하게 된다. 그림 9는 ZRP의 zone radius에 따른 효율성의 결과를 보여준다. 이 결과에서 보면 zone radius가 2인 경우 최적의 효율성을 제공함을 확인할 수 있기 때문에 zone radius는 2홉으로 가정하였다. 각 소스 노드는 512 KByte의 패킷을 초당 4개씩 전송하게 되고, 실험에 사용된 MAC layer는 NS-2.26에 포함되어 있는 IEEE 802.11을 사용하였다.

위의 <표 1>와 같은 파라미터 값을 바탕으로 시뮬레이션 하였다. Ariadne와 SEAD의 파라미터의 값은 참고 논문 [8],[10]의 파라미터를 기본으로 하여 시뮬레이

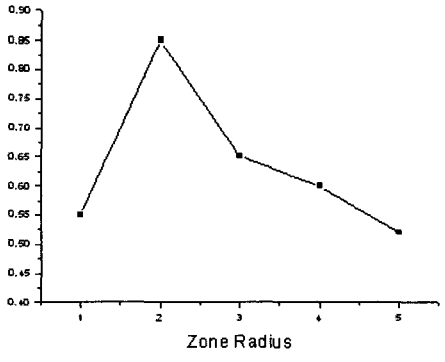


그림 9. zone 반경에 따른 효율성
Fig. 9. Efficiency by zone radius.

표 1. ZRP 시뮬레이션 파라미터
Table 1. ZRP simulation parameter.

항 목	값
네트워크 크기	1500 x 300m
노드의 수	50개
시뮬레이션 시간	900 sec
Zone 반경	2 (hop)
이동 속도	20 (m/s)
IARP 업데이트 시간	15 sec
beacon 주기	5 sec
데이터 패킷 크기	512 (Kbyte)

표 2. SEAD, Ariadne 시뮬레이션 파라미터
Table 2. SEAD, Ariadne simulat.

SEAD parameter	
경로설정 업데이트 시간	15 s
해쉬 길이	80 bits
Ariadne parameter	
초기 RREQ Timeout	2 s
최대 RREQ Timeout	40 s
Cache Size	32 routes
해쉬 길이	80 bits

션 하였다.

위의 <표 2>와 같은 파라미터 값을 바탕으로 시뮬레이션 하였다. ZRP 모델의 링크 계층 복잡성을 줄이기 위해 비트 오류율, 전파지연, 안테나 이득, 채널 일치 등의 설정들을 생략했고, 주요한 파라미터 이외의 값들은 기본설정 값을 사용하였다. 노드의 전송 반경은 한 노드에서 발생된 패킷이 직접 전송 될 수 있는 거리를 말한다.

2. 시뮬레이션 결과

본 시뮬레이션에서의 평균 경로 탐색 시간은 소스 노드에서 경로 탐색을 위해 RREQ를 보낸 후, RREP를 받을 때까지의 시간으로 측정하였고, 평균 패킷 수신율은 소스 노드에서 전송된 데이터에 비례하여 목적 노드에서 수신된 데이터의 비율을 계산하였고, 패킷 오버헤드는 경로설정 메시지를 전송할 때 오버헤드를 계산하였다.

그림 10은 ZRP 제안 방식과 Ariadne, SEAD의 평균

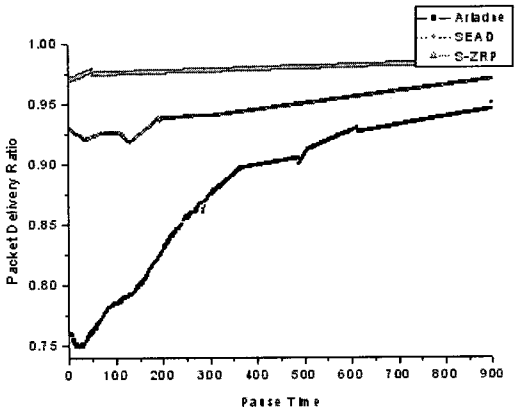


그림 10. 평균 데이터 수신율
Fig. 10. packet delivery ratio.

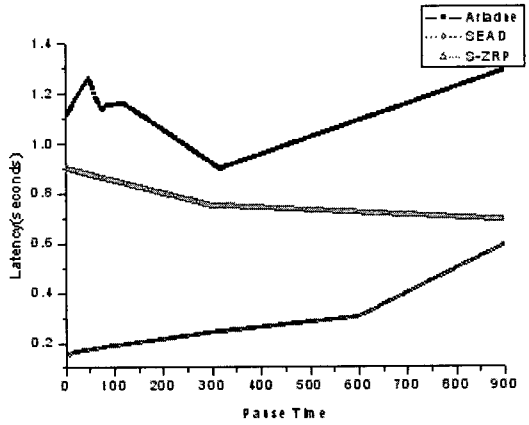


그림 11. 경로설정 탐색 시간
Fig. 11. Path establishment seek time.

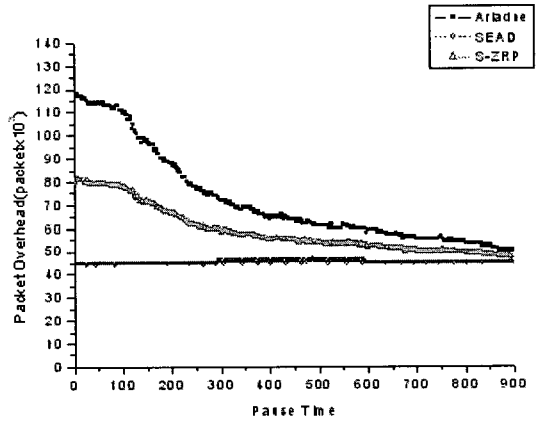


그림 12. 패킷 오버헤드
Fig. 12. packet overhead.

데이터 수신율(packet delivery ratio)을 나타낸다. ZRP 제안 방식은 다른 두 방식보다 일관된 출력을 보여준다. = ZRP는 zone안에서 경로설정 테이블을 관리하기 위해서 경로설정 메시지를 주기적으로 보내기 때문에 pause time이 증가할수록 평균데이터 수신율이 증가하는 것을 알 수 있다.

그림 11은 경로 설정 탐색 시간을 비교하였다. 경로 설정 탐색 시간을 보면 제안한 기법은 Ariadne보다 더 빠른 대응 능력을 보이지만 SEAD 보다는 약간 느린 결과를 보이고 있다. 이러한 이유는 zone 내에서는 SEAD와 거의 비슷한 성능을 보여주지만 zone 외부에서는 SEAD 보다 경로 설정 탐색 시간이 길어지기 때문에 이러한 결과를 보여준다. 모든 pause time에서 ZRP는 SEAD보다 느린 경로설정 탐색 시간을 보여주고 있다. 그 이유는 ZRP에서 오버헤드의 증가로 네트워크 capacity가 감소하기 때문이다.

그림 12는 packet 오버헤드를 보여주고 있다. 네트워크에서 오버헤드의 증가는 네트워크 내에서의 혼란을 야기 시킨다. packet 오버헤드 부분에서는 제안한 기법은 Ariadne보다 더 적고 SEAD보다는 많은 결과를 보여준다.

SEAD나 Ariadne은 장점과 단점을 모두 가지고 있다. SEAD는 빠른 경로설정 탐색 시간을 가지고 있지만, 수시로 노드들이 경로설정 업데이트 메시지를 주고받기 때문에 네트워크 capacity가 감소하는 문제가 있다. 또한 Ariadne는 네트워크 capacity 면에서는 뛰어나지만 경로설정 탐색시간이 느린 문제가 있다. S-ZRP는 이러한 문제점을 해결할 수 있는 특징을 시뮬레이션을 통하여 보여주고 있다.

V. 결 론

본 논문에서는 MANET 환경에서 테이블 기반 방식과 요구 기반 방식을 혼합한 ZRP를 바탕으로 하여 좀 더 효율적이고 잦은 토폴로지의 변화에 빠르게 대응할 수 있는 라우팅 경로 탐색 기법으로 제안되었다. 이러한 ZRP에 기존의 전력소비가 많고 속도가 느린 대칭키와 비대칭키 방식이 아닌 해쉬 체인을 사용하는 안전한 경로 탐색 알고리즘인 S-ZRP를 제안하였다. S-ZRP는 경로설정 패킷에 대한 무결성 보장과 근원지 인증을 통해 경로설정 패킷을 안전하게 전송할 수 있다.

제안한 기법은 성능분석을 통하여 경로 설정 탐색 시간은 Ariadne 보다는 더 빠른 대응 능력을 보이고, packet 오버헤드는 SEAD 보다 더 적은 결과를 보이고 있다. 또한 평균 데이터 수신율에서는 Ariadne나 SEAD 보다 더 좋은 성능을 보여주고 있다. SEAD는 빠른 경로설정 탐색 시간을 가지고 있지만, 수시로 노드들이 경로설정 업데이트 메시지를 주고받기 때문에 네트워크 capacity가 감소하는 문제가 있다. Ariadne는 네트워크 capacity 면에서는 뛰어나지만 경로설정 탐색 시간이 느린 문제가 있다. S-ZRP는 경로설정 탐색 시간과 packet 오버헤드 문제점을 해결할 수 있는 특징을 시뮬레이션을 통하여 확인 할 수 있었다.

MANET에서는 각 노드가 라우터의 역할도 해야 하기 때문에 일반 유선 기반 망에 비해 노드의 부하가 많은 단점을 가진다. 이러한 각 노드의 부하를 줄이고 동시에 빠른 경로 설정 탐색 시간을 보면 S-ZRP 경로 설정 방법이 효과적이다.

참 고 문 헌

[1] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April, 1999, pp. 46-55.

[2] 김경자, 장태무, "애드혹 네트워크에서 ZRP를 기반으로 하는 경로 탐색 기법," 정보처리학회논문지 C, 제3권, 293-300쪽, 2004년 6월.

[3] 권오성, 정의헌, 김준년 "MANET에 대해 QoS를 지원하는 ZRP의 성능연구", 한국통신학회 논문지 제28권 3A호 200-214쪽,2003년 2월.

[4] Don Coppersmith, Markus Jakobsson, "Almost Optimal Hash Sequence Traversal," Scientific Literature Digital Library, Dec. 2000.

[5] Don Coppersmith, Markus Jakobsson, "Almost Optimal Hash Sequence Traversal", Scientific Literature Digital Library, 2002.

[6] Z. J. Haas and M. R Realman, "The Zone Routing Protocol for Ad Hoc Networks,"Internet Draft draft-zone-routing-protocol-01.txt, Aug., 1998.

[7] Z. J. Haas and M. R Realman, "The Bodercast Resolution Protocol(BRP) for Ad Hoc Networks," Internet Draft draft-zone-brp-protocol-02.txt, July., 2002.

[8] Z. J. Haas and M. R Realman, "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks," Internet Draft draft-zone-iarp-protocol-02.txt, July., 2002.

[9] Peh Chern Liang, Tan Tong Joo, Teo Meng Wee, "Ad Hoc Wireless Networks-A Study on Zone Routing Protocol", School of Computing, National Univercity of Singapore, 2004.

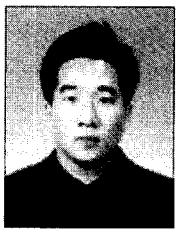
[10] Jan Schaumann, "Analysis of the Zone Routing Protocol", http://www.netmeister.org/misc/zrp, 2002.

[11] Yih-Chum Hu, Adrian Perrig, David B. Johnson, "Secure Efficient Distance Vector Routing for mobile wireless ad hoc networks," Fourth IEEE

Workshop on Mobile Computing Systems and Applications, Dec. 2003.
[12] Charles E. Perkins, Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" ,The ACM SIGCOMM Conference on Communications Architectures, Oct. 2002
[13] Tao Wan, Evanglos Kranakis, P.C. van Oorschot, " Securing the Destination Sequenced Distance Vector Routing Protocol (S-DSDV)", IEEE Wireless Communications, Vol 4, Aug. 2004.
[14] Yih-Chum Hu, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," The 8th ACM International Conference on Mobile Computing and Networking, Dec. 2002.
[15] Chai-Keong Toh, Georgia Elizabeth M. Royer, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, Vol. 6, Issue 2, April 1999, pp. 46-55.

저 자 소 개

서 대 열(학생회원)
2004년 서울산업대학교 전자 정보공학과 학사 졸업
2006년~현재 광운대학교 전자 통신공학과 석사 재학중
<주관심분야 : IEEE 802.15.4, Ad-hoc Security, Sensor Security, ZigBee Security>



김 진 철(정회원)
1995년 광운대학교 전자공학과 학사 졸업
1997년 광운대학교 전자공학과 석사 졸업
2006년~현재 광운대학교 전자공학과 박사과정
<주관심분야 : PKI, WPKI, Mobile Ad-hoc Network>

김 경 목(정회원)
1996년 서울산업대학교 전자공학과 학사 졸업.
2002년 광운대학교 전자통신 공학과 석사 졸업.
2006년 광운대학교 대학원 전자 통신공학과 박사 졸업.
<주관심분야 : Optical Internet, MPλS, GMPLS>

오 영 환(종신회원)
2004년 현재 광운대학교 전자통신공학과 교수
<주관심분야 : Network and Device Reliability>