Ad Hoc 네트워크를 위한 안전한 경로발견 프로토콜 제안†

(A Proposal of Secure Route Discovery Protocol for Ad Hoc Network)

박영호*, 김진규**, 김철수***
(Young-Ho Park, Jin-Gyu Kim, Cheol-Su Kim)

요 약 Ad hoc 네트워크는 고정된 기반 망의 도움없이 이동 단말만으로 구성된 자율적이고 독립적인 네트워크로 최근 다양한 분야에서의 활용이 논의되고 있다. 그러나, ad hoc 네트워크는 구성이 변하기 쉬운 환경이므로 불법 노드가 네트워크 자원소비 및 경로방해 등의 동작이 용이하므로 라우팅 프로토콜 보호가 필요하다. 따라서, 본 논문에서는 해쉬함수만을 이용한 경로발견 프로토콜과 해쉬함수 및 공개키 암호화 방식을 이용한 경로발견 프로토콜을 제안한다. 첫 번째 제안한 프로토콜은 active 공격에 약하나 전송패킷의 데이터 양이 적고 각 홉에서 처리하는 연산량이 적다는 장점이 있으며 두 번째 제안한 프로토콜은 active 공격에 강하다.

핵심주제어 : ad hoc 네트워크, 경로발견 프로토콜, 해쉬함수, 공개키 암호화 방식,

Abstract Ad hoc network is a collection of mobile nodes without using any infrastructure, it is using in the various fields. Because ad hoc network is vulnerable to attacks such as routing disruption and resource consumption, it is in need of routing protocol security. In this paper, we propose two secure route-discovery protocols. One is a protocol using hash function. This protocol is weak in active attack but has some merits such as small data of transmission packet and small computation at each hop. The other is a protocol using hash function and public key cryptography. This protocol is strong in active attack.

Key Words : ad hoc network, route discovery protocol, hash function, public key cryptography

1. 서 론

무선 ad hoc 네트워크는 고정된 기반 망의 도움없이 이동 단말만으로 구성된 자율적이고 독립적인 네트워크이다. 무선 ad hoc 네트워크에서의 단말은 능동적이며 네트워크의 참여와 이탈이 자유로우며 대등하게 네트워크를 구성하는 주체가 된다. 이는 고정되고 중앙 집중적인 기반 망에서의 단말이 수직적이고 수동적으로 동작하는 것과는 비교된다. ad hoc 네트워크는 구성이 단순하고 융통성 있으며, 일시적인 필요에 의한 임시 네트워크의 구성에 용이하기 때문에 다양한 분야에서의 응용이 논의되고 있다.[1,2]

무선 ad hoc 네트워크는 구성이 변하기 쉬운 환경이므로 불법 노드가 네트워크 자원소비 및 경로방해 등의 동작이 용이하다. 한 불법노드가 목적노드에 한 홉 떨어져 있다고 하면 목적노드로의 모든 경로는 그 노드를 통과할 것이며 이 불법노드는 경로요구 및 경로응답 패킷을 변경하여 데이터가 잘못 전달되도록 할 수 있고 라우팅 트래픽을 범람시켜 통신을 거절할 수도 있다. 이러한 고의적 행동들은 네트워크

† 본 논문은 2005년 동일재단 학술연구비 지원에 의하여 연구되었음.
* 상주대학교 전자전기공학부 부교수
** 상주대학교 전자전기공학부 조교수
*** 경주대학교 컴퓨터 · 멀티미디어공학부 부교수

동작을 불가능하게 할 수 있을 뿐 아니라 통신 전에 경로를 발견하는데 긴 지연을 일으킬 수도 있다. 따라서, ad hoc 네트워크에서의 라우팅 프로토콜 보호가 필요하다.[2-5]

라우팅 프로토콜에 발생할 수 있는 대표적인 공격은 경로방해 공격 및 자원소비 공격으로 DoS(denial of service) 공격의 한 형태로 볼 수 있다. 경로방해 공격은 정당한 데이터 패킷을 잘못된 경로로 가도록 하며 자원소비 공격은 네트워크 자원인 전력, 메모리 그리고 대역폭을 소비하도록 네트워크에 패킷을 주입하는 것이다.[4,6]

최근 연구된 무선 ad hoc 네트워크에서의 대표적인 안전한 라우팅 방식으로는 Ariadne 프로토콜[7], ARAN(authentication routing for ad hoc networks) 프로토콜[8], SAODV(secure AODV) 프로토콜[9] 등이 있다. Ariadne 등은 DSR(dynamic source routing) 방식에 기초한 ad hoc 네트워크에서의 안전한 라우팅 프로토콜인 Ariadne 프로토콜을 제시하였다. 이 프로토콜에서는 목적노드가 경로요구 패킷을 인증하며 데이터 인증을 위하여 TESLA(timed efficient stream loss-tolerant authentication) 프로토콜[10], 디지털 서명 그리고 MAC 기술을 사용한다. 또한, 경로요구 패킷의 노드 목록에서 노드가 빠지는 것을 막기 위하여 홉당 해쉬 기술을 사용한다. Kimaya 등은 AODV(ad hoc on-demand distance vector) 프로토콜[11]에 기초한 ARAN 프로토콜을 제시하였다. ARAN 프로토콜은 안전한 경로를 제공하기 위하여 인증서를 사용한다. ARAN에서의 경로발견은 시작 노드의 방송(broadcast)경로 발견 메시지에 의해 이루어지며 각 경로 메시지는 시작노드에서 목적노드로 이르는 각 홉에서 인증된다. Manel 등은 SAODV 프로토콜을 제안하였으며 이 방식은 경로요구와 경로응답 패킷을 인증하기 위하여 서명을 사용하고 각 홉을 인증하기 위하여 해쉬 체인을 사용한다.

Ariadne 프로토콜은 효율적인 대칭키 암호화 방식을 사용하나 네트워크 상에서 도청하는 passive 공격과 데이터 패킷을 삽입하는 공격은 막지 못한다. 또한, Ariadne 프로토콜은 발견된 경로 상에서 active-1-1 공격에 약하다. ARAN 프로토콜은 인증을 위해서 공개키 암호화 방식을 사용하기 때문에 서명검증에 요구된 위조 제어패킷을 네트워크에 과다하게 하는 DoS 공격에 특히 약하다.

본 논문에서는 기존의 경로발견 프로토콜들을 분석하여 ad hoc 네트워크에서 보다 효율적이고 안전한 두개의 경로발견 프로토콜을 제안한다. 해쉬함수만을 이용하여 제안한 경로발견 프로토콜은 Ariadne 프로토콜에 기초하여 제안한 방식이며 Ariadne 프로토콜과 마찬가지로 active 공격에 약하나 Ariadne 프로토콜보다 전송패킷의 데이터 양이 적고 각 홉에서 처리하는 연산량이 적다는 장점이 있다. 해쉬함수 및 공개키 암호화 방식을 이용한 제안한 경로발견 프로토콜은 경로요구 시는 해쉬함수만을 이용하여 제안한 경로발견 프로토콜과 같으나 경로응답 시 경로의 각 홉에서 공개키 방식으로 암호화를 하여 시작노드에서 각 홉에 대한 인증 및 홉을 가장한 active 공격에 강하다.

2. Ariadne 프로토콜

대칭키 방식을 이용한 대표적인 라우팅 프로토콜로는 Ariadne 프로토콜이 있다. Ariadne 프로토콜은 요구시 경로를 설정하고 시작노드에서 목적노드로 패킷을 전송한다. Ariadne 프로토콜은 목적노드가 경로요구의 인증을 검증한다. 경로요구 패킷에서 각 영역의 적법성을 확인하기 위하여 시작노드는 비밀키 K_{SD}로 패킷 데이터의 MAC(message authentication code)를 포함시키며 목적노드는 분배된 키 K_{SD}로 경로요구 패킷의 인증 및 새로운 것임을 쉽게 검증할 수 있다. 또한, 경로요구 패킷의 노드목록에서 노드가 제외되는 것을 막기 위하여 홉당 해쉬기술을 사용한다. 이 프로토콜에서 시작노드와 목적노드는 비밀키 K_{SD}와 K_{DS}를 분배된 것으로 가정하고 모든 노드는 TESLA 일방향 키 체인을 가진다고 가정하며 모든 노드는 서로다른 노드의 TESLA 일방향 키 체인의 인증키를 안다고 가정한다.

경로요구 패킷은 8개의 영역으로 구성되며 <ROUTE REQUEST, initiator, target, id, time interval, hash chain, node list, MAC list>와 같다. initiator와 target은 시작과 목적노드의 주소를 나타내며 시작노드는 id를 경로발견을 시작하는데 최근 사용되지 않았다는 식별자로 사용한다. Time interval은 목적지에서 경로요구 패킷의 예측도착 시간에서 TESLA 시간간격이다. 해쉬 체인 값은 $MAC_{K_{SD}}(initiator, target, id, time interval)$로 계산되며 노

$$S: h_0 = MAC_{K_{SD}}(REQUEST, S, D, id, ti)$$
$$S \rightarrow broadcast: < REQUEST, S, D, id, ti, h_0, (), () >$$

$$A: h_1 = H[A, h_0]$$
$$M_A = MAC_{K_{A_n}}(REQUEST, S, D, id, ti, h_1, (A), ())$$
$$A \rightarrow broadcast: < REQUEST, S, D, id, ti, h_1, (A), (M_A) >$$

$$B: h_2 = H[B, h_1]$$
$$M_B = MAC_{K_{B_n}}(REQUEST, S, D, id, ti, h_2, (A, B), (M_A))$$
$$B \rightarrow broadcast: < REQUEST, S, D, id, ti, h_2, (A, B), (M_A, M_B) >$$

$$C: h_3 = H[C, h_2]$$
$$M_C = MAC_{K_{C_n}}(REQUEST, S, D, id, ti, h_3, (A, B, C), (M_A, M_B))$$
$$C \rightarrow broadcast: < REQUEST, S, D, id, ti, h_3, (A, B, C), (M_A, M_B, M_C) >$$

$$D: M_D = MAC_{K_{DS}}(REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_C))$$
$$D \rightarrow C: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, () >$$
$$C \rightarrow B: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, (K_{C_n}) >$$
$$B \rightarrow A: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, (K_{C_n}, K_{B_n}) >$$
$$A \rightarrow S: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, (K_{C_n}, K_{B_n}, K_{A_n}) >$$

<그림 1> Ariadne 경로발견 프로토콜

드목록과 MAC 목록은 비워둔다.

그림 1은 Ariadne에서의 경로발견 프로토콜의 예를 나타낸 것이다. 한 노드 A가 경로요구 패킷을 수신하면 같은 경로발견에서 경로요구 패킷을 이미 수신했는지를 확인하기 위해 최근 수신한 경로요구 패킷의 <initiator, id> 값의 표를 검사하며 이미 수신하였다면 그 패킷을 무시한다. 노드 A는 또한 time interval을 검사한다. 만약, time interval이 타당하지 않으면 수신한 패킷을 무시한다. 만약, time interval이 타당하면 경로요구 패킷의 노드목록에 자신의 주소 A를 첨부하고 해쉬 체인 영역에 $H[A, hash\ chain]$ 값으로 대체하고 MAC 목록에 MAC 값을 첨부한다. 노드 A는 MAC 값을 계산하기 위하여 TESLA 키 K_{A_i}를 사용한다.

목적노드가 경로요구 패킷을 수신하면 해쉬 체인 값을 검사함으로써 경로요구 패킷의 타당성을 검사한다. 만약, 타당하다면 목적노드는 시작노드로 경로응답 패킷을 전송한다. 경로응답 패킷은 <ROUTE REPLY, target, initiator, time interval, node list, MAC list, target MAC, key list>로 구성된다. 경로응답 패킷은 경로요구 패킷의 노드목록에 있는 노드를 따라 시작노드로 전송된다.

경로응답 패킷을 처리하는 노드는 응답패킷의 키 목록 영역에 키를 첨부하고 패킷에 나타난 경로를 따라 패킷을 전송한다. 시작노드가 경로응답 패킷을 수신하면 키 목록에 있는 키가 맞는지, 목적 MAC 값 M_D가 맞는지 그리고 MAC 목록에 있는 각 MAC 값들이 맞는지 검사한다. 만약, 모든 절차가 타당하면 시작노드는 경로응답 패킷을 받아들인다.

3. ARAN 프로토콜

ARAN 프로토콜은 안전한 경로를 제공하기 위하여 인증서를 사용한다. ARAN에서의 경로 발견은 시작노드의 방송경로 발견 메시지에 의해 이루어지며 각 경로 메시지는 시작노드에서 목적노드로 이르는 각 홉에서 인증된다. ARAN은 신뢰된 인증서버(T)를 사용하며 그 공개키는 모든 노드에 알려진다. 각 노드는 ad hoc 네트워크에 들어가기 전 인증서버로부터 인증서를 요구해야 하고 인증서버는 노드의 실체를 인증한 후 인증서를 배부한다. 한 노드 S는 다음과 같이 인증서버로부터 인증서를 수신한다.

$$T \rightarrow S: cert_S = [S, K_{S+}, t, e]K_{T-}$$

여기서 S는 시작노드의 주소, K_{S+}는 S의 공개키, t는 인증이 이루어진 timestamp이고 e는 인증서가 만료

$$S \rightarrow broadcast: < (REQUEST, D, cert_S, N, t)K_{S-} >$$
$$A \rightarrow broadcast: < ((REQUEST, D, cert_S, N, t)K_{S-})K_{A-}, cert_A >$$
$$B \rightarrow broadcast: < ((REQUEST, D, cert_S, N, t)K_{S-})K_{B-}, cert_B >$$
$$C \rightarrow broadcast: < ((REQUEST, D, cert_S, N, t)K_{S-})K_{C-}, cert_C >$$

$$D \rightarrow C: < (REPLY, S, cert_D, N, t)K_{D-} >$$
$$C \rightarrow B: < ((REPLY, S, cert_D, N, t)K_{D-})K_{C-}, cert_C >$$
$$B \rightarrow A: < ((REPLY, S, cert_D, N, t)K_{D-})K_{B-}, cert_B >$$
$$A \rightarrow S: < ((REPLY, S, cert_D, N, t)K_{D-})K_{A-}, cert_A >$$

<그림 2> ARAN 경로 발견 프로토콜.

되는 시간이다.

그림 2는 ARAN 경로발견 프로토콜 예를 나타낸 것이다. 경로발견을 시작하기 위하여 시작노드 S는 목적지 D, 시작노드의 인증서, 난수 N 그리고 timestamp t를 포함하는 서명된 경로요구 패킷을 방송한다. N과 t는 네트워크에서 패킷이 새로운 것임을 나타낸다. 노드 C는 B의 인증서 값 $cert_B$를 검사하고 서명값을 검사한다. C는 시작노드 S의 인증서 $cert_S$를 확인하고 수신된 경로요구 패킷의 서명값을 확인하기 위하여 인증서 내의 키를 사용한다. 만약, 서명값이 맞으면 이전 B의 서명값을 제거하고 원 경로요구 패킷에 C의 서명값을 첨가해서 패킷을 방송한다.

경로요구 패킷이 목적지 노드 D에 도착했을때 D는 서명한 경로응답 패킷을 수신한 이전 노드 C로 전송한다. 경로응답 패킷은 경로요구 패킷이 전송된 한방향의 경로로 전송되며 각 노드에서의 서명값 처리과정은 경로요구와 같다.

4. SAODV(secure AODV) 프로토콜

SAODV 프로토콜 방식은 경로요구와 경로응답 패킷을 인증하기 위하여 서명을 사용하고 홉을 인증하기 위하여 해쉬체인을 사용한다. 네트워크의 노드들은 SAODV 서명으로 AODV 라우팅 패킷을 인증한다. SAODV 프로토콜에서는 경로요구 패킷에 하나의 서명 확장자를 포함한다. 시작노드는 예측된 네트워크 크기에 기초하여 최대 홉 수를 선택하고 (최대 홉 수 +1) 길이의 일방향 해쉬함수를 발생하며 이 해쉬체인은 거리 인증자로 사용된다. 시작노드는 경로요구 패킷과 해쉬체인 값을 서명하며 이 서명 값과 해쉬체인 값은 서명 확장자에 포함된다. 서명 확장자는 경로요구 패킷 헤드의 홉 수에 기초한 해쉬체인의 요소를 포함하며 이 값은 홉 수 인증자이다. 만약, 해쉬체인 값 $h_0, h_1, ..., h_N$이 $h_i = H[h_{i+1}]$과 같이 발생된다면 홉 수 인증자 h_i는 $N-i$의 홉 수와 일치한다. 경로요구 패킷 헤드에서 홉 수 영역을 검증하기 위하여 한 노드는 해쉬체인을 따를 수 있다. 예를 들어

$$S \rightarrow broadcast: < (REQUEST, id, S, seq_S, D, oldseq_D, h_0, N)_{K_S-}, 0, h_N >$$
$$A \rightarrow broadcast: < (REQUEST, id, S, seq_S, D, oldseq_D, h_0, N)_{K_S-}, 1, h_{N-1} >$$
$$B \rightarrow broadcast: < (REQUEST, id, S, seq_S, D, oldseq_D, h_0, N)_{K_S-}, 2, h_{N-2} >$$
$$C \rightarrow broadcast: < (REQUEST, id, S, seq_S, D, oldseq_D, h_0, N)_{K_S-}, 3, h_{N-3} >$$

$$D \rightarrow C: < (REPLY, D, seq_D, S, lifetime, h_0', N)_{K_D-}, 0, h_N' >$$
$$C \rightarrow B: < (REPLY, D, seq_D, S, lifetime, h_0', N)_{K_D-}, 1, h_{N-1}' >$$
$$B \rightarrow A: < (REPLY, D, seq_D, S, lifetime, h_0', N)_{K_D-}, 2, h_{N-2}' >$$
$$A \rightarrow S: < (REPLY, D, seq_D, S, lifetime, h_0', N)_{K_D-}, 3, h_{N-3}' >$$

<그림 3> SAODV 경로발견 프로토콜

홉 수 영역이 i이면 홉 수 인증자 h_{ca}는 $H^i[h_N]$이다. 홉 수 길이 N과 해쉬체인 값 h_N는 경로요구 패킷의 서명 확장자에 포함되며 서명에 의해 인증되기 때문에 한 노드는 해쉬체인 값인 $h_N = H^{N-i}[h_{ca}]$를 보장할 수 있다.

그림 3은 SAODV에서의 경로발견 프로토콜을 나타낸 것이다. 한 노드 C에 경로요구 패킷이 수신되면 노드 C는 먼저 경로요구 패킷의 각 영역이 타당한지 확인하기 위하여 경로요구 패킷을 인증한다. 노드 C는 각 경로 발견에 하나의 경로요구 패킷을 보내기 위하여 중복금지 기능을 수행한다. 노드 C는 경로요구 패킷의 홉 수 영역을 증가시키고 홉 수 인증자를 해쉬하여 경로요구 패킷을 방송한다. 경로요구 패킷이 목적노드에 도착하면 목적노드는 경로요구 서명확장에 있는 인증 값을 검사한다. 만약, 경로요구 패킷이 타당하면 경로응답 패킷을 전송한다. 한 노드 B가 C로부터 경로응답 패킷을 수신하면 서명확장 값을 검사한다. 만약, 서명이 타당하면 노드 B는 목적노드 D의 다음 노드가 C라는 경로테이블을 설립한다.

SAODV 프로토콜에서는 경로응답 이중서명 확장자의 사용을 통해 중간노드 응답을 허용한다. 경로요구에 응답하는 한 중간노드는 경로응답 이중서명 확장자를 포함한다. 아이디어는 목적노드로 경로를 설립하는 것이며 중간노드는 목적노드로부터 전송된 경로응답 패킷을 전송해야만 한다. 만약, 중간노드가 경로응답 패킷과 서명 값을 저장했다면, 그 노드는 경로응답 패킷의 순서번호가 경로요구 패킷의 순서번호보다 더 크면 경로응답 패킷을 전송한다. 중간노드에서 계산된 서명 값은 이러한 경로응답 패킷의 영역을 인증하는데 사용된다.

ARAN 프로토콜과 SAODV 프로토콜은 AODV 프로토콜에 기초한 방식이나 두 프로토콜의 주된 차이점은 ARAN 프로토콜은 이전 홉을 인증하기 위하여 인증서버를 이용하며 SAODV 프로토콜은 해쉬 체인을 사용하는 것이다. 또한, ARAN 프로토콜은 경로유지를 위해 경로에러가 발생한 노드에서 서명한 메시지를 시작노드로 전송하나 SAODV 프로토콜은 경로에러 메시지가 전송되는 각 노드에서 경로에러 메시지를 서명한 값을 전송한다.

5. 제안한 경로발견 프로토콜

Ariadne 프로토콜은 효율적인 대칭키 암호화 방식을 사용하나 네트워크 상에서 도청하는 passive 공격과 데이터 패킷을 삽입하는 공격은 막지 못하고 발견된 경로 상에서 active-1-1 공격에 약하다. 또한, Ariadne 프로토콜은 전송 홉 수가 증가하면 각 홉의 MAC값과 키의 값이 전송되므로 전송데이타 양이 증가되며 경로응답 패킷에 각 홉의 키가 평문으로 전송되므로 키가 노출된다. ARAN 프로토콜은 인증을 위해서 공개키 암호화 방식을 사용하기 때문에 서명검증에 요구된 위조 제어패킷을 네트워크에 과다하게 하는 DoS 공격에 특히 약하다. ARAN 프로토콜과 SAODV 프로토콜은 공개키 암호화 방식을 사용하므로 Ariadne 프로토콜에 비해 각 홉에서의 연산처리량이 많다. 또한, 경로요구와 경로응답 패킷에 경로에 관한 정보를 포함하고 있지 않으므로 각 홉에서 경로 테이블을 관리해야 하는 부하가 있다.

$S: h_0 = MAC_{K_{SD}}(REQUEST, S, D, id, ti)$
$S \rightarrow broadcast: < REQUEST, S, D, id, ti, h_0, ( ) >$
$A: h_1 = H[A, h_0]$
$A \rightarrow broadcast: < REQUEST, S, D, id, ti, h_1, (A) >$
$B: h_2 = H[B, h_1]$
$B \rightarrow broadcast: < REQUEST, S, D, id, ti, h_2, (A, B) >$
$C: h_3 = H[C, h_2]$
$C \rightarrow broadcast: < REQUEST, S, D, id, ti, h_3, (A, B, C) >$

$D: h_0' = MAC_{K_{DS}}(REPLY, D, S, t_i)$
$D \rightarrow C: < REPLY, D, S, ti, h_0', (A, B, C) >$
$C: h_1' = H[C, h_0']$
$C \rightarrow B: < REPLY, D, S, ti, h_1', (A, B, C) >$
$B: h_2' = H[B, h_1']$
$B \rightarrow A: < REPLY, D, S, ti, h_2', (A, B, C) >$
$A: h_3' = H[A, h_2']$
$A \rightarrow S: < REPLY, D, S, ti, h_3', (A, B, C) >$

<그림 4> 해쉬함수만을 이용한 경로발견 프로토콜

본 논문에서는 해쉬함수만을 이용하여 경로인증을 하는 경로발견 프로토콜과 해쉬함수 및 공개키 암호화 방식을 이용하여 경로인증 및 경로상의 각 홉의 인증을 하는 프로토콜을 제안한다. 그림 4는 해쉬함수만을 이용하여 경로상의 홉과 패킷을 인증하는 제안한 경로발견 프로토콜이다. 본 프로토콜은 경로상의 홉에서 해쉬함수만 계산하면 되므로 적은 부하만

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

$S \rightarrow broadcast : < REQUEST, S, D, id, ti, h_0, ( ) >$

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

$A \rightarrow broadcast : < REQUEST, S, D, id, ti, h_1, (A) >$

$B : h_2 = H[B, h_1]$

$B \rightarrow broadcast : < REQUEST, S, D, id, ti, h_2, (A, B) >$

$C : h_3 = H[C, h_2]$

$C \rightarrow broadcast : < REQUEST, S, D, id, ti, h_3, (A, B, C) >$

$D : h_0' = MAC_{K_{DS}}(REPLY, D, S, t_i)$

$D \rightarrow C : < (REPLY, D, S, ti)_{K_D-}, h_0', (A, B, C) >$

$C : h_1' = H[C, h_0']$

$C \rightarrow B : < ((REPLY, D, S, ti)_{K_D-})_{K_C-}, h_1', (A, B, C) >$

$B : h_2' = H[B, h_1']$

$B \rightarrow A : < (((REPLY, D, S, ti)_{K_D-})_{K_C-})_{K_B-}, h_2', (A, B, C) >$

$A : h_3' = H[A, h_2']$

$A \rightarrow S : < ((((REPLY, D, S, ti)_{K_D-})_{K_C-})_{K_B-})_{K_A-}, h_3', (A, B, C) >$

<그림 5> 해쉬함수 및 공개키 방식을 이용한 경로발견 프로토콜

을 허용하는 ad hoc 네트워크에 적합한 방식이다. 경로요구 패킷은 MAC 값이 연산되는 것을 제외하면 Ariadne 프로토콜과 유사하다. 한 노드 A가 경로요구 패킷을 수신하면 같은 경로발견에서 경로요구 패킷을 이미 수신했는지를 확인하기 위해 최근 수신한 경로요구 패킷의 <initiator, id> 값의 표를 검사하며 이미 수신하였다면 그 패킷을 무시한다. 노드 A는 또한 time interval을 검사한다. 만약, time interval이 타당하지 않으면 수신한 패킷을 무시한다. 만약, time interval이 타당하면 경로요구 패킷의 노드목록에 자신의 주소 A를 첨부하고 해쉬 체인 영역에 $H[A, hash\ chain]$ 값으로 대체한다. 경로응답 패킷은 경로요구시 설정된 경로로 전송되며 패킷은 경로요구시와 같은 형태이다. 본 프로토콜은 Ariadne 프로토콜과 마찬가지로 active 공격에 약하나 Ariadne 프로토콜보다 전송패킷의 데이터 양이 적고 각 홉에서 처리하는 연산량이 적다는 장점이 있다.

그림 5는 해쉬함수 및 공개키 암호화 방식을 이용하여 경로상의 각 홉과 패킷을 인증하는 프로토콜을 제안한 것이다. 본 프로토콜에서의 경로요구는 제안한 해쉬함수만을 이용하여 경로인증을 하는 프로토콜과 같다. 목적노드가 경로요구 패킷을 수신하면 해쉬 체인 값을 검사함으로써 경로요구 패킷의 타당성을 검사한다. 만약, 타당하다면 목적노드는 시작노드로 경로응답 패킷을 전송한다. 경로응답 패킷은 경로요구시 설정된 경로로 전송된다. 경로응답 패킷의 전송시 각 홉은 자신의 비밀키로 수신된 $(REPLY, D, S, t_i)_{K_i-}$ 값을 계산하고 경로요구와 같이 해쉬함수 값을 첨부한다. 시작노드가 경로응답 패킷을 수신하면 경로상의 각 홉의 공개키를 이용하여 $(REPLY, D, S, t_i)$ 값을 구한 후 시간 t_i가 허용된 시간 내에 도착하였는지 검사한다. 만약, 허용된 시간내에 경로응답 패킷이 도착하였다면 해쉬함수 값을 검사하여 경로인증을 한다. 본 프로토콜은 경로응답의 각 홉이 자신의 비밀키로 암호화 하는 과정이 있고 시작노드에서 공개키로 복호화하는 과정이 있어 정당한 홉을 가장한 active 공격에 강하다.

6. 결 론

본 논문에서는 해쉬함수만을 이용한 경로발견 프로토콜과 해쉬함수 및 공개키 암호화 방식을 이용한 경로발견 프로토콜을 제안하였다. 해쉬함수만을 이용

한 제안한 경로발견 프로토콜은 경로상의 홉에서 해쉬함수만 계산하면 되므로 적은 부하만을 허용하는 ad hoc 네트워크에 적합한 방식이다. 본 프로토콜은 Ariadne 프로토콜과 마찬가지로 active 공격에 약하나 Ariadne 프로토콜보다 전송패킷의 데이터 양이 적고 각 홉에서 처리하는 연산량이 적다는 장점이 있다. 해쉬함수 및 공개키 암호화 방식을 이용한 경로발견 프로토콜은 경로응답의 각 홉이 자신의 비밀키로 암호화 하는 과정이 있고 시작노드에서 공개키로 복호화하는 과정이 있어 정당한 홉을 가장한 active 공격에 강하다. 향후 ad hoc 네트워크 상에서 시뮬레이션을 통해 제안한 프로토콜과 기존의 Ariadne 프로토콜 등을 비교함으로써 제안한 프로토콜들을 보다 체계화시키는 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] 권혜연, 신재욱, 이병복, 최지혁, 남상우 "이동 Ad-Hoc 네트워크 서비스," 전자통신동향분석, 제 18권, 제4호, pp.23-35, 2003년 8월

[2] 신진섭, 김진규, 박영호,"이동 Ad Hoc 네트워크에서의 경로발견에 관한 연구," 한국산업정보학회 춘계학술대회 논문집, pp.49-54, 2005년 5월

[3] P.Papadimitratos, Z.J.Haas, and P.Samar "The Secure Routing Protocol(SRP) for Ad Hoc Networks," Internet Draft, December 2002.

[4] Yih-Chun Hu and Adrian Perrig "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy, pp.28-39, May/June 2004.

[5] S.Gupte and M.Singhal "Secure Routing in Mobile Wireless Ad Hoc Networks," Elsevier, Ad Hoc Networks, pp.151-174, 2003.

[6] S.Marti et al. "Mitigating Routing Misbehaviour in Mobil Ad Hoc Networks," MOBICOM 2000, ACM Press, pp.255-265, 2000.

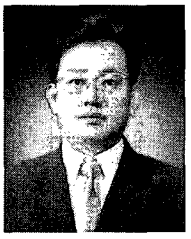
[7] Y.C. Hu, A.Perrig, and D.B.Johnson,"Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," MOBICOM 2002, ACM Press, pp.12-23, 2002.

[8] K. Sanzgiri et al,"A Secure Routing Protocol for Ad Hoc Networks," ICNP 2002, IEEE Press, pp.78-87, 2002.

[9] M. G. Zapata and N. Asokan "Securing Ad Hoc Routing Protocols," WISE 2002, ACM Press, pp.1-10, 2002.

[10] A.Perrig, R. Canetti, and B. Whillock "TESLA: Multicast Source Authentication Transform Specification," IETF Internet Draft, October 2002.

[11] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp.90-100, February 1999,

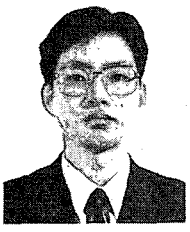


박 영 호 (Young-Ho Park)

종신회원

- 1989년 2월 경북대학교 전자공학과(공학사)
- 1991년 2월 경북대학교 대학원 전자공학과(공학석사)
- 1995년 8월 경북대학교 대학원 전자공학과 (공학박사)
- 1996년 3월 ~ 현재 상주대학교 전자전기공학부 부교수
- 2003년 8월 ~ 2004년 7월 Oregon State University 방문 교수

<관심분야> : 네트워크 보안, 광통신 보안 등



김 진 규 (Jin-Gyu Kim)

- 1990년 2월 경일대학교 전기공학과(공학사)
- 1994년 2월 경북대학교 대학원 전기공학과(공학석사)
- 1998년 8월 경북대학교 대학원 전기공학과(공학박사)
- 2000년 7월 ~ 2001년 8월 경북대학교 전자전기공학부 BK조교수
- 2001년 9월 ~ 현재 상주대학교 전자전기공학부 조교수

<관심분야> : 전력통신, 정보보호 등

김 철 수 (Cheol-Su Kim)

정회원

- 1989년 2월 경북대학교 전자공학과(공학사)
- 1991년 2월 경북대학교 대학원 전자공학과 (공학석사)
- 1997년 2월 경북대학교 대학원 전자공학과 (공학박사)
- 1995년 3월 ~ 1998년 2월 김천대학 전자통신과
- 1998년 3월 ~ 현재 경주대학교 컴퓨터·멀티미디어공학부 부교수

<관심분야> : 광통신, 정보보호 등