대칭키 암호화를 이용한 Ad Hoc 네트워크에서의 안전한 경로발견 프로토콜 제안†

(A Proposal of Secure Route Discovery Protocol for Ad Hoc Network using Symmetric Key Cryptography)

박 영 호*, 이 상 곤**, 문 상 재***
(Young Ho Park, Sang Gon Lee, Sang Jae Moon)

요 약 Ad hoc 네트워크는 구성이 변하기 쉬운 환경이므로 불법 노드가 네트워크 자원소비 및 경로방해 등의 동작이 용이하므로 라우팅 프로토콜 보호가 필요하다. 본 논문에서는 대칭키 암호화 방식을 이용하여 효율적이고 안전한 경로발견 프로토콜을 제안한다. 제안한 프로토콜은 대칭키 암호화 방식을 이용하여 각 홉에서 처리하는 연산량을 줄이며 경로응답 시 암/복호화 과정이 있어 정당한 홉을 가장한 active 공격에 강하다

핵심주제어 : ad hoc 네트워크, 경로발견 프로토콜, 대칭키 암호화

Abstract 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 an efficient and secure route discovery protocol for ad hoc network using symmetric key cryptography. This protocol has small computation loads at each hop using symmetric key cryptography. In the Route Reply, encryption/decrytion are used to guard against active attackers disguising a hop on the network.

Key Words : ad hoc network, route discovery protocol, symmetric key cryptography

1. 서 론

무선 ad hoc 네트워크는 고정된 기반 망의 도움 없이 이동 단말만으로 구성된 자율적이고 독립적인 네트워크이다. 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 동작을 불가능하게 할 수 있을 뿐 아니라 통신 전에 경로를 발견하는데 긴 지연을 일으킬 수도 있다. 따라서, ad hoc 네트워크에서의 라우팅 프로토콜 보호가 필요하다.[1-4]

라우팅 프로토콜에 발생할 수 있는 대표적인 공격은 경로방해 공격 및 자원소비 공격으로

† 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0026)
* 경북대학교 이공대학 전자전기공학부 교수
** 동서대학교 컴퓨터정보공학부 교수
*** 경북대학교 전자전기컴퓨터학부 교수

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.[1,3,5]

최근 연구된 무선 ad hoc 네트워크에서의 대표적인 안전한 라우팅 방식으로는 Ariadne 프로토콜[6], ARAN(authentication routing for ad hoc networks) 프로토콜[7], SAODV(secure AODV) 프로토콜[8], Youngho 프로토콜[9] 등이 있다.

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. 최근 Youngho 등은 경로응답 시 경로의 각 홉에서 공개키 방식으로 암호화를 하여 시작노드에서 각 홉에 대한 인증 및 홉을 가장한 active 공격에 강한 프로토콜을 제안하였으나 각 홉에서 공개키 암호화를 수행하여야 하므로 연산 부하가 비교적 많다는 단점이 있다.

본 논문에서는 무선 ad hoc 네트워크에서의 효율적이고 안전한 경로발견 프로토콜을 제안한다. 제안한 프로토콜에서는 ad hoc 네트워크의 각 노드에서 연산량을 줄이기 위하여 대칭키 암호화 방식을 사용한다. 또한, 대칭키 암호화 방식에서 사용될 키를 안전하게 분배하기 위하여 ad hoc 네트워크 노드들의 검증자, EOR 및 해쉬함수를 이용한다. 본 프로토콜은 ad hoc 네트워크 경로상의 각 노드에서 연산 부하가 적으므로 DoS 공격에 강하고 경로응답 시 암/복호화 과장이 있어서 active 공격에도 강하다.

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

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

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

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

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

<그림 1> Ariadne 경로발견 프로토콜

2. 기존의 대표적인 프로토콜

2.1 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[10] 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 노드목록과 MAC 목록은 비워둔다. 그림 1은 Ariadne에서의 경로발견 프로토콜의 예를 나타낸 것이다.

2.2 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 만료되는 시간이다. 그림 2는 ARAN 경로발견 프로토콜 예를 나타낸 것이다. 한다.

2.3 SAODV(secure AODV) 프로토콜

SAODV 프로토콜 방식은 경로요구와 경로응답 패킷을 인증하기 위하여 서명을 사용하고 홉을 인증하기 위하여 해쉬체인을 사용한다. 네트워크의

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

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

<그림 2> ARAN 경로 발견 프로토콜.

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

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

<그림 3> SAODV 경로발견 프로토콜

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 해쉬 함수를 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 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.

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.

2.4 Youngho 프로토콜

Youngho 등은 해쉬함수 및 공개키 암호화 방식을 이용하여 경로상의 각 홉과 패킷을 인증하는 프로토콜을 제안하였다.[9] 본 프로토콜은 경로응답의 각 홉이 자신의 비밀키로 암호화 하는 과정이 있고 시작노드에서 공개키로 복호화하는 과정이 있어 정당한 홉을 가장한 active 공격에 강하나 각 홉에서 암/복호 시 공개키 연산을 수행하므로 연산 부하가 비교적 많다는 단점이 있다.

그림 4는 Youngho 프로토콜의 예를 나타낸 것이다. 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.

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

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

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

<그림 4> Youngho 프로토콜.

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.

3. 기존의 프로토콜 분석

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 MAC 값과 키의 값이 전송되므로 전송 데이타 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 연산 처리량이 많다. 또한, 경로요구와 경로응답 패킷에 경로에 관한 정보를 포함하고 있지 않으므로 각 홉에서 경로 테이블을 관리해야 하는 부하가 있다. Youngho 프로토콜은 경로응답 시에만 공개키 방식을 이용하여 암호화가 이루어지므로 ARAN이나 SAODV 프로토콜보다는 연산이 줄어드나 대칭키 암호화 방식을 이용하는 것 보다는 연상량이 많다.

4. 제안한 프로토콜

본 논문에서는 서버의 검증자, EOR 및 해쉬함수를 이용하여 각 노드의 비밀 키를 시작노드에 안전하게 전달하며 경로응답 시 경로의 각 홉에서 대칭키 암호화 방식으로 암호화를 하여 시작노드에서 중간경로 홉에 대한 인증을 수행하는 프로토콜을 제안한다.. 본 프로토콜은 ad hoc 네트워크에 들어오는 각 노드는 그들의 검증자를 서버에 안전하게 등록한다고 가정한다. 여기서, 노드 A의 검증자는 $v_A = H[K_A]$와 같다. 또한, Ariadne 프로토콜과 같이 경로요구 패킷에서 각 영역의 적법

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

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

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

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

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

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

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

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

$D: M = H[v_D \oplus D \oplus id] \oplus K_{DD}$

$h_4 = MAC_{K_{DD}}(REQUEST, S, D, id, ti, M, (A, B, C))$

$D \rightarrow Server: < REQUEST, S, D, id, ti, M, (A, B, C), h_4 >$

$Server: N_i = H[v_S \oplus i] \oplus H(v_i)$

$h_5 = MAC_{K_{DD}}(REPLY, D, S, ti, (N_A, N_B, N_C, N_D))$

$Server \rightarrow D: < REPLY, D, S, ti, (N_A, N_B, N_C, N_D), h_5 >$

$D: h_0' = MAC_{K_{DS}}(REPLY, D, S, t_i\ (N_A, N_B, N_C, N_D))$

$L_D = N_D \oplus H[v_D] \oplus K_D = H[v_S \oplus D] \oplus K_D$

$D \rightarrow C: < (REPLY, D, S, ti)_{K_D}, (N_A, N_B, N_C, N_D), h_0', (A, B, C), (L_D) >$

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

$L_C = N_C \oplus H[v_C] \oplus K_C = H[v_S \oplus C] \oplus K_C$

$C \rightarrow B: < ((REPLY, D, S, ti)_{K_D})_{K_C}, (N_A, N_B, N_C, N_D), h_1', (A, B, C), (L_D, L_C) >$

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

$L_B = N_B \oplus H[v_B] \oplus K_B = H[v_S \oplus B] \oplus K_B$

$B \rightarrow A: < (((REPLY, D, S, ti)_{K_D})_{K_C})_{K_B}, (N_A, N_B, N_C, N_D), h_2', (A, B, C), (L_D, L_C, L_B) >$

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

$L_A = N_A \oplus H[v_A] \oplus K_A = H[v_S \oplus A] \oplus K_A$

$A \rightarrow S: < ((((REPLY, D, S, ti)_{K_D})_{K_C})_{K_B})_{K_A}, (N_A, N_B, N_C, N_D), h_3', (A, B, C), (L_D, L_C, L_B, L_A) >$

<그림 5> 제안한 경로발견 프로토콜

성을 확인하기 위하여 시작노드는 비밀키 K_{SD}로 패킷 데이터의 MAC를 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 서로 다른 노드의 TESLA 일방향 키 체인의 인증키를 안다고 가정한다.

그림 5는 해쉬함수와 EOR 연산만을 이용하여 경로상의 홉과 패킷을 인증하는 제안한 경로발견 프로토콜이다. 경로요구는 목적노드 D까지의 과정은 2장에서 기술한 Youngho 프로토콜과 동일하다. 목적노드 D는 경로요구 패킷을 수신하면 해쉬체인 값을 검사함으로써 경로요구 패킷의 타당성을 검사한다. 만약, 타당하다면 목적노드 D는 서버와의통신에서 패킷인증에 사용될 키 K_{DD}를 발생하고 메시지 M을 계산하여 패킷에 첨부한다. 해쉬 값 h_4와 h_5는 목적노드와 서버간의 패킷 인증을 위한 값이다. 서버는 수신한 패킷의 타당성을

검사한다. 만약 타당하다면 서버는 노드목록에 있는 노드와 목적노드의 N_A, N_B, N_C, N_D 값들을 계산하여 목적노드에게 전송한다. 이때 N_i 값들은 각 노드들의 검증자 값을 이용하여 $N_i = H[v_s \oplus i] \oplus H[v_i]$와 같이 계산되며 경로 응답시 각 노드에서 사용할 암호화키를 시작노드에게 안전하게 전송하기 위하여 사용된다.

목적노드가 서버로부터 패킷을 수신하면 해쉬값 h_5을 검사함으로써 패킷의 타당성을 검사한다, 만약, 타당하다면 목적노드는 시작노드로 경로응답 패킷을 전송한다. 경로응답 패킷은 경로요구시 설정된 경로로 전송된다. 목적노드 D는 암호화에 사용할 키 K_D를 발생하고 $(REPLY,\ D,\ S,\ t_i)$ 값을 K_D로 암호화한 $(REPLY,\ D,\ S,\ t_i)_{K_D}$ 를 계산하고 경로요구와 같이 해쉬함수 값 $h_0^{'}$를 첨부한다. 또한, 서버로부터 수신한 N_D에 각 노드의 검증자를 해쉬한 $H[v_D]$ 값과 K_D를 EOR 하여 L_D를 생성하여 경로응답 패킷에 첨부한다. 이 L_D는 시작노드에서 노드 D에서 사용한 키 값 K_D를 계산하는데 사용된다.

경로상의 노드 C가 경로응답 패킷을 수신하면 암호화에 사용할 키 K_C를 발생하고 수신된 $(REPLY, D, S, t_i)_{K_D}$ 값을 K_C로 암호화한 $((REPLY, D, S, t_i)_{K_D})_{K_C}$를 계산하고 경로요구와 같이 해쉬 체인 값을 첨부한다. 또한, L_C를 생성하여 경로응답 패킷에 첨부한다. 시작노드가 경로응답 패킷을 수신하면 경로상의 각 노드의 키 K_i는 수신한 L_i에 $H[v_s \oplus i]$를 EOR하여 구하며 이 키 값들을 이용하여 $(REPLY, D, S, t_i)$ 값을 구한 후 시간 t_i가 허용된 시간 내에 도착하였는지 검사한다. 만약 허용된 시간 내에 경로응답 패킷이 도착하였다면 해쉬 체인 값을 검사하여 경로인증을 한다. 이때, 각 홉에서 암호화에 사용한 키 K_i는 경로설정이 이루어질 때마다 새로운 값을 발생하여 사용하며 서버에 등록한 검증자에 사용된 P_i는 i 노드의 비밀키이다.

본 프로토콜은 경로상의 노드에서 해쉬함수와 EOR, 대칭키 암호화 연산만 처리하면 되므로 DoS 공격에 강하며 홉에서 적은 부하를 요구하는 ad-hoc 네트워크에 적합한 방식이다. 또한, 본 프로토콜은 경로응답의 각 노드에서 발생한 키로 암호화하고 시작노드에서 복호화하는 과정이 있어 정당한 홉을 가장한 active 공격에 강하다.

5. 결 론

본 논문에서는 기존의 경로발견 프로토콜들을 분석하여 ad hoc 네트워크에서의 각 노드에서 연산 부하를 줄이고 안전한 경로발견 프로토콜을 제안하였다. 본 프로토콜은 서버의 검증자, EOR 및 해쉬함수를 이용하여 각 노드의 비밀 키를 시작노드에 안전하게 전달하며 경로응답 시 경로의 각 홉에서 대칭키 암호화 방식으로 암호화를 하여 시작노드에서 중간경로 홉에 대한 인증을 수행한다. ARAN 프로토콜, SAODV 프로토콜, Youngho 프로토콜 등이 암호화를 위해 공개키를 사용한 것과 달리 본 프로토콜에서는 대칭키 암호화 방식을 이용하여 각 노드에서 처리할 연산 부하가 적으므로 DoS 공격에 강하다. 또한, 경로응답 시 각 홉과 시작노드에서 암/복호화 과정이 있어 정당한 홉을 가장한 active 공격에도 강하다

참 고 문 헌

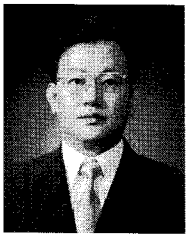
[1] 박영호, 이경근, 이상곤, 문상재,"무선 Ad Hoc 네트워크에서의 안전한 라우팅 프로토콜에 관한 연구," 정보보호학회지, Vol.15, No.3, pp.76-81, 2005년 6월

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

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

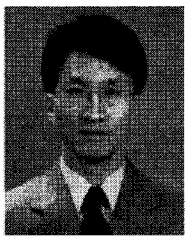
[4] S.Gupte and M.Singhal "Secure Routing in Mobile Wireless Ad Hoc Networks," Elsevier, Ad Hoc Networks, pp.151-174, 2003.

[5] S.Marti et al. "Mitigating Routing Misbehaviour in Mobil Ad Hoc Networks," MOBICOM 2000, ACM Press, pp.255-265, 2000.
[6] 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.
[7] K. Sanzgiri et al,"A Secure Routing Protocol for Ad Hoc Networks," ICNP 2002, IEEE Press, pp.78-87, 2002.
[8] M. G. Zapata and N. Asokan "Securing Ad Hoc Routing Protocols," WISE 2002, ACM Press, pp.1-10, 2002.
[9] YoungHo Park, Hwangjun Song, KyungKeun Lee, CheolSoo Kim, SangGon Lee, and SangJae Moon, "Secure Route Discovery Protocol for Ad Hoc Network," IEICE Trans. Fundamentals, Vol.E90-A, No.2, pp.539-541, February, 2007.
[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,



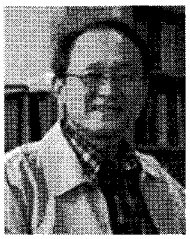
박 영 호 (Young Ho Park)

- 종신회원
- 1989년 2월 경북대학교 전자공학과(공학사)
- 1991년 2월 경북대학교 대학원 전자공학과(공학석사)
- 1995년 8월 경북대학교 대학원 전자공학과(공학박사)
- 2003년 8월 ~ 2004년 7월 Oregon State University 방문 교수
- 1996년 3월 ~ 2008년 2월 상주대학교 전자전기공학부 교수
- 2008년 3월 ~ 현재 경북대학교 이공대학 전자전기공학부 교수
- 관심분야: 네트워크 보안, 광통신 보안 등



이 상 곤 (Sang Gon Lee)

- 1996년 2월 경북대학교 전자공학과(공학사)
- 1998년 2월 경북대학교 대학원 전자공학과(공학석사)
- 2003년 2월 경북대학교 대학원 전자공학과(공학박사)
- 2003년 8월 - 2004년 7월 호주 QUT ISRC(암호학연구소) 방문 교수
- 1991년 3월 ~ 1997년 2월 창신대학 전자통신과 조교수
- 1997년 3월 ~ 현재 동서대학교 컴퓨터정보공학부 교수
- 관심분야: 네트워크 보안, 보안 프로그래밍 등



문 상 재 (Sang Jae Moon)

- 1972년 2월 서울대학교 공과대학(공학사-전자공학)
- 1974년 2월 서울대학교 대학원(공학석사-전자공학)
- 1984년 6월 미국 U.C.L.A. (공학박사-통신공학)
- 1984년 7월 ~ 1985월 6월 미국 OMNET 회사 컨설턴트
- 1984년 7월 ~ 1985년 6월 미국 U.C.L.A 포스트닥터
- 2001년 2월 ~ 2002년 2월 한국정보보호학회 회장
- 1974년 12월 ~ 현재 경북대학교 전자전기컴퓨터학부 교수
- 관심분야: 네트워크 보안, 암호학 등