익명성을 지원하는 효율적인 MANET On-Demand 라우팅 프로토콜†

이승윤, 오희국
한양대학교 컴퓨터공학과
e-mail: sylee@infosec.hanyang.ac.kr, hkoh@hanyang.ac.kr

Efficient Anonymous On-Demand Routing Protocol in MANET

Sung-Yun Lee, Hee-Kuck Oh
Dept of Computer Science and Engineering, Han-Yang University

요 약

모바일 에드혹 네트워크(MANET)에서 익명 라우팅을 위해 각 노드가 익명ID를 이용하여 MAC 단에서 익명으로 서로를 인증하고 네트워크 단에서 익명 라우팅 수행하는 AODV 기반의 라우팅 기법이 제안된바 있다[4]. 하지만 기존의 제안된 방법은 익명ID가 변경될 때마다 페어링 연산을 통해 재인증을 해야 하며, 라우팅 경로 중간의 노드들은 메시지의 연결성을 없에게 위해 매홉마다 암·복호화를 반복하여 상당히 비효율적이다. 본 논문은 기존논문의 노드 인증 기법을 확장하여 실제 메시지의 교환 과정에서 일어나는 홉 간 암호화 횟수를 줄이고, 임시 인증값을 이용한 노드 상호간의 빠른 인증 기법을 사용하여 노드간의 인증과 익명성을 보장하는 보다 효율적인 프로토콜을 제안한다.

1. 서론

MANET은 노드의 이동성으로 인해 네트워크의 구조가 실시간으로 변하고 그에 따라 라우팅 정보도 함께 변하는 특성이 있다. 특정 노드와의 통신을 원하는 소스노드는 라우팅 정보를 주기적으로 갱신하여 최신의 라우팅 정보를 유지(proactive, table-driven)하거나, 통신이 필요한 시점에서 라우팅 경로를 설정(reactive, on-demand)하여 원하는 목적노드와 통신을 할 수 있다. 테이블 기반의 대표적 라우팅 프로토콜은 DSDV[1]가 있으며, 요구 기반의 대표적 라우팅 프로토콜은 DSR[2]이 있다. AODV[3] 프로토콜은 테이블 기반 방식의 라우팅 기법을 요구기반의 방식에 적용할 수 있도록 고안된 프로토콜이며 실제로 라우팅이 필요할 때 경로를 설정하지만 테이블 기반 방식과 비슷한 라우팅 테이블을 가지고 있다.

네트워크 통신의 프라이버시에 대한 관심이 높아 감에 따라 MANET을 이용함에 있어서도 안전성뿐만 아니라 익명성에 대한 요구가 나타나게 되었고 이에 관련된 여러 연구[4][5][6]가 있어 왔다. 본 논문은 기존에 발표된 AODV 방식의 익명 라우팅 프로토콜[4]을 기반으로 한 익명성을 제공하는 보다 효율적인 요구기반 방식의 라우팅 프로토콜을 제안한다. 본 논문은 기존의 방법보다 빠르게 인증하고, 경로를 설정함에 있어서도 RREP(Route Reply)패킷의 암 복호화 회수를 반으로 줄임으로서 보다 효율적인 익명성 제공 라우팅 프로토콜을 제안한다.

† 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성·지원사업의 연구결과로 수행되었음.

2. 관련연구

2.1. MANET 익명성 기준

본 논문에서는 제공하는 익명성의 요소를 아래와 같이 정의한다[6].

- Identity privacy
  - 소스 노드와 목적 노드의 실제 ID를 경로상의 중간 노드들은 알 수 없고 반대의 경우도 마찬가지이다.
- Location privacy
  - 네트워크상의 어떤 노드도 소스 노드와 목적 노드의 정확한 위치를 알 수 없다(Weak Location Privacy).
  - 경로상의 중간 노드들은 소스 노드나 목적 노드까지의 거리(i.e. 홉 수)에 대한 어떤 정보도 알 수 없다.
- Route Anonymity
  - 경로상의 또는 경로 밖의 악의적 노드가 소스노드 또는 목적지 노드로 가는 패킷을 트레이스 할 수 없다(메시지의 연결 불가능성).
  - 경로 밖의 악의적 노드는 경로의 어떤 부분의 정보도 알 수 없고 소스 노드와 목적지 노드의 전송 패턴이나 행동 패턴을 추측 할 수 없다.

2.2. 페어링 기법

본 논문에서는 페어링기반의 암호화 방법을 사용한다. G_1을 소수인 위수 q를 갖는 덧셈 순환군 이라 하고, G_2를

동일한 위수 q를 갖는 곱셈 순환 군이라 할 때 *bilinear map* $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 이라 하면 $P, Q \in G_1$에 대해 다음과 같이 $\hat{e}(aP,bQ) = \hat{e}(P,bQ)^a = \hat{e}(aP,Q)^b = \hat{e}(P,Q)^{ab} = \hat{e}(abP,Q) = \hat{e}(P,abQ)$를 만족한다. 또한 G_1의 원소 P, aP, bP, cP가 주어졌을 때, $\hat{e}(P,P)^{abc}$를 계산하는 문제를 Bilinear Diffie-Hellman Problem(BDHP)라 하며 이것은 다항식 시간 내에 계산하는 것이 어렵다고 알려져 있다 [4].

2.3. 기존 프로토콜의 문제점

익명성을 제공하는 기존AODV 기반 MANET프로토콜은 공개키로 암호화된 트랩도어를 사용[7]하여 연산량이 많고 비효율적이며 메시지의 연결 불가능성 또한 고려하지 않은 경우가 있다. 익명ID를 사용하는 프로토콜[4]의 경우 새로운 익명ID를 사용할 때마다 페어링 연산을 해야 하며, 경로 중간의 노드들은 메시지의 연결성을 없애기 위해 매홉마다 암·복호화를 반복하여 상당히 비효율적이다. 그리고 *RREQ*패킷에서 목적지 노드의 실제ID를 숨기지 않음으로 인해 드러나는 목적지 노드의 위치를 숨기기 위해 *RREQ*플루딩의 제한을 두지 않음으로 모든 노드가 한 번씩 플루딩을 하게 된다.

3. 제안하는 프로토콜

제안하는 프로토콜은 MAC-layer에서의 노드간의 인증과 Network-layer에서의 익명 라우팅 프로토콜로 나누어진다. 본 논문에서 사용되는 표기법은 아래의 <표 1>과 같다.

<표 1> 표기법

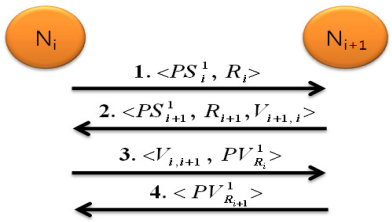
N_i	노드 $i(0 \le i \le n)$ N_0:소스노드, N_n:목적지노드
ID_n	N_n(목적지 노드) ID
PS_i^n	N_i의 n번째 익명 ID
$x(\in Z_q^*)$	그룹 마스터 키
R_i	N_i가 생성한 난수
H_1	임의의 입력을 G_1의 원소로 매핑하는 해시함수
H_2	일반적인 해시함수
prof	인증되었음을 알리는 노드의 증명값
$K_{R_i}^n$	N_i가 n번째 세션에서 생성한 세션 마스터키 Seed
seq_n	목적지 노드의 Seq#
$LinkID_{prev}$	경로상의 이전 노드의 링크ID
▬	경로상의 다음 노드의 링크ID
Hoplimit	소스노드에 의해 생성되는 랜덤한 Hop limit 값

네트워크 초기에 각 노드는 신뢰기관(TA: Trusted Authority)으로부터 아래의 <표 2>와 같은 초기 값들을 지급 받는다.

<표 2> 각 노드가 TA로부터 지급받는 초기 값

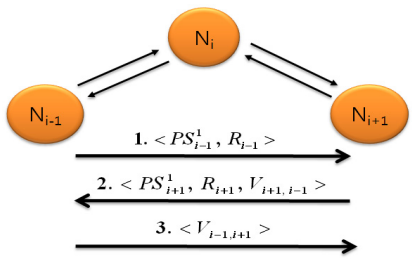
3.1. MAC-layer의 익명 인증 프로토콜

네트워크에 참여한 각 노드들은 아래와 같은 방법으로 초기 인증을 수행한다.



- $V_{i+1,i} = H_2(R_{i+1} \| R_i \| \mathbf{0} \| K_{i+1,i})$
- $V_{i,i+1} = H_2(R_i \| R_{i+1} \| \mathbf{1} \| K_{i,i+1})$
- $K_{i,i+1} = \hat{e}(H_1(PS_i^1), H_1(PS_{i+1}^1))^x$
  $= \hat{e}(H_1(PS_{i+1}^1), H_1(PS_i^1))^x = K_{i+1,i}$
- $PV_{R_i}^1 = \{prof, K_{R_i}^1\}_{K_m}$

(그림 1) 네트워크 초기의 한 홉 인증



(그림 2) 네트워크 초기의 두 홉 인증

각 노드는 (그림 1)에서 *PS*값을 이용해 인증을 시도하고 *V*값을 검증함으로써 익명으로 인증하게 되며 인증시에 생성한 $K_{i,i+1}(=K_{i+1,i})$를 이용하여 링크 ID(L)와 홉간 암호화에 사용되는 세션키($Skey$)를 아래와 같이 확립한다.

$$\begin{cases} Skey_{i,i+1}^{\gamma} = H_2(R_i \| R_{i+1} \| 2^* \gamma \| K_{i,i+1}) \\ L_{i,i+1}^{\gamma} : \ H_2(R_i \| R_{i+1} \| 2^* \gamma + 1 \| K_{i,i+1}) \end{cases}$$

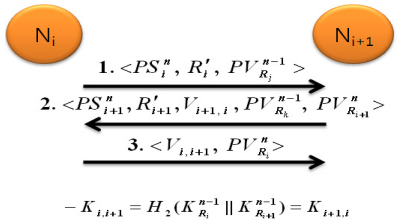
인증을 마치면 각 노드는 두 홉 거리 안에 있는 각 노드들과 $(L, Skey)$쌍을 확립하게 되며 이를 이용하여 익명 통신을 하게 된다. (그림 2)와 같은 두 홉 인증시에 N_i는 N_{i-1}과 N_{i+1}의 인증 메시지를 중계하면서 중계되는 정보를 이용하여 N_{i-1}과 N_{i+1} 사이에서 생성되는 링크ID를 얻게 된다. 그러므로 각 노드가 가지는 정보는 아래의

<표 3>과 같다.

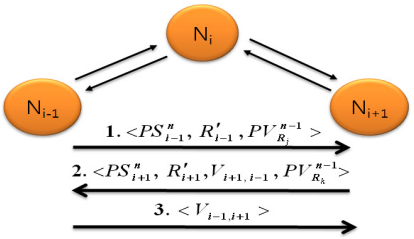
<표 3> 인증 완료 후 노드(N_i)가 가지는 정보

	$N_i \Leftrightarrow N_{i+1}$	$N_i \Leftrightarrow N_{i+2}$	$N_{i-1} \Leftrightarrow N_{i+1}$
Master Key	$K_{i,i+1}$	$K_{i,i+2}$	$K_{i-1,i+1}$
LinkID	$L^{\gamma}_{i,i+1}$	$L^{\gamma}_{i,i+2}$	$L^{\gamma}_{i-1,i+1}$
Session Key	$Skey^{\gamma}_{i,i+1}$	$Skey^{\gamma}_{i,i+2}$	

모바일 환경에서 노드가 이동하여 다시 인증해야 할 경우 초기 인증에서 획득한 PV값을 이용해 효율적으로 인증이 가능하다. 재인증 기법은 아래의 (그림 3)과 같다.



(그림 3) 한 홉 재인증



(그림 4) 두 홉 재인증

재인증시에 (그림 3)의 노드 N_{i+1}은 N_i로부터 받은 $PV_{R_j}^{n-1}$값을 K_m을 이용하여 복호화 하고 자신의 PV값을 이용하여 페어링 연산 없이 해당 세션의 마스터키를 생성하고 인증값을 생성한다. 각 노드는 V값을 이용해 서로를 인증하고 초기 인증과 같은 방식으로 링크ID와 세션키를 확립한다.

3.2. Network-layer의 익명 라우팅 프로토콜

MAC-layer에서 익명인증을 마친 각 노드는 확립한 링크ID와 세션키를 이용하여 Network-layer에서 효율적인 익명 라우팅을 수행한다. 각 노드는 아래와 같은 세 개의 테이블을 유지하며 라우팅 경로를 설정한다.

- Reverse Route Table
  - 엔트리는 $< ID_n, seq_n, PS_{i-2}, PS_{i-1} >$으로 구성됨.
- Forward Route Table
  - 엔트리는 $< ID_n, seq_n, LinkID_{prev},$ [illegible] $>$으로 구성됨.
- Target LinkID Table
  - 엔트리는 $< LinkID_n >$으로 구성됨.

소스노드(N_0)에 의해 만들어지고 전송되는 $RREQ$ 패킷은 $< RREQ, RREQseq, Hoplimit, ID_n, seq_n, PS_{i-1}, PS_i >$으로 구성된다. $RREQseq$값은 해당 $RREQ$패킷 최신성을 검증하는 값이며 seq_n값은 목적노드로의 경로 최신성을 검증하는 값이다. $RREQ$패킷은 플루딩되며 패킷을 받은 경로상의 중간 노드는 $Hoplimit = Hoplimit - 1$로 업데이트 하면서 플루딩을 진행하며 $Hoplimit \leq 0$이 되면 메시지는 무시되고 플루딩을 중지한다. 메시지를 받은 중간노드는 Reverse Route entry를 생성하여 테이블에 기록한다. 각 노드가 유지하는 테이블의 엔트리는 설정된 타이머에 의해 일정시간 동안만 유지된다.

$RREQ$를 받은 목적노드는 $RREP$메시지를 생성하며 패킷은 $< L^{\gamma(i)}_{n,n-1(\text{or } n-2)}, \{RREP, ID_n, seq_n\}_{Skey^{\gamma(i)}_{n,n-1(\text{or } n-2)}} >$로 구성된다. 목적노드는 $RREP$패킷을 전송하며 패킷의 구성에서 보인바와 같이 한 홉 또는 두 홉 이전의 노드를 목적지로 하여 메시지를 보낼 수 있으므로 자신의 Target LinkID 테이블에 $L^{\gamma(i+1)}_{n,n-1(\text{or } n-2)}$를 기록한다. $RREQ$ 메시지를 받은 경로상의 중간 노드는 자신이 가지고 있는 링크ID를 확인하여 자신의 이전 노드에게 가는 메시지이면 그대로 메시지를 패싱하고 자신에게 온 메시지이면 메시지를 복호화하여 Forward Route 테이블을 작성한다. 테이블의 링크ID는 현재 패킷에 사용할 것 다음의 링크ID를 기록하며 현재 사용할 $(L, Skey)$를 이용해 $RREP$메시지를 재 암호화 하고 링크ID를 붙여 전송한다. 중간노드도 목적지 노드와 같이 한 홉 또는 두 홉 이전의 노드를 목적지로 하여 메시지를 보낼 수 있다. 최종적으로 소스노드에 $RREP$메시지가 도달하면 경로가 완성된다. 경로설정 과정은 (그림 5)에 자세히 나타나 있다.

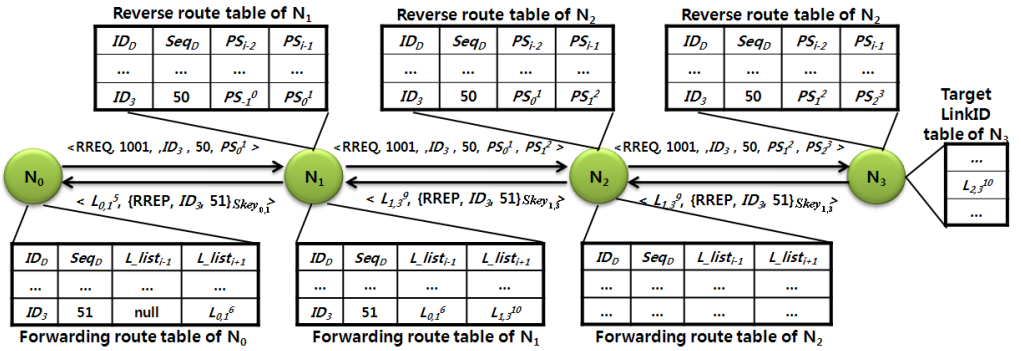
경로의 설정이 완료되면 데이터 패킷은 설정된 경로에 따라 $< L^{\gamma(i+1)}_{i,i+1(\text{or } n+2)}, DATA >$와 같은 형식으로 전송된다.

4. 분석

4.1. 익명성 분석

본 프로토콜은 익명 ID를 이용하므로 실제ID가 드러나지 않는다. 그러므로 Identity privacy를 만족한다. $RREQ$ 패킷에서 목적지의 실제 아이디가 사용되나 $RREQ$메시지는 랜덤 $Hoplimit$만큼 플루딩 되므로 실질적으로 얻을 수 있는 정보는 없다.

패킷의 주소는 링크ID로 대체되므로 인증된 노드 외에는 링크ID를 식별할 수 없다. 메시지의 연결성에 있어서도 홉 간에 전송되는 $RREP$메시지가 항상 달라 패킷을 트레이스 하는 것이 불가능하므로 Route Anonymity를 만족한다. 프로토콜에서 최대 두 홉 까지 메시지를 보낼 수 있으므로 두 홉 간의 $RREP$메시지는 연결될 수 있으나 전체 라우팅 경로의 측면에서 생각할 때 실질적으로 어떤 정보도 주지 못한다.



(그림 5) Network-layer 에서의 route discovery

메시지의 연결가능성과 더불어 패킷에는 소스 또는 목적지 노드의 거리에 관련된 정보는 포함되지 않으므로 노드 사이에서 전송되는 패킷을 통해 거리에 관련된 어떤 정보도 얻을 수 없으므로 Location privacy를 만족한다.

4.2. 안전성 분석

MAC-layer인증 부분에서 각 노드는 그룹 마스터키에 의해 만들어진 *SP*값을 이용한 페어링 기법으로 세션 마스터키를 생성하고 인증한다. BDHP문제는 어렵다고 가정하였으므로 이것은 안전하다. 세션키는 패킷전송 1회당 한 번만 사용되므로 한 세션에 하나의 키를 사용하는 것보다 안전성이 높다.

4.3. 효율성 분석

기존의 프로토콜은 새로운 *PS*값을 사용하기 위해 매번 페어링 연산을 통해 인증을 해야 했으나 제안하는 방법은 대칭키 연산과 해쉬를 이용해 효율적으로 인증한다. 또한 두 홉 인증을 통해 *RREP*메시지가 두 홉에 한 번씩 복호화 되고 암호화 될 수 있으므로 암 복호화 과정을 최대 50% 까지 줄일 수 있다. 그리고 적절한 *Hoplimit*값을 도입하여 소스와 목적지 노드의 위치를 찾을 수 있는 확률은 높아졌지만 정확한 위치는 찾을 수 없고 MANET환경의 특성상 네트워크 토폴로지 또한 계속 변화하므로 실질적으로 공격 노드에게 유용한 정보를 주지는 못한다. 반면에 네트워크 전체적으로 볼 때 전송되는 메시지의 양은 네트워크 전체 플루딩에 비해 상당히 줄일 수 있다.

5. 결론

MANET 라우팅에서의 익명성 제공은 사용자의 프라이버시 보호의 측면에서 중요한 문제이다. 본 논문은 MANET환경에서의 보다 효율적으로 익명성을 제공하는 라우팅 기법에 대해 제안 하였다. MAC-layer에서의 효율적인 재인증 기법을 제시하였고, 두 홉 인증을 통해 인증거리를 넓힘으로서 경로설정과정에서 암·복호화 횟수를 줄이는 방법을 제안하였다. 본 논문은 제시된 기준에 의한 익명성 요구 조건을 만족시키며, 보다 효율적인 라우팅 경로 설정이 가능하다.

참고문헌

[1] C. E. Perkins, and P. Bhagwat. “DSDV: Routing over a Multihop Wireless Network of Mobile Computer” In C. Perkins, editor, Ad Hoc Networking, chapter 3, pp. 53-74. Addison-Wesley, 2001.

[2] D. Johnson, D. Maltz, and J. Broch “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks” In C. Perkins, editor, Ad Hoc Networking, chapter 5, pp. 139-172. Addison-Wesley, 2001.

[3] C. E. Perkins, and E. M. Royer “The Ad Hoc On-Demand Distance-Vector Protocol” In C. Perkins, editor, Ad Hoc Networking, chapter 6, pp. 173-219. Addison-Wesley, 2001.

[4] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang “MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks” IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, Vol. 5, No. 9, September 2006.

[5] Rongxing Lu, Zhenfu Cao, Licheng Wang, and Congkai Sun “A secure anonymous routing protocol with authenticated key exchange for ad hoc networks” Computer Standards & Interfaces, Vol. 29, No. 5, July 2007.

[6] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, and Robert H. Deng "Anonymous Secure Routing in Mobile Ad-Hoc Networks" 29th Annual IEEE International Conference on Local Computer Networks, 2004.

[7] Reza Shokri, Maysam Yabandeh, and Nasser Yazdani "Anonymous Routing in MANET using Random Identifiers" Sixth International Conference on Networking, 2007.