애드혹 네트워크에서의 간소화된 익명성 DSR 기법

공춘엄, 추현승*
성균관대학교 전자전기컴퓨터학과
e-mail : cukong@ece.skku.ac.kr

Simplified ANonymous Dynamic Source Routing Scheme for Ad-hoc Networks (SANDSR)

Chun-Um Kong, Hyunseung Choo*
School of Information and Communication Engineering, Sungkyunkwan University

요 약

적대적이고 급변하는 애드혹 네트워크에서 각 노드들은 항상 적대적인 공격자들로부터 위조나 변조의 공격을 받을 수 있어서 통신 내용과 경로의 보안성이 필요하다. AnonDSR 기법은 보안성을 유지하면서 익명성을 효율적으로 보장하는 것으로 알려져 있지만 기존 기법에 비해 암호키를 설립하는 추가적인 절차를 수행하므로 통신 수행시간이 길어지는 문제가 발생한다. 제안 기법에서는 암호키 설립 단계와 통신경로를 설정하는 단계를 동시 수행하고 데이터 전송시에는 공유키로 암호화를 추가적으로 수행해서 보안 강도를 높인다. 결과적으로 제안기법은 AnonDSR 에 비해 매번 통신 수행시간이 최대 31% 향상되고 보안성도 강화된다.

1. 서론

전장과 같이 적대적이고 동적으로 급변하는 애드혹 네트워크에서 각 노드들은 항상 이동이 가능하므로 적대적인 공격자들로부터 위조나 변조의 공격을 받을 수 있고 도청도 당할 수도 있다. 그래서 애드혹 네트워크에서는 보안의 중요성이 강조되고 있다.

모바일 애드혹 네트워크의 대표적인 익명성 보안 라우팅 기법에는 AnonDSR[4]이 있다. 이 기법은 암호화에 대칭키와 공개키를 혼합해서 사용하고 키 설립, 익명성 경로보장, 익명성 데이터전송 프로토콜로 구성된다. 하지만 이 기법은 다른 기법들이 통신 경로 설정과 데이터 전송 프로토콜만을 수행하는 것과는 다르게 키 설립 프로토콜이라는 추가적인 절차를 수행하므로 통신 수행시간이 타 기법들보다 길어진다.

제안 기법은 키 설립 프로토콜의 핵심인 출발지와 목적지 노드들이 대칭키를 공유하는 절차를 익명성 경로보장 프로토콜에서 통합하여 동시에 수행한다. 그리고 익명성 데이터 전송시에는 공유하는 대칭키로 암호화를 추가적으로 수행하므로 보안 강도를 높인다. 그러면 AnonDSR 에 비해 통신 수행시간 측면에서 최대 31%의 성능이 향상되고 보안성도 강화된다.

이후 본 논문의 2 장에서 기본 용어를 알아보고 3 장에서는 제안 기법을 설명한다. 4 장에서는 성능평가를 보여주고 5 장에서 결론을 내린다.

2. 용어 및 표기법

사용되는 용어 및 표기법은 표 1 과 같다.

<표 1> 용어 및 표기법

표기	의미	표기	의미
ID_A	노드 A 의 식별자	K_X	임의의 대칭키
N_X	임의의 익명성(nonce) 값	K_A	노드 A 의 대칭키
N_A	노드 A 와 연관되는 익명성(nonce) 값	H()	단방향 해쉬 함수
PK_{temp}	일시적인 공개키	PK_A	노드 A 의 공개키
SK_A	노드 A 의 개인키	P	패딩
PL	패딩 길이	$Sign_A$	노드 A 의 서명
$E_K(M)$	대칭키 K 로 암호화된 메시지 M	$E_{PK}(M)$	공개키 PK 로 암호화된 메시지 M

익명성 값은 노드를 식별하는데 ID 를 사용하는 대신에 유일한 난수 값을 생성해서 익명성을 보장한다. 트랩도어는 출발지에서 암호화한 메시지를 목적지에서만 복호화해서 확인할 수 있게 하는 기법이다. 암호화 기법인 오니언은 노드에서 소유하고 있는 비밀키로 중첩해서 암호화한다.

3. 제안 기법

3.1 익명성 경로 보장 프로토콜

익명성 통신을 위해 출발지와 목적지 노드가 중간 노드들의 ID 대신 익명성 값(N_X)과 대칭키(K_X)를 확보한다.

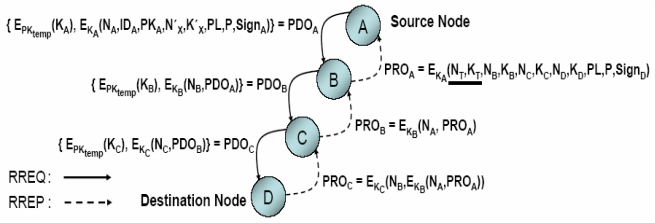
RREQ 단계에서는 메시지를 브로드캐스트하고 트랩도어 기법을 사용한다.

<ANON-RREQ, PK_{temp}, tr_{dest}, onion>

ANON-RREQ 는 익명성 통신을 원하는 RREQ 메시지이다. tr_{dest} 는 트랩도어 기법으로 목적지 노드만이 복호화할 수 있게 목적지 노드의 공개키로 암호화한다. 예를 들어, $tr_{dest} = E_{PKdest}(N_T,K_T,ID_{dest},SK_{temp})$라면 목적지

* Corresponding Author

노드의 공개키(PK_{dest})로 암호화되어 개인키(SK_{dest})를 가지고 있는 목적지 노드만이 복호화할 수 있다. 그 결과, 공유할 익명성 값(N_T)과 대칭키(K_T) 그리고 실제 목적지의 주소(ID_{dest})를 확인할 수 있다. 그림 1 은 메시지 암 · 복호화 과정(PDO, PRO) 을 나타낸다.



(그림 1) PDO 와 PRO

RREP 단계에서는 RREQ 과정을 통해 목적지 노드가 알게 된 전체 경로의 익명성 값과 대칭키들을 출발지 노드도 가질 수 있게 암호화해서 전송한다.

<ANON-RREP, N_{next}, PRO>

ANON-RREP 는 익명성 통신을 원하는 RREP 메시지이다. N_{next} 는 다음 익명성 값을 의미하므로 노드를 이동할 때마다 갱신된다. PRO 는 PDO 의 역순으로 형성된다. 익명성 값으로 경로상의 노드를 찾은 후에 그 노드의 대칭키로 PRO 를 복호화한다. 출발지 노드(A)에 도착하면 경로상의 모든 익명성 값과 대칭키를 목적지 노드와 공유하게 된다.

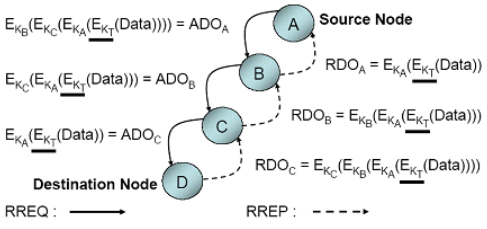
3.2 익명성 데이터 전송 프로토콜

출발지와 목적지 노드는 이미 전체 경로의 대칭키와 익명성 값을 모두 소유하고 있어서 각 노드의 대칭키를 이용해 오니언 방식으로 암호화한다.

<ANON-DATA, N_{src}, onion>

ANON-DATA 는 데이터 전송을 알리는 메시지이다. N_{src} 는 처음에 시작하는 노드의 익명성 값을 나타내고 경로상의 노드에 도착할 때마다 다음 노드의 익명성 값으로 교체된다. 경로 암호화 포맷인 onion 은 출발지와 목적지 노드는 전체 경로상의 대칭키와 공유하는 대칭키를 가지므로 오니언 방식으로 데이터를 암호화한다.

ADO_A 는 출발지 노드(A)에서 데이터를 암호화하는데 이미 전체 라우팅 경로를 알고 있으므로 중간노드의 순서대로 그들의 대칭키를 이용해서 암호화한다. 그리고 마지막에 복호화되는 대칭키는 출발지 노드의 대칭키(K_A)와 출발지와 목적지 노드만이 공유하는 대칭키(K_T)를 동시에 사용해서 보안성을 강화한다. RDO 도 ADO 와 동일한 과정으로 데이터의 암호화를 수행하는데 중간노드의 순서가 역순이 되는 것만 다르다. 오니언 방식인 ADO 와 RDO 는 그림 2 와 같다.

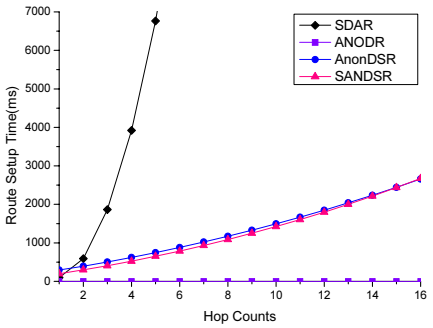


(그림 2) ADO 와 RDO

4. 성능평가

Pentium 4 2.60GHz, 768MB RAM 의 컴퓨터 환경에서 모의 실험을 수행한다. 네트워크 환경은 전체 노드 수는 500 개이고 하나의 노드에 이웃하는 노드의 수는 4 개이다.

공개키의 암· 복호화 시간은 대칭키의 암· 복호화 시간보다 오래 걸리고 공개키는 암호화보다 복호화에 더 긴 시간이 소요된다. 그리고 제안 기법이 AnonDSR 에 비해 통신 수행시간 면에서 최대 31%의 성능이 향상되고 출발지와 목적지 노드간의 홉 수가 가까울수록 더 좋은 효율성을 나타난다.



(그림 3) 익명성 라우팅 기법들의 통신수행시간 비교

5. 결론

본 논문에서 제안한 기법은 3 단계 프로토콜로 구성된 AnonDSR 을 2 단계 프로토콜로 축소시키고 익명성 데이터 전송시에는 공유하는 대칭키로 오니언 방식의 암호화를 추가적으로 수행하므로 보안 강도를 높인다. 그 결과, AnonDSR 에 비해 매번 통신 수행시간이 최대 31%줄어들고 데이터 전송시의 보안성도 강화된다.

Acknowledgment

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. IITA-2006-(C1090-0603-0046) . 교신저자: 추현승.

참고문헌

[1] F. Kargl, A. Geis, S. Schlott, and M. Weber, "Secure Dynamic Source Routing," HICSS, 2005.

[2] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks," MobiHoc, 2003.

[3] A. Boukerche, K. El-Khatib, L. Korba, and L. Xu. "A Secure Distributed Anonymous Routing Protocol for Ad Hoc Wireless Networks," Journal of Computer Communications, 2004.

[4] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," SASN, 2005.