ID 기반 암호시스템을 이용한 이동적응망에서의 안전한 라우팅 프로토콜

이윤호°,김희열,정병천,이재원,윤현수

한국과학기술원 전산학전공

{yhlee°, hykim,bcchung,jaewon,hyoon}@camars.kaist.ac.kr

Secure Routing Protocol for Ad hoc Networks using ID Based Cryptosystem

Youn-ho Lee° ,Heeyoul Kim, Byung-Chun Chung, Jaewon Lee,Hyunsoo Yoon

CS Division, KAIST.

요 약

이동적응망에서의 안전하고 신뢰성있는 통신을 위하여 안전한 라우팅 프로토콜은 필수적이다. 본 논문에서는 안전한 라우팅 프로토콜을 제안한다. 제안 프로토콜은 기존의 프로토콜과는 달리 ID 기반 암호시스템을 사용하여 전체 경로길이에 관계없이 상수개의 암호학적 인자로서 경로상의 모든 단말의 인증이 가능하며, 이에 따라 경로 발견 과정시 소모되는 네트워크 자원의 양이 이전보다 감소하게 되는 장점이 있다.

1. 서 론

이동적응망의 효율성을 위해서 이동적응망에 적합한 라우팅 프로토콜은 필수적이다. 이동적응망에 대한 라우팅 프로토콜에 대해서는 많은 연구가 있었다. 이후 제안된 프로토콜에 대한 많은 최적화 방법이 제안되어 많은 라우팅 성능의 향상이 있었다. 그러나 현재까지의 이동적응망에 적합한 라우팅 프로토콜에 대한 연구는 라우팅의 효율성에 중점을 둔 방식에 많이 치우쳐져 있었다. 특히 이동적응망의 특성상, 군사적인 용도로 사용될 수 있으며 또한 최근에는 사람이 접근하기 어려운 상황에서 사용되는 무인기기간의 통신에도 사용될 수 있다. 따라서 이러한 상황에서의 라우팅 프로토콜은 보안성과 신뢰성을 갖추어야 한다.

ID 기반 암호시스템은 1984년 Shamir가 개념을 제안하였다[1]. ID 기반 암호시스템은 기존의 공개키 기반 구조와는 달리 초기화 설정 이후로는 고정된 기반 구조가 필요없는 장점이 있다.

본 논문에서는 이러한 ID 기반 암호시스템을 이용하여 안전한 라우팅 프로토콜을 제안한다. 기존의 프로토콜과는 달리 제안 프로토콜은 암호학적으로 사용되는 인자의 수를 경로의 길이와 관계없이 상수개로 줄여 네트워크 자원을 절약할 수 있다. 뿐만 아니라, 각 단말의 시간이 동기화되어야 하는 가정이 없으면서도 동시에 라우팅 경로에 있는 모든 단말의 인증이 가능하다. 또한 공개키 암호시스템을 사용하면서도 고정된 공개키 기반 구조가 필요 없으며 동시에 공개키 기반 구조를 사용함으로써 발생하는 부가적인 네트워크 자원을 절약할 수 있으므로 이동적응망에 매우 적합한 프로토콜이라 할 수 있다. 본 논문에서 제안한 프로토콜은 DSR과 같은 주문형 라우팅 프로토콜 중에 source routing을 수행하는 라우팅 프로토콜에 응용 가능하다[2].

* 본 연구는 청단정보기술 연구센터를 통하여 과학재단의 지원을 받았고 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

2. 관련 연구

이동적응망에서의 안전한 라우팅 프로토콜에 관하여 최근 많은 연구가 있었다[3-5]. ARAN (Authenticated Routing for Ad hoc Networks[4])은 인증 서버가 필요한 공개키 기반구조를 이용하여 안전한 라우팅 프로토콜을 설계하였다. 따라서 경로 요청/응답 과정에서 모든 단말들은 라우팅 관련 작업을 수행하고 패킷을 전송할 때마다, 자신의 인증서를 부가적으로 붙여야만 하는 단점이 존재한다. 또한 경로 상의 모든 단말들을 인증할 수 없는 단점이 있다. SRP (Secure Routing Protocol [5])는 임의의 두 단말 상에 공유된 비밀키를 가정하였다. SRP 의 가장 큰 문제는 경로 요청 단말과 목적지 단말 사이에 존재하는 중간 단말들에 대한 인증 과정이 없는 것이다. Ariadne[3]은 주문형 라우팅 프로토콜에 응용할 수 있는 안전한 라우팅 프로토콜이다. 이 프로토콜은 TESLA(Timely Efficient loSs toLeration Authentication protocol) [6] 동보 메시지 인증 방법을 응용한 프로토콜로서, 이전

프로토콜과는 달리 라우팅 경로 요청시, 경로 상에 있는 모든 중간 단말들에 대한 인증이 가능한 장점이 있다. 그러나 Ariadne 은 각 단말간의 시간 동기화 및 최대 전송 지연 시간을 미리 알아야 하고, 자신을 제외한 모든 단말들에 대한 해쉬 사슬값을 공유, 갱신해야 하는 단점이 있다. 또한 프로토콜 과정에서 각 중간 단말의 MAC 값을 패킷에 부가시켜야 하는 단점이 있으며 이는 라우팅 과정에서 생기는 경로 요청 패킷의 길이를 더욱 길어지게 한다. 따라서 망 자원을 많이 소비하는 단점이 존재한다.

3. 제안 프로토콜

본 장에서는 개선된 안전한 라우팅 프로토콜을 제안한다. 개선된 프로토콜은 ID 기반 암호시스템을 사용하며 전체 시스템의 환경은 IBE 시스템의 환경을 가정한다[7]. 본 프로토콜에서 각 단말의 주소는 곧 각 단말의 ID 가 된다.

환 경

이동적응망에 참여하는 임의의 단말 i 는 다음과 같은 정보를 갖고 있다.

- IBE 시스템에서 가정한 시스템 parameter 및 일방향 해쉬 함수 $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow F_q$, $H_4 : \{0,1\}^* \rightarrow \{0,1\}^n$
- 자신의 개인키 $sn_i P$

그리고 단말 i 의 ID값인 ID_i 와 자신의 공개키 $n_i P$ 는 $n_i P = H_2(ID_i)$ 인 관계를 갖는다. 여기서 n_i 는 아무에게도 알려지지 않은 값이다.

망 상에 존재하는 공격자에 대한 가정은 다음과 같다. 공격자는 Medium Access Control 계층 이하의 공격은 수행할 수 없다. 그리고 그 이상의 계층에서 공격자는 자신이 수신 받은 패킷의 내용을 임의로 삽입, 제거, 변형시킬 수 있다고 가정한다. 마지막으로 경로 요청을 시작하는 출발지 단말과 경로 요청의 대상이 되는 목적지 단말은 신뢰할 수 있는 동작만을 수행한다고 가정한다.

3.1 경로 요청 프로토콜

망 상의 임의의 단말 S는 다음과 같은 과정으로 목적지 D에 대한 경로 정보를 얻을 수 있다. 여기서 경로 요청 패킷을 받는 경로 상의 중간단말은 1~k라 하며 경로 요청 패킷은 아래와 같은 구조를 가지고 있으며 패킷의 내용 중 W, U, V 는 암호학적 인자이다. 또한 seq 는 각 단말에서 전송하는 메시지의 sequence 번호이며 이 번호는 단말 별로 관리된다. 마지막으로 $Sign_A(M)$ 은 메시지 M을 A 단말의 개인키로 전자 서명한 값이다. 본 논문에서 가정하는 환경에서의 전자 서명 알고리즘은 다른 논문의 알고리즘을 이용한다[8].

$$< \text{RouteRequest}, SouceID, DestinationID, seq, Sign_S(M), (IntermediateID-list), W, U, V >$$
$$(M = (\text{RouteRequest} \| SouceID \| DestinationID \| seq \| W))$$

- 경로 요청 단말

1) S는 임의의 난수열 $\sigma_S \in \{0,1\}^n$ 을 생성하고, 이와 자신의 $ID_S \in \{0,1\}^n$ 값을 이용하여 $r = H_3(ID_S, \sigma_S) \in F_q$ 를 생성한다.

2) 생성된 r 및 자신의 개인키 $sn_s P$ 를 이용하여 rP 를 생성하고, 이를 이용하여 다음의 값을 생성한다.

$$\hat{e}(rP, sn_s P) = g^{rsn_s} \quad (g = \hat{e}(P,P))$$

$$(\hat{e}(sP, H_2(ID_D)))^r \oplus r = (\hat{e}(sP, n_D P))^r \oplus r = g^{rsn_s} \oplus r \quad (g = \hat{e}(P,P))$$

3) 1), 2) 에서 생성한 값을 이용하여 다음과 같은 패킷을 만들어 동보한다.

$$< \text{RouteRequest}, ID_S, ID_D, seq, Sign_S(M), (), rP, g^{rsn_S} \times \sigma_S, g^{rsn_d} \oplus r >$$

- 중간 단말

1) 경로 상에서 경로 요청 패킷을 받은 중간 단말 $i \quad (1 \le i \le k)$ 는 다음과 같은 패킷을 수신 받는다.

$$< \text{RouteRequest}, ID_S, ID_D, Sign_S(M), seq, (ID_1, ...ID_{i-1}), W, U, V >$$

2) 이후 중간 단말은 S의 전자 서명을 검증한 후, 그것이 올바르다면 수신 받은 패킷에 자신의 ID_i 를 추가한 후, U 값에 자신의 개인키 값과 rP 값을 이용하여 새로운 U 값을 만든다

$$U = U \times \hat{e}(rP, sn_i P)$$

3) 이후 생성된 패킷을 다시 동보한다. 동보하는 패킷의 내용은 다음과 같다.

$$< \text{RouteRequest}, ID_S, ID_D, seq, Sign_S(M), (ID_1, ...ID_{i-1}), ID_i, W, U, V >$$

- 목적지 단말

1) 목적지 단말 D는 다음과 같은 패킷을 수신 받는다.

$$< \text{RouteRequest}, ID_S, ID_D, seq, Sign_S(M), (ID_1, ..., ID_k), W, U, V >$$

2) 목적지 필드에 있는 값이 자신의 값과 일치하는지 확인한 후, 만약 일치한다면 자신의 개인키 $sn_D P$ 값을 이용하여 다음과 같은 연산을 수행하여 r' 값을 얻는다.

$$r' = V \oplus \hat{e}(W, sn_D P)$$

3) 이후 ID-list 항목 안에 있는 각 ID에 해당하는 공개키를 얻게 되며 그 연산 과정은 아래와 같다.

$$\{n_i P \mid n_i P = H_2(ID_i), 1 \le i \le k\}$$

4) 시스템 인자 sP 와 3)의 과정에서 얻은 공개키 및 2)에서 얻은 r' 값을 이용하여 다음과 같은 연산을 수행하여 A 값을 얻는다.

$$A = \{\hat{e}(sP, \textstyle\sum_{i=1}^{k} n_i P)\}^r$$

5) 에서 얻은 A 값을 이용 다음과 같은 연산을 수행하여 σ' 을 얻

은 후, 그 이후의 과정을 수행하여 r' 값이 아래의 계산결과와 같은 값인지 비교하는 방법으로 r'값의 유효성을 확인한다.

$$\sigma' = U \times V^{-1} \ , \ r' \stackrel{?}{=} H_3(\sigma', ID_S)$$

6) 5)의 작업이 통과될 경우, 다음과 같은 경로 응답 패킷을 생성하여 그 안에 있는 ID의 경로를 따라 전송한다. 통과되지 않을 경우 경로 요청 패킷은 제거된다.

$$< \text{RouteReply}, \text{seq}, (ID_S, ID_1, .., ID_k, ID_D), W, V \oplus \sigma', Sign_D(M) >$$

$$(M = (\text{RouteReply} \mid \text{seq} \mid ID_S \mid ID_1 \mid ... \mid ID_k \mid ID_D \mid W \mid V \oplus \sigma'), Sign_D : signature\ of\ D)$$

이후 목적지 단말에서 보낸 경로 응답 패킷을 받은 중간 단말과 경로 요청 단말은 D의 전자 서명을 이용하여 전체 메시지의 무결성을 검증한 후, 경로 요청 패킷을 처리하는 과정과 유사한 방법으로 경로 상의 전체 단말이 올바른 프로토콜을 수행했다는 것을 검증한다. 검증결과가 올바를 경우 경로를 자신의 캐쉬에 저장한다. 검증 비용은 검증 연산 한번으로 가능하며 이것은 펜티엄 1GHz에서 약 10ms 정도 소모되는 연산이다[9].

3.2 경로 유지 프로토콜

만약 임의의 두 단말 S,D 사이에서 통신을 수행하다가 이전에 있었던 특정 단말 A,B 사이의 연결이 끊어진 경우, 연결이 끊어진 것을 발견한 단말 A는 S에게 다음과 같은 라우팅 오류 패킷을 전송한다.

$$< \text{RouteError}, \text{seq}, (\text{path from A to S}), (ID_A, ID_B), Sign_A(M) >$$
$$(M = (\text{RouteError} \mid seq \mid (\text{path from A to S}) \mid ID_A \mid ID_B))$$

A 와 S상에 있는 각 중간 단말들은 이러한 A와 B사이의 연결의 끊어짐을 자신들의 라우팅 정보에 반영한다.

4. 성능 분석

제안 라우팅 프로토콜은 보안 관련 인자가 패킷 당 4개로 고정되어 있다. 만약 소수 p 의 길이를 512 bit를 사용한다면 2048bit로 고정되는 것이다. 제안 프로토콜과 같이 경로 중간 단말의 인증을 수행하는 Ariadne 프로토콜은 MAC(Message Authentication Code)의 길이를 80bit로 사용하였고, 그 외 해쉬 및 MAC에 사용되는 키 정보가 첨가되므로 이것의 길이를 각 80bit라 하면, 패킷 당 192+160*k의 보안 관련 정보가 부가된다. 따라서 경로 상의 중간 단말의 개수가 12를 넘을 경우, 제안 알고리즘이 유리하다. 그러나 현재 일반적으로 사용하는 해쉬/MAC 길이가 128bit 이상임을 감안할 경우 제안 프로토콜은 경로 상의 중간 단말의 수가 더 적을 경우에도 유리하다. 라우팅 성능 면에서 살펴보면 제안 프로토콜이 공개키 연산을 이용하여 불리하나, 그 대신 제안 프로토콜은 경로 상의 중간 단말들이 경로에 대한 캐쉬 작업이 가능한 장점이 있다.

5. 제안 프로토콜의 안전성

제안 프로토콜에서 사용한 대부분의 암호학적 기법은 이전 논문에서 제안된 프로토콜을 응용한 것이며 따라서 이러한 부분은 다른 논문에 안전성이 증명되었다[7-8]. 따라서 본 논문에서 안전성 증명을 위해 중요한 부분은 프로토콜에서 사용한 U값의 안전성에 관한 것이다. 이것은 임의의 ID의 쌍 ID_1, ID_2의 공개키의 합 $(n_1+n_2)P$에 대하여 같은 공개키 값의 합을 갖는 ID의 쌍 ID_3, ID_4를 찾을 수 없음으로써 안전성이 증명된다. 자세한 증명 부분은 논문의 지면상 생략한다. 자원 소모 공격에 대한 대비는 암호학적 방법이 아닌 패킷 전송량등 다른 인자들을 갖고 판단할 수 있다.

6. 결론 및 향후 연구과제

본 논문에서는 이동적응망에서 안전한 라우팅 프로토콜을 제안하였다. 제안 프로토콜은 ID 기반 암호시스템을 이용하기 때문에 초기 설정 이후 추가적인 기반구조가 필요없는 장점이 있으며 ID 기반 암호시스템의 특성으로 인하여 이전에 제안되었던 안전한 라우팅 프로토콜에 비하여 망 자원 소모량을 줄일 수 있었으며 또한 상대적으로 적은 연산량으로 라우팅 경로에 있는 모든 단말들에 대한 인증을 수행할 수 있었다. 향후 연구과제로는 ID 기반 암호시스템을 이동적응망의 다른 보안 분야에도 적용시키는 것이다. ID 기반 암호시스템은 기반 구조가 없는 면에서 이동적응망과 유사한 특징이 있다. 뿐만 아니라 임의의 두 단말 사이의 키 교환 등에서 두 단말 사이에 전혀 통신이 필요 없는 등 많은 면에서 기존의 암호시스템보다 좀 더 유용한 기능을 제공한다. 이러한 기능을 확장시킨다면 이동적응망의 보안을 위해 많은 응용이 가능할 것이다.

7. 참고 문헌

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", Proc. Crypto'84 pp47-53

[2] David. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", Proc. IEEE Workshop on Mobile Computing Systems and Applications, pp 158-163, 1994.12

[3] Yih-Chun Hu, Adrian Perrig, David B.Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proc. Mobicom'02

[4] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, and Clay Shields,"A Secure Routing Protocol for Ad Hoc Networks.", Technical Report UM-CS-2001-037, EECS. University of Michigan, 2001.

[5] Panagiotis Papadimitratos and Zygmunt J.Haas, "Secure Routing for Mobile Ad hoc Networks" , Proc. The SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002.1

[6] Adrian Perrig, Ran Canetti, Dawn SOng, J.D. Tygar , Efficient and Secure Source Authentication for Multicast

[7] Dan Boneh, Matthew Franklin,"ID-Based Encryption from the Weil-Pairing", Proc. Asiacrypt'02 ,2002.12

[8]K.Peterson, "ID-based Signatures from Pairings on Elliptic Curves", Cryptology-eprint-archive", 2002-04

[9]Paulo S.L.M. Barreto, Hae Y.Kim, Ben Lynn and Michael Scott,"Efficient Algorithms for Pairing-Based Cryptosystems", *Advances in Cryptology -- Crypto'2002*, Springer-Verlag (2002), pp. 354--368.