이동 네트워크에서의 회귀분석을 이용한 키 선분배 및 인증 메커니즘

김수정° 김미희 김은아 채기준
이화여자대학교, 컴퓨터학과
{iris1993°, mihui, dmsk999, kjchae}@ewha.ac.kr

A Key Pre-distribution and Authentication Mechanism using Regression Analysis in NEMO

Soojeong Kim°, Mihui Kim, Eunah Kim, Kijoon Chae
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

네트워크 단위로 이동성을 제공하는 네트워크 이동성(NEtwork MObility, NEMO)프로토콜에서 방문 네트워크(Visited Network)는 이동네트워크의 홈 네트워크(Home Network)를 통해 이동 네트워크(Mobile Network)를 인증한다. 안전한 인증이 이루어지기 위해서 홈 네트워크의 인증 서버와 이동 네트워크 간의 사용할 키가 필요하게 된다. 그러나 두 엔터티간 키 협정을 위해 메시지를 주고받는 것은 서비스 에러나 공격에 취약하고 대역폭이나 밧데리 등이 제한적인 무선 환경에서는 적절하지 않다. 많은 키 결정 알고리즘에서 사용되는 공개키 기반 알고리즘은 이런 무선 환경에 적절하지 않다. 또한 비밀키 선분배 방식은 인증 서버가 자신이 인증해야할 모든 노드와의 키쌍을 가지고 있어야 한다는 점에서 확장성 문제를 지닌다. 이런 문제를 해결하기 위해, 본 논문에서는 회귀분석을 이용하여 쉽게 노드가 가지고 있는 키를 계산하고, 비밀키 인증서를 이용하여 간편하고 빠르게 인증을 수행할 수 있는 새로운 키 선분배 및 인증 메커니즘을 제안한다.

1. 서 론

최근 무선 네트워크의 기술 발달로 많은 기기들이 이동성 지원을 요구하고 있다. 그러나 기존의 Mobile IPv6는 이동성 지원을 위한 시그널 양이 단말과 비례한다는 점에서 대역폭 낭비가 심하다. 이동 네트워크 기술[1]은 Mobile IPv6를 바탕으로 여러 이동 단말과 하나 이상의 이동 라우터를 이동 네트워크라는 단위로 묶어 이동성을 제공한다. 이때 노드들은 이동 라우터를 통해 인터넷에 접속하기 때문에 이동과 관련된 아무런 작업이 필요 없고 그만큼 바인딩(binding) 시그널이 줄어 인터넷 접속 비용 절감과 여러 노드가 동시에 바인딩 업데이트를 하며 발생하는 바인딩 스톰 문제를 해결할 수 있다. 이동 라우터는 이동시 자신의 홈 에이전트(Home Agent, HA)에 바인딩 하여 생성된 양방향 터널을 통해 패킷을 주고받으면서 통신을 이어가게 된다. 그러나 그림 1에서 보듯이 NEMO의 경우 여러 네트워크들이 계층적으로 이루어 질 수 있어, 이동 네트워크가 방문 네트워크로 이동한 경우 자신과 연결된 상위 네트워크를 통해서만 인터넷 서비스를 받을 수 있고, 또한 이동 네트워크 역시 방문 네트워크의 구성원이 되어 향후 자신이 하위 계층으로 연결될 새로운 이동 네트워크에게 서비스를 제공해야 한다. 따라서 방문 네트워크와 이동 네트워크의 상호인증이 필수적이다.

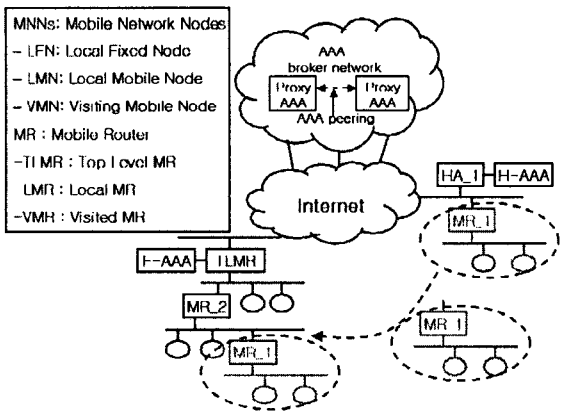

그림 1. 기본적인 이동 네트워크 구조

방문 네트워크가 이동 네트워크에 대한 정보를 가지고 있다면, 인증이 쉽게 이루어 질 수 있으나, 없다면 이동 네트워크의 홈 네트워크에게 이동 네트워크의 정보를 물어 보는 방식으로 인증이 이루어져야 한다. 홈 네트워크는 이동 네트워크가 자신에게 속해 있는지를 인증하기 위해서는 인증 정보를 주고 받아야 하며 이때 교환하는 메시지의 비밀성 유지를 위하여 안전한 암호화가 이루어져야 한다. 그러나 서로 다른 네트워크에 위치한 두 엔터티가 키 협정을 위해 메시지를 주고 받을 경우 (IKE의 경우

최고 6번의 메시지를 주고받는다[2].) 서비스 에러나 공격에 취약하고 대역폭이나 밧데리 등이 제한적인 무선 환경에서는 적절하지 않다. 많은 키 결정 알고리즘에서 사용하는 *Diffie-Hellman*과 같은 공개키 알고리즘은 이러한 무선 환경에 적절하지 않다. 또한 현재 대다수의 비밀키 선분배 알고리즘은 인증 서버가 자신이 인증해야 할 모든 노드와의 키쌍을 가지고 있어야 한다는 점에서 메모리와 키 검색 등의 확장성 문제를 지닌다. 이런 문제를 해결하기 위해, 본 논문에서는 회귀분석을 이용하여 쉽게 노드가 가지고 있는 키를 계산할 수 있는 새로운 키 선분배 방식을 제안한다. 이 방식은 임계치 성질(Threshold property)을 가짐으로써 일정수의 노드가 협력하기 전에는 키풀(key pool)이 밝혀지지 않는 장점을 가진다. 또한 모바일 라우터가 가져야 할 정보를 적게 했으며, 확장성 문제도 해결할 수 있다.

본 논문은 먼저 제안된 메커니즘에 적용될 관련 연구와 기본 가정을 설명하고 이를 바탕으로 보안에 사용될 키 선분배 방식과 그 키와 대칭키 인증서를 이용한 모바일 라우터의 인증 방안을 설명한 다음, 결론을 맺기로 한다.

2. 관련연구 및 가정

2.1 회귀분석 모델

회귀분석은 여러 개의 독립변수($x_1, x_2, ..., x_m$)와 하나의 종속변수(y)사이의 함수관계를 알아 내는 통계적인 방법으로서 다음과 같은 관계식으로 나타내게 된다.

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_m x_m + \epsilon$$

$\beta_0, \beta_1, \beta_2, ..., \beta_m$는 회귀계수로 모수이다. ϵ는 y를 측정할 때 발생하는 오차이다. 우리는 측정값(y)과 예측값($\hat{y}$)의 차 즉 오차를 최소로하기 위한 최소오차제곱합(Min $\Sigma (y_j - \hat{y}_j)^2$)을 이용하여 모수를 추정할 수 있다[3]. 다음은 추정된 회귀식이다.

$$\hat{y} = b_0 + b_1 x_1 + b_2 x_2 + ... + b_m x_m$$

n개의 관찰점들을 한데 묶어서 행렬로 표기하면, 다음과 같이 표기할 수 있다.

$$\hat{y} = Xb$$

$$\begin{Bmatrix} \hat{y}_1 \\ \hat{y}_2 \\ \hat{y}_3 \\ \cdot \\ \cdot \\ \cdot \\ \hat{y}_n \end{Bmatrix} = \begin{Bmatrix} 1\ x_{11}\ x_{21}\ x_{31} \ldots x_{m1} \\ 1\ x_{12}\ x_{22}\ x_{32} \ldots x_{m2} \\ 1\ x_{13}\ x_{23}\ x_{33} \ldots x_{m3} \\ \cdot \\ \cdot \\ \cdot \\ 1\ x_{1n}\ x_{2n}\ x_{3n} \ldots x_{mn} \end{Bmatrix} \begin{Bmatrix} b_1 \\ b_2 \\ : \\ \cdot \\ b_m \end{Bmatrix}$$

그림 2. 행렬로 표현된 회귀 모형

이때 b는 최소오차제곱합에 의해 $b=(X'X)^{-1}X'$ 로 나타낼 수 있다(X'는 X의 전치행렬이다.) 따라서 위의 식은 최종적으로 다음과 같이 나타낼 수 있다.

$$\hat{y} = X(X'X)^{-1} X'y$$

2.2 비밀키 인증서

본 논문에서는 선분배된 키에 대한 인증서를 Park의 비밀키 인증서[4]를 수정하여 구현하도록 한다. 인증서버(*Authentication Server*, AS)의 비밀키로 인증서를 만든 Park의 비밀키 인증서 방식을 향후 제안된 프로토콜을 NEMO의 양방향 인증으로 확대하기 위해서 각 이동 라우터에게 선분재된 키를 이용하여 인증서를 만들도록 수정하였다.

모바일 라우터는 홈 네트워크에 인증서 신청시 한 네트워크에 정한 단방향 해쉬함수를 이용해 자신만의 해쉬 체인(hash chain)을 만들어 그 체인의 초기값과, 자신의 식별자를 자신의 홈 네트워크의 AS에 등록한다. 그러면, AS는 받은 정보를 자신의 키로 암호화하고 거기에 제너레이터 행렬을 곱하여 모바일 노드에게 인증서를 발행한다. 모바일 노드는 자신의 홈 네트워크에서 다른 네트워크로 이동시 자신을 인증받기 위해 인증서에 자신의 정보를 에러코드로 바꾼 것을 더해 홈 네트워크의 인증서버로 보내준다. 인증서버는 제너레이터 행렬의 신드롬 행렬을 이용하여 인증서와 에러 코드를 분리할 수 있다. 인증서버는 이러한 방법으로 에러 코드에서 모바일 노드의 정보를 빼내어 인증서와 함께 모바일 노드를 인증하게 된다.

3. 제안하는 메커니즘

본 논문에서는 홈 네트워크의 인증 서버가 키를 생성하여, 분배하고, 키를 재 계산하여 모바일 라우터의 진위 여부를 인증하는 방법을 명시한다.

3.1 키 스페이스의 생성

인증서버(AS)는 유한필드 GF(q)를 따르는 n-by-m 행렬 X와 n-by-1 행렬 y를 생성한다. 이 두 행렬은 인증서버가 비밀리에 저장해야 할 정보이다. 위의 두 행렬을 이용하여 n개의 키로 구성된 키 스페이스 행렬인 $\hat{y}$을 만든다. 따라서 n개의 키를 가진 키 스페이스가 생성되었다. 인증서버는 모바일 라우터에게 자신의 키 스페이스에서 랜덤하게 키를 분배하게 된다. 따라서 인증해야할 모바일 라우터의 수가 증가하여도 그 수만큼 키 스페이스에 키를 추가할 필요가 없고, 다수의 모바일 라우터에 같은 키를 할당하여도 인증서버에 모바일 라우터와 키에 관련된 정보를 직접 저장하지 않기 때문에 보안상 안전하다.

3.2 비밀키 인증서 생성 및 키 선분배

인증서버(AS)는 모바일 라우터에게서 받은 해쉬체인 초기값과 식별자를 키 스페이스에서 i번째 키를 랜덤하게 뽑아 그 키로 암호화 하고 그것에 제너레이션 행렬을 곱하여 암호화된 인증서와 키 그리고 그 키에 대한 정보인 X의 i번째 행을 모바일 라우터에 할당한다.

MR ⟶ AS : seed(hash chain), ID

MR ⟵ AS : c, $\hat{y}_i$, X_i

$c = ([r_0 || ID])\ \hat{y}_i + G$, 암호화된 인증서

$\hat{y}_i$ = ith row of $\hat{y}$ = key

X_i = ith row of $X = (1\ x_{1i}\ x_{2i}\ x_{3i} \ldots x_{mi})$

3.3 인증을 위한 키 재계산

3.3.1 모바일 라우터

암호화된 인증서와 키 정보를 받은 모바일 라우터가 자신의 홈 네트워크에서 방문 네트워크로 이동하였을 경우, 방문 네트워크는 모바일 라우터에대한 사전 지식이 없을 경우를 가정하자. 방문 네트워크에서는 EAP구조에서와 같이 모바일 라우터의 홈 네트워크내의 인증 서버에게 모바일 라우터의 진위여부를 확인 받은 후 모바일 라우터를 인증해야 할 것이다. 따라서 모바일 라우터는 자신의 진위 여부를 인증서버에 확인 받아야 한다. 모바일 라우터는 자신이 가진 키의 정보와 해쉬 체인의 순서를 에러코드화 하여 홈 네트워크의 인증서버에 보내 주게 된다. 다음은 에러 코드화 하여 인증서와 합쳐져 인증서버에 보내지는 과정을 도식화 한 것이다.

$z_i = [\, X_i \,||\, r_j \,||\, j \,]$

: rj 는 모바일 라우터가 가진 해쉬 체인의 j 번째 값

z_i → [Error code Generator] → $e^{(i)}$

$e^{(i)}$: z_i 의 에러 코드

MR → AS : $c + e^{(i)}$

3.3.2 홈 네트워크의 인증 서버

인증서버는 받은 인증서와 에러코드의 합을 제너레이션 행렬의 신드롬 행렬을 이용하여 둘을 분리하게 된다. 분리된 에러코드를 원래의 형태로 바꾸어 키 정보 Xi 와 해쉬 값 r_j를 추출하고, 해쉬 함수에 해쉬 값을 넣고 j 번 실행하여, 초기값을 구한다.

$e^{(i)}$ → [Error code Identifier] → z_i

$z_i = [\, X_i \,||\, r_j \,||\, j \,]$

$r_0 = h(h(\cdots(h(r_j))\cdots))$ j 번 실행 하여 초기값 계산

추출한 키 정보를 구하는 방법은 간단하다. 회귀함수 $\hat{y} = Xb$ 에서 b 행렬에 주목하자, b 는 $(X'X)^{-1}X'y$ 로 이루어진 m-by-1 행렬이다.

$$\begin{Bmatrix} \hat{y}_1 \\ \hat{y}_2 \\ \hat{y}_3 \\ \cdot \\ \cdot \\ \cdot \\ \hat{y}_n \end{Bmatrix} = \begin{Bmatrix} 1\ x_{11}\ x_{21}\ x_{31}\ldots x_{m1} \\ 1\ x_{12}\ x_{22}\ x_{32}\ldots x_{m2} \\ 1\ x_{13}\ x_{23}\ x_{33}\ldots x_{m3} \\ \cdot \\ \cdot \\ \cdot \\ 1\ x_{1n}\ x_{2n}\ x_{3n}\ldots x_{mn} \end{Bmatrix} \begin{Bmatrix} b_1 \\ b_2 \\ b_3 \\ : \\ \cdot \\ b_m \end{Bmatrix}$$

그림 3. 키 계산 과정

그림 3 에서 보듯이 인증 서버는 모바일 라우터가 가지는 X_i를 알면 모바일 라우터가 가지고 있는 키 $\hat{y}_i$를 구할 수 있다. 키를 구한 인증 서버는 암호화된 인증서 c $(c = ([r_0||ID])\hat{y}_i + G)$ 에서 G를 분리하고, 구한 키로 복호화 하여 모바일 라우터의 ID를 확인하고 앞에서 구한 해쉬 체인의 초기값과, 인증서 내의 초기값과 같은지를 확인하여 모바일 라우터의 진위를 판별하게 된다.

4. 결론

본 논문은 기존 대칭키 알고리즘에 근거한 키 선분배 방식의 확장성 문제를 해결하는 방안을 제시하였다. 대칭키를 사용하되, 키 스페이스라는 공동의 키를 랜덤하게 사용하고, 인증서버가 키와 모바일 라우터를 1:1로 매핑하여 저장하여야 하는 비 효율성 및 인증서버가 공격당했을 때 모바일 라우터들이 가지는 키가 쉽게 노출된다는 보안상 문제를 없애고 키 정보만으로 키를 쉽게 구할 수 있게 하였다.

만약 인증서버가 $(X'X)^{-1}X'$를 미리 계산하고 있다면, 키를 찾기 위해 (mn^2 or m^2n)번의 multiplication modulo가 실행되어야 하고, 만약 행렬 b인 $(X'X)^{-1}X'y$를 계산하고 있다면, 단지 m번의 multiplication modulo 만이 필요하게 된다. 이는 공개키 기반의 인증서와 비교시 상당히 적은 양이다[5].

이렇게 구한 키를 이용하여 대칭키 인증서를 통한 모바일 라우터의 인증이 수행된다. 암호화된 인증서에서 정보를 추출하는 모든 계산이 행렬로 이루어지기 때문에 계산이 빠르고 안전성에 비해 노드가 저장하여야 할 정보의 양을 최소화 할 수 있다.

본 논문의 회귀분석을 이용한 키 선분배 및 인증 메커니즘은 m개의 모바일 라우터가 협약을 맺지 않는 이상 안전성이 보장되는 m-secure 성질을 가진다. 임계치 성질을 높이기 위해 Blom의 정리를 이용한 Pariwise 키 선분배 방식[5]처럼 행렬 X나 y를 여러개 두어 키 스페이스의 풀(pool)을 만들어 모바일 라우터가 랜덤한 몇 개의 풀에서 랜덤하게 키와 키정보를 제공 받도록 확장하는 것도 쉽게 가능할 것이다. 또한 해쉬 체인을 사용하여 양방향 인증 등으로 확장할 경우 되풀이 공격(replay attack)을 쉽게 해결할 수 있다.

앞으로 향후 연구로서 제안한 키 선분배에서의 키 스페이스 추가 삭제 방법 및 이것을 이용한 NEMO에서의 양방향 인증 메커니즘을 구현하고자 한다.

5. 참고문헌

[1]Ryuji Wakikawa, Alexandru Petrescu and Pascal Thubert, " Nemo Basic Support Protocol," Internet draft, IETF, Dec. 2003. Work in progress.

[2] Carlton R. Davis, " IPSec Securing VPNs", Osborne/McGraw-Hill, 2001.

[3]박성현, " 제3판 회귀분석" , 민영사, Sep.1998.

[4]Chang-Seop Park, " Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems," Computer Networks 44, p267~p273, 2004.

[5]Wenliang Du and Jing Deng, " A Pairwise Key Pre-distribution Scheme for Wireless Sensor Network," CCS'03, Oct. 2003.