무선 애드 혹 네트워크에서 보안성이 강화된 그룹 키 합의 프로토콜

김성진, 김호희, 이재욱, 김순자
경북대학교 전자전기컴퓨터학부
e-mail:goodluck@knu.ac.kr

Securely Improved Group Key Agreement Protocol in Wireless Ad Hoc Networks

Sung-Jin Kim, Jae-Wook Lee, Ho-Hee Kim, Soon-Ja Kim
SChool of Electrical Engineering and Computer Science,
Kyungpook National University

요 약

무선 애드 혹 네트워크의 사용이 증가함에 따라 네트워크의 보안 또한 매우 중요하게 인식되어 지는 추세이지만, 현재 무선 애드 혹 네트워크의 보안성 표준안에 대한 정의가 미흡한 상황이다. 현재까지 많은 연구를 통해 제안된 키 관리 프로토콜은 오직 특정 상황에만 적용 가능한 단점을 가지고 있다. 2005년 무선 애드 혹 네트워크에서 안전한 그룹 통신을 위한 새로운 키 합의 프로토콜인 CRTDH 프로토콜이 제안되었다[1]. 이 프로토콜은 효율적으로 그룹 키를 계산할 수 있고, 멤버들의 높은 이동성을 지원한다. 하지만 그룹 키 설정 과정에서 공격자가 송신자와 수신자 사이에서 전달되는 메시지를 위조 할 수 있고, 키의 재설정 과정에서 그룹이 변경 되어도 이전 그룹 키와 동일하게 계산 될 수 있다. 즉 중간자(Man-in-the-middle) 공격과 LCM(Least Common Multiple) 공격에 취약하다. 본 논문에서는 두 가지 공격에 대한 해결책을 제시하여 보안성이 강화된 그룹 키 합의 프로토콜을 제안한다.

1. 서론

최근 무선 네트워크의 발전은 회사, 가정, 군대 등 여러 방면에서 컴퓨터와 네트워크의 사용방법을 근본적으로 바꿔 놓았다. 이러한 네트워크상의 정보 보안 역시 매우 중요해 졌다. 일반적으로 유선 네트워크의 보안 서비스는 신뢰하는 기관에서 제공한다. 그러나 무선 애드 혹 네트워크 환경에서는 네트워크의 특수성 때문에 신뢰하는 기관이 제공하는 보안 서비스를 이용 할 수 없다. 따라서 구성된 네트워크 멤버들이 직접 보안 서비스를 제공해야 한다. 최근 이러한 보안 서비스 제공 문제에 대해 많이 연구 되고 있으며, 특히 키 관리와 인증에 대한 연구가 많이 진행되고 있다[3,4,5,6].

일반적인 무선 애드 혹 네트워크 환경에서는 보안성에 대한 표준안이 잘 정의 되어 있지 않아서, 지금까지 제안된 대부분의 프로토콜은 각각 다른 전제 조건을 제시 하거나 보안성 요구 사항이 상황에 따라 틀리다. 즉 현재까지 연구된 프로토콜의 대부분이 특정 환경에서만 적용 가능하도록 설계 되었다.[2]

Balachandran등이 제안한 CRTDH는 무선 애드 혹 네트워크에서 새롭고 효과적인 그룹 키 동의 프로토콜을 제시하고 있다. 이 프로토콜은 안전한 그룹 통신과 모든 멤버가 그룹 키 동의 프로토콜에 동일한 공헌을 하기 위해, Chinese-Remainder Theorem과 Diffie-Hellman key exchange를 이용한다. 이 프로토콜은 효과적인 방법으로 키 동의를 실행하며, 멤버들의 순서화 또는 구조화를 배제한다. 또한 그룹 키 참여에 필요한 정보를 미리 알기위해 신뢰하

본 연구는 경북대학교 연구 교수 지원으로 수행되었음.

는 기관이나 중심 개체가 존재하지 않는다.[1]

그룹 키 설정과정에서 전달되는 broadcast 메시지를 송신자와 수신자 사이에서 공격자가 메시지를 위조해서 보낼 수 있고, 키의 재설정 과정에서 그룹이 변경되어도 이전 그룹 키와 동일하게 계산 될 수 있다. 다시 말해서 Man-in-the-middle 공격과 Least Common Multiple(LCM) 공격에 취약하다.

본 논문에서는 이러한 공격을 방지 수 있도록 보안성이 강화된 CRTDH 프로토콜을 제안한다. 이 프로토콜은 기존의 특징을 그대로 유지하면서 보안성을 강화했다.

본 논문의 나머지 부분은 다음과 같다. 2장에서는 Balachandram등이 제안한 CRTDH 프로토콜과 문제점에 대해서 설명하고, 3장에서는 보안성을 강화한 그룹 키 합의 프로토콜을 소개한다. 4장에서는 제안하는 프로토콜의 보안성 분석에 대하서 논의하고, 5장에서 결론을 내린다.

2. CRTDH 프로토콜

2005년 Balachandram등이 제안한 CRTDH 프로토콜은 키 합의단계와 멤버의 가입 및 탈퇴 동작으로 이루어져 있다. 여기서는 키 합의 단계만 설명한다.

2.1 키 합의 프로토콜

그룹 키 설정을 위해 모든 멤버 $U_i(i=1,\cdots,n)$는 동시에 다음 절차를 순서대로 실행한다.

단계 1. Diffie-Hellman(DH) 개인 값 x_i을 선택하고, 공개 값 $y_i = g^{x_i} \bmod p$을 계산한다. (Diffie-Hellman 계산에서 g는 생성자이고, p는 prime modulo 이다. 이 정보는 공개하고, 이 값을 공유하지 않으면 초기에 broadcast round가 필요하다)

단계 2. DH 공개 값 y_i을 그룹의 모든 멤버들에게 broadcast 한다.

단계 3. 그룹의 모든 멤버들로부터 DH 공개 값을 받아서 다음과 같이 각각 DH 키 값으로 만든다. $m_{ij} = y_j^{x_i} \bmod p$ $(j=1,\cdots,i-1,i+1,\cdots,n \quad j \neq i)$

단계 4. 단계 3에서 계산한 모든 멤버들의 DH 키 값에서 Least Common Multiple (LCM)을 계산한다.(lcm_i)

단계 5. 그룹 키의 값이 될 임의의 수 k_i $(k_i < \min(m_{ij}, \forall j))$을 선택한다. $D(D \neq k_i)$와 $D_p(\gcd(D_p, lcm_i) = 1)$을 임의로 선택한다.

단계 6. CRT를 풀어서 결과 값 crt_i을 그룹 내의 모든 멤버들에게 broadcast한다.

$crt_i = k_i \bmod lcm_i$

$crt_i = D \bmod D_p$

단계 7. 그룹의 모든 멤버들로부터 crt_j을 받아서 $k_j = crt_j \bmod m_{ij}$ $(i \neq j)$ 계산 후 그룹 키를 계산한다.

그룹 키 : $GK = k_i \oplus \cdots \oplus k_n$

$k_j \equiv crt_j \bmod LCM_j \equiv crt_j \bmod m_{ij}$이 성립하면 모든 멤버들은 동일한 그룹 키를 계산 해 낼 수 있다. 그룹 내의 모든 멤버들은 broadcast 값 U_i로부터 crt_i , U_{i+1}로부터 crt_{i+1} , U_n로부터 crt_n을 받는다. 값을 받은 멤버들은 $m_{(i,1)}, \cdots, m_{(i,i-1)}$, $m_{(i,i+1)}, \cdots, m_{(i,n)}$을 이용해서 $k_1, \cdots, k_{i-1}$, $k_{i+1}, \cdots, k_n$을 계산 할 수 있다. 그러면 모든 멤버들은 그룹 키를 계산하는데 필요한 모든 값을 가지게 된다. 그러므로 그룹 내의 모든 멤버는 동일한 키를 계산할 수 있다.

2.1 문제점

CRTDH 프로토콜은 그룹 키 설정과정에서 송신자와 수신자 사이에 전달되는 broadcast 메시지를 공격자가 위장 공격 할 수 있다. 공격자가 송신자와 수신자 사이에서 DH 공개 값 y_i와 CRT를 푼 값 crt_i를 y_i'와 crt_i'로 변경한 메시지를 송신하게 되면 모든 참가자들의 동일한 그룹 키 계산이 불가능해진다. 이와 같은 Man-in-the-middle 공격을 방지하기 위해서 broadcast 메시지가 수신자에게 전달되는 안전한 방법이 필요하다.

CRTDH 프로토콜은 또한 LCM 공격에도 취약하다. 이 공격은 LCM 값이 그룹에서 유일하지 않기 때문에 가능하다. 다시 말해서, 멤버들이 그룹에 가입하고 탈퇴하더라도 예전과 동일한 LCM 값으로 유지 될 수 있다.

3. 제안하는 그룹 키 합의 프로토콜

이 장에서는 보안성이 강화된 CRTDH 프로토콜을 제안한다. 기존의 프로토콜은 그룹 키 설정 과정 중 단계 2와 단계 6에서 broadcast 메시지를 암호화하지 않고 전송하기 때문에 공격자가 메시지를 변경해서 보낼 수 있다. 제안하는 프로토콜에서는 broadcast 메시지를 정당한 수신자만 내용을 볼 수

있게 하여 공격을 방지 한다. 구체적으로 broadcast 메시지를 특정 멤버에게만 전달하기 위해, m_{ij}이 키가 되는 대칭키 암호화 기법으로 broadcast 메시지를 암호화해서 전달하는 방법이다. 또 LCM 공격을 막기 위해서는 그룹에 새로운 멤버가 가입하거나 기존의 멤버가 탈퇴 할 때 $lcm_j \bmod m_{ji} = 0$이면, 개인 값 x_i대신 $(x_i + 1)$의 값으로 다시 계산하는 방법을 이용한다. 이 프로토콜은 system setup, 키 합의 프로토콜, 가입 및 탈퇴 동작으로 구성된다.

3.1 system setup

단계 1. 키 설정에 참여하는 의사 표현 메시지(M)를 그룹 멤버들에게 전달한다.

단계 2. Diffie-Hellman(DH) 개인 값 x_i을 선택하고, 공개 값 $y_i = g^{x_i} \bmod p$을 계산한다.

단계 3. DH 공개 값 y_i을 그룹의 모든 멤버들에게 broadcast 한다.

단계 4. 그룹에서 메시지(M)를 전달한 모든 멤버들로부터 DH 공개 값을 받아서 다음과 같이 각각 DH 키 값으로 만든다.

$m_{ij} = y_j^{x_i} \bmod p$

$(j = 1, \cdots, i-1, i+1, \cdots, n \quad j \neq i)$

3.2 키 합의 프로토콜

단계 1. 그룹 키의 값이 될 임의의 수 k_i을 선택하고, $\{k_i$를 $y_j^{x_i} (= m_{ij})$로 암호화 한다. $[(\{k_i\}_{y_j^{x_i}}, member\ j), \cdots, (\{k_i\}_{y_n^{x_i}}, member\ n)] = A_i$ 계산 후 broadcast한다.

단계 2. 그룹의 모든 멤버들로부터 A_i값을 받아 복호화 후, $k_i, \cdots, k_n$ 값을 얻는다.

단계 3. System setup 단계 4.에서 계산한 모든 멤버들의 DH 키 값에서 LCM 값을 계산 한다.(lcm_i)

단계 4. 그룹 키의 값이 될 임의의 수 b_i $(b_i < \min(m_{ij}, \forall j), (b_i \neq k_i))$을 선택하고, $(k_i)_p (\gcd((k_i)_p, lcm_i) = 1)$을 선택한다.

단계 5. 아래의 CRT를 푼다.

$$crt_i \equiv b_i \bmod lcm_i$$
$$crt_i \equiv k_i \bmod (k_i)_p$$

단계 6. $\{crt_i\}$를 키 $y_j^{x_i}$로 암호화 한다. $[(\{crt_i\}_{y_j^{x_i}}, member\ j), \cdots, (\{crt_i\}_{y_n^{x_i}}, member\ n)] = B_i$ 계산 후 broadcast 한다.

단계 7. 그룹의 모든 멤버들로부터 B_i값을 받아서 복호화 후 다음과 같이 crt_j 값을 계산한다. $b_j = crt_j \bmod m_{ij} (i \neq j)$

모든 멤버들로부터 b_i와 k_i값을 얻으면 그룹 키를 계산한다.

$GK = (b_1 \oplus k_1) \oplus \cdots \oplus (b_n \oplus k_n)$

$b_j \equiv crt_j \bmod LCM_j \equiv crt_j \bmod m_{ij}$이 성립 하면 모든 멤버들은 동일한 그룹 키를 얻을 수 있다. 그룹 내의 모든 멤버들은 broadcast 값 A_i을 복호화 해서 $k_i, \cdots, k_n$ 값을 받고, U_i로부터 crt_i , U_{i+1}로부터 crt_{i+1} , U_n로부터 crt_n을 받는다. 값을 받은 멤버들은 $m_{(i,1)}, \cdots, m_{(i,i-1)}, m_{(i,i+1)}, \cdots, m_{(i,n)}$을 이용해서 $b_1, \cdots, b_{i-1}, b_{i+1}, \cdots, b_n$을 계산 할 수 있다. 마침내 그룹 내의 모든 멤버들은 그룹 키를 계산하는데 필요한 모든 값을 가지게 된다. 그러므로 그룹 내의 모든 멤버는 동일한 키를 계산할 수 있다.

3.3 가 입

기존 그룹 멤버가 (U_1, U_2, U_3, U_4) 이고, 멤버 U_5가 그룹에 들어올 때 다음과 같이 동작한다.

단계 1. 새로 들어 올려는 멤버 U_5와 가장 가까이 있는 멤버가 기존 그룹 키의 hash 값 $h(GK)$와 각 멤버의 DH 공개 값 y_1, y_2, y_3, y_4을 공유한다.

단계 2. System setup단계와 key agreement단계를 실행함으로써 기존의 멤버들과 CRT 값 crt_5, DH 공개 값 y_5을 공유한다. 만약 key agreement 단계 3을 실행하면서 $lcm_5 \bmod m_{15} = 0$ 이면 (x_i+1)의 값으로 다시 계산한다.

단계 3. 기존의 멤버들은 CRT 값 crt_5 와 DH 공개 값 y_5를 받아서 b_5와 k_5을 계산할 수 있고, 새로운 그룹 키를 계산한다.

$GK_{\neq w} = h(GK) \oplus (b_5 \oplus k_5)$

3.4 탈 퇴

현재 그룹 멤버가 (U_1, U_2, U_3, U_4) 이고, 멤버 U_2가 그룹에서 나갈 때 다음과 같이 동작한다.

단계 1. 현재 남아 있는 멤버 중 한 멤버가(U_1)가 key agreement단계를 다시 실행한다. 만약 key agreement 단계 3을 실행

하면서 $lcm_1 \bmod m_{1j} = 0$이면 (x_i+1)의 값으로 다시 계산한다.

단계 2. 탈퇴한 멤버 U_2을 제외한 현재 그룹에 남아 있는 다른 멤버들은 broadcast 값 A_i , B_i 값을 계산 후 새로운 $b_1^{'}$, $k_1^{'}$값으로 새로운 그룹 키를 계산한다.

$$GK_{\neq w} = h(GK) \oplus (b_1^{'} \oplus k_1^{'})$$

4. 보안성 분석

기존의 프로토콜은 그룹 키 설정과정에서 공격자가 송신자와 수신자 사이에서 DH 공개 값 y_i와 CRT를 푼 값 crt_i를 $y_i^{'}$와 $crt_i^{'}$로 변경한 메시지를 송신한다. 변경된 메시지를 받은 모든 참가자들은 동일한 그룹 키 계산이 불가능해 진다. 이와 같은 Man-in-the-middle 공격을 방지하기 위해서 broadcast 메시지가 수신자에게 전달되는 안전한 방법이 필요하다. 제안하는 그룹 키 합의 프로토콜은 그룹 키 설정 과정에서 broadcast 메시지를 정당한 수신자만 내용을 볼 수 있게 하여 공격을 방지할 수 있다. 구체적으로 broadcast 메시지를 특정 멤버에게만 전달하기 위해, m_{ij}이 키가 되는 대칭키 암호화 기법으로 broadcast 메시지를 암호화해서 전달하기 때문에 공격자가 메시지를 함부로 변경하지 못한다.

LCM 공격은 그룹 키 설정 과정에서 LCM 값이 그룹 내 에서 유일하지 않기 때문에 가능하다. 멤버들이 그룹에 가입하고 탈퇴하더라도 예전과 동일한 LCM 값으로 유지 될 수 있어서, 동일한 LCM 값으로 새로운 그룹 키를 계산할 수 있다. 이런 현상을 이용한 LCM 공격을 막기 위해서는 그룹에 새로운 멤버가 가입하거나 기존의 멤버가 탈퇴 할 때 $lcm_j \bmod m_{ji} = 0$이면, 개인 값 x_i대신 (x_i+1)의 값으로 다시 계산한다. 개인 값 x_i대신 (x_i+1)로 바꿈으로써 더 이상 LCM 값이 동일 할 수 없다. 현재 그룹의 멤버가 아니면 더 이상 그룹 키를 계산할 수 없다.

5. 결론

지금까지 많은 무선 애드 혹 네트워크의 보안성에 대한 프로토콜들이 제안 되었지만, 가장 일반적인 무선 애드 혹 네트워크 환경에서 제안된 프로토콜은 CRTDH이다. CRTDH 프로토콜의 문제점은 broadcast 메시지를 공격자가 변경 할 수 있었고, LCM 값이 같아지는 경우가 있어 새로운 그룹 키 계산이 가능했다. 이 논문에서 제안하는 그룹 키 합의 프로토콜은 broadcast 메시지가 변경되는 문제점을 특정 멤버만이 볼 수 있도록 대칭키 암호화방식으로 broadcast 메시지를 암호화해서 전송한다. 또한 LCM 값을 다르게 하기 위해 $lcm_i \bmod m_{ij} = 0$ 이면 (x_i+1)의 값으로 다시 계산해서 LCM 값을 다르게 한다. 이러한 방법을 토대로 보안성이 강화된 CRTDH 프로토콜을 제안하고, 제안하는 프로토콜은 기존특징을 그대로 유지 하면서 기존 보다 보안성을 강화 한다.

참고문헌

[1] Balachandran, R., Ramamurthy, B., Zou, X., Vinodchandran, N.: CRTDH: An efficient key agreement scheme for secure group communications in wireless ad hoc networks. Proceedings of IEEE ICC 2005 (2005)

[2] Xukai, Amandeep Thukral, Byrav Ramamurthy : An Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks. Springer-Verlag Berlin Heidelberg 2006 (2006)

[3] Weimerskirch, A., Thonet, G.: A distributed light-weight authentication model for ad-hoc networks. Proceedings of the 4th International Conference Seoul on Information Security and Cryptology (2001) 341-354

[4] Wu, B., Wu, J., Fernandez, E., Magliveras, S.: Secure and efficient key management in mobile ad hoc networks. Proceedings of the 1st Int'l workshop on Systems and Network Security (SnS2005) (2005)

[5] Khalili, A., Katz, J., Arbaugh, W.: Toward secure key distribution in truly ad-hoc networks. Cryptobytes, Volume 5, No. 2 (RSA Laboratories, Summer/Fall 2002) (2002) 2-13

[6] Zhu, S., Xu, S., Setia S., Jajodia, S.: LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks. IEEE International Conference on Distributed Computing Systems (2003)