Ad-Hoc 네트워크에서의 안전한 라우팅을 위한 인증 및 키 생성에 관한 연구

강서일*, 이임영*
*순천향대학교 컴퓨터 공학부
e-mail:kop98@sch.ac.kr

A Study on Authentication and Key Generation for Secure Routing in Ad-Hoc Network

Seo-il Kang*, Im-yeong Lee*
*Division of Computer Science and Engineering, Soonchunhyang University

요 약

Ad-Hoc 네트워크는 임의 디바이스들이 무선 통신을 통해서 임의 네트워크 망을 구성하여 통신 서비스를 제공받는 것을 말한다. 특히 유비쿼터스 환경에서의 언제 어디서나 통신을 하기 위해서는 이동성과 자유로운 네트워크의 조인 및 탈퇴가 이루어져야 한다. 또한 통신에서 제 3자의 위장이나 정보의 도청 그리고 안전성을 제공하기 위해서 암호화 통신이 필수적으로 요구된다. 특히 Ad-Hoc 네트워크의 디바이스간의 라우팅 구성이 유동적이라서 구성하는 디바이스간의 인증 및 키 생성과정이 필요하며, 라우팅에 대한 보안 기술의 연구는 국내/외에서 진행되어져 왔다. 본 논문에서는 기존의 안전한 라우팅 방안에 대하여 알아보고 디바이스 인증 및 키 설립을 제공하는 방식에 대하여 제안한다. 본 방식은 세션키를 설립을 위해서 키 생성 및 아이디를 기반으로 한 인증 방안을 이용한다. 그로 인해 인증서를 이용하거나 디바이스간의 인증 정보 및 상호 공유된 비밀 정보가 필요하지 않는 장점을 가지고 있다. 이와 같은 방식을 이용하므로 임의 네트워크에 조인하더라도 보안 기술을 제공할 수 있는 방안이다. 본 연구를 이용하므로 유비쿼터스 환경에서의 안전한 서비스를 제공할 수 있는 기술로 활용할 수 있다.

1. 서론

유비쿼터스 환경은 언제, 어디서나, 어떠한 네트워크, 모든 기기, 어떠한 서비스라도 제공받을 수 있어야 한다. 그러므로 장소나 이동에 구애받지 않는 방안으로 무선 통신의 디바이스를 이용하여 서비스를 제공 받을 수 있어야 한다. 그러므로 조인과 탈퇴가 빈번히 발생할 수 있으며, 네트워크의 망이 고정적이지 않고 유동적인 상태를 유지한다. 이러한 네트워크 망으로 Ad-Hoc 네트워크 망을 볼 수 있다. Ad-Hoc 네트워크의 활용되는 사용자의 디바이스는 다른 디바이스와의 통신을 하기 위해서 라우팅을 이루어야 하며, 서로 디바이스의 존재를 확인하여 정보를 전송할 수 있어야 한다. 보안 기술로 Ad-Hoc 네트워크에서의 가장 문제가 되는 것은 디바이스간의 인증 및 키 설립 과정이다. 사유는 임의 디바이스가 접근 가능한 무선 통신을 제공하므로 네트워크 망에 조인하는 디바이스를 인증할 수 있는 방안과 인증된 디바이스간의 암호화 통신을 위한 키 설립이다. 특히 대칭키를 이용하는 경우 서로 같은 키를 이용하기 위해서 사전의 비밀 정보를 공유할 수 있는 방안을 제시하여야 한다. 그러나 많은 연구가 사전 비밀 정보의 공유는 가정 사항으로 두고 있기 때문에 실제 Ad-Hoc 네트워크를 임의로 이루는 디바이스간의 키 설립은 매우 어려운 사항이다. 그리고 인증에 대한 방안도 상대방의 인증 정보를 보유하고 있어야 하는데 이렇기 위해서는 상대방이 네트워크 망에 접근하기 전에 이미 알고 있어야 한다. 이 또한 사전 공유 정보가 필요하게 된다. 그러므로 다른 방안으로 공개키 기반의 인증서를 이용하는 방안이 제시되고 진행되었다. 하지만 공개키를 이용하는 경우 사전의 공개키를 등록하는 신뢰기간이 필요하거나 인증서 체인을 검증할 수 있는 방안이 필요하게 된다. 만약 임의 공개키를 생성하여 이용하는 경우 제 3자의 위장 공개키로 인해 보안 기술에 취약점이 될 수 있다. 그러므로 인증서 기반의 공개키 방식은 기존의 Ad-Hoc 네트워크의 디바이스에 연산 능력 및 하드웨어의 제약 사항을 고려할 필요가 있다. 본 논문의 구성은 2장에서 Ad-Hoc 네트워크에서의 보안 요구 사항에 대하여 알아보고 3장에서는 기존 연구 방식에 대하여 학습한다. 4장에서는 본 논문의 제안 방식을 설명하고 5장에서는 2장의 보안 요구사항을 이용하여 제안 방식을 분석한다. 그리고 최종적으로 6장에서는 연구 결과 및 향후 방향에 대하여 알아본다.

2. Ad-Hoc 네트워크에서의 보안 요구 사항

Ad-Hoc 네트워크의 특징에 대하여 알아보고 필요한 보

안 요구 사항을 도출하여 정리한다. Ad-Hoc 네트워크는 우선 사용자 디바이스의 가입과 탈퇴가 자유롭기 때문에 제 3자의 디바이스 접근이 용이하다. 이로 인해 디바이스 간의 인증 기술이 필요하다. 인증 기술 외에도 네트워크가 다른 디바이스의 연결로 이루어짐으로 유저간의 암호 통신이 필요하게 된다. 그러므로 암호 통신을 위한 키 설립이 요구된다. 다음의 내용은 각각의 요구 사항을 정리한 것이다.

○인증 : 통신의 디바이스가 정당한지 확인 할 수 있어야 하며, 제 3자의 위장을 발견할 수 있어야 한다.

○키 설립 : 통신의 디바이스간의 안전한 키 생성이 되어야 하며, 제 3자가 키를 유추하거나 동일한 키를 생성할 수 없어야 한다.

이와 같은 보안 기술은 기본적이며, 라우팅의 참여하는 디바이스의 경로를 안전하게 연결하는데 필요하다.

3. 연구 동향

Ad-Hoc 네트워크의 안전한 라우팅을 위한 연구는 크게 인증서를 이용하는 방안과 대칭키를 이용한 방안으로 나누어 분류할 수 있게 되며, 경로에 대한 해쉬를 제공하여 경로의 설정에 대하여 무결성을 제공하게 된다.

3.1 On Identifying malicious nodes in ad-hoc networks

AODV의 라우팅 방식을 변경할 것으로 선택된 경로를 확인하고 저장하는 방식을 이용한다. 라우팅을 통해 경로를 설정하게 되면 2홉 거리의 디바이스가 경로를 검증하게 된다. 이를 위해 메시지에 대한 MAC를 생성하게 된다. 메시지의 생성 방법은 홉 카운터, 노드간의 일렬 번호, 메시지 타입 그리고 메시지 인증 코드를 포함하고 있다. 2홉이 관계의 노드끼리 일렬 번호를 이용한 메시지를 작성하게 되게 이를 2홉이 떨어진 노드가 확인하게 된다. 이와 같은 방식으로는 각각의 노드가 키를 확인하기 위해 메시지를 수집하는데 어려움이 있으며, 응답 메시지를 확인하는 방안으로 진행 된다.

3.2 An overlay Approach to data security in ad-hoc networks

인증서를 이용하는 방식으로 각각 노드가 인증서를 이용하여 인증 및 데이터의 암호화 방식을 이용한다. 인증서를 이용하므로 공개키를 활용하게 됨으로 데이터의 인증에 어려운 방안이 된다. 인증 데이터를 제공하기 위해서는 서명을 제공하여야 하는데, 이 방식에서는 서명에 대한 언급이 없으며, 중간에 노드가 참여하여 인증서 검증 과정을 위장 할 수 있는 방법이 있다. 즉 새로 참여하는 노드에 대해서는 미리 참여하고 있는 노드가 인증서를 위장하여 제공할 수 있는 문제점을 내포하고 있다. 그러나 기존에 참여한 노드는 인증서를 사전에 저장하고 있으므로 보안에 대한 위와 같은 위장이 어려움이 존재한다.

3.3 Secure Neighborhood routing Protocol

이웃 노드 발견을 목적으로 하고 있으며, 인증서에 기반하여 전자 서명을 제공하게 된다. 그러므로 라우터의 등록과 IP 및 ID에 대하여 인증 코드를 제공하고 타임스탬프를 이용하여 패킷의 유효 시간을 제공하게 된다. 그러나 제 3자가 메시지를 변역하더라도 인증서와 전자 서명되는 데이터가 연결성이 없으므로 변경의 사항을 검토할 수 없는 방안이 된다. 그러므로 아이피나 식별자에 대한 변경을 알 수 있는 무결성 체크가 필요하다.

4. 제안 방식

위와 같이 연구의 동향이 노드간의 인증 및 키 분배의 어려움 그리고 라우팅 경로의 안전한 설정 방안에 대한 필요성이 제시됨으로 본 제안 방식에서는 사용자의 아이디와 디바이스의 일련 번호를 이용하여 세션키 설립 및 경로의 설정 방안에 대하여 논의한다. 위 연구 동향의 공통적인 가정 사항은 노드의 공유된 정보 및 공개키 인증서가 필요하다. 그러나 본 제안 방식에서는 공유된 정보가 없는 상태에서 안전하게 인증하는 방안과 키 설립하는 방안에 대하여 제시한다.

4.1 시스템 계수

본 제안 방식에서 이용되는 시스템 계수는 다음과 같다.

○* : 사용자

○ID* : 사용자의 아이디

○SN* : 사용자의 디바이스 일련 번호

○r* : 사용자가 선택한 난수

○r_*^{-1}: 사용자가 선택한 난수의 역수

○g : 모듈러 연산의 지수

○n : 모듈러 연산의 법수

○SK : 노드간의 세션키

4.2 사용자의 인증 및 세션키 설립

사용자의 인증 및 세션키 설립은 사용자의 아이디와 디바이스의 일련 번호의 지수승을 모듈러 연산을 통해서 이루어진다. 사용자의 인증 및 세션키 설립 단계는 다음과 같다.

step 1. 사용자(A)는 난수(r_a)를 생성하고 자신의 디바이스의 일련 번호(SN_a)와 다음과 같은 연산 값을 생성하여 상대방(B)에게 전송한다.

$$X = g^{SN_a r_a} \bmod n$$

step 2. B의 사용자도 다음과 같이 난수(r_b) 생성 및 디바이스의 일련 번호(SN_b)를 연산하여 A에게 전송한다.

$$Y = g^{SN_b r_b} \bmod n$$

step 3. A는 자신의 SN_a를 B로부터 전송 받은 Y에 지수승하여 연산한 결과를 전송한다.

$$Q_a = (Y)^{SN_a} = g^{SN_b r_b SN_a} \bmod n$$

step 4. B도 자신의 SN_b를 A로부터 전송 받은 X에 지수승한 결과를 전송한다.

$$Q_b = (X)^{SN_b} = g^{SN_a r_a SN_b} \bmod n$$

step 5. A의 세션키 생성 및 인증 데이터 전송

1) 세션키 생성

A는 B로 전송 받은 Q_b에 선택한 난수의 역수(r_a^{-1})를 지수승하여 세션키인 ($SK = g^{SN_a SN_b} \bmod n$)를 구할 수 있다.

$$SK = (Q_b)^{r_a^{-1}} = g^{SN_a r_a SN_b r_a^{-1}} \bmod n = g^{SN_a SN_b} \bmod n$$

2) 인증 데이터

A는 B로부터 인증을 받기 위해서 생성된 세션키에 ID_a를 지수승하고 아이디를 포함하여 전송한다.

$$O_a = (SK)^{ID_a} = g^{SN_a SN_b ID_a} \bmod n$$

step 6. B의 세션키 생성 및 인증 데이터 전송

1) 세션키 생성

B는 A로 전송 받은 Q_a에 선택한 난수의 역수(r_b^{-1})를 지수승하여 세션키인 ($SK = g^{SN_a SN_b} \bmod n$)를 구한다.

$$SK = (Q_a)^{r_b^{-1}} = g^{SN_a r_b SN_b r_b^{-1}} \bmod n = g^{SN_a SN_b} \bmod n$$

2) 인증 데이터

B는 A로부터 인증을 받기 위해서 생성된 세션키에 ID_b를 지수승하고 아이디를 포함하여 전송한다.

$$O_b = (SK)^{ID_b} = g^{SN_a SN_b ID_b} \bmod n$$

step 7. A의 B의 인증은 세션키(SK)에 전송 받은 아이디를 지수승하여 인증 데이터 O_b가 동일하게 생성되는지 검증한다.

B도 Step 7의 단계를 A와 동일하게 진행한다.

4.3 안전한 라우팅의 데이터 통신

Ad-Hoc 네트워크에 참여하는 노드는 서로의 연결 상태를 확인하고 통신의 경로를 확인하여 4.2를 이용하여 인증 및 키 생성을 이루어 안전한 통신을 제공한다. 노드간의 라우팅의 메시지는 다음과 같이 이루어진다.

○메시지의 종류 : 요청 및 응답 메시지의 종류를 표현(요청 : request, 응답 : response)

○출발 ID : 통신을 요청하는 디바이스의 ID

○도착 ID : 통신의 대상 디바이스 ID

○경유 ID : 경유하는 디바이스 ID

○H( ) : 경유하는 아이디에 대한 해쉬 값

○X : 출발하는 디바이스의 4.2에 해당하는 값

○Y : 도착 ID의 4.2에 해당하는 값

○ Q_a: 4.2의 출발하는 디바이스의 값

○ Q_b: 4.2의 응답하는 디바이스의 값

○SK : 출발 응답하는 디바이스사이의 세션키

step 1. 출발 디바이스A는 다음과 같이 메시지를 구성하여 근처의 디바이스들에게 브로드캐스팅 한다.

$request, ID_a, ID_b, X$

step 2. 근처 디바이스 전송 받은 데이터에 4.2의 Y 값을 전송하고, Q의 값을 생성하여 전송한다.

$response, ID_a, ID_b, Y, Q_b$

step 3. A노드는 다음과 같이 SK를 생성하여 HMAC의 키로 이용하여 데이터를 전송한다.

$request, ID_a, ID_b, H_{SK}[ID_a \| ID_b], Q_a$

step 4. B노드는 응답으로 동일한 키를 생성하여 해쉬 값을 검증하게 되고 A의 노드 메시지를 다음 노드로 전송하게 된다.

$request, ID_a, ID_b, ID_c, X$

step 5. C노드는 앞의 B노드와 동일하게 응답으로 Y와 Q의 값을 생성하여 전송하고 이를 받은 A 노드는 동일하게 응답 값 및 해쉬 값을 전송하여 안전한 경로를 확보하게 된다.

이와 같은 과정을 통해서 안전한 라우팅 경로를 확보하여 대칭키를 이용하여 암호화 메시지를 전송할 수 있다.

5. 제안 방식 분석

제안 방식에 대하여 다음과 같이 제 3자의 공격에 대하여 검토하여 검증하게 된다.

5.1. 메시지의 수정을 이용한 공격

4.2의 제안 방식을 보면 메시지의 무결성을 제공하지 못하므로 메시지를 수정하여 전송할 수 있는 확률이 존재한다. 즉 제 3자가 X값을 생성하거나 바꾸거나 다른 값으로 변경을 시도할 수 있다. 그러나 이를 방지하기 위해서 사용자의 난수를 이용하고 있다. 다음의 X값을 변경하였을 경우를 가정하면 다음과 같이 검증할 수 있다.

$X = g^{SN_a r_a} \bmod n$: 정당한 사용자가 생성한 값

$X' = g^{SN_a r'_a} \bmod n$: 제 3자가 지수승 값을 변경한 사항

X'를 B가 이용하여 생성하는 값은 Q_b이고 수정된 것으로 인해서 Q_b는 다음과 같이 생성 된다.

$$Q'_b = (X)^{SN_b} = g^{SN_a r'_a SN_b} \bmod n$$

이와 같은 값에서 r'_a의 역수는 이전 값에서 변경되었기 때문에 동일한 SK를 만들 수 없으므로 이후 인증 데이터의 O_a가 인증 하지 못하게 된다. 그러므로 메시지의 수정의 내용을 할 수 있게 된다.

5.2 메시지 생성을 이용한 공격

X의 메시지를 아예 새로 생성하여 난수의 역수를 모두 알 수 있는 경우이다. 이때 문제되는 것은 디바이스의 일련번호를 얻을 수 없다는 것이다. 즉 SN의 값을 획득하여야 하는데 이는 이미 초기 단계부터 사용자의 선택된 난수로 값이 숨겨져 있다. 그러므로 제 3자는 SN의 값을 위조할 수 없는 상태이다.

5.3 위장

1) 제 3자의 위장

제 3자가 인증을 받기 위해서는 최종 인증 데이터 O_a를 생성하여 전송하면 된다. 우선 O_a는 다음과 같이 이루어져 있다.

$$O_a = (SK)^{ID_a} = g^{SN_a SN_b ID_a} \bmod n$$

인증 데이터는 세션키를 획득하면 가능 한다. 그러나 세션키는 평문 메시지로 노출되어 전송되지 않으며 서로 난수를 제거하여 생성(4.2의 5단계)하고 ID를 지수승한 값을 전송하므로 자신의 보유하고 있는 SK값에 ID를 지수승하므로 생성하게 된다. 그러므로 위장하기 위해서 인증데이터를 생성하기 위해서는 SK의 값을 획득할 수 있어야 하나 이는 지수승의 난수 제거 및 SN을 획득하는 방안(5.2에서 설명)이 필요하다. 그러므로 제 3자의 위장은 매우 어렵다.

2) 이전 통신 디바이스의 위장

이전 통신 디바이스가 악의적인 목적을 가지고 위장을 시도할 수 있다. X의 값과 상대방의 아이디를 알고 있으므로 X의 값과 상대방의 아이디를 전송할 수 있다. 여기 중요한 점은 난수의 역수를 제거하는 방안이 된다. 역수를 알지 못한 상태에서 제거를 할 수 없고 지수의 값을 알아낼수 없으므로 지수의 SN을 구할 수 없다. 그로 인해 이전 통신의 디바이스의 위장 또한 어렵다.

이와 같이 세션키의 설립과 인증에 있어 공유 정보 없이 생성이 가능하므로 다른 연구에 비하여 가정 사항이 줄어들고 공개키 기반을 활용하지 않으므로 인해 참가 디바이스의 연산 능력을 고려할 수 있게 된다. 또한 네트워크 망에 참여하는 모든 노드들이 세션키 설립에 있어서도 상대방의 SN 넘버를 획득하지 이미 부정한 방법의 인증 데이터의 생성도 막을 수 있다.

6. 결론 및 향후 연구

본 연구를 통해서 사용자는 디바이스의 일련 번호와 난수 그리고 아이디를 이용하여 세션키 설립 및 인증을 제공할 수 있다. 이로 인해 Ad-Hoc 네트워크의 임의 접근에서도 안전한 방안을 제시할 수 있는 연구이다. 본 연구를 서비스 및 데이터 전송의 안전성을 제공하면서, 디바이스의 효율성을 높일 수 있는 방안이 된다. 하지만 향후 연구로는 통신에 이용되는 통신 횟수를 줄 일 수 있는 방안이 필요하다. 공유 정보가 없는 관계로 적어도 통신은 요청과 응답 과정으로 크게 3단계 6번의 통신(각 단계마다 두 번의 통신)이 필요하다. 이와 같은 통신량의 증가는 유동성을 제공하는 네트워크 환경에서는 부담이 될 수 있는 상황이다. 부담이 되는 것은 이전 중간 경로의 노드가 갑자기 통신로를 빠져나가는 상황을 말한다. 그러므로 향후의 연구에서는 통신 횟수의 줄일 수 있는 방안에 대한 연구가 진행되어야 할 것으로 사료된다.

참고문헌

[1]Xu-su and Rajendra v.boppana, "On identifying malicious nodes in ad hoc networks", IWCMC'07, pp.12-16

[2]Jorg liebeherr and guangyu dong, "an overlay approach to data security in ad-hoc networks"

[3]Ajay jadav and eric e.johnson, "secure neighborhood Routing protocol"

[4]강서일, 이임영,"Ad-Hoc환경에서의 경로에 따른 암호화 키에 대한 연구", 한국멀티미디어학회 학술 대회, 2007

[5]박영호, 이경근, 이상곤, 문상재, "무선 Ad Hoc 네트워크에서의 안전한 라우팅 프로토콜에 관한 연구," 정보보호학회 논문지, 제 15권 3호, pp76-81, 2005. 06

[6]이석래, 송주석, "모바일 Ad-hoc 네트워크에서 Hamming Distance를 이용한 인증프로토콜," 정보보호학회 논문지, 제 16권 5호, pp47-56, 2006. 10

[7]이원희, 구재형, 이동훈, "Ad-Hoc환경에서의 2-라운드 비대칭 키 공유 기법," 한국정보보호학회 하계정보보호학술대회, vol 13, No 1, pp89-92

[8]임지환, 김상진, 오희국, "애드혹 위치기반 라우팅을 위한 안전한 위치 서비스," 한국정보보호학회 하계정보보호학술대회 논문집, vol 16, No.1, pp665-669, 2006

[9]조우원, 김범한, 이동훈, "애드 혹 네트워크를 위한 거리기반 인증된 키 교환 기법," 한국정보보호학회 하계정보보호학술대회 논문집, Vol 16, No.1, pp.661-664, 2006.