무선센서 네트워크에서 경량화된 인증과 키 동의 프로토콜☆

A Lightweight Authentication and Key Agreement Protocol in Wireless Sensor Networks

윤 신 숙* 하 재 철**
SinSook Yoon JaeCheol Ha

요 약

최근 다양한 분야에서 응용되고 있는 무선 센서 네트워크에서는 무선 통신으로 인한 보안 측면에서의 취약성을 극복하기 위한 연구가 진행 중이다. 무선 센서 네트워크에서의 안전한 통신을 보장하기 위해서는 기본적으로 센서 노드들의 키 관리, 센서 노드들의 상호 인증과 키 동의 프로토콜이 제공되어야 한다. 이러한 보안 서비스를 지원하기 위한 일부 프로토콜들이 제안되었지만 많은 메모리와 계산량 그리고 통신량이 요구되기도 하였다. 본 논문에서는 Juang이 제안한 센서 노드간 인증 및 키 공유 기법을 개선하여 보다 경량화되고 효율적인 프로토콜을 제시한다. 기존 방식에서는 센서간의 키 동의를 위한 센서 정보를 등록 센터까지 전송하였으나 제안 방식에서는 베이스 스테이션까지만 전송하도록 개선함으로써 공유키 설정에 필요한 통신량과 계산량을 개선하였다.

Abstract

Recently, there are many researches on security to remove vulnerability which is caused by wireless communication in wireless sensor networks. To guarantee secure communication, we should basically provide key management for each node, mutual authentication and key agreement protocol between two nodes. Although many protocols are presented to supply these security services, some of them require plentiful storage memory, powerful computation and communication capacity. In this paper, we propose a lightweight and efficient authentication and key agreement protocol between two sensor nodes, which is an enhanced version of Juang's scheme. In Juang's protocol, sensor node's information used to share a secret key should be transmitted to registration center via a base station. On the contrary, since node's information in our protocol is transmitted up to only base station, the proposed scheme can decrease computation and communication cost for establishing the shared key between two nodes.

keyword : Authentication, Key Agreement, WSN

1. 서 론

무선 센서 네트워크는 실시간 트래픽 모니터링이나 빌딩의 안전성, 화재발생 등을 모니터링하고, 군사적 자료수집, 지진 활동의 분산 측정, 실시간 오염측정 등 넓은 분야에서 적용될 수 있다. 무선 센서 네트워크는 초소형 센서들로 구성되기 때문에 저장 메모리, 연산량, 에너지, 통신 반경 등의 제약이 따른다. 센서들이 적대적 환경에 노출될 수도 있고 무선 통신을 쉽게 도청할 수 있으며, 악의적인 공격자가 메시지를 변조하거나 재전송 공격을 시도할 수도 있기 때문에 안전한 무선 통신을 제공하는 것이 매우 중요하다.

안전한 무선 센서 네트워크의 통신을 위하여 키 관리 방법에 대한 다양한 연구가 진행되어 왔

* 정 회 원 : 호서대학교 컴퓨터공학과 박사과정
yss28@hanmail.net
** 종신회원 : 호서대학교 정보보호학과 부교수
jcha@hoseo.edu(교신저자)
[2008/07/14 투고 - 2008/07/15 심사 - 2008/11/06 심사완료]
☆ 이 논문은 2008년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임(과제번호 :20080155)

다. 무선 센서 네트워크 환경에서는 베이스 스테이션(Base Station, BS)과 노드, 혹은 노드간 인증과 키 동의가 안전하게 이루어져야 함은 물론 효율적인 구현을 위한 다음과 같은 요구 사항이 고려되어야 한다.

1) 유연한 공유 키 생성 : 노드의 수가 증가해도 그에 관계없이 공유키 생성이 용이해야 한다.
2) 단일 등록 : 노드는 키 등록 센터에 한 번만 등록하면 다른 통신자와 세션키 교환 등을 쉽게 할 수 있어야 한다.
3) 자유로운 패스워드 선택 : 센서 노드의 배터리 교체나 초기화시 패스워드 선택이 자유롭게 할 수 있어야 한다.
4) 적은 통신량과 연산량 : 노드는 높은 대역폭과 많은 연산량을 제공할 수 없다는 점을 고려하여 적은 통신량과 연산량을 가지도록 한다.
5) 동적 참여 : 기존 노드가 설치되었을 때 새로운 노드를 추가하는데 문제가 없어야 한다.
6) 동기화 : 노드의 능력이 제한되므로 가급적 노드들 사이에 동기화에 필요한 시간정보가 사용되지 않는 것이 유용하다.

Perrg 등이 제안한 SPINS는 SNEP과 μTESLA으로 구성되어 있는데 SNEP은 데이터의 기밀성(confidentiality), 인증(authentication), 무결성(integrity), 신규성(freshness)을 제공하는 일대일 통신이고, μTESLA는 베이스 스테이션으로부터 인증된 브로트캐스트를 제공한다[1]. SNEP에서 노드는 베이스 스테이션과 공유하는 하나의 마스터 키를 사용하고 있다. 그러나 μTESLA는 모든 노드들이 시간 동기화가 필요하고 실제 네트워크 전송 지연이 있을 수 있어 이를 고려한 키 노출 지연시간의 설정이나 패킷을 저장하기 위한 추가 동간 등이 요구되는 단점이 있다. Huang 등이 제안한 타원곡선 암호체계와 대칭키 암호체계를 결합한 혼합 인증 키 생성 방식을 제안 하였으나 공개키 방식을 사용함으로써 아직까지는 구현상의 부담이 크며 연산량이 많아지는 단점이 있다[2]. 또한, LEAP에서는 노드가 배치될 때 일시적으로 초기 비밀 키를 사용하여 인접 노드와의 공유 키 쌍을 설정한다. 일정 시간동안 공유 키 쌍을 만든 후 공격자의 공격이 시작되기 전에 초기 비밀 키를 삭제하는 방법을 사용한다. 이 방식은 공유키를 만드는 시간이 노드 배치 후 일정하게 제한되며 그 동안에는 공격자의 공격이 없어야 한다는 제한 요소가 있다[3]. Chan 등이 제안한 PIKE는 두 센서 노드 사이에 사전에 분배된 키를 공유하는 신뢰할 수 있는 중간 노드를 사용한다. 신뢰할 수 있는 중간 노드는 두 노드와 공유된 키를 교환할 수 있지만, 일부 센서 노드가 노출될 때는 수동적, 능동적 공격에 취약한 특성이 있다[4].

또한, 최근 Juang은 WISA-2007에서 등록 센터(Registration Center, RC)에서 센서 노드간의 키 동의 정보를 전송하는 형태의 인증 및 키 동의 프로토콜을 제안하였다[5]. 지금까지 연구 결과의 장단점을 분석한 결과 Juang의 방법은 안전성과 구현의 효율성면에서 많은 장점을 가지고 있다. 하지만 가장 큰 문제는 노드간의 세션키 공유 등을 위한 모든 통신이 등록 센터까지 전송된다는 점이다. 이로 인해 통신량과 계산량이 현격하게 증가되는 단점을 가지고 있었다.

따라서 본 논문에서는 Juang 방식이 가지는 장점을 대부분 유지하면서 통신량과 계산량을 줄일 수 있는 방법을 연구하였다. 본 논문의 핵심은 노드간의 세션키 공유 등을 위한 통신이 베이스 스테이션까지만 전송하도록 개선함으로써 결국 공유키 설정을 위한 통신량과 계산량을 개선하였다. 그리고 센서 노드가 해당 베이스 스테이션을 벗어나는 경우 그에 따른 비밀키를 갱신하도록 프로토콜을 설계하였다. 2장에서 기존에 관련 연구를 살펴보고, 3장에서 효율적인 인증과 키 공유에 대한 제안을 하고, 4장에서는 안전성과 효율성을 비교 분석한 후 5장에서 결론을 맺도록 한다.

2. 관련 연구

무선 센서 네트워크에서 센서 노드들은 주기적 신호를 전송하여 가장 가까운 베이스 스테이션을 찾고, 라우팅 토폴로지를 형성한다. 통신 반경 안에 있는 이웃 노드들과 자체 네트워크를 구성한다. 베이스 스테이션은 노드들에게 메시지를 보내고 센서 노드들의 라우팅을 다루고, 등록 센터와 비밀키를 공유할 수 있다. 등록 센터는 키 분배 센터로도 불리며 키와 네트워크를 관리하며 외부 네트워크에도 연결할 수 있다. Juang의 논문에서는 베이스 스테이션과 등록 센터는 계산과 통신 능력이 우수하며 안전하고 신뢰성 있다고 가정하였다. 또한, 통신 유형을 다음과 같이 다섯 가지로 구분하였는데 여기에서는 노드와 노드, 노드와 베이스 스테이션간의 통신을 집중적으로 다룬다.

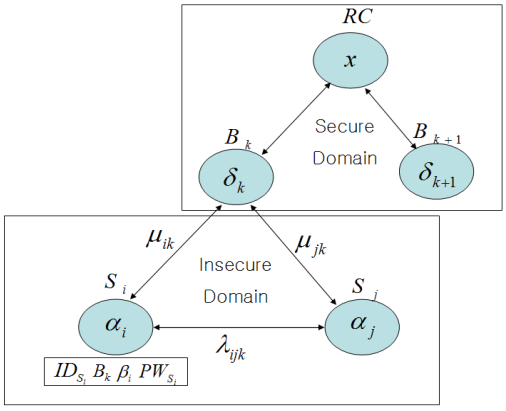
(1) 노드→베이스 스테이션: sensor reading
(2) 베이스 스테이션→노드: request
(3) 노드→노드: self-organizing network
(4) 베이스 스테이션→노드들: queries
(5) 노드→노드들: 브로드캐스트, 라우팅 정보 업데이트

2.1 용어 및 표기

무선 센서 네트워크에서 인증과 키 동의에 필요한 기호는 다음과 같다.

S_i : 센서 노드 i
B_k : 베이스 스테이션 k
RC : 등록 센터(Registration Center)
ID_{S_i} : S_i의 ID
PW_{S_i} : S_i의 패스워드
ID_{B_k} :B_k의 ID
$\|$: 연접(concatenation) 연산자
$\oplus$: XOR 연산자
h : 일방향 함수
x : 센터의 마스터 키
δ_k : B_k의 비밀키, $h(x\|ID_{B_k})$
α_i : S_i의 비밀키, Juang 방식에서는 $h(x\|ID_{S_i})$
제안 방식에서는 $h(\delta_k\|ID_{S_i})$로 계산
μ_{ik} : S_i와 B_k의 공유키, $h(\alpha_i\|ID_{B_k})$
λ_{ijk} : S_i와 S_j의 공유키, $h(\mu_{ik}\|ID_{S_j})$

위의 기호와 정의를 바탕으로 무선 센서 네트워크 구조와 사용되는 키를 나타낸 것이 그림 1이다. 본 논문에서는 센서 노드나 베이스 스테이션이 일정 공간에 고정된 고정형(static) 무선 센서 네트워크를 가정하며 노드는 보안 위협에 취약하지만 베이스 스테이션과 등록 센터는 통신 능력과 계산 능력이 우수하고 신뢰성 있게 보호 된다는 것을 전제로 한다[1,3,4,5]. 즉, 그림 1에서 보는 바와 같이 노드 자체와 베이스 스테이션과의 통신 구간은 공격자의 위협으로부터 안전하지 않음을 가정한다.



(그림 1) 무선 센서 네트워크에서 사용되는 키

2.2 무선 센서 네트워크에서 인증과 키 동의

Juang이 제안한 인증 및 키 동의 프로토콜을 살펴보면 다음과 같다[5]. 마스터 키 x는 등록 센터에 의해 안전하게 보호된다. 베이스 스테이션 B_k와 등록 센터 RC는 비밀키 $\delta_k = h(x \| ID_{B_k})$를 공유한다.

1) 등록 단계

센서 노드 S_i가 자신의 ID_{S_i}와 패스워드 PW_{S_i}를 RC에 보내 등록을 요청한다. RC는 S_i의 비밀정보 $\alpha_i = h(x||ID_{S_i})$ 와 $\beta_i = \alpha_i \oplus PW_{S_i}$를 계산한다. 센서 노드의 EEPROM에 ID_{S_i}와 β_i를 저장하여 초기화 한다. 이 센서 노드는 초기화된 후에 PW_{S_i}를 입력할 수 있고, 센서 노드는 $\alpha_i = \beta_i \oplus PW_{S_i}$를 계산하여 RAM에 저장한다. 그리고 배터리 교체나 전원이 꺼져 지워지는 경우, 패스워드 PW_{S_i}를 다시 입력하여 α_i를 계산할 수 있다.

2) 공유키 설정 단계

센서 노드 S_i가 다른 센서 노드 S_j와 안전한 통신을 원한다면, S_i와 S_j는 인증과 키 동의를 위해서 비밀키 λ_{ijk}를 공유해야 한다. 또한 S_i와 B_k는 인증과 키 동의를 위해서 비밀키 μ_{ik}를 공유해야 한다. S_i는 α_i, ID_{B_k}, ID_{S_j}로부터 공유된 비밀키 $\mu_{ik} = h(\alpha_i||ID_{B_k})$, $\lambda_{ijk} = h(\mu_{ik}||ID_{S_j})$를 계산할 수 있다. 즉, 통신을 먼저 원하는 당사자 S_i는 모든 공유키를 만들 수 있다.

그러나 B_k는 μ_{ik}를 계산할 수 없어 RC에 요청해서 받을 수 밖에 없다. 그림 2는 노드 S_i와 베이스 스테이션간의 공유 키 μ_{ik}를 만드는 과정을 나타낸 것이다. 또한 S_j가 공유키 λ_{ijk}를 가지고 있지 않다면, B_k에 요청을 해서 받아야 하는데 B_k도 λ_{ijk}를 계산할 수 없어 RC에 요청해서 μ_{ik}를 받을 수 밖에 없다. 즉, 여기서 문제의 핵심은 베이스 스테이션에서 노드의 비밀키 α_i를 모르기 때문에 μ_{ik}를 계산할 수 없어 이를 얻기 위해 항상 등록 센터와 통신을 해야 한다는 점이다. 이것이 Juang 방식에서 프로토콜이 복잡하게 되는 원인이 된다.

그림 3은 S_j가 S_i와 공유키 동의를 위한 프로토콜이며 이를 도시한 것이다. 여기서 KR은 키 요구 메시지이고 N_i는 신규성(freshness)을 제공하기 위한 파라미터이다. 여기서 3단계까지는 베이스 스테이션이 등록 센터로부터 μ_{ik}를 전송받기 위한 과정이고 4단계는 S_j에게 λ_{ijk}를 전송하는 단계이다.

1단계: $S_j \rightarrow B_k : N_1, ID_{S_i}, ID_{S_j}$

2단계: $B_k \rightarrow RC : N_2, ID_{B_k}, E_{\delta_k}(ID_{S_i}, KR, h(ID_{S_i} \| ID_{B_k} \| KR \| N_2))$

3단계: $RC \rightarrow B_k : E_{\delta_k}(\mu_{ik}, h(ID_{s_i} \| ID_{B_k} \| KR \| N_2 \| \mu_{ik}))$

4단계: $B_k \rightarrow S_j : E_{\mu_{jk}}(\lambda_{ijk}, h(ID_{S_i} \| ID_{B_k} \| ID_{S_j} \| KR \| N_1 \| \lambda_{ijk}))$

추가적으로 만약 베이스 스테이션이 S_j와의 공유키 μ_{jk}를 알지 못하고 있었다면 한번 더 단계 2와 3을 거쳐 등록 센터로부터 전송받아야 한다. 따라서 베이스 스테이션은 두 노드간의 키 공유를 위해 등록 센터와 최소 1회, 최대 2회까지 통신을 해야 한다.

S_i	B_k	RC
$[ID_{S_i}][ID_{B_k}][\beta_i]$	$[ID_{B_k}][\delta_k]$	$[ID][x]$
$ID_{S_i} \rightarrow$	$N_2, ID_{B_k},$	
$\mu_{ik} = h(\alpha_i \| ID_{B_k})$	$E_{\delta_k}(ID_{S_i}, KR, h(ID_{S_i} \| ID_{B_k} \| KR \| N_2))$	$\rightarrow \mu_{ik} = h(\alpha_i \| ID_{B_k})$
		$\leftarrow E_{\delta_k}(\mu_{ik}, h(ID_{s_i} \| ID_{B_k} \| KR \| N_2 \| \mu_{ik}))$
	μ_{ik}	

(그림 2) Juang의 노드-베이스 스테이션간 공유키 설정 기법

S_i	S_j	B_k	RC
$[ID_{S_i}][ID_{B_k}][\beta_i]$	$[ID_{S_j}][ID_{B_k}][\beta_j]$	$[ID_{B_k}][\delta_k]$	$[ID][x]$
$\mu_{ik}=h(\alpha_i\|\|ID_{B_k})$	$N_1, ID_{S_i}, ID_{S_j} \rightarrow$	$N_2, ID_{B_k},$	
			$\rightarrow \quad \mu_{ik}=h(\alpha_i \parallel ID_{B_k})$
$\lambda_{ijk}=h(\mu_{ik}\|\|ID_{S_j})$		$E_{\delta_k}(ID_{S_i}, KR, h(ID_{S_i} \parallel ID_{B_k} \parallel KR \parallel N_2))$	
			$\leftarrow E_{\delta_k}(\mu_{ik}, h(ID_{s_i} \parallel ID_{B_k} \parallel KR \parallel N_2 \parallel \mu_{ik}))$
		$\lambda_{ijk}=h(\mu_{ik} \parallel ID_{S_j})$	
		$E_{\mu_{jk}}(\lambda_{ijk}, h(ID_{S_i} \parallel ID_{B_k} \parallel ID_{S_j} \parallel KR \parallel N_1 \parallel \lambda_{ijk}))$	
	$\lambda_{ijk} \quad \leftarrow$		

(그림 3) Juang의 노드간 공유키 설정 기법

3) 노드와 베이스 스테이션간 인증 및 세션키 동의

S_i와 B_k 사이의 세션키는 각각 랜덤수를 생성하고 공유키 μ_{ik}를 이용하여 생성한다. 랜덤값 ru_n, rs_n은 세션키 $sk_n=h(ru_n \parallel rs_n \parallel \mu_{ik})$를 생성하기 위한 값이고, N_3, N_4는 메시지의 신규성을 확인하기 위한 것이다. 즉, 세션키를 계산하기 전에는 상호인증을 위해 다음과 같은 단계를 가진다.

1단계: $S_i \rightarrow B_k : N_3, ID_{S_i}, E_{\mu_{ik}}(ru_n, h(N_3 \parallel ID_{S_i} \parallel ID_{B_k} \parallel ru_n))$

2단계: $B_k \rightarrow S_i : N_4, E_{\mu_{ik}}(rs_n, h(N_3 \parallel N_4 \parallel ID_{S_i} \parallel ID_{B_k} \parallel rs_n))$

3단계: $S_i \rightarrow B_k : E_{sk_n}(N_4+1)$

4) 노드간 인증 및 세션키 동의

S_i와 S_j사이의 세션키도 위와 비슷한 방법으로 생성된다. 단지 세션키 설정에 사용되는 공유키가 λ_{ijk}라는 것만 다르다. S_i와 S_j는 랜덤값 ru_n, rs_n을 생성 후 서로 교환한 후, 세션키 $sk_n=h(ru_n \parallel rs_n \parallel \lambda_{ijk})$를 생성한다.

Juang 방식은 통신을 위한 센서들 사이에 공유키 생성과 키 관리가 쉬우며, 베이스 스테이션을 이용한 키 동의 및 인증을 효율적으로 할 수 있다. 그리고 새로운 센서 노드의 추가나 삭제가 가능할 수 있다.

그러나 연산량과 통신량이 비교적 많아지게 된다. 그 이유를 분석해 보면 위에서 언급한 바와 같이 노드간의 모든 공유키 생성을 위해 베이스 스테이션은 최대 2회까지 등록 센터를 거쳐야 하므로 통신 부하 및 계산량이 많아지게 된다. 또한, 노드와 베이스 스테이션간의 공유키 설정시에도 등록 센터와 통신해야 하므로 통신량 증가가 필연적이다. 결국, 노드가 베이스 스테이션이든 다른 노드와 통신을 하는 경우든지 중간에 위치한 베이스 스테이션은 매 세션마다 등록 센터와 통신해야 하므로 등록 센터는 상당한 부담을 갖게 된다.

3. 효율적인 인증과 키 동의 기법

Juang 기법은 공유키 생성에서 베이스 스테이션이 노드와의 공유키 μ_{ik}를 가지고 있지 않으면 등록 센터 RC에 등록을 요청하고 확인해야 하는 번잡함이 있다. 따라서 본 논문에서는 베이스 스테이션의 비밀키를 이용하여 이 센서 노드와의 공유키를 생성하게 하여 연산량과 통신량을 줄일 수 있는 방식을 제안한다.

3.1 인증 및 키 동의 프로토콜

개선 방식의 핵심은 베이스 스테이션에도 신뢰

할 수 있으므로 노드의 ID_{S_i}를 알면 비밀키를 생성할 수는 있도록 한 것이다. 그러나 노드가 정해진 베이스 스테이션하에서 다른 곳으로 이동할 경우에는 키 갱신이 필요하며 이때 키 갱신은 기등록 센터에서만 수행하도록 설계하였다.

마스터 키 x는 등록 센터 RC에 의해 안전하게 보호된다. 베이스 스테이션 B_k와 등록 센터 RC는 비밀키 $\delta_k = h(x \| ID_{B_k})$를 공유한다.

1) 등록 단계

센서 노드 S_i는 자신의 ID_{S_i}와 패스워드, PW_{S_i}를 RC에 보내 등록 을 요청한다. RC는 S_i의 비밀 정보 $\alpha_i = h(\delta_k \| ID_{S_i})$와 $\beta_i = \alpha_i \oplus PW_{S_i}$를 계산한다. 여기에서 RC는 노드의 비밀키 α_i를 계산할 때 Juang의 방식과 달리 RC의 마스터 키를 이용하지 않고 해당 베이스 스테이션의 비밀키 δ_k를 사용한다는 점이다. 센서 노드는 EEPROM에 ID_{S_i}, PW_{S_i}, β_i 그리고 ID_{B_k}를 저장하고 RAM에 α_i를 계산하여 둠으로써 초기화 과정을 마친다.

2) 공유키 설정 단계

노드와 베이스 스테이션간의 공유 키 설정은 아주 간단하다. 베이스 스테이션은 노드로부터 ID_{S_i}만 받으면 자신의 비밀키를 이용하여 공유키 α_i를 바로 계산할 수 있다. 이를 나타낸 것이 그림 4이다.

센서 노드 S_i가 다른 센서 노드 S_j와 안전한 통

S_i	B_k
$[ID_{S_i}][ID_{B_k}][\beta_i]$	$[ID_{B_k}][\delta_k]$
$ID_{S_i} \rightarrow$ α_i	$\alpha_i = h(\delta_k \| ID_{S_i})$

(그림 4) 제안하는 노드-베이스 스테이션간 공유키 설정 기법

신을 원한다면, S_i와 S_j는 인증과 키 동의를 위해 비밀키 λ_{ijk}를 공유해야 한다. S_i는 자신의 비밀키와 ID_{S_j}정보만으로 공유키 $\lambda_{ijk} = h(\alpha_i \| ID_{S_j})$를 만들 수 있다. 반면, S_j가 공유키 λ_{ijk}를 가지고 있지 않다면, B_k에 요청을 한다. B_k는 δ_k를 이용하여 S_i의 비밀키 $\alpha_i = h(\delta_k \| ID_{S_i})$와 $\lambda_{ijk} = h(\alpha_i \| ID_{S_j})$를 생성할 수 있다. B_k는 센서 노드 S_j에게 공유키 λ_{ijk}를 α_j로 암호화시켜 전송하면 S_j노드는 자신의 비밀키 α_j로 복호화하여 센서 노드 사이의 공유키 λ_{ijk}를 얻을 수 있다. 요약하면 다음과 같은 단계를 가지며 이를 나타낸 것이 그림 5이다.

1단계: $S_j \rightarrow B_k : N_1, ID_{S_i}, ID_{S_j}$

2단계: $B_k \rightarrow S_j$:

$E_{\alpha_j}(\lambda_{ijk}, h(ID_{S_i} \| ID_{B_k} \| ID_{S_j} \| KR \| N_1 \| \lambda_{ijk}))$

3) S_i와 B_k 사이의 인증 및 세션키 동의

S_i와 B_k 사이에는 α_i와 랜덤값, ru_n, rs_n을 이용하여 세션키, $sk_n = h(ru_n \| rs_n \| \alpha_i)$을 생성할 수 있다.

1단계: $S_i \rightarrow B_k : N_3, ID_{S_i}$,

$E_{\alpha_i}(ru_n, h(N_3 \| ID_{S_i} \| ID_{B_k} \| ru_n))$

2단계: $B_k \rightarrow S_i : N_4$,

$E_{\alpha_i}(rs_n, h(N_3 \| N_4 \| ID_{S_i} \| ID_{B_k} \| rs_n))$

3단계: $S_i \rightarrow B_k : E_{sk_n}(N_4 + 1)$

이 기법은 Juang의 기법과 동일하며 단지 sk_n을 만들 때 $sk_n = h(ru_n \| rs_n \| \mu_{ik})$을 사용하던 것을 $sk_n = h(ru_n \| rs_n \| \alpha_i)$와 같이 만든다는 점이다. 따라서 베이스 스테이션에서 α_i를 구하는데 RC에 문의하지 않고 바로 구할 수 있다는 장점을 이용한 것이다.

4) S_i와 S_j사이의 인증 및 세션키 동의

S_i와 S_j사이의 세션키를 만들기 위해 공유키 λ_{ijk}를 이용하게 되는데, 먼저 랜덤값 ru_n, rs_n을 인증해야 한다. 그리고 두 노드는 아래 인증 과정

S_i	S_j	B_k
$[ID_{S_i}][ID_{B_k}][\beta_i]$	$[ID_{S_j}][ID_{B_k}][\beta_j]$	$[ID_{B_k}][\delta_k]$
$\lambda_{ijk}=h(\alpha_i\|\|ID_{S_j})$	$N_1, ID_{S_i}, ID_{S_j} \rightarrow$	$\alpha_i=h(\delta_k \parallel ID_{S_i})$
		$\lambda_{ijk}=h(\alpha_i \parallel ID_{S_j})$
	$\lambda_{ijk} \quad \leftarrow$	$E_{\alpha_j}(\lambda_{ijk}, h(ID_{S_i} \parallel ID_{B_k} \parallel ID_{S_j} \parallel N_1 \parallel \lambda_{ijk}))$

(그림 5) 제안하는 노드간 공유키 설정 기법

을 마친 후 세션키, $sk_n=h(ru_n \parallel rs_n \parallel \lambda_{ijk})$ 계산한다.

1단계: $S_i \rightarrow S_j : N_5, ID_{S_i}, ID_{S_j}$
$E_{\lambda_{ijk}}(ru_n, h(N_5 \parallel ID_{S_i} \parallel ID_{S_j} \parallel ru_n))$

2단계: $S_j \rightarrow S_i : N_6$,
$E_{\lambda_{ijk}}(rs_n, h(N_5 \parallel N_6 \parallel ID_{S_i} \parallel ID_{S_j} \parallel rs_n))$

3단계: $S_i \rightarrow S_j : E_{sk_n}(N_6+1)$

3.2 노드의 비밀키 갱신 프로토콜

공유키 설정 단계에서 노드는 자신의 정보를 베이스 스테이션에게 전송하게 되는데 베이스 스테이션은 자신의 영역에 속한 노드인지를 먼저 판단한다. 만약, 자신의 영역에 속한 노드라면 위의 키 공유나 키 동의 프로토콜을 진행하지만 자신의 영역에 속하지 않은 노드는 RC를 통해 키 갱신을 하여야 한다. 만약, 하나의 노드가 그 전에 B_k영역에서 B_k' 영역으로 옮겨졌다고 가정하자. 이 경우 노드 S_i는 α_i를 $h(\delta_k \| ID_{s_i})$에서 $h(\delta_k' \| ID_{s_i})$로 갱신하여야 한다. 그러나 이 경우 키를 갱신하는 것이 새로운 베이스 스테이션이 아니라 RC에서만 가능하도록 설계하였다.

노드의 키 갱신이 필요한 경우는 다음과 같다. 첫째, 노드를 처음 설치하거나 위치시킬 때 원하는 베이스 스테이션의 통신 영역에 배치되지 않았거나 혹은 원하는 베이스 스테이션의 통신 신호가 미약하여 인접한 이웃 베이스 스테이션의 신호가 더 강한 경우

둘째, 관리자가 사용했던 노드를 인위적으로 다른 곳으로 위치시켜 노드를 재사용할 필요가 있을 때 그 노드를 다른 베이스 스테이션 영역에 가서 사용할 경우

셋째, 베이스 스테이션이 고장이나 파괴로 인해 다시 설치해야 할 경우 새로운 키를 사용하는 베이스 스테이션을 사용할 경우

키 갱신이 필요한 센서 노드 S_i가 가까운 베이스 스테이션 B_k'에 키 갱신 요청 정보 KU와 함께 ID_{S_i}, ID_{B_k}를 비밀키 α_i로 암호화하여 전송한다. 물론, 베이스 스테이션 안에 속한 센서 노드일 경우, 비밀키 α_i로 복호화 할 수 있고 공유키와 세션키를 생성할 수 있다. 그러나 ID_{B_k}가 틀린 경우, B_k'는 등록 센터 RC에 재등록을 요청한다.

등록 센터 RC는 $\alpha_i' = h(\delta_k' \parallel ID_{S_i})$를 계산하고 노드의 이전 비밀키 α_i로 암호화한다. 그리고 B_k'에게는 δ_k'로 암호화 하여 전송한다. B_k'는 δ_k'로 복호한 다음과 같은 메시지를 S_i에게 전송한다.

$E_{\alpha_i}(\alpha_i', ID_{B_k}', h(ID_{s_i} \parallel ID_{B_k}' \parallel N_1 \parallel \alpha_i'))$

S_i는 비밀키 α_i로 복호화 하여 새로운 α_i'와 ID_{B_k}'을 얻어 이 정보를 갱신할 수 있는데 아래는 이 과정을 상술한 것이며 그림 6은 이를 도식화한 것이다.

1단계: $S_i \rightarrow B_k' : N_1, ID_{S_i}, ID_{B_k}, KU,$
$E_{\alpha_i}(ID_{S_i}, ID_{B_k})$

2단계: $B_k' \rightarrow RC : N_1, N_2, ID_{S_i}, ID_{B_k}, ID_{B_k}', KU,$
$E_{\delta_k'}(E_{\alpha_i}(ID_{S_i}, ID_{B_k}), ID_{B_k}')$

3단계: $RC \rightarrow B_k' : E_{\delta_k'}(KU, h(ID_{B_k}' \| N_2))$

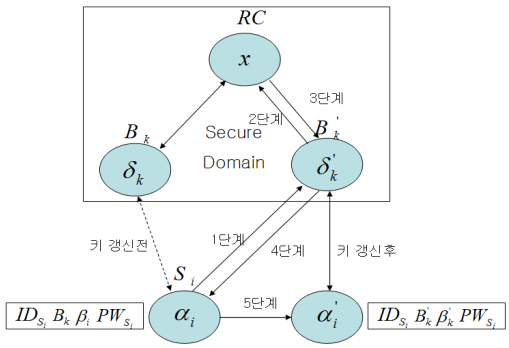
$EK = E_{\alpha_i}(\alpha_i', ID_{B_k}', h(ID_{s_i} \| ID_{B_k}' \| N_1 \| \alpha_i'))$

4단계: $B_k' \rightarrow S_i$:

$EK = E_{\alpha_i}(\alpha_i', ID_{B_k}', h(ID_{s_i} \| ID_{B_k}' \| N_1 \| \alpha_i'))$

5단계: S_i : $\alpha_i \leftarrow \alpha_i'$, $ID_{B_k} \leftarrow ID_{B_k}'$

이 키 갱신 방식에서 S_i가 안전하게 키를 갱신할 수 있는 근거는 자신이 보낸 ID_{S_i}, N_1 정보를 인증할 수 있는 EK를 만들 수 있는 객체는 α_i를 가진 RC와 이전의 베이스 스테이션 B_k뿐이지만 B_k와는 통신이 되지 않으므로 RC만이 유일하게 키를 갱신할 수 있다는 점이다. 즉, 이 경우 B_k'조차도 α_i를 알지 못하므로 인증된 α_i'을 전송할 수 없다. 또한, 베이스 스테이션 B_k'도 자신이 보낸 ID_{B_k}', N_2 정보를 인증할 수 있는 $h(ID_{B_k}' \| N_2)$를 만들 수 있는 유일한 객체는 δ_i'를 가진 RC뿐이기 때문에 RC에 대한 인증이 가능하다.



(그림 6) 노드의 비밀키 갱신 과정

4. 비교 분석

4.1 안전성 분석

무선 센서 네트워크에서 제공해야 할 기본적인 정보보호 서비스는 기밀성, 인증, 무결성, 신규성 등으로 나누어 볼 수 있다[1,5]. 이러한 서비스들은 각각 도청(eavesdropping)에 의한 비밀 키 공격[6], 중간자 공격(man-in-middle attack)[9]에 의한 인증 침해 , 변조 공격(modification attack)[8]등에 의한 무결성 침해, 그리고 재전송 공격(replay attack)[7] 등에 의한 신규성 침해의 위협을 받을 수 있다. 제안하는 상호 인증과 키 동의 방식이 상기한 정보보호 서비스를 위협하는 공격에 대한 저항성을 가지는지 분석하면 다음과 같다.

1) 도청에 의한 비밀 키 공격

공격자는 세션 키 생성을 위해 주고받는 정보를 도청하여 노드나 베이스 스테이션의 비밀 키를 찾고자 할 것이다. 제안 방식에서 공격자는 도청 정보로부터 공유키인 α_i와 λ_{ijk}를 계산할 수 없으며 이를 알지 못하면 암호화되어 전송되는 ru_n과 rs_n을 알지 못한다. 따라서 세션키인 $sk_n = h(ru_n \| rs_n \| \alpha_i)$나 $sk_n = h(ru_n \| rs_n \| \lambda_{ijk})$를 계산하지 못한다. 그러므로 제안 방식에서는 통신자간에 설정된 세션키를 사용하여 데이터를 암호화하면 기밀성을 제공할 수 있다.

2) 중간자 공격

중간자 공격은 불법적인 제 3자가 노드와 베이스 스테이션간 혹은 노드간 통신에 참여하여 두 통신자를 속여 인증을 통과하거나 비밀 정보를 획득하거나 혹은 잘못된 정보를 전송하는 공격이다. 제안 방식에서는 세션키를 설정 과정에서 사용되는 ID와 랜덤 값 ru_n, rs_n을 각각 해쉬한 후 공유한 키로 인증하여 보내는 상호 인증 방식을 사용하고 있다. 따라서 제안 프로토콜은 두 통신자간의 강한 상호 인증을 제공하게 됨으로써 불법적인 중간자에 의한 공격은 불가능하게 된다.

3) 변조 공격

변조 공격은 공격자가 데이터를 변조하는 공격으로서 이를 통해 공격자의 잘못된 정보를 보내거나 인증을 통과하기 위함이다. 제안 프로토콜에서는 노드와 베이스 스테이션간의 공유키를 설정

후 이 공유키 α_i를 이용하여 관련 정보를 암호화해서 전송한다. 따라서 중간의 암호문이 변경되면 제대로 복호할 수 없으며 인증 또한 성립되지가 않는다. 그러나 공격자는 노드와 베이스 스테이션 의간 공유키 α_i나 노드간의 공유 키 λ_{ijk}를 계산할 수 없어 중간의 암호화되어 전송되는 메시지를 변조할 수 없다.

4) 재전송 공격

재전송 공격은 공격자가 이전에 사용된 정보들을 다시 사용하여 인증이나 키 동의를 얻는 공격을 말한다. 그러나 노드와 베이스 스테이션 혹은 노드간 통신에서 사용된 N_4, N_5, N_6, N_7가 암호화된 메시지가 매번 다르게 전송하도록 하여 메시지의 신규성을 확인하게 되는 역할을 하게 되므로 공격자는 이전 정보를 이용한 재전송 공격을 할 수 없다. 이 방식은 각 통신자간의 시간 동기화가 필요하지 않으면서도 이전 정보의 재전송 공격을 무력화할 수 있다.

4.2 효율성 분석

Juang 방식과 제안 방식의 메모리 저장량, 연산량과 통신량을 비교해 본다. 표 1의 비교에서 보면 키 공유시에는 제안 방식이 저장량, 연산량,

(표 1) 효율성 비교(S : 암/복호, H : 해쉬)

	Juang방식[5]	제안방식	비고
E1	320 bits	320 bits	β_i : EEPROM α_i : RAM
E2	160 bits	160 bits	δ_k
E3	1 H	1 H	α_i
E4	None	None	δ_k(사전 계산)
E5	2S+3H (S_i, B_k)	1 H (B_k)	μ_{ik}(Juang's) α_i(Proposed)
E6	6S+9H (S_i, S_j, B_k, RC)	2S+5H (S_i, S_j, B_k)	λ_{ijk}
E7	6S+6H (S_i, S_j)	6S+6H (S_i, S_j)	$sk_n \leftarrow f(\lambda_{ijk})$
			3장 1절 참조
E8	6S+6H (S_i, B_k)	6S+6H (S_i, B_k)	$sk_n \leftarrow f(\alpha_i)$ 3장 1절 참조
E9	None	8S+4H (S_i, B_k, RC)	3장 2절 참조
E10	1248 bit	544 bit	3장 1절 참조
E11	800 bit	96 bit	3장 1절 참조
E12	992 bit	992 bit	3장 1절 참조
E13	896 bit	896 bit	3장 1절 참조

통신량에서 효율성이 높은 것을 볼 수 있다. 비교에서는 해쉬 함수의 출력은 160비트, 랜덤수 N_i, ru_n, rs_n는 96비트 그리고 각 ID값도 96비트로 가정하였다. 비교를 위해 대부분 Juang의 논문[5]에서 제시한 기준을 따랐으며 비교 조건이나 근거가 차이가 있는 경우는 일부 수정을 하였다. 계산량과 통신량 산출을 위한 프로토콜의 자세한 설명은 3장에서 기술하였으며 각 항목은 다음과 같은 의미를 나타낸다.

E1: 노드 메모리
E2: 베이스 스테이션 메모리
E3: 노드 등록을 위한 연산량
E4: 베이스 스테이션 등록을 위한 연산량
E5: 노드와 베이스 스테이션의 키 공유 연산량
E6: 노드와 센서 노드의 키 공유 연산량
E7: 노드 사이의 인증과 키 동의 연산량
E8: 노드와 베이스 스테이션의 키 동의 연산량
E9: 노드의 비밀키 갱신 연산량
E10: 노드 사이의 키 공유를 위한 통신량
E11: 노드와 베이스 스테이션간 키 공유 통신량
E12: 노드 사이의 인증과 키 동의를 위한 통신량
E13: 노드와 베이스 스테이션간 키 동의 통신량

제안 방식과 Juang 방식의 가장 큰 차이는 표의 E5와 E6 항목에서 보는 바와 같이 노드와 베이스 스테이션의 키 공유 연산량과 노드와 센서 노드의 키 공유 연산량이다. Juang 방식에서는 노드와 베이스 스테이션간의 키 공유를 위해 2번의 암/복

호화 연산과 3번의 해쉬 연산이 필요했지만 제안 방식에서는 베이스 스테이션에서 단지 한 번의 해쉬 연산만으로 공유키 α_i를 계산할 수 있다. 또한 노드간의 키 공유를 위해서도 Juang 방식에서는 두 개의 노드, 베이스 스테이션 그리고 등록 센터에서 6번의 암/복호화 및 9번의 해쉬 연산이 필요하다. 그러나 제안 방식에서는 2번의 암/복호와 5번의 해쉬 연산만으로 해결이 가능하다. 그러나 공유키가 설정된 이후 세션키를 설정하는 단계에서는 표에서 E7과 E8 항목에서 보듯이 Juang 방식과 제안 방식이 동일한 연산량을 가진다.

또한, 통신량 측면에서도 공유 키 설정을 위한 통신량은 크게 줄어든다. 비교 항목 E10과 E11에서 보면 노드간의 키 공유 과정에서는 1248비트에서 544비트로, 베이스 스테이션과의 키 공유 과정에서는 800비트에서 96비트로 감소시킬 수 있다. 특히, 노드와 베이스 스테이션간의 공유 키 α_i 설정을 위해서는 노드가 베이스 스테이션에 자신의 ID_{S_i}만 전송하면 되므로 96비트의 통신량만 필요하다. 이러한 점에서 Juang과 비교하면 통신량과 계산량을 크게 줄일 수 있음을 알 수 있다.

그러나 제안 방식에서 한 가지 단점은 각 노드의 키가 자신이 속한 베이스 스테이션에 의존적이므로 해당 베이스 스테이션이 변경될 경우에는 비밀키를 갱신해야 한다. 물론 노드의 위치가 고정적인 환경하에서는 베이스 스테이션을 변경할 필요가 없기 때문에 노드의 비밀키 갱신할 필요가 없다. 노드의 키 갱신을 위해서는 8번의 암/복호화와 4번의 해쉬 연산이 필요하다.

5. 결 론

무선 센서 네트워크가 미래 컴퓨팅 환경에서 중요한 역할을 할 것이다. 연구 범위와 적용 범위도 다양해짐에 따라 센서 네트워크에서의 안전한 통신을 위한 키 분배와 관리가 중요하게 되었다. 무선 센서 네트워크에서는 세션키 설정을 위한 메모리량과 연산량, 통신량이 많이 요구되지 않으면서도 상호 인증과 키 동의를 효율적으로 할 수 있는 프로토콜이 필요하다. 제안한 사용자 인증 및 키 동의 방식은 센서 네트워크의 여러 가지 보안 요구 사항들을 만족하고 키를 공유함에 있어 노드와 베이스 스테이션, 베이스 스테이션과 등록 센터간의 통신량과 계산량을 크게 줄일 수 있다.

참 고 문 헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, Vol. 8. No. 5, pp. 521-534, 2002.

[2] Q. Huang, J. Cukier, H. Kobauashi, B. Liu and J. Zhang, "Fast Authenticated Key Establishment Protocols for Self-organizing Sensor Networks", In Proc. of the 2nd SCM International Conference on Wireless Sensor Networks and Applications, pp. 141-150, 2003.

[3] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", In 10th ACM Conference on Computer and Communication Security(CCS), 2003).

[4] H. Chan, A. Perrig, PIKE:Peer Intermediaries for Key Establishment in Sensor Networks, IEEE Infocom, Vol. 1, pp. 524-535, 2005.

[5] W. S. Juang, "Efficient User Authentication and Key Agreement in Wireless Sensor Networks", WISA 2007, LNCS 4298, pp. 15-29, Springer-Verlag, 2007.

[6] S. Bellovin and M. Merritt, "Encrypted Key Exchanged: Password-Based Protocols Secure Against Dictionary Attacks, In Proc. of IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

[7] P. Syverson, "A Taxonomy of Replay Attacks", In Proc. of Computer Security Foundations Workshop

Ⅶ, pp. 187-191, 1994.
[8] C. Yang, T. Chang and M. Hwang, "Cryptanalysis of Simple Authenticated Key Agreement Protocols", IEICE Trans. Fundamentals, Vol. E87-A, No. 8, pp. 2174-2176, 2004.
[9] W. Stallings, Cryptography and Network Security, 4th Edition, Prentice Hall International, 2007.

◐ 저 자 소 개 ◑

윤 신 숙 (SinSook Yoon)
1994년 단국대학교 화학과 졸업
2008년 호서대학교 컴퓨터공학과 졸업
2008년~현재 호서대학교 컴퓨터공학과 박사과정
E-mail : yss28@hanmail.net

하 재 철 (JaeCheol Ha)
1989년 경북대학교 전자공학과 졸업
1993년 경북대학교 전자공학과 석사
1998년 경북대학교 전자공학과 박사
1998년~2006년 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년~2007년 나사렛대학교 정보통신학과 부교수
2006년~2006년 QUT in Australia 연구 교수
2007년~현재 : 호서대학교 정보호호학과 부교수
2002년~현재 : 한국정보보호학회 이사, 논문지 편집위원
2008년~현재 : 한국인터넷정보학회 논문지 편집위원
E-mail : jcha@hoseo.edu