Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 11 pp. 7541-7548, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.11.7541
ISSN 1975-4701 / eISSN 2288-4688

센서네트워크 환경에서 경량화된 키 교환 및 상호인증 라우팅 프로토콜

이광형[1*], 이재승[2], 민소연[3]
[1]서일대학교 인터넷정보과, [2]숭실대학교 컴퓨터공학과, [3]서일대학교 정보통신과

A design on Light-Weight Key Exchange and Mutual Authentication Routing Protocol in Sensor Network Environments

Kwang-Hyoung Lee[1*], Jae-Seung Lee[2], So-Yeon Min[3]
[1]**Department of Internet Information, Seoil University**
[2]**Department of Computer Science and Engineering, Soongsil University**
[3]**Depatment of Information Communication, Seoil University**

요 약 Wireless Sensor Networks 기술은 노드들을 다양한 지역에 분포시킴으로서, 군사적 목적의 탐색 역할은 물론 산업에서의 기기 관리, 공정 관리, 특정 지역 모니터링 등 다양한 분야에 활용이 가능한 기술이다. 하지만, 무선 센서 네트워크 환경에서 센서 노드의 경우 초소형 하드웨어를 사용함에 따른 에너지, 처리 능력, 메모리 저장능력 등의 한계점을 가지고 있으며, 이러한 한계를 극복하기 위해 다양한 라우팅 프로토콜 방법이 제안되었다. 하지만, 기존 라우팅 프로토콜의 경우 에너지 효율성에 초점을 둠으로서 상호간 통신할 때, 보안에 매우 취약하며, 이를 극복하기 위해 기존의 암호화 시스템을 도입하기에는 센서의 처리 능력 과 메모리 등에 한계점을 가지고 있다. 따라서, 본 논문에서는 에너지 효율성을 고려하면서 동시에 통신 과정에서 상호인증 기법 및 키 생성과 갱신 시스템을 도입함으로서 다양한 보안위협에 대응할 수 있는 상호인증 방법을 제안한다.

Abstract Wireless Sensor Networks is the technology which is used in explore role for military purposes, as well as various fields such as industrial equipment management, process management, and leverage available technologies by distributing node into various areas. but there are some limitations about energy, processing power, and memory storage capacity in wireless sensor networks environment, because of tiny hardware, so various routing protocols are proposed to overcome it. however existing routing protocols are very vulnerable in the intercommunication, because they focus on energy efficiency, and they can't use existing encryption for it, Because of sensor's limitations such like processing power and memory. Therefore, this paper propose mutual authentication scheme that prevent various security threats by using mutual authentication techniques and, Key generation and updating system as taking into account energy efficiency

Keywords : LEACH, Sensor, Sensor Authentication, Sensor Network, Sensor Routing Protocol

1. 서론

무선 센서 네트워크는 데이터를 수집할 때, 환경의 제약 없이 활용이 가능한 기술로서, 노드들을 다양한 지역에 분포시켜, 군사적 목적의 탐색 역할은 물론 산업에서의 기기 관리, 공정 관리, 특정 지역 모니터링 등에 활용

본 논문은 2015년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Kwang-Hyoung Lee(Seoil Univ.)
Tel: +82-2-490-7226 email: dreamace@seoil.ac.kr
Received September 10, 2015 Revised November 2, 2015
Accepted November 6, 2015 Published November 30, 2015

이 가능하다. 센서 네트워크는 수많은 노드들로 이루어져 있다. 노드는 용도에 따라 원하는 지역에 배포가 가능하며, 접근이 힘든 지역의 경우 환경의 제약 없이 노드들을 무작위로 배포할 수 있다[7][14-15]. 배포된 노드들은 서로 통신을 하며 데이터를 주고받으며 네트워크를 구축하고 수집된 데이터는 베이스 스테이션(Base Station)으로 전송하게 된다[8].

센서 네트워크의 일반적인 구조는 하나의 베이스 스테이션과 데이터 수집을 위해 특정 지역에 분포된 수많은 노드들로 이루어져 있다. 노드들이 수집한 정보들은 베이스 스테이션으로 전송된다. 이때, 센서 노드들의 특성상 소형 하드웨어를 사용하는 제약으로 인해 노드들의 에너지에 한계에 의한 다양한 문제가 야기 될 수 있다[4][12][17]. 또한, 노드들에게는 에너지를 공급을 위한 전원 공급 장치가 필요하지만, 센서 노드들의 경우 보통 군사적 목적 및 비실제적 환경에 배치됨으로서 노드들의 배터리를 충전하거나 교체하는 것은 거의 불가능 하다[13]. 따라서, 센서 환경에서는 에너지 효율성을 고려하여 적은 에너지로도 통신을 할 수 있는 기술을 고려해야 한다[5]. 센서 네트워크 환경에서 노드들은 경로를 설정할 때, 주변 상황을 고려한 자율적 경로 설정을 하는 Ad-Hoc 방식을 사용한다[9]. 센서 네트워크환경에서는 노드들이 협력을 통해 데이터를 베이스스테이션까지 전송하기 때문에, 각각 노드들의 수명은 네트워크의 환경 전체의 수명을 결정짓는 중요한 요인이다. 즉, 센서 노드의 하드웨어적 한계를 극복하여 네트워크 수명 유지를 위한 다양한 라우팅 프로토콜들이 제안되었다[10].

본 논문에서는 이러한 라우팅 프로토콜 과정에서 센서노드의 에너지 한계를 극복하기 위해 에너지 효율성을 고려한 상호인증 및 키 생성 기법을 제안한다[16].

2. 관련 연구

2.1 LEACH 라우팅 프로토콜

LEACH 프로토콜[11][18][19][20]은 센서 노드들의 에너지가 통신 거리에 따라 증가한다는 점을 이용하여 통신 거리와 함께 에너지의 소모를 노드들이 균등하게 소모할 수 있는 클러스터 기반 라우팅 프로토콜 기술이다.

LEACH 프로토콜의 경우 다음과 같은 전제를 기본으로 두고 있다.

- 센서 필드 상에 있는 모든 센서 노드들은 싱크 노드까지 1-hop 전송이 가능하다.
- 센서 노드의 경우 수신 전력의 세기를 제공하며, 송신 전력을 변동할 수 있는 전력 컨트롤이 가능하다.
- 센서 노드들은 베이스스테이션으로 전송할 데이터가 주기적으로 발생한다.
- 서로 인접한 센서 노드들이 수집한 데이터는 상관관계가 높다.

LEACH 라우팅 프로토콜에서 노드들은클러스터 헤드를 임의로 선출하고 선출된 클러스터헤드를 통해서 각각 클러스터를 형성 한다. 클러스터에 포함된 노드들은 각각 데이터를 수집하며, 수집한 데이터를 클러스터 헤드에 전송한다. 클러스터 헤드는 노드들이 보낸 정보들을 종합하여 최종적으로 베이스 스테이션에게 전송하게 된다. 클러스터내의 노드들의 데이터를 수집하고 베이스 스테이션에 통신하는 등 클러스터 헤드는 다른 노드에 비해 에너지 소모량이 많으며, 특정 노드에 일이 과중된다면 센서 네트워크 전체에 악영향을 끼칠 수 있다. LEACH 라우팅 프로토콜에서는 이처럼 특정 노드에 집중된 에너지 소모를 분산시키기 위해서 클러스터 헤드를 라운드 별로 새롭게 선출하는 방식을 통해 특정 노드에 일이 집중되는 현상을 방지하였다, LEACH 라우팅 프로토콜은 클러스터 헤드를 하지 않은 노드들 중에서 클러스터 헤드를 선출하고 새롭게 선출된 클러스터 헤드가 남아 있는 노드와 함께 새롭게 클러스터를 형성하는 방식으로 구성된다. 여기서 새로운 클러스터가 형성되고 만료되는 시점까지의 시간을 '라운드'라고 표현한다. 라운드는 주기적으로 반복됨으로써 지역 내 모든 노드들이 클러스터헤드에 한번 씩 선정되며 이를 통해서 클러스터 헤드에 집중된 에너지 소모를 분산시키게 된다. 노드들이 모두 클러스터 헤드를 하게 되면, 다시 모든 노드가 클러스터 헤드가 될 자격을 가지며 이와 같은 주기를 'Group of Round'라고 한다. LEACH 라우팅 프로토콜의 시간은 네트워크상의 모든 노드들이 모두 동기화 되어야 한다.

2.2 Distance-Bounding Protocol

Distanec-Bounding Protocols은 Brands와 Chaum에 의해 제안된 프로토콜**[14]**로 일반적 Distanec-Bounding Protocols의 과정을 살펴보게 되면 저속 → 고속 → 저속의 순서로 진행하게 된다. 처음 저속 단계에서는 서로의

공유 값을 교환하게 되며, 고속 단계에서는 공유된 값을 이용하여 한 비트씩 정보를 빠르게 교환 한다. 마지막 저속단계에서는 이전 단계의 수행 결과를 검증하게 된다. 저속 단계의 경우 사용 용도나 상황에 따라 생략될 수 있지만, 고속단계의 경우 Distanec-Bounding Protocols의 핵심 단계로서 반드시 진행되어야 한다. Distanec-Bounding Protocols 고속단계는 암호학적, 수학적 연산 없이 단순 과정으로 이루어져 있어 수 나노초 정도의 매우 빠른 연산의 수행이 가능하다. Distanec-Bounding Protocols의 고속단계를 살펴보게 되면, 검증자(V)는 증명자(P)에게 이전 공유된 값을 이용하여 한 비트씩 보내게 되고, P는 그에 대한 응답으로 이전 공유된 값을 이용하여 한 비트씩 빠른 속도의 응답비트를 보내게 된다. 검증자(V)는 비트를 주고 받는 과정의 시간을 계산하여 상한 값 이내에 되었는지 판단하여 증명자(P)의 적합성을 확인할 수 있다[6].

Table 1. Notation

Notation	Meaning
α_i	V Random nonce value
β_i	P Random nonce value
γ_i	$\alpha_i \oplus m_i$ Calculation results
m_i	$m_1 \| \| ... \| \| m_n$

Distance-Bounding Protocols의 기본 구조는 아래 그림과 같으며, 이 구조는 첫 번째 저속 단계를 생략하여, 고속단계와 저속단계의 2가지 단계로 이루어져 있다.

첫 번째 고속단계에서는 검증자가 랜덤 비트 0과 1중 한 비트를 증명자에게 전송하며, 비트를 받은 증명자는 응답으로 역시 랜덤 비트 0과 1중 한 비트를 전송하게 된다. 같은 과정을 n번 진행한 후, 검증자는 교환을 통해 얻은 비트들을 연접하여 α 를 얻는다.

두 번째, 저속단계에서는 먼저, 이전의 실행을 얻은 비트 교환 결과의 상한 값을 체크하고, 상한 값 이내에 비트 교환이 이루어 졌다면, 증명자는 α값을 서명하여 검증자에게 전송하여 자신이 실제 증명자가 맞음을 검증받는다.

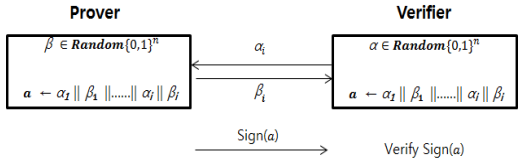

Fig. 1. Distance-Bounding Protocol

3. 제안 내용

본 논문에서는 센서네트워크 환경에서 LEACH 라우팅 프로토콜 과정 중 Distance-Bounding을 이용한 상호인증 기법을 제안한다. 제안하는 기법은 송신 측에서 한 비트의 정보를 전송하면, 수신 측 에서는 수신한 비트에 대한 응답으로 비밀정보 한 비트를 전송하며, 이 과정을 연속적으로 시행함으로서 인증 절차를 수행 한다.

Table 2. Proposed Notation

Notation	Meaning
N_v, N_p	Nonce
k	Shared key
R_i^0, R_i^1	3n bit a divided
sk	Session Key
nk	f() Function Shared Key
n_1^i	Remain bit
c_i	Random bit

3.1 클러스터 헤드-노드 인증

센서 필드에 있는 노드가 확률기반의 알고리즘을 통해 클러스터헤드를 선출한다. 선출된 클러스터 헤드는 자신이 클러스터 헤드임을 메시지를 통하여 알리면, 이 메시지를 받은 멤버 노드는 가장 강하게 수신되는 전파를 가진 클러스터 헤드를 자신의 클러스터 헤드로 결정하고, Join메시지와 함께 난수 N_v 암호화하여 전송한다. 이를 수신한 클러스터 헤드는 응답으로 난수 N_p를 암호화하여 전송한다. 이때, 암호화에 사용되는 키는 사전에 공유된 키 k를 이용한다. 상호 난수 교환이 완료되면 클러스터 헤드와 노드는 난수를 이용하여 인증절차를 수행 한다. Fig. 2는 인증 절차 프로토콜을 나타낸 것이다.

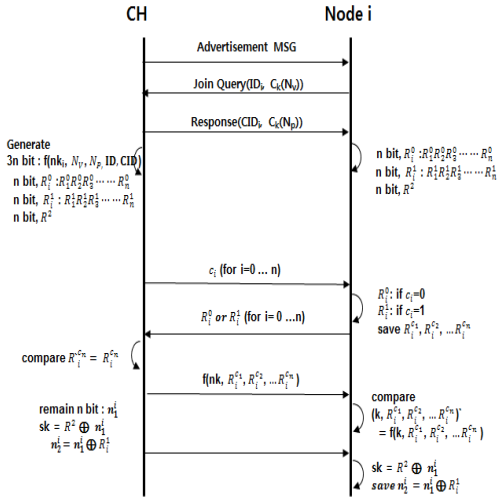

Fig. 2. Clusterhead-Node Authentication

① 먼저, 확률 기반 알고리즘을 통해 클러스터 헤드로 선정된 노드는 브로드캐스트를 통해 본인이 클러스터 헤드를 선정되었음을 광고 한다.

② 광고 메시지를 받은 노드i 는 가장 강하게 수신된 메시지의 클러스터 헤드에게 본인의 ID와 난수 N_v를 암호화 하여 클러스터 헤드에게 전송 한다.

③ 노드i 로부터 메시지를 수신한 클러스터 헤드는 본인의 아이디 CID와 N_p를 암호화 하여 노드 i에게 전송한다.

④ 난수 N_v, N_p 를 공유하게 된 클러스터 헤드와 노드는 f()함수를 이용하여 3*n 비트의 정보를 저장하며, 이를 각각 n비트 크기로 분배 한다.

⑤ 클러스터 헤드는 인증 절차를 수행하기 위해 랜덤한 수 c_i를 생성하여, 한 비트씩 노드 i 에게 전송한다.

⑥ 클러스터 헤드로부터 한 비트씩 수신한 노드는 이에 대한 응답으로 c_i가 0일 경우 R^0 의 i번째 비트를, 1일 경우 R^1의 i번째 비트를 클러스터 헤드에게 전송 한다.

⑦ 클러스터 헤드는 노드 i에게 전송한 c를 기반으로 $R'^{c_n}_i$을 생성하며, 노드 i의 응답 값을 취합한 $R_i^{c_n}$값과 비교하여 올바른 노드로부터 데이터가 전송 되었는지 확인 한다.

⑧ 노드 i를 인증한 클러스터 헤드는 수신한 $R_i^{c_n}$ 값들과 nk를 f()함수를 이용하여 생성된 값을 노드 i에게 전송 한다.

⑨ 클러스터 헤드로부터 값을 수신한 노드 i를 동일한 방법으로 값을 생성하여 클러스터 헤드로부터 받은 값과 비교함으로서 클러스터 헤드를 검증하게 된다.

⑩ 클러스터 헤드와 노드는 R^2 이용하여 세션키와 이후에 사용할 비밀 값 n_2^i 를 생성하고 저장함으로서 인증과정을 종료하게 된다.

3.2 베이스스테이션–클러스터헤드 인증

선출된 클러스터 헤드는 자신이 클러스터 헤드로 선출된 것을 베이스 스테이션에게 알리기 위해 본인의 ID와 난수 N_p를 암호화하여 전송한다. 이를 수신한 베이스 스테이션은 본인의 ID와 난수 N_v 암호화하여 전송한다. 교환이 완료되면 베이스 스테이션과 클러스터 헤드는 난수를 이용하여 인증절차를 수행 한다. Fig. 3은 인증 절차 프로토콜을 나타낸 것이다.

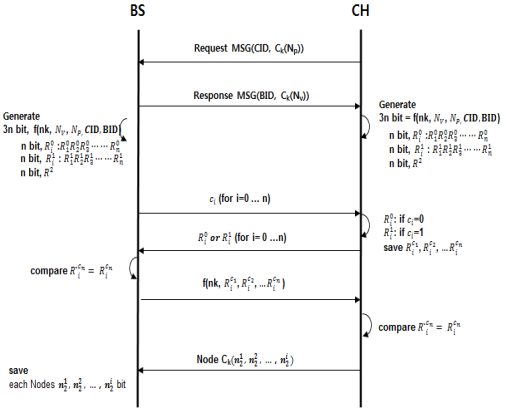

Fig. 3. Basestation-Clusterhead Authentication

① 확률기반의 알고리즘을 통해 선출된 클러스터 헤드는 본인이 클러스터 헤드로 선정된 것을 알리기 위해 본인의 식별 값 CID와 난수 N_p를 암호화하여 베이스 스테이션에게 전송 한다.

② 클러스터 헤드로부터 메시지를 수신한 베이스 스

테이션은 본인의 아이디 BID와 N_v를 암호화 하여 클러스터 헤드에게 전송한다.

③ 난수 N_v, N_p 를 공유하게 된 베이스 스테이션과 클러스터 헤드는 f()함수를 이용하여 3*n 비트의 정보를 저장하며, 이를 각각 n비트 크기로 분배 한다.

④ 베이스 스테이션은 인증 절차를 수행하기 위해 랜덤한 수 c_i를 생성하여, 한 비트씩 노드 i 에게 전송한다.

⑤ 베이스 스테이션으로부터 한 비트씩 수신한 클러스터 헤드는 이에 대한 응답으로 c_i가 0일 경우 R^0 의 i번째 비트를, 1일 경우 R^1의 i번째 비트를 베이스 스테이션에게 전송 한다.

⑥ 베이스 스테이션은 클러스터 헤드 에게 전송한 c를 기반으로 $R'^{c_n}_i$을 생성하며, 클러스터 헤드의 응답 값을 취합한 $R_i^{c_n}$값과 비교하여 올바른 노드로부터 데이터가 전송 되었는지 확인 한다.

⑦ 클러스터 헤드를 인증한 베이스 스테이션은 수신한 $R_i^{c_n}$ 값들과 nk를 f()함수를 이용하여 생성된 값을 클러스터 헤드에게 전송 한다.

⑧ 클러스터 헤드로부터 인증값을 수신한 베이스스테이션은 동일한 방법으로 인증 값을 생성하여 클러스터 헤드로부터 받은 값과 비교 함으로서 클러스터 헤드를 검증하게 된다.

⑨ 클러스터 헤드는 3*n bit에서 사용하고 남은 n비트를 암호화 하여 베이스 스테이션에게 전송하며, 베이스 스테이션은 각각의 클러스터 헤드로부터 받은 각 노드들의 비밀 값을 저장함으로서 인증과정을 마치게 된다.

3.3 신규 라운드 과정

한 번의 라운드가 종료되게 되면 확률 기반 알고리즘을 통해 새로운 클러스터 헤드가 선정 된다. 선정된 클러스터 헤드는 Node 들에게 광고하여 클러스터를 형성 한다. 이 과정에서 베이스 스테이션과 통신을 통해 이전 노드들의 n_2^i 값을 얻음으로서 노드와 인증 과정에서 키로 사용하게 된다.

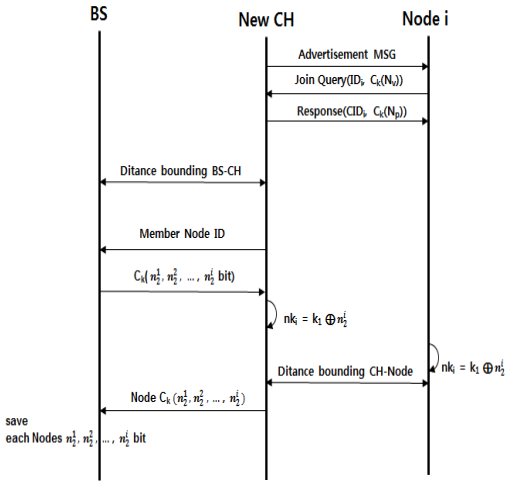

Fig. 4. New Round Protocol

① 새로운 라운드가 시작 되면 확률 기반 알고리즘을 통해 클러스터 헤드를 새롭게 선정 한다. 선정된 클러스터 헤드는 브로드캐스트를 통해 본인이 클러스터 헤드를 선정되었음을 노드들에게 광고 한다.

② 광고 메시지를 받은 노드i 는 가장 강하게 수신된 메시지의 클러스터 헤드에게 본인의 ID와 난수 N_v를 암호화 하여 클러스터 헤드에게 전송 한다.

③ 노드i 로부터 메시지를 수신한 클러스터 헤드는 본인의 아이디 CID와 N_p를 암호화 하여 노드 i에게 전송한다.

④ 새로운 클러스터 헤드와 노드 i의 가입 및 응답이 완료되면 베이스 스테이션과 클러스터 헤드는 3.2의 Distance Bounding BS-CH 과정을 진행 한다.

⑤ 클러스터 헤드는 현재 자신에게 접속해 있는 노드들의 ID를 베이스 스테이션에게 전송 한다.

⑥ 베이스 스테이션은 3.2 과정에서 저장해 놓은 각 노드들의 n bit값 n_2^i을 클러스터 헤드가 보내준 노드 iD에 맞게 도출하여 암호화 한 후 새로운 클러스터 헤드에게 전송 한다.

⑦ 클러스터 헤드와 노드는 상호간 f()에 사용할 nk_i을 계산한 후 3.1의 Distance Bounding CH-Node 인증 과정을 진행 한다.

⑧ 클러스터 헤드와 노드간 인증 결과로 도출된 새로

Table 3. Security Evaluation Table

	Blundo's Protocol[1]	PCGR[2]	Dave's Protocol[3]	Proposed scheme
Relay attack	x	x	o	o
Replay attack	x	x	x	o
Eavesdropping	o	o	x	o
Leaked key	x	o	o	o
Mutual authentication	Not-support	Support	Not-support	Support
Forward security and Error detection	Not-support	Support	Support	Support

운 $n_{2,}^1 n_2^2, \cdots, n_2^i$ 값들을 클러스터 헤드는 다시 베이스 스테이션에게 전송하게 되며 베이스 스테이션은 이를 저장하고, 클러스터 헤드가 새롭게 선정 되었을 때, 다시 사용하게 된다.

4. 보안성 평가

본 논문에서는 Distance-Bounding 과정을 통해 각 노드가 물리적으로 근거리에 있는지 판단함으로서 Relay attack에 안전하며, 각각 베이스 스테이션, 클러스터 헤드, 센서 노드가 생성한 난수를 이용하여 R_i^0, R_i^1 를 생성하고, 랜덤 값 c에 대한 응답 값으로 약속된 R_i^0, R_i^1를 주고 받는 과정에서 챌린지 비트에 대한 응답 비트 중 1 bit의 위치만 잘못되어도 error detection이 가능하며, 이를 통해 forward security와 상호인증이 가능하다. 메시지 재사용 공격과 메시지 위변조 공격시에는 메시지를 탈취할 당시의 세션키가 아닌 새롭게 생성한 세션키 $sk = R_i^0 \oplus n_1$ 를 사용하며, 타임스탬프를 통해서도 이전 메시지의 재사용으로 인한 공격에 대하여 안전하다. 스니핑의 경우, 각 노드 간 전송되어지는 메시지들은 지속적으로 갱신되어 지는 노드 간 비밀키 $nk_i = k_1 \oplus n_2^i$ 를 이용하여 암호화를 적용한 후 전송되기 때문에 안전하며, 스푸핑의 경우 이미 상호인증이 완료된 노드들이며, 스푸핑 공격을 받더라도 초기 공유하고 있는 노드 간 비밀키를 알지 못하기 때문에 안전하다.

5. 결론

본 논문에서는 센서 네트워크 환경에서 사용되는 에너지 효율적 라우팅 프로토콜인 LEACH라우팅 프로토콜을 살펴보고 라우팅 프로토콜 과정에서 기존 라우팅 프로토콜의 환경을 고려하여 적은 에너지 소비로도 상호인증 및 세션 키 생성 등 다양한 보안위협에 대응할 수 있도록 Distance-Bounding 프로토콜을 이용함으로서 에너지 효율성을 고려한 상호인증 라우팅 프로토콜을 제안하였다.

제안하는 방식은 기존의 라우팅 프로토콜이 지니고 있던 재사용 공격, 위변조 공격, 스니핑, 스푸핑 등 다양한 보안 위협에 대응할 수 있었으며, 에너지 효율성 또한 기존의 라우팅 프로토콜과 큰 차이를 보이지 않았다. 즉, 기존 라우팅 프로토콜에 비해 보안성은 향상되었지만 노드의 수명에는 별다른 지장을 주지 않는다는 것을 확인할 수 있었다.

References

[1] Carlo Blundo, Alfredo De Santis, Amir Herzbeerg, Shay Kutten, Ugo Vaccaro, Moti Yung, Perfectly-Secure Key Distribution for Dynamic Conferences. Information and Computation, 1995.

[2] Wensheng Zhang, Guohogn Cao, Group Rekeying for Filtering False Data in Sensor Net-works: A Predistribution and Local Collaboration-Based Approach. IEEE INFOCOM, 2005.
DOI: http://dx.doi.org/10.1109/INFCOM.2005.1497918

[3] D. Singelee and B. Preneel, Location verification using secure distance bounding protocols. In Proceedings of Second IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS'05). IEEE Computer

Society, 2005.
DOI: http://dx.doi.org/10.1109/mahss.2005.1542879

[4] I.F.Akyildiz, " A Survey on Sensor Networks", IEEE Communication Magazine, Vol.40, No.8, pp102-114, Aug 2002.
DOI: http://dx.doi.org/10.1109/MCOM.2002.1024422

[5] G. Anastasi, M. Conti, M. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," Ad Hoc Networks, Vol. 7, No. 3, pp. 537-568, 2009.
DOI: http://dx.doi.org/10.1016/j.adhoc.2008.06.003

[6] G. Hanckeand M. Kuhn," An RFID distance bounding protocol," in proc.1st IEEE international Conf.security Privacy Emergin Areas Commun. Netw, pp.67-73, 2005.
DOI: http://dx.doi.org/10.1109/SECURECOMM.2005.56

[7] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann, "Scalable Coordination for Wireless Sensor Networks: Self-Configuring Localization Systems," Proceedings of the Sixth International Symposium on Communication Theory and Applications (ISCTA '01), 2001.

[8] R. Zhang, H. Zhao, and M. A. Labrador, "A Grid-based Sink Location Service for Large-scale Wireless Sensor Networks", IWCMC 2006.
DOI: http://dx.doi.org/10.1145/1143549.1143687

[9] M. Chu, H. Haussecker, and F. Zhao, "Scalable Information Driven Sensor Querying and Routing for Ad Hoc Heterogeneous Sensor Networks," International Journal of High Performance Computing Applications, Vol. 16, No. 3, pp. 293-313, 2002.
DOI: http://dx.doi.org/10.1177/109434200201600309O1

[10] D. Estrin, D. Culler, K. Pister, and G. Sukhatme, "Connecting the Physical World with Pervasive Networks," Pervasive Computing IEEE, Vol. 1, No. 1, pp.59-69, 2002.

[11] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan "Energy-efficient routing protocols for wireless micro sensor networks" in Proc.33rd HawaiiInt. Conf.System Sciences(HICSS) ,Maui, HI, Jan.2000.

[12] S. Dulman, T. Nieberg, J. Wu, and P. Havinga, "Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks," Wireless Communications and Networking(WCNC 2003) workshop, Vol. 3, pp. 1918-1922, 2003.
DOI: http://dx.doi.org/10.1109/wcnc.2003.1200680

[13] Stfan Brands, David Chaum, "Distance Bounding Protocols", Springer Berlin/Heidelberg, Advances in Cryptology－EUROCRYPT '93 , Vol.765 of Lecture Notes in Computer Science, pp.344-359, May 1993.
DOI: http://dx.doi.org/10.1007/3-540-48285-7_30

[14] S. Madhavi, Secured Data Aggregation Scheduling in Ubiquitous Quantum Sensor Networks, *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.4 No.1, pp.17-30, June 2014.
DOI: http://dx.doi.org/10.14257/AJMAHS.2014.06.02

[15] Carlos Ramos, Zita Maria Almeida do Vale, Semantic Key Pre-Distribution Protocol For Multi-Phase Wireless Sensor Networks, *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.1 No.1, pp.17-28, June 2011.
DOI: http://dx.doi.org/10.14257/AJMAHS.2011.06.05

[16] Farkhod Alisherov, The Security in the Vehicular Ad Hoc Network (VANET) Using Expedite Message Authentication Protocol (EMAP), *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology,* Vol.1 No.1, pp.99-106, Dec. 2011.
DOI: http://dx.doi.org/10.14257/AJMAHS.2011.12.03

[17] Kokula Krishna Hari K, Long CAI, Enhancement of TCP congestion control based on relative delay and Bandwidth Estimation, *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.2 No.2, pp.45-60, Dec. 2012.
DOI: http://dx.doi.org/10.14257/AJMAHS.2012.12.01

[18] J. O. Park, S. K. Kim, Mutual Authentication and Key Establishment Mechanism for Secure Data Sharing in M2M Environment, *The Journal of The Institute of Internet, Broadcasting and Communication (IIBC),* Vol. 15, No. 4, pp.33-41, Aug. 31, 2015.
DOI: http://dx.doi.org/10.7236/JIIBC.2015.4.33

[19] C.-H. Lee, J.-Y. Lee, DL-LEACH: Hierarchical Dual-Hop Routing Protocol for Wireless Sensor Network, *The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)*, Vol. 15, No. 5, pp.139-145, Oct. 31, 2015.
DOI: http://dx.doi.org/10.7236/JIIBC.2015.5.139

[20] J.-Y. Lee, Energy Improvement of WSN Using The Stochastic Cluster Head Selection, *The Journal of The Institute of Internet, Broadcasting and Communication (IIBC),* Vol. 15, No. 1, pp.125-129, Feb. 28, 2015.
DOI: http://dx.doi.org/10.7236/JIIBC.2015.1.125

이 광 형(Kwang-Hyoung Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 졸업(공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 인터넷정보과 부교수

<관심분야>
멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, DRM, USN, 학습콘텐츠

이 재 승(Jae-Seung Lee) **[정회원]**

- 2013년 2월 : 평생교육진흥원 컴퓨터학과(공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2015년 2월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

<관심분야>
시큐어코딩, Sensor Network

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템