논문 13-38B-10-03

한국통신학회논문지(J-KICS) '13-10 Vol.38B No.10
http://dx.doi.org/10.7840/kics.2013.38B.10.801

WSN의 에너지 효율적 운영을 위한 신뢰성이 보장된 IDE-LEACH 프로토콜

조 영 복◆, 우 성 희*, 이 상 호°

IDE-LEACH Protocol for Trust and Energy Efficient Operation of WSN Environment

Young-bok Cho◆, Seng-hee Woo*, Sang-ho Lee°

요 약

WSN은 수백에서 수 만개에 달하는 SN들로 구성된다. WSN은 에너지 불균형 문제 해결을 위해 각 라운드마다 클러스터헤드를 새롭게 선택하고, 안전한 통신을 위해 노드 인증방식을 사용하고 있다. 그러나 이런 방법은 각 라운드마다 재-클러스터링을 수행함으로 SN의 오버헤드를 가중시키는 원인이 되고 안전한 통신을 제공하기 위한 인증단계는 빈번히 발생되는 AREQ/AREP 메시지 처리로 노드의 오버헤드를 더욱 가중시키고 있다. 라서 이 논문에서는 WSN 환경에서 에너지 효율적 운영과 신뢰성이 보장된 IDE-LEACH(Identity based Encryption : IDE) 프로토콜을 제안한다. 제안 프로토콜은 기존 LEACH 기반의 프로토콜보다 통신에 평균적으로 20%까지 네트워크 수명을 연장하였고, 통신에 참여하는 모든 노드는 기지국으로부터 인증을 거친 신뢰할 수 있는 노드들로 구성된다.

Key Words : Wireless Sensor Network, Authentication, LEACH, IDE, Energy Efficiency, Trust

ABSTRACT

WSN consists of hundreds to thousands of sensor nodes. In order to solve the problem of energy consumption imbalance cluster head is reelected in every round, while node authentication scheme is utilized for secure communication. However, re-clustering increases the overhead of sensor nodes and during the node authentication phase the frequent AREQ/AREP message exchange also increases the overhead. Therefore, a secure and energy efficient protocol , by which overhead of sensor nodes is reduced and long time communication is achieved, is required for wireless sensor network. In this paper, an energy efficient and reliable IDE-LEACH protocol for WSN is proposed. The proposed protocol is prolongs networks lifetime about average 20% compared to the LEACH-based protocols and all attending nodes in communication form BS authentication consisted of trusted nodes.

Ⅰ. 서 론

최근까지 무선 센서 네트워크(Wireless Sensor Networks:WSN)는 저전력 무선통신 기술과 MEMS와 같은 하드웨어 기술의 발달로 대규모의 구성이 가능해졌으며, 다양한 분야에서 응용되고 있다. 이러한 WSN은 스마트 센서와 집적화 기술의 도움으로 네트워크를 구성하는 센서노드(Sensor Node:SN)

◆ First Author : 충북대학교 전자정보대학 소프트웨어학과 초빙교수, bogicho@gmail.com, 정회원
° Corresponding Author : 충북대학교 전자정보대학 소프트웨어학과 교수, lee@paper.korean.ac.kr, 종신회원
* 한국교통대학교 의료정보공학과 교수, shwoo@ut.ac.kr, 종신회원
논문번호 : KICS2013-08-365, 접수일자 : 2013년 8월 28일, 최종논문접수일자 : 2013년 9월 30일

의 수는 수백에서 수 만개에 달한다.[1,2,5,6] 또한 무선 통신의 특성으로 메시지의 도청, 노드 탈취 및 손상, 감청, 서비스 거부 공격 등 라우팅 공격에 매우 취약하고[3], 대부분의 기존 연구에서는 인증키 생성을 위해 SN은 기지국(Base Station:BS)과 직접 통신을 수행한다. 그러나 현실적으로 SN과 BS가 직접통신을 시도하는 것은 어려운 일이다. 또한 네트워크의 안전성을 고려한 인증과 암호화 처리를 위한 인증요청 메시지(Authentication Request Message:AREQ)와 인증응답 메시지(Authentication Reply Message:AREP)의 많은 처리는 SN의 오버헤드를 가중시키는 문제점을 갖는다[2-8]. 따라서 이 논문에서는 SN의 메시지 처리로 인한 오버헤드를 줄이고 오랜 시간 동안 통신에 참여해 통신 유지가 가능한 에너지 효율적인 운영 프로토콜을 제안한다. 제안 논문은 에너지 효율을 기반으로 수집된 데이터의 신뢰성을 보장하기 위해 SN에서 ID 기반의 암호화를 이용해 데이터를 전송한다. 또한 통신에 참여하는 노드는 초기 등록과정에서 BS와 클러스터 헤드(Cluster Head:CH)에게 인증된 멤버노드(Member Node:MN)으로 외부로부터의 데이터 접근을 방지하기 때문에 무선에서 전송되는 데이터의 무결성을 보장할 수 있다. 이 논문의 구성은 2장에서 관련연구로 LEACH 기반 프로토콜 Low-Energy Adaptive Clustering Hierarchy Protocol(LEACH), Improve Energy of LEACH Protocol(IE-LEACH), Improve Energy of LEACH Protocol(IL-LEACH)의 분석과 ID기반 암호화에 대해 설명한다. 3장에서는 WSN 환경에서 에너지 효율을 향상시킨 신뢰성이 보장된 IDE-LEACH(Identity based Encryption:IDE) 운영 프로토콜을 제안한다. 4장에서는 제안방법의 평가를 위한 실험환경을 기술하고, 에너지 소비량과 전체 생명주기를 기존 모델들과 비교 및 분석하여 평가한다. 마지막으로 5장에서는 이 논문의 결과와 향후 연구과제에 대해 간략히 기술한다.

Ⅱ. 관련연구

2.1. LEACH 기반의 프로토콜

LEACH 프로토콜(Low-Energy Adaptive Clustering Hierarchy Protocol)[2]은 계층 기반 라우팅의 대표적인 기법으로 SN의 균등한 에너지 소비를 목표로 동작된다. 각 클러스터는 하나의 CH와 여러 개의 MN들로 구성된다. MN은 데이터를 수집하고, 클러스터헤드는 MN이 수집한 데이터를 병합하여 기지국까지 전달한다. LEACH 프로토콜은 CH의 에너지 소비를 균등하게 분산시키기 위해 라운드마다 무작위로 CH를 선출하는 방식으로 모든 노드가 한 번씩 CH가 될 수 있는 기회를 부여하고 매 라운드마다 CH를 새로 선출한 후 재-클러스터링을 수행한다. LEACH 프로토콜에서는 CH 선출시 SN의 잔여 에너지에 대한 고려가 없기 때문에 임의의 SN은 에너지가 고갈되어 통신에 참여할 수 없는 경우가 빈번히 발생되고 이는 전체 네트워크의 불균형 문제점을 갖는다. IE-LEACH 프로토콜[6]은 기존 LEACH 프로토콜에서 CH는 MN의 전송 데이터의 유무에 상관없이 TDMA 슬롯을 전체에 할당해 모든 라운드에서 활성모드로 동작되는 에너지 비효율성 문제를 해결함으로 LEACH 프로토콜의 에너지 효율을 향상시킨 프로토콜이다. 송신 데이터를 보유한 SN에게만 타임 슬롯을 할당함으로 SN의 에너지 소비를 줄이고 결정 단계를 추가하여 초기 설정단계에서 수행되는 연산은 기존 LEACH 프로토콜보다 많아졌지만 에너지 효율성은 향상되었다. 그러나 일정 시간에 전송 데이터가 없는 MN의 경우 타임 슬롯을 할당받지 못한 경우 MN은 해당 라운드 동안 슬립모드를 유지해야 하는 문제점을 갖는다. IL-LEACH 프로토콜[9]은 LEACH 프로토콜에서 각 클러스터마다 MN의 수가 달라 네트워크 전체 에너지 소비의 불균등 문제점을 개선하기 위해 제안된 방식이다. 모든 클러스터는 동일한 수의 MN으로 구성함으로 네트워크 전체 에너지 소비를 균등하게하고, 동시에 에너지 효율을 향상시켰다. 또한 LEACH와는 다르게 에너지 소모가 많은 투표 단계 없이 CH를 재설정하지만 라운드 마다 임계값을 계산하는 ACK-Flag로 인한 오버헤드가 발생되는 문제점을 갖는다. [표 1]은 기존 LEACH 기반으로 동작되는 프로토콜의 설정단계와 안정단계에서 발생되는 오버헤드와 각 프로토콜의 특징을 정리하였다.

표 1. LEACH 기반의 프로토콜 특징
Table 1. LEACH based protocol distinction

	LEACH	IE-LEACH	IL-LEACH
setup	selected CH, cluster configuration	decision phase	the first round is the same as LEACH
steady-state	data transfer	join-REQ data transfer	ACK-Flag data transfer
feature	each round make re-clustering	check transfer node through join-REQ , check and data transfer .	threshold based select CH by using ACK-flag

2.2. ID 기반의 암호화 프로토콜

1985년 공개키 암호 시스템에서 공개키의 효율성을 위해 전자우편 주소나 주민등록번호처럼 수신자의 신원정보를 공개키로 이용하는 ID기반 암호화 시스템은 Shamir에 의해 처음 제안되었다[10,11]. 송신자는 암호화를 위해 누구나 알 수 있는 수신자의 고유한 신원정보를 공개키로 사용하고 공개키를 이용해 수신자를 인증한다. 이것은 인증기관에 정당한 수신자를 먼저 인증 받아야 하는 복잡함과 이에 따른 비용과 비효율성 문제를 해결할 수 있다는 장점을 갖는다[10]. 또한 2001년 Weil Pairing 기반의 IDE 암호 시스템이 제안되고 Bilinear map의 수학적 구조를 이용한 ID기반의 암호를 구현하였다[12-15].

$$Pair(a \bullet X, b \bullet Y) = Pair(b \bullet X, a \bullet Y)$$

위에서 사용된 ' • '는 타원곡선상의 점들의 곱을 나타낸 것이다. X와 $(a \bullet X)$를 알고 a를 찾는 역계산은 불가능하다. 키 서버는 s와 P를 난수를 이용해 생성하고 P와 $(s \bullet P)$값은 모든 사용자에게 전달한다. [그림 1]은 Pairing 기반의 ID 암호화 방식을 도식화 한 것이다.

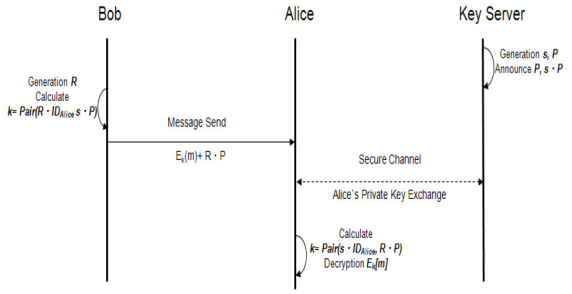

그림 1. Pairing 기반의 ID 암호화
Fig. 1. Pairing based Identity Encryption

Ⅲ. 에너지 효율적 운영을 위한 신뢰성이 보장된 IDE-LEACH프로토콜

WSN 환경에서 SN이 안전하게 오랜 시간 동안 통신에 참여할 수 있는 운영 프로토콜이 필요하다. 또한 MN의 신뢰성을 기반으로 수집된 데이터의 무결성 보장이 필요하다. 따라서 이 논문에서는 WSN 환경에서 에너지 효율적 운영을 위한 신뢰성이 보장된 IDE-LEACH 프로토콜을 제안한다. 제안 방식은 기존 LEACH 기반의 경우 SN에서 발생되는 메시지 처리로 인한 오버헤드 문제를 최소화하고 SN은 오랜 시간 안전하게 통신에 참여할 수 있도록 지원한다. 제안기법의 라운드 형식은 설정단계와 안정단계로 구성된다. 설정단계는 클러스터링 단계로 CH를 선택하고 MN을 구성한 후 클러스터헤드 후보노드를 형성한다[15]. 안정단계에서는 SN이 주변 정보를 수집하고 CH로 전송한다. CH는 수집된 정보를 통합하여 기지국으로 전송하게 된다. [표 2]은 제안 프로토콜 메시지에서 사용하는 계수를 정리한 것이다.

표 2. 인증에 사용되는 파라미터
Table 2. Parameter of using Authentication

Notation	Meaning
$ID_{CH}, ID_{BS}, ID_{MN}$	ID of cluster head/base station /member Bode
P_{BS}, PH_{pri}	hash value of BS parameter
$H(\,)$, TS	hash function / time stamp
CHH_{Pub}	hash vale of cluster head ID
r, α	random value/ base station/ master key
$E_{ID_{CH}}$, V_{cert}	encryption using ID of CH/ authentication value between CH and BS
γ_{MN}, γ_{CH}, γ_{BS}	random number of MN, CH, and BS
$(\alpha \bullet \beta)$	public value thorough random form key value
$[\bullet]$	multiplication of points on the Elliptic curve
VS_i, LoT	authentication value of SN/ period
SK , SN_{MN}	session key/ serial number of MN

3.1. 세션키 생성

초기 네트워크가 구성되기 전 BS에서 모든 SN의 등록이 선행됨을 가정한다. 기지국과 CH사이 상호 인증이 가능한 세션키(SK)를 생성한다. 세션키는 LEACH 프로토콜에서 IDE를 기반으로 생성한다. CH와 기지국간의 인증을 위한 인증값(V_{cert})을 송수신한다. 기지국에서 V_{cert}을 검증하기 위해 CH로 세션키를 전달하는 과정은 다음과 같다.

① 기지국은 키 서버에서 생성한 난수 α,β를 이용해 $(\beta,\alpha \bullet \beta)$를 계산하고 모든 SN에게 브로드케스팅 한다. 이때 α는 기지국의 마스터키가 된다.

② CH는 기지국에게 세션키를 요구한다.

③ 기지국은 세션키 요청 메시지를 수신하고 CH에게 인증값(V_{cert})을 요청한다.

④ CH는 자신의 랜덤 값 (γ_{CH_i})과 인증 값을 생성하여 전달한다. 해쉬 함수로 $PH_{pri} = H(\beta)$, $CHH_{pub} = H(ID_{CH_i})$를 계산하고 $\delta_{CH} = CHH_{CH_i} + \gamma_{CH_i}, \beta \bullet PH_{pri}$ 를 생성한다. 인증 값 생성을 위해 CH는 계산된 δ값을 기지국의 ID로 $K = (r \bullet ID_{BS}, \alpha \bullet \beta)$ 생성하고 CH의 ID로

$K=(r \cdot ID_{CH}, \alpha \cdot \beta)$을 생성해서 P_{BS}를 암호화한 후 연접연산으로 기지국에게 인증 값 ($V_{cert}=E_{BS}(\delta)\|E_{CH}(P_{BS})$)을 송신한다.

⑤ 기지국은 수신한 인증 값을 복호화하고 P_{BS}를 검증한다. 기지국에서 난수 γ_{BS}를 생성한 후 세션키 $SK=\alpha \cdot (\delta \oplus \gamma_{BS} \cdot \beta)$를 생성한다.

⑥ 기지국은 생성한 세션키를 PH_{pri}로 $K=(r \cdot PH_{pri}, \alpha \cdot \beta)$를 암호화해 CH에게 전달한다.

3.2. 클러스터링과 멤버노드 구성

기지국에 등록된 SN을 가지고 초기 클러스터링을 통해 MN을 구성한다. 클러스터링은 설정단계와 안정단계로 설정단계는 클러스터링을 수행하고 안정단계는 데이터 전달을 수행하는 LEACH 프로토콜과 동일하다. CH는 클러스터링으로 분할된 MN 사이 식별 값을 송수신한 후 BS로 전송한다. BS는 식별 값을 인증 후 CH에게 키 값을 전송하고 기지국은 키 값으로 식별 값을 복호화해 MN에게 승인 메시지를 전송한다.

① MN이 구성되기 전 기지국은 모든 SN을 등록한다. MN 은 CH에게 등록요청 메시지를 전송한다.

② CH는 MN을 기지국에 등록하기 위해 노드 식별 값 요청 메시지를 전송한다.

③ MN은 γ_{MN}와 $K=(r \cdot ID_{CH_i}, \alpha \cdot \beta)$를 생성하고 SN_{MN}을 암호화한다. γ_{MN}을 자신의 ID로 $K=(r \cdot ID_{MN_i}, \alpha \cdot \beta)$값을 생성하여 암호화 한 다음 연접하여 ID_{MN}와 함께 전송한다. $M=[E_{ID_{CH}}(SN_{MN})\|E_{ID_{MN}}(\gamma_{MN})], ID_{MN_i}$

④ MN의 SN_{MN}을 수신한 CH는 세션키로 암호화하고 BS에게 개인키와 인증요청메시지 $M=SK[E_{ID_{CH}}(SN_{MN_i}), E_{ID_{MN}}(\gamma_{MN})], ID_{MN_i}$를 전송한다.

⑤ BS는 CH로부터 받은 메시지를 복호화한후 SN_{MN}을 인증한다. CH와 MN의 키값을 생성하고 세션키로 암호화한 메시지 $M=SK(K_{CH_i}, K_{MN_i})$를 CH로 전송한다.

⑥ CH와 MN은 키 값을 수신하고 CH는 MN 아이디를 복호화 한 후 타임 스템프를 생성하고 MN의 인증 값 $VS_{MN_i}=(\gamma_{MN} \oplus SN_{MN}\|TS)$을 생성한다.

⑦ CH는 수신한 MN의 인증 값(VS_{MN_i})을 기지국에 등록한 후 MN의 승인 메시지를 전송한다.

CH는 기지국을 통해 MN의 인증을 거친 후 데이터 수집에 참여할 수 있다. 인증된 안전한 노드에서 수집된 데이터의 무결성을 보장하기 위해 수집된 데이터는 암호화를 통해 전달한다. 제안 프로토콜에서 MN은 CH를 통해 서비스를 요청하고 상호간의 식별 값(V_{cert})을 송수신 한다. CH는 식별 값을 검증하고 MN을 기지국에 저장하기 위해 통신에 참여할 MN을 인증한 후 인증된 MN을 기지국에 전달한다. 제안 프로토콜의 통신참여 시간을 계산하기위해 [표 3]과 같이 변수를 정의한다.

표 3 에너지 소비량 변수 정의
Table 3. Definition of Energy consumption variables

Notation	Meaning
m	m-bit message size
M_e	m-bit encryption message
KG_{MN}	MN in the amount of energy consumed to key generation
KG_{CH}	CH in the amount of energy consumed to key generation
SC	Spreading code to prevent signal interference
KG_{tot}	The amount of energy consumed to key generation (cluster)
$KG_{cluster}$	The amount of energy consumed to encryption (cluster)
T_{DC}	data merge hours(cluster header)
$DE_{cluster}$	The amount of energy consumed in the data collection

클러스터마다 소비되는 에너지양은 CH와 MN에서 소비되는 에너지양의 합으로 계산되고, 그룹키를 사용해 통신에 참여하는 경우 클러스터에서 소비되는 에너지양을 측정한다. 클러스터에서 소비되는 에너지는 클러스터헤드, 멤버노드, 키 생성에 소비되는 에너지양의 합을 의미한다. CH가 인증키를 이용해 통신에 참여하는 경우 소비되는 에너지양은 CH와 기지국간의 통신(E_{CH-BS}), CH와 MN간의 통신(E_{CH-MN})으로 구분된다. 이때 클러스터에서 암호화된 메시지를 d 거리상에 위치한 노드로 전송하는 경우에 소비되는 에너지양을 계산한다. [표 4]는 MN에서 인증키를 이용해 통신에 참여할 때 소비되는 에너지양과 클러스터에서 암호화를 위해 소비되는 에너지양을 정의한 것이다.

표 4. 에너지 소비량 정의
Table 4. Definition of Energy consumption

	Definition
cluster communication	$E_{cluster} = E_{CH} + (\frac{N}{N_c} - 1) \times E_{MNs} + KG_{MN} + KG_{CH}$
Encrypted message delivery (in a cluster)	$E_{CH} = E_{CH-BS} + E_{CH-MN}$ $E_{CH-BS} = M_c E_{node} (\frac{N}{N_c} - 1) + M_c \frac{N}{N_c} (E_{node} + e_{amp} d_{BS}^4) + KG_{CH}$ $E_{CH-MN} = M_c E_{node} (\frac{N}{N_c} - 1) + M_c \frac{N}{N_c} (E_{node} + e_{fs} d_{MN}^2) + KG_{MN}$
authentication MN	$E_{MN} = M_c E_{node} + (M_c \times e_{fs} \times d_{CH}^2) + KG_{MN}$
encryption of CH	$KG_{cluster} = ((M_c E_{node} + M_c e_{fs} d_{CH}^2) + (M_c E_{node} + M_c e_{amp} d_{BS}^4))$

Ⅳ. 실험 및 평가

4.1. 실험환경

이 논문에서는 WSN 환경에서 에너지 효율적 운영을 위한 IDE-LEACH 프로토콜의 운영을 제안하였고 에너지 효율성 평가를 위해 무선 에너지 소비 모델을 기반으로 네트워크 시뮬레이터 NS-2에서 에너지 소비율을 실험하였다. 실험을 위한 시스템 및 환경변수는 [표 5]과 같이 정의한다.

표 5. 시스템 환경 및 환경 변수
Table 5. System environment and environment variable

Parameter	Value
OS	Linux CentOS
network size/number of node	100*100 / 100~1000
initial energy	2J
packet header /message size	25 / 500bytes
delay / transmission rate	50μs / 100kbps
ε_{fs} / ε_{amp}	10pJ/bit/m^2 / 0.0013pJ/bit/m^4
data tmasmit speed/ delay loss(μ)	1Mbps / 2/4.3
communication radius(R)/max-hop(h)	(Mulit)10m,(Single)20m / 3
encryption / decryption	0.64ms / 0.42ms

4.2. 실험결과

[그림 2]은 기지국을 중앙 필드에 위치시키고 SN을 1000개로 구성한 환경에서 SN의 통신 참여시간을 실험한 결과이다. 제안 프로토콜을 LEACH, IL-LEACH, IE-LEACH들과 비교해본 결과 제안 논문은 통신에 참여하는 노드수가 증가하였다. [그림 3]는 제안 논문에서 LEACH 프로토콜을 IDE 방식으로 암호화하여 MN을 인증하는 경우와 암호화를 제공하지 않는 경우 전체 에너지 소비량을 비교해본 결과 암호화를 사용하는 경우 초기 라운드에서 암호화를 사용하지 않는 경우보다 에너지 소비량이 증가함을 보였으나 라운드가 지속되면서 추가적인 노드의 삽입이 발생하지 않기 때문에 전체 네트워크의 에너지소비량의 변화는 큰 영향을 주지 않음을 볼 수 있다.

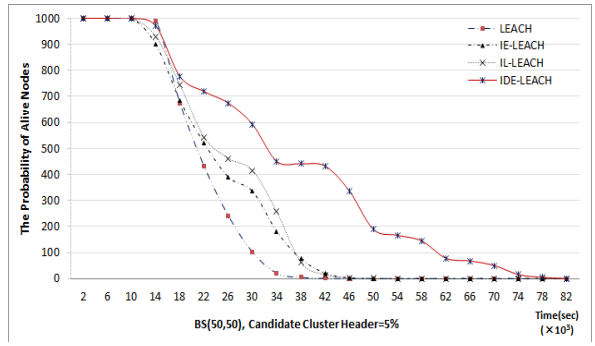

그림 2. 통신 참여시간(암호화 사용안함)
Fig. 2. The communication time (not encryption)

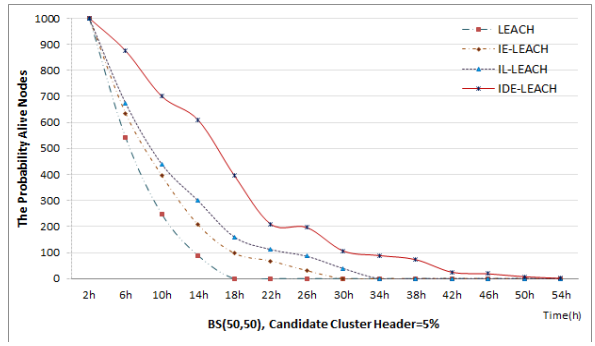

그림 3. 통신 참여시간(암호화 사용)
Fig. 3. The communication time(encryption)

4.3. 안전성 분석

제안 프로토콜의 안전성을 평가하기 위해 다음과 같은 물리적 공격, 데이터의 무결성 공격, 중간자 공격 및 재전송 공격, 데이터의 기밀성등 위협들에 대한 제안 프로토콜의 안전성을 기술한다. 물리적 공격은 조작된 장치에 인가된 인증 토큰을 삽입하거나 조작된 소프트웨어를 설치하는 공격으로 제안 프로토콜은 SN과 CH의 시리얼번호를 등록후 기지국으로부터 인증을 수행하기 때문에 안정성을 제공한다. 데이터의 무결성 공격은 악의적인 소프트웨어 업데이트 혹은 설정 변경, 사물 통신의 소유주, 사용자의 잘못된 설정 변경을 통한 공격이 가능하다. 또한 접근 제어리스트의 잘못된 구성으로 취약성이 발생할 수 있다. 그러나 제안한 인증 프로토콜에서

는 CH가 MN에게 *VS*를 부여하고 CH는 MN의 *VS*을 기지국에 저장하여 관리함으로 변경을 통한 공격이 어렵다. 중간자 공격 및 재전송공격은 활성화된 네트워크의 취약성을 이용하는 공격에 대한 보안 위협으로 제안 프로토콜에서는 기존 IDE 인증 방식에서 세션키 생성 알고리즘으로 생성되어진 생성키 $[\alpha \cdot (\delta \oplus \gamma_{BS} \cdot \beta)]$을 활용한다. CH와 기지국간의 안전한 데이터를 송수신 할 수 있어 프로토콜의 공격인 중간자공격 및 재전송 공격을 통한 인증이 불가능하게 된다. 데이터의 기밀성 위협은 MN이 네트워크에 전송한 메시지 도청에 대한 위협이 일어날 수 있다. 그러나 제안 프로토콜은 생성된 세션키를 활용해 데이터를 안전하게 송수신함으로써 사용자의 데이터와 프라이버시 공격이 불가능하게 된다.

V. 결 론

WSN 환경에서 에너지 효율을 위해 클러스터링 기반의 라우팅과 다양한 경량의 인증기법을 제안하고 있다. 기존의 클러스터링 기반의 프로토콜은 각 라운드마다 CH를 새롭게 선출하고 재-클러스터링을 수행함으로 SN의 오버헤드를 발생시킨다. 또한 MN의 인증시 발생되는 많은 메시지 처리로 인해 SN의 오버헤드는 더욱 가중되었고, SN에 가중된 오버헤드는 통신시간을 단축시키는 원인이 되었다. 그 중 가장 대표적인 방법으로 사용되는 LEACH 프로토콜은 다양한 방법으로 향상된 알고리즘(IE-LEACH, IL-LEACH)이 제안되었으나 모두 LEACH 기반의 재-클러스터링 단계로 인한 오버헤드 문제는 해결하지 못하고 있다. 따라서 이 논문에서는 재-클러스터링 단계를 후보노드를 이용해 최소화하고 통신에 참여하는 MN의 인증을 통해 안전한 데이터 수집이 가능한 에너지 효율적인 IDE-LEACH 운영 프로토콜을 제안하였다. 제안 프로토콜인 IDE-LEACH는 기존 LEACH 기반의 클러스터링 방식을 제공하면서 매 라운드마다 발생되는 재-클러스터링으로 인한 오버헤드 문제를 IDE 기반의 인증 프로토콜을 사용해 인증을 위한 AREQ/AREP 메시지를 줄여 기존 LEACH프로토콜보다 약 20%의 에너지 효율성을 제공하였다.

References

[1] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6-28, Dec. 2004.

[2] W. S. Juang, "Efficient user authentication and key agreement in wireless sensor networks," in *Proc. Int. Workshop Inform. Security Applicat. (WISA '06)*, pp. 15-29, Jeju Island, Korea, Aug. 2006.

[3] T. T. Huyen and E. N. Huh, "A reliable 2-mode authentication framework for ubiquitous sensor network," *J. Korean Soc. Internet Inform. (KSII)*, vol.10, no.3, pp. 51-60 Jun. 2008.

[4] T. T. Huyen and E. N. Huh, "An efficient signal range based key pre-distribution scheme ensuring the high connectivity in wireless sensor network," in *Proc. Int. Conf. Ubiquitous Inform. Management Commun. (ICUIMC'08)*, pp. 441-447, Suwon, Korea, Jan.-Feb. 2008.

[5] C. Perrig, "SPINS: security protocols for sensor networks," *J. ACM Wireless Networks*, vol. 8, no. 5, pp. 521-534, Sep. 2002.

[6] S. H. Lee and J. B. Suk, "Improvement of energy efficiency of LEACH protocol for wireless sensor networks," *J. Korea Inform. Commun. Soc. (KICS)*, vol. 33, no. 2, pp. 76-81, Feb. 2008.

[7] G. Yang, C. M. Rong, C. Veigner, J. T. Wang, and H. B. Cheng, "Identity-based key agreement and encryption for wireless sensor networks," *J. China Univ. Posts Telecommun.*, vol. 12, no. 4, pp. 54-60, Dec. 2006.

[8] B. S. Kim and H. B. Lim, "A study on node authentication mechanism using sensor node's energy value in WSN," *J. Inst. Electron. Eng. Korea (IEEK)*, vol. 48, no. 2, pp. 86-95, Mar. 2011.

[9] Y. Y. Choo, H. J. Choi, and J. W. Kwon, "Algorithm improving network life-time based on LEACH protocol," *J. Korean Inst. Commun. Inform. Sci. (KICS)*, vol. 35, no. 8. pp. 810-819, Aug. 2010.

[10] M. L. Kim, H. S. Kim, and Y. D. Son, "The conversion method from ID-based encryption

to ID-based dynamic threshold encryption," *J. Korea Inst. Inform. Security Cryptology (KIISC)*, vol. 22, no. 4, pp. 733-744, Aug. 2012.

[11] H. Chan and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," in *Proc. IEEE INFOCOM Conf.*, pp. 524-535, Miami, U.S.A., Mar. 2005.

[12] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Advances Cryptology Conf. (CRYPTO 2001)*, pp. 213-229, Santa Barbara, U.S.A., Aug. 2001.

[13] A. Shamir, "Identity-based crypto systems and signature schemes," in *Proc. Advances Cryptology (CRYPTO 84)*, pp. 47-53, Santa Barbara, U.S.A., Aug. 1984.

[14] Y. B. Cho and S. H. Lee, "An IDE based hierarchical node authentication protocol for secure data transmission in WSN environment," *J. Korean Inst. Commun. Inform. Sci. (KICS)*, vol. 37B, no. 3, pp. 149-157, Mar. 2012.

조 영 복 (Young-bok Kim)

2006년 3월 충북대학교 전자계산학과 석사
2012년 8월 충북대학교 전자계산학과 박사
2012년 8월~현재 충북대학교 전자정보대학 소프트웨어학과 초빙교수

<관심분야> 센서네트워크, 네트워크보안, 정보보안, 의료정보

우 성 희 (Seng-hee Woo)

1993년 2월 충북대학교 전자계산학과 석사
1999년 2월 충북대학교 전자계산학 박사
1995년 9월~2005년 12월 청주과학대학컴퓨터과학과 교수
2006년 1월~현재 한국교통대학교 의료정보공학과 교수

<관심분야> 침입차단 및 방지, 의료정보보호, 정보보안, 컴퓨터네트워크, 컴퓨터보안

이 상 호 (Sang-ho Lee)

1981년 2월 숭실대학교 자계산학과 석사
1989년 2월 숭실대학교 전자계산학과 박사
1981년 3월~현재 충북대학교 전자정보대학 소프트웨어학과 교수

<관심분야> 네트워크보안, Protocol Engineering, Network Management