Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.759

무선 센서 네트워크에서 그리드 정보를 활용한 위치 기반 키 관리 연구*

최 재 우,[1†] 김 용 현,[2] 김 주 엽,[2] 권 태 경[1‡]
[1]연세대학교 정보보호연구실, [2]국방과학연구소 국방사이버센터

A Study of Location-based Key Management Using a Grid for Wireless Sensor Networks*

Jaewoo Choi,[1†] Yonghyun Kim,[2] JuYoub Kim,[2] Taekyoung Kwon[1‡]
[1]Information Security Lab., Graduate School of Information Yonsei University
[2]Defense Cyber Warfare Center, Agency for Defense Development

요 약

본 논문에서는 WSN을 위한 위치 기반의 키 관리 기법에 대해서 제고한다. 기존의 위치 기반의 키 관리 기법들에 대해 알아보고 그 중 LDK (Location Dependent Key management) 기법을 집중적으로 파악하였다. 이를 통해 LDK 기법에서 고려하지 못한 통신 간섭 문제를 개선하기 위하여 그리드 정보를 활용한 키 생성 기법과 키 보정과정을 활용하는 기법을 제안하였다. 시뮬레이션을 통하여 보안성이 높은 환경에서 제안 기법이 기존의 LDK보다 접속율은 향상하였고 절충율은 감소하였음을 확인하였다. 또한, 육면체 형태의 AN 배치를 통해 네트워크 비용을 줄일 수 있음을 시뮬레이션을 통해 확인하였다.

ABSTRACT

This paper proposes a location-based key management scheme in wireless sensor networks, and among the existing location-based key management techniques, we focused on the LDK (Location Dependent Key management). In order to improve the problems occurred by communication interference, we introduced the key revision process and the method of key establishment using grid information. According to the simulation of this scheme, it increased connectivity while decreased compromise ratio than those of the previous LDK, futhermore, we confirmed that a hexagon distribution of AN reduces the network cost.

Keywords: WSN, Key Management, Location

I. 서 론

2014년 가트너 자료를 따르면 IoT (Internet of Things)는 2020년 260억 개의 기기가 네트워크로 연결될 것으로 예측하면서 IoT 시장의 발전 가능성을 높게 평가하였다[13]. 이에 IoT의 기반 기술 중 WSN (Wireless Sensor Networks) 기술 연구가 활발히 진행되고 있다. 특히 군, 의료, 산업현장,

접수일(2014년 11월 17일), 수정일(1차: 2015년 4월 8일, 2차: 2014년 6월 1일), 게재확정일(2015년 7월 13일)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (ITP-2015-H8501-15-1008)
† 주저자, jw.choi@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

교통 등의 다양한 환경에 적용하는 연구가 계속해서 진행되고 있다[1].

WSN의 여러 연구 분야 중에서 중요한 분야가 보안이다. 실세계의 데이터를 측정하여 활용하기 때문에 보안의 중요성은 크다. 우리는 보안 연구 분야 중 WSN 키 관리 기술에 대해 연구를 진행하였다.

WSN 키 관리 기술은 2002년 Eschenauer 등[2]의 연구를 시작으로 지금도 많은 연구가 이루어지고 있다. WSN 키 관리는 크게 대칭키 기반과 공개키 기반으로 나누어지며 한 쌍의 키 관리, 사전 랜덤 키 분배, 위치기반 키 관리 등 다양한 방법의 키 관리 기법이 존재한다. 센서 노드의 하드웨어적 제한으로 인하여 효율성, 확장성, 이기종 지원 등이 WSN 키 관리 기법의 주요 연구 목표이다.

WSN에서 위치정보는 매우 중요하고 활용 가능성이 높은 정보이다. 이를 활용하는 연구로써 위치기반의 키 관리가 한 축으로 자리매김하였다. 그중 그리드 기반의 키 관리 기법은 센서 노드를 지정된 그리드에 위치시켜야 한다는 특징이 있다. 이 특징은 활용분야에 따라 단점이 될 수 있다. 예를 들어 군에서 군사 지역에 적 탐지를 위하여 WSN을 활용할 경우 센서 노드를 원하는 그리드에 위치시키기는 쉽지 않을 것이다. 그리드를 사용하지 않고 센서 노드의 위치 자체에 따르는 키 관리 기술은 Anjum의 LDK(Location Dependent Key Management) 스킴[3]이 있다, 본 논문은 Anjum의 스킴에 기반을 둔다.

본 논문의 구성은 다음과 같다. 2장에서는 WSN에서의 위치 기반의 키 관리 기술에 대한 관련 연구들을 알아본다. 3장에서는 LDK를 기반으로 하는 스킴을 제시하며 4장에서 시뮬레이션을 통하여 제안한 스킴을 분석하고 토의한다. 마지막으로 5장을 통해 결론을 맺는다.

II. 관련 연구

WSN을 위한 위치 기반 키 관리 기법 중 대부분은 그리드 정보를 활용한다. 그리드 정보는 센서 노드가 배치될 지형을 그리드로 분할한 후 그 좌표를 활용하는 것이다. 위의 경우 센서 노드는 해당 그리드에 배치되어야 한다는 전제 조건이 생긴다. 이는 배치될 지역에 따라서 제약조건이 될 수 있다.

Huang 등[4]은 배치 정보를 알고 있다는 가정하에 그리드 그룹 스킴을 제안하였다. 대량의 키 집합에서 랜덤하게 키를 분배하지 않고 특정한 키를 분배하는 방식을 사용하였다. 그리드 좌표와 센서 노드의 아이디를 조합하여 식별자로 활용하고 해당 식별자와 Blom 스킴을 센서 노드에 사전 분배하는 방식을 제안하였다.

Ito 등[5]은 위치를 추정하는 확률 밀도 함수를 사용하여 2차원 그리드 당 한 개의 키를 할당하고 센서 노드의 통신 범위 내의 랜덤한 위치에 있는 센서 노드에 해당 그리드에 할당된 키를 요청하는 방식을 제안하였다.

Liu 등[6]의 논문은 두 개의 변수를 갖는 다항식을 이용하여 한 쌍의 키를 생성하는 과정에서 센서 노드의 그리드 상 위치를 ID로 활용하였다.

Du 등[7]의 논문은 그리드에 키 풀에서 추출한 서브 키 집합을 할당하는 방식을 제안하였다. 해당 논문에서는 센서 노드가 위치할 좌표를 계산하는 비균일 확률 밀도 함수를 사용하였다.

Anjum[3][8]은 2006년 사전 저장된 키 링과 논스를 조합하여 키를 생성하는 논문을 발표하였으며 이후 2010년에는 위의 논문을 확장하여 발표하였다. LDK는 그리드 위치에 종속적인 위의 스킴들과는 다르게 센서 노드 위치 자체에 의존적인 스킴이다. 전송 세기를 조절하여 일정 거리까지만 데이터를 전송하는 AN (Anchor Node)의 특성을 이용하여 지역을 분할한다. 센서 노드는 사전에 공통키 k, 해시 함수 H를 저장한 상태에서 현장에 배치된다. AN은 전파 세기를 달리하여 논스를 전송하고, 이후 센서 노드는 전송받은 논스를 가지고 해시 함수를 통해 키를 생성한다. 센서 노드는 이웃 노드와 공통된 키를 찾고 일정 개수 이상의 키를 공유하였을 때 $k = H(k_1, k_2, \cdots, k_q)$방식으로 공유키를 생성하게 된다. Fig. 1은 LDK의 작동원리를 간단하게 보여주는 그림으로써 전파세기에 따라 다른 논스를 전송할 때 센서 노드가 배치된 위치에 따라 전송받게 되는 논스를 보여준다.

Faghani 등[9]의 논문은 2006년의 LDK를 확장하는 스킴 SLDK (Sectorized Location Dependent Key Management)를 제안하였다. LDK의 스킴을 기반으로 하면서 AN의 통신 범위를 8개의 섹터로 분할하는 방식을 추가하여 노드 탈취에 대한 보안성을 강화하였다.

본 논문에서는 LDK를 기반으로 하여 연구를 진행하였다. 따라서 다음 장에서는 LDK에서 발생할 수 있는 문제점을 살펴보고 이를 보완하는 스킴을 제안

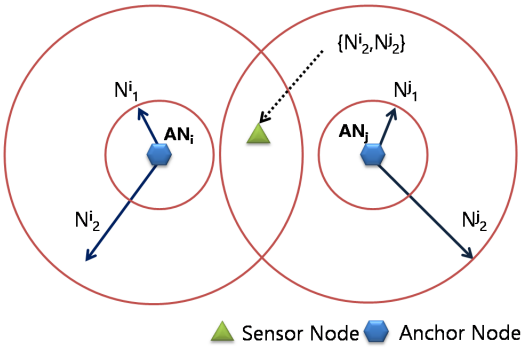

Fig. 1. Illusion of LDK

한다.

III. 제안 기법

3.1 표기법

다음의 Table 1은 제안 기법을 설명하는 데 쓰이는 변수들에 대한 표기법과 그 의미를 설명한다.

Table 1. Notation

Notation	Meaning
AN	Anchor node that sends nonces
ANset	The set of anchor nodes
SN	Sensor node
SNset	The set of sensor nodes
K_c	Pre-installed network key
G	Pre-distributed information of nige grids
H	Pre-distributed hash function
C_n	The total number of received nonces
N_r	The r-th nonce
C_{common}	The number of common keys shared with neighbor node
q	The minimum number of keys to generate a shared key
K_t	The key made of nonce and grid information
K_q	The set of q-common keys
K_s	Shared key generated between two nodes

3.2 LDK의 문제점

기존 LDK는 통신의 간섭을 고려하지 않았다. Wu 등[10]의 논문에서는 MicaZ에서 간섭으로 인해 40%의 패킷 손실이 일어남을 확인하였다. 패킷 손실이 일어나면 AN으로부터 전송받는 논스 개수에 영향을 끼칠 수 있다. 만약 간섭으로 인해 노드의 위치상에서 전송받아야 할 논스를 받지 못한다면 이웃 노드와의 공유한 논스의 개수가 부족하여 정상적인 상황에서는 키 동의가 이루어져야 하는 상황에서 키 동의가 이루어지지 않아 암호화 통신이 불가능하게 되는 상황이 발생할 수 있다. 노드 간의 연결 불가능 문제는 전체 네트워크의 운용성에 관련 있는 문제로 볼 수 있다. 또한, 기존 논문은 C_{common}이 매우 낮은 상황을 고려하였다. 하지만 전송받은 논스를 조합하여 키를 생성하기 때문에 C_{common}이 높을수록 논스 정보 노출 시에 논스를 통한 키 추출이 어려울 것이다[3]. 해당 변수는 보안성을 관련 있는 변수이기 때문에 본 논문에서는 C_{common}을 높인 상황을 고려하였다.

3.3 제안 기법(LDK+)

본 논문에서 제안하는 스킴 LDK+는 그리드 정보를 활용하여 이웃 노드로부터 논스를 보정하는 단계를 추가하였고 새로운 키 생성과정을 고안하였다. 기존의 LDK와 마찬가지로 각 센서 노드는 사전에 k_c, H를 저장하고 추가로 G를 저장한다. 추가된 그리드 정보는 센서 노드가 배치될 그리드 좌표와 이웃 8방향의 그리드 좌표로 구성된 총 9개의 그리드 좌표이다. 이는 센서 노드가 지정된 그리드 위치에 벗어난 상황도 고려하였고 [11] 이는 해당 그리드 내에 위치해야 한다는 기존 그리드 기반 연구의 제약조건을 약화시키는 역할을 한다. Fig. 2는 제안 스킴인

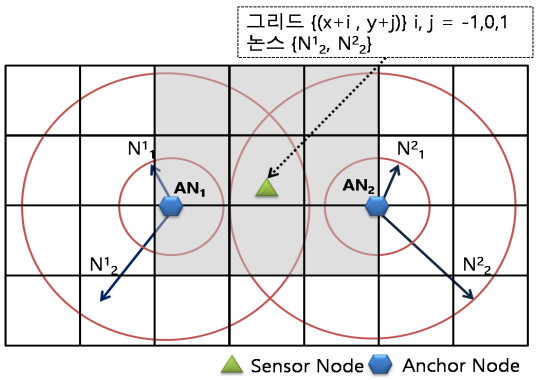

Fig. 2. Illusion of the proposed scheme

LDK+의 구성 형태를 나타낸다. 센서 노드 간의 키 생성은 사전 분배 단계, 초기화 단계, 키 생성 단계, 키 동의 단계의 총 4단계로 이루어진다. 다음은 키 생성의 각 단계를 자세히 설명한다.

3.3.1 사전 분배 단계

사전 분배 단계에서는 센서 노드가 배치되기 전 키 관리에 필요한 정보들을 사전에 저장한다. 센서 노드에 저장되는 요소로는 공유키가 생성되기 전에 암호화 통신을 위한 네트워크 키 k_c, 키 생성에 활용되는 해시 함수 H, 9개의 그리드 정보 G이다. 다음의 식 1은 사전 분배 단계의 알고리즘을 나타낸다.

$$\begin{aligned} &AN_{set} = AN_1, AN_2, \cdots, AN_n \\ &SN_{set} = SN_1, SN_2, \cdots, SN_m \\ &SN_{set} \leftarrow K_c, G, H \end{aligned} \tag{1}$$

3.3.2 초기화 단계

초기화 단계는 센서 노드가 AN으로부터 논스를 전달받는 과정이다. 이 단계에서 논스 보정과정이 이루어진다. AN은 전송 세기를 달리하여 센서 노드에 k_c로 암호화한 논스를 전달한다. 이후 센서 노드는 자신이 배치될 그리드의 좌표를 k_c로 암호화하여 주변 노드에 전송한다. 동일한 그리드 좌표를 가지고 있는 주변 센서 노드는 자신이 받은 논스의 개수를 센서 노드에 전송하고 전송받은 논스의 개수가 자신이 가지고 있는 논스의 개수보다 크다면 해당 주변 센서 노드에 논스를 요청하는 메시지를 전송하여 주변 노드로부터 논스를 보정 받는다. 센서 노드는 보정 과정을 통하여 정상적인 시나리오에서 받아야 하는 논스와는 다른 논스들을 가질 수 있지만 해당 보정 과정은 전송받는 논스의 종류보다 개수를 증가시키는 거에 목적이 있다고 볼 수 있다. 다음의 식 2는 초기화 단계의 알고리즘을 나타낸다. 여기서 N_{uv}는 u번째의 AN에서 v의 전파 세기로 전송된 논스를 의미한다. 또한, SN_o, SN_l은 임의의 노드를 가리킨다.

$$\begin{aligned} &AN_{set} \rightarrow SN_{set}: E_{K_c}(N_{uv}) \\ &(1 \le u \le n, 1 \le v \le powerlevel) \\ &SN_o \rightarrow SN_l: E_{K_c}(G(x,y)) \\ &SN_l \rightarrow SN_o: E_{K_c}(C_n) \\ &SN_o: IF\ C_n\ of\ SN_o < C_n\ of\ SN_l \\ &\qquad SN_o \rightarrow SN_l: request\ nonces \\ &\qquad SN_l \rightarrow SN_o: ACK(E_{K_c}(N_r)) \\ &\qquad\qquad (1 \le r \le C_n\ of\ SN_l) \end{aligned} \tag{2}$$

3.3.3 키 생성 단계

키 생성 단계에서는 센서 노드가 가지고 있는 논스와 9개의 그리드 정보를 조합하여 키를 생성한다. 따라서 (논스의 개수 * 9)개의 키를 생성할 수 있다. 하나의 논스와 하나의 그리드 정보를 합친 후 사전키를 이용하여 해시함수를 하여 하나의 키를 생성하고 논스는 삭제한다. 다음의 식 3은 키 생성 단계의 알고리즘을 나타낸다.

$$SN_{set}: K_t = H_{K_c}(N_r \mid G(x,y)) \tag{3}$$

3.3.4 키 동의 단계

키 동의 단계에서는 이웃 노드와 공유키를 생성한다. 센서 노드는 자신이 생성한 모든 키를 암호화하고 이에 대한 MAC값을 붙인다. 해당 MAC값은 전송하는 키 집합의 무결성을 보장한다. 이웃 노드는 전송받은 키 중에 같은 키가 있는지 확인하고 일정 개수 이상의 키가 같다면 동일한 키들을 XOR 연산하여 공유키를 생성한다. 다음의 식 4는 키 동의 단계의 알고리즘을 나타낸다. 여기서 $k_1, k_2, \cdots, k_t$ 는 노드가 식 3을 통해 논스와 그리드 정보를 사용하여 생성한 각각의 키를 의미한다.

$$\begin{aligned} &SN_o \rightarrow *: E_{K_c}(K_1 \| K_2 \| \cdots \| K_t) \mid MAC \\ &SN_*: IF\ Num\ of\ common\ key > q \\ &\qquad SN_l \rightarrow SN_o: E_{K_c}(K_q) \mid MAC \\ &\qquad SN_o, SN_l: K_s = K_i \oplus \ldots \\ &\qquad\qquad (K_i \in K_q, i = 1,2,\cdots,q) \\ &\quad ELSE \\ &\qquad SN_l \rightarrow SN_o: none\ msg \end{aligned} \tag{4}$$

3.3.5 노드 추가 및 폐지

네트워크가 구성된 후 새로운 센서 노드가 추가될

수 있고 배터리가 방전되거나 악의적인 공격에 손상되어 노드를 폐지해야 할 경우가 생길 수 있다. 노드 추가 프로세스는 다음의 과정을 거쳐 이루어진다.

1) 추가 노드 :베이스 스테이션에 배치될 지역의 그리드 정보와 자신에 대한 인증을 요청

2) 베이스 스테이션 : 노드를 인증 후 해당 노드에 대한 작은 크기의 키 풀을 생성하여 노드에 전달

3) 추가 노드 : 배치된 노드는 주변 노드에게 아이디와 그리드 정보를 전송하여 노드 추가 이벤트를 알림

4) 이웃 노드 : 주변 노드 중 같은 그리드 정보를 가지고 있는 노드만 이웃 노드로 인식하고 추가된 노드의 아이디와 함께 베이스 스테이션에 링크키 요청

5) 베이스 스테이션 : 추가된 노드에 대한 키 풀에서 랜덤으로 하나의 키와 해당 인덱스를 추출하여 전송

6) 이웃 노드 : 추가된 노드에게 해당 키 인덱스를 전달하여 새로운 링크키를 공유

5) 과정에서 베이스 스테이션에서 노드까지의 키 전송은 멀티 홉 링크키로 암호화되어 안전하게 해당 노드까지 전달된다. 또한, 각 노드들은 주기적으로 자신이 네트워크에 참여하고 있음을 알리는 상태 알림 메시지를 전송한다. 이 메시지가 일정 간격으로 오지 않을 경우 베이스 스테이션에 해당 노드에 대한 폐지 요청을 한다. 베이스 스테이션은 해당 노드의 상태확인 요청을 하여 상태를 확인한 후 최종적으로 모든 노드에게 해당 노드가 폐지되었음을 알려 해당 노드에 대한 링크키를 삭제한다.

기존의 LDK는 AN이 주기적으로 새로운 논스를 전송하여 키를 갱신하였다. 하지만 주기적인 키 생성 과정은 많은 통신과 계산 과정이 필요하다. 이는 무선 센서 네트워크의 생명주기와도 연결되는 문제이다. 또한, 노드가 탈취되어 네트워크 키가 노출되었을 경우 새롭게 전송되는 논스가 노출될 수 있다. 따라서 본 논문에서 제안하는 LDK+에서는 네트워크 키는 네트워크 초기화에만 사용하여 네트워크 키 사용을 제한하면서 노드의 추가 및 폐지를 제공한다.

IV. 분 석

기존 논문에서 스킴의 효율성과 보안성을 측정하는 지표로서 활용하고 있는[2, 12, 3] 접속율과 절충율 분석을 위해 MATLAB을 활용하여 시뮬레이션을 진행하였다.

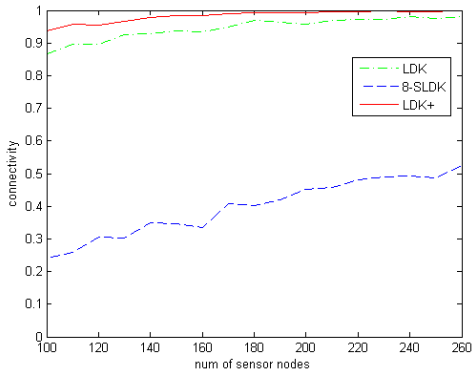

Fig. 3. Connectivity according to number of sensor nodes

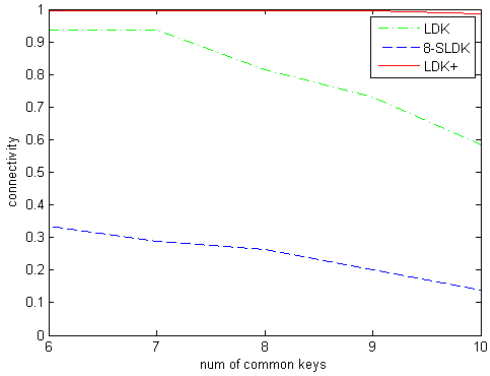

Fig. 4. Connectivity according to number of common keys

4.1 접속율 (Connectivity)

접속율은 이웃 노드와 암호화 통신을 위해 상호간에 키를 동의할 확률을 나타내는 것을 의미한다. 랜덤으로 분배되는 정보를 활용하여 노드 간에 키를 생성하기 때문에 두 노드가 통신 범위 안에 있어도 키를 생성하지 못할 가능성이 있기 때문에 접속율은 무선 센서 네트워크의 효율성을 나타내는 지표로서 활용된다.

센서 노드를 설치할 지역을 20 x 20 그리드로 분할하였고 그리드 당 AN을 배치하여 총 400개의 AN이 설치된 환경을 가정하고 LDK와 LDK+ 각각의 접속율을 측정하였다. 사용된 수치는 같은 환경에서 총 10번의 시뮬레이션을 통해 계산된 평균값을 사용하였다. 위에서 가정한 환경에서 AN의 전파 세기는 2단계로 나뉘고 통신 범위는 1 유닛 (unit)으로 설

Table 4. Summary of simulation results

Comparison		LDK	8-SLDK	LDK+
Connectivity	The num of nodes	High	Low	High
	The num of common keys	High (Up to 7)	Low	High (Holding up to 10)
Compromise ratio		Low	Very low	Low

정하고 SN의 통신 범위는 2 유닛으로 설정하였다. 또한 C_{common}는 6으로 설정하였다. Fig. 3은 위의 환경에서의 LDK, 8-SLDK[9], LDK+의 접속율에 대한 시뮬레이션 결과이다. LDK+가 LDK보다 접속율이 높았고 센서 노드의 수가 증가할수록 접속율이 증가하였다. Fig. 4는 각 스킴의 C_{common}에 따른 접속율을 나타낸다. 통신 범위가 3 유닛인 센서 노드를 150개 무작위로 배치하는 환경에서 C_{common}의 변화에 따른 접속율을 비교했을 때 LDK는 떨어지는 반면 LDK+는 유지하였다. 전체적으로 8개의 섹터로 나눈 8-SLDK의 접속율은 낮게 측정되었다.

이밖에도 다양한 환경을 가정하여 시뮬레이션을 진행하였다. 100개의 센서 노드를 배치하고 C_{common}을 1로 하였을 경우 각 센서 노드의 통신 범위가 2 유닛일 때의 접속율은 0.933이었고 3 유닛일 때는 1 이었다. 결국, 접속율은 배치된 각각의 센서 노드의 통신 범위 내에 이웃 노드가 있다면 통신이 이루어지는 것으로 보인다. 이상적으로 센서 노드가 고르게 퍼져 배치되었다면 센서 노드 간의 접속율을 1로 설정하여 네트워크를 구성할 수 있을 것이다.

제안 스킴에서 보안성에 영향을 끼치는 C_{common}에 따른 접속율은 AN으로부터 받은 논스의 개수에 따라 달라질 수 있다. 가정한 네트워크에서 각 센서 노드는 평균적으로 15개의 논스를 전송받았다. 이때 C_{common}이 증가할수록 접속율이 낮아졌는데 LDK는 6일 때 상대적으로 급격하게 떨어진 반면 LDK+는 19일 때 급격하게 떨어졌다. 따라서 LDK+에서는 C_{common}이 18로 설정하였을 때 가장 보안성을 높일 수 있는 한계치라 여겨진다.

AN의 개수는 센서 네트워크를 형성하는 비용과 관련이 있다. AN의 개수를 줄이면서 동시에 기존의 접속율을 유지할 수 있다면 네트워크 생성 비용을 절감할 수 있다. AN의 수를 줄이려는 방법으로 육면체(Hexagon) 형태의 배치 방식으로 AN를 배치하여 시뮬레이션을 수행하였다. 기존의 400개의 AN이 배치된 환경에서 육면체 형태로 배치하였을 때 200개의 AN을 가지고 네트워크를 형성할 수 있다. AN의 통신 범위를 1.6 유닛으로 하고 나머지 조건은 기존 시뮬레이션과 동일하게 하였을 경우 100개의 센서 노드의 접속율은 기존의 환경과 거의 동일하였다. 따라서 육면체 형태로 배치하였을 경우 AN의 개수는 줄이면서 거의 동일한 접속율을 유지할 수 있음을 시뮬레이션을 통하여 확인하였다.

4.2 절충율 (Compromise ratio)

절충율은 탈취 공격에 의해 노출된 정보가 전체 네트워크에 미치는 영향력으로서 무선 센서 네트워크에서의 보안성을 나타내는 지표이다.

절충율에 대한 시뮬레이션은 Chan 등의 논문에서 식 5를 참고하였다[12]. m은 한 센서 노드가 보유한 키 링의 크기, S는 키 풀의 크기, x는 탈취된 노드 수, q는 두 노드 간 키 생성 시 최소 공유되어야하는 최소의 키 개수를 나타낸다.

$$\sum_{i=q}^{m}(1-(1-\frac{m}{|S|})^{x})^{i}\frac{p(i)}{p} \quad (5)$$

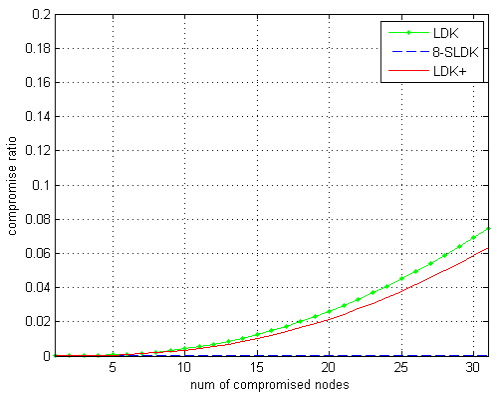

Fig. 5. Comparison of compromise ratio

Fig. 5는 시뮬레이션 결과를 나타낸다. LDK와 8-SLDK는 m의 크기를 7로 설정하였고 LDK+는 63으로 설정하였다. LDK+는 9개의 그리드 정보와 조합하여 키를 생성하기 때문에 보유하게 되는 키의 개수가 높게 측정되었기 때문이다. C_{common}이 6일 때 전체적으로 절충율은 0.08이하로 낮게 측정되었다. LDK+의 절충율은 LDK보다는 낮지만 8-SLDK보다는 높았다. 하지만 C_{common}이 6일 때 LDK+는 8-SLDK에 비해 접속율이 높기 때문에 실현가능성은 LDK+가 높을 것이다.

4.3 시뮬레이션 요약

시뮬레이션 결과를 종합하자면 보안성을 높인 환경에서 LDK+는 높은 접속율을 보였고 절충율은 상대적으로 LDK보다는 낮고 8-SLDK보다는 높았지만 절대적인 수치 자체가 낮음을 확인하였다. Table 2는 시뮬레이션 결과를 요약한 내용이다.

V. 결 론

본 논문에서는 F. Anjum의 스킴인 LDK[3]를 개선하는 스킴 LDK+를 제안하였다. 기존 AN의 전파 세기에 따라 논스를 전송하여 지역을 분할하는 방식에 그리드 정보를 활용한 키 보정과정을 추가하였고 그리드 정보를 조합한 키 생성과정을 제안하였다. 이는 간섭으로 발생할 수 있는 논스 개수 부족 현상을 방지하고자 하였다.

시뮬레이션을 통하여 특정 환경에서 LDK에 비해 LDK+가 접속율은 높고 절충율은 낮음을 보임으로써 배치된 노드가 정상적으로 이웃 노드와의 통신 가능성 측면에서의 안정성과 정보 노출이 네트워크에 영향을 끼치는 정도 측면에서의 보안적인 측면이 강화되었음을 확인하였다. 또한, 육면체 형태의 AN 배치를 통해 AN의 수를 줄이면서 거의 동일한 접속율을 유지하여 네트워크 생성 비용을 줄일 수 있음을 확인하였다.

References

[1] L. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Infomatics, vol. 10, no. 4, pp. 2233-2243, Jan. 2014.

[2] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proceedings of the 9th ACM conference on Computer and communication security, pp. 41-47, Nov. 2002.

[3] F. Anjum, "Location dependant key management in sensor networks without using deployment knowledge," Wireless Networks, vol. 16, no. 6, pp. 1587-1600, Aug. 2010.

[4] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware Key Management Scheme for Wireless Sensor Networks," Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 29-42, Oct. 2004.

[5] T. Ito, H. Ohta, N. Matsuda, and T. Yoneda, "A Key Pre-Distribution Scheme for Secure Sensor Networks Using Probability Density Function of Node Deployment," Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 69-75, Nov. 2005.

[6] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," ACM Transactions on Information and System Security, vol. 8, no. 1, pp. 47-77, Feb. 2005.

[7] W. Du, J. Deng, Y. Han, and P. Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 1, pp. 62-77, Jan.-Mar. 2006.

[8] F. Anjum, "Location dependent key management using random key-predistribution in sensor networks," Proceedings of the 5th ACM workshop on Wireless security, pp. 21-30, Sep. 2006.

[9] M. Faghani and S. Motahari, "Sectorized Location Dependent Key Management," Proceedings of Wireless and Mobile Computing, Networking and Communications, pp. 388-393, Oct. 2009.

[10] Y. Wu, J. Stankovic, T. He, and S. Lin, "Realistic and Efficient Multi-Channel Communications in Wireless Sensor Networks," Proceedings of the IEEE INFOCOM 2008, pp. 13-18, April. 2008.
[11] T. Kwon, J. Lee, and J. Song, "Location-Based Pairwise Key Predistribution for Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 8, no. 11, pp. 5436-5442, Nov. 2009.
[12] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proceedings of the 2003 IEEE Symposium on Security and Privacy, pp. 197-213, May. 2003.
[13] Gartner Says the Internet of Things, http://www.gartner.com/newsroom/id/2684915, 2014.

〈저자소개〉

최 재 우 (Jaewoo Choi) 학생회원
2014년 2월: 한국산업기술대학교 게임공학과 졸업
2014년 3월~현재: 연세대학교 정보대학원 석박통합과정
〈관심분야〉 정보보호, 센서 네트워크 보안 등

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 공학박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, HCI 보안 등

김 용 현 (Yonghyun Kim) 정회원
1993년 2월: 광운대학교 전자공학과 학사
1995년 2월: 광운대학교 전자공학과 석사
2013년 2월: 광운대학교 전자통신공학과 공학박사
1995년 1월~현재: 국방과학연구소 책임연구원
〈관심분야〉 센서네트워크 보안, 센서노드 배치, 센서신호처리 등

김 주 엽 (Juyoub Kim) 정회원
1992년 2월: 경기대학교 경영정보학과 학사
1995년 7월: 서강대학교 경영학과(MIS) 석사
1995년~1999년: 국방정보체계연구소
1999년~현재: 국방과학연구소
〈관심분야〉 무선센서네트워크, 네트워크 프로토콜, HLA 등