Journal of Korean Institute of Intelligent Systems, Vol. 23, No. 6, December 2013, pp. 558-564
http://dx.doi.org/10.5391/JKIIS.2013.23.6.558

LEAP기반의 무선 센서 네트워크에서 가변적 상태를 고려한 에너지 효율적 다음 홉 노드 선택 기법

Dynamic States Consideration for Next Hop Nodes Selection Method to Improve Energy Efficiency in LEAP based Wireless Sensor Networks

남수만* · 조대호*†
Su-Man Nam, and Tae-Ho Cho†

*성균관대학교 정보통신대학
† College of Information and Communication Engineering, Sunkyunkwan University

요 약

무선 센서 네트워크는 제한된 에너지 자원을 포함하고 개방된 환경에서 스스로 운영된다. 이러한 센서 노드들은 한 필드에서 스스로 운영되기 때문에 싱크홀 공격이 쉽게 발생되어 공격자를 통해 센서들을 훼손시킬 수 있다. 싱크홀 공격은 초기에 구성된 라우팅 경로를 변경하여 훼손된 노드에서 중요한 정보를 탈취한다. LEAP은 싱크홀 공격에 반대하여 네 개의 키를 사용하여 모든 노드의 상태와 패킷을 인증하기 위해 제안되었다. 이 기법은 베이스 스테이션까지 패킷들을 안전하게 전송함에도 불구하고, 패킷들은 다음 홉 노드 상태 확인 없이 구성된 경로를 따라 전달된다. 본 논문에서, 우리는 이 문제를 해결하기 위해 에너지 효율성을 위한 다음 홉 노드 선택 기법을 제안한다. 우리의 제안 기법은 잔여 에너지, 공유된 키의 수, 여과된 허위 패킷의 수를 간주하여 다음 홉 노드를 평가한다. 설정된 임계값에 대해서 다음 홉 노드의 적합성 기준을 만족할 때 패킷은 다음 홉 노드에 전송된다. 우리는 효과적인 노드 선택을 통해 에너지 효율성과 공격 발생 지역의 우회를 향상시키는 것을 목표로 한다. 실험 결과는 LEAP과 비교하였을 때 싱크홀 공격에 반대하여 최대 6%의 에너지 절약과 함께 제안 기법의 타당성을 보여준다.

키워드 : 무선 센서 네트워크, 네트워크 보안, 로컬 암호화 인증 기법, 싱크홀 공격, 다음 홉 노드 선택

Abstract

Wireless sensor networks (WSNs) contain limited energy resources and are left in open environments. Since these sensor nodes are self-operated, attacks such as sinkhole attacks are possible as they can be compromised by an adversary. The sinkhole attack may cause to change initially constructed routing paths, and capture of significant information at the compromised node. A localized encryption and authentication protocol (LEAP) has been proposed to authenticate packets and node states by using four types of keys against the sinkhole attack. Even though this novel approach can securely transmits the packets to a base station, the packets are forwarded along the constructed paths without checking the next hop node states. In this paper, we propose the next hop node selection method to cater this problem. Our proposed method evaluates the next hop node considering three factors (i.e., remaining energy level, number of shared keys, and number of filtered false packets). When the suitability criterion for next hop node selection is satisfied against a fix threshold value, the packet is forwarded to the next hop node. We aim to enhance energy efficiency and a detour of attacked areas to be effectively selected Experimental results demonstrate validity of the proposed method with up to 6% energy saving against the sinkhole attack as compared to the LEAP.

Key Words : Wireless sensor networks, Network security, Localized encryption and authentication protocol, Sinkhole attack, Next hop node selection

접수일자: 2013년 3월 31일
심사(수정)일자: 2013년 4월 7일
게재확정일자 : 2013년 11월 17일
† Corresponding author
이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A2A2A01013971).

1. 서 론

무선 센서 네트워크(wireless sensor networks)는 자동화된 원격 정보 수집을 목적으로 과학적, 의학적, 군사적, 상업적 용도 등 다양한 응용 개발에서 폭넓게 활용된다[1, 2]. 이러한 무선 센서 네트워크는 이벤트를 감지(sensing), 계산(computing), 그리고 무선 통신(wireless communication)하는 다수의 센서 노드와 그 센서들로부터 이벤트 보고서(event report)를 수집하여 사용자에게 정보를 제공하는 베이스 스테이션(base station; 이하 BS)으로 구성한다[1]. 하지만 센서 노드는 소형 하드웨어의 구성과 개방된

환경의 운영으로 에너지, 메모리, 통신 범위 등의 제약을 통해 공격자가 쉽게 네트워크를 훼손시킬 수 있다[3].

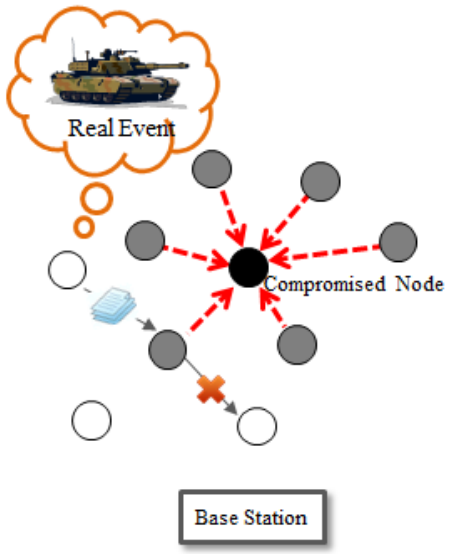


그림 1. 센서 네트워크에서 싱크홀 공격
Fig. 1. Sinkhole attacks in a sensor network

그림 1은 한 센서 네트워크에서 훼손된 노드로부터 발생하는 싱크홀 공격[3, 4]을 보여준다. 이 공격은 공격자가 한 센서 노드를 훼손시키고, 그 훼손된 노드로부터 주변의 노드에 허위 HELLO 메시지[5]를 전달하여 라우팅 경로를 변경시켜 자신을 베이스 스테이션처럼 위장시킨다[3, 4]. 만약 공격당한 한 중계 노드가 한 보고서를 받았다면, 그 중계 노드는 훼손된 노드에 그 보고서를 전달하고, 그 훼손된 노드는 그 보고서를 파괴하여 데이터 전달을 방해한다. 게다가, 싱크홀 공격은 훼손된 노드를 통해 베이스 스테이션이 알기 어렵게 공격을 시도하기 때문에 모든 패킷(보고서, 메시지)은 키들을 통하여 보안 강화를 위한 암호화 통신이 요구된다.

이러한 공격의 피해를 줄이기 위해 Zhu 등은 로컬 암호화 인증 기법(localized encryption and authentication protocol; 이하 LEAP)[4]을 제안하였다. LEAP은 센서 네트워크에서 단일 키의 메커니즘 운영과 달리 보안 강화를 충족시키기 위해 두 노드 사이에서 4개의 키를 통하여 메시지와 보고서를 인증한다. 이 프로토콜은 4개의 키를 통해 훼손된 노드로부터 발생하는 메시지와 보고서를 검증하여 공격 피해의 확산을 줄인다. 그렇지만, 이 기법은 두 노드 사이에서 강력한 검증 수행에도 불구하고 보고서를 보내기 전에 다음 홉 노드 선택을 통하여 에너지 절약을 위한 전송과 안전한 경로를 위한 전달이 필요하다.

본 논문에서는 효율적인 다음 홉 노드 선택을 통해 에너지 효율성을 향상시키고 안전한 경로로 보고서를 전달하는 방법을 제안한다. 제안 기법에서는 부모 노드가 보고서를 다음 홉 노드(자식 노드)에 전달하기 전에 그 노드의 적합성을 평가한다. 다음 홉 노드의 적합성은 세 개의 입력 요소(에너지 잔여량, 이웃 노드와 공유하는 키의 수, 제거된 허위 메시지의 수)를 통해 평가되고, 부모 노드에게 알린다. 만약 평가된 적합성이 임계값을 만족한다면, 그 부모 노드는 다음 홉 노드를 선택한다. 그래서 우리의 제안 기법은 실험 결과에서 보듯이 다음 홉 노드 선택을 통해 LEAP과 비교하였을 때 같은 보안 레벨을 유지하고 에너지를 절약시킨다.

본 논문의 2장에서는 LEAP과 동기에 대해 설명하고 3장에서는 제안 기법을 상세히 설명한다. 4장에서는 LEAP과 비교한 실험 결과를 보여주고, 5장에서 결론 및 향후 연구에 관해 서술한다.

2. 배경 및 동기

이 장에서는 안전한 키 관리 프로토콜인 LEAP과 본 논문의 동기에 대해서 설명한다.

2.1 로컬 암호화 인증 기법(LEAP)

LEAP[4]은 일부 지역의 훼손 노드로부터 이웃 노드의 피해를 줄이기 위해 센서 네트워크를 위한 키 관리 프로토콜(key management protocol)인 LEAP을 제안하였다. LEAP은 서로 다른 특징의 네 가지 키를 사용하고, 키의 설명은 다음과 같다.

- Individual Key (IK): 한 노드와 BS가 공유하는 키로, 이벤트 감지 시 메시지 인증 코드(message authentication code)[6] 생성을 위해 사용
- Pairwise Key (PK): 이웃 노드와 공유하는 키로, 보고서가 전달할 때 다음 지역에 위치한 클러스터 헤더(cluster header; 이하 CH) 노드 인증을 위해 사용
- Cluster Key (CK): 한 클러스터 내에서 모든 이웃 노드와 공유하는 키로, 클러스터 헤더(cluster header; 이하 CH)의 노드 인증을 위해 사용
- Group Key (GK): 네트워크에 있는 모든 노드와 고유한 키로, 모든 메시지의 복호화를 위해 사용

일반적으로 노드의 IK는 일반 데이터를 암호화하고, PK와 CK는 주변의 이웃 노드를 인증하고, GK는 메시지를 인증 인증을 통해 훼손 노드로부터 센서 네트워크의 생존 가능성을 극대화한다[7].

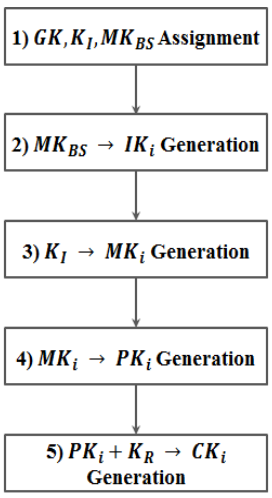
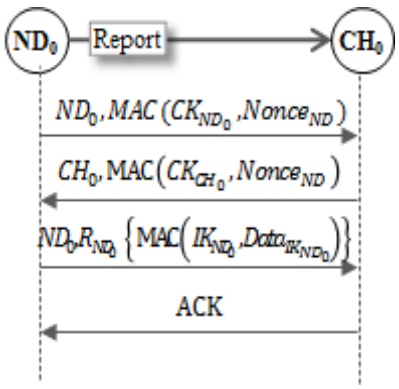
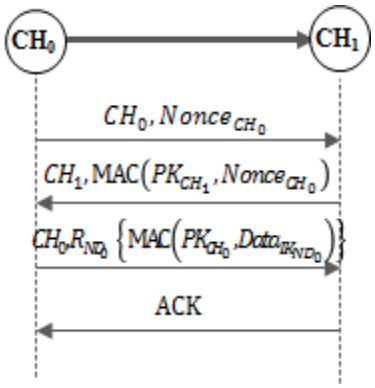


그림 2. 키 생성 과정
Fig. 2. Key generation process

그림 2는 4개의 키 생성 과정을 보여준다. 키들의 생성은 다음과 같은 과정을 통해 보여준다. 센서 노드가 배치되기 전에 BS는 1) 모든 노드에 GK, K_I (Initial Key), BS의 Master key (MK)를 할당하고, 2) BS의 MK를 통해 각 노드의 IK를 생성한다. 3) BS로부터 할당받은 K_I를 통해 각 노드의 MK를 생성하고, 4) 각 노드의 MK를 통해 이웃 노드와 공유하는 PK를 생성한다. 마지막으로 5) 각 노드에서 생성된 PK와 랜덤 함수를 통해 CK를 생성한다. 그리하여 LEAP은 위의 다섯 과정을 통해 네 개의 키를 생성한다.



(a)



(b)

그림 3. 두 노드 사이의 키 인증: (a) 일반 노드와 CH 사이의 인증, (b) CH들 사이의 인증
Fig. 3. Key authentication between two nodes: objects are (a) authentications between a normal node and a CH, (b) authentications between two CHs

그림 3은 일반 노드와 CH, 그리고 두 CH 사이에서 키 인증 방법을 나타낸다. 우리는 ND를 일반 노드로, CH를 클러스터 헤더 노드로 간주한다. 그림3-(a)는 같은 클러스터 내에서 ND와 CH 사이의 키 인증 과정을 보여준다. ND_0에서 이벤트 보고서를 전달하기 전에 ND의 CK와 임시 값(Nonce)이 포함된 맥을 CH_0에 전송한다. CH_0는 자신의 CK를 통해 그 맥을 인증하고, 새로운 맥을 생성하여 응답한다. ND_0는 CH_0로부터 받은 맥을 인증하고, 보고서를 CH_0에 보낸다. CH_0는 보고서를 받은 후 ACK (acknowledgement) 메시지를 ND_0에 보낸다. 그림3-(b)는 다른 클러스터에서 두 CH 사이의 키 인증 과정을 보여준다. CH_0는 보고서를 전달하기 전에 CH_1에 임시 값을 전달한다. CH_1은 자신의 PK와 함께 전달받은 임시 값을 CH_0에 보낸다. CH_0는 전달받은 맥을 자신의 PK를 통해 인증하고, 보고서를 CH_1에 보낸다. 보고서를 받은 CH_1은 ACK 메시지로 응답한다. 이러한 과정을 반복하여 LEAP은 두 노드 사이의 인증을 통해 다음 홉 노드를 보증하고 안전한 경로로 보고서를 BS까지 보낸다. 반면에, 공격자가 한 노드를 훼손시켜 싱크홀 공격을 위해 허위 HELLO 메시지[5, 8]를 이웃 노드들에 전달한다면, 이웃 노드들은 자신의 CK와 GK를 사용하여 그 허위 메시지를 제거한다.

2.2 동기

센서 네트워크는 센서 노드의 제한적인 하드웨어 특징 때문에 공격자는 한 노드를 훼손시켜 싱크홀 공격을 쉽게 발생시킨다. 이 공격을 효과적으로 탐지하기 위해 LEAP은 네 개의 키들을 통해 훼손된 노드로부터 발생한 허위 HELLO 메시지를 감지한다. 하지만 초기에 설정된 경로는 센서 네트워크 상태에 따라 에너지 향상과 공격 발생 지역을 우회하기 위해 전송 과정에서 라우팅 경로를 변경해야 한다. 그리하여 우리의 제안 기법은 한 평가 함수를 통해 다음 홉 노드 상태를 고려하여 효과적인 다음 홉 노드를 선택한다.

3. 제안 기법

이 장에서는 제안 기법에 대해 상세히 기술하겠다.

3.1 가정

센서 네트워크의 센서 노드는 MICA2 mote[9]를 사용을 가정한다. 모든 센서 노드는 cluster based model을 통해 센서 필드에 균일하게 배치된다. 초기 라우팅 패스는 directed diffusion[10]과 minimum cost forwarding algorithm[11]을 통해 구성된다. 모든 보고서는 베이스 스테이션을 향해 전송된다.

3.2 제안기법

본 논문에서, 제안 기법은 평가 함수를 통해 다음 홉 노드를 효율적으로 선택해서 전체 네트워크의 에너지 효율성을 향상한다. 제안 기법에서 모든 센서 노드는 LEAP과 같이 초기에 4개의 키를 생성한다. 한 지역에서 이벤트가 발생하였을 때 보고서를 생성하고 다음 CH(자식 CH)에 보고서를 전송한다. 이때, 한 중계 CH(부모 CH)는 자식 CH의 상태를 고려하여 전송을 결정한다. 그 부모 CH는 보고서를 다음 CH에 보내기 전에 그 자식 CH의 적합성을 평가한다. 만약 그 부모의 적합성이 임계 값 이하라면, 그 부모 CH 범위 내에서 새로운 CH를 선택하고 적합성이 임계 값보다 큰 새로운 자식 CH를 선택한다. 다음은 다음 홉 노드 선택하는 단계이다.

- 단계 1: 한 부모 CH는 이미 설정된 경로에서 한 자식 CH에 임시 값을 전송
- 단계 2: 그 자식 CH는 평가 함수를 통해 결과 도출한 다음 부모 CH에 알림
- 단계 3: 만약 도출한 적합성이 임계 값 이하라면, 부모 CH는 자신의 범위 내에서 새로운 노드 탐색하고, 단계

1과 단계 2 반복하고, 새로 찾은 자식 CH의 적합성이 임계 값 이상이라면 그 부모 CH는 새로운 자식 CH에 보고서 전달

- 단계 4: 보고서를 전달 받은 새로운 CH는 부모 CH에 ACK 메시지 전송

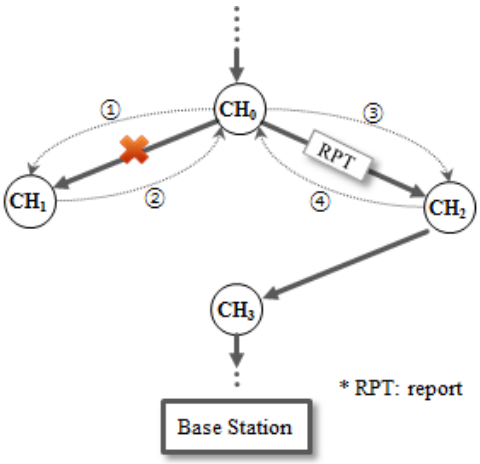


그림 4. 다음 홉 노드 선택
Fig. 4. Next hop node Selection

그림 4는 중계 CH에서 보고서를 전달하기 위해 자식 CH를 선택하는 과정을 보여준다. CH_0는 한 중계 CH(부모 CH)이며 보고서 전달을 위해 다음 CH(자식 CH)를 선택하고, CH_1과 CH_2는 CH_0의 이웃 CH들이다. CH_0과 CH_1 사이의 경로는 센서 노드 배치 후에 초기에 설정되었다. CH_0는 보고서를 받은 후에 이미 경로가 설정된 다음 CH에 보고서를 전달하기 전에 한 평가 함수를 통해 CH_1의 적합성을 평가한다. 평가된 적합성은 CH_0에 전달되고, CH_0는 초기에 설정된 임계 값과 비교한다. CH_1의 적합성이 임계 값 이하라면 CH_0는 자신의 범위 내에서 CH_2를 찾고, CH_2의 적합성을 평가한다. CH_0는 CH_2의 적합성 만족에 따라 CH_2에 보고서를 전달한다. 전달된 보고서는 CH_3를 거쳐 다중 홉을 거쳐 BS까지 전송된다.

3.3 평가 함수

제안 기법은 기본 정보 중에서 다음 홉 노드 상태의 적합성을 평가하기 위한 효율적인 입력 요소 세 개를 고려한다. 그 입력 요소들은 센서 노드의 잔여 에너지 레벨(ENG), 이웃 노드가 공유하는 PK의 수(NPK), 그리고 노드가 제거된 허위 메시지 수(NFM)이다. 평가 함수의 식은 다음과 같다.

$$f(i) = \frac{ENG + NPK}{NFM} \quad (1)$$

식 (1)에서 i는 각 센서 노드의 식별자(ID)이다. 입력 요소에서 ENG는 노드의 잔여 에너지 레벨로 앞으로 그 노드가 운영될 상태를 나타내며, NPK는 이웃 노드와 공유하는 키의 수로 보고서가 전달될 수 있는 다음 CH를 의미한다. NFM은 각 노드에서 제거된 허위 메시지 수로 훼손된 노드로부터의 피해를 말한다. 그래서 우리는 ENG와 NPK를 통해 효율적인 다음 홉 노드의 선택을 유도하고, NFM를 사용하여 증가한 허위 메시지를 피해 다음 홉 노드의 선택을 막는다. 만약 NFM이 '0'이라면, 우리는 기본으로 '1'를 설정한다.

3.4 다음 홉 노드 선택의 예

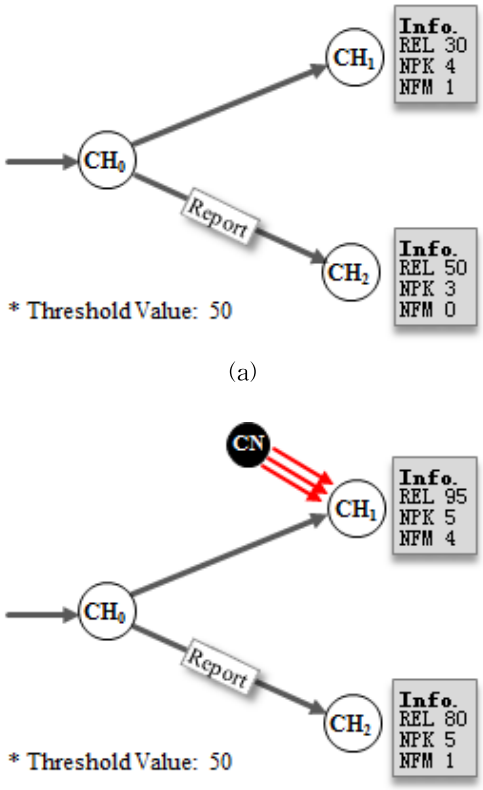


그림 5. 다음 홉 노드 선택의 예: (a) 정상 상태에서 다음 홉 노드 선택 (b) 공격 발생 상태에서 다음 홉 노드 선택
Fig. 5. Examples of next hop node's selection: objects are (a) next hop node selection for normal states, (b) next hop node selection for attack generations

그림 5는 다음 홉 노드 선택의 예를 보여준다. 우리는 그림 5의 (a)와 (b)에서 CH_0는 부모 CH 노드이고, CH_1과 CH_2는 CH_0의 자식 CH로 간주한다. 또한, CH_0과 CH_1 사이의 경로는 초기에 설정되었다. 그림 5의 (a)에서 CH_0는 CH_1에 보고서를 전달하기 전에 CH_1의 상태를 요청한다. CH_1은 평가 함수에 따라 결과가 34(=(30+4)/1)이기 때문에 이미 설정된 임계값과 비교한 후 자신의 주변에서 다른 노드를 찾는다. 탐색된 CH_2는 평가 함수에 의해 결과가 53(=(50+3)/1)이기 때문에 다음 홉 노드로 적합하다. 그래서 CH_0는 다음 CH의 에너지 상태와 이웃의 수를 고려하여 통신의 수를 줄이기 때문에 에너지를 절약하고 보고서를 BS까지 전달한다. 그림 5의 (b)에서 CH_1과 CH_2는 평가 함수에 따라 25(=(95+5)/4), 85(=(80+5)/1)이기 때문에 다음 홉 노드는 CH_2가 된다. 이러한 과정의 반복하여 보고서는 여러 중계 CH들을 거쳐 BS까지 안전한 경로로 전달된다.

4. 실험 결과

우리의 실험 결과는 제안 기법과 LEAP의 성능을 비교하였다. 한 센서 필드의 크기는 1,000×1,000m^{2}고, 한 클러스터 크기는 100×100m^{2}로서 그 센서 필드에 100개의 클러스터가 구성된다. 한 클러스터는 한 개의 CH 노드와 아홉 개의 일반 노드들이 균일하게 배치된다. 각 노드는 한 바이트 기준으로 데이터를 보낼 때 에너지가 16.25μJ이 소모되고, 받을 때 12.5μJ이 소모되며, 맥을 만들 때 15μJ이 소모된다. 우리는 임시 값과 ACK 메시지는 한 바이트, HELLO 메시지는 12바이트, 그리고 보고서는 36바이트의 크기로 간주한다. 훼손된 노드는 5 홉의 한 클러스터에서 발생하였고, 그 훼손된 노드는 그 클러스터에서 이웃 노드들에 허위 HELLO 메시지로 위협한다.

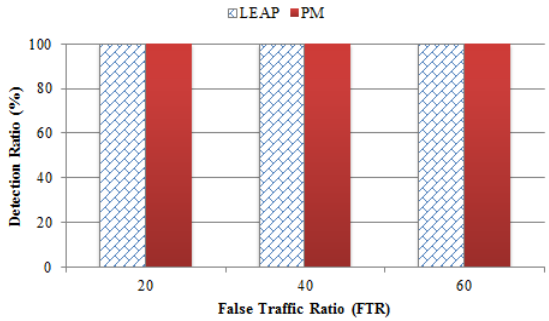


그림 6. 허위 트래픽 비율에 따른 감지 비율
Fig. 6. Detection Ratio versus False traffic ratio

그림 6은 허위 메시지 비율과 감지 비율의 측정을 보여준다. 허위 트래픽 비율(false traffic ratio)은 총 이벤트의 수 분의 허위 HELLO 메시지의 수이다. 훼손된 노드는 FTR 만큼 한 클러스터에서 노드에 허위 메시지를 전달한다. 우리는 각각 20%, 40%, 그리고 60%의 허위 트래픽을 점점 증가시킴으로 허위 트래픽의 수의 증가에도 불구하고, 두 기법은 훼손된 노드로부터 발생한 허위 HELLO 메시지는 같은 보안 레벨로 제거되었다.

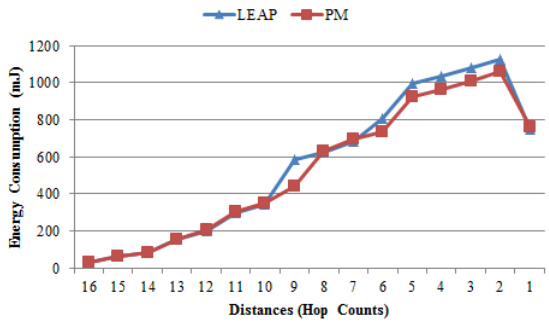


그림 7. 거리(홉) 마다 에너지 소모
Fig. 7. Energy consumption versus distances (Hop counts)

그림 7은 BS로부터 거리마다 센서 노드의 에너지 소모의 평균을 보여준다. 앞에서 언급했던 것처럼 훼손된 노드는 홉 5에 위치한다. 두 기법은 BS로부터 먼 홉에 위치한 노드들의 에너지 소모는 비슷하지만, BS로부터 가까운 홉에 있는 노드들은 노드의 밀집도 영향으로 에너지 소모에 차이가 있다. 제안 기법은 효율적인 노드 선택으로 에너지 효율성이 LEAP보다 크게 향상되었다. 그러므로 우리의 제안 기법은 LEAP과 비교하였을 때 노드 밀집도가 높은 지역에서 효율적인 다음 홉 노드 선택을 통해 에너지가 크게 절약되었다.

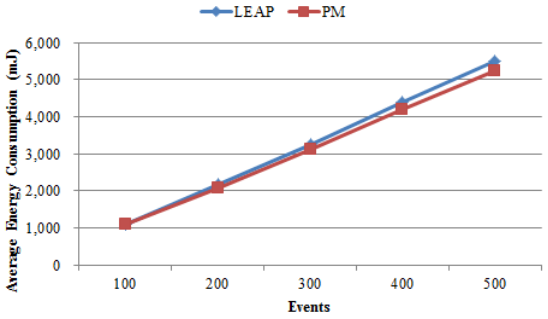


그림 8. 이벤트 마다 평균 에너지 소모
Fig. 8. Average energy consumption per events

그림 8은 이벤트를 발생시켰을 때 전체 네트워크의 평균 에너지 소모를 측정하였다. 두 기법은 이벤트가 드물게 발생했을 때는 에너지 소모의 큰 차이는 없지만, 이벤트가 500개 발생하였을 때 제안 기법은 LEAP보다 약 6%의 에너지가 향상되었다. 따라서 우리의 제안 기법은 LEAP과 비교하였을 때 에너지 효율성이 뛰어나고, 이는 전체 센서 네트워크의 수명이 연장될 수 있다.

5. 관련 연구

현재 연구되는 대부분의 무선 센서 네트워크 보안 기술은 키 분배 및 관리, 인증, 보안을 위한 네트워크 구조, 라우팅 등 다양한 보안 요소들이 결합되어 이루어진다[12]. 일반적으로 무선 통신의 기기에서는 안전한 통신을 위해 복잡한 키 관리가 필요 없는 공개키 방식을 사용한다. 그렇지만, 센서 네트워크에서는 센서들의 하드웨어 제약으로 키 관리와 보안 프로토콜을 위해 대칭키 방식이 제안되고 있다[13].

[14]에서 SPINS (security protocols for sensor networks)은 센서 네트워크 초기에 발표되어 SNEP (secure network encryption protocol)과 μTESLA (timed efficient stream loss-tolerant authentication)를 사용한다. 이 기법은 해시 체인(hash chain)을 이용하여 데이터 인증을 제공하고, 전달 과정 중에 한 패킷이 분실되더라도 다음 패킷을 통해 이전 패킷들을 검증할 수 있다. 하지만, 모든 노드의 시간 동기화가 요구되고, 전송 지연을 고려하여 키 노출 지연 시간의 설정 및 패킷의 저장을 위한 시간이 요구된다.

다음으로 [15]에서는 전송되는 데이터의 중요도에 따라 세 가지의 보안 레벨을 나누어 암호화 키를 사용하는 방법을 제안하였다. 보안 1은 노드의 암호화 키를 사용하여 데이터를 전송하고, 보안 2는 지역 키를 사용하여 네트워크의 보안 위협을 최소화시킨다. 마지막으로 보안 3은 마스터 키로부터 추출된 MD5를 사용하여 데이터를 암호화한다. 그

리고 보안 3이 가장 높은 레벨이다. 이 기법에서 역시 각 센서 노드가 완전한 시간 동기화가 필요하고 정확한 노드의 위치가 요구되는 단점이 있다.

LEAP은 베이스 스테이션과의 인증뿐만 아니라 단방향 키 체인을 기반으로 네 가지 형식의 키를 사용하고 노드 간 인증을 통해 데이터를 베이스 스테이션까지 전달한다. 이 기법은 네 가지 형식의 키를 통해 위의 문제들을 해결했고, in-network 프로세싱이 가능함과 동시에 이웃 노드가 보안 위협에 노출되더라도 보안을 유지할 수 있다.

6. 결론 및 향후 연구

본 논문에서, 우리는 다음 홉 노드 선택으로 LEAP과 비교하였을 때 에너지 효율성이 향상하는 방법을 제안하였다. 우리의 제안 기법은 다음과 같이 기여하였다.

- 에너지 절약
- 공격 지역 우회

제안 기법은 에너지 잔여 레벨, 이웃 노드와 공유하는 키의 수, 그리고 여과된 허위 메시지 수를 고려해서 한 평가 함수를 통해 효율적으로 다음 홉 노드를 선택한다. 실험 결과를 통해 보았듯이, 제안 기법에서는 LEAP과 비교하였을 때 보안 레벨은 유지하면서 최대 6%의 에너지 효율성을 향상했다. 앞으로 입력 요소를 기반으로 인공 지능 시스템을 적용하여 네트워크 상황에 따라 다음 홉 노드 선택 방법에 대하여 연구할 것이다.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *Communications Magazine, IEEE,* vol. 40, pp. 102-114, Aug. 2002.

[2] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks,* vol. 3, pp. 325-349, 2005.

[3] X. Du and H. -. Chen, "Security in wireless sensor networks," *Wireless Communications, IEEE,* vol. 15, pp. 60-66, Aug. 2008.

[4] S. Zhu, S. Setia and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," *Proc. of the 10th ACM Conf. on Computer and Communications Security, ACM,* pp. 62-72, 2003.

[5] S. Zhu, S. Setia and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans.Sen.Netw.,* vol. 2, pp. 500-528, nov, 2006.

[6] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *Selected Areas in Communications, IEEE Journal on,* vol. 23, pp. 839-850, 2005.

[7] S. H. Kim, Y. S. Kang, B. H. Chung, and K. I. Chung, "Technical Trend of Security in Ubiquitous Sensor Networks," *Electronics and Telecommunications Trends,* vol. 20, pp. 93-99, Feb. 2005.

[8] C. H. Lim, "LEAP++: A robust key establishment scheme for wireless sensor networks," *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on,* 2008, pp. 376-381.

[9] Crossbow Technology Inc., "MICAz: wireless measurement system," Available: http://bullseye.xbow.com, [Accessed: Nov. 10, 2013]

[10] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed Diffusion: A scalable and robust communication paradigm for sensor networks," *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking,* pp. 56-67, 2000.

[11] F. Ye, A. Chen, S. Lu and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in *Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on,* 2001, pp. 304-309.

[12] J. H. Nah, K. J. Chae and C. K. I., "Research Tread for Sensor Network Security," *Electronics and Telecommunications Trends,* vol. 20, pp. 112-122, Feb. 2005.

[13] Wenliang Du, Jing Deng, Y. S. Han, Shigang Chen and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *INFOCOM 2004. Twenty-Third AnnualJoint Conference of the IEEE Computer and Communications Societies,* 2004, pp. 597.

[14] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, "SPINS: security protocols for sensor networks," *Wirel.Netw.,* vol. 8, pp. 521-534, sep, 2002.

[15] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on,* 2002, pp. 139-144.

저 자 소 개

남수만(Su-Man Nam)

2009년 : 한서대학교 컴퓨터정보학과 이학사

2013년 : 성균관대학교 대학원전자전기컴퓨터학과 공학석사

2013년～현재 : 성균관대학교 대학원 전자전기컴퓨터학과 박사과정

관심분야 : 모델링 및 시뮬레이션, 무선 센서 네트워크, 인공 지능, 네트워크 보안

Phone : +82-31-290-7221

E-mail : smnam@ece.skku.ac.kr

조대호(Tae Ho Cho)
1983년: 성균관대학교 전자공학과 학사
1988년: Univ. of Alabama 전자공학과 석사
1993년: Univ. of Arizona 전자 및 컴퓨터공학과 박사

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 지능 시스템, 모델링 방법론
Phone : +82-31-290-7221
E-mail : taecho@ece.skku.ac.kr