Journal of Korean Institute of Intelligent Systems
Vol. 26, No. 4, August 2016, pp. 267-272
http://dx.doi.org/10.5391/JKIIS.2016.26.4.267

ISSN(Print) 1976-9172
ISSN(Online) 2288-2324

INSENS 기반의 무선 센서 네트워크에서 싱크홀 공격을 방어하기 위한 강화된 경로 설정 기법

Secure route determination method to prevent sinkhole attacks in INSENS based wireless sensor networks

송규현* · 조대호†**
Kyu-Hyun Song* and Tae-Ho Cho**†

성균관대학교 정보통신대학, *†**성균관대학교 소프트웨어대학**
*College of Information and Communication Engineering, Sungkyunkwan University
**† College of Software, Sungkyunkwan University

요 약

무선 센서 네트워크는 제약적인 하드웨어 자원과 무선 통신의 특징으로 인해 외부 침입에 취약하다. 따라서 공격자는 네트워크에 침입하여 싱크홀 공격을 시도할 수 있다. 이러한 싱크홀 공격을 방지하기 위해서 INSENS가 제안되었다. INSENS는 세 개의 대칭키를 사용하여 싱크홀 공격을 방지한다. 하지만 INSENS는 노드의 훼손을 고려하지 않기 때문에 훼손된 노드를 통해 싱크홀 공격이 다시 발생한다. 본 논문에서는 훼손된 노드를 통해 발생하는 싱크홀 공격을 이웃 노드들의 상태 정보를 사용하여 방지하는 기법을 제안한다. 제안 기법은 i) 공격을 안전하게 방지하여 네트워크의 신뢰성을 향상하고, ii) 에너지 소비 절감을 목표로 한다. 실험 결과 제안기법은 보고서의 신뢰성을 평균 71.50% 향상하고 에너지 소비를 평균 19.90% 절감한다.

키워드 : 무선 센서 네트워크, 네트워크 보안, 싱크홀 공격, 침입 강인, 보안 라우팅

Abstract

Wireless sensor networks (WSNs) are vulnerable to external intrusions due to the wireless communication characteristics and limited hardware resources. Thus, the attacker can cause sinkhole attack while intruding the network. INSENS is proposed for preventing the sinkhole attack. INSENS uses the three symmetric keys in order to prevent such sinkhole attacks. However, the sinkhole attack occurs again, even in the presence of INSENS, through the compromised node because INSENS does not consider the node being compromised. In this paper, we propose a method to counter the sinkhole attack by considering the compromised node, based on the neighboring nodes' information. The goals of the proposed method are i) network reliability improvement and ii) energy conservation through effective prevention of the sinkhole attack by detecting compromised nodes. The experimental results demonstrate that the proposed method can save up to, on average, 19.90% of energy while increasing up to, on average, 71.50%, the report reliability against internal sinkhole attacks in comparison to INSENS.

Key Words : Wireless Sensor Networks, Network security, Sinkhole attacks, Intrusion tolerance, Secure routing

Received: Jun. 14, 2016
Revised : Aug. 10, 2016
Accepted: Aug. 11, 2016
†Corresponding authors
taecho@skku.edu

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01059484)
This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484)

1. 서 론

무선 센서 네트워크(Wireless Sensor Networks; 이하 WSN)는 넓은 지역의 정보를 수집하는 목적으로 의학, 군사, 과학 등 다양한 분야에서 활용된다[1, 2]. 이러한 WSN은 감지한 이벤트를 전달하는 다수의 센서 노드들과 수집된 데이터를 정보화하여 사용자에게 제공하는 기지국(Base Station; 이하 BS)으로 구성된다[1, 3-6]. 하지만 낮은 하드웨어 자원과 무선 통신을 기반으로 하는 WSN은 공격자가 네트워크에 침입하여 싱크홀 공격을 발생할 수 있다[7, 8]. J. Deng 등은 싱크홀 공격을 방어하기 위해 침입 강인 무선 센서 네트워크 라우팅 프로토콜(INtrusion-tolerant routing for wireless SEnsor NetworkS; 이하 INSENS)을 제안하였다. INSENS는 외부 노드가 네트워크에 침입하는 것을 세 가지의 대칭키를 사용하여 차단한다[8]. 하지만 개방된 환경에 배치되어 운영 중인 센서 노드는 물리적으로 보안에 취약하므로 공격자에 의해 쉽게 훼손되고 보안 정보가 노출된다. 공격자는 훼손된 노드와 보안 정보를 사용하여 WSN에 다시 싱크홀 공격을 발생할 수 있다[7, 9]. 이러한

싱크홀 공격에 대응하기 위해서는 기존과 다른 새로운 방식의 대응 기법이 필요하다. 본 논문에서는 훼손 노드를 사용한 싱크홀 공격을 방지하기 위해서 이웃 노드들의 경로 요청(Route request; 이하 REQ) 메시지와 경로 설정 상태를 확인하여 싱크홀 공격을 탐지하고 방지하는 기법을 제안한다. 제안 기법은 위조된 REQ 메시지를 이웃 노드의 상태 정보를 통해 탐지하고 제거하여 싱크홀 공격을 방지함으로써 불필요한 에너지 소비를 줄이고 네트워크의 신뢰성을 향상하는 것을 목표로 한다.

본 논문의 2장에서는 싱크홀 공격, INSENS, 훼손 노드를 사용한 싱크홀 공격에 관해 서술하고, 연구의 필요성에 대해 제시한다. 3장에서는 제안 기법에 관해 상세히 기술한다. 4장에서는 INSENS와 제안 기법을 비교한 실험결과를 보여주고 5장에서 결론 및 향후 연구에 관해 서술한다.

2. 관련 연구

본 장에서는 싱크홀 공격과 INSENS에 대해 설명하고 훼손 노드를 통한 싱크홀 공격과 연구의 필요성에 대해 제시한다.

2.1 외부 싱크홀 공격

WSN은 낮은 하드웨어 자원과 외부에서 접근하기 쉬운 무선 통신을 사용하기 때문에 공격자의 노드가 네트워크에 쉽게 침입할 수 있다. 이렇게 침입한 공격자의 노드를 외부 노드라 칭한다. 공격자는 싱크홀 공격을 발생하기 위해 외부 노드를 최적의 경로 또는 BS로 속이는 위조된 REQ 메시지를 방송한다. 싱크홀 공격은 WSN의 이벤트 보고서를 공격자가 가로채기위해 라우팅 경로를 변경하는 공격이다. 이러한 공격을 외부 싱크홀 공격이라 한다[10]. 외부 싱크홀 공격으로 인해 라우팅 경로가 변경된 노드들은 이벤트 보고서를 외부 노드로 전달하게 된다[7].

외부 싱크홀 공격에 대응하기 위해서 INSENS와 LEAP이 제안되었다[8, 10]. LEAP는 Individual key와 Pairwise key, Cluster key, Group key를 사용하여 외부 노드를 차단한다[11]. 하지만 많은 키를 사용하는 LEAP은 노드에 저장할 수 있는 키의 한계로 인해 대규모 네트워크를 구성하기 어렵고, 새로운 노드의 참여와 차단이 어렵다. 본 논문에서는 이러한 문제점이 해결된 강화된(Enhanced) INSENS를 기반으로 한다[8].

2.2 INSENS

싱크홀 공격을 방지하기 위해 J. Deng 등은 강화된 INSENS를 제안하였다. 강화된 INSENS는 기본(Basic) INSENS와는 다른 특징을 갖는다. 1) 기본 INSENS에서 사용하던 BS와 각 노드 사이에 공유된 pairwise key를 사용하지 않고, 단일키인 글로벌 키(global key; 이하 GK)를 사용하여 이웃 노드를 인증한다. 2) 경로가 중간에 단절되는 것을 해결하기 위해 여러 개의 BS와 다중 경로를 설정한다. 3) 각 노드는 라우팅 테이블(Routing table)을 저장하지 않고, REQ 메시지의 송·수신과 단방향 해시 체인(one-way hash chain 이하; OHC)만으로 부모 노드를 결정하고 다중 스페닝 트리의 경로를 구성한다. OHC는 메시지의 재사용을 방지하기 위해 사용된다[8].

2.2.1 INSENS의 동작과정

강화된 INSENS(Enhanced INSENS ; 이하 INSENS)의 동작 과정은 이웃 노드 인증, 키 교환, 경로 요청 및 설정으로 이루어진다. 이웃 노드 인증 과정은 사전에 주입된 GK를 사용하여 통신 범위 안에 있는 이웃 노드들과 각각의 페어와이즈 키(Pairwise key; 이하 PK)를 생성한다. 키 교환 과정은 각 노드가 클러스터 키(Cluster key; 이하 CK)를 생성하고 각각의 이웃 노드에게 PK를 사용하여 자신의 CK를 알려준다. 경로 요청 및 설정 단계는 Fig. 1과 같다. BS는 경로 설정을 위해 자신의 OHC와 ID를 CK로 암호화하여 REQ 메시지를 생성하고 방송한다(Fig. 1(a)). 메시지를 수신한 노드들은 BS의 CK를 사용하여 메시지를 복호화하고 OHC 함수를 사용하여 얻은 새로운 OHC로 메시지를 검증한다. 메시지의 OHC가 유효하면 노드는 BS를 부모 노드로 설정하고 새로운 OHC를 REQ 메시지에 삽입하여 방송한다(Fig. 1(b)). 위와 같은 과정을 반복하여 경로를 설정한다(Fig. 1(c))[8].

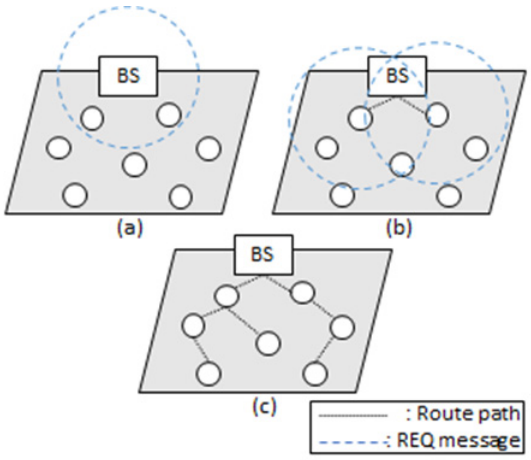

그림 1. INSENS의 라우팅 경로 설정 과정
Fig. 1. Routing path setup process of INSENS

2.2.2 내부 싱크홀 공격 시나리오

센서 노드는 개방된 환경에 배치되기 때문에 물리적으로 보안에 취약하다. 공격자는 이러한 취약점을 이용하여 구성 노드의 일부를 탈취하고 보안 정보와 제어권한을 획득한다. 이렇게 보안 정보가 공격자에게 노출된 노드를 훼손 노드(compromised node)라 한다

[10]. 공격자는 훼손 노드를 사용하여 내부 싱크홀 공격을 시도한다. INSENS에서 싱크홀 공격을 발생하기 위해서는 다음과 같은 제약사항이 따른다.

각 노드는 이웃 노드들의 정보만 가지고 있다. 따라서 BS 사칭 공격을 발생하기 위해서는 BS의 이웃 노드를 훼손하여 BS의 보안 정보를 획득하여야 한다.

BS에서 75m 이내[12]의 이웃 노드를 훼손하는 것은 관리자에 의해 쉽게 차단될 수 있다.

관리자를 피해 BS의 이웃 노드를 훼손하고 위조된 REQ 메시지를 방송하여도 이웃 노드인 BS가 그 메시지를 수신하기 때문에 공격이 차단된다.

따라서 공격자는 INSENS 기반의 WSN에 싱크홀 공격을 발생하기 위해서 라우팅 테이블을 갖지 않는 특징을 이용한다. 공격자는 획득한 보안 정보인 OHC와 CK를 사용하여 정상적인 REQ 메시지와 동일하게 메시지를 위조한다. 정상적인 REQ 메시지 (1)와 위조된 REQ 메시지(2)의 구조는 다음과 같이 같다.

$$REQ \| ID_x \| E_{CK_x}(OHC \| ID_{BS}) \quad (1)$$

$$REQ \| ID_x \| E_{CK_x}(OHC \| ID_{BS}) \quad (2)$$

REQ는 메시지 타입이고, ID_x는 REQ 메시지의 송신 노드인 x의 ID이다. CK_x는 노드 x의 CK이며, ID_{BS}는 최초 경로를 요청한 BS의 ID이다. 공격자는 BS의 ID를 사용하여 REQ 메시지를 직접 생성하고 BS가 방송한 메시지인 것처럼 위조한다. 이렇게 위조한 REQ 메시지를 공격자가 방송함으로써 노드들은 라우팅 경로를 공격자 중심으로 변경한다. 공격 과정은 Fig. 2와 같다.

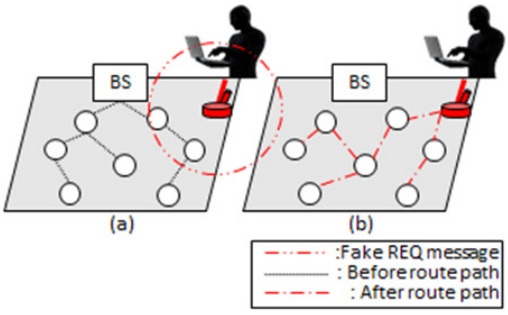

그림 2. 훼손 노드를 이용한 내부 싱크홀 공격
Fig. 2. Internal sinkhole attack using the compromised node

INSENS의 노드들은 라우팅 테이블을 저장하지 않기 때문에 BS의 위치를 모른다. 따라서 위조된 REQ 메시지의 OHC 정보만을 확인하고 메시지를 정상으로 판단하여 라우팅 경로를 공격자 중심으로 변경하게 된다.

2.3 동기

내부 싱크홀 공격을 방어하기 위해 선행 연구자들은 [13-15]과 같은 많은 연구를 진행하였다. 기존 연구들은 지역별 도달한 보고서의 개수를 기반으로 공격을 탐지하거나, 라우팅 테이블을 기반으로 공격을 탐지한다. 하지만 보고서 기반의 탐지 기법은 공격 형태에 따라 일부 보고서가 전달될 수 있어 공격 탐지의 어려움이 있고, 라우팅 테이블 기반의 탐지 기법은 라우팅 테이블을 저장하지 않는 INSENS에는 적합하지 않다. 따라서 이에 적합한 보안 기법의 연구가 필요하다.

3. 제안 기법

본 장에서는 제안 기법에서 가정한 사항들과 공격 모델, 제안 기법의 동작 과정에 관해 설명한다. 가정 사항은 다음과 같다. WSN는 MICA2 mote[12]를 사용하고, 모든 노드는 다수의 이웃 노드를 가지고 있으며, 양방향 통신을 사용한다. 최초 경로 설정 과정에는 훼손 노드가 없다고 가정한다.

3.1 공격 모델

공격 모델에는 외부 싱크홀 공격과 내부 싱크홀 공격이 있다. 외부 싱크홀 공격은 임의의 위치에서 보안 정보 없이 REQ 메시지를 방송한다. 내부 싱크홀 공격은 기존에 배치된 노드 중 임의로 하나를 훼손하여 보안 정보를 사용한 REQ 메시지를 방송한다[16].

3.2 동작 과정

제안 기법은 에너지 소비를 최소화하기 위해 REQ 메시지가 확산(flooding)되는 것을 이용한다. 메시지의 확산은 한 노드가 이웃 노드들이 방송하는 REQ 메시지로 인해 여러 번 메시지를 수신하게 되는 것을 의미한다. 제안 기법의 동작 과정은 송신 노드 확인 단계, 대기 단계, 이웃 노드 정보 확인 단계로 동작한다. 1) 송신 노드 확인 단계에서는 송신 노드가 BS이면 이웃 노드 정보 확인단계를 수행한다. 송신 노드가 BS가 아닐 경우에는 대기 단계를 수행한다. 2) 대기 단계에서는 일정 시간 다른 REQ 메시지의 수신을 기다리고 메시지가 수신되면 경로를 설정한다. 메시지가 수신되지 않으면 수신된 REQ 메시지를 공격으로 의심하고 이웃 노드 정보 확인 단계를 수행한다. 3) 이웃 노드 정보 확인 단계는 상황에 따라 다르게 동작한다.

송신 노드가 BS이면 수신 노드는 OHC 확인 요청(OHC Check Request 이하; OHC_CR) 메시지를 방송하고 BS와의 PK를 통해 응답 메시지를 확인한다.

송신 노드가 BS가 아니고 일정 시간 다른 REQ 메시지가 수신되지

않은 경우에는 송신 노드의 부모 노드가 OHC_CR 메시지를 방송하여 응답 메시지를 확인한다.

OHC_CR 메시지(3)과 응답 메시지(4)의 구조는 다음과 같다.

$$OHC\_CR \| ID_x \| E_{CK_x}(OHC+1, nonce) \quad (3)$$

$$ACK \| ID_y \| E_{K_{x,y}}(nonce) \quad (4)$$

ID_x는 노드 x의 ID이다. CK_x는 노드 x의 CK이고, CK로 암호화된 메시지는 이웃 노드만 확인할 수 있다. $OHC+1$은 OHC를 1증가시킨 값이다. ID_y는 노드 y의 ID이고 $K_{x,y}$는 기존에 공유된 노드 x와 노드 y의 PK이다. PK를 통해 두 노드 간 비밀 통신을 할 수 있다. $nonce$는 난수 값으로 메시지의 재사용을 방지하기 위해 사용된다. Fig. 3은 정상적인 경로 요청이 발생했을 때 제안 기법의 동작 과정이다. BS에서 경로 요청을 발생하면, 이웃 노드들은 이웃 노드 정보 확인단계를 수행하여 BS를 인증하고 경로를 설정한다.

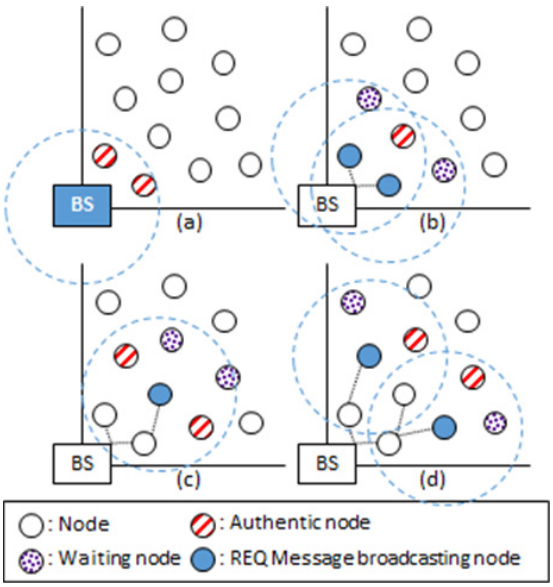

그림 3. 제안 기법의 정상적인 경로 설정
Fig. 3. Normal routing setup of proposed method

Fig. 4는 제안 기법이 싱크홀 공격을 방지하는 과정이다. Fig. 4(a)와 같이 공격자는 훼손 노드를 통해 위조된 REQ 메시지를 방송하여 싱크홀 공격을 시도한다. REQ 메시지를 수신한 이웃 노드들은 일정 시간 동안 대기 단계를 수행한다. 이후 다른 REQ 메시지가 수신되지 않기 때문에 Fig. 4(b)와 같이 기존 경로의 부모 노드가 OHC_CR 메시지를 방송하여 이웃 노드의 상태 정보를 요청한다. OHC_CR 메시지를 수신한 노드들은 메시지의 OHC+1과 자신의 OHC가 같지 않기 때문에 ACK 메시지를 방송하지 않는다. 응답 메시지를 수신하지 못한 기존 경로의 부모 노드는 Fig. 4(c)와 같이 경보를 발생하고, 라우팅 경로에서 훼손 노드를 제거한다. 본 논문의 제안 기법을 통해 내부 싱크홀 공격을 방지함으로써 WSN의 신뢰성 향상과 공격으로 인해 소비되는 불필요한 에너지 소비 절감을 목표로 한다.

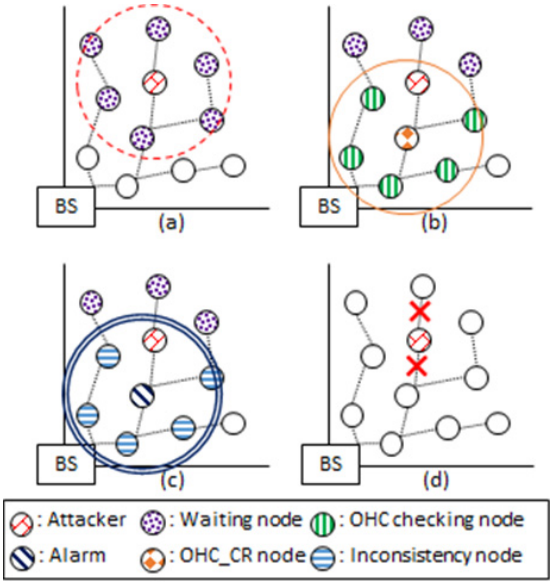

그림 4. 제안 기법의 싱크홀 공격을 방지 과정
Fig. 4. sinkhole attack preventing process of proposed method

4. 시뮬레이션 및 결과

본 연구는 C++을 사용하여 WSN의 시뮬레이션 환경을 구현하였다. 구현 환경은 INSENS를 적용한 WSN의 환경과 제안 기법을 적용한 센서 네트워크 환경이 있다. 싱크홀 공격 모델에는 외부 싱크홀 공격과 내부 싱크홀 공격이 있다. 실험환경은 필드 크기는 1000 m^2이며, BS의 개수는 2개이다. 노드의 개수는 1,500개이다. 메시지 송신과 수신에 소비되는 에너지는 1Byte당 16.25와 12.5μJ이며, 메시지의 암·복호화에 사용되는 에너지는 9μJ이다[17]. 대기 시간은 경로 요청 수신 후 0.00046초이다[12]. Fig. 5는 INSENS와 제안 기법에서 정상적인 경로 요청과 싱크홀 공격 발생 시 소비되는 에너지양에 대한 비교이다. 제안 기법은 외부 싱크홀 공격과 내부 싱크홀 공격 모두 방지하여 에너지의 소비가 적다. 하지만 INSENS는 내부 싱크홀 공격 때문에 노드들이 경로를 변경하게 되면서 에너지의 소비가 증가하게 된다. 이후 내부 싱크홀 공격이 발생한 INSENS의 노드들은 OHC가 증가되어 정상적인 경로 요청에 경로를 설정하지 않아 에너지가 감소하는 것처럼 보인다. Fig. 6은 공격 발생 빈도(False Request Ratio; 이하 FRR)에 따른 에너지 소비량이다. 제안 기법은 FRR이 증가할수록 모든 공격을 방지하여 에너지 소비가 지속해서 감소하는 반면, INSENS는 공격 발생 후 정상적인 경로를 설정하지 않아 에너지가 감소하는 것처럼 보인다.

따라서 FRR이 증가할수록 연속적인 내부 싱크홀 공격이 증가하고 정상적인 경로 요청이 줄기 때문에 60% 이상부터 에너지 소비량이 다시 증가한다. Fig. 7은 공격 발생 빈도에 따른 BS에 도달한 보고서의 개수를 보여준다. INSENS는 공격으로 인해 경로가 변경되면서 BS에 도달하는 보고서의 개수가 점차 감소하다가 60%부터 BS에 보고서가 도달하지 않는다. 하지만 제안기법은 내부 싱크홀 공격을 방지하여 보고서가 BS까지 안전하게 도달한다. 제안 기법은 FRR이 증가할수록 모든 공격을 방지하여 에너지 소비가 지속해서 감소하는 반면, INSENS는 공격 발생 후 정상적인 경로를 설정하지 않아 에너지가 감소하는 것처럼 보인다. 따라서 FRR이 증가할수록 연속적인 내부 싱크홀 공격이 증가하고 정상적인 경로 요청이 줄기 때문에 60% 이상부터 에너지 소비량이 다시 증가한다.Fig. 7은 공격 발생 빈도에 따른 BS에 도달한 보고서의 개수를 보여준다. INSENS는 공격으로 인해 경로가 변경되면서 BS에 도달하는 보고서의 개수가 점차 감소하다가 60%부터 BS에 보고서가 도달하지 않는다. 하지만 제안기법은 내부 싱크홀 공격을 방지하여 보고서가 BS까지 안전하게 도달한다. 실험결과 제안 기법을 통해 싱크홀 공격을 안전하게 방지하여 메시지의 도달률이 전체 평균 71.50% 향상되고, 에너지 소비는 19.90% 절감한다.

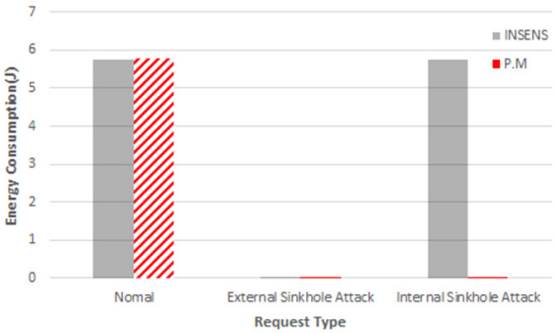

그림 5. INSENS와 제안 기법의 에너지 소비량 비교
Fig. 5. Energy consumption comparison of proposed method (P.M) and INSENS

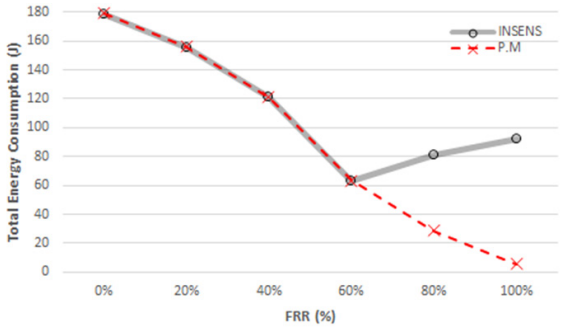

그림 6. FRR에 따른 총 에너지 소비량
Fig. 6. Total energy consumption according to FRR

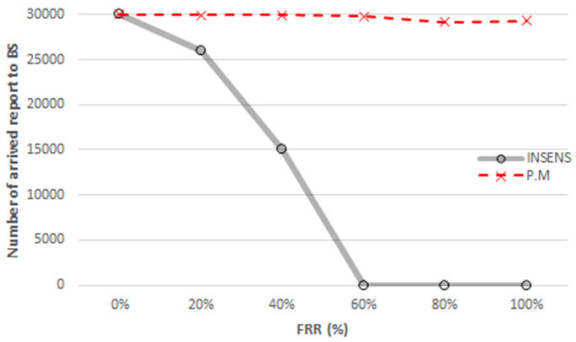

그림 7. FRR에 따른 보고서 도달 갯수
Fig. 7. Number of arrived report according to FRR

5. 결론 및 향후 연구

본 논문에서는 내부 싱크홀 공격을 방지하기 위해 강화된 경로 설정 기법을 제안하였다. 제안 기법은 노드의 밀집도가 높은 WSN 환경에서 REQ 메시지가 확산되는 것을 이용한다. 정상적인 경로 요청일 때, 각 노드는 여러 이웃 노드에서 방송되는 REQ 메시지는 여러 번 수신하기 때문에 이를 이용하여 불필요한 검증을 최소화하고 공격 의심 상황에서는 이웃 노드들의 상태 정보를 사용하여 REQ 메시지를 검증한다. 제안 기법은 이웃 노드들의 상태 정보를 사용하여 위조된 REQ 메시지를 검증하기 때문에 키를 통한 암호화 기법이 가지던 키 노출에 대한 보안적 한계를 해결한다. 따라서 제안 기법을 통해 보안 정보가 노출 된 상황에서도 내부 싱크홀 공격을 안전하게 방지하여 WSN의 신뢰도를 향상하고, 불필요한 에너지 소비를 절감한다. 하지만 제안 기법은 밀집도가 낮은 WSN의 환경에서 이웃 노드를 2개 이하로 갖는 특정 노드에서는 공격을 탐지하기가 어렵다. 따라서 향후 연구로는 노드의 밀집도의 영향을 받지 않고 싱크홀 공격을 방지하는 연구를 진행할 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, 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] Jong-Kyun Jeong and In-Ho Ra. Asynchronous and adaptive massage passing scheme for wireless sensor networks. *Journal of Korean Institute of Intelligent Systems* 23(3), pp. 196-201.

2013.

[4] Hyun-Tae Kim and In-Ho Ra. A fault-tolerant QoS routing scheme based on interference awareness for wireless sensor networks. *Journal of Korean Institute of Intelligent Systems* 22(2), pp. 148-153. 2012.

[5] Hyuk Park and Tae Ho Cho. Partial path selection method in each subregion for routing path optimization in SEF based sensor networks. *Journal of Korean Institute of Intelligent Systems* 22(1), pp. 108-113. 2012.

[6] Tae Hyoung Kim, Geuntaek Kang and Won Chang Lee. Clustering algorithm for efficient use of energy in wireless sensor network. *Journal of Korean Institute of Intelligent Systems* 20(1), pp. 36-41. 2010.

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

[8] J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Comput. Commun.*, vol. 29, pp. 216-230, 2006.

[9] E. Shi and A. Perrig, "Designing secure sensor networks," *Wireless Communications, IEEE*, vol. 11, pp. 38-43, 2004.

[10] S. Zhu, S. Setia and S. Jajodia, "LEAP : Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, pp. 500-528, 2006.

[11] Su-Man Nam and Tae-Ho Cho. Dynamic states consideration for next hop nodes selection method to improve energy efficiency in LEAP based wireless sensor networks. *Journal of Korean Institute of Intelligent Systems* 23(6), pp. 558-564. 2013.

[12] (Accessed: Jan. 11, 2016). MICAz: wireless measurement system. Available: http://trl.iba.edu.pk/Memsic-set-2.pdf.

[13] E. C. Ngai, J. Liu and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Comput. Commun.*, vol. 30, pp. 2353-2364, 2007.

[14] N. Gandhewar and R. Patel, "Detection and prevention of sinkhole attack on AODV protocol in mobile adhoc network," *in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on*, 2012, pp. 714-718.

[15] I. Krontiris, T. Giannetsos and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in Networking and Communications, 2008. WIMOB'08. *IEEE International Conference on Wireless and Mobile Computing*, 2008, pp. 526-531.

[16] Kyu-Hyun Song and Tae-Ho Cho. Improvement robust bidirectional verification scheme for detecting routing attacks in enhanced INSENS based seneor netowrks. 2015, .

[17] 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.

저 자 소 개

송규현(Kyu-Hyun Song)

2014년 : 백석대학교 정보통신공학부 공학사
2014년~현재 : 성균관대학교 대학원 전자전기컴퓨터공학과 석사과정

관심분야 : 네트워크 보안, 무선 센서 네트워크, 인공지능, 모델링 시뮬레이션, 보안 시뮬레이션
Phone : +82-31-290-7221
E-mail : songku3000@skku.edu

조대호(Tae Ho Cho)

1983년 : 성균관대학교 전자공학과 공학사
1988년 : Univ. of Alabama 전자공학과 공학석사
1993년 : Univ. of Arizona 전자 및 컴퓨터공학과 공학박사
1995년~현재 : 성균관대학교 정보통신공학부 교수

관심분야 : 무선센서 네트워크, 모델링 시뮬레이션, 지능시스템, 모델링 방법론, 네트워크 보안 시뮬레이션, 전자적 자원관리
Phone : +82-31-290-7221
E-mail : taecho@skku.edu