Journal of Korean Institute of Intelligent Systems
Vol. 26, No. 2, April 2016, pp. 113-119
http://dx.doi.org/10.5391/JKIIS.2016.26.2.113

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

JKIIS

무선 센서 네트워크에서 에너지 효율성 향상을 위해 공격정보를 활용한 동적 여과 기법의 키 재분배 기법

Key Re-distribution Scheme of Dynamic Filtering Utilizing Attack Information for Improving Energy Efficiency in WSNs

박동진* · 조대호†**
Dong-Jin Park* and Tae-Ho Cho**†

***성균관대학교 소프트웨어플랫폼학과, **† 성균관대학교 전자전기컴퓨터학과**
*College of Software, Sungkyunkwan University
**† College of Information and Communication Engineering, Sungkyunkwan University

요 약

무선 센서 네트워크는 제한된 자원과 무선 통신 사용으로 공격자에게 취약하기 때문에 공격자는 쉽게 노드를 훼손할 수 있고 허위 보고서 주입 공격과 같은 다양한 공격을 시도한다. 허위 보고서 주입 공격은 허위 보고서를 전달하는 과정에서 발생하는 에너지 고갈과 기지 노드에 허위 알람을 일으켜 금전적 손실을 발생시킨다. 이 문제를 다루기 위한 기존 기법 중 하나인 동적 여과 기법은 허위 보고서를 탐지함으로써 에너지를 절약할 수 있다. 동적 여과 기법의 키 분배 단계는 공격이 발생한 소스 노드 근처의 노드가 허위 보고서를 탐지할 수 있는 키를 갖지 못할 수 있다. 따라서 지속적인 공격에 노출될 경우 불필요한 에너지 손실이 발생한다. 본 논문에서는 이러한 문제를 개선하기 위해 키 재분배 기법을 제안한다. 제안 기법은 초기에 분배된 비밀 키를 사용하여 빠른 허위 보고서 탐지를 통해 에너지를 절약한다. 실험 결과는 기존 기법과 비교하였을 때 최대 26.63% 에너지 절약과 최대 15.92%의 탐지 성능 향상을 보인다.

키워드 : 무선 센서 네트워크, 허위 보고서 주입 공격, 동적 여과 기법, 키 재분배

Abstract

Wireless sensor networks are vulnerable to an adversary due to scarce resources and wireless communication. An adversary can compromise a sensor node and launch a variety of attacks such as false report injection attacks. This attack may cause monetary damage resulting in energy drain by forwarding the false reports and false alarms at the base station. In order to address this problem, a number of en-route filtering schemes has been proposed. Notably, a dynamic en-route filtering scheme can save energy by filtering of the false report. In the key dissemination phase of the existing scheme, the nodes closer to the source node may not have matching keys to detect the false report. Therefore, continuous attacks may result in unnecessary energy wastage. In this paper, we propose a key re-distribution scheme to solve this issue. The proposed scheme early detects the false report injection attacks using initially assigned secret keys in the phase of the key pre-distribution. The experimental results demonstrate the validity of our scheme with energy efficiency of up to 26.63% and filtering capacity up to 15.92% as compared to the existing scheme.

Key Words : Wireless Sensor Network, False Report Injection Attack, Dynamic En-route Filtering Scheme, Key Re-distribution

Received: Jan. 15, 2016
Revised : Apr. 20, 2016
Accepted: Apr. 20, 2016
†Corresponding authors
thcho@skku.edu

1. 서 론

무선 센서 네트워크(wireless sensor network; 이하 WSN)는 필드에 분배된 노드를 통해 주변 이벤트를 감지하여 실시간 관리를 통한 모니터링 시스템 등 사람의 접근이 힘든 넓은 지역에 이용되고 있다[1-3]. WSN은 다수의 소형 센서 노드와 센서 노드로부터 감지된 이벤트 데이터가 모이는 기지 노드(base station; 이하 BS)로 구성된다[4]. 대규모 WSN에서는 수천 개의 센서 노드를 배치하고 이를 클러스터 단위로 나누어 클러스터 헤드 노드(cluster head; 이하 CH)를 선정 혹은 배치하여 구성할 수 있다[5]. 이러한 CH는 자신의 클러스터에 속한 멤버노드로부터 이벤트 데이터를 받아 보고서 형태로 다음 노드에 전달한다.

많은 수의 센서 노드는 개방된 환경에 배치된 저가형 제품으로, 연산 능력이나 메모리 그리고 에너지 등의 자원이 한정되어 있어 쉽게 노드가 훼손될 수 있고 허위 보고서 주입 공격이나 서비스 거부 공격, 그리고 선택적 전달 공격 등 각종 보안 공격에 쉽게 노출될 위험이 있다. 그러므로 노드의

이 논문은 2015년도 정부(미래창조부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2013R1A2A2A01013971).

제한된 자원을 고려한 보안 기법의 연구가 이루어지고 있다.

WSN에서 공격자는 임의의 이벤트 데이터를 주입하여 BS의 허위 알람을 일으키고 데이터를 보고서 형태로 전달하는 과정에서 제한된 에너지를 갖는 WSN의 수명을 단축시키는 허위 보고서 주입 공격(false report injection attack)을 가할 수 있다. 따라서 공격으로 발생한 허위 보고서를 가능한 조기에 검출하는 것이 매우 중요하다. 허위 보고서 주입 공격을 탐지하기 위한 기법으로 키 사전 분배 단계, 키 배포 단계 그리고 보고서 전달 단계의 3단계로 동작하는 동적 여과 기법(dynamic en-route filtering scheme; 이하 DEF)이 Yu와 Guan에 의해 제안되었다[6]. DEF는 인증 키와 비밀 키를 사용하여 전달 과정에서 허위 보고서를 감지할 수 있는 기법이다. 하지만 DEF는 공격에 지속적으로 노출 시, 보안을 위해 많은 에너지를 소비하는 키 배포 단계를 거치더라도 공격 상황을 고려한 배포 방식이 아니기 때문에 공격이 탐지되기 전까지 지속적인 불필요한 에너지 소모가 있을 수 있다.

본 논문에서는 공격 상황을 고려하여 공격 발생 클러스터 바로 다음 홉에서 검증될 수 있도록 하는 방법을 제안한다. 제안 기법은 전달 노드에서 공격을 탐지하여 폐기 시킨 허위 보고서를 카운트하고 특정 임계값 이상이 되었을 때, 키 재분배 요청 메시지를 BS에게 전달한다. BS는 허위 보고서가 보다 조기에 탐지될 수 있도록 적절한 키 재분배를 시행하여 노드의 불필요한 에너지 소비를 절약한다[7]. 실험 결과는 기존 기법에 비교하였을 때 최대 26.63%의 에너지를 절약하였고 최대 15.92%의 허위 보고서 탐지 성능이 향상 되었다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구에 대해 살펴보고, 3장에서 제안 기법을 소개하며 4장에서 제안 기법의 성능 평가를 보이고, 끝으로 5장에서는 결론을 맺는다.

2. 관련 연구

본 장에서는 허위 보고서 주입 공격에 대해 2.1에서 설명하고 2.2에서 허위 보고서 주입 공격을 막는 다른 기존 기법들을 소개한다. 마지막으로 2.3에서 DEF를 소개한다.

2.1 허위 보고서 주입 공격

허위 보고서 주입 공격은 BS의 기만이나 네트워크의 제한된 에너지의 고갈을 목적으로 허위 보고서들을 네트워크에 주입하는 공격이다[8]. 그림 1은 무선 센서 네트워크에서 훼손된 노드(compromised node)를 통해 공격자가 허위 보고서 주입 공격 시의 모습을 간략하게 보여준다. 공격자는 필드 상에 분배된 몇몇 노드를 탈취하여 제어권을 획득하고 이렇게 탈취한 훼손된 노드를 이용해 네트워크에 실제 존재하지 않는 이벤트 정보를 담은 허위 보고서를 생성하고 네트워크 내에 주입한다. 이렇게 생성된 허위 보고서는 정상 라우팅 경로를 따라 중간에서 탐지되지 못한 채 BS까지 전달되고 허위 보고서를 받은 BS는 허위 보고서의 내용을 확인하고 잘못된 알람을 발생시킨다. 이는 보고서 내용에 대응하는 적절한 조치 동작에 혼란을 일으키게 되고, 금전적과 시간적 손실을 준다. 또한 전달 경로 상의 정상 노드들은 훼손된 노드를 통해 만들어진 공격자의 악의적인 허위 보고서를 전달하기 위해 에너지를 소비하는 불필요 에너지 손실이 발생하고 계속된 공격으로 결국 전체 네트워크 수명이 감소하게 되는 결과를 초래한다. WSN에서 노드 간 메시지 인증 기능을 제공하는 보안 프로토콜을 적용할 경우 훼손된 노드는 자신이 탈취한 키와 전송 범위 안의 다른 훼손 노드가 가진 키를 이용해 인증 정보를 생성하여 메시지 인증 기능을 무력화시킨다. 허위 보고서 주입 공격 외에 특정 지역을 파괴하는 싱크홀 공격과, 정상 보고서를 선택적으로 보내는 선택적 전달 공격이 있는데, 싱크홀 공격의 피해 범위는 지역적이고, 선택적 전달 공격의 피해 범위는 한 경로 상에 일부의 노드들이다. 하지만 허위 보고서 주입 공격의 피해 범위는 한 경로상의 모든 노드들과 BS까지 영향을 미치는 점에서 에너지의 제한을 가진 WSN에 심각성을 나타낸다.

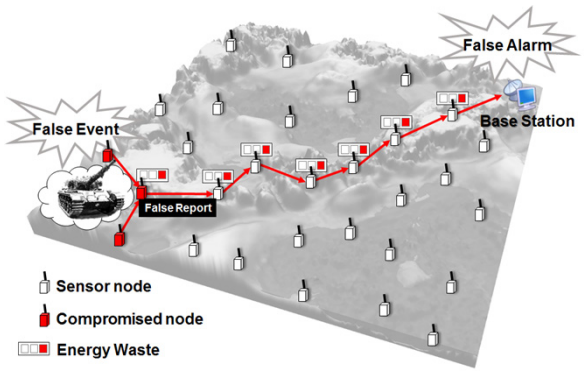

그림 1. 무선 센서 네트워크에서 허위 보고서 주입 공격
Fig. 1. False report injection attack in WSN

2.2 기존 기법들

En-route에서 허위 보고서 주입 공격을 방어하기 위해 VEBEK[9] 기법과 BECAN[10] 기법이 제안되었다. VEBEK는 VEBEK-I 과 VEBEK-II 모드로 구성되어 키 갱신의 오버헤드를 최소화하여 에너지를 절약하는 가상 에너지 기반 기법이다. 하지만 이 기법은 데이터 전달 경로가 고정되어 있다는 특징이 있다. DEF는 전달 경로가 고정되어 있지 않아 동적 상황에 더 적합하며 데이터 유실이 발생했을 때 다른 이웃 노드로 재전송할 수 있다. BECAN은 bit-compressed 인증기술과 CNR 기반 탐지 메커니즘을 통해 대역폭을 개선하고 높은 탐지 성능과 신뢰성을 가진 기법이다. 하지만 이 기법은 훼손된 노드로부터 발생할 수 있는 다른 공격에 대해서는

방어할 수 없다는 특징을 가진다. DEF는 허위 보고서 주입 공격뿐만 아니라 선택적 전달 공격, 보고서 중단 공격을 방어할 수 있다.

2.3 동적 여과 기법(DEF)

DEF는 클러스터 기반으로 구성된 WSN에서 허위 보고서 주입 공격을 방어하기 위한 기법이다. 이 기법은 노드에 인증 키와 비밀 키를 적재시켜 필드에 분배하고 라우팅 경로를 따라 각 클러스터의 모든 멤버 노드의 인증 키를 CH가 취합하여 메시지를 전달한다. 전달받은 전달 노드는 해당 메시지로부터 인증 키들을 추가로 메모리에 적재한 후 이벤트 보고서의 허위 유무를 확인하는 데 사용한다. DEF는 그림 2와 같이 3단계 동작 과정을 가진다.

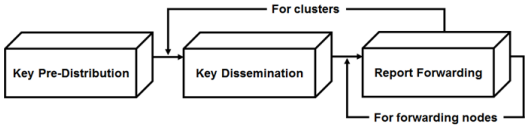

그림 2. 동적 여과 기법의 3단계 동작 과정
Fig. 2. Three-step operation phases of DEF

키 사전 분배 단계는 센서 노드가 처음 배포될 때 한 번만 실행되며 필드에 배포 전 BS에서 이루어진다. 각 노드는 서로 다른 시드 키(seed key)를 적재하고 시드 키로부터 공통의 해쉬 함수(hash function)를 사용해 인증 키를 생성, 해쉬 체인(hash chain)으로 구성한다. 이때 노드의 메모리가 충분하다면 생성된 인증 키를 모두 가지고 있고 그렇지 않으면 시드 키를 가지고 인증 키는 필요할 때마다 생성한다. 또한, $l+1$개의 비밀 키를 가지는데 이는 l개의 키($y-key$)와 클러스터 내의 다른 노드와 구분된 한 개의 키($z-key$)를 각각의 전역 키 풀에서 선택한 것이다.

키 배포 단계는 4단계의 절차를 가지는데 첫 번째로, 클러스터에 속한 각 노드는 자신이 가진 $l+1$개의 비밀 키 중 다른 노드와 구분되는 한 개의 키를 사용하여 현재 자신의 인증 키를 암호화한다. 노드의 인증 키 메시지 구성은 (1)과 같다.

$$\begin{aligned} Auth(v_i) = \{\, & v_i,\ j_i,\ id(y_1^{v_i}),\ id(y_1^{v_i}),\ k_{j_i y_1}^{v_i v_i}, \\ & \cdots,\ id(y_l^{v_i}),\ id(y_l^{v_i}),\ k_{j_i y_l}^{v_i v_i}, \\ & id(z^{v_i}),\ id(z^{v_i}),\ k_{j_i z}^{v_i v_i} \} \end{aligned} \tag{1}$$

여기서 j_i는 현재 인증 키의 인덱스이며 $j_i = 1$이면 첫 번째 배포를 뜻한다. $id(y_1^{v_i})$는 $y-key$풀에 있는 $y_1^{v_i}$의 인덱스이며 $\{\cdot\}_{y_1^{v_i}}$는 키 $y_1^{v_i}$로 암호화한 것을 말한다. 두 번째로, CH는 자신이 속한 클러스터의 모든 노드로부터 인증 메시지를 $K(n)$으로 취합한다. $K(n)$은 (2)와 같다. 여기서 $v_1, \cdots, v_n$은 클러스터에 속한 노드이다.

$$K(n) = \{\, Auth(v_1),\ \ldots,\ Auth(v_n) \} \tag{2}$$

세 번째로, CH는 $q(q>1)$개의 전달 노드를 자신의 이웃 중에서 선택하고 $K(n)$을 전달한다. q개의 전달 노드를 두는 이유는 경로상의 이웃 노드가 훼손되었을 경우 $K(n)$의 재분배 없이 다른 노드에 전달 할 수 있도록 하기 위함이다. 마지막 네 번째에서 전달 노드가 $K(n)$을 수신하였을 때 다음과 같이 동작한다.

1) $K(n)$이 최소 t개의 구분된 z키 인덱스를 가졌는지 검증 후 그렇지 않으면 $K(n)$이 위조되었다고 판단하고 폐기한다.
2) $K(n)$의 비밀 키 인덱스를 확인 후 같은 비밀 키 인덱스가 있다면 해당 메시지를 복호화하여 인증 키를 자신의 메모리에 저장한다.
3) $K(n)$을 q개의 이웃 노드들에 전달하는데 이때 배포되는 최대 홉 수($h_{\max}$)까지 전달되었다면 $K(n)$을 폐기한다. 각 노드는 $K(n)$이 BS에 도달하거나 $h_{\max}$까지 배포될 때까지 위 동작을 반복한다.

마지막으로 보고서 전달 단계에서는 이벤트를 감지한 센서 노드가 새로운 인증 키를 가지고 이벤트 정보에 대한 메시지 인증 코드(message authentication code; 이하 MAC)[11]을 생성하고 이를 자신의 CH에 보낸다. 이때 CH가 보고서를 생성하는데 참여하는 센서 노드의 수(t)는 노드가 분배되기 전에 미리 정해지며, CH는 해당 보고서를 q개의 이웃 노드에 전달한다. 전달 받은 노드가 보고서를 받았다는 메시지를 보내면 센서 노드의 인증 키를 노출시켜 보고서를 검증하고 검증 정보를 다음 홉 노드에 알려준다. 해당 과정은 보고서가 BS에 도달하거나 허위 보고서라고 탐지될 때까지 반복한다.

3. 제안 기법

본 장에서는 제안 기법의 배경이 된 DEF의 문제점에 대해 3.1에서 설명하고 3.2에서 제안 기법의 개요, 3.3에서 제안 기법을 위한 가정 사항을 언급하고 3.4에서 제안기법을 상세하게 소개한다.

3.1 동기

DEF는 토폴로지에 변화가 있어 키 분배 단계를 다시 거치지 않는 한, 손상된 노드의 MAC에 대한 탐지 능력이 고정되어 있기 때문에 공격에 지속적으로 노출 시 허위 보고서가 탐지되기 전까지 존재하지 않는 보고서를 전달하는 불필요한 에너지 소모가 발생한다. 탐지 능력의 개선을 꾀하고자 키 분배 단계를 임의로

시행할 수도 있지만, 이는 많은 에너지를 소비하기 때문에 그 시점을 정하는 것은 매우 중요하다. 또한, 네트워크의 토폴로지 변화에 따른 키 분배 단계를 거쳐 탐지 능력에 변화가 있더라도 훼손된 노드를 통한 지속적인 공격 발생임을 파악 및 고려하지 않은 방법이기 때문에 기존과 같은 문제가 계속 발생할 수 있다. 따라서 본 논문에서는 효율적인 키 재분배 기법을 통해 지속적인 공격 노출 시 허위 보고서를 보다 조기에 탐지하여 기존에 발생하던 불필요한 에너지 소모를 최소화하는 방법을 제안한다.

3.2 개요

DEF는 배포 전 단계에서 적재 받은 비밀 키의 변화가 없다는 특성이 있다. 이 특성을 이용하여 제안 기법은 DEF에서 보고서 전달 단계를 수정하고 키 재분배 단계를 추가한 것이다. 보고서를 전달받은 전달 노드가 보고서의 허위 유무를 판단할 때 허위 보고서로 탐지되면, 허위 보고서가 생성된(소스) 클러스터의 소스 CH를 확인하고 카운트를 한다. 같은 CH에서 계속 공격이 들어와 카운트 값이 일정 값을 초과하면 BS에게 키 재분배 요청 메시지를 보낸다. 그림 3은 이러한 제안 기법의 과정을 나타낸다.

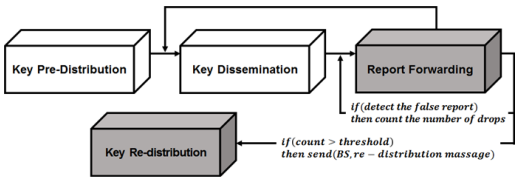

그림 3. 제안 기법의 동작 단계
Fig. 3. Operation phases of proposed scheme

3.3 가정

본 논문에서는 다음과 같은 가정들을 가진다. 키 사전 분배 단계는 노드가 필드에 배포 전, 이루어지기 때문에 BS는 모든 노드의 키 정보를 알고 있다. BS는 전역 키 풀을 통해 모든 키를 가지므로 허위 보고서가 중간에 탐지되지 못하고 BS까지 전달되었을 때 보고서의 허위 유무를 확인한다. 네트워크의 토폴로지 변화는 없다. 전달 노드는 탐지한 허위 보고서 개수를 저장하는 공간을 가지고 있다. 전달 노드는 $K(n)$으로부터 인증 키를 메모리에 저장할 때 복호화한 비밀 키를 함께 저장한다. 전달 노드에서 BS에게 요청하는 키 재분배 요청 메시지의 구조를 다음과 같이 정의한다.

$$FN \rightarrow BS : CH_{ID} \| KI_A \| KI_S$$

여기서 FN은 전달 노드(forwarding node)이고 CH_{ID}는 허위 보고서를 생성한 소스 CH의 ID이다. KI_A는 허위 보고서를 탐지한 인증키의 인덱스를 말하며 이 인증키를 저장하기 위해 사용된 비밀 키의 인덱스가 KI_S이다. $\|$는 연속된 결합을 의미한다. 제안 기법은 키 재분배 요청 메시지를 BS까지 전달하는데 드는 에너지와 BS에서 취합한 인증 키들을 키 재분배 노드까지 전송하는데 드는 에너지가 부가적으로 필요하다. 제안 기법은 이러한 부가적인 에너지 소모보다 키 재분배를 실행하여 허위 보고서가 바로 다음 홉에서 검출되어 얻는 에너지양이 더 큰 것을 목표로 한다.

3.4 상세 설명

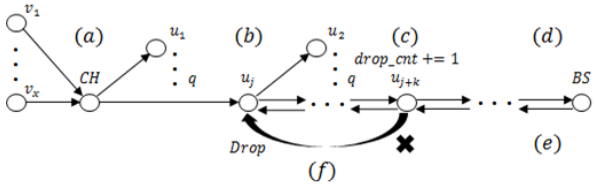

그림 4. 제안 기법의 실행 단계
Fig. 4. Execution phases of proposed scheme

그림 4는 제안 기법의 전체 실행 과정을 보여준다. 클러스터 내에 훼손된 노드 v_1~v_x와 CH가 허위 보고서를 생성하여 q개의 이웃 노드에 보고서를 전송한다(그림 4(a)). 이를 받은 다음 전달 노드 u_j가 보고서를 검증한다(그림 4(b)). 허위 보고서임을 탐지 못 하고 다음 q개의 이웃 노드에 보고서를 전송한다. 경로 상의 전달 노드 중 u_{j+k}노드가 허위 보고서임을 탐지하고 이를 폐기한다. 이때, 수신한 보고서를 통해 소스 CH 별 카운트 값을 저장한다(그림 4(c)). 공격이 지속적으로 발생하여 특정 CH의 카운트 값이 임계값을 초과하면 전달 노드는 키 재분배 요청 메시지를 BS에게 암호화하여 전달한다 (그림 4(d)). BS는 모든 키를 알고 있으므로 해당 메시지를 복호화하여 CH_{ID}와 KI_A, 그리고 KI_S를 저장한다. CH_{ID}값을 통해 해당 클러스터를 확인하고 소스 클러스터 내에 KI_A와 동일한 인증 키를 가진 노드가 있는지 확인한다. 만약 있다면 해당 노드를 의심 노드로 판단하고 적절한 조치를 취한다. 이에 대한 조치는 본 논문에서는 다루지 않는다. 만약 훼손된 노드가 인증 키를 갱신하여 소스 클러스터 내에 동일한 인증 키를 가진 노드를 찾을 수 없다면 KI_S와

표 1. 제안 기법의 BS 알고리즘
Table 1. BS algorithm of proposed scheme

```
1:  if BS receives (request_message)
2:    then Decrypt (request_message)
3:    Check source cluster by CH_ID value
4:    if KI_A == node.auth_key in src_cluster
5:      then Judge the node to suspicious node
6:    else
7:      if KI_S == node.secret_key in src_cluster
8:      then collect auth_keys of same secret key
9:      send to next hop node of src_cluster
10:     end if
11:   end if
12: end if
```

동일한 비밀 키를 가진 노드를 확인하고 노드들의 인증 키들을 취합하여 소스 CH 바로 다음 홉 전달 노드인 u_j에게 암호화하여 전송한다(그림 4(e)). 이는 취합된 인증 키 중 공격자로부터 탈취된 인증 키가 있기 때문이다. 해당 메시지를 받은 u_j는 복호화 후 메모리에 인증 키들을 저장한다. 만약 또다시 탈취된 인증 키로 공격자가 허위 보고서를 보낸다면 이를 바로 다음 홉 노드인 u_j에서 빠르게 탐지한다(그림 4(f)). 알고리즘 1은 제안 기법에서 BS가 키 재분배 요청 메시지를 받은 후의 수행과정을 pseudo-code로 보여준다.

4. 성능 평가

본 장에서는 제안 기법의 성능을 평가한다. 4.1에서 실험 환경에 대해 설명하고 4.2에서 실험 결과를 보인다.

4.1 실험 환경

실험 환경은 다음과 같이 구성한다. 센서 필드의 크기는 $1,000 \times 1,000\,m^2$이며 노드의 수는 총 1,000개로 900개의 일반 센서 노드와 100개의 CH로 구성되어 필드 상에 임의로 배포된다. BS의 위치는 (1000, 1000)이며, 각 노드는 l = 2의 y-key와 한 개의 z키를 각각의 키 풀(크기 20)에서 랜덤하게 가진다. 1 바이트를 전송하기 위해 필요한 에너지는 16.25 μJ, 필요 수신 에너지는 12.5 μJ이며 MAC 검증 시 75 μJ을 소모한다[12]. 보고서의 크기는 24 바이트, MAC은 1 바이트로 한다. 노드의 에너지 자원은 1J이다. 5개의 클러스터를 택하여 허위 트래픽 비율(false traffic ratio; 이하 FTR)에 따라 허위 보고서 주입 공격이 발생하며 훼손된 노드는 클러스터 내에 센서 노드와 CH 모두 가능하다. 노드의 전달 과정에서 패킷 손실은 없으며 보고서는 1,000번을 실행한다.

4.2 실험 결과

실험은 DEF와 제안 기법의 에너지와 허위 보고서 탐지 성능을 각각 비교하여 실행하였다. 제안 기법은 전달 노드에서 BS로 키 재분배 요청 메시지를 전송하는 임계값(α)을, 실험을 통해 최상의 경우(α=20)와 보통의 경우(α=50)로 파악하여 실험하였다. 그림 5는 FTR에 따른 제안 기법인 키 재분배 실행 횟수를 나타낸다. α의 값이 더 낮은 20일 때, 키 재분배 횟수가 더 많음을 알 수 있다.

그림 6는 FTR에 따른 네트워크의 전체 에너지 소비량을 보여준다. 두 기법 모두 FTR이 증가할수록 BS까지 전달되지 않고 그 전에 탐지되는 허위 보고서의 수가 많아지기 때문에 전체 에너지 소모량이 줄어든다. DEF와 제안한 기법의 에너지 차이는 제안한 키 재분배 단계를 통해 허위 보고서가 탐지되는 홉 수가 줄어들어

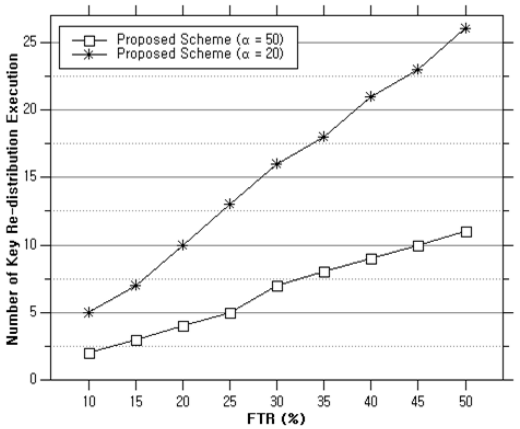

그림 5. FTR에 따른 키 재분배 실행 수
Fig. 5. Number of key re-distribution execution versus the FTR

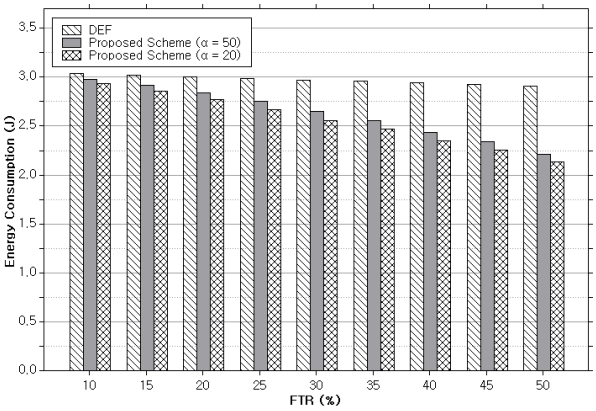

그림 6. FTR에 따른 에너지 소비량
Fig. 6. Energy consumption versus the FTR

불필요한 에너지 소모를 줄였기 때문이다. FTR이 증가할수록 두 기법의 에너지 차이가 증가됨을 볼 수 있는데 이는 제안 기법을 통해 보다 조기에 탐지되는 허위 보고서 양이 많아지기 때문이다. 기존 기법과 비교하였을 때 제안 기법의 에너지 절약은 FTR이 10%일 때 최대 3.22%, 20%일 때 최대 7.76%, 그리고 50%일 때 최대 26.63%의 에너지 효율을 보인다. FTR이 증가함에 따라 더 많은 에너지 절약을 확인하였다. 따라서 제안 기법은 기존 기법보다 평균 14.17%(α=20)의 에너지를 절약한다.

그림 7은 허위 보고서가 탐지되는 개수를 나타낸다. 두 기법 모두 FTR에 따라 발생한 허위 보고서를 80%이상 검출 할 수 있다. 제안한 기법이 탐지 성능에서 근소한 향상을 보이는 이유는 다음과 같다. 허위 보고서가 중간 전달 노드에서 탐지되지 않고 BS까지 도달했을 때, BS는 전달 노드와 동일하게 소스 CH 별로 카운트를 하고 해당 값이 임계값을 초과하면 키 재분배를 실행한다. 따라서 기존에는 탐지되지 않아 BS까지 전달되었던 허위 보고서가 소스 CH 다음 홉에서 탐지되기 때문에 탐지 성능이 향상된다. α의 값이 다른 두 제안기법의 탐지 성능이 같은 이유는 허위 보고서를 탐지 못하고 BS

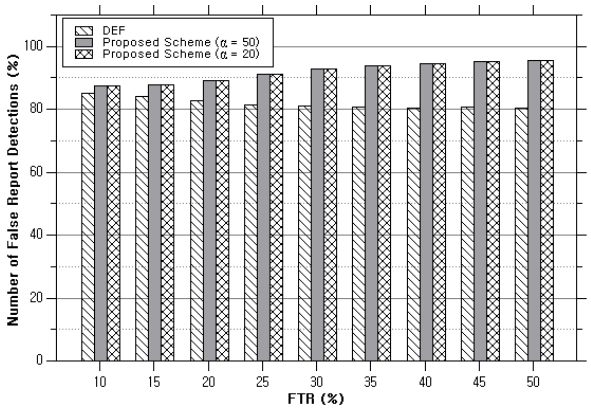

그림 7. FTR에 따른 허위 보고서 탐지 비율
Fig. 7. Ratio of dropped false report versus the FTR

까지 도달한 허위 보고서 중 같은 소스 클러스터에서 발생한 허위 보고서의 수가 임계값만큼 보다 발생하지 않았기 때문이다. 즉, 두 제안 기법의 BS가 허위 보고서를 카운트하여 실행한 키 재분배 횟수는 같음을 알 수 있다. 제안 기법은 기존 기법과 비교하였을 때 FTR이 10%일 때 최대 3.03%, 20%일 때 최대 7.26%, 그리고 50%일 때 최대 15.92%의 성능 향상을 확인하였다.

5. 결론

WSN은 개방된 필드에 배치되고 센서 노드의 제한적인 자원 때문에 쉽게 훼손되고 보안 공격에 취약하다. 따라서 공격을 방어하기 위한 프로토콜이 필요하고 이를 WSN에 적용 시, 에너지 자원을 고려함이 필수적이다. 제안된 기법은 DEF에서 훼손된 노드를 통해 인증 키를 탈취한 공격자가 허위 보고서 주입 공격을 지속적으로 가했을 때 생기는 에너지 소모를 줄이는 것이다. 결과적으로 실험을 통해 다음과 같은 이점을 얻는다.

1) 에너지 효율 향상 : 전달 노드에서 허위 보고서를 탐지하고 키 재분배 요청 메시지를 통해 공격 발생 클러스터 다음 홉 전달 노드에 키 재분배를 실행한다. 동일한 탈취된 인증 키로 공격 발생 시, 바로 다음 홉에서 이를 탐지하여 불필요 에너지 소모를 줄인다.
2) 보안성 향상 : 중간 전달 노드에서 탐지되지 않고 BS까지 전송된 허위 보고서에 대해 BS도 카운트를 하여 임계값 초과 시, 해당 소스 클러스터 다음 홉에 키 재분배를 실행하여 탐지 성능을 높인다.

향후 연구 분야로는 전달 노드가 BS로 키 재분배 요청 메시지를 전달하는 조건인 α의 적절한 선택에 대한 것과 다양한 공격과 프로토콜 환경에서 제안 기법의 효율성을 높이고자 한다.

References

[1] S. H. Lee, S. Lee, H. Song and H. S. Lee, "Wireless sensor network design for tactical military applications: Remote large-scale environments," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, 2009, pp. 1-7.

[2] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan and W. Westhoff, "Wireless sensor networks for flash-flood alerting," in *Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on*, 2004, pp. 142-146.

[3] H. Park and T. H. 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.

[4] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, pp. 2292-2330, 2008.

[5] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, pp. 1713-1723.

[6] Z. Yu and Y. Guan, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," *IEEE/ACM Transactions on Networking (ToN)*, vol. 18, pp. 150-163, 2010.

[7] D. J. Park and T. H. Cho, "Efficient Key Re-dissemination Method for Saving Energy in Dynamic Filtering of Wireless Sensor Networks," *The Korea Society of Computer and Information*, vol. 23, pp. 71-72, 2015, 7.

[8] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, 2004, pp. 259-271.

[9] A. S. Uluagac, R. A. Beyah, Y. Li and J. A. Copeland, "VEBEK: Virtual energy-based encryption and keying for wireless sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 9, pp. 994-1007, 2010.

[10] R. Lu, X. Lin, H. Zhu, X. Liang and X. Shen, "BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *Parallel*

and Distributed Systems, IEEE Transactions on, vol. 23, pp. 32-43, 2012.

[11] A. Perrig, R. Szewczyk, J. Tygar, V. Wen and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Networks*, vol. 8, pp. 521-534, 2002.

[12] S. M. Nam and T. H. Cho, "Dynamic States Consideration for Next Hop Nodes Selection Method to improve Energy Efficiency in LEAP based Wireless Sensor," *Ournal of Korean Institute of Intelligent Systems*, vol. 23, pp. 558-564, 2013.

저 자 소 개

박동진(Dong-Jin Park)

2015년 : 성균관대학교 컴퓨터공학 공학사

2015년~현재 : 성균관대학교 소프트웨어 플랫폼학과 석사과정

관심분야 : 무선센서 네트워크, 네트워크 보안, 모델링 시뮬레이션

Phone : +82-31-290-7221

E-mail : jin1307e@skku.edu

조대호(Tae-Ho Cho)

1983년 : 성균관대학교 전자공학과 공학사

1988년 : University of Alabama 전자공학과 공학석사

1993년 : University 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 : thcho@skku.edu