한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

센서 네트워크의 INSENS에서 싱크홀 공격을 탐지하기 위한 강인한 양방향 인증 기법

송규현°, 조대호*
°*성균관대학교 정보통신대학
e-mail: {songku3000, thcho}@skku.edu°*

Robust Bidirectional Verification Scheme for Detecting Sinkhole Attacks in INSENS of Sensor Networks

Kyu-hyun Song°, Tae-ho Cho*
°*College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

무선통신을 기반으로 하는 WSN은 통신의 특성상 네트워크보안에 취약점을 가진다. 무선통신의 취약점은 누구나 네트워크에 접근이 가능하다는 것이다. 이에 따라 침입에 강인한 무선 센서 네트워크인 INtrusion-tolerant routing protocol for wireless SEnsor NetworkS(INSENS)가 제안됨으로써 WSN의 초기 라우팅 설정 시 침입하는 공격자를 사전에 차단할 수 있게 되었다. 그러나 라우팅 설정 후에 노드가 공격자에 의해 훼손당하게 된다면, 노드의 주요정보를 이용해 공격자는 또다시 라우팅 공격이 가능해진다. 본 논문에서는 공격자에 의해 훼손된 노드가 라우팅 공격 중 대표적인 공격인 싱크홀 공격 메시지를 방송하였을 때, 페어와이즈 키를 통해 효과적으로 공격메시지를 차단하는 양방향인증기법을 제안한다. 이로써 INSENS에서 발생하는 싱크홀 공격을 차단함으로써 WSN의 보안 강화에 기여한다.

키워드: 무선 센서 네트워크(wireless sensor network), INSENS(intrusion-tolerant routing protocol for wireless sensor networks), 훼손(compromise), 싱크홀 공격(Sinkhole attack), 탐지(detecting)

I. 서 론

최근 소형 전자기기의 발달로 인해 저비용, 저전력, 다기능의 소형 센서 노드가 개발되었다. 이에 따라 무선통신을 기반으로 하는 WSN (Wireless Sensor Network; 이하 WSN)이 등장하였다. 다기능의 WSN은 군사, 의료, 환경 등 다양한 분야에 걸쳐 사용이 가능하다[1]. WSN은 노드에 장착된 센서를 통해 주변 환경의 데이터를 모으고 이를 BS에 방송하여 데이터를 정보화한다. 생성된 정보는 사용자의 용도에 따라 필요한 곳에 쓰인다. 그러나 공격자는 이러한 데이터를 도청, 파기, 훼손하기 위해 자신의 악의적인 노드를 WSN에 침입시켜 라우팅 공격을 시도한다. 이와 같은 악의적인 노드를 사전에 차단하기 위해 Jing Deng은 INSENS (INtrusion-tolerant routing protocol for wireless SEnsor NetworkS; 이하 INSENS)프로토콜을 제안하였다[2]. 이 프로토콜은 초기 라우팅 설정 시 공격자의 침입을 사전에 차단하는 것이 가능하다. 그러나 INSENS는 라우팅 설정이 완료된 구성원 노드를 공격자가 훼손시킨다면 또다시 라우팅 공격이 가능해진다. 이러한 라우팅 공격 중 대표적 공격은 싱크홀 공격(sinkhole attack)이 있다. 싱크홀 공격은 자신이 BS라고 속이는 방법과 자신이 BS까지의 최단경로라고 속이는 방법으로 공격한다. 이 두 공격 모두 WSN의 라우팅을 변경하여 자신에게 메시지가 도달하게 한 후 메시지를 훼손하는 공격이다[3]. 본 논문은 INSENS를 기반으로 하는 WSN의 구성원 노드가 공격자에 의해 훼손되어 싱크홀 공격이 발생했을 때, 이를 사전에 차단하는 기법을 제안한다. 논문의 구성은 다음과 같다. 2장에서는 INSENS와 싱크홀 공격을 소개하고, INSENS를 대상으로 한 싱크홀 공격에 대해 알아본다. 3장에서는 INSENS에서 발생한 싱크홀 공격을 감지하고 이를 차단하는 방법에 대해 제안한다. 4장에서는 결론을 논의한다.

II. 관련 연구

본 장은 돌진공격(rushing Attack)[4]을 감지하기 위한 Basic INSENSE를 기반으로 둔 Enhanced INSENSE에 대해서 상세하게 설명한다.

1. INSENS의 정의

INSENS프로토콜은 최초 라우팅 설정 시 침입하는 공격자의 노드가 WSN에 구성원이 되는 것을 사전에 차단한다. INSENS의 동작과정은 크게 이웃노드인증, 라우팅 요청 및 설정으로 총 2가지로 나뉜다. 이웃노드 인증 메시지는 다음과 같다.

$$ECHO||E_{global_{KEY}}(ID_x||nonce)$$

ECHO는 메시지의 종류이며 ||는 연접을 뜻한다. global_KEY는 노드가 배치되기 전 노드들에 직접 주입한 대칭 키로서 인가되지 않은 공격자의 침입을 방지한다. ID는 ECHO메시지를 발송한 노드의 ID이며, nonce는 랜덤으로 생성된 숫자이다. 이 메시지를 받은 노드는 응답메시지를 만들어서 방송한다. 응답메시지는 다음과 같다.

$$ECHOBACK||E_{global_{KEY}}(ID_y||nonce+1||K_{y,x})$$

노드x는 위 메시지를 수신하면 ID를 비교하고 $ID_x<ID_y$ 이면 x로 부터생성 된 nonce$(K_{x,y})$를 페어와이즈 키(pairwise key)로 설정하고, $ID_x>ID_y$ 이면 y로부터 생성된 nonce를 페어와이즈 키로 설정한다. 그리고 노드는 새로운 클러스터 키(Cluster key)[5]를 만들어 이웃노드에 페어와이즈 키로 암호화하여 알려준다. 일정 시간이 지난 노드는 글로벌 키를 외부침입자가 알지 못하게 자신의 ID와 함께 MAC (Message Auth entication Code; 이하 MAC)계산을 하여 인증된 노드라는 것을 알려주는 키 K를 만들고, 또한 임의의 숫자와 함께 MAC계산을 하여 yi로 글로벌 키를 은닉한다. 이 두 값은 이후 새로운 노드 추가 시 인가된 노드인지 파악하는 데 사용한다. 인증과정이 끝난 WSN은 라우팅 설정을 위해 센서 노드들과 BS들과의 다중 라우팅을 구성함으로써 공격자에 의해 차단되는 노드를 최소화한다. 다중 라우팅 요청메시지는 다음과 같다.

$$REQ||ID_A||E_{CK_A}(OHC||ID_{BS})$$

CK_A는 A 노드의 클러스터 키를 의미하며, E는 암호화하는 것을 의미한다. OHC (One-way Hash Chin; 이하 OHC)는 단방향 해시 체인으로서 인가되지 않은 공격자가 현재 방송된 OHC의 값을 습득하여도 다음 OHC 값을 알 수 없으므로 침입하는 것을 막는 역할을 한다. 이 메시지를 통해 WSN은 다중 스패닝 트리(Multiple Spanning Trees)를 구성한다[2].

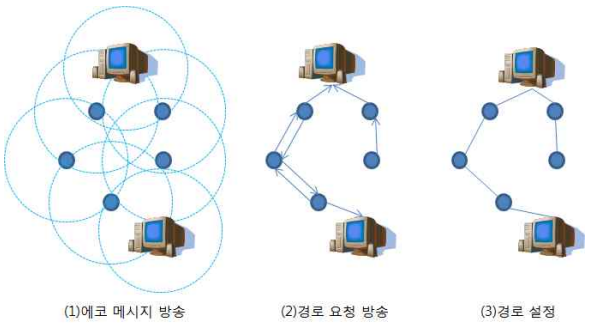

그림 1. INSENS의 동작과정
Fig. 1. Operation of INSENS

2. 싱크홀 공격

싱크홀 공격은 모든 메시지를 공격자 자신에게 도달하도록 라우팅을 변경하고, 자신에게 도달한 메시지를 훼손시키는 공격이다. 싱크홀 공격은 크게 두 가지 형태로 나뉜다. 한 가지는 공격자 노드가 자신이 BS인 것처럼 노드들을 속이는 공격이며, 또 다른 한 가지는 자신이 BS까지의 최단 경로라고 속이는 공격이다[3]. 공격당한 WSN은 공격자 노드에 메시지를 방송하고 공격자는 그 메시지를 파기, 훼손, 위변조를 통해 BS의 잘못된 판단, 통신상의 에러 등 혼란을 발생시킨다. 최악의 경우에는 WNS 운영을 할 수 없게 된다. 싱크홀 공격은 그림 2와 같다.

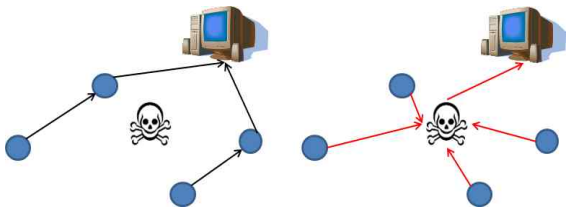

그림 2. 싱크홀 공격
Fig. 2. Sinkhole Attack

3. INSENS를 대상으로 한 싱크홀 공격

공격자는 싱크홀 공격을 시도하기 위해 라우팅이 구성된 WSN의 구성원 노드를 훼손시켜 노드의 주요정보인 yi, K, OHC, ID, 자신의 클러스터 키, 이웃노드의 클러스터 키와 페어와이즈 키, OHC-F (OHC를 생성하는 함수; 이하 OHC-F)를 습득한다. 공격자는 이 정보를 가지고 라우팅 요청 메시지를 만든다. 그리고 공격자는 노드를 사용하여 라우팅 변경을 시도한다. 하지만 INSENS는 다중 라우팅을 구축하기 때문에 노드 간에 계층관계가 성립되지 않는다. 따라서 공격자가 최단경로라 속이는 공격을 시도하더라도 무용지물이 된다. 그리하여 공격자는 BS사칭공격(BS로 속이는 공격; 이하 BS사칭공격)을 시도한다. 노드들은 라우팅 요청메시지의 OHC 값을 확인하여 BS를 인증하기 때문에 인가된 모든 노드는 다음의 OHC 값을 알 수 있도록 OHC-F를 가지고 있다. 이것을 이용하여 공격자는 다음 OHC 값을 만든다. 공격자의 라우팅 요청 메시지는 다음과 같다.

$$REQ||ID_{H-A}||E_{CK_{H-A}}(OHC||ID_{H-A})$$

H-A는 포획당한 노드의 ID이다. 메시지를 수신한 노드는 자신이 가지고 있는 OHC-F를 이용하여 도출된 값과 OHC 값을 비교하여 방송된 메시지가 BS에서 방송된 메시지인지 확인한다. 하지만 공격자가 보낸 메시지의 OHC 값 역시 OHC-F로 만들어진 값이므로 정상노드는 공격자의 노드를 BS라 인식하게 된다. 이후 모든 노드가 같은 형태로 라우팅 설정을 하게 된다. 이 결과 싱크홀 공격으로 훼손된 WSN의 라우팅 설정이 완료된다.

III. 본론

본 논문은 라우팅 설정이 완료된 INSENS기반의 WSN내에서 공격자에 의해 포획된 노드가 BS사칭공격을 시도하기 위한 라우팅

요청메시지를 방송할 때, 공격자의 메시지를 차단하기 위해 연구를 진행하였다. 공격자는 관련 연구에 제안된 BS사칭공격을 시도한다고 가정한다.

1. 초기 이웃노드 인증단계

최초 노드가 배치되기 전 BS는 각 노드와 대칭 키 방식의 페어와이즈 키를 Key-F (키 생성함수; 이하 Key-F)를 사용하여 생성한다. 이 키는 라우팅 요청 및 설정단계에서 노드가 받은 경로요청메시지가 BS에서 방송된 메시지가 맞는지 확인하기 위해 BS와의 양방향검증에 사용된다. 키를 생성하는 함수인 Key -F는 BS에서만 갖고 있다. 결과적으로 BS와 노드 간의 페어와이즈 키는 BS에서만 생성할 수 있다. BS는 생성된 키를 각 노드에 주입한다. 이후 기존방식과 같은 방법으로 글로벌 키를 주입하고, 각 노드를 배치한다. BS는 노드와의 통신을 위해 이웃노드 인증과정을 수행한다. 이웃노드 인증 메시지는 다음과 같다.

$$ECHO||E_{global_{KEY}}(ID_x||nonce||ID_{BS_1})$$

$$ECHOBACK||E_{global_{key}}(ID_y||nonce+1||K_{y,x}||ID_{BS_1})$$

기존 INSENS의 인증 메시지에 BS의 ID를 추가하여 방송한다. BS의 ID는 라우팅 요청단계에서 수신된 라우팅 요청 메시지가 어느 BS에서 방송된 메시지인지 확인하는 데 사용한다. 노드들은 자신에게 도달한 인증 메시지의 BS ID를 저장한다.

2. 라우팅 설정단계

이웃노드 인증이 끝나면 BS는 경로요청 메시지를 방송한다. 방송 메시지는 다음과 같다.

$$First\,REQ||ID_{BS}||E_{CK_{BS}}(OHC||ID_{BS})$$

First REQ 메시지를 받은 이웃노드 A는 ID를 통해 이웃노드에서 방송한 메시지인지 확인하고, 노드의 클러스터 열쇠로 복호화하여 OHC와 BS의 ID를 확인한다. 정상적인 BS의 ID이면 신뢰성을 위해 자신이 가지고 있는 BS와의 페어와이즈 키를 사용하여 피드백 메시지로 BS와 양방향 검증을 시도한다. 피드백 메시지는 다음과 같다.

$$FDBK||ID_A||E_{Pairwise_{A,BS}}(OHC||nonce)$$

nonce는 A 노드가 생성한 난수 값이다. nonce는 이후 돌아오는 응답메시지가 자신이 방송한 메시지에 대한 응답이 맞는지를 확인하는 데 사용된다. 피드백 메시지를 받은 BS는 노드의 ID를 확인하고 자신과 A 노드의 페어와이즈 키를 사용하여 메시지를 복호화한다. 그리고 OHC 값을 자신의 OHC 값과와 비교한다. 같다면 BS는 nonce 값을 저장하고, nonce+1을 한다. +1을 한 nonce 값을 사용하여 자신의 ID를 MAC계산한다. 그리고 응답메시지를 방송한다. 메시지는 다음과 같다.

$$OK||ID_{BS}||E_{Pairwise_{A,BS}}(MAC(nonce+1, ID_{BS}))$$

메시지를 수신한 노드 A는 BS의 ID를 자신이 생성한 nonce에+1을 통해 MAC계산을 하고 맞으면 REQ메시지를 노드들에 방송한다. REQ메시지의 구조는 다음과 같다.

$$REQ||ID_A||E_{CK_A}(OHC||ID_{BS}||\\MAC(nonce+1, ID_{BS}))$$

MAC는 라우팅 설정을 완료하기 전에 BS에서 발생한 메시지가 맞는지에 대한 재확인을 위해 사용된다.

3. 실험결과

본 실험은 기존 INSENS와 제안 기법으로 구성된 각각의 WSN에서 라우팅설정 후 한 노드가 공격자에 의해 훼손되었을 때를 가정한다. 공격방법은 훼손된 노드를 통해 싱크홀 공격인 BS사칭공격으로 라우팅 변경을 시도한다. 그 결과는 그림 3의 그래프와 같다.

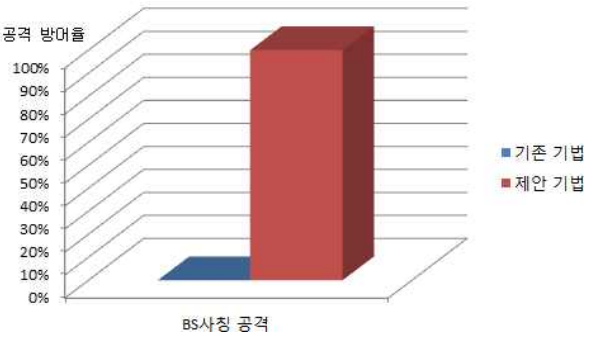

그림 3. 싱크홀 공격 탐지율 그래프

Fig. 3. success rate graph of Sinkhole attack

세로축은 싱크홀 공격의 방어율이고, 가로축은 기법의 종류이다. 탐지율에 대한 계산은 다음과 같다.

$$\text{싱크홀 공격 메시지 차단 횟수}/\text{싱크홀 공격 메시지 발생 횟수}\times 100$$

이 실험 결과를 통해 제안 기법이 싱크홀 공격을 사전에 차단한다는 것을 알아보았다.

Ⅳ. 결 론

본 논문에서는 INSENS를 기반으로한 WSN에서 공격자에 의해 훼손된 노드가 발생하는 싱크홀 공격메시지를 제안 기법을 이용해 사전에 차단하는 방법을 제안하였다. 이를 통해 INSENS의 신뢰성과 보안 강화에 기여한다.

ACKNOWLEDGMENT

이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2013R1A2A2A01013971)

참고문헌

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirici, "A survey on Sensor network,", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.

[2] J. Deng, and R. Han S. Mishra, “INSENS: Intrusion-tolerant routing for wireless sensor networks,”, Ad hoc Network, Vol. 29, No. 2, pp. 216-230, July 2006.

[3] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,”, Ad hoc network, Vol. 1, No. 2, pp. 293-315, 2003.

[4] Y. Hu, A. Perrig, D. Johnson, “Rushing attacks and defense in wireless ad hoc network routing protocols,”, Proceedings of the 2nd ACM workshop on Wireless security, ACM, pp. 30-40, 2003.

[5] S. Zhu, S. Setia, S.Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks-10th ACM Conference on Computer and Communications Security (CCS'03),” Washington DC, USA, Oct 2003.