디지털산업정보학회 논문지 제6권 제3호-2010년 9월

디렉티드 디퓨젼 기반의 무선 센서 네트워크에서의 싱크홀 공격을 막기 위한 트랜잭션 서명기법에 관한 연구

김 태 경*

Transaction Signing-based Authentication Scheme for Protecting Sinkhole Attack in Directed Diffusion based Wireless Sensor Networks

Kim, Tae Kyung

〈Abstract〉

In this paper, We propose a transaction signing-based authentication scheme for protecting sinkhole attacks in wireless sensor networks. Sinkhole attack makes packets that flow network pass through attacker. So, Sinkhole attack can be extended to various kind of attacks such as denial of service attacks, selective delivery or data tamper etc. We analyze sinkhole attack methods in directed diffusion based wireless sensor networks. For the purpose of response to attack method, Transaction signing-based authentication scheme is proposed. This scheme can work for those sensor networks which use directed diffusion based wireless sensor networks. The validity of proposed scheme is provided by BAN logic.

Key Words : Sinkhole, Wireless sensor network, Authentication

Ⅰ. 서론

무선 센서 네트워크는 미래의 유비쿼터스 환경에 기반이 될 중요한 기술이다. 센서 네트워크는 저비용으로 데이터의 수집 및 측정을 하는 응용들에 의해 폭넓게 이용될 수 있다. 이러한 센서 네트워크의 주된 이점들 중 하나는 스스로 네트워크를 구성할 수 있고 동적 라우팅 프로토콜을 사용할 수 있기 때문에 노드의 분포 및 설정이 용이하다는 점이다[1]. 무선 센서 네트워크는 대상 지역 내 사용자의 관심 정보에 해당하는 이벤트 발생 시 이를 감지하여 사용자에게 보고하는 것을 목적으로 하는 네트워크이다[2]. 무선 센서 네트워크는 많은 수의 센서 노드와 하나 이상의 싱크 노드(Sink node) 로 구성되며, 센서 네트워크는 대부분 광범위 환경에 배치되므로 단말의 전원을 자주 교환하는 것이 어렵기 때문에 센서, 무선 통신 모듈, 프로세서 등이 저소비 전력을 사용해야 한다. 또한 단말의 설치가 용이하고 모니터링 대상에 영향을 주지 않기 위해서는 단말의 소형화와 경량화가 필수적으로 요구된다[3-4]. 싱크 노드는 사용자와 직접 연결된 노드로서 센서 노드들로부터 수집된 정보를 가공하여 사용자에게 제공한다. 무선 센서 네트워크의 주 적용 분야로

* 서울신학대학교 교양학부 교수

는 교통, 방범 보안 및 재해대책에 많이 사용되고 있다.

이러한 무선 센서 네트워크는 기반시설 없이 열린 환경에서 동작하므로 다양한 보안 위협에 노출하게 된다[5]. 가장 대표적인 공격으로 싱크홀 공격(sinkhole attacks)에서 공격자는 라우팅 관련 메시지를 위조함으로써 자신이 획득한 노드를 통해 센서 네트워크 내의 대부분의 트래픽이 통과하도록 한다. 해당 공격 노드는 수신한 데이터에 서비스 거부, 선택적 전달 또는 데이터 위변조 공격 등을 시도할 수 있다[6]. 이러한 싱크홀 공격은 네트워크의 오버헤드를 가중시키고 전체 네트워크의 배터리 소모를 가속화 시켜 전체 네트워크의 수명을 단축시키고 또한 다른 공격을 적용하기가 용이하므로 싱크홀 공격에 대한 대응방법은 신중하게 고려되어야 한다.

본 논문에서는 센서 네트워크에서의 대표적인 라우팅 기법인 디렉티드 디퓨젼(Directed Diffusion: DD)[6] 방식의 싱크홀 공격에 대한 취약성을 설명하고 이를 방어할 수 있는 대응 기법을 제안하였다. 제안 기법에서 센서 필드에 배치된 베이스 노드(Base Node)들은 디렉티드 디퓨젼에서 사용되는 라우팅 메시지인 경로 강화 메시지의 인증 방법을 이용하여 싱크홀 공격인지 아닌지를 판별한다. 즉 싱크홀 공격 발생으로 인한 다양한 공격들을 방어하기 위한 대응 기법을 센서 노드의 인증으로 그 해결책을 제시하는 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 센서 네트워크에서의 대표적 라우팅 기법인 디렉티드 디퓨젼 기법의 동작 과정 및 싱크홀 공격에 대한 취약성에 대해 설명하였으며, 3장에서는 제안 기법의 동작 과정을 설명하였다. 4장에서는 제안한 프로토콜의 안정성을 제시하였으며, 5장에서는 결론 및 향후 연구계획을 정리하였다.

Ⅱ. 관련연구

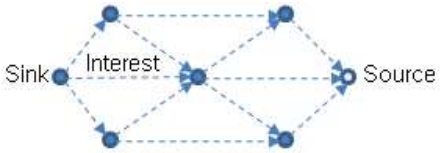
2.1 디렉티드 디퓨젼

디렉티드 디퓨젼은 데이터 중심적(data centric) 라우팅 프로토콜로서 노드의 주소가 아닌 데이터를 기준으로 메시지 라우팅이 이루어지는 특징을 갖고 있다. 디렉티드 디퓨젼의 동작은 크게 1) 관심 정보 배포, 2) 기울기 설정, 3) 강화된 경로를 통한 이벤트 정보 전달로 나누어진다. 관심 정보 배포 단계에서는 센서 노드들이 수행해야 할 감지 임무에 해당하는 관심 메시지(interest message)가 브로드캐스트(broadcast) 방식을 통해 전체 센서 네트워크에 전달된다. 관심 메시지를 수신한 노드는 해당 메시지를 보낸 노드에 대해 기울기(gradient)를 설정한다. 기울기는 이벤트 감지 및 이벤트 메시지 수신 시 이를 전달할 노드 ID와 전송률 정보를 담고 있다.

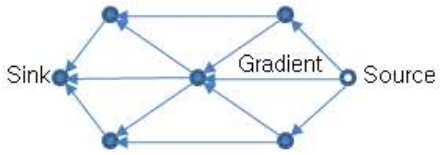
대상 지역에서 이벤트 발생 시 이를 감지한 노드들은 미리 설정된 기울기에 의거하여 싱크 노드 방향으로 메시지를 전달한다. 싱크 노드가 관심 정보에 해당하는 이벤트 정보를 수신하면 여러 이웃 노드 중 한 노드를 선택하여 경로 강화 메시지를 보낸다. 경로 강화 메시지가 이벤트 감지 노드까지 전달되면 이벤트 발생 지역에서 싱크 노드까지의 최적의 경로를 따라 이벤트 메시지가 전달된다. <그림 1>은 디렉티드 디퓨젼의 동작 과정을 순서대로 보여 준다[6].

2.2 디렉티드 디퓨젼에서의 싱크홀 공격

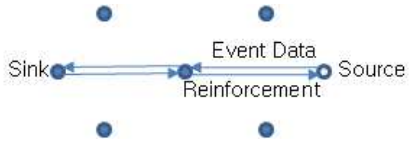
싱크홀 공격 (Sinkhole attack)이란 센서 네트워크의 일 대 다 통신 방식을 이용한 공격으로 공격 노드는 주변 노드들에게 싱크 노드까지의 효율적인 경로를 제공하는 것처럼 위장하여 네트워크 트래픽의 전달 경로에 자신을 포함시키는 공격이다. 이를 위해 공격 노드는 센서 네트워크에서의 라우팅 관련 메시지를 위조 혹은 재전송한다. 디렉티드 디퓨젼에서의 데이터 전달은 싱크 노드



(a) 관심 메시지 배포



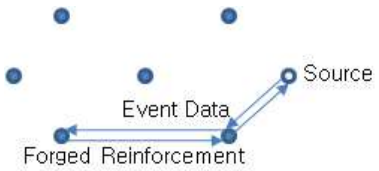
(b) 기울기(Gradient) 설정



(c) 강화된 경로를 통한 이벤트 정보 전달

<그림 1> 디렉티드 디퓨젼 방식의 동작 과정

까지의 거리를 고려하지 않기 때문에 공격자는 디렉티드 디퓨젼에서의 경로 강화 메시지를 위조하여 주변 노드들에게 전송한다. 이를 수신한 노드들은 이벤트 정보를 감지 혹은 수신 시 이를 공격 노드를 통한 경로로 전달한다. 공격 노드는 이렇게 수집한 이벤트 정보를 이용하여 선택적 전달 공격, 데이터 위조 공격 등을 시도한다. <그림 2>는 디렉티드 디퓨젼에서의 싱크홀 공격 과정을 나타낸 것이다.

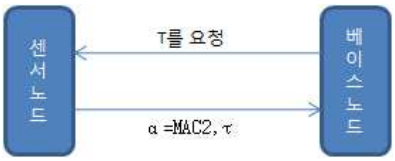


<그림 2> 디렉티드 디퓨젼에서의 싱크홀 공격

공격자는 센서 네트워크 내 노드를 획득하여 싱크홀 공격을 수행하도록 재설정 할 수 있다. 공격 노드는 주변 노드들이 서로 주고받는 메시지를 도청하여 현재 사용자가 요구하는 이벤트의 종류를 알아낼 수 있으며, 또한 이벤트 감지 노드들에게 위조된 경로 강화 메시지를 보내어 이벤트 정보가 공격 노드에게 전달되도록 라우팅 경로를 변경시킬 수 있다. 디렉티드 디퓨젼에서 각각의 노드는 가장 높은 전송률을 요구하는 노드에 이벤트 정보를 전송한다. 따라서 공격 노드가 높은 전송률 값을 포함하는 경로 강화 메시지를 위조하여 전송하면 이를 수신한 노드들은 이벤트 감지 및 이벤트 메시지 수신 시 공격 노드로 전송한다. 공격 노드는 수집한 이벤트 정보에 대해 선택적 전달 공격, 위조 데이터 공격을 수행할 수 있다[7]. 또한 웜홀(wormhole attack) 공격도 발생시킬 위험이 증가하게 되는데, 웜홀 공격은 일반적으로 두 개의 공격 노드가 쌍을 이루어 동작하며, 하나의 공격 노드가 주변의 정상 메시지를 도청하여 터널을 통해 맞은 편 공격 노드로 전달하면 이를 수신한 공격 노드는 해당 메시지를 자신의 주변 지역 노드들에게 브로드캐스팅 하여, 웜홀을 통과한 메시지를 수신한 정상 노드들은 해당 메시지가 자신의 이웃 노드로부터 온 것으로 오인하게 할 수 있다. 그러므로 무선 센서 네트워크에서 이러한 MITM(Man-In-The-Middle) 공격을 차단할 수 있는 인증기법이 필요하다.

Ⅲ. 제안 인증 메커니즘

앞서 지적한 보안 문제를 해결하기 위해 <그림 3>과 같은 인증서기반의 트랜잭션 서명기법을 제안하였다. 인증서기반의 트랜잭션 서명기법[8]은 안전한 인터넷 뱅킹을 위해 사용되는 인증기법으로 본 논문에서는 무선 센서 네트워크에 이 기법을 적용하였다. 여기서 각 센서는 자신의 인증서를 소유하고 있으며, 경로 강화 메시지를 입력으로 하는 트랜잭션 기반의 인증방식을 나타내고 있다.



<그림 3> 인증서기반의 트랜잭션 서명기법

<그림 3>에서 사용된 기호의 정의는 다음과 같다.

- H_k: 일방향 해쉬함수
- K : 공유키
- T: 경로 강화 메시지 정보
- T_p: T의 부분 정보
- $T \supseteq T_p$: 센서 노드의 개인키
- SK(A): 베이스 노드의 공개키
- PK(A): 베이스 노드의 개인키
- ρ: 노드의 PIN 값
- ζ : 동기정보
- A: 베이스 노드
- B: 센서 노드

- 센서 노드에서의 작업 수행
  - 토큰 정보: K를 사용하여 해쉬
    $\alpha = MAC1 = H_K(T_P, \rho, \zeta) = f(K, T_P, \rho, \zeta)$
  - $SK_{(B)}$를 사용하여 서명
    $\beta = sign_{SK(B)}(\alpha) = (MAC1)$
  - $PK_{(A)}$를 사용하여 암호화
    $\gamma = E_{PK_{(A)}}(T)$
- 센서 노드에서 베이스 노드로 β,γ의 정보 전송
- 베이스 노드에서의 작업 수행
  - γ를 복호화
  - α를 생성
  - β를 검증

일반적으로 인증방식은 OTP 기반의 트랜잭션 서명 방식과 유사하다. 센서 노드는 OTP 지원 모듈과 공인인증서를 저장하고 있기 때문에 OTP 생성을 위한 키(k)를 가지고 MAC1(α)을 생성하고, 인증서에 포함된 개인키를 이용하여 서명해 MAC2(β)를 생성하여 베이스 노드에 전송한다.

MAC2(β)와 경로 강화 메시지(T)를 베이스노드의 개인키로 암호화한 γ를 수신한 베이스 노드는 등록된 PIN(ρ), 공유키(k) 그리고 동기정보(ζ)를 사용하여 $f(k, T_P, \rho, \zeta)$을 생성하여 검증하고, β를 복호화 한다. 베이스 노드는 공개키로 서명된 MAC2를 검증하여 MAC1과 동일하면 경로 강화 메시지의 정보를 정상적인 정보로 인지하고 라우팅 정보에 반영한다.

Ⅳ. 유효성 검증

본 절에서는 해당 제안 기법이 싱크홀 공격에 대응 가능함을 제시하기 위하여 BAN 로직을 사용하여 제안 프로토콜을 검증하였다. BAN 로직은 분산 네트워크 환경에서 개체들의 인증에 관한 프로토콜의 검증과 분석을 위하여 만들어진 로직이다. 정형명세를 위해서 사용된 표시들은 [9]에 제시된 표현을 사용하였다.

BAN 로직의 핵심 요소는 통신 주체들 간에 전송되는 메시지가 최근의 것이고 적절한 키를 사용하여 암호화가 되었다면 인증될 수 있다는 정의에서부터 시작된다. 이 정의는 암호화에 사용되는 알고리즘이 안전하다는 것을 가정하고 있으며, 많은 보안 프로토콜에 대한 분석과 암호 분석을 위한 도구로서 사용되고 있다.

4.1 제안 프로토콜의 검증

인증 프로토콜의 기술을 위해 전통적인 보안 명세에서는 주체 사이에 단순히 메시지만을 나열하거나 상징적으로 보내는 사람, 받는 사람, 메시지의 내용들을 보여주는 것에 치중하였다. 그러나 이러한 명세는 로직에서 조작하기 힘들 뿐 아니라 메시지에 포함된 내용으로부터

명백한 의미를 얻어낼 수 없다. 따라서 보안 명세를 통해 프로토콜의 정확한 의미뿐만 아니라 주고받는 메시지의 의미를 명확히 나타낼 필요가 있다. 그러므로 본 논문에서는 BAN 로직[9]을 이용하여 제시한 메커니즘을 정형 명세하고, 검증하고자 한다.

제안 프로토콜을 BAN 로직에 따라 정규화한다면 식 (1)과 같이 기술할 수 있으며, 식(2)부터 식 (7)까지는 가정을 나타내고 있다.

$$\beta=\alpha=<X,\zeta>_{\rho},\rho_{K_k},A\overset{K_k}{\longleftrightarrow}B,A\overset{\rho}{\Leftrightarrow}B, \quad (1)$$
$$A\overset{\zeta}{\Leftrightarrow}B,\xrightarrow[K_B^{-1}]{K_{(B)}},\gamma=M,\xrightarrow{K_{(A)}}A_{K_{(A)}}$$

$$A|\equiv A\overset{K_k}{\longleftrightarrow}B \quad (2)$$

$$A|\equiv A\overset{\rho}{\Leftrightarrow}B \quad (3)$$

$$A|\equiv A\overset{\zeta}{\Leftrightarrow}B \quad (4)$$

$$A|\equiv \xrightarrow{K_{(A)}}A \quad (5)$$

$$A|\equiv \xrightarrow{K_{(B)}}B \quad (6)$$

$$B|\equiv(\zeta) \quad (7)$$

정규화된 프로토콜을 가정과 공리를 사용하여 로직을 다음과 같이 검증할 수 있다.

- 단계 1: A는 가정 (2), (3), (4), (7)가정에 의해 K_k와 ρ를 가지고 있으며, 시드(seed) 정보로서 ζ을 가지고 있다.
- 단계 2: 가정 (5)와 BAN 로직의 message-meaning rule의 공개키 암호방식[9]로부터 베이스 노드는 센서 노드가 전송한 γ를 읽을 수 있고, 트랜잭션 X를 확인할 수 있다.
- 단계 3: (2) 가정과 nonce-verification rule[9]의 공리로부터 베이스 노드는 최근의 ζ을 생성하고 (2), (4)의 가정에 의해 동일한 α를 생성할 수 있다. 이때 베이스 노드는 message-meaning rule 대칭키와 비밀키 암호 방식에 대한 메시지 규칙 공리에 의해 센서 노드로부터 생성된 트랜잭션이라는 것을 믿을 수 있다.
- 단계 4: 베이스 노드는 (1)의 가정과 nonce-verification rule[9]의 공리에 의해 센서 노드의 개인키(K^{-1})로 서명된 β를 센서 노드의 공개키(K)를 사용하여 검증하고, 센서 노드가 최근에 거래 요청한 트랜잭션서명이란 것을 믿을 수 있다. 이상의 논리적인 검증을 통해 베이스 노드는 센서 노드가 전송한 트랜잭션 요청 정보를 검증할 수 다.

4.2 싱크홀 공격 공격에 대한 대응 분석

공격자는 라우팅 정보를 변경하기 위한 경로 강화 메시지 M을 위조하여 공격 노드를 통한 경로로 전달하기 위해 M'로 변경하여 공격을 시도한다. 공격자는 $\gamma'=M',\xrightarrow{K_{(A)}}A_{K_{(A)}}$를 생성하여 싱크홀 공격을 시도한다. 베이스 노드는 단계 2에서 M'를 추출하고 단계 3을 수행한다.

여기서 베이스 노드가 생성한 α'는 $<M',N>,\rho_{K_k}$이고, 실제로 센서 노드가 시도한 α는 $<M,N>,\rho_{K_k}$이기 때문에 해당 트랜잭션은 거절이 되어 선택적 전달 공격, 데이터 위조 공격 등을 시도할 수 없다. 그러므로 디렉티드 디퓨젼 기반의 무선 센서 네트워크에 대한 싱크홀 공격을 효과적으로 차단할 수 있다.

Ⅴ. 결론

무선 센서 네트워크는 최근 주요 이슈가 되고 있는 네트워크 기술로서 그 활용분야가 더욱 확대될 것으로 예상되고 있다. 그러나 센서 네트워크는 무선 통신의 특성

과 제한된 성능 및 자원으로 인해 여러 가지 공격에 노출되어 있다. 특히 라우팅 프로토콜의 경우 공격에 노출되기 쉬우며 공격이 발생하면 최악의 경우 서비스 불능 상태가 될 수 있다. 그러므로 본 논문에서는 무선 센서 네트워크 환경에서 안전하고 효율적으로 싱크홀 공격을 방어할 수 있는 트랜잭션 서명기법의 인증 방안에 대한 연구를 수행하였다.

본 논문에서 제시한 인증 알고리즘의 안전성을 제시하기 위해 BAN 로직을 이용하여 그 유용성을 증명하였으며, 향후 연구계획으로는 무선 센서 네트워크와 다른 네트워크가 융합된 컨버전스 네트워크 환경에서 다양한 공격을 차단할 수 있는 효율적인 인증 방식에 대한 연구를 수행할 것이다.

참고문헌

[1] 최병구, 조응준, 홍충선, "무선 센서 네트워크 환경에서 링크 품질에 기반한 라우팅에 대한 효과적인 싱크홀 공격 탐지 기법," 정보과학회논문지 제14권 9호, 2008년 12월, pp. 901~905.

[2] N. Xu, "A Survey of Sensor Network Applications," Tech. Rep., University of Southern California, 2002.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, Vol. 40, No. 8, 2002.

[4] J. N. AlKaraki, A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE Wireless Communication Magazine, Vol. 11, No. 6, 2004, p. 628.

[5] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, Vol. 1, No. 23, 2003.

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in Proceedings of ACM Mobicom, Boston, MA, 2000.

[7] 문수영, 조대호, "디렉티드 디퓨젼 기반의 무선 센서 네트워크에서의 싱크홀 공격과 그 대응 방법," 정보처리학회 춘계 학술대회 제19권 1호, 2009년, pp. 309~311.

[8] 임형진, 이정근, 김문성, "안전한 인터넷 뱅킹을 위한 트랜잭션 서명기법에 관한 연구," 한국 인터넷 정보학회 9권 6호, 2008년, pp. 73~79.

[9] M. Burrows, M. Abadi, R. Needham: A logic of authentication. ACM Transactions on Computer Systems, 8(1):18 - 36, February 1990.

■ 저자소개 ■

김 태 경
Kim, Tae Kyung

2008년 3월~현재 서울신학대학교 교양학부 교수
2006년 3월~2008년 2월 서일대학 정보기술계열 정보전자전공 교수
2005년 8월 성균관대학교 전기전자및컴퓨터공학과 (공학박사)
2001년 8월 성균관대학교 정보통신공학과 (공학석사)
1997년 2월 단국대학교 수학교육과 (이학사)

관심분야 : 네트워크보안, 그리드 네트워크, USN
E-mail : tkkim@stu.ac.kr

논문접수일 : 2010년 7월 30일
수 정 일 : 2010년 8월 20일
게재확정일 : 2010년 8월 26일