한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

LEAP 기반의 무선 센서 네트워크에서 싱크홀 공격을 탐지하기 위한 키 인증 기법

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

Key Authentication Method for Detecting Sinkhole Attacks of LEAP based Wireless Sensor Networks

Jae-jin Lee°, Tae-ho Cho*
°*College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

무선 센서 네트워크는 개방된 환경에 단거리 무선 통신으로 정보를 수집하는 센서 노드와 이를 수집하는 베이스 스테이션으로 운영된다. 이러한 센서 네트워크의 특징으로 인해 공격자를 통해 쉽게 훼손될 수 있으며 대표적인 공격방법으로 싱크홀 공격이 있다. LEAP은 싱크홀 공격에 대응하기 위해 네 종류의 키를 사용하여 노드 간 인증을 하도록 제안되었다. 이 기법은 보안성을 유지하기 위해 주기적으로 베이스 스테이션까지의 경로를 갱신한다. 본 논문에서는, 내부 싱크홀 공격을 LEAP과 같은 키의 인증을 통하여 탐지하는 기법을 제안한다. 제안 기법은 이전 노드, 다음 노드와의 키 인증을 통해 공격을 탐지한다. 공격이 탐지되면 해당 노드를 네트워크에서 제외하고 경로를 갱신하며 갱신된 경로를 통해 새로운 키를 배포한다. 그러므로 제안 기법은 이전 노드, 다음 노드와의 키 인증을 통해 싱크홀 공격을 탐지함으로써 전체 네트워크 보안성 향상을 목적으로 한다.

키워드: 무선 센서 네트워크(Wireless Sensor Networks), 네트워크 보안(Network Security), 로컬 암호화 인증 기법(LEAP), 싱크홀 공격(Sinkhole Attack), 탐지(Detection)

I. 서 론

무선 센서 네트워크(Wireless Sensor Network)는 단거리 무선통신이 가능한 다수의 센서 노드와 센서 노드를 통해 정보를 수집하는 베이스 스테이션으로 구성된다. 센서 노드는 무선 통신의 특성과 주로 개방된 환경에 제한적인 하드웨어 자원으로 운영되기 때문에 공격자에 의해 쉽게 네트워크를 훼손당할 수 있으며 최악에는 서비스 불능 상태가 될 수 있다[1]. 대표적인 공격 형태 중 하나로 싱크홀(Sinkhole) 공격이 있다[2]. 이 공격은 악의적인 노드가 자신을 베이스 스테이션이나 목적지에 더 가까이 있다고 허위 메시지를 광고하여 훼손된 노드로 많은 노드의 데이터 트래픽을 거치도록 만든다. 훼손된 노드로 보고서가 전달되면, 보고서를 파괴하거나 허위 보고서를 전달, 또는 네트워크의 트래픽을 조절하여 정상적인 데이터 전달을 방해한다. 또한, 추가적인 공격을 더욱 쉽게 수행할 수 있다. 이러한 공격에 대응하기 위해 2003년 S. Zhu 등에 의해 로컬 암호화 인증 기법(Localized Encryption and Authentication Protocol; 이하 LEAP)이 제안되었다[3]. LEAP은 센서 노드들이 가지고 있는 메시지 교환 방식에 따라 다른 보안 요구사항을 충족시키기 위해 단일 키 메커니즘 대신 각각의 센서 노드에 네 종류의 키를 사용한다. 이 프로토콜은 네 종류의 키를 통해 검증 후 탐지된 훼손 노드를 제외한다. 위와 같은 검증으로 LEAP은 외부공격에 대해 예방과 탐지를 할 수 있지만, 내부 공격에 대해서는 취약하여 효과적인 내부 공격에 대한 탐지가 필요하다. 본 논문에서는 내부 싱크홀 공격에 대한 훼손 여부를 경로 갱신 시 이전 노드와 다음 노드 간의 키 인증을 통해 공격을 탐지하는 기법을 제안한다. 2장에서는 관련 연구로 LEAP, 싱크홀 공격, 기존 싱크홀 탐지 기법 중 링크 품질 지표, 홉 카운트 기반 라우팅에 관해 설명한다. 3장에서는 제안기법을 기술하고, 4장에서는 이 논문의 결과와 추후 연구과제에 대해 간략히 기술한다.

II. 관련 연구

2. 관련연구

2.1 로컬 암호화 인증 기법

LEAP은 훼손된 노드로부터 전체 네트워크의 피해를 줄이기 위해 제안된 센서 네트워크의 키 관리 프로토콜(Key Management Protocol)이다. LEAP은 각각의 센서 노드에 다음과 같은 네 종류의 키를 사용한다. 한 노드와 베이스 스테이션 간 공유하는 키로, 네트워크에 배치되기 전 생성되는 Individual Key (I.K), 한 노드와 이웃노드

간 공유하는 키로, 메시지 암호화에 사용하는 Pairwise Key (P.K), 한 노드와 인접한 이웃 노드 간에 공유하는 키로 메시지 전파에 사용하는 Cluster Key (C.K), 네트워크에 있는 모든 노드와 베이스 스테이션 간 공유하는 키로 메시지 복호화에 사용하는 Group Key (G.K)로 구성되어있다. 그림 1은 센서 노드 u의 종류별 키 생성과정을 나타내며 그 절차는 다음과 같다.

그림 1. 키 생성 과정
Fig. 1. Key generation process

Step 1) 센서 노드 u는 배치되기 전 베이스 스테이션으로부터 G.K, K_u (Initial key), K^m(베이스 스테이션의 Master key)를 할당한다.
Step 2) 베이스 스테이션은 K^m과 랜덤함수를 통해 각 노드의 I.K를 생성한다.
Step 3) 센서 노드 u는 랜덤함수를 통해 이웃노드 v와 P.K를 생성한다.
Step 4) 센서 노드 u는 각각의 이웃 노드 vi의 P.K와 랜덤함수를 통해 C.K를 생성한다.

형성된 네트워크에서 LEAP은 주기적으로 갱신한 경로를 통해 새로운 G.K를 전달하여 보안성을 유지한다.

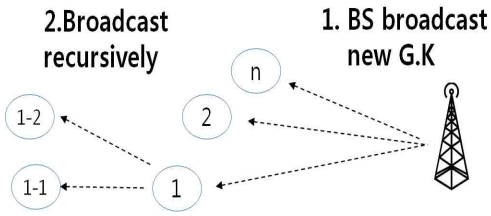

그림 2. 갱신 된 G.K의 배포과정
Fig. 2. Updated G.K broadcast process

그림 2와 같이 새로 갱신된 G.K는 베이스 스테이션으로부터 이웃 노드들에 전파되고 그 다음 노드로 재귀적으로 배포된다.

2.2 싱크홀 공격

싱크홀 공격은 베이스 스테이션으로 사칭 또는 목적지로 향하는 가장 효율적인 경로로 사칭하여 주위 노드들을 속여 트래픽을 훼손된 노드로 끌어들이는 공격이다. 하나의 싱크홀 노드가 존재하는 것만으로도 위치에 따라 네트워크에 큰 악영향을 미칠 수 있다. 또한, 차후 선택적 전달공격(Selective Forwarding Attack), 웜홀 공격 (Wormhole Attack)과 같은 공격을 가능하게 함으로써 더 큰 악영향을 미칠 수 있다.

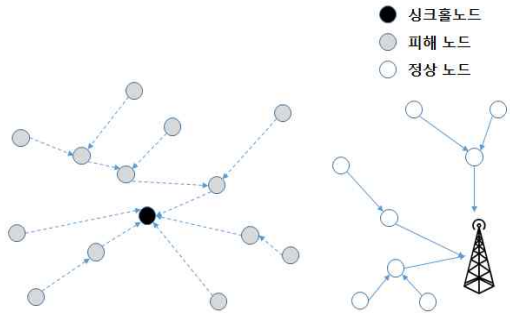

그림 3. 싱크홀 공격
Fig. 3. Siknhole Attack

그림 3은 싱크홀 공격이 발생한 경우의 네트워크 상태를 나타낸다. 주변 노드들의 데이터 트래픽이 싱크홀 노드로 거치기 때문에 다른 추가적인 공격을 수행할 경우 더욱 넓은 범위의 노드들이 공격에 노출되게 된다. 싱크홀 공격을 탐지하기 위해 제안된 기법으로는 다음과 같은 기법들이 있다.

2.2.1 링크 품질 지표

링크 품질 지표(Link Quality Indicator; 이하 LQI)는 수신된 패킷의 신호강도나 품질을 나타낸다. 링크 품질 지표는 수신기의 에너지, 신호 대 잡음 비 혹은 이들의 조합으로 계산이 가능하다[4]. 높은 LQI 값은 좋은 품질의 연결을 의미한다. 공격 탐지를 위해 다수의 일반 노드와 소수의 탐지 노드를 구분하여 배치해야 하는 단점이 있다.

2.2.2 홉 카운트 기반 라우팅

홉 카운트 기반 라우팅(Sinkhole attack detection for hop-count based routing)은 모든 센서 노드가 베이스 스테이션으로 주기적으로 데이터를 전송한다고 가정한다[5]. 선택적 전달공격은 싱크홀 공격이 이루어진 다음 자주 발생하는 공격이다. 이러한 공격의 경우, 훼손된 노드는 의도적으로 일부 패킷을 전달하지 않고 베이스 스테이션은 특정주기 동안 데이터를 전달받지 못한 노드의 목록을 만들어 다음 홉의 정보를 모아 훼손된 노드의 탐지가 가능하다. 하지만 이 기법은 싱크홀 공격을 통한 다른 추가적인 공격이 이루어지지 않으면 탐지할 수 없다는 단점이 있다.

III. 본 론

3.1 가정

본 논문에서는 TinyOS beaconing protocol과 유사한 라우팅 프로토콜을 사용한다고 가정한다[2],[6]. 훼손된 노드 발견 시 훼손 노드의 이웃 노드는 훼손된 노드와의 P.K를 삭제하고 이웃 노드 목록에서 삭제한다. 그 후 갱신된 이웃 노드 목록을 통하여 C.K와 경로를 갱신한다. 갱신된 경로를 통하여 새로운 G.K를 배포한다. 노드가 공격자에 의해 훼손되면 해당 노드가 가지고 있는 모든 정보는

공격자에게 노출되며 베이스 스테이션은 공격자에 의해 훼손되지 않는다고 가정한다. 공격자는 경로가 다시 설정되기 전에 1번의 공격만 성공하며 내부 싱크홀 공격만 시도 한다고 가정한다.

3.2 제안기법

본 논문에서, 제안 기법은 이전 노드와 다음 노드 간의 키 인증을 통해 내부 싱크홀 공격에 대한 훼손 여부를 검증하여 전체 네트워크의 보안성을 유지한다. 제안기법에서 센서 노드는 네 종류의 키(I.K, P.K, C.K, G.K)를 생성한다. 다음의 네 가지의 경우 훼손 여부와 함께 경로, C.K, G.K를 갱신하고 갱신된 경로를 통해 G.K를 배포한다. 1) 노드의 훼손이 탐지되었을 때, 2) 노드의 에너지 고갈로 인해 네트워크에서 제외되었을 때, 3) 새로운 노드가 추가되었을 때, 4) 기존에 정해진 주기가 되었을 때. 그림 4는 노드 B가 이전 노드 A와 다음 노드 C와의 인증과정을 나타내며 그 절차는 다음과 같다.

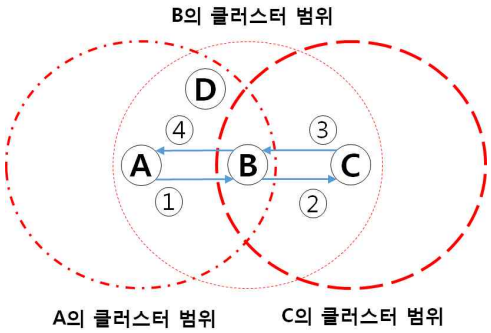

그림 4. 노드 A의 인증과정
Fig. 4. verify process with node A

① 노드 B의 다음 노드가 C로 요청이 들어왔을 때 노드 B는 이전 노드 A와 키 인증을 통해 노드 B의 훼손 여부를 검증한다.
② 노드 B가 훼손되었을 경우 기존의 노드 B의 정보는 모두 노출되었다고 가정하므로 노드 A와의 인증과정에서는 탐지되지 않을 가능성이 매우 높다. 노드 B는 다음 노드 C와의 인증을 시도한다.
③ 노드 B가 정상일 경우 노드 C와의 인증이 된 후 노드 C로부터 클러스터 범위 내에 있음을 확인받는다. 노드 C와의 인증이 실패할 경우 노드 C는 노드 B가 훼손된 노드임을 알 수 있다. 훼손된 노드 발견 시 훼손된 노드와의 P.K를 삭제하고 노드 A는 새로운 노드 D와 검증과정을 반복한다.
④ 노드 A는 노드 B로부터 노드 C와의 인증 여부를 통해 노드 B가 정상 노드임을 확인 후 경로를 갱신한다.

노드 B가 훼손 노드일 때 다음의 경우와 같이 행동할 수 있으며 각각의 경우에 대한 상황은 다음과 같다.

Case 1) 노드 B가 베이스 스테이션으로 사칭

노드 B는 노드 A와는 인증이 가능하지만, 노드 A의 이웃목록을 조작하는 것은 불가능하다. 그러므로 노드 A의 이웃목록에 베이스 스테이션이 없다면 노드 B가 훼손되었다고 판단된다.

Case 2) 노드 B가 노드 C가 베이스 스테이션이라고 사칭

노드 B는 노드 A와 인증이 가능하고 자신의 이웃목록을 조작하는 것 역시 가능하다. 하지만 베이스 스테이션과는 인증이 불가능하다. 베이스 스테이션으로 인증을 요청하여 공격을 탐지한다. 노드 B가 베이스 스테이션과 이웃 노드일 수도 있지만, 가정에 의해 베이스 스테이션은 훼손되지 않기 때문에 노드 B가 훼손되었다고 판단된다.

Case 3) 노드 B가 임의의 정상 노드 C로 전송

노드 B는 노드 A와 인증이 가능하다. 노드 B는 이웃 노드 목록을 조작하여 임의의 정상 노드 중 한 홉 내의 다른 노드로 라우팅 정보를 위조하는 Spoofing, Alteration 공격이 가능하지만, 노드 C의 경로까지 위조할 수는 없기에 라우팅 루프(Routing Loop)는 생성할 수 없으며 노드 C의 검증 과정에서 노드 B가 훼손되었음을 판단된다.

훼손 노드가 감지되면 해당 노드를 네트워크에서 제외하고 훼손 노드의 이웃 노드들로부터 훼손 노드의 P.K를 삭제한 다음 경로, C.K, G.K를 갱신한다. 제안 기법은 Case 1), Case 2), Case 3)에 대해 네 종류의 키를 사용하여 이전 노드, 다음 노드와의 인증을 통해 공격을 탐지한다. 훼손 노드가 탐지되면 훼손 노드의 이웃 노드들은 훼손 노드와의 P.K를 삭제하고 이웃 노드 목록에서 훼손 노드를 삭제한다. 훼손된 노드의 이웃 노드들만 훼손 노드를 제외하고 경로, C.K를 갱신하며, 갱신된 경로를 통해 새로운 G.K를 배포하여 보안성을 유지한다.

Ⅳ. 결 론

본 논문에서, 우리의 제안기법은 센서 네트워크에서 싱크홀 공격을 탐지하기 위한 키 인증 기법이다. 제안 기법은 이전 노드와의 인증, 다음 노드와의 인증을 통해 노드의 훼손 여부를 탐지한다. 훼손 노드의 이웃 노드들은 훼손 노드의 P.K를 삭제하고 이웃 노드 목록에서 훼손 노드를 삭제한다. 갱신된 이웃 노드 목록을 통하여 C.K와 경로를 갱신한다. 베이스 스테이션은 갱신된 경로를 통하여 새로운 G.K를 재귀적으로 배포한다. 향후 연구 과제로는 동시에 다수의 공격이 들어왔을 때 탐지하는 기법, 다수의 서로 다른 공격을 탐지하는 기법에 대해 연구할 것이다.

Acknowledgement

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

참고문헌

[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] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, In First IEEE International Workshop on Sensor Network Protocols and Applications, pp 113-127, May 2003.

[3] 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.

[4] IEEE Computer Society, “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, IEEE 802.15.4 Standard, pp.1-320, Sept. 2006.

[5] Ngai, E.C.-H. Jiangchuan Liu, Lyu, M.R. "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", ICC 2006, Proceedings of the IEEE International Conference on Communications, Istanbul, Turkey, vol. 8, pp. 3383-3389 ,June. 2006.

[6] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. “System architecture directions for networked sensors”. ASPLOS IX Proceedings of the ninth international conference on Architectural support for programming languages and operating systems, pp. 93-104, Dec, 2000.