무선 센서 네트워크 환경에서 안전한 통신을 위한 그룹 해싱 기법

이희만*, 강정호*, 김정호**, 전문석*
*숭실대학교 컴퓨터공학과
**숭실대학교 정보보안학과
e-mail:heeman930@ssu.ac.kr
kjh7548@naver.com
kimpocjstk@ssu.ac.kr
mjun@ssu.ac.kr

Group hashing for Secure Communications in Wireless Sensor Network

Hee-man Lee*, Jung-Ho Kang*, Jung-ho Kim**, Moon-Seog Jun*
*Dept of Computer Science, Soong-sil University
**Dept of Information security, Soong-sil University

요 약

무선 센서 네트워크에서 무선 전송 매체를 통한 통신으로 유선 네트워크에 비해 보안이 매우 취약하며 Sensor Node는 매우 제한된 통신, 계산 능력으로 기존에 다양한 암호화 방식 적용이 어렵기 때문에 데이터의 eavesdropping와 capture가 발생할 수 있다. 본 논문은 이러한 환경에서 지역적으로 같은 보안방식을 사용하여 한 지역 패킷이 노출되면 그룹 전체에 노출로 이어지는 취약점을 방지하기 위해서 BaseStation은 각 그룹의 ClusterHeader가 사용할 서로 다른 해시 알고리즘을 주기적으로 갱신하여 악의적인 사용자의 노드 eavesdropping 및 capture를 방지하고 안전한 통신을 수행하고자 한다. 제안된 기법은 기존 논문들의 비해 프로토콜의 효율성과 안전성을 보였다.

1. 서론

무선 센서 네트워크(Wireless Sensor Network)에서는 일정한 목적으로 데이터를 수집, 응용하는 기술로 온도와 습도, 화재방지등 다양한 곳에서 사용이 되고 있다. 이러한 센싱에 필요한 장치들은 지속적인 전원 공급 장치가 없을 뿐만 아니라 적은 메모리, 계산능력, 제한된 통신으로 다양한 암호화방식 적용이 제한되기 때문에 보안이 취약하다. 공격자는 Sensor Node간 트래픽을 쉽게 엿볼 수 있고, 주변 노드에게 잘못된 정보를 제공함으로써 Sensor Node의 흉내를 낼 수 있다. 또한 센서 네트워크에서 BaseStation의 하위 레벨에서 동일한 암호화 방식을 사용하기 때문에 하나의 Sensor Node감염 및 패킷 노출은 네트워크 전체의 노출로 이어질 수 있다. 이러한 문제는 Sensor Node 및 ClusterHeader의 안정적인 통신을 위하여 보안 취약점을 해결해야 한다.

본 논문에서는 센서 네트워크 환경을 서로 다른 그룹으로 지정하고 그룹마다 주기적인 해시 알고리즘 갱신을 통해 지속적인 eavesdropping와 capture을 통해 악의적인 사용자의 데이터 위협을 방지한다. 2장에서는 기존에 제안된 방법들에 대해 알아본 후 3장에서 이 논문에서 제안하는 방법에 대해 자세히 기술한다. 4장에서는 안전성분석을 하고, 5장에서는 결론을 제시한다.

2. 관련 연구

이 장에서는 무선 센서 네트워크 환경에서 취약점을 보완한 논문 및 최신 기술 동향을 살펴본다.

2-1 IDE 기반 방식

IDE 기반 방식은 기존 AM-E[1] 방식에서 노드와 BaseStation 간에 통신에서 데이터 노출 위험을 보완하고자 센서 네트워크 구조를 계층 구조로 분할하고 통신 전 IDE기반 방식[2]으로 인증 후 안전한 통신을 제안하고 있다. 하지만 무선 센서 네트워크에서 IDE기반의 신원 기반 암호시스템은 Sensor Node 하드웨어상 암호 시스템을 구축할 수 없을 뿐만 아니라 구축을 하더라도 악의적인 사용자가 노출된 평문에 접근 할 수 있기 때문에 취약하다.

2-2 이중 해쉬 체인 방식

이중 해쉬 체인 기반의 방식[3]은 랜덤 키 사전분배 기술과 이중 해쉬 체인을 조합한 키 사전 분배 기법으로 각 세션을 분할 한 후 키 풀과 ID생성 그리고 랜덤하게 풀(pool)에서 추출한 데이터를 이중 해쉬 체인 L을 사용하여 클러스터의 Key값으로 암호화 한 후에 전송하는 프로토

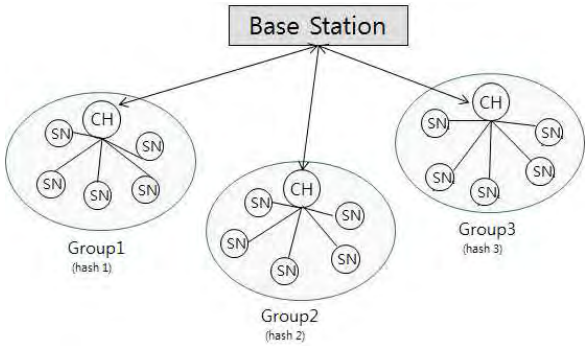
콜이다. 하지만 이중 해쉬 체인 방식을 사용할 경우 무리한 해싱 체인 연산을 하고 제안과 같을 시에 추가로 해싱 값과 비교할 수 있는 데이터를 보내야 하기 때문에 Sensor Node의 전송 패킷이 늘어나게 되고 결국 에너지의 비효율성을 초래 할 수 있다. 또한 Sensor Node와 ClusterHeader는 같은 해쉬 함수를 사용하기 때문에 노드 및 헤더에 대한 감염은 모든 센서네트워크의 노출이 되기 때문에 취약하다.

2-3 최신 기술 동향

현재 다양한 센서 네트워크에 적용되는 네트워크 프로토콜은 표준화된 인터페이스 없이 다양한 기술이 적용이 되고 있으며, 실제적으로 PKI같은 기술 적용이 힘들다. 이에 대해 경량화된 대칭 알고리즘이나 ECC와 같은 모듈 개발에 집중이 되고 있다.

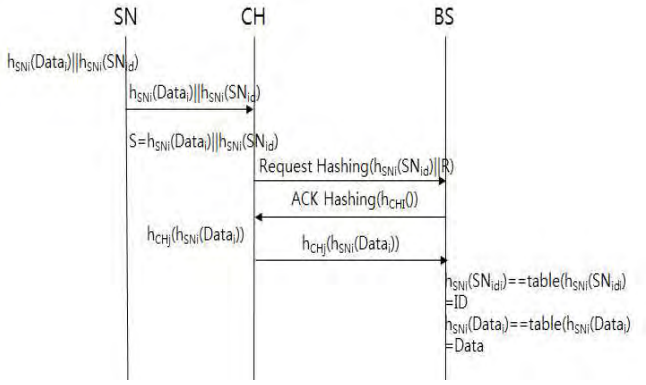
3. 제안

제안하는 구조는 [그림-1]과 같이 하나의 BaseStation과 하위 레벨의 같은 목적은 가진 그룹이 존재한다. 그룹의 장으로 ClusterHeader가 있고 그 하위 레벨로 Sensor Node가 존재한다. 각 그룹은 서로 다른 해시 알고리즘을 사용하고 있으며 일정 기간후에 BaseStation은 각 클러스터에게 갱신된 해시 알고리즘을 전송한다.



[그림-1] 제안 구조

각 Sensor Node는 [그림-2]와 같이 해시 알고리즘을 사용하여 Data와 ID를 해시(1)하고 ClusterHeader에게 보낸다.



[그림-2] 제안 프로토콜

수신한 ClusterHeader는 받은 패킷의 일부를 가지고 Basestation에게 해시 알고리즘을 요청(2)하고 보낸 데이터의 인증 후 해당 해시 알고리즘을 수신(3)한다. 이후 받은 해시를 통해 센싱된 데이터를 해시하여 BaseStation에게 보내면 수신측은 저장된 해시 데이터 테이블을 통해 센서 노드의 ID(4)와 센싱 데이터를 추출(5)한다.

$$
\begin{aligned}
&(1)\, h_{\ N}(\ \ ata_i)||h_{SNi}(SN_{id})\\
&(2)\, RequestHashing(h_{SNi}(SN_{id})||R)\\
&(3)\, h_{CHJ}(h_{SNi}(Data_i))\\
&(4) h_{SNi}(SN_{id}) \equiv table(h_{SNi}(SN_{id}i) = ID\\
&(5) h_{SNi}(Data_i) \equiv table(h_{SNi}(Data_i) = Data
\end{aligned}
$$

4. 제안 프로토콜 안전성 분석

제안 모델은 각 노드들의 그룹에 기반하여 서로 다른 hash function를 사용해서 안전하게 제안 했다.

4-1 도청공격(Eavesdropping Attack)

도청 공격은 데이터 송·수신간에 주고받는 내용을 도청하여 정보를 알아내는 공격이다. 기존의 논문[2]은 패킷이 암호화 되지 않고 노출이 될 뿐만 아니라 그룹 전체가 같은 보안방식을 사용하기 때문에 감염된 노드의 악의적인 행동을 막을 수 없다. 본 논문에서는 Sensor Node 및 ClusterHeader는 그룹에 기반한 해시 알고리즘을 사용하고 BaseStation이 hash된 데이터 테이블을 가지고 판별하기 때문에 악의적인 사용자가 패킷을 주고 받을 때 도청하더라도 해석할 수 없을 뿐 아니라 감염된 Sensor Node 및 ClusterHeader도 해석이 불가능 하다.

4-2 캡처 공격(capture attack)

캡처 공격은 도청공격에 기반하여 계속적인 데이터 수집후에 추론하여 공격하는 기법이다. 기존의 논문[3]에서는 불필요한 해시를 사용할 뿐만 아니라 해시 체인을 상용하여 하나의 노출이 전체의 노출로 이어질 수 있다. 하지만 본 논문에서는 각 그룹마다, 장치마다의 해시알고리즘이 다르고 일정 기간에 따라 해시알고리즘이 변경되기 때문에 데이터를 capture하여 공격하더라도 BaseStation에서 패킷은 폐기 된다.

5. 결 론

본 논문은 안전한 통신을 위해 그룹 기반으로 서로 다른 해시 알고리즘을 주기적으로 갱신하고 또한 그룹안에서 계층별로 다른 해시를 사용하기 때문에 계속적인 Eavesdropping Attack과 capture attack공격에 안전하다.

참고문헌

[1] T.T Huyen, Eui-Nam huh, "A reliable 2-mode authentication framework for Ubiquitous sensor network", *Journal of Korean Society for Internet Information, 2008*

[2] Young-bok Cho, Sang-ho Lee "An IDE based Hierarchical Node Authentication Protocol for Secure Data Transmission in WSN Environment", KICS2011-10-458 '12-03 Vol.37B No.03

[3] Yoon-su Jeong, Yong-Tae Kim, Gil0Cheol Park, Sang-Ho Lee "A Key Pre-distribution Scheme Using Double Hash Chain for Strong Security Strength of Wireless Sensor Node", KICS2007-12-545, '08-08 Vol. 33 No. 8