ISSN:1226-7244 (Print)
ISSN:2288-243X (Online)
j.inst.Korean.electr.electron.eng.Vol.21,No.4,348~352,December 2017
논문번호 17-04-03
http://dx.doi.org/10.7471/ikeee.2017.21.4.348
18

해쉬 함수 기반의 무선 센서 네트워크 인증에 관한 연구

A Study on Authentication of Wireless Sensor Networks based on Hash Function

배성현*, 문영준**, 김해문***★

Sung-Hyun Bae*, Young-Joon Moon**, Hae-Mun Kim***★

Abstract

A lot of researches have done for WSN(Wireless Sensor Networks) authentication. Those are divided by whether using certificates or not for the authentication. In this paper, we proposed certificateless protocol.

As simplifying the process of authentication, overall the process become faster and the load of the sensor node is decreased. Using the method we proposed, the energy consumption is decreased. That is because instead using keyed hash authentication code(HMAC) simple one way hash function was used. The study confirmed that it could operate on sensor nodes with extremely limited resources and low processing power.

요 약

WSN(Wireless Sensor Network)에 대한 인증은 많은 연구가 이루어지고 있다. 인증하는 방법에는 인증서를 사용하는지 여부에 따라 구분할 수 있다. 본 논문에서는 인증서를 사용하지 않는 프로토콜을 제안한다. 인증의 처리과정을 단순화하여 처리속도가 전반적으로 빨라지고, 센서 노드의 부하를 줄일 수 있다. 또한 HMAC(Keyed Hash Authentication Code)을 사용하는 대신에 단순 해쉬 함수를 사용하기 때문에 에너지 소비도 감소될 수 있다. 이 연구는 극히 한정된 자원과 낮은 처리 능력을 가진 센서 노드상에서도 작동할 수 있음을 확인했다.

Key words : WSN(Wireless Sensor Networks), Authentication, Hash Function, Identity, Session Key

* Dept. of Aviations Information & Communication KyungWoon University.
** Dept. of Electronics Engineering, Kyungpook National University
*** Dept. of Materials & Energy Engineering, KyungWoon University.
★ Corresponding author
E-mail: seadoor@nate.com, Tel: +82-54-479-1158
Manuscript received Dec, 5, 2017; revised, Dec, 20, 2017 ; accepted, Dec, 22, 2017

Ⅰ. 서론

무선 인터넷의 발전으로 사물 인터넷이라는 개념이 도입되고, 그 도입을 위해서 선행된 WSN (무선 센서 네트워크)의 연구가 필요로 하게 되었다 [1]. WSN(Wireless Sensor Network)은 센서가 설치되는 환경에서 수집한 데이터의 통신과 처리를 가능하게 하는 작고 자율적인 장치로 구성된다 [2]. 낮은 비용으로 망의 구성을 빠르게 할 수 있다는 장점으로 모니터링, 건물 보호, 오염 탐지등 다양한 분야에 사용된다.

WSN은 IoT(Internet of Things)를 구성하는 핵심 기술로써 많은 연구가 진행되어 왔다. 그 가운데 있어서 접근제어(Access Control)를 잘 지킬 수 있는 기본 솔루션으로써의 인증(Authentication)은 핵심을 차지하고 있다고 할 수 있다 [3].

최근 이러한 인증에 관한 연구는 2가지로 나눌 수 있다. 인증서를 가지고 하는 연구와 인증서를 사용하지 않는 연구이다 [4-5]. 인증서를 기반으로 하는 경우에는 제3의 중재자(인증기관)가 필요하며 인증기관은 다량의 처리기능 및 많은 메모리를 필요로 한다. 또한 인증서 처리는 한정된 에너지 소스를 가지고 있는 센서에게는 부담이 된다. 반면 인증서를 사용하지 않는 프로토콜의 경우에는 인증기관이 없으므로 망의 구성이 편리하며 센서의 부담을 줄여줄 수 있다.

본 연구에서는 Hamza Khemissa et al.[5]이 제안한 인증서를 사용하지 않는 프로토콜에서 게이트웨이 노드의 불필요성에 대해 분석하고, 연산량과 센서의 부담을 줄이면서 센서 노드의 전반적인 속도를 향상할 수 있는 경량화된 인증 프로토콜을 제안 및 분석하였다.

II. 본론

1. 관련 연구

가. WSN 인증 방법

무선으로 정보를 주고 받는 것을 뜻하는 WSN는 정보를 무선으로 전송함으로써 도/감청에 취약하다 [6]. 따라서 인증과 데이터의 무결성등 보안 문제가 크게 대두되었다. 그 중에서 인증을 해결할 수 있는 방법 가운데 인증서를 필요로 하는 방법과는 다른 인증서를 필요로 하지 않는 기법을 사용할 수 있다면 무거운 인증서를 다루는 것보다는 좀 더 경량화에 도달할 수 있다는 생각에 Hamza Khemissa et al.[5]는 인증서가 필요 없는 프로토콜을 제안하였다. 이들은 HMAC과 XOR을 사용하여 인증을 처리함으로써 경량화 하였다 [6].

나. 기존 연구 분석

Xue et al.[7]은 WSN의 5가지의 기본 모델을 제시하였는데, 4가지는 사용자가 센서에 접근하기 전에 게이트웨이 노드를 반드시 경유하게 되어 있으며 나머지 1가지는 원격 사용자가 바로 센서에 접근 가능하게 되어 있다. Hamza Khemissa et al.[5]이 사용한 방법은 원격 사용자가 센서에 접근하는 방법의 변형인 센서쪽에서 먼저 접속을 요청한다. 변형된 네트워크 구조는 그림 1과 같이 나타낼 수 있다.

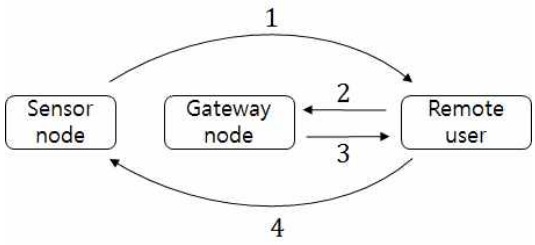

Fig 1. Network architecture.
그림 1. 네트워크 구조

다. 사용된 표기법

본 연구에 사용된 표기법은 표 1과 같다.

Table 1. Used notation.
표 1. 사용된 표기법

Notation	Description
$\|$	Concatenation
$\oplus$	Exclusive-or operation (XOR)
N	Nonce value of the sensor node
M	First nonce value of the remote user
W	Second nonce value of the remote user
h()	A one way hash function
$E_K()$	AES-128 encryption using session key K

라. Hamza Khemissa et al.[5]의 프로토콜 분석

(1) 등록단계

그림 2에서와 같이 센서 노드는 먼저 게이트웨이 노드에 등록된 다음 원격 사용자에 등록된다. 게이트웨이 노드는 센서 노드의 비밀키와 원격 사용자의 공개키를 알고 있으며, 센서 노드와 게이트웨이 노드 사이에는 안전한 채널이라고 가정한다.

센서는 안전한 채널을 통해 센서 노드의 Id_i와 지원되는 cipher suite의 목록을 게이트웨이 노드로 전송한다. 게이트웨이 노드는 사용될 cipher suite를 선택하고 Id_i와 센서의 비밀키 X_i를 이용해서 마스크된 아이디 $MSId_i$를 계산한다.

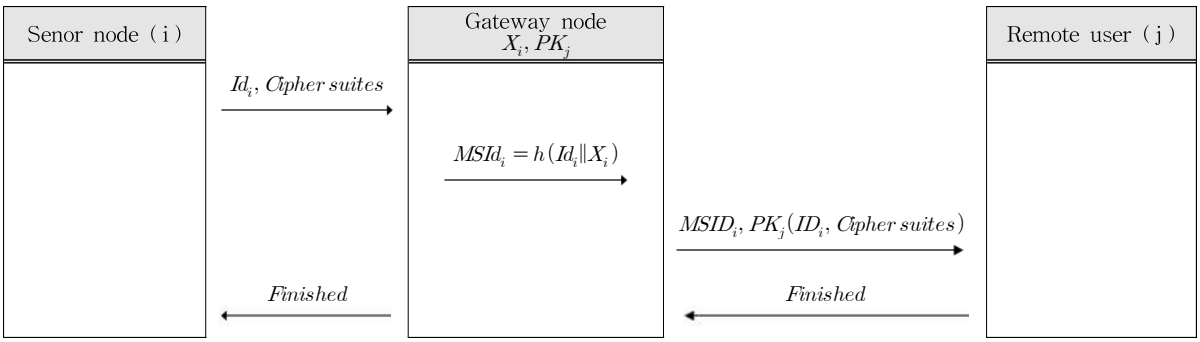

Fig 2. Registration phase.
그림 2. 등록 단계

원격 사용자의 공개키로 Id_i와 cipher suite를 암호화해 $MSId_i, PK_j(Id_i, ciphersuite)$를 원격 사용자에게 전송한다. 원격 사용자는 개인키로 복호 후 cipher suite에 포함된 센서 노드의 비밀키로 Finished 메시지를 암호화해서 전송한다. 마지막으로 게이트웨이 노드가 센서 노드로 Finished 메시지를 보내는 것으로 등록 단계는 마무리된다.

(2) 인증단계

그림 1과 같은 단계를 통해 인증 및 키 설정을 한다. 자세한 프로토콜 실행 단계는 생략하고, 보안적인 부분만 언급한다. 그림 1에서 보안적인 취약점이 존재하는 단계는 게이트 노드와 원격 사용자 간의 메시지 전달과정이다. 그림 1에서와 같이 2번에서 전송하는 메시지는 $MSId_i, N, M, HMAC(MSId_i, N, M)$이고, 3번에서 전송하는 메시지는 $N, M, T, HMAC(M, Id_i, S)$이다. 여기서 게이트 노드는 단순히 nonce S를 생성할 뿐 다른 역할을 하지는 않는다. 3번에서 N, T가 노출됨으로써 공격자는 $S = N \oplus T$를 통해 S를 계산할 수 있다. HMAC의 인자인 N은 1, 2, 3번에서 T는 3번에서 전송되는 메시지의 도청이 가능하므로 마찬가지로 S를 계산할 수 있다.

만약에 $MSId_i$를 생성하는데 사용되는 X_i값을 알게 된다면 이 값으로 충분히 HMAC값을 알 수 있으므로 3번으로 전송하는 메시지 $N, M, T, HMAC(M, Id_i, S)$은 HMAC값과 함께 변조가 가능하다. 게이트웨이 노드로 전송되는 N, M도 노출되어 있기 때문에 같은 조건 과정을 통해서 변조가 가능하다.

따라서 다음 절에서는 불필요한 게이트웨이 노드의 참여를 제한하여도 안전하며, 인증서를 사용하지 않은 프로토콜로서 경량화한 단순 해쉬 기반의 프로토콜을 제안한다.

2. 제안하는 인증 프로토콜

가. 등록 단계

Hamza Khemissa et al.[5]의 등록 단계와 동일하게 그림 2와 같이 2단계의 전송 단계를 통해서 센서 노드와 게이트웨이 노드사이, 게이트웨이 노드와 원격 사용자 사이로 나누어 메시지를 전송함으로써 등록이 이루어진다.

나. 인증 단계

제안하는 인증 단계의 프로토콜은 그림 3과 같다. Hamza Khemissa et al.[5]의 인증 프로토콜과 비교했을 때 가장 두드러진 변화는 인증에 있어서 S(Sensor node)→R(Remote user)→G(Gateway node)의 3단계 통신 흐름에서 R→G와 G→R의 통신 메시지가 생략되고 오직 S↔R 사이의 통신만으로 인증 및 키 설정이 이루어 진다. 각 단계의 진행 과정은 다음과 같다.

(a) 센서 노드는 Random nonce N 생성, $MSId_i, N, h(MSIdi, N, X_i)$를 원격 사용자에게 전송한다. 원격 사용자는 $h(MSIdi, N, X_i)$를 검증하고, 일치한다면 Random nonce M과 세션키 $K = h(X_i, N, M)$을 생성함과 동시에 센서 노드를 인증하게 된다.

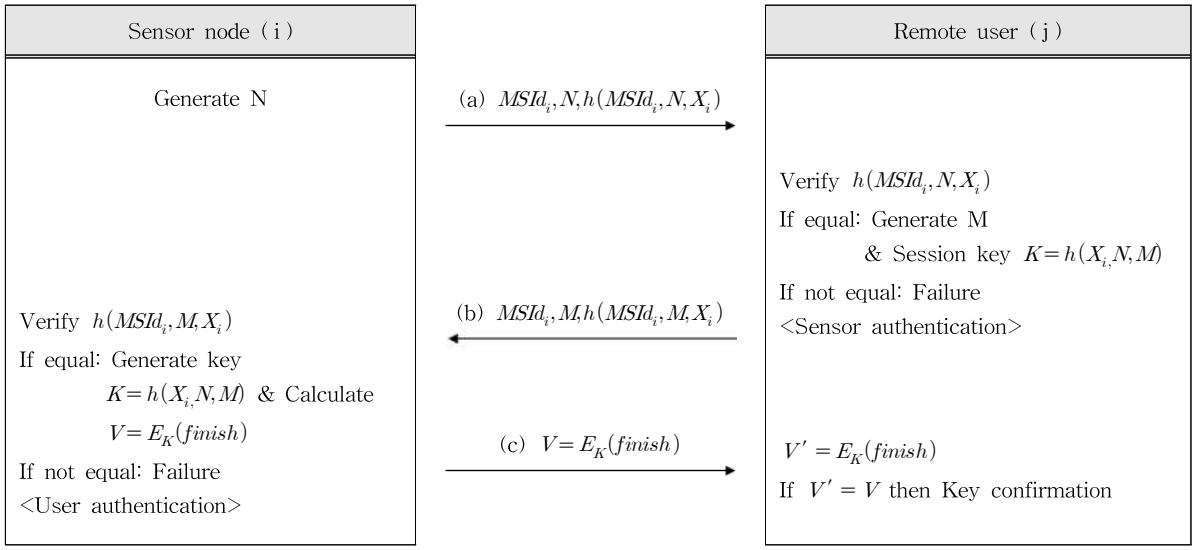

Fig 3. Proposed authentication phase.
그림 3. 제안한 인증 단계

(b) 원격 사용자는 $MSId_i, M, h(MSId_i, M, X_i)$를 센서 노드로 전송한다. 센서 노드는 해쉬값 $h(MSId_i, M, X_i)$를 검증하고, 일치한다면 원격 사용자를 인증함과 동시에 같은 세션키 K를 생성하고 finish 메시지를 세션키 K로 암호화한 후 원격 사용자에게 전송한다.

(c) 원격 사용자는 $V' = E_K(finish)$를 생성해서 $V' = V$임을 확인함으로써 상호 인증과 키 설정 단계를 마친다.

그림 3과 같이 인증 단계에서 게이트웨이 노드의 참여가 없으며, HMAC을 사용하지 않고 단순 해쉬 함수를 사용함으로써 연산량이 감소되어 경량화된 프로토콜을 제안하였다. 다음 절에서는 제안하는 프로토콜의 보안적인 측면에서 분석하였다.

3. 제안하는 프로토콜의 보안 분석

가. 센서 노드로 가장한 재생공격

공격자가 센서 노드와 원격 사용자로 가장하여 재생 공격을 시도해도 매번 새로운 Random nonce를 생성하며, 센서 노드의 아이디에 비밀키를 합쳐서(concatenate)해쉬한 $h(Id_i \| X_i)$값으로 $MSId_i$를 사용하기 때문에 공격에 안전하다.

나. 상호인증

센서 노드와 원격 사용자에 의해 각각 생성된 랜덤 nonce와 센서 노드의 비밀키 X_i만을 사용해서 서로 인증함으로써 상호 인증이 된다.

다. Identity Protection

각각의 노드에서는 마스크된 $MSId_i$만을 사용하며, Id_i값은 등록단계에서 원격 노드와 게이트웨이 노드에 입력되기 때문에 센서 노드 Id_i의 노출을 피할 수 있다.

라. 데이터 무결성

인증의 각 단계에서 해쉬 함수를 각각 사용하기 때문에 무결성이 보장된다.

마. 세션키 설정

(a) 단계에서 원격 사용자는 해쉬값이 검증되면 세션키 K를 생성하고, (b) 단계에서 센서 노드는 마찬가지로 해쉬값이 검증되면 세션키 K가 생성된다. (c) 단계에서 $V = E_K(finish)$을 전송하여 원격 사용자와 센서 노드 사이에서 생성된 세션키 K를 검증함으로써 세션키가 설정된다.

III 결론

본 연구에서는 인증서와 인증서를 사용하지 않는 프로토콜 중에서 저전력과 저성능의 센서 노드를 고려해서 인증서를 사용하지 않는 인증 프로토콜을 제안하였다. 인증서를 사용하는 프로토콜은 인증서를 주고 받는 과정에서 센서 노드에 많은 부하가 가중된다. 따라서 인증서를 필요로 하지 않는 기존의 프로토콜을 수정/보완하여 인증 단계를 원격 사용자와 센서 노드간의 통신으로 단순화하였다. 프로토콜의 단순화로 인해 센서 노드의 송신 및 수신량을 감소함으로써 센서 노드의 전력 소비량을 낮추는게 가능하다. 기존 프로토콜 기법에서 사용된 HMAC 대신에 단순 해쉬 함수를 사용함으로써 센서 노드의 연산 처리량을 줄였으며, 보안적인 분석 부분을 통하여서도 안전함을 확인하였다. 추후 연구를 통하여 보다 경량화된 프로토콜을 찾는 것이 가능할 것으로 사료된다.

References

[1] J. Yick, B. Mukherjee and D. Ghosal, “Wireless sensor network survey,” *Computer Networks*, vol.52, pp. 2292-2330, 2008.
DOI:10.1016/j.comnet.2008.04.002

[2] S. Agemura, K. Katayama and H. Ohsaki, "On the effect of Wireless Communication Range Heterogeneity on WSN Performance," *International Conference on Information Networking (ICOIN)*, pp. 35-40, 2017.
DOI: 10.1109/ICOIN.2017.7899449

[3] *B. Schneier, Applied crypography*, John Wiley & Sons Inc., New York edition, 1996.

[4] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov and M. Ylianttila, “Two - phase authentication protocol for wireless sensor networks in distributed IoT applications,” *in Wireless Communications and Networking Conference (WCNC)*, pp. 2728 - 2733, Apr. 2014.
DOI: 10.1109/WCNC.2014.6952860

[5] H. Khemissa and D. Tandjaoui, "A Novel Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things," *2016 Wireless Telecommunications Symposium (WTS)*, London, pp. 1-6, 2016.

[6] A. D. Wood and J. Stankovic “Denial of service in sensor networks,” *Computer*, vol.35, no.10, pp. 54-62, 2002.
DOI: 10.1109/MC.2002.1039518

[7] K. Xue, C. Ma, P. Hong and R. Ding “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” *Journal of Network and Computer Applications*, vol.36, pp. 316 - 323, 2012.
DOI:10.1016/j.jnca.2012.05.010

BIOGRAPHY

Sung-Hyung Bae(Member)

2000 : BS degree in Electronics Engineering, Kyungpook National University.
2003 : MS degree in Electronics Engineering, Kyungpook National University.
2017~Present : Assistant Professor, Kyungwoon University

Young-Joon Moon(Member)

1997 : BS degree in Electrical and Computer Engineering, The Ohio State University.
2017 : MS degree in Electronics Engineering, Kyungpook National University.
2017~Present : PhD course in Electronics Engineering, Kyungpook National University.

Hae-Mun Kim(Member)

2002 : BS degree in Electronics Engineering, Kyungpook National University.
2004 : MS degree in Electronics Engineering, Kyungpook National University.
2013~Present : Assistant Professor, Kyungwoon University