MKR: 센싱 정보에 기반한 비트 스트림 암호화 방식의 센서 네트워크 보안 프로토콜*

문형철*, 박선호*, 한영주*, 정태명**
*성균관대학교 컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail : hcmoon@skku.edu*, {shpark,yjhan}@imtl.skku.ac.kr*
, and tmchung@ece.skku.ac.kr**

MKR: Bit-stream Cipher Protocol using Sensing Data in Wireless Sensor Networks*

Hyung-Chul Moon*, Sun-Ho Park*, Young-Ju Han*, Tai-Myoung Chung**
*Dept. of Computer Engineering, SungKyunKwan University
**School of Information & Communication Engineering, SungKyunKwan University

요 약

최근 몇 년 동안 센서 네트워크에 보안을 제공하기 위한 여러 연구가 진행되었고 그 결과물로 몇 가지의 보안 프로토콜이 제시되었다. 그러나 지금까지 제시된 보안 프로토콜들은 많은 시스템 자원과 부가적인 통신 횟수들을 필요로 하는 기존의 암호화 방식을 그대로 사용하고 있어 실제 센서 네트워크에 적용하여 사용하기에는 힘들다. 이의 해결 방안으로 본 논문에서는 새로운 암호화 방식을 사용하는 센싱 정보에 기반한 보안 프로토콜 모델인 MKR 프로토콜을 제시한다.

1. 서론

센서 네트워크는 센싱 기능을 갖는 초소형 디바이스인 센서(sensor)를 일반사물에 장착하고 무선 송수신 기능을 탑재하여 서로간에 무선 네트워크로 센싱 정보를 주고 받아 호스트나 인터넷상으로 정보를 전송하여 원격지 상에서 전체상황을 확인하고 제어하는 시스템으로 전원 공급 능력, 프로세싱 능력, 메모리 공간, 전송 대역폭, 그리고 전송 거리 등과 같은 사항들로 인해 제약을 받는다[1].

그러나 센서 네트워크의 주된 응용은 군사목적과 병원에서의 환자 상태 모니터링 등으로 대부분이 센싱 데이터의 기밀성과 무결성을 필요로 하는 곳이다. 그로 인해 위와 같은 제약사항에도 불구하고 보안 요구사항의 충족을 위해 보안 프로토콜을 사용해야 한다[2].

센서 네트워크의 보안 요구사항을 구현하는데 있어 가장 큰 제약사항은 전원 공급 능력과 프로세싱 능력이다. 실제 센서 전원의 80%가 무선 송수신에 의해 소비되는데 보안 프로토콜을 사용하게 되면 부가적인 전송이 일어난다[3]. 이를 위해 센서 네트워크만을 위한 몇 가지 보안 프로토콜들이 제안되어 왔으나 자원 제약 문제를 해결하진 못하고 있다. 이의 해결 방안으로 본 논문에서는 새로운 암호화 방식을 사용하는 센싱 정보에 기반한 보안 프로토콜 모델인 MKR(Message-based Key Relay) 프로토콜을 제시한다.

2 장에서는 기존의 센서 네트워크 보안 프로토콜에 대해 알아본 후 3 장에서는 본 논문에 의해 제안되는 MKR 의 구조와 동작에 대해 알아본다. 4 장에서 MKR 의 성능 분석과 함께 5 장에서는 개선사항 및 향후 과제에 대해 논하고 끝으로 6 장에서 결론을 맺는다.

2. 기존의 센서 네트워크 보안 프로토콜

기존에 센서 네트워크를 위해 제안된 보안 프로토콜은 크게 마스터 키에 기반한 방식과 공개키에 기반

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.

한 방식이 있다. 마스터 키에 기반한 방식은 마스터 키를 이용해 세션키를 공유하여 메시지를 주고 받는다. 대표적인 프로토콜로는 SPINS 와 C&R(Challenge and Response) 등이 있다. 공개키에 기반한 방식은 서로의 공개키를 이용해 세션키를 공유하고 이를 통해 메시지를 주고 받는다. 대표적인 프로토콜로는 EG(Eschenhaur-Gligor) 등이 있다.

마스터 키 방식의 장점은 공개키 방식에 비해 수행 속도가 빠르고 키 길이도 더 짧다. 공개키 방식은 사용자 인증이 가능하고 전체 키의 노출 위험이 없다.

그러나 두 방식 모두 기존의 암호화 방식들로 알고리즘 수행을 위해 많은 시스템 자원을 소비하게 되고 부가적인 통신도 필요로 한다. 그로 인해 센서 네트워크에서 구현할 경우 센서가 가진 자원의 대부분을 소비하게 된다[4].

이의 해결 방안으로 본 논문에서는 메시지 기반 암호화 기법을 이용한 보안 프로토콜 모델인 MKR 프로토콜을 제시한다.

메시지에 기반한 암호화 기법은 평문 메시지를 이용해 스트림 단위마다 랜덤하게 생성된 키로 암호화하는 기법으로 본 논문의 프로토콜을 위하여 고안한 처음으로 소개되는 새로운 암호화 기법이다.

이를 이용한 프로토콜은 센싱 데이터인 스트림 단위의 메시지를 이용해 랜덤한 키를 만들어 암호화를 한다. 그로 인해 간단한 구조의 암호화 알고리즘을 사용하더라도 전체 프로토콜에서는 충분한 암호 강도가 보장된다. 간단한 구조의 알고리즘 사용으로 프로세서 점유시간이 작고 부가적인 통신도 없어서 센서 네트워크에 적용 시 자원의 소모가 작다.

3. MKR 프로토콜

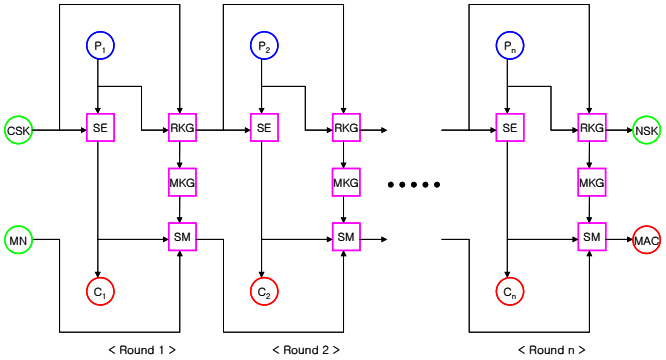
본 논문에서 제시하는 프로토콜은 베이스 스테이션(base station)과 센서 또는 센서와 센서 사이에 각각 하나의 세션이 만들어져 통신하는 것으로 가정한다. 그러나 실제 센서 네트워크에 적용하기 위해 구현하는 단계에서는 기존의 센서 네트워크 라우팅 프로토콜들과 결합시킨 형태가 되고 키의 길이도 64 비트 이상으로 확장된다.

본 논문에서는 프로토콜을 설명하기 위해 다음과 같은 표기법들을 사용한다.

$A \otimes B$: A 와 B 의 Exclusive OR 연산
$A = B$: B 의 값을 A 에 대입
$A \leftrightarrow B$: A 와 B 의 값을 교환
$P_r[m]$: r 번째 라운드의 평문 스트림에서 m 번째 비트
$C_r[m]$: r 번째 라운드의 암호문 스트림에서 m 번째 비트
$MAC_r[m]$: r 번째 라운드의 MAC에서 m 번째 비트
$MK_r[m]$: r 번째 라운드의 MAC키에서 m 번째 비트
$RK_r[m]$: r 번째 라운드의 라운드 키에서 m 번째 단위 라운드 키 (4 bits)
$RK_r[m][n]$: r 번째 라운드의 m 번째 단위 라운드 키에서의 n 번째 비트
(단, m={0,1,2,3,4,5,6,7}, n={0,1,2,3}의 범위를 가짐)

3.1. 송신측 MKR 구조와 동작

송신측 MKR 구조는 (그림 1)과 같다.



(그림 1) 송신측 MKR 구조

(그림 1)에서의 각 입출력 값과 프로토콜 모듈을 설명하면 다음과 같다.

[입출력 값]
$P_1, P_2, \ldots, P_n$: 평문 스트림 (8 bits)
$C_1, C_2, \ldots, C_n$: 암호문 스트림 (8 bits)
CSK (Current Session Key) : 현재 세션키 (32 bits)
NSK (Next Session Key) : 다음 세션키 (32 bits)
MN (Message Number) : 메시지 번호 (8 bits)
MAC (Message Authentication Code) : 메시지 인증 코드 (8 bits)

[프로토콜 모듈]
SE (Simple Encryption) : 암호화 모듈
RKG (Round Key Generator) : 라운드 키(32 bits) 생성 모듈
MKG (MAC Key Generator) : MAC 키(8 bits) 생성 모듈
SM (Simple MAC) : MAC 생성 모듈

평문 메시지는 다음과 같이 각 8 비트의 평문 스트림들로 분할된다.

$$P = P_1 \| P_2 \| \ldots \| P_n$$

송신측에서의 동작은 각 평문 스트림마다 암호화, 라운드 키 생성, MAC 키 생성, MAC 생성의 과정을 거친다.

$$C_r = SE(P_r, RK_{r-1})$$
$$RK_r = RKG(P_r, RK_{r-1})$$
$$MK_r = MKG(RK_r)$$
$$MAC_r = SM(C_r, MK_r, MAC_{r-1})$$

이 과정을 라운드(round)라 하며 한 라운드가 끝나면 현재의 라운드에서 생성된 라운드 키와 MAC 이 다음 라운드로 넘겨진다. 전체 평문 메시지가 n 개의 평문 스트림들로 분할될 경우 총 n 번의 라운드가 진

행된다.

n 번의 라운드를 마친 후 각 라운드에서 만들어진 8 비트의 암호문 스트림들을 연결하여 암호문 메시지가 만들어진다.

$$C = C_1 \| C_2 \| \dots \| C_n$$

전체 프로토콜에서의 입력 매개변수는 현재 세션키와 메시지 번호이고 출력 매개변수는 다음 세션키와 MAC 이다.

3.2. 암호화 모듈

각 라운드에서 사용되는 라운드 키는 각 4 비트의 8 개의 단위 라운드 키들로 분할되어 사용된다.

$$RK_r = RK_r[0] \| RK_r[1] \| \dots \| RK_r[7]$$

각 단위 라운드 키들에서 앞 세 비트는 전치를 위해 사용되고 마지막 한 비트는 환자를 위해 사용된다.

$$C_r[\, RK_r[m][0]\times 4 + RK_r[m][1]\times 2 + RK_r[m][2]\,] = P_r[m] \otimes RK_r[m][3]$$

암호화 모듈은 환자와 전치가 한번씩 이루어지는 단순한 적 암호 구조로 되어있으나 각 라운드마다 랜덤한 값을 갖는 라운드 키가 사용되고, 이러한 단순한 구조가 전체 라운드 수만큼 반복되어 Claude Shannon의 확산과 혼돈이 특정 패턴을 갖지 않고 완전하게 랜덤한 구조로 전개된다[5].

3.3. 라운드 키 생성 모듈

평문 스트림을 이용하여 두 개의 단위 라운드 키의 위치를 교환하고 환자를 위해 사용되는 마지막 비트의 값을 갱신한다.

$$RK_r[\, P_r[0]\times 4 + P_r[1]\times 2 + P_r[2]\,] \leftrightarrow RK_r[\, P_r[4]\times 4 + P_r[5]\times 2 + P_r[6]\,]$$
$$RK_r[\, P_r[0]\times 4 + P_r[1]\times 2 + P_r[2]\,][3] = P_r[3]$$
$$RK_r[\, P_r[4]\times 4 + P_r[5]\times 2 + P_r[6]\,][3] = P_r[7]$$

라운드 키 생성 모듈 또한 단순한 구조이나 랜덤한 값인 메시지에 기반하여 키가 생성되고 있어 매 라운드 마다 랜덤한 값을 갖는 라운드 키가 생성된다.

3.4. MAC 키 생성 모듈

각 단위 라운드 키의 네 비트를 EX-OR 연산을 수행하여 MAC 키를 위한 하나의 비트를 만들어낸다.

$$MK_r[0] = RK_r[0][0] \otimes RK_r[0][1] \otimes RK_r[0][2] \otimes RK_r[0][3]$$
$$MK_r[1] = RK_r[1][0] \otimes RK_r[1][1] \otimes RK_r[1][2] \otimes RK_r[1][3]$$
$$\vdots$$
$$MK_r[7] = RK_r[7][0] \otimes RK_r[7][1] \otimes RK_r[7][2] \otimes RK_r[7][3]$$

전체 프로토콜 동작에서 MAC 생성을 위한 키가 매 라운드마다 랜덤하게 변하게 된다.

3.5. MAC 생성 모듈

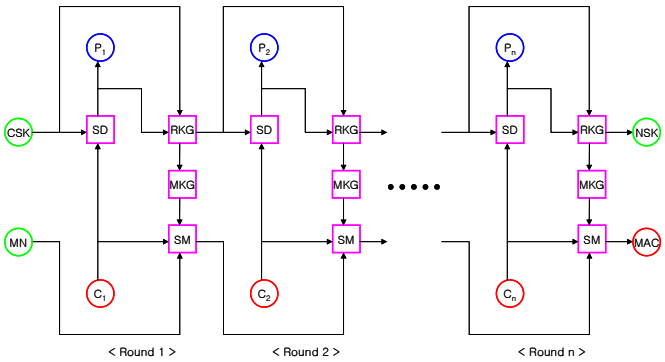
현재 라운드의 MAC 키, 암호문 스트림, 그리고 우측으로 한 비트 시프트 시킨 이전 라운드의 MAC 에 대하여 EX-OR 연산을 수행해 현재 라운드의 MAC 을 만든다.

$$MAC_r[0] = MK_r[0] \otimes C_r[0] \otimes MAC_{r-1}[1]$$
$$MAC_r[1] = MK_r[1] \otimes C_r[1] \otimes MAC_{r-1}[2]$$
$$\vdots$$
$$MAC_r[6] = MK_r[6] \otimes C_r[6] \otimes MAC_{r-1}[7]$$
$$MAC_r[7] = MK_r[7] \otimes C_r[7] \otimes MAC_{r-1}[0]$$

MAC 생성 모듈 또한 단순한 구조를 가지고 있으나 각 라운드 마다 랜덤하게 변하는 MAC 키를 사용하여 MAC 을 만들고 있어 충분히 강한 인증 강도를 제공한다.

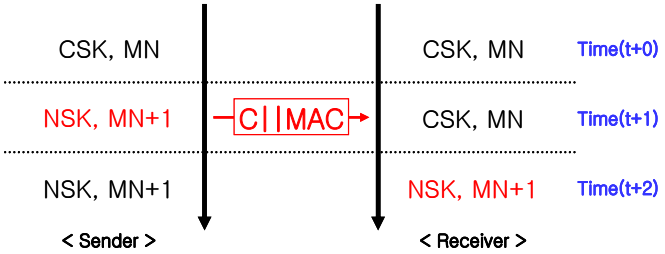
3.6. 수신측 MKR 구조와 동기화

수신측 MKR 구조는 (그림 2)와 같다.



(그림 2) 수신측 MKR 구조

송신측 프로토콜과 비교해보면 암호문 스트림에서 평문 스트림으로 데이터가 흐르고, 암호화 모듈대신 복호화 모듈(SD: Simple Decryption)이 사용된다. 복호화 모듈에선 암호화 모듈에서 행해졌던 전치의 역전치가 이루어지고, 프로토콜 구조에서 다른 부분들은 모두 동일하다. 이를 통해 송신측과 수신측의 라운드 키와 프로토콜 관련 매개변수들이 동기화된다.



(그림 3) 프로토콜 매개변수들의 동기화

(그림 3)은 실제 동기화가 어떻게 이루어 지는지를 보여주는 것으로 송신측과 수신측의 세션키와 메시지 번호가 Time(t+2)에서 동기화되는 것을 볼 수 있다.

4. MKR 의 성능 분석

4.1. 구현시의 성능

비트 레벨에서 동작하므로 하드웨어 모듈로 구현하여 센서의 성능을 높일 수 있고 최종 암호 메시지 전송 이외에 추가적인 통신이 없으므로 센서의 에너지 소비가 적다. 또한 몇 번의 EX-OR 연산만을 사용하므로 센서에서의 프로세서 점유시간이 작고 프로토콜 수행에 필요한 전체 메모리 요구량은 8 바이트로 키 길이에 비례한다.

4.2. 암호학적 기능

기밀성(confidentiality)의 제공과 함께 메시지 번호와 MAC 의 사용으로 무결성(integrity)과 데이터 인증(data authentication)을 제공한다. 또한 두 센서에 대해 하나의 세션이 열리고 각 세션의 메시지 단위마다 세션키와 메시지번호를 동기화시키므로 부인방지와 data freshness 의 기능도 제공한다.

4.3. 암호학적 강도

메시지 기반 암호화 방식에서의 평문은 암호키 생성을 위한 핵심 정보가 되며 스트림 방식의 암호 구조를 갖게 된다. 각 암호화 단계마다 랜덤한 값인 평문을 이용하여 스트림 단위마다 랜덤한 키를 만들어 사용하고 실제 전송 단위인 모든 메시지에 대해서도 매번 다른 키가 사용되므로 충분한 암호학적 강도를 보장 받을 수 있다. 그로 인해 암호화 알고리즘은 단순한 구조를 가질 수 있다.

4.4. 공격에 대한 저항성

데이터 인증을 위해 사용되는 MAC 에서 첫 라운드의 입력으로 메시지 번호가 사용되고 있다. 이는 메시지의 순서를 동기화시키고 replay attack 을 막을 수 있다[6]. 또한 프로토콜의 특성상 센서가 보관하는 키는 메시지의 전송 시마다 바뀌며 현재의 키로 이전 키를 알아낼 수 없어 메시지 단위의 키마다 perfect forward secrecy 를 제공한다[7].

5. MKR 의 개선사항 및 향후 과제

지금까지는 두 센서간의 통신으로 가정하였으나, 실제 네트워크에 적용 시 최초의 세션 설정이나 경로가 재설정되는 경우를 위해 마스터 키가 필요할 수도 있다. 마스터 키를 적용하는 방법은 전체 센서들이 동일 마스터 키를 사용하거나, 각 센서 마다 자신의 마스터 키가 있고 베이스 스테이션이 전체 마스터 키를 보관하는 방법이 있다. 더 강한 인증을 위해선 마스터 키에 대해서만 공개키 구조로 대치할 수도 있다

다음으로는 키 생성의 주요 데이터인 센싱 정보가 랜덤하지 못한 경우로 전 시간 영역에 걸쳐 동일하거나 일정한 패턴으로 반복되는 경우이다. 그러나 앞서 알고리즘에서 살펴본 것처럼 각 라운드 키들이 메시지에만 기반해서 만들어지는 것이 아니라 이전 라운드 키가 함께 사용되고 있으며 임의적으로 랜덤한 특성을 만들어주기 위해 카운터, 타임스탬프, 센서의 ID, 또는 네트워크 정보 등을 함께 이용할 수도 있다.

6. 결론

기존에 몇몇 종류의 센서 네트워크 보안 프로토콜들이 제안되었다. 그러나 실제 구현되어 사용되기에는 아직 여러 가지 제약사항이 남아있으며 이를 해결하기 위해 본 논문에서는 새로운 암호 알고리즘인 메시지 기반 암호화 방식을 적용하여 실제 센서 네트워크를 위한 보안 프로토콜 모델인 MKR 프로토콜을 제시하였고 그 세부 동작과 기존에 암호화 방식을 사용하는 프로토콜과는 다른 특징들에 대해서도 알아보았다. 차후에는 실제 구현과 시뮬레이션 기법 등을 통해 좀 더 구체적인 성능 평가와 함께 앞서 향후 과제로 남긴 사항들에 대한 연구를 통해 개선된 프로토콜을 소개한다.

참고문헌

[1] I. F. Akyildiz et al., “Wireless Sensor Networks: A Survey”, Computer Networks: The Int’l. J. Comp. and Telecommun. Net., vol. 38, no. 4, 2002, citeseer.ist.pso.edo/diffie76new.html, pp. 393–422.

[2] A. D. Wood and J. A. Stankovic, “Denial of Service in Sensor Networks”, Computer, vol. 35, no. 10, 2002.

[3] R. C. Merkle, “Protocols for Public Key Cryptosystems”, IEEE Symp. Research in Security and Privacy, Apr. 1980.

[4] Bo-Cheng Charles Lai, Hwang, D.D., Sungha Pete Kim, and Verbauwhede, I., "Reducing Radio Energy Consumption of Key Management Protocols for Wireless Sensor Networks", Low Power Electronics and Design, 2004. ISLPED '04. Proceedings of the 2004 International Symposium on, 2004.

[5] C.E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, Vol. 28, pp. 656-715, 1949.

[6] Syverson, P., "A taxonomy of replay attacks [cryptographic protocols]", Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings, June 1994.

[7] Ai-fen Sui, Hui, L.C.K., Yiu, S.M., Chow, K.P., Tsang, W.W., Chong, C.F., Pun, K.H., Chan, H.W., "An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication", Wireless Communications and Networking Conference, 2005 IEEE, March 2005.