Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1191

무선 센서 네트워크에서의 안전한 모바일 쿼리 프로토콜

임 채 훈†‡
세종대학교 컴퓨터공학과

Secure Mobile Query in Wireless Sensor Networks

Chae Hoon Lim†‡
Department of Computer Engineering, Sejong University

요 약

대규모의 센서 네트워크에서는 고정된 베이스 스테이션에서 데이터를 수집하고 네트워크를 관리하는 것은 센서노드들의 제한된 에너지를 빨리 소진시켜 네트워크의 수명을 단축시키게 되므로 바람직하지 않다. 다른 여러 가지 이유로도 모바일 싱크가 널리 활용되고 있으나, 이러한 모바일 싱크에 대한 안전한 쿼리 프로토콜에 대한 연구는 그다지 많지는 않다. 본 논문에서는 모바일 싱크가 인접 센서노드들과 안전하면서도 효율적인 쿼리 세션을 수행할 수 있는 키 관리 및 인증 프로토콜을 제안하고 안전성 및 효율성을 분석한다.

ABSTRACT

In large-scale distributed sensor networks, it is often recommended to employ mobile sinks, instead of fixed base stations, for data collection to prolong network lifetime and enhance security. Mobile sinks may also be used, e.g., for network repair, identification and isolation of compromised sensor nodes and localized reprogramming, etc. In such circumstances, mobile sinks should be able to securely interact with neighbor sensor nodes while traversing the network. This paper presents a secure and efficient mobile query protocol that can be used for such purposes.

Keywords: Wireless sensor networks, Security, Mobile sink, Query authentication

I. 서 론

대규모의 분산 센서 네트워크에서 각 센서노드가 관측 데이터를 베이스 스테이션(base station)으로 직접 전송하는 것은 안전성이나 효율성 등에서 문제가 될 수 있고, 또한 물리적으로 불가능한 경우도 있다(위험지역, 바다 등). 이 경우 주기적으로 혹은 필요에 따라 네트워크를 돌며 관측 데이터를 수집하는 모바일 데이터 수집자(mobile data collector)를 흔히 이용하며, 이는 단지 데이터를 수집하여 베이스 스테이션에 전달해 주는 모바일 릴레이(mobile relay)와 직접 현장에서 데이터를 수집하여 분석하는 데이터의 최종 사용자인 모바일 싱크(mobile sink)로 나눌 수 있다[3]. 고정된 베이스 스테이션이 없는 경우 모바일 싱크는 또한 네트워크 관리자가 될 수도 있다.

모바일 릴레이는 단지 각 센서노드와 공유키를 설정하여 1-1 통신으로 데이터를 내려 받는 것이 주된 일이므로 1-1 키설정(pairwise key establishment) 과정이 보안의 거의 전부라 할 수 있다. 그러나 모바일 싱크의 경우는 주변 노드들과의 반복적인 쿼리-응답(query-response) 과정을 필요로 하므로 좀 더 어려운 로컬 브로드캐스트 인증(local broadcast authentication)까지를 필요로 한다. 본 논문에서는 이러한 모바일 싱크을 위한 키관리 및 쿼리 인증 프로토콜을 다룬다.

접수일(2013년 11월 11일), 게재확정일(2013년 11월 21일)
† 주저자, chlim@sejong.ac.kr
‡ 교신저자, chlim@sejong.ac.kr(Corresponding author)

안전한 모바일 쿼리는 각 센서노드가 표준적인 디지털서명을 자유로이 이용할 수 있다면 전혀 문제가 될 것이 없지만, 센서 네트워크의 인프라를 구성하는 저가의 소형 정지 센서노드(stationary sensor node)들에서 공개키 암호는 안전성이나 효율성 면에서 여전히 문제가 많으므로 본 논문에서는 비밀키 암호만을 이용하는 보안에 집중하기로 한다. 이 경우 모바일 싱크와 각 센서노드 사이의 1-1 키 설정은 가장 기본적인 요구이며, 특히 여기서는 모바일 싱크의 전복(compromise) 가능성과 전복시의 피해를 최소화하는 것이 무엇보다도 중요하다. 일반 센서노드에 비해 모바일 싱크는 훨씬 더 큰 권한이 주어지므로 공격자의 주요 공격목표가 될 수 있기 때문이다[9]. 따라서 모바일 싱크 환경에서는 가장 널리 연구되고 있는 임계치 방식(threshold scheme)은 너무 위험도가 높다고 판단된다. 이런 방식에서는 상대적으로 공격이 쉬운 센서노드들을 일정 수 이상 전복시키면 모바일 싱크의 모든 비밀키를 쉽게 알아낼 수 있기 때문이다. 저장 공간을 희생하여 공개키 암호와 동일한 안전성(perfect resilience against node compromise)을 제공할 수 있는 가장 간단한 방법은 모바일 싱크에 모든 센서노드들과의 1-1 공유키를 저장시키는 것이다. 모바일 싱크는 센서노드에 비해 상대적으로 풍부한 저장 공간을 장착할 수 있고, 각 모바일 싱크가 센서필드에 파견될 때마다 모든 활동 중인 센서노드들과의 공유키를 주입시키는 것은 큰 무리는 아니라고 판단된다. 본 논문에서는 키관리를 위해 이 기법을 이용하기로 한다.

모바일 싱크의 쿼리 인증을 위해서는 로컬 브로트캐스트 인증이 필요한데, 이는 모바일 싱크-센서 노드 간의 공유키 설정과는 별개의 문제이다. 여기서 중요한 것은 공개키 암호의 디지털서명처럼 모바일 싱크-센서 노드 간의 인증채널이 반드시 비대칭적이어야 한다는 것이다. 그렇지 않다면 (예를들어 그룹키 기반의 인증처럼 대칭적인 인증채널의 경우) 센서노드들이 쉽게 모바일 싱크를 가장하여 쿼리 명령을 내릴 수 있기 때문이다. 비밀키 방식의 대표적인 비대칭적인 인증기법으로는 μTESLA[5]와 일회용 서명(one-time signature)[1] 등이 있으나, 모바일 쿼리의 로컬 브로드캐스트 인증에는 적합하지 않은 것으로 판단된다. 본 논문에서는 조금은 약한 인증기능을 제공하지만 로컬 쿼리 메시지 인증에는 충분하다고 판단되는 ([13]의 3.6절에 기술된) 키체인 기반의 단순한 인증 기법을 사용하고, 더 중요한 메시지나 관리용 커맨드(command) 등을 위해서는 디지털 서명을 같이 사용하는 방법을 취하기로 한다.

관련연구: 다양한 센서 네트워크 키 관리 방식들은 서베이 논문 [10], [11]을 참고한다. 모바일 싱크용으로 제안된 키 설정 방식으로는 폴리노미알 풀(polynomial pool) 기반의 확률론적 키 설정 방식의 변형인 [7], [8] 등이 있다. 이들은 모바일 싱크의 공격에 좀 더 강한 것으로 제안된 것이나, 직접적인 키 설정이 불가능한 경우 훨씬 복잡한 경로키 설정(path key establishment) 과정이 필요하며, 여전히 일정 수 이상의 센서노드 전복이면 모바일 싱크를 가장할 수 있으므로 보안성 향상에는 한계가 있는 것으로 보인다. [12]에서는 모바일 센서 네트워크를 위한 그룹기반의 키관리 프로토콜을 제안하고 있고, [9]에서는 모바일 싱크의 권한 제한을 통한 피해의 최소화 방안과 전복된 모바일 싱크의 제거(revocation) 방안 등을 기술하고 있다. [6]에서는 키체인을 이용한, 고정된 경로를 따르는 모바일 싱크의 데이터 수집 방법을 제안하고 있다.

II. 제안 프로토콜

2.1 준비단계

모바일 싱크는 다수의 소형 정지 센서노드들로 구성된 센서필드를 돌며 실시간으로 주변 센서노드들로부터 데이터를 수집하여 분석하는 센서 네트워크의 사용자이다. 모바일 싱크는 이동 중 각 지점에서 다수의 쿼리-응답(query-response) 과정을 반복 수행할 수 있으며, 이때 쿼리는 일반적으로 각각의 센서노드와의 일대일 통신이 아니라 통신반경 내에 존재하는 모든 센서노드들(one-hop neighbors)에 대한 브로드캐스트 메시지로 보는 것이 타당하다.

센서 네트워크를 관리/운영하는 네트워크 센터에서 센서노드 및 모바일 싱크를 초기화하는 과정은 다음과 같다 (모바일 쿼리에 필요한 부분만 기술):

- 네트워크 센터의 초기화: 네트워크 센터는 마스터키 K를 랜덤하게 선택하여 이후 모든 센서노드나 모바일 싱크의 초기화에 사용한다.
- 센서노드 초기화: 네트워크 센터는 각 센서노드 s에 유일한 식별자 ID_s를 할당하고 마스터키 K를 이용하여 s의 비밀키 $K_s = F(K, ID_s)$를 계

산, (ID_s, K_s)로 s를 초기화한다 (여기서 $F(K,.)$는 의사난수함수(pseudorandom function)를 의미).

- 모바일 싱크의 초기화: 네트워크 센터는 센서필드에 파견될 각 모바일 싱크 m에 식별자 ID_m을 할당하고 네트워크 사용기간(시작-종료시간) T_m을 지정하여 비밀키 $K_m = F(K, ID_m \| T_m)$을 계산한다 ($\|$는 연접). 이 K_m은 모바일 싱크 m에게 T_m에 명시된 유효기간 동안 센서 네트워크의 데이터를 수집/이용할 수는 권한을 부여하는 것으로 생각할 수 있다. 네트워크 센터는 또한 K_m을 이용하여 현재 필드에서 작동중인 각 센서노드 s에 대해 다음과 같은 $m-s$ 쌍방간의 공개키(pairwise public key) PK_{ms}들을 계산한다 (1에서 N까지 총 N개의 센서노드가 운영되고 있다고 가정):

$$PK_{ms} = F(K_m, ID_s) \oplus F(K_s, ID_m \| T_m) \quad (1 \le s \le N)$$

모바일 싱크 m의 초기화는 위에서 생성된 데이터 $\{ID_m, T_m, K_m, (ID_s, PK_{ms})(1 \le s \le N)\}$를 m에 저장하는 것으로 마무리된다.

센서노드의 효율적인 관리나 안전성을 위해 노드 ID에 그 노드의 종류나 역할/권한을 엔코딩하는 것이 유용할 수 있다. 예를들어 4바이트 노드 ID의 상위 4비트를 이런 용도로 할당하여 그 ID만으로 노드의 종류나 역할을 알 수 있게 하고 비밀키를 통해 이를 증명하게 함으로써 최소권한의 원칙(principle of least privilege)을 구현할 수 있다 [10]. 특히 모바일 싱크는 네트워크의 이용자나 관리자 등 다양한 권한을 가질 수 있으며, 안전성을 위해서는 자신에게 부여된 권한 내에서만 네트워크 자원을 이용하도록 해야 한다. 본 논문에서 다루는 모바일 싱크는 센서 네트워크 서비스 이용자로서의 역할을 주로 하며, 중요한 명령을 내리는 네트워크 관리자의 역할을 하는 경우 논문에서 언급된 별도의 요구조건(서명과 함께 사용)을 만족하여야 한다.

2.2 모바일 쿼리 프로토콜

모바일 싱크가 통신반경 내에 있는 인접 센서노드들과 대화하는 프로토콜은 다음과 같다:

$m \rightarrow *: ID_m, T_m, R_m$

$s \rightarrow m: ID_s, R_s, \sigma_s$

$m \rightarrow *: ID_m, 0, S_0, k, l, d, \sigma_1^1 \| \sigma_2^1 \| \cdots \| \sigma_d^1$

$m \rightarrow *: ID_m, 1, S_0, k, l, d, \sigma_1^2 \| \sigma_2^2 \| \cdots \| \sigma_d^2$

$\vdots$

$m \rightarrow *: ID_m, k, S_0, k, l, d, \sigma_1^k \| \sigma_2^k \| \cdots \| \sigma_d^k$

$m \rightarrow *: ID_m, 1, S_1, q_1$ /* first query */

$s \rightarrow m: ID_s, c_{s1}$ /* encrypted response */

$\vdots$

$m \rightarrow *: ID_m, 0, S_n, q_n$

$s \rightarrow m: ID_s, c_{sn}$

각 단계에 대한 상세기술은 다음과 같다.

1. 모바일 싱크 m은 난수 R_m을 선택하여 ID_m, T_m, R_m을 인접 노드들에 방송한다 (*는 브로드캐스트를 의미). 모바일 싱크의 무선통신범위는 센서노드들의 그것과 동일한 것으로 가정한다.

2. m의 헬로 메시지를 수신한 각 인접 노드 s는 우선 T_m을 확인하여 만일 현재 시간이 T_m의 유효기간 내에 있지 않으면 프로토콜을 종료한다. 노드 s는 이제 랜덤한 R_s를 선택, 자신의 비밀키 K_s를 이용하여 m과의 세션키 $K_{sm} = F(K_s, ID_m \| T_m)$과 MAC값 $\sigma_s = MAC_{K_{sm}}(R_s \| R_m)$를 차례로 계산하여 $\{ID_s, R_s, \sigma_s\}$로 응답한다 ($MAC_K(x)$는 키 K로 계산한 메시지 x에 대한 메시지인증코드(Message authentication Code)를 의미).

3-5. 센서노드 s의 응답을 받은 모바일 싱크는 메모리에서 ID_s에 대응하는 공개키 PK_{ms}를 찾아 s와의 세션키 $K_{ms} = PK_{ms} \oplus F(K_m, ID_s)$를 계산하여 σ_s를 검증한다. 일정한 정해진 시간 내에 d개의 센서노드 $1, 2, \cdots, d$로부터 유효한 응답을 받았다고 가정하자. 우선 m은 일방향 키체인(one-way key chain)의 최상위값 S_L을 랜덤하게 선택하여 안전한 해쉬함수 h를 이용, 예상되는 쿼리 패킷 수를 충분히 초과하는 수 L에 대해 길이 L의 키체인 $\{S_i\}_{(0 \le i \le L)}$, $S_{i-1} = h(S_i)$을 계산한다 (이 과정은 사전에 혹은 이동 중에 미리 수행될 수 있다). 또한 d개의 응답 노드에 대한 MAC값 σ_i를 계산한다:

$$\sigma_i = MAC_{K_{mi}}(S_0 \| k \| l \| d \| R_m \| R_i) \; (1 \le i \le d)$$

여기서 $K_{mi} = PK_{mi} \oplus F(K_m, ID_i)$이며, MAC값의

길이는 $|\sigma_i| = t + \lceil \log_2 d \rceil$ 비트이다 (t는 보안레벨로 인증실패 확률 2^{-t}을, $|x|$는 x의 비트길이를 의미). 모든 σ_i들을 하나의 패킷으로 보내는 것은 불가능할 수 있으므로, 각 σ_i의 일정 비트들을 모아 하나의 최대길이 패킷으로 만들어 차례로 전송하는 기법을 이용한다(마지막 패킷은 더 작을 수 있다). 우선 각 σ_i를 $\sigma_i = \sigma_i^1 \| \sigma_i^2 \| \cdots \| \sigma_i^k \quad |\sigma_i^j| = l \text{ for } j < k, (\ |\sigma_i^k| = |\sigma_i| - (k-1)l)$ 와 같이 l비트 길이로 분할한 후, 한 패킷에 d개의 l 비트 부분-MAC값을 패킹하여 전체를 k개의 패킷으로 나누어 전송한다. 여기서 l과 k는 다음과 같이 결정된다 ($MaxBits$는 허용 가능한 최대 패킷의 비트길이):

$$l = \left\lfloor \frac{MaxBits - |ID_m| - |S_0| - 32}{d} \right\rfloor, \quad k = \left\lceil \frac{|\sigma_i|}{l} \right\rceil$$

각 패킷에는 ID_m, S_0, k, l, d가 공통적으로 포함된다 (효율성을 위해 첫 번째 이 후의 인증패킷에서는 S_0, k, l, d가 생략되어도 무방하다). 여기서 k는 전송될 총 인증패킷의 수, d는 한 패킷에 들어있는 부분-MAC값의 개수, 그리고 l은 한 패킷에 포함된 부분-MAC값의 비트길이로 마지막 패킷에는 $|\sigma_i| - (k-1)l$비트 부분-MAC값이 들어간다.

단계 2에서 응답한 각 센서노드 s ($1 \le s \le d$)가 단계 3의 인증패킷을 받으면 우선 단계 2에서 계산된 세션키 K_{sm}을 이용하여 $t + \lceil \log_2 d \rceil$ 비트 길이의 MAC $\sigma_s = MAC_{K_{sm}}(S_0 \| k \| l \| d \| R_m \| R_s)$를 계산하고, 이를 $\sigma_s = \sigma_s^1 \| \sigma_s^2 \| \cdots \| \sigma_s^k$와 같이 l비트씩 k개로 분할하여 첫 인증패킷에 σ_s^1이 존재하는지 검사한다. 만일 존재하지 않는다면 s는 m과의 세션을 끝내고 나머지 패킷들을 무시한다. 만일 σ_s^1과 일치하는 것이 있다면 s는 다음 패킷을 기다려 같은 위치의 l비트가 σ_s^2와 같은지를 검사한다. 이렇게 마지막 k번째 인증패킷까지의 모든 부분-MAC값들이 일치할 때만 m을 유효한 모바일 싱크로 인정한다.

6-9. 이제 모바일 싱크 m은 인증이 완료된 센서노드들을 대상으로 쿼리 세션을 시작한다. 각 i번째 쿼리 패킷에는 ID_m, 쿼리 일련번호 i, 키체인 값 S_i, 그리고 쿼리 메시지 q_i가 포함된다. 이를 수신한 각 노드 s는 저장된 키체인 값 S_{i-1}을 이용하여 $S_{i-1} = h(S_i)$을 만족하는지 검사하여 쿼리 패킷을 인증한다. 인증이 통과되면 노드 s는 $(i-1, S_{i-1})$를 (i, S_i)로 대체하고 m과의 세션키 K_{sm}을 이용하여 응답 메시지 r_i를 암호화한 $c_{si} = E_{K_{sm}}(r_i)$를 전송한다. 쿼리 일련번호 0은 마지막 쿼리임을 나타내며, 어느 경우든 안정성을 위해 일정한 기간 동안 모바일 싱크로부터 쿼리가 없는 경우 각 센서노드는 키체인 값을 삭제하고 프로토콜을 자동 종료한다.

만일 모바일 싱크가 단순한 데이터 사용자가 아닌 네트워크 관리를 위한 중요한 명령을 내리는 네트워크 관리자의 역할을 하는 경우 위조 불가능한 강한 인증이 필요한데, 이를 위해 디지털 서명의 사용이 필수적이다. 이 경우 위 프로토콜에서 i-번째 쿼리 패킷은 $ID_m, i, S_i, q_i, sig(q_i)$와 같이 q_i에 대한 서명 $sig(q_i)$를 같이 사용할 수 있다. 이때 키체인 인증은 단지 서비스거부 공격(Denial-of-Service attack)에 대해 서명을 보호하는 역할을 수행하며 인증기능은 서명에 의해 수행된다.

III. 안전성 및 효율성 분석

3.1 안전성 분석

제안 프로토콜의 전반부(단계 1-5)는 전형적인 3단계 쌍방인증 프로토콜을 1 대 다 환경으로 확장한 것으로, 후에 사용할 키체인의 초기값 S_0의 분배까지를 포함하고 있다. d개의 센서노드들에 대한 응답을 1-1 통신 대신 브로드캐스트한 것은 효율성을 위한 것이지만, 이는 같은 정도의 안전성을 위해 1-1 통신에 비해 MAC값의 길이 $|\sigma_i|$를 약간 증가시키는 결과를 초래한다. 1-1 인증의 경우 2^{-t} 정도의 보안레벨을 달성하려면 t비트 길이의 MAC 값이면 되지만, 제안 프로토콜에서는 수신 노드가 받은 패킷에 자신의 MAC값이 존재하는 지, 어느 위치에 존재하는 지에 대한 정보가 전혀 없다 (효율성을 위해 ID 정보를 같이 보내지 않았기 때문). 따라서 수신 노드는 자신이 계산한 MAC값의 각 l비트 부분을 수신 패킷에 있는 d개의 l비트 부분-MAC값 각각과 비교하여 일치하는 것이 있는지를 확인해야 한다. 이 경우 t비트 길이의 MAC 값이 제공할 수 있는 보안정도는 대략 $d \times 2^{-t}$정도이다. 따라서 제안 프로토콜에서 t비트의 보안을 위해서는 $t + \lceil \log_2 d \rceil$ 비트 길이의 MAC값을 사용해야 한다.

제안 프로토콜의 후반부(단계 6-9)의 쿼리 인증은 현재 센서노드가 가지고 있는 인증된 키체인 값의 전

상(preimage)를 모바일 싱크가 올바로 제공할 수 있는 지의 여부를 통해 이루어지며, 그 안전성은 해쉬함수의 일방향성(one-wayness)에 의해 제공된다. 이런 메시지 인증기법은 유선 인터넷과 같이 전송 중인 메시지를 가로채서 메시지를 변경하거나 새로운 메시지를 주입시키는 등의 공격이 쉽게 가능한 환경에서는 전혀 안전성을 제공할 수 없다. 그러나 짧은 통신반경 내에서 무선매체를 통해 빛의 속도로 전송되는 모바일 쿼리에 대한 근접인증의 경우 이러한 공격은 거의 불가능하다. 단지 통신반경 내의 공격 노드가 통신방해를 통해 일부 센서노드들이 모바일 싱크가 보낸 패킷을 받을 수 없게 만든 후, 대신 자신의 메시지로 바꿔치기한 패킷을 이들에게 보내는 형태의 공격은 가능할 수 있다 ([13]의 3.6절 참조). 그러나 제안 프로토콜에서 쿼리 인증은 단계 3-5에서 S_0를 수신한 소수의 이웃 노드들에게만 적용되고, 그 응답은 모바일 싱크와의 공유키로 암호화되어 전송되므로, 이러한 공격이 가능하다고 하더라도 공격자가 얻을 수 있는 이득은 거의 없다. 오히려 어렵게 침투시킨 공격노드가 아무런 이득도 없이 발각되어 제거될 위험이 높아지므로 현실성 있는 공격으로 보기 어렵다. 그러나 네트워크 관리를 위한 명령 하달 등과 같은 중요한 응용에서는 이런 공격도 치명적일 수 있으므로, 이러한 목적을 위해서는 II장의 마지막 문단에서 언급 되었듯이 쿼리 시에 디지털 서명을 함께 사용하는 것을 권장한다. 이 경우 키체인은 디지털 서명을 서비스거부 공격으로부터 보호해 주는 역할을 하며 (키체인 검증이 실패하면 패킷을 바로 버린다), 명령에 대한 인증은 디지털 서명에 의해 수행되어 안전성을 확보할 수 있다.

마지막으로 다수의 센서노드나 모바일 싱크가 공격당해 전복되었을 때의 피해 정도를 생각해보자. 제안 프로토콜의 가장 큰 특징 중의 하나가 이런 경우에 제공되는 완전한 안전성과 피해정도의 최소화이다. 우선 아무리 많은 센서노드가 전복된다고 하더라도 이것이 모바일 싱크의 안전성에 미치는 영향은 없으며, 또한 모바일 싱크가 전복되더라도 노출되는 키는 해당 모바일 싱크에만 국한되므로 다른 센서노드나 모바일 싱크의 안전성에는 전혀 영향을 미치지 않는다. 키관리 측면에서도 모바일 싱크 m의 본질적인 유일한 비밀키는 K_m 뿐이므로 이 K_m의 안전성 확보에만 집중할 수 있다. 또한 모바일 싱크와 센서노드간의 공유키는 네트워크 센터에서 인가한 해당 업무의 수행에 필요한 최소한의 권한으로 국한되고 일정한 유효기간이 있기 때문에 모바일 싱크 전복시의 피해를 최소화할 수 있다 (유효기간을 업무처리에 필요한 최소한의 기간으로 한정할 수 있다). 이와 같이 지정된 권한 및 수명을 갖는 완전한 안전성을 제공하는 키관리 기법은 센서 네트워크의 서비스를 일반에 판매할 때에도 유용하게 사용될 수 있다. 이 경우 모바일 싱크는 적절한 계약 하에 대가를 지불하고 정해진 기간 동안 네트워크 서비스를 이용할 수 있는 권한을 획득한 모바일 유저가 될 것이고, 네트워크 센터는 모바일 유저의 배반이나 모바일 유저들 간의 공모, 등에 대해 걱정할 필요가 없을 것이다.

3.2 효율성 분석

제안 프로토콜은 의사난수함수, 해쉬함수 및 MAC 등과 같은 빠른 비밀키 연산만을 사용하고, 실제로 이들은 모두 하나의 알고리즘(해쉬함수 혹은 블록암호)만으로도 구현 가능하므로 계산효율 면에서는 거의 최적에 가깝다고 할 수 있다. 제안 프로토콜의 효율성면에서의 가장 큰 특징은 단계 3-5에서의 인증패킷의 브로트캐스트와 단계 6-9의 일방향 키체인을 이용한 쿼리 메시지 인증기법이라 할 수 있다.

제안 프로토콜의 브로드캐스트기법은 인증패킷의 개별적인 1-1 전송에 비해 두 가지 측면에서 더 큰 효율성을 제공한다. 첫째, 대부분의 널리 사용되는 센서노드(MicaZ, TelosB/Tmote Sky, IRIS 등 [4]) 들에 장착된 802.15.4 표준기반의 무선모듈처럼, 최대 패킷길이가 충분히 큰 경우, 짧은 메시지를 모아서 전송하여 전송 패킷 수를 줄임으로써 각 패킷에 수반되는 오버헤드를 상당히 줄일 수 있다. 예를들어 802.15.4 패킷의 경우, 최대 102바이트의 데이터를 전송하는데 물리계층 오버헤드 6바이트와 MAC계층 오버헤드 최대 25바이트 등 총 31바이트의 오버헤드가 필요하다 [14]. 만일 단계 3의 응답을 각 센서노드에게 1-1 통신으로 전송한다면, 예를들어 $d=16$인 경우, 총 20바이트의 데이터 패킷 $\{ID_m, S_0, \sigma_i\}$ 16개를 전송해야 한다 (ID: 4바이트, 키체인 및 MAC 값: 각 8바이트, i,k,l,d: 각 1바이트, $t=64$비트 보안레벨 가정). 반면 제안 프로토콜의 경우, $l=43, k=2$를 취하면 되므로 102바이트, 66바이트 패킷 2개만 전송하면 된다. 단순히 오버헤드를 포함한 총 전송량을 비교하면, 전자의 경우 $16\times(20+31)=816$바이트 대 후자의 경우 $102+66+2\times31=230$바이트로 제안기법으로 3.5배 정도의 통신효율을 얻을 수 있다.

둘째, 제안 브로드캐스트기법에서는 단계 2에서 응

답한 각 센서노드는 단계 3의 첫 패킷을 바탕으로 인증이 실패한 경우 세션을 조기 종료(early abort) 할 수 있어 불필요한 에너지 소모를 막을 수 있다 (예를 들어 radio를 꺼고 sleep 모드로 진입). 센서노드들은 단계 2에서 적법하게 응답했다고 하더라도 통신장애나 고의적인 제외 등 다양한 이유로 모바일 싱크의 선택에서 제외될 수 있다. 이 경우 선택되지 않은 노드들은 첫 패킷만을 수신하면 자신이 제외된 것을 바로 확인할 수 있어 세션을 바로 종료할 수 있다.

단계 6-9의 쿼리 메시지의 로컬 브로드캐스트 인증기법은 무선 센서 네트워크에 특화된 것으로 추가 설명이 필요 없는 아마도 가장 효율적인 인증기법일 것이다. 쿼리 메시지의 인증은 센서노드들이 악용할 수 없도록 하기 위해 반드시 비대칭적인 기법을 필요로 하는데 비밀키 암호만을 이용한 이보다 더 효율적인 비대칭적인 인증기법은 생각하기 어렵다. 또한 이러한 키체인 인증기법은 디지털 서명과 함께 사용하면 네트워크 관리자의 역할을 하는 모바일 싱크로까지 자연스럽게 확장될 수 있다는 장점도 있다.

마지막으로 센서노드 및 모바일 싱크의 키관리를 위한 메모리 요구량을 살펴보자. 각 센서노드의 경우 네트워크 센터와의 공유키 하나면 되므로 최적에 가깝다고 볼 수 있다. 그러나 모바일 싱크의 경우 현재 센서필드에서 동작하고 있는 모든 센서노드 s와의 1-1 공개키 PK_{ms}를 (ID_s, PK_{ms})의 형태로 저장하고 있어야 하므로 네트워크 크기에 비례하는 저장용량을 필요로 한다. 이는 이론적으로는 매우 바람직하지 않은 성질이나, 모바일 싱크는 센서노드에 비해 훨씬 고성능의 장치로 가정하여도 무리가 없으므로 현실적으로 크게 문제가 되지는 않는다. 예를들어 4바이트의 ID 길이와 10바이트(80비트)의 공개키 길이에 대해 백만개의 센서노드를 갖는 초거대 네트워크를 가정하더라도 14 메가바이트(MBytes) 정도의 저장용량이면 충분하다. 이 정도의 메모리는 micro SD 카드를 장착할 수 있는 일반 센서노드(예: SHIMMER [2])에서도 무리없이 수용할 수 있는 정도의 양이다. 대신 이 정도 메모리의 사용으로 모바일 싱크의 물리적인 나포에 대한 완전한 안전성과 모바일 싱크-센서노드 간의 공유키 분배가 추가적인 통신 없이 한 번에 가능한 효율성(non-interactive key establishment) 등을 동시에 확보할 수 있으므로 모바일 쿼리 환경에서는 현실적으로 최적의 선택에 가깝다고 할 수 있다.

IV. 결 론

본 논문에서는 모바일 싱크의 로컬 브로드캐스트쿼리를 위한 안전하면서도 효율적인 키관리 및 인증 프로토콜을 제안하였다. 제안 프로토콜은 대규모의 센서네트워크에서 에너지 효율을 위해 고정된 베이스 스테이션 대신에 모바일 싱크를 이용하여 데이터를 수집할 때 유용하게 사용될 수 있고, 또한 네트워크 관리용의 프로토콜로까지 쉽게 확장될 수 있다.

References

[1] J.Buchmann, E.Dahmen, and M.Szydlo, "Hash-based digital signature schemes," Post-quantum Cryptography, pp.35-93, 2009.

[2] A.Burns et al., "SHIMMER-A wireless sensor platform for noninvasive biomedical research," IEEE Sensors Journal, vol.10, no.9, pp.1527-1534, 2010.

[3] M.Di Francesco, S.K.Das, and G.Anastasi, "Data collection in wireless sensor networks with mobile elements: A survey," ACM Trans. on Sensor Networks, vol.8, no.1, pp.1-31, 2011.

[4] M. Johnson et al., "A comparative review of wireless sensor network mote technology," Proc of IEEE Sensors 2009, pp.1439-1442, 2009.

[5] A.Perrig et al., "SPINS: Security protocols for sensor networks," Wireless networks, vol.8, no.5, pp.512-534, 2002.

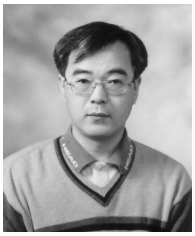
[6] A.Rasheed and R.Mahapatra "Secure data collection scheme in wireless sensor networks with mobile sink," Proc. IEEE Int. Symp. on Network Computing and Applications, pp.332-340, 2008.

[7] A.Rasheed and R.Mahapatra "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks," IEEE Trans. on Parallel and Distributed Sys., vol.22, no.1, pp.176-184, 2011.

[8] A.Rasheed and R.Mahapatra "The

three-tier security scheme in wireless sensor networks with mobile sinks," IEEE Trans. on Parallel and Distributed Systems, vol.23, no.5, pp.958-965, 2011.
〔9〕 H.Song, S.Zhu, W.Zhang, and G.Cao. "Least privilege and privilege deprivation: Toward tolerating mobile sink compromises in wireless sensor networks," ACM Trans. on Sensor Networks, vol.4, no.4, pp.1-30, 2008.
〔10〕 M.A.Simplicio Jr, P.S.L.M.Barreto, C.B.Margi, and T.C.M.B.Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," Computer Networks, vol.54, no.15, pp.2591-2612, 2010.
〔11〕 X.Xiao, V.K.Rayi, B.Sun, X.Du, F.Hu, and M.Galloway, "A survey of key management schemes in wireless sensor networks," Computer Communications, vol.30, pp.2314-2341, 2007.
〔12〕 L.Zhou, J.Ni, and C.V.Ravishankar, "Supporting secure communication and data collection in mobile sensor networks," Proc. IEEE INFOCOM, pp.1-12, 2006.
〔13〕 S.Zhu, S.Setia, and S.Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," ACM Trans. on Sensor Networks, vol.2, no.4, pp.500-528, 2006.
〔14〕 LAN-MAN Standards Committee of the IEEE Computer Socity, Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate personal area networks (LR-WPAN),

〈저자소개〉



임 채 훈(Chae Hoon Lim) 종신회원
1989년 2월: 서울대학교 전자공학과 졸업
1992년 2월: 포항공과대학교 전기전자공학과 석사
1996년 2월: 포항공과대학교 전기전자공학과 박사
1997년 2월~2002년 2월: ㈜퓨쳐시스템 기술이사
2002년 3월~현재: 세종대학교 컴퓨터공학과 교수
〈관심분야〉 암호 알고리즘/프로토콜 설계/분석, RFID/센서 네트워크 보안