무선 센서 네트워크를 위한 강한 익명성 지원 구조

A Strong Anonymity Scheme for Wireless Sensor Networks

이 중 현* 김 태 연** 조 기 환***
Junghyun Lee Taeyeon Kim Gihwan Cho

요 약

기존의 센서 네트워크 보안에 대한 연구는 인증과 비밀성, 무결성, 이용성 등을 제공하는 보안 서비스에 관심이 집중되어 왔으나 최근 센서 노드의 실제 ID의 노출 문제에 대한 관심이 증가하고 있다. 센서 노드의 실제 ID가 외부 공격자에게 노출되는 것을 방지하기 위해서는 실제의 ID를 사용하지 않고 동적인 가명을 사용하는 것이 일반적이다. 그러나 가명을 생성하는데 사용되는 비밀키(또는 해쉬키)와 현재의 가명(또는 난수)이 공격자에게 노출되었을 경우에 공격자는 쉽게 가명을 생성하는 문제가 발생한다. 본 논문에서는 센서 노드들에 대한 강한 익명성이 보장되는 구조를 제안한다. 제안된 구조는 가명을 생성하는데 사용되는 비밀정보들이 공격자에게 공모되었다고 하더라도 공격자가 해당 노드의 가명 ID들을 생성할 수 있는 확률이 매우 낮다. 그리고 보안 분석을 통해 제안된 구조가 무선 센서 네트워크에 적합함을 증명한다.

ABSTRACT

In the sensor network security area, previous works were mainly concentrated on achieving authentication, confidentiality, integrity and availability. But the ID exposure issue is recently an increasing concern in research community. To protect the ID exposure from various attacks, the most common approach is to make use of a dynamic pseudonym rather than the real ID. However, if a node's secret key (or hash key) and the current pseudonym (such as a random number) are exposed, the attacker can easily generate the previous/next pseudonyms. In this paper, we propose a security infra-structure scheme for enabling strong anonymity of sensor nodes. Our scheme ensures that the probability being able to generate a pseudonym is very low even if a sensor node has been compromised with an attacker. Security analyses have proven that our scheme is suitable for sensor network environments in terms of preserving of forward anonymity as well as backward anonymity.

☞ KeyWords : 센서 네트워크(sensor network), 익명성(anonymity), 해쉬 체인(hash chain), 인증(authentication)

1. 서 론

이동 무선센서네트워크(MWSN: Mobile Wireless Sensor Network)는 개방 환경에서 자유스럽게 이동하면서 제한된 주파수와 대역폭으로 통신하는 독립된 노드들의 집합으로 정의할 수 있다. 노드들은 사전에 결정된 토폴로지로 구성되는 것이 아니라 배치된 후에 인접한 다른 노드들과 토폴로지를 구성한다. 따라서 사람이 직접 접근할 수 없는 지역에서의 군사적 감시나 제어 통신, 재앙 지역 모니터링에 적합하다. 하지만 이러한 장치들은 근본적으로 낮은 비용과 낮은 전력, 다기능, 크기가 소형이며 근거리 통신만을 지원하는 제약점을 가지고 있기 때문에 보안 수준이 그리 높지 못하다[1,2,3].

기존의 센서 네트워크 보안에 대한 연구는 인증과 비밀성, 무결성, 이용성 등을 제공하는 보안 서비스에 관심이 집중되었다. 하지만 최근 들어 무선 센서 네트워크에서 노드의 익명성을 보장하는 문제에 대한 관심이 고조되고 있다[4,5,6]. 통신 중인 메시지에 가명을 사용하지 않고 실제 ID를

* 정 회 원 : 전북도청 홍보기획과(인터넷홍보)
leejh0926@korea.kr(제1저자)
** 정 회 원 : 서남대학교 컴퓨터정보통신학과 조교수
kimcopper@naver.com(교신저자)
*** 종신회원 : 전북대학교 컴퓨터공학부(영상정보신기술연구센터) 교수 ghcho@chonbuk.ac.kr
[2009/10/28 투고 - 2009/11/13 심사(2010/01/12 2차 - 2010/02/17 3차) - 2010/03/26 심사완료]

사용하는 경우에 공격자(attacker)는 네트워크 트래픽을 가로 채서 쉽게 트래픽을 분석하거나 BS(Base Station)와 통신하는 송신 노드의 식별자 뿐만 아니라 노드의 위치 이동을 쉽게 알 수 있게 된다. 따라서 이동하는 센서 노드가 일상적인 감시나 특정 물체를 추적하는 환경에서 데이터를 교환하는 송신자와 수신자 이외의 제삼자가 통신 중인 송수신자의 식별자를 쉽게 구별할 수 없도록 하는 것이 매우 중요하다. 다시 말해서 네트워크를 통해 전송되는 메시지의 송수신자 ID를 익명으로 처리함으로써 공격자가 실제 ID를 알 수 없도록 하는 것이 필요하다.

기존 유선 네트워크에서 사용 중인 대부분의 사용자 익명성 기술은 무선 센서 네트워크에 그대로 적용하는 것은 시스템의 성능 관점에서 적절하지 못하다. 따라서 노드간의 전송 메시지의 실제 ID를 숨기기 위해 유선 네트워크에 사용중인 암호화 알고리즘을 사용하는 것보다 비교적 비용이 적게 들고 다소 속도가 빠른 해쉬함수를 사용하는 것이 바람직하다.

Misra et al.[7]은 클러스터기반 무선 센서 네트워크에서 메시지의 익명성과 보안성을 제공할 수 있는 구조를 제안하였다. 이들의 구조는 임의의 두 노드 간에 공유키를 생성하기 위해 Blom[8]의 구조를 사용하는 대칭키 암호화 기법과 일방향 해쉬함수를 사용한다. 하지만 특정 노드의 비밀정보가 공격자에게 노출되는 경우에, 공격자는 해당 노드가 다음 메시지에 사용될 가명뿐만 아니라 이전에 사용된 가명을 쉽게 생성할 수 있기 때문에 해당 노드가 전송한 메시지의 가명 ID에 대한 전방향 익명성뿐만 아니라 후방향 익명성이 보장되지 않는 구조이다.

Ouyang[9] 등은 중간 노드를 고려하지 않고 직접 센서노드와 BS간의 통신에 있어서 노드의 익명성을 제공하기 위해 일방향 키해쉬 체인을 기반으로 하는 구조를 제안하였다. 이들이 제안한 구조는 Misra et al.[7]이 제안한 CAS구조에서 발생하는 보안 문제점을 보완하는 방식으로서 CAS 방식처럼 고정된 임의의 매개변수를 사용하지 않고 새로운 가명을 생성할 때마다 새로운 매개변수를 사용하는 방식이다. 하지만 이들 구조에서도 그 방식에 따라 가명에 대한 전방향 익명성과 후방향 익명성이 보장되지 않는다.

따라서 비밀정보가 노출되더라도 가명에 대한 전방향 익명성과 후방향 익명성이 최대한 보장되는 메커니즘이 필요하다. 따라서 본 논문에서는 기존의 방식에서 발생한 문제점들을 개선하기 위해 전방향 키 체인과 후방향 키 체인 방식을 함께 사용하는 하이브리드 구조를 제안한다.

본 논문의 구성은 다음과 같은 순서로 구성된다. 1장의 서론에 이어서 2장에서는 관련 연구를 살펴본다. 3장과 4장에서는 센서 네트워크 환경과 메시지의 익명성 보장 프로토콜을 살펴보고, 5장에서는 안정성에 관해 기술한다. 마지막으로 6장에서는 본 논문의 결론과 향후 연구방안에 대하여 기술한다.

2. 관련연구

WSNs(Wireless Sensor Networks)에서의 보안은 지난 몇 년에 걸쳐 많은 관심을 받은 관심사였다. 분산된 센서 네트워크에서 임의의 두 노드 간에 안전한 링크의 설정을 보장하기 위해 Eschenauer[1] 등은 최초로 확률적 키 사전 분배 구조를 제안했다. 그리고 Chan[3]와 Zhu[10], Du[11] 등은 더 강한 보안성과 효율성을 지원할 수 있는 구조를 제안하였다.

Kong[12] 등은 보안이 취약한 지역에 배치된 이동 ad hoc 네트워크를 위한 익명성 on-demand 라우팅 프로토콜을 제안하였다. Wadaa[6] 등은 네트워크 가상 하부구조의 익명성을 유지하기 위한 에너지 효율성 프로토콜을 제안했다. 기본 시스템과 클러스터 구조, 라우팅 구조가 네트워크 초기화 단계에서 외부 공격자에게 알려지지 않도록 통신을 랜덤화하는 구조를 정의했다. Mehta[4] 등은 전역 도청이 가능한 환경에서 위치 프라이버

시 보장 문제를 정의하고 프라이버시를 보장하는데 요구되는 통신 오버헤드에 대해 기술했다.

Misra et al.[7]은 클러스터기반 무선 센서 네트워크에서 메시지의 익명성과 보안성을 제공할 수 있는 SAS(Simple Anonymity Scheme)과 CAS (Cryptographic Anonymity Scheme)를 제안하였다. 이들의 구조는 대칭키 암호화 기법과 일방향 해쉬함수를 사용한다. SAS는 각 노드가 자신이 사용할 가명 풀(pseudonyms pool)을 관리하고 메시지를 전송할 때는 풀에서 가명을 임의로 선택하여 사용하는 방식이고, CAS는 통신하고자 하는 두 노드 간에 공유하는 비밀키와 일방향 해쉬 함수를 사용하여 가명을 생성하는 방식이다. CAS 방식에서 클러스터 내의 멤버간의 사용될 비밀키를 생성하기 위해 Blom[8]구조를 사용한다. 그리고 각 노드와 BS간에 교환되는 메시지의 가명을 생성하는데 사용되는 비밀키와 임의의 매개변수 등과 같은 비밀정보가 절대적으로 안전하다는 가정을 두고 있다. 그들이 제안한 구조의 장점은 클러스터내의 다른 노드들이 악의 있는 공격자에 의해 공모(compromise)되었다고 하더라도 공모되지 않는 노드들 간의 전달되는 메시지의 실제 ID를 알아내는 것은 매우 어렵다는 것이다. 하지만 특정 노드의 비밀 정보가 공격자에게 노출되는 경우에, 공격자는 해당 노드가 다음 메시지에 사용될 가명뿐만 아니라 이전에 사용된 가명을 쉽게 생성할 수 있기 때문에 해당 노드가 전송한 메시지의 가명 ID에 대한 전방향 익명성뿐만 아니라 후방향 익명성이 보장되지 않는 구조이다. 무선 센서 네트워크에서 더 강한 익명성을 보장하기 위해 Ouyang et al.[9]은 HIR(Hashing based ID Randomization)과 RHIR(Reverse Hashing ID Randomization)라는 두 가지 방식을 제안하였다. 이들이 제안한 구조는 Misra et al.[7]이 제안한 CAS구조에서 발생하는 보안 문제점을 보완하는 방식으로서 CAS 방식처럼 고정된 임의의 매개변수를 사용하지 않고 새로운 가명을 생성할 때마다 새로운 매개변수를 사용하는 방식이다. 하지만 이들 구조에서도 그 방식에 따라 가명에 대한 전방향 익명성과 후방향 익명성이 보장되지 않는다. HIR에서는 가명을 생성할 때 전방향 키 체인의 값과 비밀키를 사용한다. 따라서 비밀키가 노출되는 경우에 노출된 이후의 메시지에 사용될 가명을 쉽게 생성할 수 있기 때문에 전방향 비밀성이 보장되지 않는다. RHIR에서는 후방향 키 체인의 값과 비밀키를 사용하기 때문에 비밀키가 노출되는 경우에 노출된 이후의 메시지에 사용될 가명은 생성할 수는 없지만 이전에 사용한 가명은 쉽게 생성할 수 있게 된다. 하지만 본 논문에서는 기존의 구조에서 발생하는 보안 문제들을 보완하기 위해 대칭키 암호화 기법과 전방향 해쉬함수와 후방향 해쉬함수를 동시에 적용하는 구조를 제안한다.

3. 센서 네트워크 환경

3.1 센서 노드 (SN : Sensor Node)

각 노드들은 물리적인 접근이 불가능하고 적(adversary)에게 쉽게 노출되는 지역에 배치되어 자신의 위치나 민감한 데이터를 수집하여 BS에게 전달하는 역할을 수행한다. 최근 들어 센서 노드에서의 기술이 발달되어 많은 양의 데이터를 저장하고 다소 복잡한 알고리즘을 수행하는 능력을 가지고 있다.

3.2 클러스터 헤드 (CH : Cluster Head)

WSNs의 기술은 특정 지역에 센서 노드들을 배치하여 운용하는 소규모 환경에서 차츰 대규모 분산 WSNs 환경으로 변해가는 실정이다. 이러한 환경에서 데이터 군집화(aggregation)를 효율적으로 수행하고 통신비용을 줄이기 위해서는 노드들을 클러스터로 그룹화하는 방식이 필요하다[7]. 따라서 본 논문에서 가정하는 환경에서 CH는 클러스터 내의 센서 노드들 중에서 선택된 노드로서 자신의 멤버들과 메시지를 교환하고, 데이터

군집화를 수행한 다음에 BS 방향에 있는 상위 노드(다른 CH나 BS)에게 메시지를 전달하는 역할을 수행한다. 그리고 BS로부터 수신한 메시지를 하위 노드에게 전달하는 역할을 수행한다.

3.3 BS(Base Station)

유선 네트워크에 연결되어 있거나 독립 시스템인 고성능 컴퓨터로 가정한다. BS는 모든 센서 노드들 간에 사용될 비밀정보를 관리하고 메시지의 익명성뿐만 아니라 다양한 보안 서비스를 수행한다. 새로운 가명을 생성하는데 사용되는 일방향 해쉬함수를 관리하는데 이 함수는 BS를 포함한 모든 노드들이 사전에 공유하는 것으로 가정한다.

4. 메시지의 익명성 보장 프로토콜

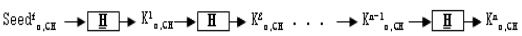
4.1 키 분배 단계

본 논문에서는 익명성을 위한 보안서비스 이외의 다른 내용은 제안한 구조의 내용에 벗어나기 때문에 언급하지 않는다. 기본적으로 각 노드는 BS에게 익명성이 보장된 데이터를 전송하기 위해서는 사전 약속이 필요하다. BS는 각 센서 노드가 자신에게 데이터를 보낼 경우에 사용될 비밀정보를 해당 위치에 배치되기 전에 각 노드에게 분배한다. 예를 들어 특정 노드를 u라고 할 경우에, BS는 인접노드와 비밀키를 생성하는데 사용될 비밀정보와 가명을 생성하는데 사용될 정보 $Seed^{f}_{u,BS}$, k개의 후방향 해쉬 함수의 출력값 ($BK^{i}_{u,BS}$, i=1, ..., k), 후방향 해쉬함수에 적용된 인덱스 값(t)을 각 센서 노드에게 안전한 채널을 통해 분배한다. 여기에서 비밀정보와 $Seed^{f}_{u,BS}$, $BK^{i}_{u,BS}$, t는 각 노드마다 다른 값을 갖게 된다.

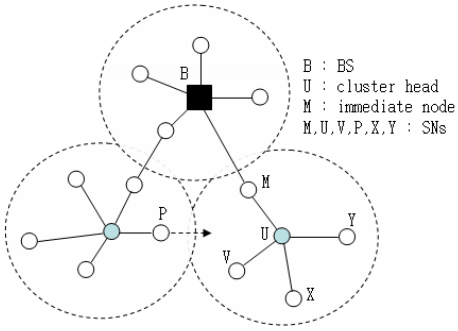
노드 BS가 노드 u에게 분배하는 비밀정보 $Seed^{f}_{u,BS}$는 실제 ID_u를 이용한 $H(ID_u)$가 아닌 임의의 난수이며, $BK^{i}_{u,BS}$는 $BK^{1}_{u,BS}(= H'(Seed^{b}_{u,BS} \oplus Seed^{f}_{u,BS}))$, $BK^{2}_{u,BS}(= H'(BK^{1}_{u,BS} \oplus BK^{n-1}_{u,BS}))$, ..., $BK^{k-1}_{u,BS}(= H'(BK^{k}_{u,BS} \oplus BK^{n-k}_{u,BS}))$에 의해서 생성되는 비밀정보 리스트이다. 여기에서 $Seed^{b}_{u,BS}$는 BS만이 알고 있는 난수이다. 그리고 해쉬함수(H')는 BS만이 알고 있기 때문에 특정 해쉬 결과 값을 알고 있더라도 그 다음에 생성되는 값을 쉽게 계산할 수 없다.

4.2 초기화 단계

각 센서 노드들은 해당위치에 배치되어 클러스터를 구성하게 되고, 특정 한 노드는 (그림 1)과 같이 클러스터 헤드 노드가 된다. 노드 CH(예, U)는 클러스터내의 멤버 노드들로부터 데이터를 수집하고 처리하여 상위 노드에게 전달하거나 상위 노드로부터 받은 메시지를 하위 노드에게 전달하는 역할을 수행한다. 이러한 처리를 원활하게 수행하기 위하여 노드 CH는 멤버 노드 중에서 상위의 노드를 Up-node로, 하위 노드를 Down-node로 지정한다. Up-node는 BS로의 메시지 전송 경로의 중간 노드이고, Down-node는 수집된 데이터를 중계하거나 수신할 하위 노드로서 하위 레벨에 있는 클러스터의 CH도 포함된다. 그리고 각 노드는 자신의 CH 노드와 익명성이 보장된 메시지를 교환하기 위해 안전한 채널을 통해 비밀정보($Seed^{f}_{u,CH}$)를 교환한다. 노드 u와 CH간에 실제 메시지를 전송할 때는 아래와 같은 방식으로 가명을 생성한다.



그리고 노드 CH는 자신의 멤버들과 안전한 통신을 하는데 필요한 비밀정보들을 저장하는 테이블을 관리한다. 표 1은 그림 1의 노드 U가 관리하는 테이블을 나타낸 것이다.



(그림 1) 클러스터로 구성된 센서 네트워크

(표 1) 클러스터 테이블(예, 노드 U)

가 명	링크	$index_c$
$H^3(sV)$	Down	3
$H^4(sX)$	Down	4
$H^2(sY)$	Down	2
$H^3(sM)$	Up	3

멤버 노드 V와 X, Y, M은 CH와 익명성이 보장되는 메시지를 교환하기 위해 안전한 채널을 통해 비밀정보 sV와 sX, sY, sM을 교환한다. 멤버 노드가 메시지를 전달할 때는 비밀정보를 이용하여 생성한 가명을 사용하여 전송한다. 예를 들어, 표 1에서 노드 X가 CH에게 네 번째 메시지를 전송할 때 사용되는 가명이다. 즉, 가명 $H^4(sX)$는 H(H(H(H(sX))))에 의해 생성된다. 그리고 멤버 노드로부터 메시지를 수신 CH는 메시지내의 가명 ID와 자신의 클러스터 테이블의 가명과 일치하는 것이 있는지를 검색하여 같은 것이 존재하면 수신하고 그렇지 않으면 폐기한다.

헤드 노드가 아닌 중간 노드 역시 Up-node와 Down-node를 위한 정보를 관리한다. 표 2는 그림 1의 노드 M이 관리하는 정보이고, 표 3은 멤버 노드 Y가 관리는 정보이다.

(표 2) 노드 테이블 M

가 명	링크	indexM
$H^2(sU)$	Down	2
$H^3(sBS)$	Up	3

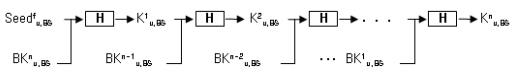
(표 3) 멤버 노드 테이블(예, 노드 Y)

가 명	링크	index
$H^3(sU)$	Up	3

4.3 메시지 전송 단계

센서 노드가 BS에 바로 인접해 있으면 중간 노드(CH나 게이트웨이 노드)를 통하지 않고 수집된 데이터를 직접 전송하면 되지만, 그렇지 않은 경우에는 중간 노드를 통해 전달되어야 한다. 이 절에서는 센서 노드와 BS간에 사용되는 가명을 생성하는 과정을 기술하고, 수집된 데이터가 중간 노드를 거쳐 BS에게 전달되는 과정을 기술한다.

새로운 가명을 생성하는데 사용되는 비밀키는 센서 노드의 계산 능력을 감안하여 일방향 해쉬 함수(H)를 사용한다. 각 센서들이 메시지를 전송할 때마다 자신의 식별자를 익명으로 보내기 위해 그림 2와 같이 BS로부터 받은 키 정보를 이용하여 가명을 생성한다. 기존의 논문[1,7] 등에서는 가명을 생성하는데 사용되는 비밀키가 고정된 반면에 본 논문에서는 가명을 생성할 때마다 새로운 비밀키를 이용한다.



(그림 2) 가명 생성 과정

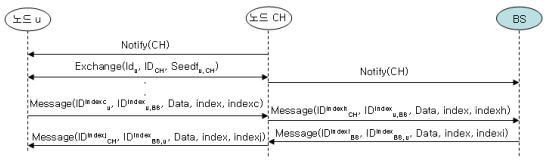
예를 들어, 특정 노드가 처음으로 메시지를 전송할 경우에 송신자 $ID^1_{u,BS}$는 $H(Seed^f_{u,BS} \oplus BK^n_{u,BS})$에 의해 생성되고, 그 다음 메시지의 가명 $ID^2_{u,BS}$은 $H(ID^1_{u,BS} \oplus BK^{n-1}_{u,BS})$에 의해 생성된다. 그리고 새로운 가명을 생성한 다음에는 즉시 입력으로 사용되는 정보들은 모두 폐기한다. 따라서 공개된 해쉬 함수 H와 비밀정보 $ID^1_{u,BS}$가 공격자에게 노출되더라도 후진 키 정보 $BK^{n-1}_{u,BS}$를 모르는 경우에는 새로운 가명 $ID^2_{u,BS}$ $(=H(ID^1_{u,BS} \oplus K^{n-1}_{u,BS}))$를 생성하는 것은 거의 불가능하다.

각 센서 노드가 특정 지역에 배치된 후에 노드들은 현재의 위치정보와 수집된 데이터를 BS나

다른 노드에게 전송하기 위해 사용되는 메시지 형식은 그림 3과 같다.

(그림 3) SN으로부터 BS에게 전송되는 메시지 형식

ID^{indexc}_{u}는 클러스터 멤버(u)의 로컬 가명이고, $ID^{indexc}_{u,BS}$는 BS만이 알 수 있는 송신자(u)의 글로벌 가명이다. Data는 노드가 수집한 데이터로서 암호화된 내용이며, MAC은 $H(BK^{n\text{-}index}_{u,BS} \oplus Data)$이다. 그리고 index와 $index_c$는 각각 로컬 가명 ID와 글로벌 가명 ID를 계산하는데 해쉬함수가 적용된 횟수를 나타낸다. 클러스터화된 센서 네트워크에서 노드 u가 메시지를 전달하고 수신하는 과정을 그림 4와 같다.



(그림 4) 연결설정과 메시지 전달과정

■ 클러스터 멤버(u)

[경우1] 센서 노드 u가 수집된 데이터가 있으면 M = {$ID^{indexc}_{u,CH}$, $ID^{index}_{u,BS}$, Data, MAC, index, $index_c$}를 상위 노드에게 전송한다.

[경우2] 상위 노드로부터 수신한 메시지의 수신자가 자신이 관리하고 있는 테이블의 ID와 일치하면 받아들이고 그렇지 않으면 수신된 메시지를 폐기한다.

[경우3] 자신(u)이 CH의 조건을 만족하면 인접 노드들과 비밀정보를 교환하고 클러스터 테이블을 관리한다.

[경우4] 그 외에는 휴식상태로 간다.

■ 클러스터 헤드(CH)

[절차1] 메시지를 수신하면 자신이 관리하는 클러스터 테이블의 첫 번째 필드에 있는 해쉬 함수 값($ID^{indexc}_{u,BS}$)과 비교하여 일치하는 것이 있는지 검색한다. 일치하는 것이 있으면 해당 링크 필드의 값이 Down인지 Up인지를 확인하고 아래 [경우 1]과 [경우 2]중 하나를 수행한다. 그렇지 않으면 수신된 메시지를 폐기한다.

[Down 노드인 경우1]
수정된 메시지 {$ID^{indexCH}_{CH,BS}$, $ID^{index}_{u,BS}$, Data, MAC, index, $index_{CH}$}를 상위 노드에 전달한다.

[Up 노드인 경우2]
수정된 메시지 {$ID^{indexCH'}_{u,CH}$, $ID^{index'}_{u,BS}$, Data', MAC', index', $index_{CH'}$}를 하위 노드에 전달한다.

[절차 2] 그 외에는 휴식상태로 간다.

■ BS(Base Station)

각 센서 노드들로부터 수신한 메시지들의 실제 ID를 알아내기 위해 그림 2와 같은 절차를 수행하여 가명에 대한 실제 ID를 생성한다.

5. 안전성과 성능 분석

본 절에서는 본 논문에서 제안한 구조에 대한 익명성 분석과 기억장소와 계산비용에 대해 기술한다.

5.1 익명성 분석

Misra et al.[7]의 구조와 Ouyang et al.[1]의 구조 등에서 해쉬함수가 정당한 노드들뿐만 아니라 공격자에게도 공개되지만 가명을 생성하는데 사용되는 비밀키가 공격자에게 노출되지 않는다는 가정 하에서는 메시지의 익명성은 보장된다. 하지만 익명성이 보장되지 않는 경우는 (1) 클러스터내의 한 노드 또는 두 노드를 제외한 모든 노드들이 공격자에게 공모되었을(compromised) 경우 (2) 가명

을 생성하는데 사용되는 비밀키가 공격자에게 노출되는 경우이다. 표 4는 비밀키가 노출된 경우에 제안된 구조와 기존 구조들에서 메시지 익명성의 보장여부를 나타낸 것이다.

(표 4) 익명성 보장

구 분	CAS[7]	HIR[1]	RHIR[1]	제안된 구조
전방향 익명성	×	×	○	○
후방향 익명성	×	×	×	○

첫 번째 경우는 최악으로써, 공모되지 않는 두 노드가 메시지를 전송할 때마다 새로운 가명을 사용한다고 하더라도 공격자는 전송되는 메시지들의 송신자나 수신자를 쉽게 추측할 수 있다. 다시 말해서 메시지를 교환하는 두 노드의 실명은 알 수 없지만 연속적으로 전송되고 있는 메시지의 송신자나 수신자를 확인할 수 있다. 두 번째는 우연적이거나 적극적인 공격에 의해서 공격자가 비밀키를 알아내는 경우로서, 공격자는 그 비밀키를 사용하여 전송중인 메시지의 송신자나 수신자를 알아내거나 정당한 노드로 가장하여 시스템을 공격할 수 있다. 특정 메시지에 사용되는 가명을 생성하는데 사용되는 비밀키를 알아내는 방법은 해쉬함수에 그 이전 메시지에 사용된 가명과 임의의 값을 적용한 다음 출력된 값과 해당 메시지의 가명과의 관계를 비교하는 것이다. 하지만 비밀키의 길이가 K비트인 경우를 가정했을 때 특정 비트 스트림이 실제 비밀키와 같을 확률은 $1/2^K$이다. 따라서 이전 메시지의 가명과 비밀키를 사용한 해쉬함수의 출력 값과 해당 메시지의 가명과의 관계를 밝혀내기 위해 2^K번의 연산을 수행해야 한다. 일반적으로 한 메시지에는 두 개의 가명(ID^{index}_u, $ID^{index'}_v$)을 사용하는데 이들 가명에 사용되는 비밀키를 알아내기 위해서는 2×2^K번의 연산을 수행해야 한다. 게다가 기존의 구조들과 달리 본 논문에서 제안한 구조는 가명을 생성하기 위해 해쉬함수를 두 번 사용하기 때문에 $2\times2\times2^K$번의 연산이 필요하다. 예를 들어, K가 32인 경우는 $2\times2\times2^{32}$번, K가 64인 $2\times2\times2^{64}$번의 연산을 수행해야 한다. 그리고 skipjack[13]을 사용하여 64비트 블록 암호를 생성하는데 걸리는 시간이 약 0.42㎳라고 가정한 경우에 비밀키를 알아내는데 $2\times2\times2^{64}\times0.42$㎳의 시간이 소요되기 때문에 정해진 시간 내에 원하는 비밀키를 알아낸다는 것은 매우 어렵다. 따라서 본 논문에서 제안한 구조는 기존의 구조들에 비해 더 강한 익명성이 보장된다.

5.2 기억장소와 계산 비용

이 절에서는 각 노드들 간에 익명성이 보장된 메시지 교환을 위해 각 노드에서 필요한 기억공간과 계산 비용을 기존의 구조들과 비교분석한다. 모든 노드는 조건에 따라서 CH(클러스터헤드)가 될 수 있다. 그리고 CH는 클러스터내의 멤버뿐만 아니라 인접 클러스터의 CH와 통신을 한다. 따라서 클러스터의 최대 크기(최대 멤버 수)는 S라고 하고, 하나의 가명을 표현하기 위해 K비트가 사용된다고 가정한다.

제안된 구조와 기존의 구조들에 있어서 필요한 기억공간은 표 5와 같다. 먼저, 각 노드 u는 BS와 익명성 통신을 하기 위해 비밀정보($Seed^f_{u,BS}$)와 n개의 비밀키($BK^n_{u,BS}$), 인덱스가필요하다. 그리고 CH가 클러스터 헤드인 경우에 클러스터의 멤버(예, 노드 v)와 통신하기 위해 비밀정보($Seed^f_{u,v}$)와 비밀키($BK^n_{u,v}$), 인덱스가 필요하고, 인접 클러스터의 노드 CH'와 통신하기 위해서는 비밀정보($Seed^f_{u,CH'}$)와 비밀키($BK^n_{u,CH'}$), 인덱스가 필요하다. 또한 CH가 멤버들에게 방송 통신을 하기 위해서는 ($Seed^f_u$)와 비밀키(K^n_u), 인덱스가 필요하다. 따라서 한 노드가 익명성 통신을 위해 필요한 전체 기억공간은 2K+nK+3SK+3SK+3K = 5K+nK+6SK이다. 예를 들어, 전체 센서 노드가 10000개이고, 클러스터의 크기가 1000, 비밀키(후진키)가 5000, 가명 공간이 8바이트인 경우에, 각 노드가 필요한 기억공간은 5×8B+5000×8B+6×1000×8B = 88,040B ≒ 88KB 이다. 반면에 CAS[7]은 필요한 기억 공간이 약 56KB이고, HIR[1]은 약 48KB이다.

(표 5) 한 노드가 필요한 기억공간과 계산비용

구 분	CAS[7]	HIR[1]	RHIR[1]	제안된 구조
기억공간	6K + 7SK	6K + 6SK	5K + nK + 6SK	5K + nK + 6SK
계산비용	2T + O(1)	2T + O(1)	2T + O(1)	3T + O(1)

한 노드가 메시지를 전송하기 위해서는 송신자와 수신자의 가명이 필요하고, 메시지를 수신하기 위해서는 메시지의 수신자가 자신인지를 비교하는 연산이 필요하다. 따라서 가명을 생성하는데 필요한 해쉬계산 비용과 수신자 확인을 위한 비교연산 비용은 표 5와 같다. 여기에서 T는 해쉬함수를 1번 수행하는 시간을 나타낸다. skipjack[13]을 사용하여 64비트 블록 암호를 생성하는데 걸리는 시간이 0.42㎳이하이고 비교연산을 수행하는데 걸리는 시간을 $O(1)$로 가정한 경우에, 기존의 구조에서는 약 0.84㎳+$O(1)$이하의 시간이 소요되고, 제안된 구조에서는 약 1.26㎳+$O(1)$이하의 시간이 소요된다.

따라서 위에서 기술한 바와 같이 제안된 구조에서 필요한 기억공간과 계산 시간은 64비트 블록 암호를 사용하는 mica mote 등과 같은 센서 노드에서 충분히 사용가능하다고 판단된다.

6. 결 론

본 논문은 센서 네트워크에서 노드의 익명성이 보장되는 프로토콜을 제안하였다. 각 노드 간에 교환되는 메시지의 가명을 생성하는데 사용되는 비밀키와 현재의 가명 ID 등과 같은 비밀정보의 일부가 공격자에 노출되었다고 하더라도 해당 노드가 다음 메시지에 사용될 새로운 가명뿐만 아니라 이전에 사용된 가명을 쉽게 생성할 수 없도록 하는 구조이다. 기존의 연구에서는 가명으로 사용될 정보를 전방향 해쉬함수 또는 후방향 해쉬함수의 결과 값을 사용하였지만 본 논문에서 제안한 구조는 두 방식을 혼합한 구조이다. 따라서 그 성능과 기억장소 활용도면에서 기존의 방식들에 비해 떨어지지만 현재의 ID를 생성하는데 사용되는 비밀키가 노출되더라도 메시지의 가명에 대한 전방향 익명성과 후방향 익명성이 강하게 보장되는 구조이다. 향후 필요한 연구 과제는 실제 무선 센서 네트워크 환경에서 제안된 기술을 구현하는 것이다.

참 고 문 헌

[1] L. Eschenauer, and V. D. Gligor, "A Key-management Scheme for Distributed Sensor Networks," in Proc. on 9th ACM Conference on Computer and Communications Security, pp.41-47, 2002.

[2] T. Kim, K. Wang, and K. Cho, "A Secure Key Agreement Scheme in Low-energy Wireless Sensor Networks," Lecture Notes in Computer Science 4096(EUC 2006), pp.78-88, 2006.

[3] H. Chan, A. Perrig, and D. Song, "Random Key Pre-distribution Schemes for Sensor Networks," in Proc. on IEEE Symposium on Research in Security and Privacy, May, 11-14, pp.197-213, 2003.

[4] K. Mehta, D. liu, and M. Wright "Location Privacy In Sensor Networks Against A Global Eavesdropper," in Proc. on IEEE Conference on Network Protocols (ICNP 2007), 2007.

[5] Y. Hu and H. J. Wang, " A Framework for Location Privacy in Wireless Networks," in Proc. on ACM SIGCOMM Asia Workshop 2005, April 12-14, 2005.

[6] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, " On Anonymity in Wireless Sensor Networks," in Proc. on Tenth International Conference of Parallel and Distributed Systems," 2004.

[7] S. Misra and G. Xue, "Efficient Anonymity Schemes for clustered Wireless Sensor

Networks," International Journal of Sensor Networks, vol. 1, no. 1/2, pp.50-63, 2006.

[8] R. Blom, "An Optimal Class of Symmetric Key Generation System," Advances in Cryptology: in Proc. on EUROCRYPT 84, lecture Notes in Computer Science, Springer-Verlag, pp.335-338, 1985.

[9] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, S. Zhang, J. Ford, and F. Makedon, "Providing Anonymity in Wireless Sensor Networks," in Proc. on 10th Conference on Parallel and Distributed Systems (ICPADS 2004), 7-9. July 2004.

[10] S. Zhu, S. Setia, and S. Jajodia, "Establishing Pairwise Keys for Secure Communication in Ad Hoc Networks: A probabilistic Approach," in Proc. on 11th IEEE International Conference on Network Protocols (ICNP'03), pp.1-10, 2003.

[11] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," in Proc. on ACM Conference on Computer and Communications Security (CCS'03) pp.42-51, 2003.

[12] J. Kong and X. Hong, "ANODR: ANonymous On Demand Rounting with Untraceable routes for mobile ad-hoc networks," in Proc. on 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp.291-302, 2003.

[13] C. Karlof, N. Sastry and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," Second International Conference on Embedded Networked Sensor Systems, SenSys'04, Baltimore, MD, pp.162-175, 2004.

◐ 저 자 소 개 ◑

이 중 현

1994년 전북대학교 산림자원학과 졸업(학사)
2001년 전북대학교 대학원 컴퓨터정보학과 졸업(이학석사)
2009년 전북대학교 대학원 정보보호공학과 수료
2004년 ~ 현재 전북도청 홍보기획과(인터넷홍보)
관심분야 : 센터네트워크, 시스템&네트워크 보안
E-mail : leejh0926@korea.kr

김 태 연

1983년 전남대학교 계산통계학과 졸업(학사)
1988년 전남대학교 대학원 전산통계학과 졸업(이학석사)
1996년 전남대학교 대학원 전산통계학과 졸업(이학박사)
1996년 ~ 현재 서남대학교 컴퓨터정보통신학과 조교수
관심분야 : 네트워크 보안, 이동 컴퓨팅, 센서 네트워크
E-mail : kimcopper@naver.com

조 기 환

1985년 전남대학교 계산통계학과 졸업(학사)
1987년 서울대학교 대학원 전산통계학과 졸업(이학석사)
1996년 Newcastle 대학교 대학원 전산학과 졸업(이학박사)
1987년 ~ 1997년 한국전자통신연구원 선임연구원
1997년 ~ 1999년 목포대학교 컴퓨터과학과 전임강사
1999년 ~ 현재 전북대학교 컴퓨터공학부(영상정보신기술연구센터) 교수
관심분야 : 이동컴퓨팅, 무선 네트워크 보안, 센서 네트워크, 차량안전통신
E-mail : ghcho@chonbuk.ac.kr