韓國 컴퓨터情報學會 論文誌
第11卷 第1號, 2006. 3.

2006-11-1-2-4

유비쿼터스 네트워크에서 저 전력 센서노드의 익명성

김동명*, 우성희**, 이상호***

Anonymity for Low-Power Sensor Node in Ubiquitous Network

Dong-Myung Kim*, Sung-Hee Woo**, Sang-Ho Lee***

요 약

유비쿼터스 네트워크 통신에서 각 센서는 저 전력과 초경량으로 인해 여러 가지 제한을 가지므로 그동안 센서의 특성을 고려한 여러 가지 연구가 진행되어 왔다. 본 논문에서는 센서노드의 신분정보의 노출을 최소화하기 위하여 alias를 사용함으로써 등록과 인증을 수행하는 과정을 개선하고 익명성을 제고하는 방법을 제안하였다. 등록과 인증과정에서 센서노드의 제한된 기능을 고려하여 RA(Relay Agent)를 도입하였고 SM(Service Manager)로부터 alias를 부여받아 각 센서노드의 신분정보의 익명성을 개선하였다. 센서노드의 개인 정보는 등록 및 인증과정은 물론 node간의 통신과정에서 안전한 보안이 보장되었으며, 계산 량 및 보안성 분석결과 센서노드의 계산 량 증가 없이 RA, SM의 연산 량 일부증가 만으로 보안수준이 향상되었음을 확인하였다.

Abstract

The sensors in a ubiquitous network are limited because of the low power and ultra light weight, so many studies have revolved around the sensor. This study improves the process of the registration and authorization and suggests a way to minimize discloser of privacy by using an alias. We introduce RA(Relay Agent) for the restrict function of sensor node, and improve anonymity for private information of each sensor node by assigning alias from SM(Service Manager) in procedure of registration and authentication. The privacy of sensor node is secure in procedure of registration, authentication, and communication between nodes. We could improve the level of security with the only partial increment of computation power of RA and SM without an increase in the amount of sensor nodes.

▸ Keyword : 유비쿼터스 네트워크(Ubiquitous Network), 프라이버시(Privacy), 익명성(Anonymity), 보안(Security), 저 전력 센서노드(Low Power Sensor Node), 별명(Alias)

• 제1저자 : 김동명
• 접수일 : 2006.03.05, 심사완료일 : 2006.03.21
* 충북대학교 대학원 전자계산학과 박사수료, ** 충주대학교 전기전자 및 정보공학부 부교수,
*** 충북대학교 전기전자컴퓨터공학부 교수

Ⅰ. 서 론

유비쿼터스 센서네트워크는 사용자주변의 주변기기가 통신을 가능하게 함으로써 자율적으로 정보를 수집하고 관리하는 구성요소로 설치 및 사용이 용이하고 비용이 적게 든다는 장점이 있어 제반 자동화는 물론 군사 및 의료 목적으로도 그 활용이 늘어나고 있다.

센서네트워크는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저 전력의 센서들로 구성된 환경으로 센서노드는 제한된 배터리로 전력을 공급받으며 데이터 처리능력과 단거리 무선 통신이 가능하며 Smart Dust, WINS등 센서 네트워크의 응용분야가 넓어지면서 정보 들을 신뢰하고 동시에 개인의 프라이버시를 보장 받을 수 있도록 하기 위한 센서노드의 보안성은 매우 중요하게 연구되고 있다. 센서네트워크에서 높은 안전성을 제공하기 위해 많은 계산으로 적은 전력을 한없이 소비한다면 센서노드에 매우 부적절하다고 할 수 있다. 따라서 이런 유비쿼터스 환경에서 센서노드간의 안전한 통신을 위해서는 노드의 등록과 인증을 정해진 절차와 과정이 필요하며 노드의 하드웨어적인 구성은 물론 키의 생성 및 인증과 통신방법 등 다양하게 연구되어 왔다 [1~5].

본 논문은 유비쿼터스 네트워크에서 통신을 위해 alias를 사용함으로써 센서노드의 개인정보를 보호하고 센서의 특성을 고려한 효율적인 통신방법을 제안하였다. 기 제안된 프로토콜에서의 RM, AM을 합하여 Relay Agent(RA) 로 통합 하고 서버 및 각 노드와의 통신을 담당하여 노드간의 중계기능은 삭제함으로써 노드의 저 전력, 저 성능의 특성을 고려하였다[3].

본 논문 2장에서 주제에 관련된 연구내용을 분석하였으며 3장에서는 사용된 통신 및 알고리즘을 분석하였다. 또한 4장에서 제안된 알고리즘의 우수성을 분석하였다.

Ⅱ. 관련 연구

2.1 Chaum 의 MIX Channel

MIX의 개념을 추적 불가능한 email의 송수신을 위하여 처음 소개되어 이동통신망에 적용될 수 있도록 변형하였다 [6~7]. MIX 채널은 송신자와 수신자 사이에 라우터역할을 수행하는 채널로 MIX 채널에 입력된 메시지 M은 랜덤 값 R이 추가되어 공개키인 암호화 되어 address A로 전송되어지고 다음과 같이 개인키로 복호화 된다.

K1(R1, Ka(R0, M), A)—> Ka(R0, M), A.
각 메시지는 MIX 채널에서 중첩되어 암호화되므로 각 메시지는

Kn(Rn, K<n-1>(R<n-1>, ... , K2(R2, K1(R1, Ka(R0, M), A))...))
로 생성되어 다음단계에서는

K<n-1>(R<n-1>, ... , K2(R2, K1(R1, Ka(R0, M), A))...)
의 형태로 채널에 따라 전달된다.

송수신자 사이에 일종의 라우터 역할을 하는 MIX 체인을 생성하여 체인내의 모든 관련자가 암호화에 참여하도록 하여 최소한 하나의 MIX만 정직하다면 메시지의 보안을 유지할 수 있는 장점이 있으나 송수신에 많은 부하가 따르고 과정에 일부 MIX의 중단이 발생하는 경우 전체기능이 무력화되는 단점이 있으나 경로가 짧은 경우 보안성 향상을 위해서 사용이 가능하다.

2.2 Varying ID

Varying ID의 개념은 센서노드의 저 전력을 고려하여 연산방식으로 hash function을 사용하였고 센서네트워크에서 ID를 통신 할 때 마다 Random No.를 통해 센서노드의 익명성을 강화하였으며, message 전송 시 serial No.를 사용하여 중간에 비 인가된 사용자의 개입을 차단하였다 [8]. 따라서 각 센서노드에서 필요한 필드는

- 센서의 ID: ID
- Transaction Number: TN
- 최종 송신완료 TN: LSN
- 기타 필요항목

따라서 데이터베이스의 필드도 위 내용이 포함되며 센서노드와 서버의 통신에서 TN, LSN 의 차이인 dTN 을 전송함으로써 공격자의 개입을 인지하도록 하였다.

2.3 추적불가능성(Untraceability)

프라이버시의 요구수준은 제공되는 서비스의 내용이나 투입되는 비용 등 다양한 요소에 따라 결정되며 프라이버시의 요구수준을 2차원 매트릭스의 형태로 표현하였다. 매트릭스의 열은 프라이버시의 객체로 프라이버시의 노출될 수 있는 피해 대상자이며, 행은 개인정보에 접근하는 주체로 이동네트워크 사용자의 경우 사용자, 홈 도메인, 원격도메인을 각각 f, h, r로 표현하였다[9~10].

객체는 H(Home Domain), R(Remote Domain), L (Legitimate Network Entities), E(Eavesdropper) 로 구분하였으며 각 셀의 내용은 접근 가능한 경우 1, 로 접근 불가능한 경우 0으로 표시하였다. 가장 기본적인 GSM 모바일 통신에서 TMSI(Temporary Mobile System Identifiers) 의 경우 <표 1>과 같이 다음의 형식으로 표현 가능하다.

표 1. TMSI 의 보안 맵
Table 1. Security Map of TMSI

	H	R	L	E
f	1	1	1	0
h	1	1	1	1
r	1	1	1	1

따라서 전체적인 보안의 수준을 5단계로 구분하여 각 주체가 객체에 접근가능한지 여부를 분석하였다. <표 2>의 기준에 의하면 TMSI는 Class 1의 보안수준을 만족하고 있다.

표 2. Asokan 의 보안수준
Table 2. Security level of Asokan

단계	설 명
Class1	Hiding User Identity from Eavesdropper
Class2	Hiding User Identity from Foreign Authorities
Class3	Hiding Home Domain Identity from Third parties
Class4	Hiding Home Domain Identity from Foreign Authorities
Class5	Hiding User Behavior from Eavesdropper

2.4 [RM-AM] 모델

저 전력으로 인한 센서노드의 짧은 동작기간을 보완하기 위하여 RM(Register Manager), AM(Authentification Manager)를 도입하여 센서노드의 등록과 인증에 필요한 기능을 대행토록 함으로써 노드의 계산 량을 최소화하는 알고리즘을 제안하였다[4~5].

이때 RM, AM은 각자의 제한된 데이터베이스를 유지하며 센서노드 및 Manager 간의 통신은 전송거리가 짧은 노드의 통신알고리즘인 hop-by-hop 방식으로 처리하였다.

III. 프로토콜 설계

3.1 센서노드의 구성 및 통신

시스템은 (그림 1) 같이 센서노드(Sensor Node), RA (Relay Agent)와 SM(Service Manager)으로 구성된다. 센서노드는 MCU와 센서 인터페이스 및 RF모듈이 탑재되며 저 전력 으로 최소한도의 계산능력과 기억기능을 가진다. 센서간의 통신은 무선으로 이루어지며 hop-by-hop 방식으로 통신이 이루어진다.

센서 중 계산능력과 통신능력이 우수한 노드를 RA라 칭하며 하나의 RA는 50개 이내의 센서노드 및 SM과의 중계기능을 담당한다. 또한 RA는 서버와의 중간에 위치하여 서버와의 통신 및 암호화를 통한 중계를 담당한다.

SM은 데이터베이스를 가지고 노드 및 RA에 대한 제반 정보를 관리하며 신뢰할 수 있는 개체이다. SM은 노드의 ID 및 PW를 가지고 있으며 RA의 공개키를 보유하고 있다.

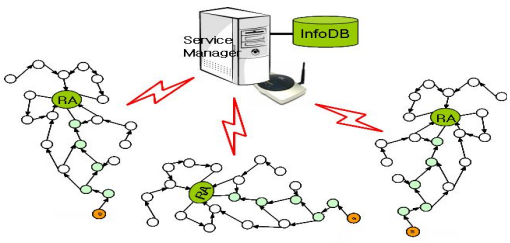

그림 1. 노드의 구성
Fig 1. Structure of Nodes

3.2 요구사항

노드는 제한된 기능을 고려하여 통신과정에서는 XOR 연산을 사용한다. 저 전력 센서노드 중간에 통신과 계산능력이 우수한 RA를 설정 하였다. RA와 SM간의 통신은 대칭키를 사용 한다. 약 50개 내외의 센서노드에 RA 1개가 존재한다고 가정하였고 RA는 SM과의 중계 및 키 분배와 통신을 담당하며 SM은 데이터베이스를 활용하여 RA를 통하여 노드 간의 통신정보를 관리한다.

[4]에서 RM과 AM을 사용하는 저 전력 알고리즘을 실험하여 설계의 우수함을 증명하였다. 본 논문에서는 RM, AM을 RA로 통합하여 단순한 중계 기능을 가지도록 현실화하였으며 노드는 최소기능의 계산 및 기억 기능을 가지도록 설정하였다. 따라서 RM, AM 이 각자 가졌던 DB를 SM만이 가지는 것으로 변경하였다.

통신은 각 노드의 ID를 사용하지 않고 alias를 사용하도록 변경하였으며 통신 방식을 Node→RA→SM의 과정을 거치도록 변환하였다.

다른 노드는 물론 중간의 RA는 통신 노드의 개인정보를 보호하여 은폐하였으며 알고리즘을 등록 및 인증으로 구분하여 기술하였다. 각 과정에서 메시지의 반복 송신을 방지하기 위하여 Time stamp를 사용하였다. 본 제안 알고리즘에 사용된 기호는 <표 3>과 같다.

표 3. 알고리즘에 사용된 기호
Table 3. Algorithm Symbols

표 기	설 명
ID_A	A의 ID
PW_A	A의Password
TS_A	A의 Time stamp
PrK_{RAi}	RAi의 개인 키
PuK_{RAi}	RAi의 공개 키
SK_{AB}	A, B 의 세션 키
$Alias_A$	A의 alias
M_{SM}	SM 의 메시지

노드간의 통신을 위해서 등록과 인증의 과정이 필요하며 각 과정의 처리내용은 다음과 같다.

3.3 등록 알고리즘

초기에 각 노드는 ID와 PW만을 가지고 등록을 시작한다. 각 노드의 등록을 위한 과정은
(그림 2)와 같이 진행된다.

(1) 각 노드는 등록을 위하여 자신의 ID와 PW를 XOR한 값과 Time stamp를 RA 에 송신한다. TS는 Time stamp 로 메시지의 복제를 방지하기 위하여 생성 후 전송하며 최종적으로 alias를 수신한 경우 이를 확인하기 위하여 사용한다.

$$Node \rightarrow RA: f((ID_A \,||\, PW_A), TS_A)$$

(2) Ra 는 노드로 부터 수신내용을 자신의 개인키로 암호화하여 SM에 송신한다.

$$RA \rightarrow SM: F((f(ID_A \,||\, PW_A), TS_A), PrK_{RAi})$$

(3) SM 은 수신한 블록을 RA의 공개키로 복호하여 노드로 부터 전송내용을 추출하고 제반 정보는 Database에 저장한다. SM은 생성한 alias를 노드의 PW로 hash 하고 다시 RA의 공개키로 암호화하여 RA에 전송한다.

$$SM \rightarrow DB: ID_A, PW_A, TS_A$$
$$SM \rightarrow RA: F((ID_A, M_{SM}, TS_A)||PW_A), PuK_{RAi})$$

(4) RA는 수신한 메시지 블록을 자신의 개인키로 복호화하여 결과를 노드에 전송한다. 이때 RA는 노드의 PW를 알 수 없기 때문에 노드에 전송되는 정보를 알지 못한다.

$$RA \rightarrow Node: ((ID_A, M_{SM}, TS_A)||PW_A)$$

(5) 노드는 수신한 메시지 블록을 PW로 XOR하여 자신의 ID 및 등록 확인 메시지인 MSM을 수신하며 TSA 를 통하여 메시지의 공정성을 확인한다.

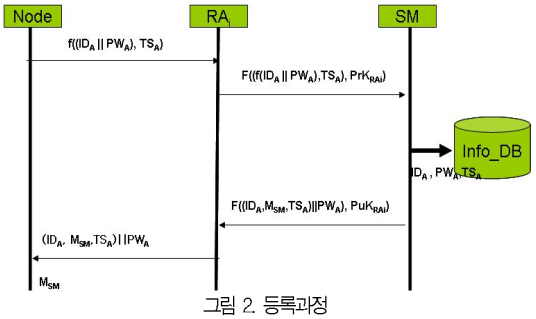

그림 2. 등록과정
Fig 2. Registration Procedure

3.4 인증 알고리즘

등록을 마친 노드는 다른 노드와의 통신이 필요한 경우 인증이 필요하며 통신을 위한 세션 키가 필요하다. 각 노드는 서버에 접속하여 세션 키와 함께 통신에 ID를 대신하여 사용할 alias를 발급받으며 alias 및 세션 키는 매 통신 개시 전에 발급된다.

다른 노드와의 통신을 원하는 노드가 서버에 세션 키를 받는 과정은 (그림 3)과 같다.

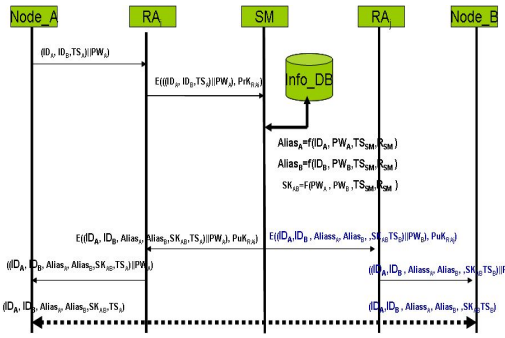

그림 3. 인증과정
Fig 3. Authorization Procedure

(1) 각 노드는 통신을 위한 인증신호를 소속한 RA에 자신 및 통신상대 노드의 ID를 TS와 함께 전송한다.

Node→RA: $((ID_A, ID_B, TS_A)||PW_A)$

(2) 이를 수신한 RA는 자신의 비밀 키로 암호화하여 이를 서버에 전달한다.

RA→SM: $E(((ID_A, ID_B, TS_A)||PW_A), PrK_{RAi})$

(3) 서버는 수신한 자료를 RA의 공개키로 복호화하고 노드 A의 PW로 XOR 하여 ID 및 TS를 얻는다.

SM: $D(E((ID_A, ID_B, TS_A)||PW_A), PubK_{RA}) \rightarrow ID_A, ID_B, TS_A$

(4) 서버는 Database를 조회하여 노드 A, 노드 B에 대한 등록정보를 검색하고 이를 자료로 alias 및 세션 키를 생성한다. 생성된 자료를 먼저 노드의 PW로 XOR한 후 각각 통신대상자가 속한 RA에 각 RA의 공개키로 암호화 하여 전송한다.

SM→DB: ID_A, ID_B

$Alias_A=f(ID_A, PW_A, TS_{SM}, R_{SM})$

$Alias_B=f(ID_B, PW_B, TS_{SM}, R_{SM})$

$SK_{AB}=F(PW_A, PW_B, TS_{SM}, R_{SM}),)$

SM→RAi: $F(((ID_A, ID_B, SK_{AB}, Alias_A, Alias_B, TS_A)||PW_A), PuK_{RAi})$

SM→RAj: $F(((ID_A, ID_B, SK_{AB}, Alias_A, Alias_B, TS_B)||PW_B), PuK_{RAj})$

전송되는 자료를 RA의 공개키로 암호화함으로써 다른 RA가 수신한 경우에도 그 내용을 알 수 없으며 전송내용은 수신하는 노드의 PW로 XOR되어 있어 결과적으로 SM과 노드 간에 MIX 채널이 형성된다.

(5) 이를 수신한 RA는 자신의 개인키로 수신한 자료를 복호화 하여 해당 노드에 전송한다.

RAi→ Node A: $((ID_A, ID_B, SK_{AB}, Alias_A, Alias_B, TS_A)||PW_A)$
RAj→ Node B: $((ID_A, ID_B, SK_{AB}, Alias_A, Alias_B, TS_B)||PW_B)$

이때 복호한 자료는 각 노드의 Password로 함수 화 되어 있으므로 각 RA는 해당 노드 및 노드에 전송되는 내용을 알 수 없다.

(6) 자료를 수신한 노드는 자신의 PW로 RA로 부터 전송된 자료를 복호하여 통신대상자의 ID, alias 및 세션 키를 얻는다.

Node A, B: ID_A, ID_B, SK_{AB}, $Alias_A$, $Alias_B$

이때 PW를 모르는 다른 노드는 자료를 전송해도 복호화가 불가능하므로 세션 키를 알 수 없으며 인증을 신청한 노드는 복호화한 후 TS를 확인함으로써 자료에 대한 인증을 통해 정당성을 확인할 수 있게 된다. 또한 수신한 alias 와 세션 키를 이용하여 통신을 수행하게 되므로 불법적인 사용자가 통신과정에서 메시지를 채팅해도 세션 키를 모르면 내용을 알 수 없다. 또한 내용이 해석되어도 통신대상자의 alias 만 노출되므로 해당 alias 의 ID는 알 수 없기 때문에 통신대상자의 신분정보가 보호된다.

Ⅳ. 성능 분석

정보자산의 위험은 정성적, 정량적 및 체크 리스트 방법에 의하여 분석이 가능하다[11]. 본 논문에서는 센서노드의 저 전력으로 인한 기능을 단순화하고 보안성을 제고시키기 위하여 RA를 도입하였고, 센서노드의 통신과정에서 세션키 와 함께 ID 대신 alias를 사용토록 함으로써 노드의 익명성을 구현하였다. 이 과정에서 필요한 계산 량과 보안성을 체크리스트 방법에 의해서 분석하면 다음과 같다.

4.1 계산 량

등록 및 연산과정에서 발생되는 계산 량을 <표 4>와 같이 분석하였다.

계산 량 측면에서는 전체적으로 증가한다. 이는 전송과정에서 암·복호화에 필요한 계산 량 이므로 연산은 RA 및 SM에서 발생되어 등록과 인증과정에서 각각 1회씩 일어나게 되어 통신과정에서의 누진적인 부하가 발생하지 않게 된다. 다만 등록 및 인증과정에서 센서노드의 XOR 연산이 1회씩 증가하나 전체적인 성능에 영향을 미치지 않는다.

표 4. 알고리즘의 계산 량 분석
Table 4. Calculation Amounts of the algorithm

		RIM-AM논문	제안논문
등록	Node(XOR)	1	2
	RA	1	2
	SM	1	2
	transfer	3	5
인증	Node(XOR)	1	2
	RA	2	2
	SM	1	3
	transfer	11	7

결과적으로 센서노드의 부담을 최소화하고 보안성을 향상시키기 위해서 필요한 연산을 RA나 SM에 전가시킴으로 시스템 전체의 부하 부담 없이 필요로 하는 보안목표를 달성할 수 있게 되었다.

4.2 보안성

가장 보편적으로 사용되고 있는 GSM TMSI의 경우 가장 기본적인 보안성이 보장되므로 <표 5의 (a)>와 같은 보안 맵으로 표현된다.

[4] 논문에서는 신뢰성 있는 내부 사용자(F)를 가정하였으므로 <표 5의 (b)>와 같이 외부사용자 및 접근 자에 대하여는 보안이 보장되나 내부 사용자 및 관리자에 대하여는 보안상 취약성을 가지게 된다. 그러나 본 제안논문의 경우 내부 노드의 전송 내역 및 ID를 등록한 후 alias를 사용하여 통신이 이루어지고 SA에서 각 노드 간 사실적인 터널링이 이루어짐으로 중간 Agent 인 RA에게 노드의 정보가 누출되지 않음으로 SA만이 신뢰성 있는 관리자로 간주되어 완전한 익명성이 보장되므로 맵은 (c) 와 같은 도표로 표현될 수 있다.

표 5. 알고리즘의 보안수준 비교
Table 5. Comparison of the algorithm security level

	H	R	L	E
f	1	1	1	0
h	1	1	1	1
r	1	1	1	1

(a) TMSI-GSM Mobil

	H	R	L	E
f	1	0	0	0
h	1	1	1	1
r	1	0	0	0

(b) RIM-AM논문

	H	R	L	E
f	1	0	0	0
h	1	0	0	0
r	1	0	0	0

(c) 제안논문

따라서 alias를 사용함으로써 센서노드의 부하 부담 없이 센서의 익명성을 보장하고 외부 및 내부관련자의 보안성을 향상시켜 [9]의 기준으로 [4]에서는 Class 3의 보안수준을 가지며 본 논문에서는 Class 5의 보안수준을 유지할 수 있게 된다. 위의 제안내용을 다음의 여러 형태의 공격에 대하여 보안측면에서 분석하면 다음과 같다.

공격자가 노드를 사용했던 정보를 획득하여 재사용 공격(Replay Attack)을 시도하는 경우 SM의 인증단계에서 TS를 예측할 수 없기 때문에 안전하며 공격자가 정당한 사용자인 노드로 위장하여 위장 공격(Impersonation Attack)으로 SM을 속이고자 하는 경우에는 alias에 해당하는 PW 및 TS를 알아야 하기 때문에 불가능하다. 또한 n명의 RA가 공모하여 alias를 알고자 하는 공모 공격(Conspiracy Attack)의 경우 각 노드의 PW로 XOR 연산

이 필요하므로 PW의 길이에 따라 추론에 필요한 연산시간이 소모되므로 사실상 이 문제를 푸는 것은 방지되며 통신에 참여한 RA가 수신 여부를 부인하는 경우 전송된 내용은 해당 RA의 개인키로 암호화 또는 복호화 되어야 전송이 가능하므로 부인방지의 효과가 있다.

V. 결론

유비쿼터스 센서네트워크는 그 특성상 제한된 처리능력 및 에너지를 가지고 있어 특성에 맞는 통신 방식이 필요하다. 최근 개인정보를 보장 받을 수 있는 안전한 통신방식에 대한 연구가 절실히 필요한 실정이다. 따라서 본 논문은 저 전력의 센서네트워크의 센서에 alias를 할당하고 통신 가능 거리가 단거리임을 고려한 안전한 통신 방식을 제안하였으며 성능 면에서 기존의 연구와 비교하였다.

센서노드의 소형화 경량화에 따른 연산기능의 제한과 저 전력을 고려하여 노드의 연산 및 통신량을 최소화 하기 위해 RA를 도입하였다. 다른 노드와의 통신을 위하여 ID 대신 SM으로 부터 세션마다 부여받는 alias를 사용함으로써 불법 사용자가 통신 및 수신 메시지를 채팅한다하여도 신분정보가 보호되며 간단한 XOR 연산을 통해서 등록 및 인증과정에서 내부 이용자에게도 신분정보에 대한 보안을 유지할 수 있도록 설정하였다.

결과적으로 노드의 연산 및 통신부하를 최소화하면서 각 노드의 신분정보가 2단계 상승함으로써 전체시스템의 연산 및 통신량의 부담 없이 신분 및 통신보안기능의 향상이 되었다.

따라서 위의 알고리즘은 센서노드 이외에 송수신 노드의 신분정보 보호가 필요한 다양한 연구 분야에서 응용이 가능하다고 사려 된다.

앞으로 SM이 신뢰하지 못할 경우에 대한 MIX channel 적용 방향제시와 위 알고리즘에 연산 시간을 고려한 분석 모델을 적용함으로써 계산 시간에 대한 비교분석이 연구되어야 할 것이다.

참고문헌

[1] MD. Abdul Hamid & Prof. Choong Seon Hong, “Location Privacy and Authentication for Low-cost Sensor Node Devices Using Varying Identifiers”, 한국컴퓨터종합학술대회2005논문집, Vol. 32, pp.412-414, 2005

[2] 정윤수, 이영진, 황윤철, 이상호, “유비쿼터스 환경에서 프라이버시를 보장하는 인증 프로토콜”, 한국통신학회 추계학술지, Vol.32, 2005

[3] 김동명, 조영복, 이상호, “유비쿼터스 센서 망 에서의 계층적 그룹 키 생성방안”, 한국정보보호학회 동계학술발표 논문집 Vol.14, pp.281-284, 2004

[4] Y.B. Cho, D.M. Kim, S.H. Lee, “Mutual Authentication Protocol Using a Low-Power in the Ubiquitous Computing Environment”, International Symposium on Remote Sensing ISRS 2004, pp.91-94, 2004

[5] 조영복, 정윤수, 김동명, 이상호, “유비쿼터스 센서네트워크에서의 저 전력 상호 인증 프로토콜”, 한국컴퓨터정보학회논문지, pp. 187-197, 2005

[6] D. Chaum, “Security Without Identification: Transaction Systems to Make Big Brother Obsolete”, Communications of the ACM, Vol. 28, pp.1030-1044, Oct. 1985

[7] David Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, Vol. 24, Feb. 1981

[8] M. A. Hamid, C. S. Hong, “Location Privacy and Authentication for Low-Cost Sensor Node Devices Using Varying Identifiers”, 한국컴퓨터종합학술대회2005, Vol 32, pp.412-414, 2005

[9] D. Samfat, R. Molva, N. Asokan, “Untraceability in Mobile Networks”, Proceedings of the ACM International Conference on Mobile Computing and Networking, Berkeley, Nov. 1995

[10] N. Asokan, “Anonymity in a Mobile Computing Environment”, Proceedings of the Workshop on Mobile Computing Systems and Applications, Santa Cruz, Dec. 1994

[11] 김강, 박진섭, 김봉희, “정보시스템 보안을 위한 위험 분석 모델”, 한국컴퓨터정보학회 논문지, pp.60-67, 2002

저 자 소 개

김 동 명

2005. 2 충북대학교 전자계산학과 박사과정 수료

2002. 3 대덕대학 평생교육원 전임교수

우 성 희

2006. 3 ~ 현재 : 충주대학교 전기전자 및 정보공학부 부교수

95. 9 ~ 2006. 2 청주과학대학 컴퓨터과학과 부교수

1992. 2 충북대 전자계산학 이학박사

이 상 호

1989. 2 숭실대학교 대학원 전자계산학과 공학박사

1981. 3 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수