韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-2-7

신용모델 기반의 경량 상호인증 설계

김 홍 섭*, 조 진 기**, 이 상 호***

A Design of Lightweight Mutual Authentication Based on Trust Model

Hong-Seop Kim*, Jin-Ki Cho**, Sang-Ho Lee***

요 약

유비쿼터스 센서 네트워크(USN)는 유비쿼터스 환경을 위한 핵심 기술이다. USN은 센서 정보의 도청, 비 정상적인 패킷의 유통, 데이터 위·변조 및 서비스 거부 공격 등과 같은 다양한 공격의 취약성이 존재하며 이에 대한 대책이 요구된다. 특히, USN은 배터리 용량 및 연산능력이 제한된 한정된 자원하에서 운용되어야 하는 제약 사항을 지니고 있다. 이로 인하여 USN 보안 기술은 저 전력 소모 및 최소 연산량을 유지하기 위한 경량화된 설계가 반드시 필요하다. 본 논문에서는 위의 문제를 해결하기 위해 신용모델(trust model)에 기반한 경량화된 USN 상호인증 방법을 제안한다. 제안된 인증 모델은 주관 논리 모델로 표현되는 신용정보를 기초로 하여 센서노드들을 인증하기 때문에 계산량을 줄일 수 있다. 따라서 배터리 소모를 줄일 수 있으며 결과적으로 센서노드의 생존 기간 연장이 가능하다.

Abstract

Ubiquitous Sensor Network(USN) is the very core of a technology for the Ubiquitous environments. There is the weakness from various security attacks such that tapping of sensor informations, flowing of abnormal packets, data modification and Denial of Service(DoS) etc. And it's required counterplan with them. Especially, it's restricted by the capacity of battery and computing. By reasons of theses, positively, USN security technology needs the lightweighted design for the low electric energy and the minimum computing. In this paper, we propose lightweight USN mutual authentication methology based on trust model to solve above problems. The proposed authentication model can minimize the measure of computing because it authenticates the sensor nodes based on trust information represented by subjective logic model. So it can economize battery consumption and resultingly increse the lifetime of sensor nodes.

▸ Keyword : USN, 상호인증(Mutual Authentication), 신용모델(Trust Model)

• 제1저자 : 김홍섭
• 접수일 : 2005.06.24, 심사완료일 : 2005.07.12
* 충북대학교 대학원 전자계산학과 박사과정 (청주 주성대학 컴퓨터프로그래밍과 부교수)
** 충북대학교 대학원 전자계산학과 박사과정 (부산경상대학 멀티미디어컴퓨터과 조교수)
*** 충북대학교 전기전자컴퓨터공학부 교수

Ⅰ. 서 론

오늘날의 네트워크 환경은 무선망(wireless network)에 대한 관심 및 보급이 폭발적으로 증대되고 있다. 특히, 최근에는 제록스(Xerox) 팔로 알토 연구소의 마크 와이저 박사가 제안한 유비쿼터스 컴퓨팅(Ubiquitous computing)의 개념[1]이 새롭게 대두되어 지구촌 도처에 산재된 수많은 크고 작은 다양한 컴퓨터 시스템을 유·무선망으로 통합 연결하여 언제 어디서나 다양한 장비로 이들을 접속해 정보를 얻고 공유할 수 있는 기술에 대한 다양한 연구를 활발히 진행 중에 있다.

유비쿼터스 환경을 구현하는 핵심 기술중 하나는 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network:USN)이다. USN 기술은 RFID(Radio Frequency IDdentification)와 같은 전자태그 및 센서(sensor)장치들을 사물, 생명체 또는 주변 환경에 부착하여 수집된 인식 정보를 기초로 주변의 각종 상황정보를 탐지하여 실시간으로 이를 관리하기 위한 기술이다[2]. 이러한 USN 기술은 비상대응정보관리, 에너지관리분야, 의료모니터링, 군수물류, 재고관리, 전투지역 관리 등과 같은 민·관·군 다양한 분야에 응용할 수 있다[1].

USN은 "첫째, 센서노드의 수가 수십에서 수만 개까지 응용분야에 따라 가변적이다.", "둘째, 망의 일부 구성요소의 장애가 전체 망에 영향을 주어서는 안된다.", "셋째, 망의 형태(topology)가 극히 가변적이다.", "넷째, 구성되는 센서노드는 배터리 용량, 처리, 저장 및 통신기능에 제한이 있다." 등과 같은 제약사항이 존재한다. 특히 배터리 용량 및 컴퓨팅 파워가 제한되는 제약사항을 해결하기 위한 저전력 소비 구조의 설계는 USN 관련 기술 개발에 반드시 필요한 방향이 된다.

이같이 USN 기술은 가까운 장래에 국내·외적으로 널리 사용될 기술이며 이에 대한 그동안 연구는 주로 USN 서비스의 구성 및 라우팅과 같은 기본 동작 등에 대한 연구 개발 중심으로 진행되어 왔으며 보안분야에 대한 연구는 상대적으로 많이 결여되어 왔다.

하지만 USN은 센서 정보의 도청, 비 정상적인 패킷의 흐름, 데이터 위·변조 및 서비스 거부 공격 등과 같은 다양한 공격에 취약하며 이에 대한 대책이 요구된다 [3].

특히, USN은 배터리 용량 및 연산능력이 제한된 한정된 자원하에서 운용되어야 하는 환경적인 제약 사항을 지니고 있다. 이러한 환경적인 요인으로 인하여 USN을 지원하기 위한 보안 기술은 저 전력 소모 및 최소의 연산량을 유지하는 측면에서 경량화된 설계가 반드시 필요하다.

이에 대하여, 본 논문에서는 신용모델(trust model)에 기반한 USN 환경하에서의 구성 센서노드 상호간의 경량화된 상호인증 방법을 제안하며 논문의 구성은 다음과 같다. 제 2 장에서는 USN 보안과 관계된 기존 연구동향을 고찰한다. 제 3 장에서는 신용모델의 표현기법을 고찰한다. 제 4 장에서는 신용모델에 기반한 USN의 경량화된 상호인증 방법을 제안한다. 마지막 제 5 장에서는 결론을 맺는다.

Ⅱ. 관련연구

이 장에서는 USN 보안 요구사항, USN을 위해 기존에 제안된 인증방식 및 신용모델에 기반한 연구동향을 고찰한다.

2.1 USN의 보안 요구사항

일반적으로 USN의 구성 센서들은 안전하지 않은 위치에 언제든지 설치될 수 있다. 이러한 환경에 놓인 각 센서노드들은 상호간에 전송되는 자료들이 방송(broadcasting)되는 과정에서 다양한 형태의 보안 공격의도를 지닌 악성노드들의 공격으로 부터 쉽게 노출 될 수 있는 사례와 같이 센서노드들의 보안 신뢰성을 보장받을 수 없다[3].

센서들의 보안의 안정성을 유지하기 위해서 비밀성(confidentiality), 상호인증(mutual authentication), 무결성(integrity), 신선성(freshness), 경량성 등이 보장 되어야 한다[4].

특히, 신선성은 기존에 이미 전송되었던 보안 정보의 재사용을 방지하기 위한 기술로서 현재 보낸 정보가 가장 최근에 보낸 정보임을 보장하기 위한 서비스이다.

USN은 서론에서 언급한 바와 같이 일반적인 컴퓨터 환경과는 달리 제한된 CPU 성능, 저장공간, 배터리 전력 등과 같은 제약 사항을 갖기 때문에 적은 연산량과 저 전력 소모 구조를 지닌 경량화된 보안구조가 필수적이다. 이에 기존 유선망에서 주로 사용되어 왔던 공개키 암호화 알고리

즘 등을 기반으로 하는 보안서비스는 현실적으로 적용하기가 어렵다[5,6]. 그리고 대부분의 USN 키 관리 및 보안 프로토콜 연구에는 대칭키 기반의 암호 방식을 이용하는 방법이 제안되고 있다.

2.2 기존 상호인증 방식

USN의 보안 기술을 지원하기 위해 제안된 연구동향은 SPINS(Security Protocols for Sensor Networks)[4], LEAP(Localized Encryption and Authentication Protocol)[7], Deng[8] 등의 연구가 있다.

2.2.1 SPINS [4]

SPINS 프로토콜은 SNEP(Secure Network Encryption Protocol)과 μTESLA(The "Micro" version of the Timed Efficient Stream Loss-tolerant Authentication)로 구성된다.

SNEP은 데이터의 기밀성과 노드 상호간의 데이터 인증 과정 및 과거에 사용된 데이터의 재사용 공격이 불가능하게 하기 위한 키 재설정에 대한 보안기능을 제공한다.

μTESLA 프로토콜은 기존 유선망에서 사용되었던 μTESLA 프로토콜을 변형하여 센서망에 적합하게 설계된 인증 프로토콜이며 키를 알고있는 노드에 의해 해석이 가능한 대칭키 기반의 인증방식을 제공한다. μTESLA는 노드 상호간에 공유하는 비밀키의 노출을 최대한 늦추어 주는 기능을 제공하여 비 대칭키 방식을 사용하는 효과를 나타낼 수 있다. 하지만 인증 대상이 되는 노드의 수가 증가할 경우 지연시간이 길어져서 활용이 어렵고, 노드 상호간 시간의 동기화가 필요한 단점을 지닌다.

2.2.2 LEAP [7]

LEAP는 단일키를 사용하는 구조로는 대량 노드들로 구성된 대규모 센서망의 안전한 키 관리 구조 설계가 불가능한 문제를 해결하기 위해 제안되었다.

LEAP는 4개의 암호 키와 키 설정 프로토콜로 구성되는데 암호키는 베이스스테이션(Base Station:BS)과 공유하는 개인키, 망에 존재하는 모든 노드와 공유하는 방송키, 센서노드 상호간의 공유하는 Pairwise 키 및 클러스터를 구성하는 이웃 노드 상호간에 공유하는 클러스터 키로 구성된다.

이 방법은 4개의 암호키를 사용하여 개인키 유출방지, 이웃한 센서노드의 인증 및 방송과정 중에 송수신되는 메시지의 유출 방지가 가능하며 이에 따른 USN의 생존성을 극대화 할 수 있는 장점을 지닌다. 하지만 경량성은 떨어진다.

2.3 신용모델

신용(trust)의 사전적 의미는 "틀림없다고 믿음", "믿고 의심하지 않으며, 틀림없다고 믿음", "평판이 좋고 인망이 있음."으로 그 뜻을 나타내고 있다.

이러한 신용의 개념은 과거 컴퓨터 기술 분야에서 불 확신성의 표현 및 판단을 위한 기법으로 많이 연구되어 왔다. 최근에는 이러한 신용모델을 주로 전자상거래, P2P(Peer to Peer) 망 등의 보안 문제 개선을 위해 연구되어 왔다[9,10,11,12]. 최근에는 유비쿼터스 및 MANET(Mobile Ad-Hoc Network) 분야의 보안 라우팅 분야에 적용이 시도되고 있다[9,13,14,15].

노드 사이의 신용관계를 정의하기 위해서는 노드 사이의 신용도를 평가하기 위한 각 노드의 신용정보를 표현해야 되는데 이러한 신용정보의 표현 방법에는 댐스터-세이퍼(Demster-Safer)의 확률모델[16], 퍼지논리(fuzzy logic) 모델 및 확률론에 근거한 주관논리(subjective logic) 모델[17]이 존재한다.

Josang의 연구[17]에서는 현실 세계 대상들의 믿음과 불확신의 정도를 주관논리에 기반한 신용으로 표현하기 위한 모델을 제안하였다. 또한 Xiaoqi 등의 연구[13]에서는 Josang의 연구에서 제안된 신용모델을 MANET 라우팅에 적용하여 자기조직적인 경량화된 안전한 경로 확보에 적용될 수 있음을 증명하였지만, 악의적 의도를 지닌 노드의 신규 참여에 대한 인증 방법이 결여되어 있다.

III. Josang의 신용모델

이 장에서는 Josang의 연구에서 제안된 주관논리에 기반한 신용모델을 적용한 USN의 구성 노드 상호간의 신용정보를 표현하기 위한 방법을 고찰한다.

3.1 신용관계

신용관계(trust relation)는 개체 상호간의 신용정보를 설정하고 유지하는 형태를 나타내며 관계된 개체 상호간에 신용의 정도를 나타내는 신용값을 갖고 상호간의 신용관계는 직접신용(direct trust)과 간접신용(indirect trust) 관계로 정의된다.

직접신용 관계는 (그림 1(a))에서와 같이 1 홉(hop) 단위로 직접 인접한 노드 사이의 신용관계로 정의하며 인접한 노드 상호간에 상대방 노드의 신용정보를 관리하게 된다. 예를 들어, 서로 인접한 노드 A와 B가 서로 상대 노드의 신용정보를 갖고 서로를 직접 신용하는 관계를 의미한다.

간접신용 관계는 (그림 1(b))와 같이 2홉 이상 떨어진 특정 노드에 대한 신용관계를 믿을만한 제 3의 노드의 신용권고를 기초하여 정의된다. 예를 들면, 간접신용 관계는 (그림 1(b))에서 노드 A와 B는 직접 신용관계를 지니고 있는데 노드 A가 새로운 노드 C에 대한 신용정보를 확보하기 위해 C의 신용정보를 갖고 있는 인접한 이웃 노드인 B의 권고를 통하여 C에 대한 신용정보를 확보할 수 있는 관계를 의미한다.

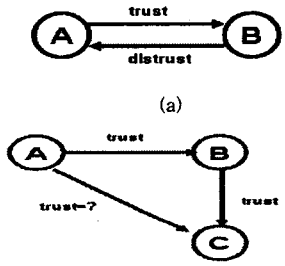

그림 1. 신용관계
Fig. 1. Trust relation

3.2 신용정보의 표현

특정 노드 x에 대한 신용정보($\omega(x)$)는 (식 1)과 같이 정의된다[17]. 여기서, $\beta(x)$는 노드 x에 대한 믿음(belief)의 정도, $\delta(x)$는 노드 x에 대한 불신(disbelief)의 정도, $\mu(x)$는 노드 x에 불확신(uncertainty)의 정도를 표현한다. 그리고 각 신용정보 구성요소들의 관계는 (그림 2)와 같다. 그리고 신용정보 구성요소의 개별적인 값은 0.0과 1.0 사이에 존재하며 구성요소 모두의 합($\beta(x)+\delta(x)+\mu(x)$)은 1이 된다[17].

$$\omega(x)=\{\beta(x),\delta(x),\mu(x)\} \quad \cdots\cdots (1)$$

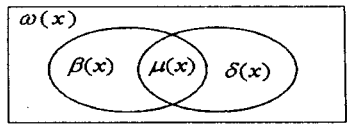

그림 2. 신용정보의 구성
Fig. 2. Configuration of trust information

3.2.1 노드 상호간의 직접 신용정보의 표현

(그림 1(a))와 같이 인접한 이웃 노드 A는 B에 대한 신용정보를 (식 2)와 같이 표현한다. (식 2)에서 β(A:B)는 노드 A의 노드 B에 대한 믿음의 정도, δ(A:B)는 노드 A의 노드 B에 대한 불신의 정도 그리고 μ(A:B)는 노드 A의 노드 B에 대한 불확신의 정도를 표현한다.

$$\omega(A:B)=\{\beta(A:B),\delta(A:B),\mu(A:B)\} \quad \cdots\cdots (2)$$

망(network)을 구성하는 각 노드들의 실제 신용정보의 계산은 통신 성공 빈도(S:Success) 및 실패 빈도(F:Fail)를 근거로 하여 (식 3)과 같이 β(A:B)는 노드 B의 통신 성공 확률, δ(A:B)는 노드 B의 통신 실패 확률, μ(A:B)는 믿음정도 및 불신의 변경빈도에 따른 확률로 표현된다. 여기서 S 값은 정상적인 통신이 이루어질 경우마다 1씩 증가되며, F 값도 비 정상적인 통신이 이루질 경우마다 1씩 증가된다.

$$\beta(A:B)=\frac{S}{S+F+\alpha},\quad \delta(A:B)=\frac{F}{S+F+\alpha},\quad \mu(A:B)=\frac{\alpha}{S+F+\alpha} \quad \cdots\cdots (3)$$

예를 들어, 노드 A와 인접한 노드 B의 통신 성공빈도(S)가 8이고, 실패빈도(F)가 6이고 믿음정도 및 불신의 변경빈도(α)가 2일 경우 β(A:B)는 0.5, δ(A:B)는 0.375, μ(A:B)는 0.125로 계산된다. 결과적으로 노드 A는 노드 B에 대한 신용정보(ω(A:B))로 {0.5, 0.375, 0.125}의 값을 얻게 되며 노드 A는 B에 대하여 믿음의 정도 50%, 불신의 정도를 37.5% 그리고 불확신의 정도를 12.5%로 표현한다.

3.2.2 신용권고를 통한 간접 신용정보의 표현

신용권고(trust recommendation)는 2 홉 이상 떨어진 노드에 대한 신용정보를 인접 이웃노드를 통하여 대상 노드에 대한 신용권고를 받아 신용정보를 취득하는 간접 신용관계이다.

신용권고는 신용정보의 조합(trust combination)에 의하여 표현된다[17]. 그리고, (그림 3)과 같이 노드 A, B, C에 대하여 ω(A:B), ω(B:C)가 결정되어 있을때 노드 A는 노드 C에 대한 신용정보를 노드 B의 신용권고를 통하여 결정한다. 신용권고는 (식 4)와 같이 정의되며, (식 4)는 다시 ω(C,A:B)≡ω(A:B)⊗ω(B:C)로 표현된다[17]. (식 4)에서 믿음의 정도(β(C,A:B)), 불신의 정도(δ(C,A:B)), 불확신의 정도(μ(C,A:B))는 (식 5)와 같이 계산된다.

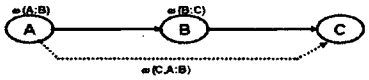

그림 3. 신용권고
Fig. 3. Trust recommendation

$$\omega(C,A:B)=\{\beta(C,A:B),\delta(C,A:B),\mu(C,A:B)\} \quad \cdots\cdots\cdots (4)$$

$$\begin{aligned}\beta(C,A:B)&=\beta(A:B)\bullet\beta(B:C)\\ \delta(C,A:B)&=\beta(A:B)\bullet\delta(B:C)\\ \mu(C,A:B)&=\delta(A:B)+\mu(A:B)+\beta(A:B)\bullet\mu(B:C)\end{aligned} \quad \cdots\cdots\cdots (5)$$

(그림 4)와 같이 노드 A가 2홉 이상의 거리에 위치한 노드 C에 대한 신용정보를 인접한 여러 이웃노드 X={$x_1, x_2, \ldots, x_n$}들로 부터 권고받을 경우에 인접된 여러 노드의 신용정보 권고안을 종합하여 합의된 신용정보를 표현하기 위해 (식 6)과 같이 정의하며 이를 합의조합(consensus combination)이라고 정의한다.

$$\omega(C,A:X)=\left(\sum_{i=1}^{n}\beta(C,A:x_i)/n,\sum_{i=1}^{n}\delta(C,A:x_i)/n,\sum_{i=1}^{n}\mu(C,A:x_i)/n\right) \quad \cdots\cdots (6)$$

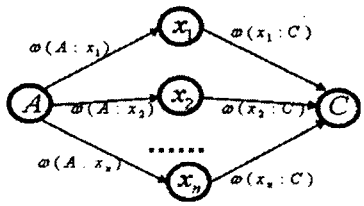

그림 4. 다수 노드의 신용권고
Fig. 4. Trust recommendation for multiple nodes

Ⅳ. 신용모델에 기반한 상호인증

이 장에서는 USN 센서노드들과 같은 그룹의 BS 노드간의 신용모델에 기반한 상호인증 방법을 제안한다.

4.1 USN 구성모델

이 논문에서 제안하는 인증방법의 기본 센서구성은 미국 버클리 대학의 CITRIS(Center for Information Technology Research in the Interest of Society)에서 제안한 스마트더스트(Smart-Dust)의 센서망(sensor network) 모델[4,5]을 (그림 5)같이 적용한다.

(그림 5)에서 센서들을 BS를 중심으로 1홉 단위로 그룹핑(grouping)하고, 각 노드들은 그룹내의 BS를 중심으로 "노드:BS", "BS:노드", "BS:그룹내의 모든 노드"들의 통신 그리고, 그룹 상호간의 "BS:BS"를 통한 통신 방식을 가정한다.

BS의 역할은 외부 센서망과의 연동 및 수 많은 그룹내 구성 노드들과의 통신, 관리기능을 수행하는데 필요한 충분한 자원을 보유하게 된다. 센서노드는 메모리 소자를 내장하고 있는 8 비트급의 마이크로프로세서를 장착하여 자체적으로 정보 수집 및 자료 처리능력(10 MIPS~50 MIPS)을 지닌 스마트 센서(smart sensor)이며 "Mote"라고도 불리운다[4].

(그림 5)에서는 2개의 통신 그룹을 정의한다. 그룹1은 BS1을 중심으로 m개의 센서노드($\{n_{11}, n_{12}, n_{13}, .., n_{1m}\}$)들로 구성되며 그룹2는 BS2을 중심으로 n개의 센서노드 ($\{n_{21}, n_{22}, n_{23}, \ldots, n_{2n}\}$)로 구성한다.

이와 같이 i번째 그룹은 임의의 j개의 센서노드 ($\{n_{i1}, n_{i2}, n_{i3}, \ldots, n_{ij}\}$)로 구성한다. 서로 다른 그룹에 소속된 센서노드의 정보는 관리 대상이 되는 센서노드가 소속된 그룹의 BS를 통하여 관리된다.

센서노드의 신용관계의 정의는 같은 그룹내의 BS와 노드 상호간은 (식 2), (식 3)의 직접신용 관계를 설정하여 인증에 활용한다. 또한 다른 그룹에 소속된 노드와의 신용관계는 (식 4), (식 5)의 간접신용 관계로 정의한다.

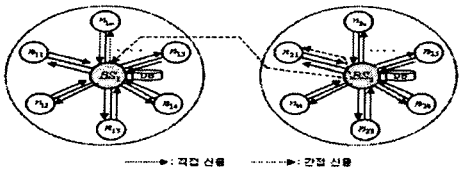

그림 5. USN의 구성
Fig. 5. Configuration of USN

4.2 신용정보의 관리

USN을 구성하는 BS 및 센서노드들은 인접한 이웃노드들의 신용정보 값을 관리하기 위해 (그림 6)과 같이 신용정보 데이터베이스를 관리한다. 신용정보 데이터베이스에는 인접된 노드의 식별자(identifier)를 관리를 관리하는 노드 ID, 인접된 이웃 노드들N={N1,N2,...,Nn}의 신용정보, 통신 성공/실패의 빈도수를 나타내는 S와 F 값, 그리고 제한시간(expire time)을 관리한다. 특히, USN 구성 노드는 높은 이동 특성 및 이에 따른 망 구성 노드의 변화가 심하므로 영구적인 인접노드의 신용정보 구성은 의미가 없어지게 된다. 이에 대한 대응 방안으로 신용정보 데이터베이스에 제한시간을 주어 인접된 노드의 신용정보가 데이터베이스에 기록되어 일정시간이 지난후에 인접노드의 존재유무를 확인한 후 대상 노드가 삭제되었을 경우 자동으로 관련된 신용정보를 재구성하기 위해 사용된다.

ID	신용정보	상태		제한시간
		S	F	
N_1	{β,δ,μ}			
.....	.....	.....	.....	.....
N_n	{β,δ,μ}			

그림 6. 신용정보데이터베이스
Fig. 6. Trust information database

4.3 신용기반 상호인증

이 절에서는 제 3 장에서 제시된 신용모델을 적용하여 (그림 5)와 같이 구성된 USN에서 센서노드들과 BS 사이의 경량화된 상호인증 방법을 제안한다.

제안하는 신용모델 기반 상호인증 과정은 BS 노드가 등록된 센서노드들의 정보를 수집하는 과정에서 매번 계산량이 많은 키 인증과정에서의 전력 소모를 줄이기 위해 앞서 3장에서 기술한 신용모델을 적용하여 센서노드와 BS 상호간의 인증과정을 수행한다.

제안하는 전체적인 인증과정은 (그림 7)과 같다. (그림 7)에서 노드 등록(Registration)은 신용모델 기반 상호인증을 수행하기 위한 전처리 과정으로 신규 센서노드가 망에 추가되거나, BS 노드에 등록되어 있지 않은 새로운 센서노드들에 대하여 BS 와 센서노드 상호간에 안전하게 설정된 대칭키 기반의 마스터키(master key) 인증을 통하여 보안 안전성을 확보하고 신용정보 초기화 과정을 수행한다. 이 과정을 통하여 모든 센서노드들의 신규 등록 초기에 마스터키 인증을 통한 초기 보안 안전성을 확보할 수 있다.

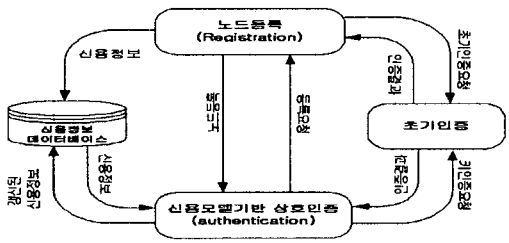

그림 7. 신용기반 상호인증
Fig. 7. Mutual authentication based on trust model

4.3.1 센서노드의 등록

이 절에서는 새로운 센서노드가 망에 참여하거나 기존 센서노드의 정보가 BS의 신용정보 데이터베이스에 존재하지 않을 경우의 인증과정을 설계한다.

등록과정에서는 신규 노드에 대한 보안 안전성을 확보하기 위해 초기인증을 (그림 8)과 같이 수행한다. 초기인증 과정은 센서노드와 BS 사이의 상호 인증을 위해 대칭키를 기반으로 하는 마스터키를 적용한다. 그리고 마스터키는 사전에 안전하게 분배되어 설정되었음을 가정한다.

(그림 8)에서 신규 센서노드가 망에 추가시 센서노드는 자신의 존재 사실을 알리기 위해 먼저 노드가 소속될 통신 그룹의 BS에게 센서노드 자신의 식별자(ID_{n_i})와 함께 "hello"라는 메시지를 생성하여 전송하고 자신의 랜덤수(R_n)을 생성한다.

이를 전달받은 BS는 연결설정을 요구하는 센서노드의 식별자에 대하여 보안 측면에서 안전한 노드인가를 식별하기 위해 자신의 랜덤수(R_b)를 생성하고 생성된 랜덤수를 센서노드와 BS 사이에 사전에 설정된 대칭키 기반의 마스터키(MK_{ij})로 암호화한 인증메시지($E_{MK_{ij}}(R_b)$)를 센서노드에게 전송한다. BS 노드로 부터 암호화된 인증메시지를 수신한 센서노드는 BS가 전송한 인증메시지를 복호화

$(D_{MK_{ij}}(E_{MK_{ij}}(R_b)))$하여 BS가 보낸 랜덤수에 1을 더하여 $R_b^{'}$를 생성하고 $R_b^{'}$와 센서노드에서 생성된 R_n을 BS와 센서노드 사이에 설정된 마스터키로 암호화$(E_{MK_{ij}}(R_b^{'}, R_n))$하고 BS에게 전송한다.

센서노드로 부터 암호화된 $R_b^{'}$, R_n을 수신한 BS는 자신의 마스터키(MK_{ij})를 사용하여 복호화하여 $R_b^{'}$과 R_b를 검증하고 검증결과 센서노드가 보낸 $R_b^{'}$의 값이 "R_b+1"의 값이면 센서노드와 BS 자신과 동일한 키를 지녔다고 판단하여 센서노드에 대하여 인증하게 된다. 그리고 다시 BS는 센서노드와의 상호인증을 위해 센서노드가 전송한 R_n 에 1을 더하여 $R_n^{'}$을 계산하고 암호화$(E_{MK_{ij}}(R_n^{'}))$하여 센서노드에게 전송한다. 센서노드는 BS가 송신한 $E_{MK_{ij}}(R_n^{'})$를 복호화하여 $R_n^{'}$과 R_n을 검증하고 검증결과 BS 노드가 보낸 $R_n^{'}$의 값이 "R_n+1"의 값이면 센서노드와 BS 노드 자신과 동일한 키를 지녔다고 판단하여 센서노드 역시 BS 노드에 대하여 인증하게 된다. 이러한 초기인증과정은 키 인증 과정에서의 에너지 소모 및 통신 부하를 줄이기 위해 센서노드가 처음 등록될때 한번만 시행하게 되며 등록이 완료된 후 센서노드들에 대한 인증은 신용기반의 경량화된 상호인증 방법을 적용한다.

표 1. 인증기호
Table 1. Authentication notation

기호	의미	비고
ID_{n_i}	i번 센서노드(N_i)의 ID	
ID_b	BS 노드의 ID	
R_n	센서노드의 랜덤수(nonce)	
R_b	BS 노드의 랜덤수(nonce)	
MK_{ij}	j번째 그룹의 BS와 같은 그룹의 i번 노드사이의 상호인증을 위한 마스터키 (Master Key)	사전 설정
{m}	메시지 단위	
$E_{MK_{ij}}(x)$	마스터키를 사용하여 x를 암호화 한다.	
$D_{MK_{ij}}(x)$	마스터키를 사용하여 암호화된 x를 복호화 한다.	
$m_1 \mid\mid m_2$	2개의 메시지 m_1, m_2를 결합한다.	

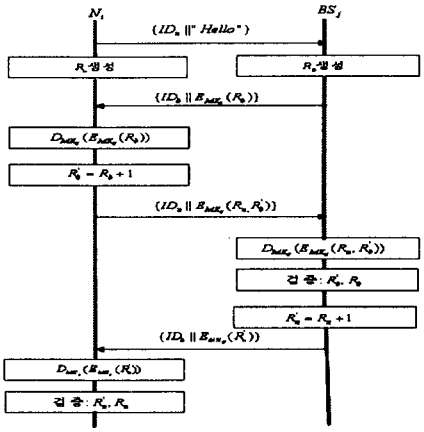

그림 8. 초기인증
Fig. 8. Early authentication

초기인증을 수행한 후 BS 노드는 초기인증의 결과를 근거로 초기 신용값을 (식 2)와 (식 3)에 의해 계산하게 된다. 초기인증이 통과된 센서노드의S=0, F=0이 되며 초기 신용정보는 "ω(BS:i)=(0,0,1)"로 계산한후 센서노드의 등록 요구를 허락(accept)한다. 초기인증이 통과되지 않은 센서노드에 대한 초기 신용값은 "ω(BS:i)=(0,1,0)"로 설정하며 센서노드의 등록 요구를 거부(reject)한다.

초기인증을 통해 등록 허용 또는 거부를 결정한후 결정된 센서노드의 신용정보를 신용정보 데이터베이스에 기록한 후 등록 절차를 종료한다.

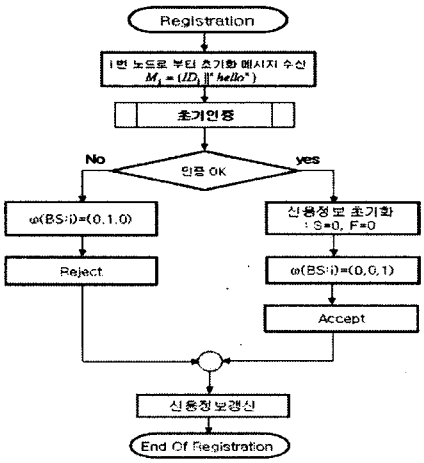

그림 9. 센서노드의 등록알고리즘
Fig. 9. Registration algorithm of sensor node

4.3.2. 신용기반 상호인증

초기등록이 끝난 센서노드들에 대해서는 계산량이 많은 대칭키 기반의 마스터키를 사용하는 센서노드의 인증 절차의 수행 횟수를 줄이기 위해 (그림 10)과 같이 센서노드 상호간의 신용정보를 기초로 인증을 수행한다.

BS 노드와 같은 그룹에 소속된 센서노드에게 각 노드가 지닌 정보(Data)를 전송하라는 명령을 방송하거나 각 센서노드가 습득된 정보를 BS 노드에게 전송하여 할 경우, 임의의 i 번째 센서노드(N_i)는 BS 노드에게 자신의 식별자(ID_{n_i})와 수집된 정보(Data)로 구성된 메시지(M_i)를 BS에게 전송한다.

센서노드로부터 메시지를 수신한 BS 노드는 먼저, 자신의 신용정보 데이터베이스에서 수신된 식별자(ID_{n_i})에 해당하는 센서노드의 신용정보가 존재하는 가를 검색하여 존재하지 않을 경우는 앞 절에서 기술한 등록과정을 수행한다.

센서노드의 신용정보가 BS의 신용정보 데이터베이스에 존재할 경우 BS는 메시지를 전송한 센서노드에 대한 경량화된 인증을 수행하기 위해 신용정보 데이터베이스에 수록된 신용정보를 검색하여 결정된 임계치(Δ:threshold)를 설정하여 〈표 2〉와 같이 인증한다. 〈표 2〉의 조건으로 인증이 수행된 후 변화된 S와 F의 값을 갖고 해당 센서노드의 인증후 (식 3)과 같이 신용정보 값을 재계산한 후 신용정보 데이터베이스를 갱신한다.

표 2. 신용 인증조건
Table 2. Trust authentication condition

신용정보			인 증 판 정
β	δ	μ	
⟩Δ			인증을 허락하고 센서노드의 정보를 수신한 후 S의 값을"S=S+1"로 변경한다.
	⟩Δ		인증을 거부하고 센서노드의 정보를 무시하고 F의 값을 "F=F+1"로 변경한다.
		⟩Δ	불확실한 노드이므로 마스터키 인증을 수행한후 인증이 성공되면 정보를 수신한 후 S의 값을 "S=S+1"로 변경시키고, 인증이 실패하면 정보를 무시하고 F의 값을 "F=F+1"로 변경한다.
≦Δ	≦Δ	≦Δ	

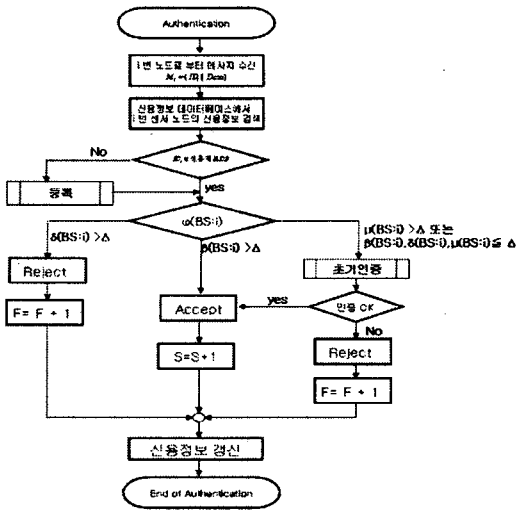

그림 10. 신용기반 상호인증 알고리즘
Fig. 10. Mutual authentication algorithm based on trust model

〈표 2〉에서 임계치는 적용되는 USN의 특성에 따라 동적으로 설정이 가능하게 제안한다.

예를 들어, BS는 등록이 안전하게 통과된 같은 그룹의 i 번 센서노드(N_i)의 직접신용정보(ω(BS:N_i))가 {0.53, 0.35, 0.12}로 결정되어 BS의 신용정보 데이터베이스에 관리하고 있고, 임계치는 0.5임을 가정한다. 이때, N_i가 BS에게 센서정보를 전송하면 BS는 (그림 10)과 같이 N_i에 대한 신용평가를 수행한 결과 믿음의 정도(β(BS:N_i))는 0.53이기 때문에 정의된 임계치(0.5)보다 크다. 그러므로 BS는 〈표 2〉의 조건에 근거하여, 마스터키 인증이 필요 없는 신용있는 노드로 판단하여 신용정보를 갱신하고 마스터키 인증 없이 믿고 N_i가 송신한 정보를 수신하게 된다. 하지만, 만일 임계치가 0.6으로 결정되어 있다면 BS는 N_i의 신용평가 결과 믿음의 정도(β(BS:N_i))는 0.53이기 때문에 정의된 임계치(0.6)보다 작다. 그러므로 〈표 2〉의 조건에 따라 마스터키 인증을 수행한 후, 마스터키 인증 결과에 따라 N_i가 송신한 정보를 BS가 안전하게 수신한다.

이와 같이, 본 장에서 제안된 신용기반 상호인증 모델에서는 설정되는 임계치에 따라 보안 요구수준 및 이에 따른 경량성 조절이 가능하다. 여기서 적용되는 임계치는 앞 3장에서 기술한 바와 같이 신용정보 구성요소의 각 요소의 값이 0.0과 1.0사이에 존재하기 때문에 이 범위 내에서 임계치의 값은 USN의 응용 분야에서 요구하는 보안 요구수준에 따라 동적으로 설정한다.

4.4 평가

이 절에서는 본 논문에서 제안한 신용모델 기반의 상호인증 모델의 보안 안전성 및 경량성 측면에서 평가 분석한다.

4.4.1 보안 안전성 분석

보안 안전성 평가에 대한 기준은 보안기술이 요구되는 분야의 비밀성, 인증, 무결성, 신선성 등과 같은 보안 요구조건을 만족하는 기능이 부여 되었는가를 주요 평가대상으로 한다[1]. 이에 본 논문에서 제안한 신용기반 상호인증 모델은 (그림 7)에서와 같이 신규 센서노드가 그룹에 추가될 경우 초기인증 과정에서 먼저 BS와 센서노드 상호간에 설정된 대칭키 기반의 마스터키를 사용하여 정당한 마스터키를 보유한 센서노드 만이 통신 그룹에 참여가 가능하므로 초기인증의 안전성 확보가 가능하며, 이를 기반으로 USN에 참여하고 있는 모든 센서노드들이 안전함을 보장할 수 있다.

제안된 신용기반 상호인증 모델은 2.1절에서 기술한 USN 보안 요구조건 중 비밀성, 상호인증, 신선성 측면에서의 보안 안전성을 다음과 같이 지원한다.

(1) 비밀성

초기인증 과정에서 BS와 센서노드 상호간에 인증을 위해 R_n과 R_b를 송·수신하는 과정에서 마스터키로 암호화하여 전송하기 때문에 BS와 센서노드 상호간의 인증메세지의 비밀보장이 가능하므로 악성 노드의 도청 공격으로부터 안전하다.

(2) 신선성

초기인증에 사용되는 랜덤수 R_n과 R_b는 초기인증이 수행될 때마다, 새롭게 무작위로 생성이 되기 때문에 재사용이 불가능하며, 이는 신선성을 지원한다.

(3) 상호인증

초기인증 단계에서 센서노드(N_i)와 j번째 그룹의 BS 상호간에 안전하게 설정된 마스터키(MK_{ij})를 보유한 대상만이 R_n과 R_b의 복호화가 가능하기 때문에 상호인증을 지원한다.

초기인증을 통과한 센서노드들은 자신이 수집한 정보를 BS에게 전송하고자 할때, 특정 수준 이상의 신용도가 높다고 판단되는 센서노드들은 매번 BS와의 마스터키 인증을 수행하지 않고, BS의 신용정보 데이터베이스에 관리되고 있는 각 센서노드의 신용정보 값을 비교하여 4.3.2절의 〈표 2〉와 같이 센서노드와 BS 사이의 신용정보 평가를 통한 상호인증을 지원한다.

4.4.2 경량성 분석

본 논문에서 제안된 신용모델 기반 인증모델은 신규 노드 등록절차의 초기인증을 통해 사전에 안전한 노드들만 USN에 참여를 허가한다. 그리고, 초기인증 과정을 통해 구성된 안전한 USN에서 구성노드 상호간의 신용정보를 평가하여 인증을 수행한다.

기존 인증분야에 적용된 방식은 주로 공개키 기반 인증방식을 적용하여 세션 키의 설정, 암호화 및 복호화, 키 생성을 위한 모듈러 연산 등과 같은 계산량이 많고 복잡한 절차를 수행해야 하며 이에 따른 전력 소모가 크다.

이에 반하여, 이 논문에서 제안된 신용기반 인증 기법은 등록과정의 초기인증에 적용되는 마스터키 인증은 대칭키 방식을 사용하기 때문에 기존 공개키 방식을 사용하는 인증방식 보다 계산량을 약 10% 정도 감소시킬 수 있다[18]. 그리고, 인증메세지의 생성과정에서 기존 인증 방식[4,7]에서는 해시(hash), 모듈러 연산 등과 같은 연산과정이 요구되지만 제안된 초기인증 방식은 인증메시지의 생성을 단순한 랜덤수 생성만을 적용하기 때문에 계산량을 줄일 수 있다.

그리고, 초기인증 이후의 상호인증 과정에서 인증시 확률에 기초한 주관논리로 표현된 신용정보 평가를 통하여 인증을 수행하기 때문에 인증 절차가 간단하며 매번 마스터키 인증을 수행하는 것 보다 계산량을 줄일 수 있다.

센서노드의 통신 참여 초기에는 초기인증을 통과한 센서노드임에도 불구하고 마스터키 인증을 수행하며 이에 따른 연산 및 이에 따른 통신 부하가 발생할 수 있다. 하지만 통신에 참여하는 센서노드의 신용정보는 통신횟수 및 관련된 인증 성공 횟수가 많아질수록 믿음의 정도는 증가하는 반면에 불확신 정도 및 불신의 정도는 상대적으로 감소된다. 이 경우 믿음 정도가 지정된 임계치 이상이 되면 마스터키 인증을 수행하지 않고 신용정보만을 갖고 인증한다.

본 논문에서 제안한 것과 같이 신용정보 만을 갖고 인증을 수행할 경우 마스터키 기반의 인증 및 기존의 인증방식 보다 장기적 측면에서 각 센서노드와 BS의 연산량이 감소하게 된다. 이점은 센서노드의 인증 과정에서의 전력 소모를 최소로 할 수 있으며 결과적으로 생존기간(lifetime)을 늘릴 수 있을 것이다.

또한, 신용정보 데이터베이스 관리 측면에서도 정보 보존 및 검색하는 과정에서의 저장 공간의 확보와 검색시간의 필요에 따른 전력 소모의 문제가 발생 가능하다. 하지만, 이점은 플레시 메모리(flash memory) 등과 같은 최신의 고속, 대용량을 지원할 수 있는 극 소형 메모리 기술을 USN 구성 노드들에게 적용하여 검색시간을 줄일 수 있으며 이에 따른 노드들의 전력소모를 경량화 시킬 수 있다.

V. 결론

서론에서 살펴본 바와 같이 USN은 배터리 용량 및 연산 능력이 제한된 한정된 자원하에서 운용되어야 하는 환경적인 요인으로 인하여 USN을 지원하기 위한 보안 기술은 경량화된 설계가 반드시 필요하다.

특히, 기존 네트워크에서 지원되는 인증 기술 대부분이 공개키 기반으로 되어 있어서 연산의 복잡성 및 이에 따른 전력 소모율이 많기 때문에 경량성이 요구되는 USN에 적용하기에는 부적합하다.

이에 대하여, 본 논문에서는 신용모델에 기반한 경량화된 USN 상호인증 모델을 제안하였다. 이 논문에서 제안된 신용기반 상호인증은 "등록", "초기인증", "신용기반 상호인증" 과정으로 설계하였다.

등록과정은 신규 센서노드에 대한 자기조직적 USN 접속 기능을 제공하며 이 과정을 통하여 신규 센서노드와 BS 사이의 대칭키 기반의 마스터키를 사용한 상호인증을 수행한 후 인증된 센서노드에 대해서만 USN에 참여할 수 있게 한다.

초기인증 과정에서 BS와 센서노드사이의 상호인증을 위해 대칭키 기반의 마스터키를 사용하며 마스터키는 사전에 안전하게 설정되었음을 가정한다. 이 과정은 악성 센서노드가 거짓 신용정보를 생성하고 이를 사용하여 인증을 통과하여 USN 보안 안전성을 침해하는 것을 사전에 막고 인증의 경량성을 유지하기 위해 신규 센서노드의 USN 추가 참여 요구가 존재하거나 또는 신용기반 인증 과정중 특정 센서노드의 신용정보 값이 임계치 이하일 경우 보안 안전성 검증에 사용한다.

신용기반 상호인증 모델은 등록과정을 통하여 초기 보안 안전성이 확보된 센서노드들에 대하여 BS와 센서노드 상호간에 통신이 일어날 경우 데이터를 전송한 센서노드가 얼마나 믿을 수 있는 대상인가를 인증하기 위해 본 논문 제 3장에서 기술한 Josang의 신용모델에 기초하여 설계하였다. 설계된 신용기반 인증모델은 기존의 연산량이 많고 절차가 복잡한 공개키 기반의 인증 기법을 적용하지 않고 주관논리에 기초한[17] 신용정보를 계산하고 이를 비교하여 인증하기 때문에 인증 과정의 연산량 및 절차를 줄일 수 있으며 이에 따른 경량성을 높일 수 있다. 이점은 센서노드의 한정된 배터리 소모를 줄일 수 있으며 결과적으로 센서노드의 생존 기간 연장이 가능하다.

본 논문에서는 같은 USN 그룹내의 BS와 센서노드 상호간의 직접 신용 인증만을 고려하였지만 만일 다른 그룹에 소속된 센서노드에 대하여 인증하기 위해서는 제 3장에서 제시된 간접신용모델을 적용하여 인증이 가능하다. 하지만 제안된 방법은 센서노드들만의 자기조직적 특성을 지닌 신용기반 상호인증 방법 및 방대한 지역에 분포된 센서노드들의 신용 인증을 효율적으로 수행하기 위한 모델 확장을 필요로 한다. 또한 본 연구에서는 이미 초기인증이 안전하게 통과되고 신용정보가 기준치 이상인 BS에 등록된 센서노드들 중에서도 ID 위장 공격에 대한 신용정보 인증에 대한 과정이 미흡하며 이에 대한 확장이 요구된다.

이와 관련된 앞으로의 연구 진행 계획으로 첫째, 시뮬레이션 도구를 사용하여 제시된 모델의 보안 안전성 및 경량성의 실험적 입증, 둘째, ID 위장 공격에 대한 신용정보기반 상호인증에 대한 연구, 셋째, 방대한 USN에서의 신용모델에 기반한 그룹 단위의 확장된 계층적 인증 모델 연구 및 넷째, 초기인증 과정에서 적용되는 마스터키의 안전한 분배 및 설정 방식에 대한 연구를 수행할 계획이다.

참고문헌

[1] 서운석, 신순자, 김유정, 신상철, "센서네트워크 보안 프로토콜 소개와 향후과제", 한국정보과학회지, 제22권, 제 12호, pp. 60-66, 2004년 12월.

[2] 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호기술동향", 한국전자통신연구원 전자통신동향분석, 제 20권, 제5호, pp. 63-72, 2005년 2월.

[3] 김신효, 강유성, 정병호, 정교일, "U-센서 네트워크 보안 기술동향", 한국전자통신연구원 전자통신동향분석, 제20권 제5호, pp.93-99, 2005년 2월.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Cullar and J.D. Tygar, "SPINS:Security Protocols for Sensor Networks," Wireless Networks Journal (WINET), Vol. 8. No. 5, pp. 521-534, 2002.

[5] 조영복, 정윤수, 김동명, 이상호, "유비쿼터스 센서네트워크에서의 저전력 상호인증 프로토콜", 한국컴퓨터

정보학회논문지, 제 2권, 제34호, pp. 187-197, 2005년 5월.
[6] 박태진, 박준식, 박재두, "차세대 이동통신용 고효율, 저전력 VCO에 관한 연구", 한국컴퓨터정보학회논문지, 제7권, 제 3호, pp. 109-114, 2002년 9월.
[7] S. Zhu, S. Setia and S. Jajodia. "LEAP:Efficent Security Mechanisms for Large-Scale Distributed sensor Networks," The 10th ACM Conference on Computer and Communications Security (CCS '03) Washington D.C., Oct. 2003.
[8] J.Deng, R. Han, and S. Mishra, "Security Supprort for In-network Processing in Wireless Sensor Networks," 2003 ACM Workshop on the Security of Ad-Hoc and Sensor Network(SASN '03), Oct. 2003.
[9] H. Yang, X. Meng, and S. Lu, "Self-organized network layer security in mobile ad hoc networks," in Proceedings of ACM Workshop on Wireless Security (WiSe'02), Atlanta, USA, Sep. 2002.
[10] T. Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," in Proceedings of the European Symposium on Research in Computer Security. Brighton, UK: Springer-Verlag, pp. 3-18, 1994.
[11] R. Yahalom, B. Klein, and T. Beth, "Trust elationships in secure systems a distributed authentication perspective," in Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy (RSP '93), pp. 150-164, 1993.
[12] A. Abdul-Rahman and S. Halles, "A distributed t rust model," in Proceedings of New Security Paradigms Workshop '97, pp. 48-60, 1997.
[13] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, "A Trust Model Based Routing Protocol for secure Ad-Hoc Networks," in Proceedings 2004 IEEE Aerospace Conference, Mar. 2004.
[14] E. Gray, J.-M. Seigneur, Y. Chen, and C. Jensen, "Trust propagation in small worlds," in Proceedings of the 1st International Conference on Trust Management,, May. 2003.
[15] L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks," in Proceedings of the Security Protocols Workshop. Cambridge, UK: Springer-Verlag, Apr. 2002,http://citeseer.nj.nec.com/eschenauer02trust.html.
[16] Y. Teng, V. V. Phoha, and B. Choi, "Design of trust metrics based on dempster-shafer theory," 39th Annual ACM Southeast Conference, Mar. 2001.
[17] A, Josang, "A logic for uncertain probabilities," Intetnational Journal of Uncertainty, Fuzzyness and Knowledge-Based Systems, Vol. 9, pp. 279-311, 2001.
[18] W. Du, J. Deng, Y. S. Han, S. Chen and P. K. Varshney, "A key Management Schema for Wireless Sensor Networks Using Deployment knowledge," IEEE. INFOCOMM 2004, 2004.

저 자 소 개

김 홍 섭

1998년~현재 : 충북대학교 대학원 전자계산학과 박사과정(수료)
1994년~현재 : 청주 주성대학 컴퓨터프로그래밍과 부교수
〈관심분야〉 네트워크보안, 네트워크 구조, 네트워크관리

조 진 기

1995년~현재 : 충북대학교 대학원 전자계산학과 박사과정(수료)
1991년~현재 : 부산경상대학 멀티미디어컴퓨터과 조교수
〈관심분야〉 프로토콜엔지니어링, 네트워크보안

이 상 호

1989년 : 숭실대학교 대학원 전자계산학과 (Ph. D)
1982년~현재 : 충북대학교 전기전자컴퓨터공학부 교수
〈관심분야〉 프로토콜엔지니어링, 네트워크보안, 네트워크구조