韓國 컴퓨터情報學會 論文誌
第10卷 第6號, 2005. 12.

2005-10-6-2-5

USN 상호인증을 위한 개선된 신용모델 설계

김 홍 섭*, 이 상 호**

Design of An Improved Trust Model for Mutual Authentication in USN

Hong-Seop Kim*, Sang-Ho Lee**

요 약

유비쿼터스 환경의 핵심 기술인 USN은 배터리 용량 및 연산능력이 제한된 자원하에서 운영되어야 하며 이로 인하여 USN은 저 전력소비 및 최소의 연산량을 유지하기 위한 경량화된 설계가 반드시 요구된다. 이전의 $J\phi sang$의 신용모델에 기반한 USN 상호인증 방법은 최소의 연산 기능만을 적용하여 경량화된 상호인증이 가능하다는 특징이 있으나, 신용을 표현하기 위한 구성요소들의 속성이 경량성의 측면에서 미비점을 갖는다. 본 논문에서는 USN에서의 경량 상호인증에 적용하기 위해 $J\phi sang$의 모델을 개선한 신용모델을 제안한다. 제안된 USN 신용모델은 오직 신용 표현 대상(x)의 믿음(belief)의 정도만을 적용하여 신용정보를 정의한다. 정의된 신용정보는 확률 및 논리 연산(AND)에 기초하여 정보를 계산하기 때문에 기존 $J\phi sang$의 신용모델 보다 계산량 측면에서 경량성을 가진다.

Abstract

Ubiquitous Sensor Network(USN), the core technology for the Ubiquitous environments, must be operated in the restrictive battery capacity and computing. From this cause, USN needs the lightweight design for low electric energy and the minimum computing. The previous mutual authentication, based on $J\phi sang'$s trust model, in USN has a character that makes the lightweight mutual authentication possible in conformity with minimum computing. But, it has an imperfection at the components of representing the trust from a lightweight point of view. In this paper, we improve on the $J\phi sang'$s trust model to apply a lightweight mutual authentication in USN. The proposed trust model in USN defines the trust information with the only degree of trust-entity (x)'s belief. The defined trust information has a superiority over the $J\phi sang'$s trust model from a computing point of view, because it computes information by probability and logic operation(AND).

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

• 제1저자 : 김홍섭
• 접수일 : 2005.10.17, 심사완료일 : 2005.12.15
* 충북대학교 대학원 전자계산학과 박사과정 (청주 주성대학 컴퓨터프로그래밍과 부교수)
** 충북대학교 전기전자컴퓨터공학부 교수

Ⅰ. 서 론

오늘날 IT 패러다임의 급격한 변화에 따라 휴대폰, PDA 등과 같은 다양한 이동 통신, 센서(sensor) 및 극소형 장비 등을 적용하는 시공(時空)을 초월한 인간 친화적인 모바일 컴퓨팅(mobile computing) 서비스 환경에 대한 요구가 사회의 다양한 분야에서 폭발적으로 증대되고 있다.

특히, 최근에는 제록스(Xerox)의 팔로 알토(Palo Alto) 연구소의 마크 와이저(Mark Weiser) 박사가 제안한 유비쿼터스 컴퓨팅(Ubiquitous computing)의 개념이 새롭게 대두되어 관련된 다양한 연구를 활발히 진행 중에 있다[1].

유비쿼터스 환경을 구현하는 핵심 기술중 하나는 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network:USN)이다. USN 기술은 전자태그 및 센서(sensor)장치들을 사물, 생명체 또는 주변 환경에 부착하여 수집된 인식 정보를 기초로 주변의 각종 상황정보를 탐지하여 실시간으로 이를 관리하기 위한 기술이며 민•관•군 다양한 분야에 응용할 수 있다[1,2,3]. 그리고 USN 기술 개발을 위해서는 규모, 설치환경의 열악성, 형태(topology), 안정성 및 자원의 경량성 측면에서 존재하는 제약조건의 극복이 선행되어야 한다.

이같이 USN 기술은 가까운 장래에 국내•외적으로 널리 사용될 기술임에도 불구하고 관련된 연구는 주로 USN 서비스의 구성 및 라우팅과 같은 기본 동작 등에 대한 연구 개발 중심으로 진행되어 왔으며 보안 분야에 대한 연구는 상대적으로 많이 결여되어 왔으나 USN은 설치되는 장소가 군사 전투지역, 재난지역 등과 같이 환경이 극히 열악한 지역에 대부분 구성되며 이에 따른 센서 정보의 도청, 비 정상적인 패킷의 흐름, 데이터 위•변조 및 서비스 거부 공격 등과 같은 다양한 공격에 취약하며 이에 대한 대책이 요구된다[4]. 특히, USN 보안기술은 앞서 서술된 USN의 제약조건중 한정된 자원하에서 운용되어야 하는 요인으로 인하여 저 전력 소모 및 최소의 연산량을 유지하는 측면의 경량화된 설계가 반드시 필요하다.

이에 김홍섭[3]의 연구에서는 USN을 위한 계산 부담을 줄이는 상호인증을 위하여 $J\phi sang$의 신용계산 모델에 기반한 상호인증 방법을 제안하였다.

이 논문에서는 USN에서의 경량화된 상호인증을 지원하기 위해 $J\phi sang$의 신용계산 모델을 USN에 적합하게 계산의 경량성 측면에서 개선한 신용모델을 제안하며 논문의 구성은 다음과 같다. 제 2 장에서는 USN 인증과 관계된 연구동향 및 신용기반 보안 기술의 연구동향을 고찰한다. 제 3 장에서는 $J\phi sang$신용계산 모델을 개선한 USN 신용모델을 설계한다. 제 4 장에서는 3장에 제안된 USN 신용모델의 적용방향과 기존 $J\phi sang$의 신용계산 모델과의 차이점을 비교 분석한다. 마지막 제 5 장에서는 제안된 USN 신용모델의 응용 및 향후 관련 연구 분야를 제안한다.

Ⅱ. 관련연구

이 장에서는 기존 USN 보안관련 연구 및 신용 기반 보안 관련 연구동향을 고찰한다.

2.1 기존 USN 보안관련 연구

USN 구성 센서들의 보안 안정성을 유지하기 위해서 <표 1>과 같이 비밀성(confidentiality), 상호인증(mutual authentication), 무결성(integrity), 신선성(freshness), 익명성(Anonymity), 경량성(lightweightness) 등과 같은 보안 요구조건이 보장 되어야 한다[5].

표 4. USN 보안요구
Table 1. Security requirement of USN

요구	보안기능	적용기술
비밀성	전송되는 정보는 불법적인 도청으로부터 안전하다.	암호화
상호인증	통신에 참여하는 개체들은 서로 상대방을 믿음의 관계임을 보장한다.	-키 관리, -개체인증 -자료인증
무결성	전송되는 정보는 불법적인 위•변조로부터 안전하다.	MAC 등
익명성	통신에 참여하는 개체외에는 상대방의 정보를 알 수 없음을 보장한다.	
신선성	한번 사용된 보안정보는 재사용으로 인한 공격으로부터 안전하다.	랜덤수 생성, 1회용 사용 등
경량성	USN에서의 최소 연산량 지원 등과 같은 자원소비를 최소로 함을 보장한다.	

USN은 일반적인 컴퓨터 환경과는 달리 열악한 자원지원 환경에 대한 제약 사항을 갖기 때문에 적은 연산량과 저 전력 소모 구조를 지원하기 위해 USN의 보안관련 연구는 주로 경량암호화 기술 및 인증 기술 측면에서 수행되어 왔다[6].

경량 암호화 기술 측면에서 비 대칭키(asymmetric key) 방식의 공개키 방식보다 속도가 빠른 대칭키(symmetric key)를 기반으로 하는 암호화 방식이 많이 적용되고 있다[7,8,9,10]. 하지만 대칭키 방식은 비밀키 유출 가능성에 대한 안전한 키 관리 및 분배 방식에 대한 연구가 함께 요구된다.

인증기술 측면에서는 주로 SPINS(Security Protocols for Sensor Networks)[5], LEAP(Localized Encryption and Authentication Protocol)[11], L. Echenaur와 V. D. Gligor의 랜덤키 사전분배 프로토콜[12], FFS(Feige-Fiat-Shamir) 인증 프로토콜[13,9], KM(Karl-Matsumoto) 상호인증 프로토콜[14,15] 등의 연구가 있다.

2.2 신용기반 보안연구

신용(trust)의 개념은 다양한 심리학, 사회과학, 수학 및 컴퓨터 과학 등과 같은 다양한 학문분야에 적용되어 왔다. 특히 컴퓨터 과학 분야에서는 신용을 불확신성(uncertainty)를 표현하고 분석하여 판단하기 위한 기법으로 많이 연구되어 왔다.

최근에는 이러한 신용모델을 주로 전자상거래, P2P(Peer to Peer) 망 등의 보안 문제 해결을 위해 연구되어 왔다[16,17,18,19]. MANET(Mobile Ad-Hoc Network), WSN(Wireless Sensor Network) 및 유비쿼터스 분야의 안전한 통신환경 지원하기 보안기술에 적용이 시도되고 있다[16,20,21,22].

노드 사이의 신용관계를 정의하기 위해서는 노드 사이의 신용도를 평가하기 위한 각 노드의 신용정보를 표현해야 되는데 이에 대해 제시된 연구 결과로 제안된 신용표현 모델은 댐스터-세이퍼(Demster-Safer)의 확률모델, 퍼지논리(fuzzy logic) 모델 및 $J\phi sang$의 신용계산 모델이 존재한다[23,24,25].

Teng 등의 연구에서는 현실세계의 불확신성을 정의하고 표현하기 위해 댐스터-세이퍼 모델을 적용한 확률 기반의 신용 표현 모델을 제안하였다[23].

Manchala 등의 연구에서는 퍼지 논리 모델에 기반한 WTS(Weighted Trust Surface)와 FTS(Fuzzy Trust Surface)를 적용하여 개체 상호간의 신용관계를 표현하였다. 그리고 신용행렬(trust Matrix)를 정의하여 이를 적용한 신용관계 검증을 위한 모델을 제안하였다[24].

$J\phi sang$의 연구에서는 현실 세계 대상들의 믿음과 불확신의 정도를 주관논리(subject logic)로 표현하기 위해 "Opinion"을 정의하고 이를 기초로 확률기반의 다양한 신용계산 모델을 제안하고 신용의 정도를 확률로 표현 가능함을 증명하였다[25].

Xiaoqi 등의 연구에서는 $J\phi sang$의 연구에서 제안된 신용계산 모델을 MANET 라우팅에 적용하여 자기조직적인 경량화된 안전한 경로 확보에 적용될 수 있음을 증명하였지만, 악의적 의도를 지닌 노드의 신규 참여에 대한 인증 방법이 결여되어 있다[20].

Shanker 등의 연구에서는 유비쿼터스 환경에서의 구성 노드 상호간 정보 관리에 $J\phi sang$의 신용계산 모델을 적용한 역할 기반 접근제어(Role Based Access Control) 방법을 제안하였다[26].

김홍섭의 연구에서는 $J\phi sang$의 신용계산 모델을 적용한 USN에서 노드 상호간의 신용관계 설정방법과 이에 기반한 대칭키 방식의 경량화된 상호인증이 가능함을 제안하였다[3].

III. USN 신용모델 설계

이 장에서는 Josang의 연구에서 제안된 신용 계산 모델을 개선한 USN에 적합한 노드 상호간의 신용정보를 표현하기 위한 방법을 제안한다.

3.1 USN 구성

이 논문에서 제안하는 USN의 기본 구성은 미국 버클리 대학의 CITRIS(Center for Information Technology Research in the Interest of Society)에서 제안한 스마트더스트(Smart-Dust)의 센서망(Sensor Network) 모델을 (그림 1)같이 적용한다[5,6]. (그림 1)에서 보는 바와 같이 USN 노드들은 일반 센서노드와 베이스스테이션(Base Station:BS)으로 구성되며 기본적인 USN의 통신은 그룹(group)내의 BS를 중심으로 "노드:BS", "BS:노드", "BS:그룹내의 모든 노드"들의 통신 그리고, 서로 다른 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 1 (a))와 같이 USN을 구성하는 개별적인 센서 노드들은 성능에 따라 최대 자료 수집 영역(sensing range)과 최대 전송영역(radio range)를 보유하게 되며 전송 및 자료 수집영역의 거리를 "r"이라고 가정하고 최대 자료수집 영역 및 수집된 자료의 전송 가능 영역은 "$\pi \bullet r^2$"으로 결정한다.

센서노드는 USN의 구성이 필요한 지역에 무작위로 살포되어 배치된다. 배치된 센서노드는 (그림 1(b))와 같이 자신의 통신 범위내에 있는 이웃 센서노드 상호간에 자기조직적(self-organization)으로 망을 형성하게 된다. 이때 각 센서들은 자신의 최대 정보 전송영역이 제한되기 때문에 원거리 전송을 위해서는 인접된 센서 노드의 중계(relay)를 필요로 한다.

(그림 1(b))는 i번 USN 통신 그룹(group)이 형성되어 BS_i을 중심으로 m개의 센서노드($\{N_{i1}, N_{i2}, N_{i3}, .., N_{1m}\}$)들이 자기조직적으로 형성된 구조를 나타내며 (그림 1(b))와 같이 형성된 USN 그룹내 센서노드의 정보는 BS_i를 통하여 관리된다.

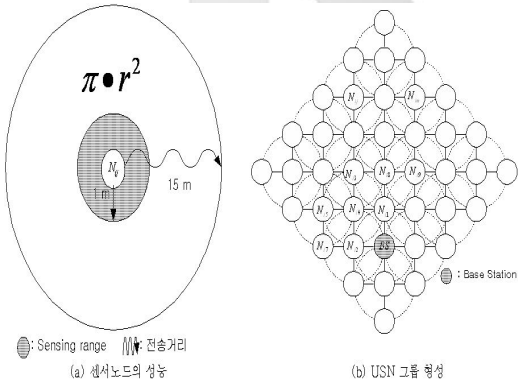

그림 1. USN 구성
Fig 1. Configuration of USN

3.2 USN 신용표현 모델

3.2.1 신용표현 모델

USN을 구성하는 임의의 i번째 구성노드에 대한 신용($\mathbb{R}_i$)은 (정의 1)과 같이 4개 요소로 구성된 튜플(tuple)로 정의한다. (정의 1)에서 E_i는 신용을 정의하고자 하는 i번 개체(entity)를 정의하며 이는 USN을 구성하는 노드들로 지정된다. ξ_{E_i}는 경험의 정보로서 i번 개체가 지닌 신용을 결정하기 위한 신용 표현의 기초정보로 적용되며 ξ_{E_i}의 값은 (f_s, f_f)로 구성된다. 여기서, (정의 1)과 같이 "f_s"값은 노드가 정상적인 동작(event)을 수행하는 횟수와 "f_f"은 노드의 비 정상적인 동작을 수행하는 횟수로 결정하며 개체가 갖는 경험정보의 초기치는 (1,1)로 정의한다. I_{E_i}는 i번 개체가 지닌 신용의 상태를 결정하기 위해 적용되는 신용정보로 정의한다. $S_{E_i\{dn\}}$는 i번 개체가 지닌 신용 상태를 표현하는 집합으로 (정의 1)과 같이 $\{Trust, Uncertainty\}$로 구성된다. 여기서 상태값이 "$Trust$"일 경우는 i번 개체가 신용상태 임을 표현하고 "$Uncertainty$"일 경우는 i번 개체가 불확신 상태에 있음을 표현한다. $S_{E_i\{c\}}$는 현재(current) 신용의 상태이며 $S_{E_i\{n\}}$는 앞으로 새롭게(new) 변화될 상태를 나타낸다. 신용상태의 변화는 (정의 1)에서 표현한 것과 같이 E_i의 현재 신용상태에서 결정된 신용정보(I_{E_i})를 적용하여 새로운 신용상태로 전이하게 된다.

[정의 1] $\mathbb{R}_i = < E_i, \xi_{E_i}, I_{E_i}, S_{E_i\{dn\}} >$

- $E_i \in \{N_1, N_2, ...N_i, ...N_m\}$: i번 신용 개체
- $\xi_{E_i} = (f_s, f_f)$: 경험의 정보

$$\begin{cases} f_s = f_s + 1 & , if\ event \in sucess \\ f_f = f_f + 1 & , \text{if}\ \ event \in fail \end{cases}$$

- I_{E_i} :개체 E_i에 대한 신용정보
- $S_{E_i\{dn\}} = \{Trust, Uncertainty\}$
  : 현재 및 새로운 신용상태 집합
- 신용상태 변화 : $\{S_{E_i\{c\}} \times I_{E_i} \rightarrow S_{E_i\{n\}}\}$

3.2.2 신용정보 계산

제2장의 관련연구에서 기술한 $J\phi sang$의 연구에서는 개체(x)에 대한 신용을 표현하고 계산하기 위해 믿음(belief)의 정도(b_x), 불신(disbelief)의 정도(d_x) 및 불확신(uncertainty)의 정도(u_x)로 구성되는 신용의견(Opinion)을 "$\omega_x = \{b_x, d_x, u_x\}$"로 정의하고 이 모델을 기초로 신용을 표현하기 위한 다양한 계산식을 제안하였다[25].

하지만, $J\phi sang$의 연구에서 제안된 계산 모델은 신용을 표현함에 있어서 계산량이 많고 이점은 USN 경량성 측면에서 적용상 부적합하다.

이에 대해, $J\phi sang$의 연구에서 제시한 이들 구성 요소들 사이의 관계를 분석하여 보면 (그림 2)와 같이 "$b_x + d_x + u_x = 1$"이 된다[3,25]. 여기서 불신의 정도(d_x)와 불확신의 정도(u_x)는 믿음의 정도(b_x)만을 기초하여 (식 1)과 같이 표현 가능하다. 그리고 (식 1)에 의해 $J\phi sang$의 연구에서 정의된 신용의견은 3가지 요소를 적용하지 않고 믿음의 정도인 "b_x"만을 갖고도 표현될 수 있음을 알 수 있다.

$$(d_x + u_x) = 1 - b_x \quad \cdots\cdots (1)$$

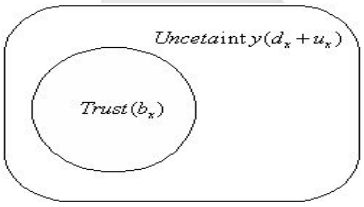

그림 2. 신용과 불확신의 관계
Fig 2. Relationship between trust and uncertainty

이에, 본 논문에서 제안하는 USN의 구성 개체에 대한 신용의 정도를 표현하기 위한 경량화된 신용정보 모델은 (식 2)와 같이 개체(E_i)에 대한 믿음(belief)의 정도를 표현하는 "$Bel(E_i)$"로 구성한다. 그리고 "$Bel(E_i)$"는 다시 개체(E_i)에 대한 (식 3)같이 개체(E_i)의 전체 경험(ξ_{E_i})중 정상적인 통신이 발생할 확률 함수($P_{E_i}(\xi_{E_i}|f_s)$)로 정의한다. $Bel(E_i)$의 계산결과는 (식 4)와 같이 0.0과 1.0 사이에 존재한다.

$$I_{E_i} = \{Bel(E_i)\} \quad \cdots\cdots (2)$$

$$Bel(E_i) = P_{E_i}(\xi_{E_i}|f_s) = \frac{f_s}{f_s + f_f} \quad \cdots\cdots (3)$$

$$Bel(E_i) \in [0,1] \quad \cdots\cdots (4)$$

예를 들어, (정의 1)에 의해 센서 노드 A의 신용($\mathbb{R}_A$)은 "$(E_A, \xi_{E_A}, I_{E_A}, S_{E_A\{cln\}})$"로 구성된다. 여기서 노드 A에서 측정된 경험정보(ξ_{E_A})를 $\{8,6\}$으로 측정될 경우 센서노드 A의 신용정보(I_{E_A})는 반올림하여 0.57로 계산되며 결과적으로 노드 A의 신용정도를 57%로 결정한다.

3.2.3 신용상태의 결정

신용평가 대상인 개체가 갖는 새로운 신용상태($S_{E_i\{n\}}$)의 결정을 위해서는 (정의 1)에서와 같이 현재의 신용상태($S_{E_i\{c\}}$)에서 (식 2), (식 3)에 의해 결정된 신용정보(I_{E_i})의 결과에 따라 (식 5)와 같이 결정한다. (식 5)에서 보는 바와 같이 신용 임계치(Δ_t)를 정의하여 (그림 3)과 같이 개체 E_i에 대한 새로운 신용상태는 믿음의 정도($Bel(E_i)$)가 Δ_t보다 크거나 같으면 새로운 신용상태($S_{E_i\{n\}}$)는 $\{Trust\}$로 결정하며 기타 조건에서는 불확신 상태인 $\{Uncertainty\}$로 결정한다.

$$S_{E_i\{n\}} \begin{cases} = Trust & , if\ Bel(E_i) \geqq \Delta_t \\ = Uncertainty & , Otherwise \end{cases} \quad \cdots (5)$$

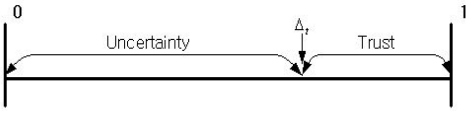

그림 3. 신용상태의 결정
Fig 3. Determination of trust state

예를 들어, 3.2.2절의 사례에서와 같이 센서노드 A의 신용정도가 57%(=0.57)로 결정되고 신용 임계치(Δ_t)를 0.5로 가정할 경우, 노드 A의 신용도가 0.57이므로 이는 정의된 신

용 임계치(0.5)보다 크다. 그러므로 노드 A의 새로운 신용상태($S_{E_A\{n\}}$)는 $\{Trust\}$로 결정되어 신용있는 노드로 평가한다.

3.3 노드 신용관계

USN 구성노드 상호간의 신용관계(trust relationship)는 노드 상호간의 신용정보를 설정하고 유지하는 형태를 나타내며 관계된 노드 상호간에 신용의 정도를 나타내는 신용정보(I_{E_i})를 갖는다. 노드 상호간의 신용관계는 직접신용(direct trust)과 간접신용(indirect trust) 관계로 정의된다

3.3.1 신용관계 속성

이러한 노드 상호간의 신용관계에는 비대칭적(asymmetric) 관계속성과 전이적(transitive) 관계속성을 지닌다. 비대칭적 관계는 (식 6)과 같이 서로 인접한 노드 i와 j가 서로 상대 노드의 신용정보를 갖고 서로를 직접 신용하는 관계가 되더라도, j에 대한 i의 신용의 정도와 i에 대한 j의 신용의 정도는 서로 다를 수 있음을 정의한다.

$$\{\exists\,(i,j) \in R_1 \text{ and } (j,i) \in R_2 \mid R_1 \neq R_2\} \quad \cdots (6)$$

전이적 관계는 (식 7)과 같이 노드 i와 j사이에 신용정보를 갖는 신용관계가 있고, j와 k사이에도 상호간의 신용정보를 갖는 신용관계가 존재할 경우 노드 A와 C사이의 신용관계를 A와 B사이의 신용관계를 통하여 설정되는 관계이다.

$$\{\exists\,(i,j) \in R_1 \text{ and } (j,k) \in R_2 \mid (i,k) \in (R_1 \times R_2)\} \quad \cdots (7)$$

3.3.2 직접신용관계

직접신용 관계는 (그림 4)에서와 같이 1 홉(hop) 단위로 직접 인접한 노드 사이의 신용관계로 정의된다. 인접한 노드 상호간에 상대방 노드의 신용정보를 관리하게 되며 (식 6)와 같은 비 대칭적 관계속성을 지닌다. 예를 들어, (그림 4)와 같이 서로 인접한 노드 i와 j가 서로 상대 노드의 신용정보를 갖고 서로를 직접 신용하는 관계이다.

그림 4. 노드 i와 j사이의 직접 신용관계
Fig 4. Direct trust relationship between node-i and j

3.3.2.1 직접관계를 지닌 노드들의 신용의 표현

서로 인접된 노드가 각각 i와 j가 존재할 경우, 노드 i와 j의 직접 관계를 신용($\mathbb{R}_{ij}$)은 (정의 2)와 같이 표현한다. $\mathbb{R}_{ij}$는 USN을 구성하는 노드 i와 j가 직접 연결된 구조를 지닐 경우 노드 j에 대한 노드 i의 신용을 표현한다.

(정의 2)에서 E_{ij}는 신용을 정의하고자 하는 i번 노드에서 관리하고자 하는 j번 노드를 표현한다. $\xi_{E_{ij}}$는 노드 i가 관리하는 노드 j의 경험의 정보로서 j번 노드의 신용을 결정하기 위한 신용 표현의 기초정보로 적용되며 $\xi_{E_{ij}}$의 값은 (f_s, f_f)로 구성된다. 여기서, $\xi_{E_{ij}}$의 값의 의미는 (정의 2)와 같다. $I_{E_{ij}}$는 i번 개체가 지닌 j번 노드의 신용의 정도를 결정하기 위해 적용되는 신용정보이다. $S_{E_{ij}\{c|n\}}$는 i번 노드가 관리하는 j번 노드의 신용 상태를 표현하는 집합으로서 구성요소 및 의미는 (정의 2)와 같다.

[정의 2] $\mathbb{R}_{ij} = < E_{ij}, \xi_{E_{ij}}, I_{E_{ij}}, S_{E_{ij}\{c|n\}} >$
- $E_{ij} \in \{N_1, N_2, \ldots N_j, \ldots N_m\}$:j번째 신용대상 개체
- $\xi_{E_{ij}} = (f_s, f_f)$:노드 i가 관리하는 노드 j의 경험정보

$$\begin{cases} f_s = f_s + 1 & , if\ event \in sucess \\ f_f = f_f + 1 & , \text{if}\ \ event \in fail \end{cases}$$

- $I_{E_{ij}}$:노드 i에서 결정되는 노드 j에 대한 신용정보
- $S_{E_{ij}\{c|n\}} = \{Trust, Uncertainty\}$
  : 노드 j의 현재 및 새 신용상태 집합
- 신용상태의 변화 : $\{S_{E_{ij}\{c\}} \times I_{E_{ij}} \rightarrow S_{E_{ij}\{n\}}\}$

3.3.2.2 직접관계를 지닌 노드들의 신용정보

직접 신용관계를 유지하는 노드 i와 j에 대하여, 노드 j에 대한 노드 i의 신용정보($I_{E_{ij}}$)는 (식 8)과 같이 구성되며 (식 8)에서 $Bel(E_{ij})$는 노드 j에 대한 노드 i의 믿음의 정도를 표현한다. $Bel(E_{ij})$의 계산은 (식 3)과 같이 노드

j에 대한 전체 경험정보($\xi_{E_{ij}}$)중 정상적인 통신이 발생할 확률 함수($P_{E_{ij}}(\xi_{E_{ij}}|f_s)$))로 계산되며 (식 4)과 같이 0.0과 1.0 사이에 존재한다.

$$I_{E_{ij}} = \{Bel(E_{ij})\} \quad \cdots\cdots (8)$$

예를 들어, 직접신용관계에 있는 센서 노드 A와 B에 대하여 $\xi_{E_{AB}} = (8,6)$, $\xi_{E_{BA}} = (4,4)$라고 가정하고 노드 B에 대한 노드 A의 신용-정보($I_{E_{AB}}$) 및 노드 A에 대한 노드 B의 신용-정보($I_{E_{BA}}$)를 계산하면 (식 8)과 (식 3)을 적용하여 노드 B에 대한 노드 A의 믿음의 정도($Bel(E_{AB})$)는 0.57, 노드 A에 대한 노드 B의 믿음의 정도($Bel(E_{BA})$)는 0.5로 결정된다. 결과적으로 노드 A는 노드 B를 57%로 노드 B는 A를 50%로 믿을 수 있음을 표현한다.

3.3.2.3 직접관계를 지닌 노드들의 신용상태 결정

직접 신용관계를 유지하는 노드 i와 노드 j가 존재할 경우, 노드 j에 대한 노드 i가 갖는 신용상태($S_{E_{ij}\{n\}}$)의 결정을 위해서는 (정의 2)에서와 같이 노드 j의 현재의 신용상태($S_{E_{ij}\{c\}}$)에 신용-정보($I_{E_{ij}}$)를 적용하여 (식 5)와 같이 결정한다.

예를 들어, 앞 사례의 결과에서 신용-임계치(Δ_t)를 0.5로 가정하고 노드 A와 B에서 각각 상대방 노드의 새로운 신용상태($S_{E_{AB}\{n\}}$,$S_{E_{BA}\{n\}}$)를 (식 5)의 규칙에 따라 결정하면 $Bel(E_{AB})$는 0.57, $Bel(E_{BA})$는 0.5가 되므로 이는 모두 정의된 신용-임계치(Δ_t)보다 크다. 그러므로 (식 5)에 의해 $S_{E_{AB}\{n\}} = \{Trust\}$, $S_{E_{BA}\{n\}} = \{Trust\}$ 결정되며 결과적으로 노드 A와 B는 모두 상대방을 신용의 대상으로 평가한다.

3.3.3 간접신용관계

간접신용 관계는 (식 7)과 같이 전이적 속성(transitive)을 지니며 (그림 5)와 같이 2홉 이상 떨어진 특정 노드에 대한 신용관계를 믿을만한 제 3의 노드의 신용권고를 받아 설정하는 관계이다.

(그림 5)에서 노드 i와 j는 직접 신용관계를 유지하고 노드 j는 노드 k와 직접 신용관계를 유지하고 있다, 그리고 노드 i와 k는 직접 연결되는 채널이 존재하지 않을 경우 노드 i가 새로운 노드 k와의 신용관계를 설정하기 위하여 노드 k와 직접 신용관계를 설정하고 있는 노드 j의 신용-권고를 통하여 노드 i가 노드 k에 대한 신용을 평가할 수 있는 관계가 간접 신용관계이다.

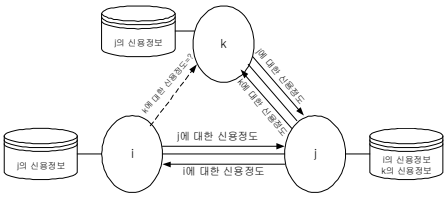

그림 5. 노드 i와 k사이의 간접신용 관계
Fig 5. Indirect trust relationship between node-i and k

3.3.3.1 간접 신용의 표현

서로 인접된 노드가 각각 i, j, k에 대하여, (정의 2)와 같이 노드 i와 j가 직접 신용(R_{ij}) 관계를 유지하고 노드 j와 k는 직접 신용(R_{jk})를 유지할 때 노드 i와 k사이의 신용관계를 R_{ij}와 R_{jk}를 사용하여 설정하려 할 경우 (그림 6)같이 노드 i와 k 사이의 간접 신용관계($\widetilde{R_{ik}}$)는 (식 9)과 같이 정의한다.

$$\widetilde{R_{ik}} = (R_{ij} \times R_{jk}) \quad \cdots\cdots (9)$$

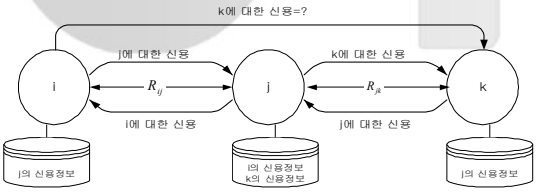

그림 6. $(R_{ij} \times R_{jk})$를 사용한 간접신용($\widetilde{R_{ik}}$)
Fig 6. Indirect trust($\widetilde{R_{ik}}$) with $(R_{ij} \times R_{jk})$

이러한 간접 신용관계 설정시의 평가 대상 노드의 신용구성은 (정의 2)와 같으며 (그림 1)에서와 같이 USN을 구성하는 노드가 특정 노드의 신용을 알고자 할 경우 신용을 알고자 하는 노드가 다른 그룹에 소속되었던지 또는 직접 연결되는 채널이 존재하지 않을 경우에 설정하여 신용정보를 습득하기 위해 적용한다.

3.3.3.2 간접 신용 평가

(그림 6)과 같이 간접 신용관계($\widetilde{R_{ik}}$)를 지닌 노드 i와 k 사이의 중간 노드 j의 신용정보를 고려한 노드 i에서의 노드 k에 대한 신용은 (식 10)과 같이 노드 j 상호간의 현재 신용상태($S_{E_{ij}\{c\}}$)에 대한 논리곱(AND)으로 결정하며 이를 간접 신용 상태의 조합(trust combination)이라고 정의한다.

$$S_{E_{ijk}\{n\}} = ((S_{E_{ij}\{c\}} \wedge S_{\{c\}}) \wedge (S_{E_{ji}\{c\}} \wedge S_{E_{kj}\{c\}})) \quad \cdots\cdots (10)$$

여기서, 2홉 이내의 간접 신용이 아니고 (그림 7)과 같이 다중 홉(multi-hop)상의 간접 신용 상태의 조합은 (식 11)같이 (식 10)을 확장하여 정의한다.

$$S_{E_{1\ldots m}\{n\}} = (\overset{m-1}{\underset{i=1}{\wedge}}(S_{E_{u+1}\{c\}}) \wedge (\overset{1}{\underset{i=m-1}{\wedge}} S_{E_{t+1i}\{c\}}) \quad \cdots\cdots (11)$$

그림 7. 다중 홉 상의 간접 신용
Fig.7. Indirect trust at multihops

예를 들어, 서로 인접된 노드 i,j,k에 대하여 노드 상호간에 설정된 직접 신용상태는 (그림 8)과 같다. 여기서, 노드 j의 권고를 받아 노드 k에 대한 노드 i의 새로운 신용상태는($S_{E_{ijk}\{n\}}$)는 (식 9)를 적용하여 "$(Trust \wedge Trust) \wedge (Trust \wedge Trust)$"로 계산되어 노드 j의 권고를 통한 노드 i에서의 노드 k의 새로운 신용상태는 "$S_{E_{ijk}\{n\}} = \{Trust\}$"이 된다. 결과적으로 i는 노드 j의 권고를 통하여 노드 k를 믿을 수 있는 신용 상태로 결정한다.

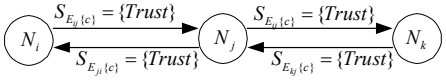

그림 8. 간접 신용상태의 결정
Fig 8. Determination of indirect trust state

3.3.3.3 신용합의

(그림 9)와 같이 노드 i와 노드 k에 대한 (식 10)과 (식 11)을 기초로 하는 간접 신용상태를 인접한 여러 이웃노드($N = \{N_1, N_2, \ldots, N_m\}$)들이 서로 다르게 권고하는 경우가 발생 가능하다. 이 경우 인접된 여러 노드의 신용정보를 종합하여 합의된 신용정보를 결정하기 위해 확률에 기반한 신용정보 계산 모형을 (식 12)와 같이 정의한다.

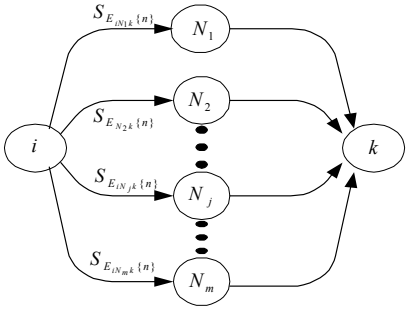

그림 9. 다수 노드의 신용합의
Fig 9. Trust consensus of multiple nodes

여기서 Θ는 (식 10)와 (식 11)을 적용하여 결정된 2홉 또는 다중 홉 상의 간접신용 관계를 통하여 결정된 신용상태($S_{iNjk\{n\}}$)에서 신용($Trust$)을 판정한 빈도수(f_t) 및 불확신($Uncertainty$)을 판정한 빈도수(f_u)를 정의하며 이들의 값은 (식 13)과 같이 결정한다.

이때, 다수 노드에서 권고하는 신용상태에 대한 합의된 신용정도는 다수의 노드에서 권고한 신용상태 전체수에서 신용($Trust$) 상태를 권고한 빈도수(f_t)에 대한 확률($P(\Theta|f_t)$)로 (식 14)와 같이 정의하며 계산된 값의 범위는 (식 15)와 같이 0.0에서 1.0 사이에 존재한다.

$$\Theta = (f_t, f_u) \quad \cdots\cdots (12)$$

$$\begin{cases} f_t = f_t + 1, if \quad S_{iNjk\{n\}} = \{Trust\} \\ f_u = f_u + 1, if \quad S_{iNjk\{n\}} = \{Uncertainty\} \end{cases} \quad \cdots\cdots (13)$$

$$P(\Theta|f_t) = \frac{f_t}{f_t + f_u} \quad \cdots\cdots (14)$$

$$P(\Theta|f_t) \in [0,1] \quad \cdots\cdots (15)$$

(식 13)를 적용하여 결정되는 합의된 노드 k에 대한 노드 i의 신용상태는 (식 16)과 같이 신용임계치(Δ_t)를 적용하여 다수 노드에서 권고된 신용 권고의 정도($P(\Theta|f_t)$)이 Δ_t 보다 크거나 같으면 합의된 새로운 신용상태는 $\{Trust\}$로 결정하며 기타 조건에서는 불확신 상태인 $\{Uncertainty\}$로 결정한다.

$$S_{\overline{iNjk\{n\}}} = \begin{cases} = Trust & ,if\ P(\Theta|f_t) \geqq \Delta_t \\ = Uncertainty & ,Otherwise \end{cases} \quad \cdots\cdots (16)$$

예를 들어, (그림 10)과 같이 노드 i와 인접하여 직접 신용관계를 유지하는 4개의 노드(N_1, N_2, N_3, N_4)들이 (식 10)을 적용하여 노드 k에 대하여 신용권고를 하였고 신용임계치(Δ_t)를 "0.6"으로 정의하였을 경우 노드 i가 결정하는 노드 k의 신용상태를 구하자. (그림 10)에서 보면 노드 k를 신용($\{Trust\}$)한다고 결정한 빈도수(f_t)는 2이고, 노드 k의 신용상태가 불확신($\{Uncertainty\}$)하다고 결정한 빈도수(f_u)도 2이다. 그러므로, Θ는 $(2,2)$로 결정되며 (식 14)에 의해 $P(\Theta|f_t)$는 0.5로 계산된다.

이 결과에 (식 16)를 적용하면 $P(\Theta|f_t)$의 값이 Δ_t보다 작으므로 노드 i는 노드 k의 신용상태($S_{\overline{iNjk\{n\}}}$)를 "$\{Uncertainty\}$"로 판단한다. 결과적으로 노드 i는 노드 k를 불확신 대상으로 평가한다.

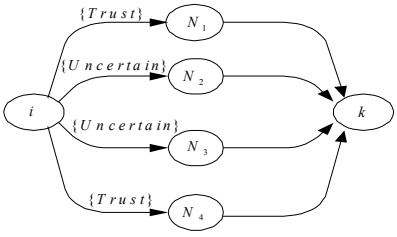

그림 10. 4개 노드의 신용합의
Fig 10. Trust consensus of four nodes

3.4 신용정보베이스 설계

USN을 구성하는 BS 및 센서노드들은 인접한 이웃노드들의 신용정보 값을 관리하기 위해 (그림 11)과 같이 신용정보베이스(Trust Information Base:TIB)를 관리한다. TIB에는 인접된 노드의 식별자(identifier)를 관리를 관리하는 노드 ID, 인접된 이웃 노드들 ($N = \{N_1, N_2, ..., N_n\}$)의 신용정보, 노드들의 경험정보($\xi_{E_i}$), 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 TIB에 제한시간을 주어 인접된 노드의 신용정보가 TIB에 기록되어 일정시간이 지난후에 인접노드의 존재유무를 확인한 후 대상 노드가 삭제되었을 경우 자동으로 관련된 신용정보를 재구성하기 위해 사용된다.

노드 ID (E_i)	경험정보(ξ_{E_i})		신용정보 (I_{E_i})	신용상태 ($S_{E_i\{c\}}$)	제한시간
	f_s	f_f			
N_1			$\{Bel(E_1)\}$		
....	....	....	.....	....	.....
N_j			$\{Bel(E_j)\}$		
...	...	...	...	....	.....
N_m			$\{Bel(E_m)\}$		

그림 11. TIB의 구성
Fig 11. Configuration of TIB

IV. 제안된 모델 적용 및 평가

이 장에서는 제3장에서 제안된 USN 신용모델에 대하여 USN에의 적용방법 제안한다. 그리고 $J\phi sang$의 연구에서 제안된 신용 계산 모델과의 차이점과 개선된 부분을 신용정보 표현상의 안전성 및 계산 경량성 측면에서 평가 분석한다.

4.1 제안된 모델의 USN 적용

제안된 신용모델은 (그림 12)와 같이 구성된 USN 환경에서 노드 상호간의 신용평가를 위해 적용 가능하다.

(그림 12)와 같이 3.3.2절에서 제안된 직접신용 관계는

"$BS_i : N_{i1}$", "$N_{i1} : N_{i8}$" 등과 같이 전송 가능 범위 내에 존재하는 노드 상호간의 신용평가를 위해 적용하며 3.3.3절에서 제안한 간접신용 관계는 "$BS_i : N_{i5}$", "$BS_i : N_{i8}$" 등과 같이 전송범위 밖의 노드 상호간의 인접된 이웃 노드들의 권고를 통한 신용평가를 위해 적용한다.

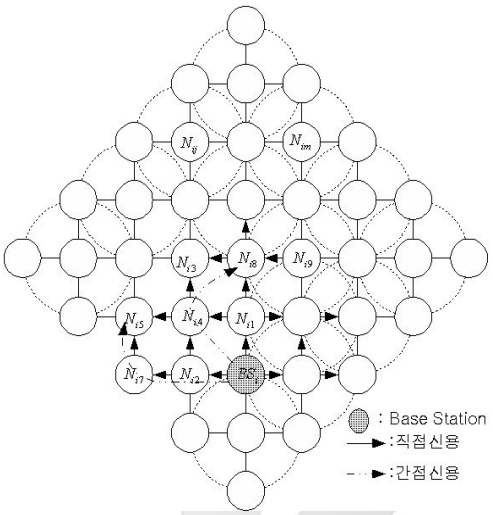

그림 12. 제안 신용모델의 USN 적용
Fig 12. Application of the proposed trust model in USN

4.2 제안 모델의 평가

본 절에서는 제안한 신용모델과 기존 $J\phi sang$의 신용모델을 신용평가에 적용할 경우에 나타나는 신용표현 안정성 및 경량성을 평가 분석한다.

4.2.1 신용정보 표현의 안정성 평가

본 논문에서 제안된 신용 모델은 3.2.2절에서 기술한 바와 같이 $J\phi sang$의 연구에서 제안된 신용모델을 USN에 적합하게 경량적으로 개선하였다.

<표 2>에서는 $J\phi sang$의 신용모델을 적용한 신용평가의 사례를 비교하기 위해 경험정보를 3가지 요소로 정의하고 각 경험정보를 김홍섭의 연구에서와 같이 정상 동작 빈도수(f_s)를 8, 비정상 동작 빈도수(f_f)를 6 및 불확신 인수(α)를 2로 가정한다[3]. 이 경험정보를 갖고 계산된 노드(x)에 대한 $J\phi sang$의 신용모델에 기반한 신용정보(w_x)는 {0.5,0.375,0.125}로 계산되며 신용임계치가 0.5로 정해졌을 경우 노드(x)를 신용상태(Trust)로 평가하고 신용임계치가 0.7로 주어질 경우는 불확신(Uncertainty)상태로 평가 한다[3].

또한, 본 논문에서 제안된 신용모델을 적용한 노드(x)에 대한 신용평가 결과는 <표 2>에서와 같이 경험정보는 (8,6)으로 정의하고 이를 (식 3)에 적용하여 노드(x)에 대한 신용정보(I_{E_x})는 0.57로 계산한다. 그리고 신용임계치가 0.5로 주어졌을 경우 (식 5)에 의해 노드(x)를 신용상태(Trust)로 평가하고 신용임계치가 0.7로 주어질 경우는 불확신(Uncertainty) 상태로 평가 한다.

표 2. 제안 신용모델과 $J\phi sang$ 신용모델의 비교
Table 2. Comparison of proposed trust model and $J\phi sang$'s trust model

		$J\phi sang$ 모델	제안모델
경험정보		$f_s = 8, f_f = 6, \alpha = 2$	$f_s = 8, f_f = 6$
신용정보 구성		$w_x = \{0.5, 0.375, 0.125\}$	$I_{E_x} = \{0.57\}$
평가	신용임계치	0.5	
	신용조건	$b_x \geq 0.5, d_x < 0.5, u_x < 0.5$	$I_{E_x} \geq 0.5$
	신용상태 결정	신용(Trust)	신용(Trust)
	신용임계치	0.7	
	신용조건	$b_x < 0.7, d_x < 0.7, u_x < 0.7$	$I_{E_x} < 0.7$
	신용상태 결정	불확신 (Uncertainty)	불확신 (Uncertainty)

<표 2>에서 노드(x)에 대하여 제안된 신용모델과 $J\phi sang$의 신용모델을 적용한 신용평가 결과를 비교하여 보면 계산과정의 차이는 존재하나 신용임계치에 따라 판단되는 노드에 대한 신용평가가 같음을 알 수 있다. 이러한 사실을 통하여 제안된 모델이 $J\phi sang$의 신용모델에 비해 신용정보의 표현에 있어 경량화가 되었으나 이에 따른 신용상태를 결정하기 위한 신용정보에는 변화가 없음이 증명된다.

4.2.2 계산 경량성 평가

제안된 모델은 대상에 대한 신용정보를 (식 2)에서와 같이 개체에 대한 믿음의 정도로 정의하였으며, 이에 따른 계산량 감소가 가능하다. 또한 직접신용관계의 정의 및 간접신용관계를 정의하고 그에 따른 신용정보를 계산하는 과정에서 <표 3>과 같이 $J\phi sang$의 신용모델은 연산식이 복잡하며 산술연산 과정에서의 계산이 복잡하다[5,6]. 반면에 본 논문에서 제안된 신용모델은 간접신용의 신용조합 연산의 수행을 복잡한 산술연산 대신 (식 10),(식 11)같이 관계된 노

드들의 현재 신용상태에 대한 논리곱(AND)연산으로 정의하여 이에 따른 계산량 감소가 가능하다. 그리고 <표 3>에서 보는바와 같이 합의 연산에서도 제안된 신용모델은 조합연산을 통해 얻어진 다수의 신용권고들에 대하여 (식 12),(식 13),(식 14),(식 16)과 같이 신용상태 권고 빈도수에 대한 확률로 계산되며 이에 따른 계산의 복잡성 감소가 가능하다.

표 3. 제안 신용모델의 계산 경량성
Table 3. Lightweightness of calculation by the proposed trust model

			$J\phi sang$ 모델	제안모델
구성요소			$w_x = \{b_x, d_x, u_x\}$	$I_{E_x} = \{Bel(E_x)\}$
신용계산	직접신용		$w_y^x = \{b_y^x, d_y^x, u_y^x\}$	$I_{E_{xy}} = \{Bel(E_{xy})\}$
	간접신용	조합	$b_z^{xy} = b_y^x \bullet b_z^y$ $d_z^{xy} = b_y^x \bullet d_z^y$ $u_z^{xy} = d_y^x + u_y^x + b_y^x \bullet d_z^y$	논리곱연산 $S_{E_{1,n}(R)} = \{\wedge_{i=1}^{n-1}(S_{E_{i(i+1)}(c)})\} \wedge \{\wedge_{i=n-1}^{1} S_{E_{i(i+1)}(c)}\}$
		합의	$b_z^{xy} = (b_z^x \bullet u_z^y + b_z^y \bullet u_z^x)/n$ $d_z^{xy} = (d_z^x \bullet u_z^y + d_z^y \bullet u_z^x)/n$ $u_z^{xy} = (u_z^x \bullet u_z^y)/n$ $n = u_z^x + u_z^y - u_z^x \bullet u_z^y$	신용상태 권고 빈도수에 대한 확률 계산 (식12)~(식 16)

연산의 수행 빈도수 측면에서 $J\phi sang$의 신용계산 모델과 제안모델[25]을 비교하여 보면 <표 4>과 같다. <표 4>에서 m은 USN의 노드의 수를 나타내며 연산의 수행 빈도수는 각 모델의 곱셈연산자 수이다.

예를 들어, m=10인 경우 간접신용의 조합 연산의 수행 빈도수는 $J\phi sang$ 신용모델은 27, 제안모델은 9가 된다. 그리고, 간접신용의 합의 연산의 수행 빈도수는 $J\phi sang$ 신용모델은 54, 제안모델은 2가 된다.

<표 4>와 위 예의 결과를 분석하여 보면, $J\phi sang$의 신용계산 모델에 비해 제안모델이 평균 3배에서 6배 만큼 계산량이 감소됨을 알 수 있다. 또한 (그림 13)에서 보는 바와 같이 간접신용의 조합 연산량 있어 USN의 노드의 수가 증가함에 따라 $J\phi sang$의 신용모델을 적용할 경우보다 제안모델의 계산량이 적어짐을 알 수 있다.

표 4. 신용모델의 연산 빈도수
Table 4. Frequency of operations in trust model

			$J\phi sang$ 모델	제안모델
구성요소			3	1
신용계산	직접신용		3	1
	간접신용	조합	$3 \bullet (m-1)$	$(m-1)$
		합의	$6 \bullet (m-1)$	2

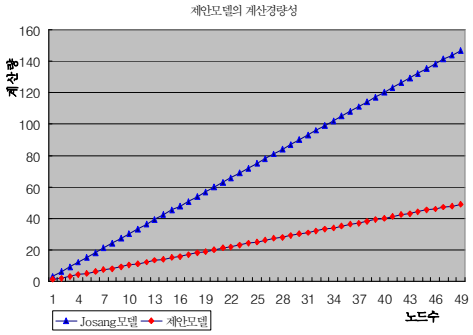

그림 13. 제안모델과 $J\phi sang$ 모델의 계산량 비교 (간접신용)
Fig 13. Comparison of calculating amount between proposed trust model and $J\phi sang$'s trust model (indirect trust)

V. 결 론

본 논문에서는 USN에 적합한 경량 신용모델을 제안하였다. 제안된 신용모델은 기존 $J\phi sang$의 연구에서 제안된 신용모델 보다 제4장의 <표 2>에 제시된 것 같이 계산 측면의 경량성이 존재한다.

또한 본 논문에서의 개선된 USN 신용모델은 김홍섭의 연구에서 제안된 USN에서의 신용기반 상호인증 모델의 "신용모델기반 상호인증" 과정에 적용 가능하다.

USN 신용모델에 기반한 상호인증 모델은 기존 연산량이 많고 절차가 복잡한 공개키 기반 인증 기법을 적용하지 않고 신용정보를 계산한다. 그리고 이를 기반으로 하여 USN 노드 상호간의 믿음의 정도를 고려하여 인증하기 때문에 인증 과정의 연산량을 줄일 수 있다. 따라서 경량성을 높이며 한정된 배터리 소모를 줄여 USN의 생존 기간 연장이 가능

하게 될 것이다.

이와 관련된 앞으로의 연구 진행 계획으로 첫째, 제안된 USN 신용모델을 적용한 기존 상호인증 모델의 개선 및 확장, 둘째, 방대한 USN에서의 계층적 그룹 단위의 신용모델 설계에 관한 연구, 셋째, 제안된 신용모델을 적용한 역할 기반 접근 통제(RBAC) 방법, 넷째, 신용모델을 적용한 다양한 USN 보안기술로의 응용에 대한 연구를 수행할 계획이다.

참고문헌

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

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

[3] 김홍섭, 조진기, 이상호, "신용모델 기반의 경량 상호인증 설계", 한국컴퓨터정보학회논문지, 제10권, 제3호, PP.237-247, 2005년.

[4] 김신효, 강유성, 정병호, 정교일, "U-센서 네트워크 보안 기술동향", 한국전자통신연구원 전자통신동향분석, 제20권, 제5호, PP.93-99, 2005년.

[5] 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.

[6] 조영복, 정윤수, 김동명, 이상호, "유비쿼터스 센서네트워크에서의 저전력 상호인증 프로토콜", 한국컴퓨터정보학회논문지, 제 2권, 제34호, PP. 187-197, 2005년.

[7] H. Chan, A. Perrig, D. Sung, "Random Key Predistribution Schemes for Sensor Networks," In Proceedings of the IEEE Security and Privacy, 2003 Symposium, P197-213, 2003.

[8] G. Gaubatz, J. P. Kaps, B. Sunar, "Public Key Cryptography in Sensor Networks-Revisited," In Proceedings of the European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), LNCS 3313, Heidelberg, Germany, 2004.

[9] J. Hoffstein, J. Pipher, J.H.Silverman, "NTUR:A new high speed public key cryptosystem," In Proceedings of the Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, Lecture Notes in Computer Science 1423 (J.P.Buhler,ed). Springer-Verlag. PP. 267-288, 1998.

[10] Kaan Yuksel, Jens-Peter Kaps, Berk Sunar, "Universal Hash Functions for Emerging Ultra-Low-Power Networks," In Proceedings of the Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Diego, CA, Jan. 2004.

[11] 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 '03, Washington D.C., Oct. 2003.

[12] L. Echenauer, V. D. Gligor, "A Key-Management scheme for Distributed Sensor Networks," In Proceedings of the 9th computer communication security, PP. 41-47, 2002.

[13] Laurent Bussard, Yves Roudier, "Authentication in Ubiquitous Computing," In Proceedings of the Workshop on Security in Ubiquitous Computing UBICOMP 2002, 2002.

[14] Minoru Matsumoto, Yasushi Takagi. "Mutual Authentication Method for Ubiquitous Service Environmentss," In Proceedings of the Global Telecommunications Conference '03. GLOBECOM '03. IEEE Vol. 3, PP. 389-393, 2003.

[15] K. E Person and D. Manivannan, "Secure Connection in Bluetooth Scaternets," System Sciences '03. In Proceedings of the 36th Annual Hawaii International Conference, PP. 10-19. 2003.

[16] 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.

[17] 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.

[18] R. Yahalom, B. Klein, and T. Beth, "Trust relationships 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.

[19] A. Abdul-Rahman and S. Halles, "A distributed trust model," In Proceedings of New Security Paradigms Workshop '97, PP. 48-60, 1997.

[20] 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.

[21] 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, 2003.

[22] 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.

[23] Y. Teng, V. V. Phoha, and B. Choi, "Design of trust metrics based on dempster-shafer theory," 39th Annual ACM Southeast Conference, Mar. 2001.

[24] D. W. Manchala, "Trust metrics, model and protocol for electronic commerce transactions," In The 18th International Conference on Distributed Computing Systems, 1998.

[25] A. *Jøsang*, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzzyness and Knowledge-Based Systems, Vol. 9, PP. 279-311, 2001.

[26] B. Shand, N. Dimmock, and J. Bacon, "Trust for Ubiquitous, Transparent Collaboration," In Proceedings 1st IEEE Annual Conference on Pervasive Computing and Communication 2003, Mar. 2003.

저 자 소 개

김 홍 섭

1998년~현재 충북대학교 대학원
전자계산학과 박사과정(수료)
1994년~현재 청주 주성대학
컴퓨터프로그래밍과 부교수
<관심분야> 네트워크보안,
네트워크구조, 네트워크관리

이 상 호

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