

논문 2020-2-6 <http://dx.doi.org/10.29056/jsav.2020.12.06>

# M2M 애플리케이션 서비스를 위한 하이브리드형 신뢰 평가 모델

김유경\*†

## Hybrid Trust Computational Model for M2M Application Services

Yukyong Kim\*†

### 요 약

IoT 환경의 최종 사용자 도메인에서 점점 더 많은 수의 지능형 M2M(Machine-to-Machine Communication) 장치가 애플리케이션 서비스를 생성하고 공유하기 위한 자원을 제공한다. 따라서 기존의 중앙집중식 서비스 제공자의 역할을 P2P 환경의 최종 사용자에게 이전하여 신뢰를 관리하는 것은 매우 유용할 수 있다. 그러나 최종 사용자가 독립적으로 서비스를 제공하거나 소비하는 비중앙집중식 M2M 컴퓨팅 환경에서는 상호간의 신뢰 구축이 가장 중요한 요인이 된다. 오작동하는 서비스를 구축하려는 악의적인 사용자들이 IoT와 같은 M2M 컴퓨팅 환경에서 보안문제를 야기할 수 있기 때문이다. 본 논문에서는 M2M 애플리케이션 서비스의 신뢰 평가를 위한 통합적인 분석과 접근방식을 제공하고, M2M 커뮤니티의 사용자들 사이의 신뢰도를 보장할 수 있는 최적화된 신뢰 평가 모델을 제시한다.

### Abstract

In the end-user domain of an IoT environment, there are more and more intelligent M2M devices that provide resources to create and share application services. Therefore, it can be very useful to manage trust by transferring the role of the existing centralized service provider to end users in a P2P environment. However, in a decentralized M2M computing environment where end users independently provide or consume services, mutual trust building is the most important factor. This is because malicious users trying to build malfunctioning services can cause security problems in M2M computing environments such as IoT. In this paper, we provide an integrated analysis and approach for trust evaluation of M2M application services, and an optimized trust evaluation model that can guarantee reliability among users of the M2M community.

**한글키워드** : M2M애플리케이션, IoT 서비스, 서비스 신뢰, 신뢰 평가, 하이브리드 모델

**keywords** : M2M application, IoT service, trustworthy service, trust evaluation, hybrid model

\* 숙명여자대학교 기초공학부

† 교신저자: 김유경(email: ykim.be@sm.ac.kr)

접수일자: 2020.11.04. 심사완료: 2020.12.07.

게재확정: 2020.12.21.

## 1. 서론

사물인터넷(IoT, Internet of Things)은 각종

사물들에 통신 기능을 내장해서 인터넷에 연결함으로써, 사람과 사물, 그리고 사물과 사물 간의 인터넷 기반 상호 소통을 다루는 개념이다. IoT 인프라에서 수십억 개의 기기종 장치들은 보편적이고 지능적인 서비스를 지원하기 위해 연결되어 있으며, 오늘날의 IoT 생태계에는 물리적 장치와 사이버 구성요소 간의 네트워킹뿐만 아니라, 이들의 사회적 상호작용이 포함되는 개념이라고 할 수 있다[1].

이러한 IoT 환경에서는, 점점 더 많은 수의 지능형 장치가 M2M(Machine-to-Machine) 애플리케이션 서비스를 생성하고 공유하기 위한 좋은 자원을 제공하게 되고, 따라서 IoT 기술은 사물들 간의 연결을 전제로 한다는 측면에서 연결되는 대상을 신뢰할 수 있어야 한다.

신뢰는 다양한 개념으로 이해되고 있지만, “특정 관계가 있는 한 대상(Trustor)이 다른 대상(Trustee)에 대해, 중요하고 특별한 행동을 할 것이라는 기대를 가지고 그 대상 (Trustee)의 행동이 야기할 위험을 감수할 의사”라는 정의가 가장 넓게 받아들여지고 있다[2].

IoT 환경은 다양한 장치들과 응용 서비스의 연결, 그리고 이들 사이에 발생하는 상호작용을 전제로 하고 있기 때문에, 사용자들이 위험과 불확실성을 경험할 가능성을 내재하고 있으므로, 이러한 신뢰의 개념은 IoT의 맥락에서도 매우 중요한 의미를 가진다고 할 수 있다. 따라서 이런 위험과 불확실성을 감수한 상태에서, 사용자들이 연결을 허용하고 어플리케이션을 실행하기 위해서는 무엇보다 먼저 신뢰가 담보되어야 한다. 그러나 어떻게 신뢰를 정의하고 측정하고 분석하고 활용할지에 대한 연구는 미흡한 단계이다.

신뢰 평가는 중앙집중형(centralized approach), 분산형(distributed approach), 그리고 하이브리드형인 비중앙집중식(decentralized approach)으로 분류해 볼 수 있다.

중앙집중형 방식에서 신뢰와 관련된 요청과 서비스는 중앙집중형 플랫폼을 통해 제공되고, 이 중앙집중형 플랫폼은 도메인에 존재하는 모든 다른 노드들이 접근할 수 있게 된다. 이런 중앙집중형 플랫폼은 신뢰 협상이나 신뢰 값의 계산뿐만 아니라 신뢰 평가를 위해 필요한 초기 정보를 제공함으로써 다른 사용자들의 의사 결정을 지원하기 위한 모든 신뢰 정보를 관리하는 책임이 있다.

반면, 분산형 접근 방식에서 각 노드는 개별적인 신뢰 에이전트가 되고, 모든 필요한 계산은 로컬에서 수행을 하게 된다. 모든 노드들은 이웃하는 노드들과 정보를 교환하고, 관찰하면서 신뢰를 평가할 수 있다. 예를 들면, 신뢰 평가자(trustor) 노드는 직접 신뢰 측정을 하거나 혹은 다른 글로벌 단말(peer)로부터 제공받은 보고를 기반으로, 자신이 가지고 있는 정보와 비교함으로써 신뢰평가 대상자(trustee)의 최종 신뢰 값을 추정할 수 있다.

하이브리드형 접근방식은 중앙집중형 방식과 분산형 방식의 장점을 결합한 형태라고 할 수 있다. 중앙집중형 접근방식에서는 한 개체가 중앙의 개체에 의존을 하기 때문에, 요청 개체에 전달해야 하는 시점에 요청에 의해서만 신뢰 정보가 계산될 수 있다. 반면에, 분산형 접근 방식은 정기적으로 신뢰를 계산하고, 이것을 토폴로지 전체에 전파를 할 수 있다. 그러나 IoT와 같은 기기종 장치들로 구성된 대규모 네트워크 환경에서는, 각 장치들은 신뢰를 평가하기 위한 정보를 유지할 만큼의 자원을 가질 수 없을 가능성이 높기 때문에, 신뢰할 수 있는 에이전트와 같은 다른 개체들의 도움이 필요하게 된다. 또한 실시간 신뢰 정보를 주고받기 위한 신뢰 데이터 흐름으로 인해 통신 오버 헤드가 발생하여 네트워크 성능과 제한된 배터리 수명에 영향을 줄 수 있다는 것을 고려해야 한다. 그래서, IoT와 같은 환경에

서 신뢰 평가는 하이브리드식으로 접근하는 것이 좀 더 적합하다고 할 수 있다.

IoT 환경의 분산적 특성으로 인해 IoT 개체들 간의 신뢰 관계 형성이 필요하다. 이러한 신뢰 관계는 주로 서비스를 통한 상호작용을 바탕으로 평가하게 되는데, 본 논문에서는 IoT 환경과 같은 M2M 애플리케이션 서비스를 위한 하이브리드 접근방식의 신뢰평가 모델을 제안한다.

논문의 구성은 다음과 같다. 먼저, 2장에서는 IoT 애플리케이션에 대한 기존의 신뢰 평가 모델에 대해 살펴보고, 3장에서 M2M 어플리케이션 서비스를 위한 하이브리드 접근방식으로 최적화된 신뢰 평가 시스템을 제안한다. 4장에서 제안된 모델에 대한 정성적 평가와 함께 실험의 결과를 제시하고, 5장에서는 결론 및 향후 연구 방향에 대하여 기술한다.

## 2. 관련 연구

정책 기반 접근방식이나 지식 기반 또는 지능형 학습 알고리즘 기반과 같은 접근방식들을 포함해서, 평판이나 피드백을 중심으로 하는 접근 방식과 같이 몇 가지 일반적인 신뢰 평가 모델이 있다. 이러한 신뢰 평가 모델은 IoT를 포함한 다양한 네트워크 환경에 대해 연구되고 있으나 주로 웹서비스와 서비스지향 아키텍처 기반의 신뢰 평가 모델을 IoT 환경으로 확장해서 적용하고 있으며, IoT에 대한 신뢰 관리 연구는 초기 단계에 있다고 할 수 있다.

현재 제시된 IoT 환경에서의 신뢰 평가 모델 대부분은 전자 상거래 서비스를 위한 소셜 네트워크에 대한 평판 시스템을 이용하거나, P2P 네트워크와 같은 분산 시스템에서 신뢰 관리 메커니즘을 기반으로 하는데, 이러한 방법은 주로 직접 관찰 정보나 제3자 정보에 의존하기 때문에

정보가 충분하지 않다는 문제가 있다[3].

일부 신뢰 모델은 신뢰 수준을 평가하기 위해 믿을 만한 에이전트(TA)와 관련된 평가 메커니즘을 도입하기도 하지만, 모바일 네트워크와 같은 일부 환경에서는 제3자 정보를 관리하기 위해 중앙집중식 시스템을 유지해야하기 때문에 직접적인 관찰 정보만 얻을 수 있다는 한계가 있다 [4]. [5]에서 제안한 퍼지모델을 이용한 평판 시스템이나, [6, 7]에서 정의한 사회적 신뢰와 QoS 신뢰도를 모두 고려한 신뢰 관리 프로토콜은 직접적인 관찰과 간접 권고를 사용하여 신뢰를 갱신하도록 했다.

일부 신뢰 모델에서는 다양한 유형의 신뢰를 평가하기 위해, 신념의 가치를 형성하는 인간의 인지과정을 모방하기도 한다. P2P 네트워크 및 소셜 네트워크의 신뢰 관리를 위해 제안된 모델은 개인 간의 상호작용을 기반으로 하여 신뢰를 평가한다[8]. [9]에서 정의한 평판은 평가대상과의 상호작용에 의해 파생된 직접적 또는 간접적 정보이며, 이 평판은 다른 개체에 대한 신뢰 수준을 평가하는 데 사용할 수 있다.



그림 1. 평판기반 신뢰 모델

Fig. 1. Reputation based trust model

그림 1에서 보는 것과 같이, 평판기반 신뢰 모델에서 각 평가자들은 평가대상자와의 상호 작용 후에, 각 상호 작용에 대한 만족도를 기록하여 평판 시스템에 피드백을 통해 제공한다. 그러면, 평판 시스템은 이런 모든 피드백을 누적하여, 특정 신뢰 평가 대상에 대해 하나의 평판 값을 생

성하게 되고, 평가자는 이런 평판 값을 의사 결정에 이용할 수 있다.

최근 대부분의 연구에서는 신뢰의 가장 중요한 요소로 평판을 다루고 있다. 기본적으로 평판 시스템은 상호 작용이 발생한 후 대상들로부터 피드백을 수집하게 된다. 이 피드백은 평판점수를 얻기 위해 여러 수학적 모델을 결합해서 계산되어 제공된다. 전자 상거래 시스템이나 웹 서비스와 관련된 여러 평판 시스템이 개발되었는데, 이러한 시스템들은 주로 중앙집중 방식으로, 상호작용이 이루어진 이후 사용자로부터 등급과 피드백을 얻은 다음, 여러 수학적 모델을 사용하여 전체 평판 점수를 계산한다[10, 11, 12]. 시간이 지남에 따라 두 개체 간에 신뢰가 설정되고 유지되어 "신뢰의 웹"이 만들어지는 신뢰 네트워크를 구축하려는 일부 연구 작업도 있다[13, 14].

본 논문에서는 기존의 연구가 전자상거래와 같은 평판기반 시스템을 IoT에 적용하였던 것에 비해, 상대적으로 SOA 기반 IoT 시스템의 신뢰 관리에 중점을 두고자 한다. 기존의 소셜 네트워크와 달리 IoT 네트워크는 수많은 기기종의 장치들이 있으며 각 장치의 저장 용량은 매우 제한적이라는 특징을 갖고 있다. 이러한 제약 조건을 고려하여 신뢰 변수 설정을 동적으로 조정하여 유사한 사회적 관심사를 공유하는 노드에서 신뢰 피드백을 선택하도록 함으로써 신뢰 추정에 대한 편향을 최소화하도록 설계한다.

### 3. 하이브리드형 신뢰평가 모델

본 논문에서 정의하는 M2M 서비스를 위한 하이브리드형 신뢰평가 모델은 동료에 대한 초기 신뢰수준에 대한 정보를 제공하거나 평가에 관여하는 중앙집권적 실체가 없다. 그림 2에서 보는 것과 같은 중앙집중형식에서 벗어난 M2M 애플

리케이션 실행 환경에서, 서비스 제공자 및 서비스에 대한 신뢰 수준은 본 논문의 주요 목표인 최적화되고 신뢰할 수 있는 신뢰 평가 시스템에 의해 보장되어야 한다. 또한 오작동 서비스를 제공하는 나쁜 의도를 가진 서비스 제공자나 장치들은 낮은 신뢰 점수로 평가되어야 하며 서비스 제공자 목록에 존재하지 않도록 해야 한다.

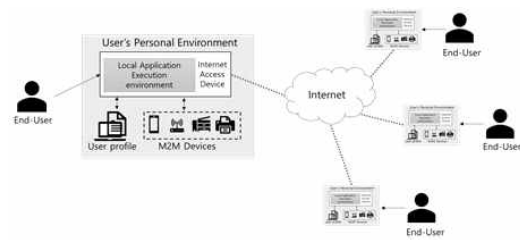


그림 2. 하이브리드형 M2M 애플리케이션 실행 환경

Fig. 2. Decentralized M2M application execution environment

#### 3.1 신뢰 평가 시스템 개요

본 논문에서는 M2M 서비스를 제공하는 네트워크 상에서 지역을 중심으로 커뮤니티를 설정하고, 커뮤니티 내의 다른 장치들이 수행하는 모든 활동을 신뢰 평가 프로세스에 포함시키고자 한다. 따라서 중앙집중형 에이전트가 아닌, 각 커뮤니티에서 신뢰 평가에 대한 테스트를 담당하는 지역 에이전트 역할을 정의한다. 분산된 방식으로 신뢰 평가가 가능하도록 하기 위해서는 지역 에이전트가 M2M 커뮤니티의 새로운 서비스의 기능과 행동에 대한 시험을 통해 신뢰정보를 제공할 수 있고, 이를 통해 커뮤니티에 소속된 멤버들에 대한 자체적인 신뢰 수준을 증가시킬 가능성을 높이고자 한다.

본 논문에서 제안하는 신뢰 평가 모델은 초기 신뢰 점수를 계산하고, 초기 점수를 기반으로 상호작용을 통해 계산되는 서비스에 대한 신뢰 등

급 산출로 이루어진다. 또한 서비스와 서비스 제공자에 대한 신뢰를 평가하기 위해서는 상호작용을 통해 얻어지는 경험치 뿐만 아니라 서비스의 기능성과 가용성 등 다른 매개변수를 고려해야 한다.

IoT환경에서 일반 센서나 IoT 장치 등과 같은 자원은 신뢰도를 평가하고 각 커뮤니티에 연결되어 있는 최종 신뢰 점수를 집계하고 계산하는 신뢰 관리자와 연결된다. 자원의 제약이 심한 IoT 환경에서, 신뢰 관리자는 각 장치에 직접 연결되는 더 강력한 네트워크 구성요소에 배포되는 것으로 가정한다. 또는 장치 자체내에 배포될 수 있다. 이렇게 생성되는 신뢰 데이터는 블록체인 네트워크로 브로드캐스트하는 방식을 이용하여, 각 신뢰 데이터를 저장하고 참여 장치 간의 신뢰 데이터 교환을 분산된 방식으로 검증할 수 있을 것이다.

신뢰 관리자(Trust Manager)는 신뢰 점수에 대한 무결성이나 유효성에 관련된 위험을 관리하게 되므로, IoT 장치 및 서비스가 서로 상호작용하고, 신뢰를 구축할 수 있는 안정적인 환경을 만들 수 있다. 이런 신뢰 관리자를 통해 평가된 신뢰 점수를 바탕으로 믿을 수 있는 서비스를 선택하고 데이터를 수집할 수 있다. 신뢰는 평가자(trustor)와 평가대상자(trustee) 사이에서의 관계로 정의할 수 있다. 이 관계는 평가가 이루어진 시간 값으로 제한이 된다. 이 신뢰 관계는 직접적인 관찰과 상호작용에서 도출되는 직접 신뢰와 커뮤니티 멤버들 사이에서 교환되는 추천사항을 바탕으로 하는 간접 신뢰로부터 파생된다고 할 수 있다. 신뢰는  $T(e_i \rightarrow e_j)_t$ 로 표현하고, 이것은 주어진 시간  $t$ 에서 평가자  $e_i$ 와 평가대상자  $e_j$  사이의 신뢰 관계를 나타낸다. 이 신뢰관계에는 다음 식 1과 같이 평가자  $e_i$ 가 시간  $t$ 에서  $e_j$ 에 대해 갖는 신뢰 점수를 나타내는  $T_{ij}(t)$ 가 할당

된다. 이 점수는 0에서 1까지의 연속 범위를 갖는다. 여기서 0은 완전한 불신을 나타내고 1은 절대적인 신뢰를 나타낸다고 할 수 있다.

$$T(e_i \rightarrow e_j)_t = T_{ij}(t) \quad \dots\dots\dots (식 1)$$

먼저 신뢰 관련 정보가 수집이 되는데, 이때 각 장치들 사이의 송수신 동작의 직접적인 관찰과 커뮤니티 멤버들에 의해 제공되는 추천값을 고려하게 된다.

신뢰는 각 장치들 또는 장치들이 제공하는 서비스에 대해 계산이 된다. 신뢰는 직접 신뢰(Direct Trust)와 간접 신뢰(Indirect Trust)로 계산되며, 각 계산은 몇가지 속성과 메트릭을 기반으로 이루어진다. 직접 신뢰는 각 장치들 사이의 협력과 서비스 능력 및 관심 커뮤니티 등을 고려하여 평가하고, 간접 신뢰는 각 멤버들에 의해 공유되는 추천 값을 기반으로 계산한다. 특정 시간 간격  $\Delta t$  동안 이루어진 과거의 평가 기록 뿐만 아니라 이런 여러 속성들을 조합하는 것은 보안을 보장하면서 좀더 효과적으로 전체적인 신뢰 값을 생성할 수 있다. (식 2)와 같이 시간 간격  $\Delta t$  동안 수행된 기록을 기반으로 이루어진 평가와 가장 최근의 신뢰 평가 값을 결합하여, 최종적인 신뢰 점수를 얻게 된다.

$$T_{ij}(t) = w_1 * \hat{T}_{ij}(t-1) + w_2 * \hat{T}_{ij}(\Delta t) \quad \dots\dots\dots(식 2)$$

여기에서  $\hat{T}_{ij}(t-1)$ 과  $\hat{T}_{ij}(\Delta t)$ 에 각각 할당되는 가중치 값  $w_1$ 과  $w_2$ 는  $w_1 + w_2 = 1$ 이고,  $0 \leq w_1, w_2 \leq 1$ 이다. 이렇게 과거에 이루어진 신뢰 평가를 고려하는 것은 각 개체들의 행동(behavior)이 항상 일정하지 않고, 종종 시간에 따라 변경되기 때문이다.

신뢰 평가를 위해서, 각 개체들은 상호작용을 하는 이웃들에 대해 협동성, 역량 및 관심 커뮤니티

니티와 같은 다양한 신뢰 속성들을 유지해야 한다. 협동성은 개체  $e_j$ 에 대해 시간 간격  $[0..t]$  동안 행위를 모니터링 한 결과를 기반으로 개체  $e_i$ 가 평가한 협력의 수준을 반영한다.

역량은 개체가 의도한 작업을 수행 할 수 있는 능력의 정도를 나타내는데, 작업을 수행하기에 충분한 능력이 있는지 여부를 확인하기 위해 보유한 에너지 및 계산 능력을 기준으로 평가한다. 관심 커뮤니티 속성은 총 커뮤니티 관심사 수에 대한 공통 커뮤니티 관심사 수의 비율로 계산된  $e_i$ 가 평가 한  $e_j$ 의 공통 관심사 또는 유사한 작업의 정도이다.

### 3.2 신뢰 매트릭스(Trust metrics)

신뢰 관리자는 다음 (식 3)을 사용하여 기본적인 신뢰값을 계산한다. 추천값을 사용하기 위해, 각 IoT 서비스에 대한 사용자의 피드백이 가능하고 유효하다고 가정한다.

$$\hat{T}_{ij} = E_{ij} * DT_{ij} + (1 - E_{ij}) * IT_{ij} \dots\dots(식 3)$$

#### (1) 직접 신뢰 측정

(식 3)에서  $DT_{ij}$ 는 QoS(Quality of Service) 속성에 따른  $e_j$ 에 대한  $e_i$ 의 평가라고 할 수 있다. 이는 여러 QoS 속성을 이용하여 각 서비스의 비 기능적 측면을 평가하여 직접 평가하게 되는 신뢰 값이다.

예를 들어,  $Q_1, Q_2, Q_3, Q_4$ 가 응답 시간이나 처리량과 같은 품질속성을 나타낸다고 하자. 그러면,  $Q = \{Q_1, Q_2, Q_3, Q_4\}$ 의 각 QoS 속성  $Q_x$ 에 대해 가중치  $w_x$ 가 할당되고,  $1 \leq x \leq 4$ 에 대해,  $0 \leq w_x \leq 1$  및  $\sum w_x = 1$ 이다.

여기에서 단위와 무관하게 균일한 측정을 하기 위해 QoS 값을 정규화해야 한다. 이 정규화를 사용하여 QoS 값은 각 IoT 장치가 제공하는 서

비스 품질에 대한 균일한 인덱스를 제공한다. 이 품질 속성을 가지고  $DT$  값을 계산하기 위해 행렬  $QM$ 을 정의한다.

$S = \{S_1, S_2, \dots, S_n\}$ 이 동일한 기능을 제공하는 서비스 집합이라고 하자. 아래 나타난 것과 같이  $QM$ 의 각 행은 서비스를 나타내고, 각 열은  $Q_x$ 를 나타낸다.

$$QM = \begin{bmatrix} q_{1,1} & q_{1,2} & q_{1,3} & q_{1,4} \\ q_{2,1} & q_{2,2} & q_{2,3} & q_{2,4} \\ \vdots & \vdots & \vdots & \vdots \\ q_{n,1} & q_{n,2} & q_{n,3} & q_{n,4} \end{bmatrix}$$

행렬을 정규화하기 위해, 두 개의 벡터를 사용한다. 첫 번째 벡터  $N = \{n_1, n_2, n_3, n_4\}$ 이며 여기서  $n_j (1 \leq j \leq 4)$ 의 값은 0 또는 1이 된다.  $n_j = 1$ 은  $q_i$ 값의 증가가 이득이 되는 경우에 사용되고,  $n_j = 0$ 은  $q_i$ 값의 감소가 이득이 되는 경우에 사용한다. 두 번째 벡터  $C = \{c_1, c_2, c_3, c_4\}$ 는 최대 정규화 값을 설정하기 위한 것으로,  $c_j (1 \leq j \leq 4)$ 는 최대 정규화 값을 설정하는 상수이다. 벡터  $V$ 의 각 요소는 다음 (식 4)와 (식 5)를 사용해서 정규화한다.

$$v_{i,j} = \begin{cases} \frac{q_{i,j}}{\frac{1}{n} \sum_{i=1}^n q_{i,j}} & \text{if } \frac{1}{n} \sum_{i=1}^n q_{i,j} \neq 0 \text{ and } n_j = 1 \\ & \text{and } \frac{q_{i,j}}{\frac{1}{n} \sum_{i=1}^n q_{i,j}} < c_j \\ c_j & \text{if } \frac{1}{n} \sum_{i=1}^n q_{i,j} = 0 \text{ and } n_j = 1 \\ & \text{and } \frac{q_{i,j}}{\frac{1}{n} \sum_{i=1}^n q_{i,j}} \geq c_j \end{cases} \quad (식 4)$$

$$v_{i,j} = \begin{cases} \frac{q_{i,j}}{\frac{1}{n} \sum_{i=1}^n q_{i,j}} & \text{if } q_{i,j} \neq 0 \text{ and } n_j = 0 \\ & \text{and } \frac{q_{i,j}}{\frac{1}{n} \sum_{i=1}^n q_{i,j}} < c_j \\ c_j & \text{if } q_{i,j} = 0 \text{ and } n_j = 0 \\ & \text{and } \frac{1}{n} \sum_{i=1}^n q_{i,j} \geq c_j \end{cases} \quad (식 5)$$

이 두 식을  $QM$ 에 적용해서 다음과 같은  $QM'$ 을 얻을 수 있다.

$$QM' = \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} & v_{1,4} \\ v_{2,1} & v_{2,2} & v_{2,3} & v_{2,4} \\ \vdots & \vdots & \vdots & \vdots \\ v_{n,1} & v_{n,2} & v_{n,3} & v_{n,4} \end{bmatrix}$$

그러면, 다음 (식 6)을 이용해서  $DT_{ij}$ 를 계산할 수 있다.  $e_i$ 와  $e_j$ 간의 상호 작용을 통해 각 QoS 속성은 로깅 데이터, 실제 실행 시간 및 사용자 요청에 대한 응답 시간과 같은 과거 상호 작용의 기록 데이터에 따라 추정할 수 있다.

$$DT_{ij} = \sum (v_{j,k} * w_k) \quad \dots\dots\dots(\text{식 6})$$

여기서  $v_{i,k}$ 는  $QM'$ 의 요소이고  $w_k$ 는 품질 값  $v_{i,k}$ 에 대한 가중치이다.

(2) 간접 신뢰 측정

실제 상황에서 사람들은 잘 모르는 사람에 대한 의견을 형성하기 위해, 잘 아는 사람들의 의견을 반영하게 된다. 대부분의 경우, 각 개인에 대한 평판을 결정하기 위해 중앙집중식 권한에 의존하지는 않는다. 간접 측정의 기본 특성 중 하나는 완전한 지역적 분석을 기반으로 한다는 것이다. 서비스의 신뢰 수준을 간접적으로 추정하기 위해, [15]에 정의된 평판 추론 알고리즘을 수정하여 적용한다. 본 논문에서는 그림 3과 같이 A의 인접 노드에서 시작하여 노드 A에서 시작하여 B 또는 B'의 평판 등급을 추론하도록 확장한다.

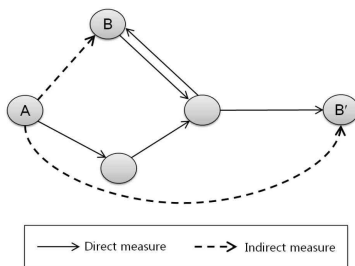


그림 3. 신뢰 관계 측정  
Fig. 3. Trust measurement

다음 그림 4는 (식 3)에서  $IT_{ij}$ 를 계산하는 데 사용되는 알고리즘이다. 다음 알고리즘에서 싱크는 등급을 요구하는 노드이고 소스는 등급이 매겨질 노드를 나타낸다. 즉, 소스는  $e_i$ 이고 싱크는  $e_j$ 가 된다. 이 매트릭스에서 소스는 신뢰 등급을 부여한 각 이웃을 폴링하고, 각 소스의 인접 노드는 싱크에 대한 등급을 반환한다. 등급은 평균값으로 계산되고, 이 평균값은 소스에서 싱크까지 추론된 신뢰 등급이며,  $Rating(a,b)$  함수는 a와 b 간의 직접 측정된 신뢰값  $QoS_{a,b}$ 를 가져온다.

```

Input: source and sink
Output: the trust value of the sink
TrustInfer(source, sink) {
  numberOfAdjacentNodesWithRatings = 0 ;
  sumOfRatings = 0 ;
  mark source seen ;
  if sink is adjacent to source
    source's rating of sink = Rating(source, sink) ;
  else
  {
    for each n adjacent to source {
      if n is unseen {
        if n has no ratingOfSink {
          mark n seen ;
          inferredRating = TrustInfer(n, sink) ;
          sumOfRatings += inferredRating ;
          n's rating of sink = inferredRating ;
          numberOfAdjacentNodesWithRatings ++ ;
          mark n unseen;
        }
        else {
          sumOfRatings += n's rating of sink ;
          numberOfAdjacentNodesWithRatings ++ ;
        }
      }
    } //end for
    if numberOfAdjacentNodesWithRatings > 0
      source's rating of sink =
        sumOfRatings/numberOfAdjacentNodesWithRatings ;
    else
      source's rating of sink = ∞ ;
  } //end else
  return source's rating of sink ;
} //end TrustInfer( )
    
```

그림 4. 간접측정값 추정 알고리즘  
Fig. 4. The  $IT_{ij}$  computation algorithm

4. 실험 및 분석

신뢰 값을 계산하기 위해, 수집된 120개의 IoT 서비스에 대해 응답 시간 (밀리 초), 처리량 (밀리초당 완료된 요청 수), 결과의 정확성(%)과

가용성(%)의 네 가지 품질 속성을 정의하였다. (식 3)에 따라 계산된 평가 결과에 따라, 신뢰수준이 가장 높은 서비스가 반환된다. 각 서비스 및 인접 노드에 대해 직접 측정 계산이 우선 이루어진다. 예를 들면, 각 서비스  $S_1, S_2, S_3, S_4$  및  $S_5$ 의 신뢰 수준은 동일 커뮤니티 내에 있는 인접 노드에 의해 평가가 된다. 서비스  $S_1$ 이  $S_7, S_{12}$  및  $S_{20}$ 과 인접하고 있다면, 경험 계수  $E_{7,1}, E_{12,1}$  및  $E_{20,1}$ 과 직접 측정 값  $DT_{7,1}, DT_{12,1}$  및  $DT_{20,1}$ 이 계산된다.  $S_1$ 이  $S_7$ 과 5 번 상호 작용하면  $E_{7,1} = 1 - e^{-2.5}$ 이다. 설명의 편의를 위해  $S = \{S_1, S_2, S_3, S_4\}$ 가  $S_7$ 에 인접한 노드들의 집합이라고 정의하고,  $QM$ 이 다음 그림 5와 같이 정의된다면, (식 4)와 (식 5)에 따라 다음과 같이  $[0, 1]$ 로 정규화된다.

$$QM = \begin{bmatrix} 0.01 & 7.3 & 99.8 & 99.4 \\ 0.03 & 7.0 & 99.5 & 99.8 \\ 0.02 & 7.2 & 99.6 & 99.8 \\ 0.03 & 7.1 & 99.7 & 99.6 \end{bmatrix}$$

$$QM' = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0.5 & 0.67 & 0.33 & 1 \\ 0 & 0.33 & 0.67 & 0.5 \end{bmatrix}$$

그러면  $DT_{i,j}$ 는  $QM'$ 의  $j$ 번째 행에 있는 요소의 가중합계로 계산된다. 가중치를 동일하게 부여한다면,  $DT_{7,1} = 3 \times (1 \times 0.25) + (0 \times 0.25) = 0.75$ 가 된다. 서비스  $S_2, S_3, S_4$  및  $S_5$ 의 경우에도 유사하게 직접 측정 값이 계산된다. 두 노드  $S_1$ 과  $S_7$ 이 서로 인접하지 않은 경우 간접 측정 값을 계산해야한다. 앞서 정의된 알고리즘은 간접 측정 값으로  $IT_{7,1}$  값을 반환한다. 그러면 이들 IT와 DT 값을 이용해서 신뢰값을 얻게 된다. 표 1은 실험에 사용된 서비스들 중에 일부 서비스에 대해 계산된 신뢰 수준입니다. 표 1에서 서비스  $S_5$ 는 품질 속성의 가중치와 상관없이 가장 신뢰할 수 있는 서비스라고 할 수 있다. 따라서 제안된 방법은 항상 서비스  $S_5$ 를 사용자의 요구 사항

을 충족하는 신뢰할 수 있는 서비스로 반환하게 될 것이다.

표 1. 신뢰수준 계산 결과 예  
Table 1. The result of evaluation

Attribute weight	Trust level				
	S1	S2	S3	S4	S5
Even	0.67	0.65	0.72	0.76	0.81
AC=0.4, RT=T=A=0.2	0.6	0.79	0.7	0.62	0.8
RT=0.4, AC=T=A=0.2	0.78	0.69	0.73	0.65	0.78

AC: Accuracy, RT: Response Time, T: Throughput, A: Availability

그림 5는 제안된 모델과 품질의 평균값에 기반한 서비스 평가 방식에 대해, 정확한 선택의 비율을 보여준다. 신뢰 모델은 직접적인 상호 작용을 기반으로하기 때문에 제안된 모델은 일정 시간이 지난 후 경험 데이터가 충분할 때 매우 유용하다고 할 수 있다. 제안된 모델의 선택의 평균 정확도는 83.63%이고 품질의 평균값을 기반으로 하는 경우의 평균 정확도는 71.58%다. 그렇지만 그림 5에서 볼 수 있듯이, 트랜잭션 처리의 누적 횟수가 250회 이상에서는 제안된 모델의 정확도가 평균값을 기반으로 하는 경우보다 확연하게 높아지는 것을 알 수 있다.

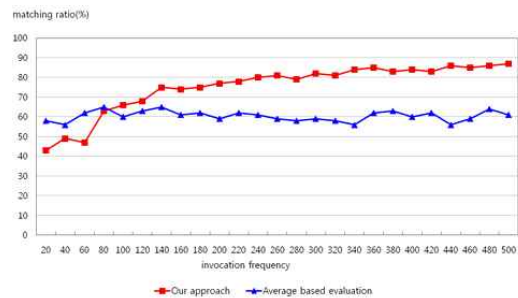


그림 5. 선택의 정확도 비율  
Fig. 5. The accuracy ratio of selection

## 5. 결론

최종 사용자가 독립적으로 서비스를 제공하거나 소비하는 비중앙집중식 M2M 컴퓨팅 환경에서는 상호간의 신뢰 구축이 가장 중요한 요인이 된다. 오작동하는 서비스를 구축하려는 악의적인 사용자들이 IoT와 같은 M2M 컴퓨팅 환경에서 보안문제를 야기할 수 있기 때문이다. 그러나 IoT와 같은 환경에서 신뢰 평가는 하이브리드식으로 접근하는 것이 좀 더 적합하다고 할 수 있다. IoT 환경의 분산적 특성으로 인해 IoT 개체들간에 형성되는 신뢰 관계는 주로 서비스를 통한 상호작용을 바탕으로 평가하게 되는데, 본 논문에서는 IoT 환경과 같은 M2M 애플리케이션 서비스를 위한 하이브리드 접근방식의 신뢰평가 모델을 제안한다. 제안된 모델은 M2M 애플리케이션 서비스의 신뢰 평가를 위해 지역을 중심으로 구성되는 커뮤니티의 한 노드가 신뢰관리자로서의 역할을 담당하는 하이브리드식의 접근방식을 사용하면서, 최종 사용자들 사이의 신뢰도를 보장할 수 있는 신뢰 평가 방법을 정의한다.

IoT 환경과 같은 M2M 컴퓨팅 환경에서, 신뢰에 대한 기존 연구는 소프트웨어 서비스 관점에서 동적배포에 대한 신뢰 평가 또는 상황정보를 활용한 신뢰 평가와 같은 기술적 이슈들을 포함하고 있다. 본 논문에서 제안된 모델은 이러한 문제를 해결하기 위해 개선되어야 한다.

## 참고 문헌

- [1] N. B. Truong, U. Jayasinghe, T.-W. Um, and G. M. Lee, "A Survey on Trust Computation in the Internet of Things", 한국통신학회지(정보와 통신), 제 33권 제 2호, pp. 10-27, Jan. 2016. <https://www.koreascience.or.kr/article/JAKO20160894992>
- [2] Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). "An Integrative Model of Organizational Trust", *The Academy of Management Review*, 20(3): 709-734. DOI: <https://doi.org/10.2307/258792>
- [3] Truong, N. B., H. Lee, B. Askwith and G. Lee, "Toward a Trust Evaluation Mechanism in the Social Internet of Things", *Sensors (Basel)*, Vol.17, No.6 (2017), Article 1346. DOI: <https://doi.org/10.3390/s17061346>
- [4] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks", *IEEE Communication Magazine*, Vol.46, No.4, pp.108-114, April 2008. DOI: <https://doi.org/10.1109/MCOM.2008.4481349>
- [5] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things", *Computer Science and Information System*, Vol. 8, No. 4, pp. 1207 - 1228, 2011. DOI: <https://doi.org/10.2298/CSIS110303056C>
- [6] J. Guo and I. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems", *Proc. of IEEE International Conference on Services Computing (SCC 2015)*, pp. 324-331, 2015. DOI: <https://doi.org/10.1109/SCC.2015.52>
- [7] F. Bao, I. R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems", *Proc. of 11th International Symposium on Autonomous Decentralized Systems (ISADS 2013)*, pp. 1 - 7, 2013. DOI: <https://doi.org/10.1109/ISADS.2013.6513398>
- [8] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social internet of things", *Proc. of IEEE International Symposium on Personal*

- Indoor and Mobile Radio Communications (PIMRC 2012), Sydney, Australia, 2012. DOI: <https://doi.org/10.1109/PIMRC.2012.6362662>
- [9] K. Aberer, and Z. Despotovic, "Managing trust in a peer-2-peer information system", Proc. of International Conference on Information and knowledge management, Atlanta, Georgia, USA, 2001, pp. 310-317. <https://doi.org/10.1145/502585.502638>
- [10] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation Systems", Communications of the ACM, vol. 43, no. 12, pp. 45-48, 2000. DOI: <https://doi.org/10.1145/355112.355122>
- [11] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "Experience with the KeyNote Trust Management System", Proc. in International Conference on Trust Management, Heraklion, Crete, Greece, 2003, pp. 284-300. DOI: [https://doi.org/10.1007/3-540-44875-6\\_21](https://doi.org/10.1007/3-540-44875-6_21)
- [12] L. Xiong, and L. Liu, "A Reputation-based Trust Model for Peer-to-Peer E-Commerce Communities", in IEEE International Conference on E-Commerce Technology (CEC), Newport Beach, 2003, pp. 275-284. DOI: <https://doi.org/10.1109/COEC.2003.1210262>
- [13] Y. Liu, W. Xue, K. Li, Z. Chi, G. Min, and W. Qu, "DHTrust: A Robust and Distributed Reputation System for Trusted Peer-to-Peer Networks", Proc. in IEEE Global Telecommunications Conference (GLOBECOM), Miami, FL, USA, 2010, pp. 1-6. DOI: <https://doi.org/10.1109/GLOCOM.2010.5683742>
- [14] T. Roosta, M. Meingast, and S. Sastry, "Distributed Reputation System for Tracking Applications in Sensor Networks", Proc. in International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose, CA, USA, 2006, pp. 1-8. DOI: <https://doi.org/10.1109/MOBIQ.2006.340449>
- [15] J. Golbeck, Computing and Applying Trust in Web-based Social Networks, Ph.D. Thesis, University of Maryland, 2005. <http://drum.lib.umd.edu/bitstream/1903/2384/1/umi-umd-2244.pdf>

저자 소개



김유경(Yukyong Kim)

2001.8 숙명여자대학교 컴퓨터과학과 박사  
 2005.9 - 2006.8 UC Davis, Post-doc.  
 2006.9 - 2013.9 한양대학교 컴퓨터공학과  
 연구교수  
 2018.2 - 현재 숙명여자대학교 기초공학부  
 교수

<주관심분야> 웹서비스 QoS평가, SOA 기  
 반 IoT 신뢰평가, 소프트웨어 품질평가