DOI: 10.3745/KIPSTC.2009.16-C.2.143

애드혹 환경에서 평판기반 신뢰 모델의 분류 및 성능평가

박 성 수[†] · 이 종 혁[††] · 정 태 명[†††]

요 약

신뢰 기반 네트워크에서 상호 통신 연결을 위해 상대 노드가 얼마나 믿을만한 노드 인지를 결정하는 문제가 가장 중요하다. 현재의 신뢰 기반 네트워크에서는 노드의 상태를 관찰함으로써 신뢰 값을 생성하고, 통신 노드를 평가하는 과정을 통해 상호 통신 연결을 수립한다. 본 논문에서는 애드혹 환경에서 새로운 노드가 클러스터 내로 진입하여 통신을 설정하고자 하는 대상 노드를 찾을 때, 사용될 수 있는 4가지의 신뢰 모델을 제안한다. 제안된 모델들은 평판 서버의 유무와 신뢰의 평가 방법들에 따라 분류 되었다. 제안된 모델을 통해서, 평판 서버가 클러스터 내에 존재하고 신뢰 평가 시 자신의 경험 정보뿐만 아니라 이웃 노드의 평판을 고려하는 경우 더 신속하게 대상 노드를 찾을 수 있음을 보인다. 제안된 모델의 성능 분석은 각 모델에서 노드의 최종 신뢰 값을 생성하기 위해 소요 되는 통신지연시간의 측정에 초점을 맞추었다.

키워드 : 신뢰, 평판, 애드혹 네트워크

Classification and Performance Evaluation of Reputation-Based Trust Model in Ad-hoc Networks

Seong-Soo Park[†] · Jong-Hyouk Lee[††] · Tai-Myoung Chung[†††]

ABSTRACT

In trust-based networks, it is very important how to decide a node is trustworthy when one node performs communications with other node. In current networks based on trust, a node creates a new trust value from observation and then establishes an intercommunication path through the process of evaluating a targeted communication node. In our paper, we propose four trust models in which a new node enters a cluster and finds a target node to create a communication in ad-hoc networks. The proposed models have been classified according to the existence of reputation server and the trust evaluation functions. Through the proposed model, we found that new node finds target node more quickly in which there exists a reputation server in the cluster and considers neighbor node's recommendation as well as own experience information when calculates trust values. As our performance analysis, we focus the communication delay time to generate a final trust value for each trust model.

Keywords : Trust, Reputation, Ad-hoc Networks

1. 서 론

신뢰(Trust)는 인터넷과 같은 개방 환경에서 비즈니스 활동을 지원하기 위해 가상의 조직을 형성 하거나, 신뢰도가 높고 낮음을 결정하는 불확실성의 문제를 해결하기 위한 방법으로 매우 중요한 역할을 한다. 개방 환경에서 비즈니스를 하기 위해서 시장성이 있는 서비스를 찾는 경우, 자율적인 고객은 많은 잠재력을 가지고 있다. 하지만 이 고객은 서비스 제공자에 대한 악의적인 공격을 증가 시키고 있다[1]. 신뢰는 사용자가 불안전하고 불확실한 정보를 토대로 하여 어떤 결정을 해야 할 때 중요한 역할을 한다. 특히 최근에 이러한 기능을 제공하는 시스템은 전자상거래나 가상 커뮤니티 분야에서 활용되고 있다[2].

전통적인 네트워크 환경에서 신뢰 설정 및 인식은 자원에 역할을 할당하는 메커니즘에 의한 접근제어 절차를 통해 수행되어 왔다. 최근의 개방형 네트워크 환경에서 고정된 역할 할당을 하는 노드는 다양한 결정들에 의해 교체될 수 있게 되었다. 이러한 결정에 영향을 주는 중요한 요소로써 평판(Reputation)이 제시되고 있다. 평판은 신뢰와 밀접한 상관성을 가지고 있다. 신뢰는 개체의 향후 행동에 대한 긍정적인 예측의 수준을 의미한다. 이러한 신뢰의 결정에 중요한 영향을 주는 것이 바로 평판이 된다. 평판은 주로 두 가지 경로를 통해서 형성될 수 있다. 우선 평가자가 피평가자에 대한 스스로의 경험을 통해서 형성할 수 있다. 다음으로

※ 본 논문은 보건복지부 보건의료기술진흥사업회 지원에 의하여 이루어진 것임 (과제번호: 02-PJ3-PG6-EV08-0001).
† 준 회 원 : 성균관대학교 컴퓨터공학과 박사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
††† 종신회원 : 성균관대학교 정보통신공학부 정교수
논문접수 : 2008년 9월 29일
수 정 일 : 1차 2009년 2월 12일
심사완료 : 2009년 2월 17일

는 평가자의 이웃 개체들로부터의 추천을 통해서 형성할 수 있다[1,3,8].

개인 컴퓨터가 증가하고 이동성의 요구가 증대 되면서 애드혹(Ad-hoc)이나 P2P(Peer-to-Peer)와 같은 미래형 네트워크는 널리 사용되고 있다. 실제로, 이러한 환경은 미래의 컴퓨터와 네트워킹 구조로 점차 자리매김 하고 있다. 애드혹 네트워크는 노드가 고정된 네트워크 구조를 형성하지 못하는 상황에서 통신이 가능 하도록 한다[4]. 본 논문에서는 중앙의 통제된 서버가 없는 애드혹 네트워크 환경에서 새로운 노드가 클러스터(Cluster) 내에 진입하여 또 다른 노드와 통신하기 위하여 상대방에 대한 신뢰 정도를 측정한 후 인증된 노드라고 판단되면 통신을 하게 되는데, 이때 통신이 시작되는 시점까지 소요되는 시간을 측정하는 4가지 모델을 제안한다. 평판 서버의 존재유무가 네트워크 전체에 어떠한 영향을 미치는지에 대한 연구, 신뢰 값 결정 시 자신의 경험만으로 결정 되는 경우에 비해 이웃 노드의 평판을 고려하여 결정하는 경우 어떠한 효과가 있는지에 대한 연구는 미래형 네트워크 구축 시 필요하다.

본 논문에서 고려하는 환경에서 주요한 위협 요인으로는 2종류가 있다. 먼저, 이기적인 노드에 의한 위협이다. 이 노드들은 자신의 자원을 최대한 절약하기 위해서 다른 노드와의 통신 설정 자체를 거부 하거나 다른 노드로의 전달이 요청된 패킷을 버리는 행위를 한다. 또 다른 유형으로는 악의적인 노드에 의한 위협이다. 이 노드들은 잘못된 라우팅 경로를 알려주는 등의 행위로 네트워크의 멤버나 네트워크 전체를 위협한다[5]. 이러한 위협으로부터 네트워크를 안전하게 보호하고 정확한 통신 설정을 통해서 패킷이 손실되는 것을 방지 하기 위해서는 신뢰를 기반으로 하는 모델이 필요하다.

클러스터 내로 진입하는 새로운 노드는 클러스터 내에 존재하는 노드들 중에서 대상 노드를 선정하여 통신 하는데, 이 과정에서 대상 노드에 대한 인증은 클러스터 내에서 가장 높은 신뢰 값을 가진 노드로 결정한다. 즉, 가장 믿을만한 노드를 선정하게 된다. 새로운 노드가 이러한 과정을 통해서 대상 노드를 찾기 위해서는 많은 시간이 요구된다. 이 문제를 해결하기 위하여 노드에 대한 다른 평가자의 평가 즉 평판을 활용할 수 있다. 지연시간을 줄임으로써 애드혹 환경에서 이동 노드가 해결해야 하는 전력 문제, 자원 절약 등의 문제를 해결하여 시스템 전체적인 효율성을 높일 수 있다.

본 논문에서 해결 하고자 하는 문제점과 공헌도는 아래와 같다.

- 개방 환경에서 상대 노드 선택 시, 신뢰도를 기반으로 선정하는 신뢰 모델을 제안
- 중앙 통제 기관이 없는 애드혹 환경에서 신뢰도를 평가할 수 있는 신뢰 평가 모델의 분류
- 애드혹 네트워크의 성능을 향상시키기 위한 방법으로 제안된 모델들의 성능을 평가

2장은 관련 연구로서 기존 신뢰의 개념, 신뢰와 평판 모델과의 상관성, 신뢰 값 생성에 대해 소개 한다. 3 장에서는 신뢰 모델 및 가정사항을 기술한다. 본 논문을 통해 제안하는 성능평가 시스템은 4장에 기술된다. 5장에서는 제안된 신뢰 모델들에 대한 성능평가 분석 결과를 기술한다. 6장에서는 결론과 향후 연구과제에 대해 기술한다.

2. 관련 연구

2.1 신뢰의 개념

신뢰 개념은 사회과학분야에서 파생되어 왔으며, “하나의 대리인이 다른 대리인의 과거 기록을 비추어 보아 미래 행동에 대해 가지는 주관적인 기대감”으로 정의한다[12]. 신뢰는 평판, 신뢰하는 견해(trusting opinion), 확률(probability) 등으로 해석 된다.

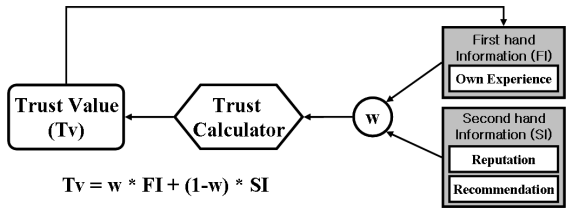
본 논문에서 사용되는 신뢰는 두 개체간의 특정한 행동에 의해 생성된 관계이다. 하나의 개체는 대상이 되는 다른 개체가 자신이 요구하는 행동을 할 것이라고 믿는다. 이러한 신뢰 관계를 $\{subject : agent, action\}$로 표현하고, 신뢰는 subject의 관점에서 agent가 행동을 원하는 대로 수행 할 것인가에 대한 확실성으로 정의한다. 그 결과 값인 신뢰 값을 $T\{subject : agent, action\}$라고 표현 한다. 이 값은 절대적인 값이 아니며, 대상자의 주관에 의해 결정되는 값이다. 따라서, 같은 행위자나 행동일지라도 다른 신뢰 값이 나올 수도 있다[7].

평판 시스템은 사회 공학적, 경제학적으로 주변에 많은 사례들이 존재한다. 사람간의 관계에서의 신뢰 관계, 신용카드 시스템 등뿐만 아니라 최근의 전자상거래 영역에서는 다양한 평판 시스템들이 활용되고 있다. 즉, 평판 시스템들과 메커니즘들은 전자상거래 영역에서 신뢰를 생성하기 위한 기술로서 사용되고 있다. 신뢰는 시간이 지남에 따라 평가 주체의 경험이나 평판 혹은 추천(Recommendation)의 결과에 따라 변경된다. 따라서, 평판 시스템은 참여자(객체)의 과거 행동에 대한 피드백을 수집, 총괄, 분배하여 신뢰의 수준을 결정하는 것을 지원하는 기술이다.

2.2 신뢰와 평판 모델과의 상관성

(그림 2-1)에서는 신뢰 시스템에서 평가 값에 대한 갱신 과정을 나타내고 있다. 시스템의 운영 조건 및 환경에 따라 개별 구성요소들의 전부 혹은 일부에 의해 신뢰가 평가될 수 있다[6]. 1차 정보 (First-hand information: FI)는 평가 대상에 대한 서비스 제공자 스스로의 경험이 요구된다. 2차 정보(Second-hand information: SI)는 서비스 제공자가 아닌 다른 평가자들로부터 제공된 정보를 나타낸다. 이전의 경험이 없는 피평가자에게 서비스를 제공하기 위해서는 기본 신뢰 정보에 의존할 수밖에 없다. 일단 신뢰 수준이 결정되고 자원 및 서비스가 제공될 경우 서비스 제공자는 주기적인 1, 2차 정보의 갱신을 통해 신뢰의 수준을 관리해야 한다.

(그림 2-1)에서 나타내는 바와 같이 w는 자신의 경험만을 고려하는 경우와 이웃 노드들의 평판까지 고려하여 신뢰 값을 결정하는 경우 사이의 편향치를 나타내는 값으로서, 이 값이 클 경우 자신의 경험이 신뢰 값 결정에 많은 영향



(그림 2-1) 신뢰의 갱신절차

을 주는 것으로 정의한다. 또한, w값이 1인 경우는 SI를 고려하지 않고 신뢰 값은 FI에 의해서만 결정된다.

2.3 신뢰 값 생성

두 노드 N과 T가 신뢰 값을 생성하는 과정을 논문 [10]에서 제안한 방법에 기초하여 기술한다. 두 노드가 관찰에 의해서 신뢰 값을 결정한다. 노드 N의 노드 T에 대한 이전 관찰에 의해서 노드 N이 노드 T와 $\{N:T,act\}$의 신뢰 관계를 형성 한다. 현재까지의 행동은 긍정적인 행동의 총 횟수인 a와 부정적인 행동의 총 횟수인 n으로 구성된다. 이 행동의 결과에 의해서 미래에 일어날 행동을 유추하여 신뢰 값(T_v)을 [0, 1]의 범위 내에서 확률로써 정의할 수 있다. 미래에 긍정적인 반응을 보일 것으로 기대되는 행동의 총 횟수는 $a+1$의 값을 가지고, 미래에 부정적인 반응을 보일 것으로 기대되는 행동의 총 횟수는 $n+1$의 값을 가진다. 따라서, 신뢰 값 생성 식은 아래와 같다.

$$T_v = \frac{a+1}{(a+1)+(n+1)} = \frac{a+1}{a+n+2} \quad (1)$$

위 (1)식에서 T_v는 현재까지의 행동의 결과를 토대로 해서 미래에 긍정적인 행동을 얼마만큼 할 것인지에 대한 확률로 표현된다.

3. 모델 및 가정사항

*Chadwick*은 논문 [8]에서 2개의 기준 축에 의해 평판 시스템을 4가지로 구분하였다. 첫 번째 기준 축은 “평가 대상 개체에 대한 평판 주체가 누구인가?”이고, 두 번째 기준 축은 “평판을 위해 평판 서버가 어떻게 정보를 수집 하는가?”에 의해 구분하였다. 이러한 기준에 의해서 의견 투표(Opinion Pull), 투표(Voting), 조사(Research), 의회 회원(Member of Parliament) 모델로 분류하였고, 이 모델들은 모두 평판 서버가 존재한다. 본 논문에서 고려하는 신뢰 모델은 우선, 평판 서버의 유무에 따라 구분한다. 그런 후에 각각의 경우마다 자신의 경험에 의한 정보만으로 노드를 선택하는 지역평판 모델과 자신의 경험과 평가자의 평가 값을 고려하여 최종 대상노드를 선정하는 투표(voting) 모델로 구분된다. 투표(voting)란 “다른 대상에 대해 투표 한다”는 의미로써 여기에서는 이웃 노드에 대해 자신의 관찰과 경험에 의해 평가하는 것을 의미한다. 이후로는 이 모델을 투표 모델로 명명한다.

평판 서버가 있는 신뢰 모델의 클러스터 구성방법 및 평판 서버 선출과정을 논문 [9]에서 제안하는 방법을 적용하여 기술한다. 먼저, 네트워크 내의 모든 노드들은 자신의 경험에 의하여 이웃 노드의 신뢰 값을 평가한다. 이웃 노드의 신뢰 값 평가 이후에, 각 노드는 가장 높은 값을 가진 노드를 보증인으로 선택한다. 그런 이후에 선택된 노드는 클러스터 헤드가 되고, 선택하는 노드는 클러스터의 멤버가 된다. 이때 만약, 헤드로 선택된 노드가 다른 클러스터의 멤버이면, 차상위 값을 가진 노드가 선택된다. 이런 방법에 의해 하나의 클러스터가 형성된다. 클러스터 헤드는 클러스터 내의 모든 멤버 노드들의 신뢰 값을 평가하여 자신의 레코드에 보관하고 멤버를 보증하고 관리하는 역할을 한다. 이러한 클러스터 구성과정에 참여하지 않는 노드가 클러스터 내의 노드와 통신을 하고자 할 때, 그 노드는 클러스터 내로 새로 진입하는 노드가 된다. 그리고 클러스터 구성과정에 참여했던 노드는 헤드의 통제를 받게 된다.

이 논문을 전개하는데 요구되는 가정사항에 대해서 기술하겠다.

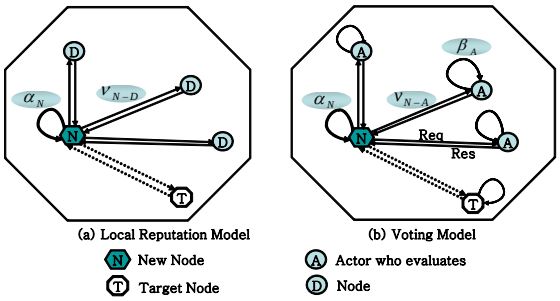
1) 새로운 노드 N은 네트워크 환경에서 평가자에게서 평판을 받아 자체의 알고리즘으로 신뢰 값을 계산할 수 있는 노드이며, 클러스터 내로 진입 후 대상 노드와 통신설정을 하기 이전까지 다른 클러스터로 이동하지 않는다.
2) 투표 모델에서 클러스터 내의 각 노드는 자신의 신뢰 값 및 다른 노드에 대한 신뢰 값을 기억하기 위한 기억공간을 가지고 있으며, 평판 기능을 한다.
3) 지역평판 모델에서 각 노드는 자신의 관찰에 의해 다른 노드의 신뢰 값을 계산하고 기억한다.
4) 제안되는 모델들은 네트워크 내에 존재하는 여러 개의 클러스터 중에서 하나의 클러스터에 한하며, 클러스터의 크기는 평판 서버 혹은 모든 노드들의 전파반경에 의해서 한정된다.

4. 성능 평가 시스템

본 논문에서는 새로운 노드 N(New Node)이 클러스터 내에 출현하여 대상 노드 T(Target Node)와 통신을 설정하기 위해 대상 노드를 찾는다. 클러스터 내의 모든 노드들 중에서 신뢰 값이 가장 높은 노드를 대상 노드로 선정하게 되면 패킷이 손실되거나 잘못된 경로로 전송되는 등의 악의적인 노드의 공격으로부터 벗어나 안전한 통신을 수행할 수 있다. 그렇기 때문에 노드 N은 신뢰 값을 계산하여 그 결과 값이 가장 높은 노드를 대상 노드로 선정하게 된다. 이를 위하여 자신의 신뢰 레코드를 이용하거나 혹은 이웃에게 평판을 요청하여 받은 후에 노드 T에 대한 신뢰 값을 산정한다. 이러한 과정을 통해서 대상 노드를 찾게 되고, 그 노드와의 통신 설정이 이루어지게 된다. 본 논문에서는 이러한 과정에서 소요되는 전송지연시간이 얼마나 발생하게 되는지 살펴보도록 한다. 평판 서버가 존재하는 경우는 클러스터 내에서 평판 서버를 제외한 가장 높은 신뢰 값을 가진 노드를 선정하는 것으로 가정한다.

4.1 평판 서버가 없는 경우

본 논문에서는 클러스터 내의 노드들이 평판 서버를 별도로 선정하지 않고 구성되어 있어서 새로 진입하는 노드가 직접 신뢰 값을 계산하고 대상 노드를 선정하는 경우에 대해서 모델링 한다.



(a) 지역평판 모델 (b) 투표 모델

(그림 4-1) 평판 서버가 없는 지역평판과 투표 모델

4.1.1 지역평판(Local Reputation) 모델

지역평판 모델의 특징은 자신이 기억하고 있는 신뢰 레코드에 의해서 최종 신뢰 값이 결정되는 모델이다. 새로운 노드가 클러스터 내로 이동하여 대상 노드를 선정하기 위해서 먼저 자신의 신뢰 레코드를 확인(α_N) 한다. 클러스터 내로 처음 들어 왔으므로 이 값은 0 이다. 그러므로, 노드 N은 노드 D들 간의 통신 상태를 관찰(v_{N-D})한 후에 신뢰 값을 결정해야 한다. 이에 소요되는 시간을 t_{tot} 라고 한다. 이 시간 동안 통신 상태를 관찰한 후, 관찰자는 신뢰 값의 최종 결과 값을 측정할 수 있다.

$$T_d^{LV} = d_1 + d_2 \tag{2}$$

- T_d^{LV} : 새로운 노드 N이 클러스터 내의 모든 노드 중에서 상대 노드를 선정하여 통신을 연결하기 위해 최종 신뢰 값을 얻는데 걸리는 전송지연시간
- d_1 : 새로운 노드(N)가 자신의 신뢰 레코드를 활용해서 대상 노드를 선정하는데 필요한 시간
- d_2 : 새로운 노드(N)가 평가자(A)들에게 평가 값을 요청하고 받는데 소요되는 시간

지역평판 모델에서는 식(2)에서 평가자에게 평가 값을 요청하고 받는 시간(d_2)을 고려하지 않으므로 아래와 같다.

$$T_d^L = d_1 \tag{3}$$

클러스터 내의 노드들 상호간에 필요한 정보를 요청하고 받는데 소요되는 시간은 데이터 전송시간을 측정하는 방법으로 널리 알려진 계산식으로 아래와 같다.

$$t_1 = \frac{Message\_Size(Byte)}{Bandwidth(Byte)} + propagation\_time \tag{4}$$

따라서, 지역평판 모델에서 대상 노드를 찾는데 소요되는 시간은 아래와 같다.

$$T_d^L = d_1 = 2 \times t_1 \times n \times t_{tot} \tag{5}$$

이때, n 은 새로운 노드 N이 클러스터로 진입할 당시의 클러스터 내의 노드 총수 이다.

4.1.2 투표 (Voting) 모델

투표 모델의 특징은 평가자(A)들이 피평가자를 자기 자신의 경험에 의한 알고리즘을 활용하여 직접 평가하고, 그 결과 값을 평판 서버 혹은 다른 노드의 요청에 의해 전송한다. 실생활에서 인간은 이런 종류의 평가를 그들이 자주 가는 가게, 그들이 만나는 사람들, 그리고 그들이 지원하는 정당 등에 대해 항상 하고 있다. 대표적인 사례로 e-Bay의 평판 서버의 활용이 투표 모델에 해당한다.

새로운 노드 N은 클러스터 내로 진입하여 통신하고자 하는 노드를 찾기 위해서 먼저 자신의 신뢰 레코드(α_N)를 확인한다. 클러스터 내로 처음 진입하였으므로 이 값은 0 이다. 이 모델에서는 신뢰 값을 생성하기 위해서 이웃 노드들에게 평가 값을 문의한다. 이러한 과정을 수행하는 시간은 아래와 같다.

$$T_d^V = d_2 \tag{6}$$

새로운 노드 N은 평가자(A)들에게 누구와 통신하면 좋을지 문의(v_{N-A})한다. 평가자들은 자신만의 알고리즘을 활용하여 2.3절의 (1)식과 같이 다른 모든 노드 A들에 대한 평가를 수행(β_A)하고 그 결과 값을 보유하고 있다가 노드 N에게 전송(v_{N-A})한다. 노드 N은 이 값을 자신의 캐쉬(Cache)에 기록 하고 그 결과 값 중에서 가장 높은 값을 가진 노드를 대상 노드로 선정한다. 이때 전송되는 신뢰 레코드의 형식은 $\{subject, agent, actiontrust\_value, t_{create}\}$ 이고, 소요되는 총 시간은 아래와 같다.

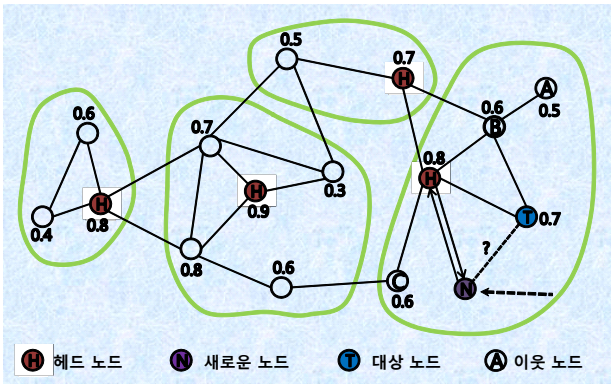
$$T_d^V = d_2 = 2 \times t_1 \times n \tag{7}$$

4.2 평판 서버가 있는 경우

본 논문에서는 클러스터 내에 평판 서버가 존재하는 경우를 가정하여 모델링 한다. 평판 서버는 클러스터 내에 있는 노드들로부터 클러스터 헤드로 선정된 노드로서 통신설정의 주체이며 통신이 이루어지는 클러스터 내에서 모든 노드와 통신이 가능하고 새로운 노드 등장 시 자동으로 연결된다. 이 서버는 평가자의 평판 결과를 취합하여 자신이 가지고 있는 알고리즘에 의해 신뢰 값을 산정한다. 그리고 항상 최신의 값을 유지하기 위하여 이 과정을 일정 주기로 반복한다.

4.2.1 네트워크 내의 클러스터 구성 모형

(그림 4-2)는 네트워크에서 클러스터 기반 신뢰 모델을 3장에서 기술한 방법에 의해 보여 준다. 클러스터 내의 헤드는 신뢰 값이 가장 높은 노드가 선정되고 클러스터 내의 모



(그림 4-2) 클러스터 기반 신뢰 모델

든 멤버 노드를 관리한다. 새로운 노드가 진입 시에서는 클러스터 내의 모든 노드에 대한 신뢰 값을 제공한다. 헤드 노드가 다른 클러스터로 이동 시에는 헤드 선별과정을 다시 거쳐서 새로운 헤드를 선출한다. 그리고 새로 선출된 헤드는 곧바로 클러스터 내의 모든 노드들에 대한 신뢰 값을 계산하는 작업을 한다.

4.2.2 클러스터 구성 및 인증서 발행 동작과정

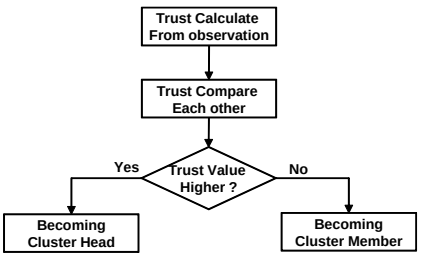
애드혹 네트워크 환경에서 새로운 노드가 클러스터 내로 진입하여 클러스터를 형성하고 신뢰 값을 인증하는 과정 및 방법을 논문 [9]에서 제안하는 방법을 적용하여 기술한다.

A. Hello 메시지 방송

새롭게 진입하는 노드들은 클러스터 헤드 검색 메시지가 포함된 hello 메시지를 방송한다. 그 메시지를 받은 어떤 헤드라도 메시지에 대한 응답을 보낸다. 헤드의 응답 메시지에는 멤버 노드의 숫자가 포함 되어있다. 만약, 이웃에 클러스터 헤드가 여러 개 있다면 그 중에서 멤버의 수가 가장 많은 헤드를 선택하고 그 헤드가 속한 클러스터의 멤버가 된다. 만약, 이웃에 클러스터 헤드가 없다면 이웃노드들과 연합해서 새로운 헤드를 선출한다. 클러스터 헤드는 진입 메시지를 받은 후에, 이전의 클러스터 헤드에게서 검증된 이전의 클러스터 값에 기초해서 진입하는 노드의 신뢰 값을 계산한다.

B. 클러스터 형성

(그림 4-3)에서는 평판 서버가 존재하는 경우 클러스터 구



(그림 4-3) 클러스터 구성 및 헤드 선출과정

성 및 헤드 선출 과정을 3장에서 기술한 방법에 의해서 표현한다. 노드가 헤드를 추천할 때, 추천 인증서를 포함한 추천 메시지를 클러스터 헤드에게 보낸다. 이러한 인증서들은 헤드를 믿는 멤버들을 얼마나 가지고 있는지 검증하는데 사용된다. 이러한 과정을 거쳐 클러스터가 구성되며, 클러스터 내에서 신뢰 값이 가장 높은 노드를 클러스터 헤드로 선정한다. 헤드를 선정하기 위해 비교되는 회수 k는 $2^k \geq n$ 을 만족하는 최소 k 가 되며, 이때 소요되는 시간은 아래와 같다.

$$T_d^{Clu} = 2 \times t_1 \times k \tag{8}$$

C. 신뢰 인증서 발행

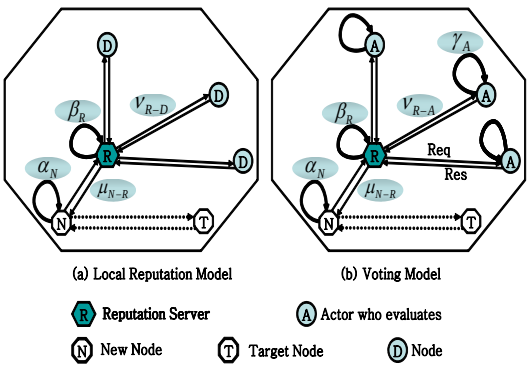
클러스터가 형성된 후, 노드는 신뢰 인증서를 헤드에게 요청한다. 헤드는 노드의 신뢰 값 인증서를 발행하고, 클러스터 헤드가 믿을만하다는 것을 검증하는 헤드의 추천 인증서를 보낸다.

D. 노드의 진입

노드의 진입은 두 가지 상황에서 실행된다. 하나는 네트워크에 새로 진입하는 경우이다. 다른 하나는 다른 클러스터에서 이동해 오는 경우이다. 첫 번째 경우는, 새로운 노드에 대한 신뢰 값 인증서나 추천 인증서를 가지고 있지 않기 때문에, 클러스터 헤드는 노드의 행동을 보고 빠른 시간 내에 그 노드에 대한 신뢰 값 계산을 해야 한다. 이때, 헤드에 의해 계산된 신뢰 값을 짧은 시간 내에 계산 되었기 때문에 정확하지 않을 수 있고, 시간이 지남에 따라 그 계산 값이 수정되면서 정확한 신뢰 값이 획득된다. 두 번째 경우는 이전의 클러스터 헤드에게서 받은 신뢰 값 인증서와 추천 인증서를 새로운 클러스터 헤드에게 준다. 이 인증서들을 이용해서 새로운 클러스터 헤드는 자신의 경험 데이터 없이도 그 노드에 대한 초기 신뢰 값을 검증하고 설정한다.

E. 노드의 다른 클러스터로 이동

하나의 클러스터에서 다른 클러스터로 이동하는 노드는 leave 메시지를 클러스터 헤드에게 보낸다. 이 메시지를 받은 후에, 클러스터 헤드는 그 노드에 대한 데이터를 지운다.



(a) 지역평판 모델 (b) 투표 모델

(그림 4-4) 평판 서버가 있는 지역평판과 투표 모델

4.2.3 지역평판 모델

새로운 노드가 클러스터 내로 진입하여 통신하고자 하는 대상 노드를 찾기 위해서 클러스터 내의 대표 노드인 평판 서버(R)에게 누구와 통신하면 좋을지 문의(μ_{N-R})한다. 이 때, R은 자신이 기억하고 있는 1차 정보(β_R)에 의해서만 신뢰 값을 결정하여 알려준다. 이런 경우 신뢰 값이 최신 값이 아닐 경우가 발생하므로 R은 현재 자신이 가지고 있는 신뢰 값을 다시 한번 갱신하기 위해서 각 노드들의 신뢰 상태를 관찰(ν_{R-D})한다. 이때 신뢰 값을 주기적으로 갱신하는데 소요되는 시간을 t_{peri} 라고 한다. 평판 서버는 자신이 보유하고 있는 1차 정보와 주기적인 관찰에 의해서 얻어진 새로운 값을 혼합하여 신뢰 최종 값을 산출하여 노드 N에게 전송(μ_{N-R}) 한다.

$$T_d^{RL} = \{(2 \times t_1) + (2 \times t_1 \times (n-1) \times t_{peri})\} \quad (9)$$

4.2.4 투표 모델

평판 서버가 별도로 존재하는 투표 모델은 이전에 설명한 투표 모델과 유사하지만 클러스터 내에 평판 기능을 하는 서버에 의해 신뢰 값이 계산되는 모델이다. 새로운 노드(N)가 통신 하고자 하는 노드를 찾기 위해 평판 서버(R)에게 문의(μ_{N-R})한다. R은 자신이 가지고 있는 신뢰 값을 전송(μ_{N-R})한다. 이 과정에서 T에 대한 신뢰 값이 R이 가지고 있는 임계치 (δ)이상 이면 곧바로 통신이 개시 되지만, 그렇지 않는 경우 R은 각 평가자(A)들에게 T에 대해 보유하고 있는 신뢰 레코드를 요청(ν_{R-A})하고 받는 과정을 추가로 수행한다. 평가자(A)들은 자신의 알고리즘을 활용하여 이웃 노드를 평가할 수 있다. 그리고 자신이 보유한 신뢰 레코드 값을 R에게 전송한다. R은 평가자들에게서 받은 신뢰 레코드 중에서 최신 정보만을 추출하여 신뢰 값을 산정하고 그 결과 값을 노드 N에게 전송한다.

$$T_d^{RV} = \{(2 \times t_1) + (2 \times t_1 \times (n-1))\} \quad (10)$$

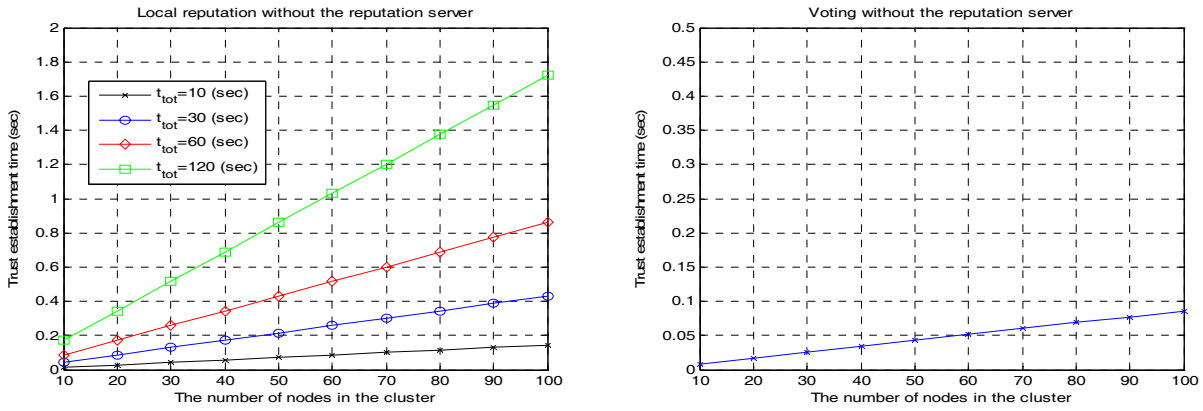
5. 성능 평가결과 분석

5.1 시스템 구성

제안된 4개의 모델의 평가를 위해, 본 논문에서는 해당하는 모델에 10개부터 100개까지의 노드가 존재한다고 가정한다. 그리고, 노드들은 11Mbps의 통신회선을 가지고 있다고 가정한다. 또한, t_{tot}의 정확한 값은 구현물이나 신뢰기법에 따라 달라지기 때문에 본 논문에서는 t_{tot}를 10, 30, 60, 120 초로 가정하고 평가한다. t_{peri}는 지역평판 모델에 따라 달라지는 값이기 때문에 본 논문에서는 10, 20, 30, 40 초로 가정하고 평가한다. 시뮬레이션에서, 각 노드가 이동하는 패턴은 논문 [11]에서 제안하는 무작위 자율지점 모델(random waypoint model)에 의해 움직인다. 각 노드의 위치는 조금씩 변경되고 이동 되는 패턴은 임의대로 움직인다. 하나의 노드는 임의의 위치에서 시작하고, 정지시간 동안 기다린다. 그런 후에 임의로 새로운 장소를 선택하고, 0~10 m/s의 속도 중에서 선택된 낮은 속도로 새로운 장소로 이동한다. 새로운 장소에 도착하면, 또 다른 임의의 정지시간 동안 기다리고 이 과정을 반복한다. 평균 정지시간은 300초 이다.

5.2 평판 서버가 없는 경우 분석

평판 서버가 없는 경우에는 노드 수가 증가함에 따라 대상 노드를 찾는데 필요한 시간이 지속적으로 상승함을 보여주고 있다. 그 이유는 자신이 모든 노드의 신뢰 값을 계산해야 하므로 노드수의 증가는 신뢰 값을 계산하는 시간에 많은 영향을 주기 때문이다. 이중에서도 (그림 5-1)의 (a) 지역평판 모델 즉, 1차 정보에 의해서만 대상 노드를 찾는 경우는 노드 수 증가에 급격하게 반응하여 대상 노드를 찾는데 소요되는 시간이 급격하게 증가함을 보여준다. 그 이유는 자신만의 경험에 의해서 최종 신뢰 값을 결정해야 하기 때문에 충분한 관찰을 통해 신뢰 값을 생성해야 한다. 또한 이 관찰시간이 증가 할수록 더욱 많은 시간이 필요하게 된다. (그림 5-1)의 (b) 투표 모델의 경우 자신의 경험과 이웃노드의 평판을 고려하여 대상 노드를 찾는 경우 즉, 1



(a) 지역평판 모델 (b) 투표 모델

(그림 5-1) 평판 서버가 없는 경우 소요시간

차 정보와 2차 정보를 결합하여 대상노드를 찾는 경우는 노드의 수에 비례하여 소요시간이 증가하지만 증가치는 많지 않음을 볼 수 있다. 그 이유는 평가자들의 평가결과를 고려하기 때문에 많은 모든 노드에 대해 오랜 시간 관찰하지 않아도 신뢰 값을 결정할 수 있기 때문이다. 따라서, 평판 서버가 없는 경우일지라도 자신의 경험과 이웃노드의 평판을 고려하여 신뢰 값을 계산하고 대상 노드를 찾는 경우가 더 효율적이다.

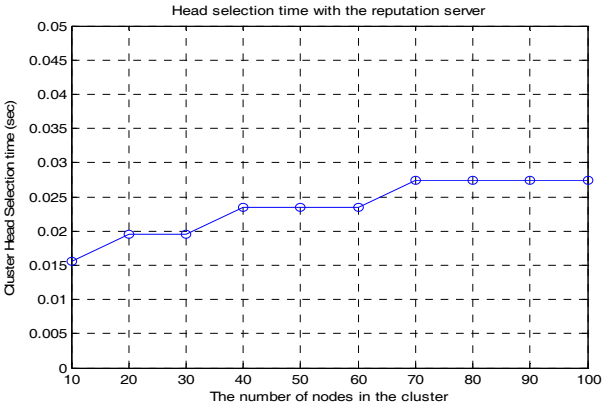
5.3 평판 서버가 있는 경우 분석

(그림 5-2)에서 평판 서버가 선정되는 시간을 산출 하였다. 이 시간은 네트워크에서 전파반경 내에 존재하는 노드들이 클러스터를 형성하고 헤드를 선정하는데 소요되는 시간이다. 만약, 새로운 노드가 클러스터 내로 진입하여 대상 노드를 찾는 과정에서 서버가 다른 클러스터로 이동하는 경우는 위에서 계산된 시간이 추가로 필요하다. 그러나, 새로운 노드가 클러스터 내로 진입 시 이미 헤드가 선정되어 있는 상태 이므로 위의 시간을 고려하지 않아도 된다.

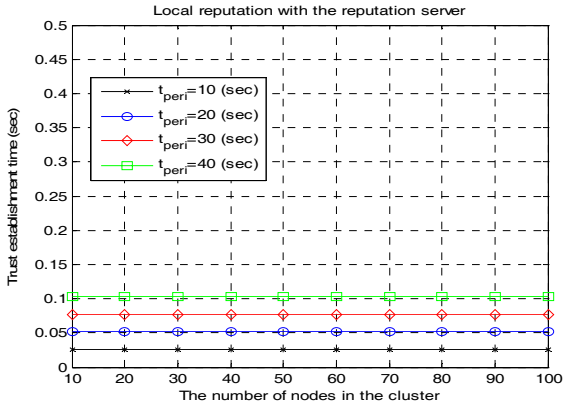
평판 서버가 존재하는 경우에는 이 서버가 클러스터 내의 모든 노드의 신뢰 값을 계산하여 그 결과 값을 가지고 있다. 새로운 노드가 클러스터 내로 진입하자마자 서버에게서 가장 높은 신뢰 값을 가진 노드를 전달받기 때문에 노드 수에 관계없이 대상 노드를 찾는데 소요 되는 시간이 일정함을 볼 수 있다. (그림 5-3)의 (a) 지역평판 모델에서는 1차 정보만 활용해서 신뢰 값을 결정하므로 서버가 보유한 신뢰 값이 항상 최신의 정보가 아닐 수 있어 신뢰 레코드를 일정 주기로 갱신하기 위한 시간이 필요하며 이 시간에 일정하게 비례하여 소요시간이 추가되었다. (그림 5-3)의 (b) 투표 모델은 서버가 1차 정보와 이웃의 평가자들에게서 받은 평판 결과인 2차 정보를 결합하여 신뢰 값을 결정하였으므로 다시 갱신할 시간이 추가로 소요되지 않는다. 왜냐하면 평가를 수행하는 이웃 노드들이 주기적으로 신뢰 값을 갱신하였고 이중에서 최신 정보만을 고려하여 신뢰 값을 결정하였기 때문이다. 이 모델이 제안된 모델 중에서 가장 짧은 시간 내에 대상 노드를 찾을 수 있음을 보였다. 이는 평판 서버가 자기자신의 경험만으로 신뢰 값을 계산하고 대상 노드를 찾는 것 보다는 이웃 노드의 평판을 고려하는 경우가 더 효율적임을 보여 주고 있다.

6. 결론 및 향후 연구과제

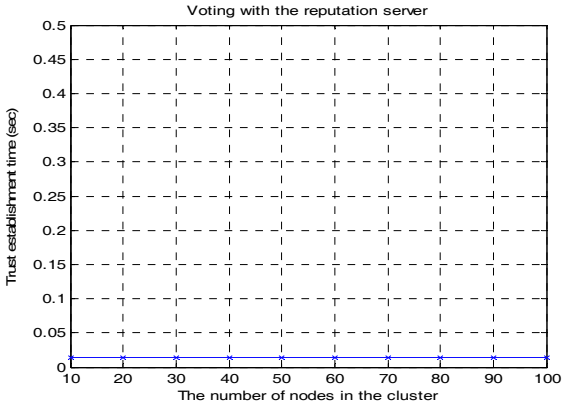
본 논문에서는 애드혹 환경에서 새로운 노드가 클러스터 내로 진입하여 통신하고자 하는 대상 노드를 찾는 시나리오를 설정하고 본 연구에서 분류하여 제안하는 모델을 통해서 평가 요소인 전송지연시간으로 성능을 분석하였다. 먼저, 평판 서버의 존재여부에 따라 모델을 분류하였고, 다음으로 신뢰 값 계산과정에서 자신의 경험만 사용하는 경우와 이웃 노드의 평판 정보를 활용하는 경우로 분류하여 평가 하였다. 성능평가 분석은 신뢰 값이 가장 높은 노드를 대상 노드로 선정하는데 소요되는 시간을 측정하고 분석하였다. 본 연구에서 활용된 신뢰는 기존의 클라이언트/서버 환경에서 클라이언트가 서버에 로그인 할 때, 서버에서 접근 권한을 확인하여 접근 가능(1) 혹은 불가능(0) 등의 형식으로 사용되던 개념을 [0, 1] 범위내의 실수를 사용하여 상대 노드를



(그림 5-2) 클러스터 헤드 선출시간



(a) 지역평판 모델



(b) 투표 모델

(그림 5-3) 평판 서버가 있는 경우 소요시간

어느 정도 인정할 것인가를 확률로써 표현하여 미래형 네트워크에서 활용하고자 하는 개념이다.

우리는 본 논문을 통하여 일반적인 네트워크 환경의 경우 노드의 수에 관계없이 클러스터 내에 평판 서버를 선정하고 1차 정보와 2차 정보를 활용하여 신뢰 값을 결정하는 경우가 성능이 뛰어남을 보였다. 또한 평판 서버를 선정하지 않는 경우라도 자신의 경험 정보만을 가지고 신뢰 값을 결정하는 경우보다는 이웃 노드의 평판 정보까지 활용하는 경우가 더 성능이 뛰어남을 보였다. 이는 평판 서버가 항상 클러스터 내의 모든 노드에 대한 정보를 가지고 있고, 이 정보를 최신으로 유지하기 위해서 이웃 노드에게서 평가된 정보를 수집하기 때문이다. 네트워크 내에서 이 최신의 정보를 클러스터 내에서 요청하는 모든 노드에게 제공함으로써 시스템 전체의 성능을 향상 시킬 수 있음을 의미한다.

향후 연구과제로는 본 연구에서 다루지 않은 평가 측정기준을 활용하여 평판 서버가 별도로 존재하는 경우가 존재하지 않는 경우에 비해서 어느 정도 성능향상을 보이는가를 평가분석하고, 인터넷 상에서 악의적인 노드의 행동유형을 파악하고 이러한 행동으로부터 보호하기 위해 노드간의 신뢰를 계산하는 새로운 모델을 개발하는데 있다.

참 고 문 헌

[1] S. Ruohomaa and L. Kutvonen, “Trust Management Survey”, iTrust 2005, LNCS Vol.3477, pp.77-92, 2005.

[2] Y. Zhong and B. Bhargava, “Authorization based on evidence and trust”, DaWaK 2002, LNCS Vol.2454, pp.94-103, 2002.

[3] I. Agudo, J. Lopez, and J. A. Montenegro, “A Representation Model of Trust Relationships with Delegation Extensions”, iTrust 2005, LNCS Vol.3477, pp.116-130, 2005.

[4] S.W. Shieh and D.S. Wallach, “Guest Editors′ Introduction: Ad Hoc and P2P Security”, Internet Computing, IEEE 9, pp.14-15, 2005.

[5] S. Marti, and H. Garcia-Molina, “Taxonomy of trust: Categorizing P2P reputation systems”, Computer Networks, Vol.50, Issue 4, pp.472-484, March, 2006.

[6] M. Kinateder, E. Baschny, and K. Rothermel, “Towards a Generic Trust Model - Comparison of Various Trust Update Algorithms”, iTrust 2005, LNCS Vol.3477, pp.177-192, 2005.

[7] Y. Sun, W. Yu, Z. Han, and K. J. Ray Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks”, IEEE JSAC special issue on security in wireless ad hoc networks, Vol.24, Issue2, 2006.

[8] D. W. Chadwick, “Operational Models for Reputation Servers”, iTrust 2005, LNCS Vol.3477, pp.108-115, 2005.

[9] S. Jin, C. Park, D. Choi, K. Chung, and H. Yoon, “Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network”, ETRI Journal, Vol.27, Issue 4, August, 2005.

[10] R. Ismail and A. Josang, “The beta reputation system”, Proceedings of the 15th Bled Conference on Electronic Commerce, 2002.

[11] J. B. David and M. A. David “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, Vol.353, pp.153-181, 1996.

[12] Gal-Oz, N., Gudes, E. and Hendler, D., “A Robust and Knot-Aware Trust-Based Reputation Model”, in IFIP International Federation for Information Processing, Vol.263; Trust Management II, pp.167-182, 2008.

박 성 수

e-mail : sspark@imtl.skku.ac.kr

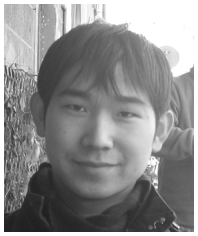
1997년 배재대학교 전자계산학과(학사)

2000년 성균관대학교 전기전자컴퓨터공학과 (공학석사)

2005년 경기대학교 전산계산교육 (교육학석사)

2007년~현 재 성균관대학교 컴퓨터공학과 박사과정

관심분야 : 네트워크 보안, AAA 및 접근제어, 신뢰 관리, 유비쿼터스 보안



이 종 혁

e-mail : jhlee@imtl.skku.ac.kr

2004년 대전대학교 정보시스템공학과(학사)

2007년 성균관대학교 컴퓨터공학과(공학석사)

2007년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정

관심분야 : 네트워크 보안, 모바일 네트워크, 프로토콜 성능 분석

정 태 명

e-mail : tmchung@ece.skku.ac.kr

1981년 연세대학교 전기공학과(학사)

1984년 일리노이주립대학 전자계산학(공학사)

1987년 일리노이주립대학 컴퓨터공학과 (공학석사)

1995년 퍼듀대학교 컴퓨터공학과(공학박사)

1985년~1987년 Waldner and Co., System Engineer

1987년~1990년 Bolt Bernek and Newman Labs. Staff Scientist

1995년~현 재 성균관대학교 정보통신공학부 정교수

2007년~현 재 한국CPO포럼 의장

2000년~현 재 한국침해사고대응협의회(CONCERT) 위원장

관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, 전자상거래 보안, 유비쿼터스 컴퓨팅 보안