제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

Peer-to-Peer 네트워크 상에서 혼합형 신뢰도 관계성 모델 및 추천 프로토콜에 대한 연구

김인호*, 용환기*
*한동대학교 전산전자공학부
e-mail:tigersky@seed.handong.edu

A Study on Hybrid Trust Relationship Model and Recommendation Protocol for Peer-to-Peer Networks

Inho Kim*, Whanki Yong*
*School of Computer Science & Electronic Engineering,
Handong Global University

요 약

Peer-to-Peer 네트워크 상에서 구성원과 구성원 사이에 필요한 정보를 이용하기 위해서 각 구성원 및 구성원이 보유한 데이터에 대한 신뢰도(Trust)를 측정하는 일은 매우 중요하다. 이 논문에서는 네트워크 상에서 구성원 사이의 신뢰도에 대한 관계성을 정의하는 기존의 신뢰도 관계성 모델의 한계점을 개선한 혼합형 신뢰도 관계성 모델을 제시하고, 신뢰도 추천 프로토콜과 신뢰도 측정에 대한 확장 및 개선점을 제안한다.

1. 서론

과거의 인터넷의 개발은 학문연구나 과학적, 군사적 목적으로 제한적 사용만을 위하여 시작되었으나 이제는 상업적, 개인적인 용도로 전환되어 세계적으로 확산되면서 정보화 시대를 주도하는 기반이 되었다.

PC의 보급과 네트워크의 일반화로 인한 상업적 서버-클라이언트 모델이 등장하면서 많은 일반 사용자들이 중앙 집중화된 네트워크를 사용하였으나 최근 하드웨어와 소프트웨어의 급속한 발전을 통하여 많은 일반 사용자들이 독자적인 네트워크 운용 및 사용을 원하게 되었고, 그에 따라 기존의 서버를 중심으로 유지되던 컴퓨터 보안과 데이터 보호가 분산 네트워크, 특별히 최근에 이슈로 등장한 Peer-to-Peer 네트워크 상에서의 개개인의 권리와 의무로 점차 이동되고 있다.

신뢰도(Trust)는 이런 Peer-to-Peer 네트워크 상에서 구성원과 구성원간의 관계성에 대한 문제로서 네트워크 상의 구성원에 대한 개인의 판단이 반영되기 때문에 분산화의 특성을 가지고 있으며, 최근의 인터넷의 성향에 적용되고 있음을 알 수 있다[4].

본 논문에서는 Peer-to-Peer 네트워크 상에서 신뢰도를 정의하고, 기존의 신뢰도 관계성 모델(Trust Relationship Model)에 대한 한계성을 개선한 혼합형 모델을 제안하며, 혼합형 신뢰도 관계성 모델에 대한 확장된 추천 프로토콜 및 신뢰도 측정을 제안하고자 한다.

2. 신뢰도(Trust)

현재 네트워크 상에서 매일 접할 수 있는 E-mail, 전자상거래 같은 웹서비스들은 셀 수 없을 정도로 급속하게 확장되고 있다. 지금까지 개인 정보 및 데이터 보안에 대한 연구는 활발하게 진행되고 있으나 이런 보안 차원을 넘어서는 웹서비스들에 대한 신뢰 정도를 판단하는 인정된 웹 기술이나 표준은 아직까지 정해지지 않고 있다. 여기서 우리는 단순한 네트워크 보안의 차원을 뛰어넘는 추상화된 개념의 신뢰도의 정의가 필요하다.

Gambetta는 그의 논문에서 신뢰도를 한 에이전트가 특정 행동을 수행 가능하게 하는 특정한 수준의 가능성이라고 정의하였으며[5], Grandison과 Sloman은 특정 분야에 대한 다양한 신뢰도의 정의를 일반화하여 문맥 속에서 의존적, 안전적으로 믿을 수 있게 동작하는 믿음이라고 재 정의하였다[6].

Abdul-Rahman과 Hailes는 이러한 정의를 통해 나타나는 신뢰도의 특징들을 통해 신뢰도 운용에 대한 연구들을 확장시켜 결과적으로 분산화, 일반화, 신뢰도에 대한 명시적인 표현, 신뢰도 추천을 이용한 일반적인 인프라구조를 이루는 모델을 적용하고자 하였다[1]. 또한 Blaze는 이러한 신뢰도 운용에 대한 4가지 원칙인 통합된 메커니즘, 유연성, 동작의 지역성(locality of action), 원칙과 메커니즘의 분리 등을 적용하여 신뢰도 운용 모델을 제안하였다[2].

3. 신뢰도 관계성 모델(Trust Relationship Model)

네트워크 상에서 구성원들에 대한 신뢰도의 정도는 각 구성원간의 관계를 통해서 결정된다. 이런 신뢰도는 앞서 언급한 것처럼 한 구성원이 각각의 다른 구성원에 대해서 모두 다른 판단을 내리게 된다.

3.1 기존 모델과 한계점

Jøsang은 그의 논문에서 구성원(entity)의 종류를 trusting entity, trusted rational entity, malicious entity의 3가지 역할로서 구분하고, 역할에 대한 다양한 신뢰도의 관계성을 통한 모델을 제시하였다[7]. 그는 이 모델에서 사람과 시스템에 대한 관계성에 주목하였으나 Peer-to-Peer 네트워크에서는 존재하는 구성원 자체의 신뢰도에 대한 평가를 필요로 하기 때문에 명시적인 신뢰도 값을 나타내고 측정하는데 한계점을 가진다.

Abdul-Rahman과 Hailes는 분산 네트워크 상에서 에이전트에 의한 신뢰도 모델을 제안하며 관계성의 속성을 3가지로 제안하였다[1].

- 신뢰도는 항상 두 구성원 사이에서 존재한다.
- 비대칭적인 관계(non-symmetrical) 또는 단방향성(unidirectional)의 관계이다.
- 조건부적 전이(conditional transitive)가 가능하다.

또한 신뢰도 관계성을 직접 신뢰도 관계성과 추천자 신뢰도 관계성의 2가지로 구분하고, 신뢰도에 대한 일반화를 위하여 신뢰도에 대한 범주(categories)와 명시적인 신뢰도 값(trust value)을 제안하였다.

위의 신뢰도 모델을 확장한 Chen과 Yeager는 Poblano 신뢰도 모델에서 구성원 자체에 대한 신뢰도뿐만이 아니라 keyword를 이용한 codat이라는 해당 구성원이 보유한 데이터에 대한 신뢰도를 제안하였다[4].

그러나 에이전트 기반의 이 두개의 모델들은 Peer-to-Peer 네트워크에서 구성원의 역할에 대한 부분을 배제하여 신뢰도 측정에 있어 구성원의 역할에 따른 여러 경우에 대한 신뢰도 측정을 고려하지 않은 단점이 있다.

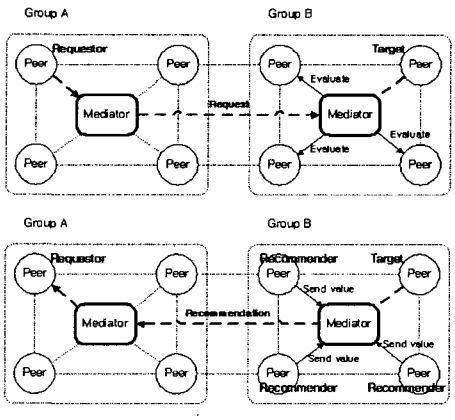
3.2 혼합형 신뢰도 관계성 모델(Hybrid Trust Relationship Model)

혼합형 신뢰도 관계성 모델에서는 기존의 keyword로 특정 지을 수 있는 집단을 통한 구성원의 특징에 대하여 특정 구성원이 필요로 하는 신뢰도에 대한 정보 요청을 할 경우 집단 내에 한 구성원이 중재자가 되어 필요한 신뢰도의 정보를 직접 전달하는 역할을 하여 개선된 효과를 볼 수 있다.

네트워크 상에 속해있는 구성원은 다음과 같은 역할을 가진다.

- 신뢰도 요청자(Trust Requester)
- 신뢰도 추천자(Trust Recommender)
- 신뢰도 중재자(Trust Mediator)

(그림 1)에서와 같이 신뢰도 요청자는 원하는 구성원 또는 데이터에 대한 신뢰도를 요청하며, 신뢰도를 요구하는 요청 메시지를 보낸다. 신뢰도 추천자는 요청 메시지를 통해 요청자가 원하는 구성원 또는 데이터에 대한 신뢰도 값이 존재할 경우 신뢰도를 위임하여 신뢰도 값을 담은 추천 메시지를 요청자에게 재 전송하게 된다.



(그림 1) 혼합형 신뢰도 모델에서 신뢰도 요구 및 추천

4. 신뢰도 추천 프로토콜(Trust Recommendation Protocol) 및 신뢰도 측정(Trust Computation)

4.1 신뢰도 추천 프로토콜

Abdul-Rahman과 Hailes는 Reputation이라는 신뢰도 값에 대한 정보를 담은 구조를 정의하고, 이 정보를 포함하여 전달하는 역할을 하는 프로토콜을 제안하였는데, RRQ(Recommendation ReQuest)는 네트워크 상에 있는 구성원에 대한 신뢰도 값을 요청하는 경우, Recommendation은 요청된 신뢰도 값을 보내주는 경우, Refresh는 유효기간이 지난 신뢰도 값을 갱신하는 경우에 사용하도록 되어있다[1].

그러나 구성원의 역할이 다양한 경우와 또한 원하는 신뢰도 값이 특정 구성원이 아닌 데이터일 경우를 고려해야 하기 때문에 현재 프로토콜만으로는 한계를 가지며, 프로토콜의 확장이 요구된다.

4.1.1 Extended RRQ

확장된 프로토콜에서 신뢰도 추천을 요청하는 메시지를 보내는 경우는 옆 구성원 또는 중재자에게 보내는 경우와 구성원 자체의 신뢰도 또는 구성원이 보유한 데이터에 대한 신뢰도 값을 요청하는 경우의 4가지로 확장되어진다.

(1) 집단 내에서 옆 구성원에게 요청하는 경우

- 구성원 신뢰도 요청

RRQ_{peer} ::= Requester_ID, Request_ID, Target_ID, Peer_Keyword, RequesterPKC, GetPKC, Expiry

- 데이터 신뢰도 요청

RRQ_{data} ::= Requester_ID, Request_ID, Data_Name, Data_Keyword, RequesterPKC, GetPKC, Expiry

여기서 Requester_ID는 요청자의 ID, Request_ID는 요청의 고유 ID, Target_ID는 신뢰도 값을 원하는 구성원의 ID, Peer_Keyword는 구성원의 서비스의 특성에 대한 Keyword, RequesterPKC는 요청자의 Public key에 대한 보증서, GetPKC는 Public key 보증서를 얻었는지에 대한 boolean 값, Expiry는 유효기간을 의미한다. 데이터의 경우는 Target_ID 대신 Data_Name을 사용한다.

(2) 중재자에게 요청하는 경우

중재자에게 요청하는 경우는 중재자의 ID(Mediator_ID)를 알아야 하며 여기서는 keyword를 통해 특정 집단의 중재자에게 메시지가 전달되도록 한다.

- 구성원 신뢰도 요청

RRQ_{peer_M} ::= Requester_ID, Request_ID, Mediator_ID, Peer_Keyword, RequesterPKC, GetPKC, Expiry

- 데이터 신뢰도 요청

RRQ_{data_M} ::= Requester_ID, Request_ID, Mediator_ID, Data_Name, Data_Keyword, RequesterPKC, GetPKC, Expiry

4.1.2 RMQ(Recommendation Mediator reQuest)

중재자가 신뢰도 추천 요구 메시지를 받았을 경우 전달된 keyword를 통해 일치하는지의 여부를 검사하고 일치할 경우 집단 구성원들에 원하는 정보를 요구하도록 하는 RMQ를 집단 전체 구성원에게 전달한다. 일치하지 않는 경우 해당 keyword와 일치하는 특성을 가진 다른 중재자에게 재 전송한다.

- 구성원 신뢰도 요청

RMQ_{peer} ::= Requester_ID, Request_ID, Mediator_ID, Peer_Keyword, RequesterPKC, GetPKC, Expiry

- 데이터 신뢰도 요청

RMQ_{data} ::= Requester_ID, Reqeust_ID, Mediator_ID, Data_Keyword, RequesterPKC, GetPKC, Expiry

4.1.3 Recommendation

신뢰도 요청 메시지를 통해서 원하는 신뢰도 값을 요청자에게 재 전송하는 메시지로서 구성원을 통해서 오는 경우와 중재자를 통해서 오는 경우로 확장된다.

- 구성원으로부터 오는 경우

$Recommendation_{peer}$ ::= Requester_ID, Request_ID, Rec_Path_{peer}, [SEQUENCE OF {Recommendation_Set, TargetPKC} | NULL]

- Rec_Path_{peer} ::= SEQUENCE OF {$Recommender_{peer}$_ID}
- Recommendation_Set ::= SET OF $Recommendation\_Slip_{(peer/data)}$
- $Recommendation\_Slip_{peer}$ ::= SET OF SEQUENCE {Target_ID, Peer_Keyword, Trust_value, Expiry}
- $Recommendation\_Slip_{data}$ ::= SET OF SEQUENCE {Data_Name, Data_Keyword, Trust_value, Expiry}

위의 메시지 구조에서 나타난 것처럼 되돌아오는 메시지는 여러 개의 신뢰도 값을 포함한다. 이때 구성원에 대한 신뢰도인 경우는 구성원에 대한 $Recommendation_Slip_{peer}$이, 데이터의 경우는 $Recommendation_Slip_{data}$이 돌아오게 된다.

- 중재자로부터 오는 경우

$Recommendation_{med}$ ::= Requester_ID, Request_ID, Rec_Path_{med}, [SEQUENCE OF {Recommendation_Set, TargetPKC} | NULL]

중재자로부터 오는 경우는 Recommendation에

대한 path가 중재자의 Path로 돌아오게 되며, 만약 원하는 신뢰도 값이 존재하지 않을 경우 중재자가 Recommendation_Set 값을 NULL로 변환하여 메시지를 반환한다.

4.1.4 Refresh

유효기간이 지났거나 변경된 신뢰도 값에 대한 수정이 필요한 경우 변경된 신뢰도 값을 옆 구성원 또는 중재자를 통해서 전파하는 메시지이다.

Refresh ::= Requester_ID, {Peer_Keyword | Data_Keyword}, [Recommendation_Set]

Refresh 메시지는 Requester_ID와 Peer_Keyword 또는 Data_Keyword가 일치하는 모든 구성원들은 전달되는 Recommendation_Set을 통해서 신뢰도 값을 갱신하도록 하는 역할을 한다.

이러한 확장 신뢰도 추천 프로토콜을 통해서 네트워크 상의 구성원들에 대한 역할의 다양화를 통한 신뢰도 요청 및 추천의 효율성을 높일 수 있다.

4.2 신뢰도 측정(Trust Computation)

Abdul-Rahman과 Hailes는 하나의 추천 경로 상에서 원하는 구성원에 대한 신뢰도 값을 아래와 같이 측정하도록 정의하였다.

$$V_{path}(T) = \frac{1}{4n}\left(\sum_{i=1}^{n} V(P_i)\right) \times V(T) \qquad (1)$$

(1)의 식에서 $V(P_i)$는 i번째 구성원의 신뢰도 값을 나타내며, $V(T)$는 목표된 구성원의 신뢰도 값이다. 전체 신뢰도 측정값은 (2)의 식과 같다.

$$V(T) = \frac{\sum_{i=1}^{n} V_{path_i}(T)}{n} \qquad (2)$$

혼합형 신뢰도 관계성 모델에서는 특정 keyword를 사용하는 구성원이 같은 keyword를 사용하는 데이터를 보유하고 있을 확률이 높으며, 구성원 자체의 신뢰도 값과 보유하고 있는 데이터의 신뢰도 값이 서로 연관성이 있음을 알 수 있다. 이러한 연관성을 수식으로 표현하면 식 (3)과 같다.

$$V(T) = \frac{\sum_{i=1}^{n} V_{path_i}(T)}{n} + \frac{V_{Data}}{n_{keyword}} \qquad (3)$$

식 (3)에서 V_{Data}는 Data의 전체 신뢰도 측정값이며, $n_{keyword}$는 구성원의 keyword와 일치하는 데이터에 대한 다른 구성원들의 신뢰도 값의 개수이다. 이를 통하여 구성원이 보유하고 있는 데이터와의 연관성을 통해서 신뢰도의 측정을 세분화할 수 있다.

5. 결론

지금까지 신뢰도 관계성 모델에 대한 소개와 신뢰도 추천 프로토콜 및 신뢰도 측정에 대한 확장에 대해서 제안하였다.

혼합형 신뢰도 관계성 모델을 통해서 기존의 신뢰도 관계성 모델의 단순성을 개선하고 확장된 신뢰도 추천 프로토콜 및 신뢰도 측정을 통해서 Peer-to-Peer 네트워크 상의 구성원의 역할의 다양화와 성능 향상을 볼 수 있었으며 신뢰도 측정에 대한 구성원 및 데이터의 연관성을 통해 보다 정확한 신뢰도의 측정을 할 수 있음을 제시하였다.

향후 연구 방향으로는 미들웨어 차원에서의 신뢰도 관계성 모델 및 프로토콜의 구현을 통해서 효율성 제고와 신뢰도 관계성 시스템의 성능 향상 및 비교에 대한 연구를 하고자 한다.

참고문헌

[1] A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model," In proc. of New Security Paradigms Workshop, 1997.

[2] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," IEEE Conf. Security and Privacy, 1996.

[3] F. M. Cuenca-Acuna and T. D. Nguyen, "Text-based Content Search and Retrieval in ad hoc P2P Communities", Technical Report DCS-TR-483, 2002.

[4] R. Chen and W. Yeager, "Polano : A Distributed Trust Model for Peer-to-Peer Networks," Sun Microsystems.

[5] D. Gambetta, "Can We Trust Trust?," In Trust : Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, pp.213-237, 1990.

[6] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications," IEEE Communication Surveys, pp. 2-16, 2000.

[7] A. Jøsang, "The Right Type of Trust for Distributed Systems," ACM New Security Paradigms Workshop, 1996.

[8] S. R. Waterhouse, D. M. Doolin, G. Kan and Y. Faybishenko, "JXTA Search: a distributed search framework for peer-to-peer networks," IEEE Internet Computing, v.6, pp. 68-73, 2002.