P2P 네트워크에서 블록 평판도를 이용한 악의적인 블록의 탐지 및 제거 방법 [1]

박희재, 김종, 홍성제
포항공과대학교 컴퓨터공학과
e-mail : {myphj, jkim, sjhong}@postech.ac.kr

Detecting and Removing Malicious Blocks using Block Reputation in P2P Networks

Heejae Park, Jong Kim, Sung Je Hong
Dept. of Computer Science and Engineering, Pohang University of Science and Technology

요 약

P2P 환경에서 사용자들이 직접 자료를 평가하여 악의적인 자료들을 탐지하는 평판도 방법들이 많이 연구되었다. 하지만 기존의 평판도 방법들은 자료 또는 파일 단위의 평판도를 적용하기 때문에 자료의 일부분에 대한 미세한 평가를 할 수 없으며, 특정 부분 때문에 평판도가 낮아서 자료 전체가 사용되지 못한다는 문제점을 가진다. 따라서 본 연구에서는 자료 일부분에 대한 평판도를 적용하는 새로운 평판도 방법을 제안한다. 제안하는 블록 기반의 평판도 방법은 자료의 부분에 대한 개별 평가를 하고 악의적인 블록을 배제함으로써 자료의 유익한 부분들만 사용할 수 있게 해 준다. 본 논문에서는 자료의 개별 블록 평판도와 피어의 신용도를 기반으로 하여 평판도 업데이트 방법과 개별 블록과 자료의 평가 방법을 제시한다. 또한 성능 평가를 통하여 제안하는 방법이 기존의 평판도 방법보다 자료에서 유익한 블록들만 추출하여 사용함을 보여주고 있으며, P2P 에서 발생하는 일인다역, 공모와 같은 공격에 안전함을 보이고 있다.

1. 서론

P2P 환경[1]은 사용자가 직접 자료를 배포할 수 있는 구조로 자료의 생산 및 배포에 있어 사용자 익명성을 보장하고 있다. 이것은 사용자가 단순히 무익한 자료나 웜과 같은 악의적인 프로그램을 배포해도 제재를 가하기가 쉽지 않다는 것을 의미한다. 따라서 사용자나 자료에 대한 과거의 평가들에 기반하여 예측할 수 있도록 하는 평판도 시스템에 대한 연구가 많이 진행되었다.

기존의 P2P 기반의 평판도 연구들은 피어의 평판도만 고려하거나 피어와 자료의 평판도를 혼용하여 사용한 방법들이다[2-5]. 피어 평판도를 고려한 모델은 피어의 이전 행동에 기반하여 해당 피어의 자료의 신뢰성을 검사하는 방법이다. 피어와 자료의 평판도를 혼용하는 모델은 피어 평판도가 가지는 약점인 피어의 백지화 방법을 보완하여 자료에 대한 평판도까지 검사하는 방법이다. 하지만 이 연구들은 공통적으로 자료를 하나의 완성본으로 간주하여 자료의 부분에 대한 평판도를 적용하지 않는다. 예를 들어 자료 A 가 a1, a2, …, an 으로 이루어진다고 할 때 이전의 평판도 연구들은 자료 A 에 대한 평판도만 고려할 뿐, A 를 이루는 각 부분 a1, a2, …, an 에 대한 세부적인 평판도를 다루지 않고 있다.

따라서 본 연구에서는 자료의 부분 평판도를 적용하는 방법과 이를 바탕으로 자료의 전체 평판도를 적용하는 방법을 제안하기로 한다. 자료의 부분 평판도를 적용함으로써 자료에서 악의적이거나 무익한 부분을 걸러낼 수 있게 되어 자료의 유익한 부분만을 사용할 수 있게 한다.

본 논문의 순서는 다음과 같다. 2 장에서는 관련 연구를 살펴보고, 3 장에서는 연구 동기와 문제를 정의하고, 4 장에서는 제안하는 방법에 대해 기술한다. 5 장에서는 제안하는 시스템의 성능 평가와 분석을 하며, 마지막으로 6 장에서는 결론을 맺는다.

2. 관련 연구

P2P 환경에서 평판도를 이용한 연구들로는 크게 피어 평판도를 이용한 연구[2,3]들과 피어와 자료 평판도를 동시에 사용한 연구[4,5]들이 있다.

피어 평판도 연구들로는 Mekouar 가 제안한 방법[2]과 EigenTrust[3]가 있다. 먼저 Mekouar 가 제안한 방법은 각 피어마다 정확한 자료를 제공하는가의 여부와 정확한 피드백을 주는가의 여부로 피어를 4 가지 클래스 중 하나로 판단한다. 각 피어의 평판도를 수치화하여 계산함으로써 악의적인 클래스에 속하는 피어들이 저절로 격리되는 방법을 사용하고 있다. EigenTrust 에서는 각 피어가 다른 피어들에 대한 신

[1] 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-(C1090-0701-0045))

뢰값을 저장하고 있다. 자료를 받고자 하는 피어가 자료를 가진 피어의 목록을 받아 그 중에서 한 피어를 선택하고자 할 때, 주변의 다른 피어들에게 해당 피어들의 평판도를 요청하여 피어들을 선택하는 방식을 취하고 있다. 하지만 피어 기반 평판도 방식은 평판도가 낮은 피어가 접속을 끊고 다른 별칭으로 들어오는 백지화(whitewashing)와 같은 방법에 취약한 단점을 지니고 있다.

이와 같은 단점 때문에 피어 평판도와 함께 자료 평판도를 고려한 연구들[4,5]이 제안되었다. XRep[4]는 Gnutella 기반의 완전히 분산된 P2P 환경에서 동작하며 모든 피어가 자료 및 다른 피어에 대한 평판도를 저장하고 있다. 자료을 요청할 때 먼저 해당 자료의 악의성 여부를 주변 피어들에게 물어본 뒤에 자료를 가진 피어 목록을 받아서 주변의 다른 피어들에게 피어의 평판도를 요청하여 어떤 피어에게 받을 것인가를 결정하는 방법이다. 한편, Iguchi[5]의 방법은 피어 평판도를 피어 공헌도와 피어 평가도로 세분화하고 피어 공헌도, 피어 평가도, 자료 평판도를 수식적으로 적용하여 자료의 악의성을 검사하고 자료를 받을 피어를 선택한다.

3. 연구 동기 및 문제 정의

P2P 환경에서는 불법적인 이득, 악의적인 사용, 악성 코드의 전파를 목적으로 하는 거짓 자료의 전송이 빈번히 일어나고 있다. 특히 자료에 악의적인 블록을 추가함으로써 자료를 주고 받는 피어들 사이에 네트워크 자원의 낭비를 가져오고, 좋게 평가받던 자료가 거짓 내용이나 무익한 수정을 통하여 좋지 않은 자료로 변질되는 경우가 발생할 수 있다. 하지만 기존의 P2P 기반 평판도 연구들은 완성된 자료를 대상으로 평가하며 자료의 부분적인 평가를 하지 않으므로 악의적인 부분들만 제외하는 것이 불가능하다.

따라서 본 연구에서는 여러 부분으로 구성되어 있는 자료를 P2P 환경에서 평가하기 위한 블록 평판도 방법을 제안하기로 한다. 제안한 방법은 자료의 일부분에 대한 평판도를 관리함으로써 무익한 부분을 제외하여 자료를 최적화시킬 수 있으며, 또한 자료의 일부분에 대한 평판도를 이용하여 전체 자료 전체에 대한 평판도까지 관리가 가능하다.

4. 제안하는 블록 평판도 방법

4.1. 시스템 모델

제안하는 모델의 각 자료는 크기가 여러 개의 블록으로 구성되어 있다.(그림 1) 블록은 완성된 정보를 담고 있는 하나의 논리적인 구조를 의미한다.

그림 1 에서는 자료가 총 11 개의 블록으로 구성되어 있음을 보여준다. 블록간의 화살표는 블록간의 의존성을 의미한다. 예를 들어 B1 블록은 B4, B5 블록이 의존하고 있으며, B1 블록이 제거되면 B4, B5 블록도 같이 제거되어야 함을 의미한다. 하지만 반대로 B5 블록이 없어지더라도 B1 블록은 없어지지 않는다.

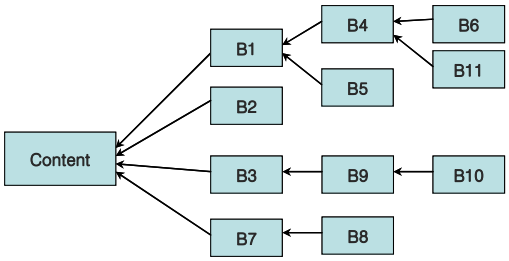

그림 1. 자료를 이루는 블록 구조도의 예

제안하는 블록 평판도 방법의 전체 시스템 모델은 그림 2 와 같다. 수퍼피어가 존재하는 P2P 구조를 바탕으로 하며, 자료는 하나 이상의 블록들의 집합으로 구성되어 P2P 내에 저장이 된다. 자료가 아닌 블록 단위로 평판도를 관리하며, 블록을 생산한 노드의 수퍼피어가 해당 블록의 평판도를 저장하게 된다.

제안하는 시스템은 다음과 같은 가정을 둔다.

- 자료에 블록을 추가할 수 있고, 자료를 이루는 기존 블록들과 의존성을 가질 수 있다.
- 한 자료를 구성하는 블록들 간에는 의존성을 가지고 있을 수도 있으며, 블록이 삭제되면 그에 의존하는 블록들은 모두 삭제된다.

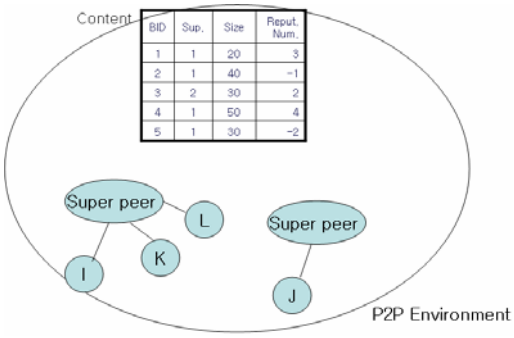

그림 2. 시스템 모델

본 논문에서 사용되는 표기는 표 1 과 같다.

표 1. 평판도 계산식에 이용되는 표기

BRepu(B)	블록 B 의 평판도
Cred(P)	피어 P 의 신용도
Sup(P)	피어 P 의 수퍼피어
size(B)	블록 B 의 크기
Rep(Q,B)	피어 Q 가 블록 B 에게 던지는 평가도. -1, 0, 1 중 하나의 값이 된다.

4.2. 블록 평판도

본 연구에서는 블록 평판도와 피어 신용도를 사용한다. 블록 평판도는 해당 블록에 대한 사용자들의 평가 수치를 의미하며, 피어 신용도는 해당 피어의 피드백이 얼마나 믿을만한 가에 대한 척도를 의미한다. 이 장에서는 평판도 및 신용도의 업데이트 방법과 적용 방법에 대해 기술하기로 한다.

4.2.1. 평판도 및 신용도 업데이트

블록 평판도는 블록을 생성할 때 초기값인 0 을 가지게 되며, 블록에 대한 피어의 평가가 있을 때 업데이트 된다. 피어의 신용도는 피어가 블록에 대해 평가를 보낼 때 업데이트 된다.

1) 피어 신용도 초기화: 피어가 처음으로 P2P 에 들어오게 되면 피어 신용도 값을 0 으로 설정한다.

2) 블록 생성 시 블록 평판도 초기화: 새로 생성된 블록 B 의 초기 평판도는 0 으로 둔다.

3) 평판도 및 신용도 업데이트: 피어 Q 가 블록 B 를 사용하고 난 뒤에 블록 B 의 평가도를 Rep(Q,B)로 설정하였다면, 블록 B 의 생성자의 수퍼피어는 이 값을 받아서 해당 블록의 평판도를 수식 (1)와 같이 업데이트한다.

$$BRepu(B)=BRepu(B)+size(B)*Cred(Q)*Rep(Q,B) \quad (1)$$

한편, 피어 Q 가 블록의 평가도를 보낼 때마다 Q 의 수퍼피어는 그림 3 과 같이 N 과 L 값을 업데이트 함으로써 피어 Q 의 신용도를 관리하게 된다.

```
If  BRepu(B) * Rep(Q,B) = 0,  then exit
If  AccessCount(B) < AcsThreshold, then exit

N = N + size(B)
If  BRepu(B) * Rep(Q,B)  > 0,
then L = L + size(B)
```

그림 3. 신용도 계산을 위한 업데이트 알고리즘

피어 Q 의 신용도는 수식 (2)와 같이 계산된다.

$$Cred(Q) = L / N \quad (2)$$

4.2.2. 평판도 및 신용도의 적용

피어 신용도는 피어가 블록을 평가할 때 수치화하여 반영이 된다(수식 (2)). 블록의 평판도는 자료를 요청하는 단계에서 이용되며 블록 자체의 사용 여부 뿐 아니라 자료 자체의 사용 여부 판단에도 이용이 된다.

1) 피어 P 가 자료 C 를 사용할 지를 판단할 때 우선 자료를 이루는 개별 블록들에 대한 보정 평판도부터 재귀적으로 계산한다.(그림 4) 각 블록들은 그림 1 과 같이 의존성 관계를 가지고 있으며, 상위 블록의 평판도는 하위 블록의 평판도에 의해 올라갈 수 있다. 평판도 보정이 끝나면 이 보정된 수치를 가지고 그림 5 의 알고리즘을 이용하여 개별 블록의 사용 여부를 판단한다. 보정된 수치가 0 이상이면 해당 블록을 사용하고 해당 블록의 하위 블록들도 재귀적으로 계산할 기회가 주어지지만, 보정된 수치가 0 보다 작으면 해당 블록은 사용하지 않고 하위 블록들 또한 모두 사용하지 않는다.

2) 개별 블록에 대한 사용 여부를 결정하면 해당 자료의 사용 여부를 판단한다. 자료를 이루는 최상위 블록들의 보정 평판도가 모두 0 보다 작으면 그 자료는 사용하지 않는다.

```
ImpBRepu(Bi) {
  RepuOfSubBls = 0

  For all Bj, Bj is child of Bi
    SubRepu = ImpBRepu(Bj);
    If SubRepu > 0  then
      RepuOfSubBls = RepuOfSubBls + SubRepu;

  Return (BRepu(Bi) + RepuOfSbuBls);
}
```

그림 4. 블록 평판도 보정 알고리즘

```
DecideBlocks(Bi) {
   If ImpBRepu(Bi) ≥ 0,  then
      USE(Bi);
      For all Bj, Bj is child of Bj
          DecideBlocks(Bj);
   Else
      EXCLUDE(Bi);
      For all Bj, Bj is child of Bj
         EXCLUDE(Bj);
}
```

그림 5. 사용할 블록들을 판단하는 알고리즘

4.3. 자료 요청 및 사용 프로토콜

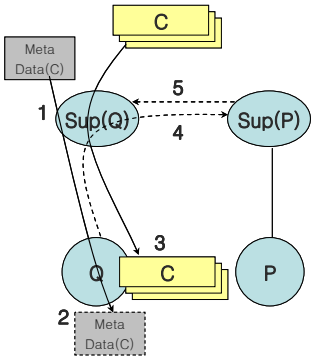

그림 6. 자료 요청 및 사용 프로토콜

피어 Q 가 자료 C 를 요청할 때의 순서는 다음과 같다.(그림 6)

1) 피어 Q 는 Q 의 수퍼피어 Sup(Q)를 통하여 C 의 메타데이터를 찾아서 가지고 온다.

2) Q 는 C 의 메타데이터에서 개별 블록들의 평판도를 얻는다. 이 평판도를 가지고 그림 4,5 의 알고리즘들을 적용하여 자료 C 를 이루는 개별 블록들의 보정 평판도를 계산하고 자료 C 의 사용 여부를 결정한다. 또한 개별 블록들의 사용 여부도 결정한다.

3) Q 가 자료를 사용하기로 결정하였다면 개별 블록의 사용 여부를 고려하여 자료 C 를 사용한다.

4) Q 는 자료의 각 블록에 대하여 평가를 할 수 있다. 평가를 하게 되면 Q 의 수퍼피어가 평가값을 받아서 해당 블록 생산자의 수퍼피어에게 평가도를 넘겨 준다. 그 수퍼피어는 블록에 대한 평판도를 수식 (1)과 같이 업데이트한다.

5) 마지막으로 Q 의 신용도를 업데이트 한다. 해당 블록 수퍼피어(그림 6 에서의 Sup(P))는 Q 의 평가도를 바탕으로 Q 의 수퍼피어에게 Q 의 평가의 신뢰성 여부를 수치로 알려준다. Q 의 수퍼피어는 그림 3 의 알고리즘을 이용하여 Q 의 신용도 변수들의 값을 업데이트 한다.

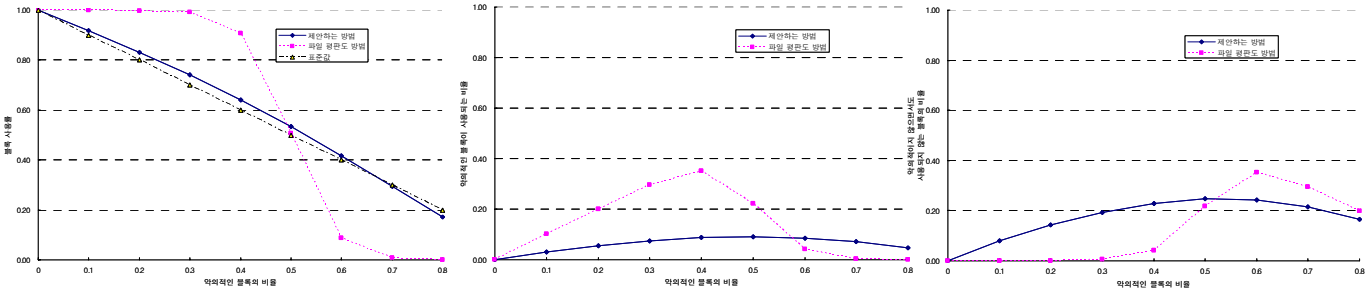

그림 7. 악의적인 블록의 비율에 따라 블록이 사용되는 비율(a), 악의적인 블록이 사용되는 비율(b), 악의적이지 않은 블록이 사용되지 않는 비율(c)

5. 성능 평가와 보안 분석

5.1. 실 험

피어 수는 1000, 자료 수는 1000 개, 자료에 속하는 블록 수는 1~100 개, 각 블록의 크기는 1~100MB, 악의적인 피어의 비율은 20%로 하여 실험을 하였다.(그림 7)

그림 7(a)는 전체 블록 중에 사용되는 블록의 비율을 가지고 이전의 파일 평판도 방법과 비교하였다. 악의적인 블록의 비율이 50% 이하에서는 파일 평판도 방법이 90% 이상의 사용률을 가지지만, 이는 악의적인 블록을 포함한 자료를 사용하게 된다는 것을 의미한다. 이에 비해 제안하는 방법은 파일 평판도 방법에 비해 블록 사용률이 낮지만, 악의적인 블록들을 제거하고 유익한 블록들만으로 구성된 자료를 사용하고 있음을 의미한다.

제안하는 방법은 파일 평판도 방법에 비해 악의적인 블록의 사용 비율이 2~4 배 정도 낮다.(그림 7(b)) 제안하는 방법이 악의적인 블록 사용률을 2~10%까지 유지하는 것은 그림 4 의 보정 평판도 알고리즘을 통하여 악의적인 블록들이 구제되기 때문이다.

제안하는 방법은 악의적이지 않으면서도 사용되지 않는 블록의 비율을 10~25%로 유지하고 있는데(그림 7(c)), 이는 악의적인 상위 블록들 때문에 사용되지 않는 유익한 하위 블록들이 존재함을 의미한다.

5.2. 분 석

P2P 기반 평판도 방법이 갖는 문제점[4]과 해결 방법은 다음과 같다.

1) 일인다역(Pseudospoofing): 일인다역 공격은 한 피어가 네트워크 상에서 여러 개의 다른 이름을 가질 때 발생하는 공격을 의미한다. 평판도가 낮은 사용자가 자신의 평판도를 초기화하기 위하여 새로운 사용자인 것처럼 네트워크에 접속하는 경우에 그 사용자의 예전의 기록들을 지울 수 있기 때문에 문제가 된다. 이와 같은 공격은 IP 기반의 인증이나 PKI 기반의 인증서를 사용함으로써 해결할 수 있다.

2) 공모(Shilling): 여러 피어들이 공동으로 잘못된 평가를 함으로써 진실을 왜곡하는 공격이다. 앞의 일인다역 공격을 통하여 단일 피어가 공모를 할 수도 있고, 친한 피어들끼리 합동하여 공모를 할 수도 있다. P2P 환경을 구성하는 피어 중 과반수 이상의 피어들이 공모를 하지 않는다고 가정한다면, 단기간에는 평판도가 잘못 계산되는 문제가 생길 수 있더라도 장기적으로 볼 때 공모하는 피어들의 신용도는 꾸준히 떨어지게 되므로, 장기적인 측면에서는 해결이 가능하다.

3) 낮은 초기값(Cold start): 자료 사용자는 평판도가 높은 자료를 사용하려는 경향이 있으며 제안하는 시스템에서는 갓 생산된 블록의 평판도는 0 의 값을 가지므로, 기존의 블록들과 비교하여 평판도가 낮을 수 있다. 하지만 이는 블록 사용 시 일정 임계치를 두어 임계치 이하에서는 평판도와 상관없이 무조건 사용하게 하는 방법을 적용하면 해결이 가능하다.

6. 결 론

본 연구에서는 피어 신용도, 자료의 부분 평판도를 이용한 블록 평판도 방법을 제시하였다. 제안하는 방법은 평판도 업데이트 알고리즘 및 적용 알고리즘을 제시하였으며, 이를 토대로 P2P 자료 요청 프로토콜을 제안하였다. 또한 실험을 통해 제안하는 방법이 기존의 평판도 방법들보다 유익한 자료들을 더 잘 추출하여 사용함을 보였으며, 간단한 분석을 통하여 일인다역 공격, 공모, 낮은 초기값 문제를 해결할 수 있음을 보여주었다.

참고 문헌

[1] S. Androutsellis-Theotokis, D. Spinellis, “A Survey of Peer-to-Peer Content Distribution Technologies,” ACM Computing Surveys, 2004.

[2] L. Mekouar, Y. Iraqi, R. Boutaba, “Peer-to-peer's most wanted: Malicious peers,” Computer Networks 50(4), pp.545-562, 2006.

[3] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina, “The Eigentrust algorithm for reputation management in P2P networks,” WWW 2003.

[4] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, F. Violante, “A reputation-based approach for choosing reliable resources in peer-to-peer networks,” ACM Conference on Computer and Communications Security, pp.207-216, 2002.

[5] M. Iguchi, M. Terada, K. Fujimura, “Managing Resource and Servent Reputation in P2P Networks,” HICSS 2004.