韓國컴퓨터情報學會 論文誌
第16卷 第7號, 2011. 7.

2011-16-7-3-2

협조적 분산시스템 환경에서 무임승차 방지를 위한 인센티브 디자인 고려사항 도출에 관한 연구

신 규 용* 유 진 철 * 이 종 덕 * 박 병 철 *

Incentive Design Considerations for Free-riding Prevention in Cooperative Distributed Systems

Kyuyong Shin* Jincheol Yoo * Jongdeog Lee * ByoungChul Park *

요 약

전통적인 클라이언트-서버 방식과는 달리 협조적 분산시스템 환경에서는 시스템에 참여하는 구성원들이 공통의 목표를 달성하기 위해 자신들의 자원을 자발적으로 제공하므로 참여자의 수에 관계없이 양질의 서비스 제공이 가능하다. 하지만 이기적인 참여자들의 경우 시스템으로부터 서비스를 제공받으면서도 자신들의 자원은 공유하지 않는 경우가 발생하는데 이를 무임승차라 한다. 협조적 분산시스템 환경에서 무임승차자의 수가 늘어나면 서비스 제공을 위한 시스템의 수용력은 줄어들게 되고, 종국에는 공유지의 비극, 즉 시스템으로부터 아무도 서비스를 제공받을 수 없는 현상이 발생한다. 따라서 성공적인 협조적 분산시스템을 구현하기 위해서는 무임승차 방지를 위한 효과적인 인센티브 메커니즘 개발이 필수적이다. 협조적 분산시스템 환경에서 인센티브 메커니즘이 갖는 중요성 때문에 지금까지 수많은 종류의 인센티브 메커니즘들이 개발되어 왔지만 인센티브 메커니즘의 성능을 판단하기 위한 기준이 불분명하였다. 따라서 본 논문은 광범위한 관련연구를 통해 협조적 분산시스템 환경을 위한 일반적인 인센티브 디자인 고려사항들을 도출한다. 본 논문에서 도출된 고려사항들은 관련 연구자들에게 협조적 분산시스템 환경에서 무임승차방지를 위한 효과적인 인센티브 메커니즘 디자인을 위한 가이드라인 및 성능 척도를 제공할 것이다.

▸ Keyword : 협조적 분산시스템, 인센티브 메커니즘, 무임승차, 디자인 고려사항

Abstract

Different from the traditional client-server model, it is possible for participants in a cooperative distributed system to get quality services regardless of the number of participants in the system since they voluntarily pool or share their resources in order to achieve their common goal. However, some selfish participants try to avoid providing their resources while still enjoying the benefits offered by the system, which is termed free-riding. The results of free-riding in cooperative distributed systems lead to system collapse because the system capacity (per participant) decreases as the number of free-riders increases, widely known as the tragedy of commons. As a consequence, designing an efficient incentive mechanism to prevent free-riding is mandatory for a successful cooperative distributed system. Because of the importance of incentive mechanisms in cooperative distributed system, a myriad of incentives mechanisms have been proposed without a standard for performance evaluation. This paper draws general incentive design considerations which can be used as performance metrics through an extensive survey on this literature, providing future researchers with guidelines for the effective incentive design in cooperative distributed systems.

▸ Keyword : Cooperative Distributed Systems, Incentive Mechanism, Free-riding, Design Considerations

• 제1저자 : 신규용 • 교신저자 : 신규용
• 투고일 : 2011.02.15. • 심사일 : 2011.03.06. • 게재확정일 : 2011.04.03.
* 육군사관학교 전자정보학과 (Dept. of Electrical Engineering and Information Science, Korea Military Academy)
※ 본 논문은 육군사관학교 화랑대연구소 2011년도 연구활동비를 지원받아 연구되었음

www.kci.go.kr

I. 서 론

많은 협조적 분산시스템 환경에서 참여자들은 공동의 목표를 달성하기 위해 계산 능력 (computing power), 저장 공간 (storage space), 혹은 네트워크 대역폭 (network bandwidth)과 같은 자원을 자발적으로 공유하는데, 통상 이런 시스템들을 협조적 분산시스템 (cooperative distribut ed system)이라 부른다. 도메인 네임 시스템, BGP-4 라우팅 정보 교환, 어플리케이션 계층의 멀티캐스트, 혹은 파일 공유 시스템들은 협조적 분산시스템의 대표적인 예라 할 수 있다. 최근에는 온라인 콘텐츠 (contents)의 빠른 확산과 더불어 BitTorrent[1, 2], Kad 네트워크[3], 그리고 Gnutella[4] 등과 같은 피투피 (Peer-to-Peer, P2P) 기반의 협조적 분산시스템들이 각광받고 있다. 최근 수행된 연구결과에 의하면 파일공유 분산시스템에서 발생하는 트래픽은 전체 인터넷 트래픽의 50%에 이르고 있는 것으로 나타났다[5]. 이는 인터넷에서 협조적 분산시스템이 차지하는 위치를 보여주는 좋은 예라 할 수 있다.

협조적 분산시스템 환경에서 제공되는 정보나 서비스는 공공재 (public goods)라 볼 수 있는데, 참여자들은 공공재의 준비를 위해 상호 협조하여야 한다. 이런 협조적 분산시스템 환경에서 모두가 만족할만한 서비스 제공을 위해서 참여자들 간의 협동이 매우 중요하다. 하지만 일부 이기적인 참여자들의 경우 공공재의 준비에 대한 책임은 회피한 채 시스템이 제공하는 이득에만 관심을 갖는다. 이와 같이 자신의 책임은 회피한 채 이득만을 추구하는 참여자를 무임승차자 (free- rider)라 부른다. 협조적 분산시스템에서 무임승차자의 증가는 공공재에 대한 준비부족을 야기하고, 종국에는 시스템이 붕괴되는 공유지의 비극 (tragedy of commons) 현상[6]을 초래한다. 실례로 Hughes[7]는 Gnutella 네트워크에 대한 측정연구를 통해 85%에 이르는 참여자들이 파일을 전혀 공유하지 않는다는 사실을 발견하였고, Handurukande[8]은 80%가 넘는 eDonkey 참여자들이 무임승차자임을 발견하였다. 이런 점을 볼 때, 무임승차는 이론에만 그치는 문제가 아니라 현실적인 문제임이 명백하다. 따라서 이러한 문제를 해결하기 위해 (참여자들에 대한 협동을 유도 혹은 강제하는) 효과적인 인센티브 메커니즘 (incentive mechanism)은 협조적 분산시스템의 성공을 위한 필수조건이라 하겠다.

이런 중요성 때문에 지금까지 협조적 분산시스템에서 참여자들로 하여금 협동을 강제하거나 유도하기 위한 다양한 종류의 인센티브 메커니즘들이 제안되었는데, 이런 인센티브 메커니즘들은 크게 금전교환 방식[9, 10], 평판 방식[11-13], 그리고 호혜주의 방식[2, 14-18] 등으로 분류될 수 있다. 하지만 이런 다양한 시도에도 불구하고 기존의 인센티브 메커니즘들의 성공은 지극히 제한적이었는데[19], 이는 인센티브 메커니즘들의 분석을 위한 객관적 성능 척도 (performance metric)가 결여되었다는 점에서 그 이유를 찾을 수 있다. 즉, 인센티브 메커니즘의 디자인 단계에서 필수적으로 고려해야 하는 사항들을 제대로 점검하지 못함으로써 많은 취약점들 (weak points)을 내포하게 되었고, 무임승차자들은 그 취약점들을 전략적으로 공략[1]함으로써 기존의 인센티브 메커니즘들을 무력화시켰다. 무임승차 방지를 위한 다양한 메커니즘 추가를 통해 현재까지 가장 성공적인 협조적 분산시스템의 하나로 알려진 BitTorrent[2, 14]에서 무임승차자의 수가 오히려 증가하고 있다는 사실은 이를 뒷받침하고 있다[20]. 따라서 효과적인 인센티브 메커니즘 디자인을 위한 핵심 고려사항 도출을 통해 객관적이고 일반적인 성능 척도 제시가 필수적이다.

본 논문은 일반적인 인센티브 디자인 고려사항들을 도출하기 위해 협조적 분산시스템 환경에서 참여자들 간의 상호 협동을 강제 혹은 유도하기 위해 제시되었던 기존의 인센티브 메커니즘들을 연구하고, 제안된 인센티브 메커니즘들을 회피 혹은 우회하기 위한 기존의 공격 방법들에 대해 자세히 분석한다. 이렇게 도출된 인센티브 디자인 고려사항들은 향후 협조적 분산시스템을 위해 개발되는 인센티브 메커니즘들의 성능 분석 및 취약점 분석의 척도로 활용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 제시되었던 인센티브 메커니즘을 자세히 연구하고, 3장에서는 기존에 제시된 인센티브 메커니즘을 우회하기 위해 무임승차자들이 사용하고 있는 전략적 우회 (strategic manipulation) 기법들에 대해 조사하고 분석한다. 4장에서는 조사 및 분석 결과를 바탕으로 협조적 분산시스템을 위한 효과적인 인센티브 디자인 고려사항들을 도출한다. 5장에서는 도출된 인센티브 디자인 고려사항들에 근거해서 현재까지 가장 성공적인 협조적 분산시스템의 하나로 알려진 BitTorrent 및 그 변종들에 대한 성능분석을 실시함으로써 성능 척도로서의 활용 가능성을 타진한다. 마지막으로 6장에서 결론 및 향후 연구방향을 제시한다.

II. 현존하는 인센티브 메커니즘들

협조적 분산시스템의 성공은 참여자들로 하여금 시스템을 위해 자신들의 자원을 자발적으로 기부하도록 동기를 부여하거나 강제하는 인센티브 메커니즘의 효과에 달려있다. 만일 자신의 자원을 기부하지 않는 참여자들이 시스템으로부터 서비스를 전혀 받을 수 없도록 할 수 있다면 무임승차는 크게

1) 무임승차자들은 인센티브 메커니즘이 부여하는 페널티 (penalty)를 우회 (bypass)하는 방법을 개발함으로써 인센티브 메커니즘을 무력화시킬 수 있다.

www.kci.go.kr

줄거나 제거될 수 있을 것이다. 이런 목적을 달성하기 위해 지금까지 다양한 종류의 인센티브 메커니즘들이 제안되었는데, 이런 인센티브 메커니즘들은 금전교환 방식[9, 10], 평판 방식[11-13], 그리고 호혜주의 방식[2, 14-18] 등으로 범주화할 수 있다. 이 장에서는 각 범주별 인센티브 메커니즘들의 특성 및 장·단점을 조사하고 분석한다.

1. 금전교환 방식 (Money)

금전교환 방식은 간단한 소액지불 (micro-payment) 메커니즘을 시스템에 도입하여 참여자들에게 제공되는 서비스의 종류에 관계없이 단일한 가치를 제공함으로써 비대칭적 이해관계 (asymmetric interest)에 놓여 있는 당사자들 간에도 거래가 성립할 수 있도록 유도한다. 이런 금전교환 방식에서는 화폐의 흐름에 따라 개발 참여자의 자원소비 및 공헌 정도를 추적할 수 있기 때문에 무임승차 여부가 쉽게 판별된다. 예를 들어, Vishnumurthy[9]는 KARMA라 불리는 가상화폐를 개발하였는데, 참여자들은 시스템에 자신의 자원을 기부함으로써 (즉, 다른 참여자들에게 서비스를 제공함으로써) KARMA를 획득할 수 있고, 이렇게 축적된 KARMA는 자신에게 서비스를 제공하는 다른 참여자에게 보상의 수단으로 재사용할 수 있다. 이런 시스템에서는 축적된 KARMA의 양을 통해 개별 참여자의 공헌 정도가 쉽게 판별되므로 추가적인 메커니즘 없이도 효과적으로 무임승차를 방지할 수 있다.

하지만 금전교환 방식을 구현하기 위해서는 통화의 창출이나 관리를 위한 별도의 기반시설 (infrastructure)이 필요하며, 이런 기반시설은 모두가 신뢰할 수 있는 신뢰주체 (trusted entity) 없이는 구현이 어렵기 때문에 시스템이 복잡해진다. 또한 시스템에 처음 참여하는 신규 참여자 (newcomer)를 다루기 위한 별도의 정책이 필요하며, 대부분의 경우 통화관리와의 연동을 위해 신규 참여자에 대한 인증 (authentication) 절차가 필요하므로 익명성 (anonymity)이 요구되는 어플리케이션들에는 적용이 제한된다.

2. 평판 방식 (Reputation)

평판 방식의 경우는 시스템 내에서 발생하는 개별 트랜잭션 (transaction)을 모니터함으로써 시스템에 대한 개별 참여자의 기여도 (즉, 평판)를 측정함으로써 서비스 우선순위를 결정하는 방식이다. 평판 방식에서 참여자 A가 다른 참여자 B의 요구를 받아들일 지 여부는 B가 지금까지 다른 참여자들에게 제공한 서비스의 질에 의해 결정된다. 비록 B가 A에게 직접 서비스를 제공한 적이 없더라도 다른 참여자 C에게 서비스를 제공했다면 A는 B의 요구를 받아들이는 것이다. 또한 여러 참여자들로부터 서비스 요구를 받는 경우, 시스템을 위해 지금까지 가장 많은 서비스를 제공한 참여자를 우선 선택한다. 따라서 평판 방식은 금전교환 방식과 마찬가지로 비대칭적 이해관계가 있는 참여자들 간의 거래를 쉽게 유도할 수 있다는 장점을 가진다. 이런 평판 방식의 대표적인 예로는 EigenTrust[11], One hop reputation[12], Sorcery[13] 등을 들 수 있다.

하지만 평판 방식의 단점은 시스템 전체에 적용할 수 있는 평판 정보를 수집하기 위해 제 3자가 제공하는 정보에 의존해야 하기 때문에 공모 (collusion)를 통한 거짓 정보 제공에 취약하며, 정확한 평판 정보를 얻기 위해 많은 계산이 필요하므로 시스템이 복잡해지는 단점이 있다. 또한 시스템이 커질수록 처리해야 하는 정보의 양이 많아지므로 확장성이 떨어져 대규모의 분산시스템에 적용하기 어렵다. 추가적으로 신규 참여자를 어떻게 다룰 것인지에 대한 딜레마에 봉착할 수 있다[2].

3. 호혜주의 방식 (Reciprocity)

금전교환 방식이나 평판 방식과는 달리 호혜주의 방식은 각각의 참여자가 자신의 경험에 비추어 서비스 대상을 결정하는 방식이다. 이 방식에서 참여자 A가 다른 참여자 B의 서비스 요구를 받아들일 지에 대한 여부는 과거 B가 A에게 제공한 서비스의 질, 혹은 B가 A에게 앞으로 제공 가능한 서비스의 질에 의해서 결정된다. 호혜주의 방식에서는 상호 이해관계 (mutual interest)에 있는 당사자들 간에만 거래가 이루어지므로 구현이 상대적으로 간단하다는 장점이 있다. BitTorrent[2, 14]의 tit-for-tat (TFT) 알고리즘과 그 변형들[15-18]은 대표적인 호혜주의 방식의 인센티브 메커니즘들이다. 호혜주의 방식은 구현의 간편성 때문에 현재 가장 널리 사용되고 있다.

하지만 호혜주의 방식을 적용한 시스템에서는 비대칭적 이해관계가 있는 참여자들 간의 거래가 제한되어 시스템이 경직될 수 있다는 단점 때문에 비대칭적 이해관계에 있는 참여자들 간의 활발한 거래를 유도하기 위한 방안들이 추가되어야 한다. BitTorrent의 optimistic unchoking (OU)이나 전방위 보상 (pay-it-forward)[24] 기법은 호혜주의 방식의 시스템에서 비대칭적 이해관계에 있는 참여자들 간의 거래를 촉진하기 위해 사용되는 방안들이다.

III. 전략적 우회 기법

앞장에서 설명된 인센티브 메커니즘들은 협조적 분산시스템 환경에서 무임승차에 페널티를 부여하여 참여자들로 하여금 시

2) 만일 신규 참여자에게 높은 평판을 부여하면 신분세탁 (whitewashing)과 같은 무임승차 공격에 취약하고, 너무 낮은 평판을 부여하게 되면 참여 초기에 시스템에 공헌할 것이 없는 신규 참여자에 대한 진입장벽이 커져 시스템 성장 동력을 잃는다.

www.kci.go.kr

스템을 위해 공헌하도록 유도하기 위한 목적으로 고안되었다. 하지만 실제로는 기존의 인센티브 메커니즘에 의해 부여되는 페널티를 피할 수 있는 다양한 전략적 우회 기법들이 개발되어 인센티브 메커니즘들을 무력화하고 있다. 이런 전략적 우회는 인센티브 메커니즘 디자인 단계에서 미처 고려하지 못한 취약점들을 공략하는 방식으로 구현되는데, 이타주의 공략 (exploiting altruism), 부정행위 (cheating), 큰 시야 공략 (large-view-exploit), 신분세탁 (whitewashing)과 시빌 (Sybil) 공격, 그리고 공모 (collusion)등이 대표적인 예이다.

1. 이타주의 공략 (exploiting altruism)

무임승차자들은 시스템 안에 존재하는 이타적인 참여자들을 공략할 수 있다. 예를 들어 하나의 BitTorrent 스웜 (swarm) 안에는 통상 시더 (seeder)라 불리는 다수의 이타주의적 참여자들이 있는데, 시더들은 파일을 분배하기 위해 아무런 조건 없이 자신의 업로드 대역폭을 공유한다. 무임승차자들은 이런 시더들을 찾아 서비스를 요청함으로써 자신의 자원을 공유하지 않으면서 공짜로 파일을 다운로드할 수 있다[6, 19]. 하지만 이기적인 참여자 (selfish participant)가 지배적인 협조적 분산시스템 환경에서는 이타주의 공략만으로는 얻을 수 있는 효과가 상대적으로 작으므로 다른 전략적 우회 기법들과 병행되는 것이 일반적이다.

2. 부정행위 (cheating)

호혜주의 방식에서 과거에는 서로 거래가 없었지만 상호 이해관계가 있는 (즉 서로에게 관심이 있는) 참여자 A와 B가 처음으로 거래를 시작하는 경우 먼저 서비스를 제공하는 측은 상대방이 추후 자신에게 상응하는 서비스로 보상해 줄 것으로 예상하고 자신의 자원을 공유한다. 예를 들어 BitTorrent의 리처 (leecher)들은 OU를 통해 기존에 거래가 전혀 없던 참여자들에게도 서비스를 제공하는데, 그 이면에는 서비스 수혜자가 향후 TFT를 통해 자신에게 보상 (reciprocation)할 것이라는 기대가 담겨있다. BitTorrent의 경우 전체 시스템 자원의 20%를 이런 목적으로 할당한다. 이와 비슷하게 평판 방식의 하나인 EigenTrust[11]의 경우도 전체 시스템 자원의 10%정도를 평판정보가 전혀 없는 참여자들에게 할당한다. 이런 일련의 자원 할당은 신규 참여자들의 활발한 참여유도를 위해서 필수불가결한 요소이다. 하지만 무임승차자들은 서비스를 받은 이후 보상을 거부하는 부정행위를 통해 무임승차를 실현할 수 있다.

3. 큰 시야 공략 (large-view-exploit)

대규모의 협조적 분산시스템에서는 하나의 참여자가 시스템 안의 모든 참여자에 대한 정보를 알 수도 없고 알 필요도 없다. 대부분의 경우 적정 수의 참여자에 대한 정보만 가지고도 문제없이 서비스를 주고받을 수 있다[25]. 예를 들어 BitTorrent의 경우 구현방식에 따라 다소 차이는 있지만 한 참여자가 약 50명 내외의 다른 참여자와 이웃 (neighbor)관계를 설정하고 서로 서비스를 주고받는다. 이와 같이 제한된 시야 (view)를 갖는 경우 무임승차자가 이타주의 공략이나 부정행위를 통해서 무료로 받을 수 있는 서비스의 양은 상당히 제한적일 수밖에 없으므로 효과적인 무임승차를 실현하기 어렵다. 따라서 무임승차자들은 가능한 많은 참여자들과 이웃관계를 설정함으로써 무임승차 효과를 극대화하는데, 이런 공격방법을 큰 시야 공략 (large-view-exploit)이라 부른다. 이 공격방법은 아주 간단하지만 대단히 효과적인 공격방법으로 알려져 있다[19, 25, 26].

4. 신분세탁 (whitewashing) 및 시빌 (Sybil) 공격

만일 무임승차 공격을 받은 참여자들이 무임승차자의 신분 (identity, ID)을 기억할 수 있다면 동일한 무임승차자가 한 참여자로부터 지속적으로 무료 서비스를 받는 것은 극히 제한될 수밖에 없다. 예를 들어 BitTorrent에서 무임승차자 A가 참여자 B로부터 서비스 받은 후 보답을 거부한다면 B는 TFT 메커니즘을 통해 A에 대한 서비스 제공을 중단할 것이다. 그러나 TFT는 개별 참여자가 하나의 신분을 지속적으로 사용한다는 가정 하에서 효과를 거둘 수 있다. 만일 무임승차자 A가 일정 서비스를 받은 이후에 자신의 신분을 바꿔버리면 피해자 B는 무임승차자 A를 다른 참여자로 판단할 것이고, OU를 통해 계속 서비스를 제공하게 될 것이다. 실제로 대규모의 분산시스템 환경에서는 무임승차자를 비롯한 참여자들이 신분을 바꾸거나 (whitewashing[11, 15]) 다수의 신분 (Sybil[27, 28])을 만드는 것이 매우 쉬운 것으로 알려져 있다. 따라서 무임승차자들은 신분세탁이나 시빌 공격을 통해 다른 참여자들을 지속적으로 속이면서 무임승차를 할 수 있다.

5. 공모 (collusion)

무임승차자들은 시스템에 대한 공헌을 피하면서 자신들의 이익을 극대화하기 위해 서로 협동할 수 있다. 예를 들어 평판 방식은 거짓 비난 (false accusation)이나 거짓 칭찬 (false praise)에 매우 취약한 것으로 알려져 있는데[19, 29], 무임승차자들은 자신들의 평판을 높이거나 다른 참여자들의 평판을 낮추기 위해 서로 협조할 수 있다. 대규모의 분산시스템에서는 참여자들 간에 발생하는 각각의 트랜잭션을 증명하거나 감시하기가 매우 어렵기 때문에 무임승차자들 간의 공모를 발견하

www.kci.go.kr

거나 공모에 대한 페널티를 부여하기 어렵다.

IV. 인센티브 디자인 고려사항들

앞서 2장과 3장에서 살펴본 바와 같이 협조적 분산시스템에 적용하기 위한 효과적인 인센티브 메커니즘을 디자인하기 위해서는 다양한 사항들을 염두에 두어야 한다. 처음으로 고려해야 할 사항은 단순성 (simplicity)과 확장성 (scalability)이다. 아무리 좋은 인센티브 메커니즘이라 할지라도 복잡하여 구현할 수 없다면 무용지물이 될 수밖에 없다. 지금까지 수많은 종류의 금전교환 혹은 평판 방식의 인센티브 메커니즘들이 개발되었지만 구현이 복잡하여 실제로는 사용되지 못하고 있다는 사실은 이를 뒷받침 한다. 또한 시스템에 참여하는 사용자 수가 증가하더라도 개별 사용자가 경험하는 서비스의 질에 차이가 있어서는 안 된다. 다음으로는 시스템에 공헌을 많이 하는 참여자가 양질의 서비스를 받을 수 있도록 보장해야 하는데, 이는 공평성 (fairness) 정도로 판단할 수 있다. 인센티브 메커니즘을 통해 공평성을 보장받을 수 있다면 참여자들은 자기 자신의 이익을 극대화하기 위해 자발적으로 시스템에 공헌할 것이다. 하지만 지나치게 공평성을 강조하는 시스템에서는 신규 참여자에 대한 참여유도 (bootstrapping)가 제대로 되지 않을 수 있는데, 그 이유는 신규 참여자의 경우 참여 초기에 제공할 수 있는 서비스가 없기 때문이다. 신규 참여자에 대한 참여유도가 제대로 되지 않는 시스템은 성장 동력을 잃기 때문에 경직될 수밖에 없다. 바로 여기에 효과적인 인센티브 메커니즘 디자인의 딜레마 (dilemma)가 존재한다. 공평성을 잃지 않으면서도 신규 참여자에 대한 진입장벽을 낮추어야 하는 모순 (contradiction)을 해결해야 하는 것이다. 이와 더불어 효과적인 인센티브 메커니즘이 되기 위해서는 무임승차자들이 택할 수 있는 다양한 전략적 우회 기법에 대한 견고성 (robustness)을 제공해야 하며, 비대칭적 이해관계 (asymmetric interest)에 있는 참여자들 간에도 활발한 거래 (transaction)가 이루어 질 수 있도록 보장해야 한다.

1. 단순성과 확장성 (simplicity and scalability)

협조적 분산시스템에 적용하기 위한 인센티브 메커니즘은 분산시스템 환경에서 구현이 용이하고, 인센티브 도입으로 인한 시스템 부담이 적어야 한다. 기존의 금전교환 방식[9, 10]이나 평판 방식[11, 12]의 인센티브 메커니즘들의 경우 인센티브 메커니즘 구현을 위해 중앙집중식 하부구조가 추가로 필요하거나, 구현이 복잡하여 대규모의 분산시스템 환경에 적용하기는 제한된다. 따라서 평판 방식처럼 모든 (혹은 대다수) 참여자들의 의견일치 (consensus)가 이루어져야 한다든지 시스템 내 참여자들 간에 발생하는 모든 트랜잭션을 모니터해야 하는 식의 인센티브 메커니즘은 분산시스템 환경에 적합하지 않다. 즉, 모든 의사결정은 개별 참여자가 자신의 개인적인 경험만을 바탕으로 내릴 수 있어야 한다. 신뢰성 문제를 해결하기 위해 제 3의 신뢰주체 (trusted third party)가 요구되는 방식 또한 분산시스템 환경에 적합하지 않으며, 신분에 대한 인증 (authentication)을 요구하는 방식도 분산시스템이 가지는 장점인 익명성 (anonymity)을 해치기 때문에 피해야 한다. 마지막으로 인센티브 메커니즘 도입에 의한 참여자당 추가부담 (overhead)이 일정하여 시스템의 확장성을 제한하지 않아야 한다.

2. 신규 참여자 유도 (newcomer bootstrapping)

시스템에 처음으로 참여하는 신규 참여자의 경우 참여 초기에는 다른 참여자들을 서비스할 수 있는 방법이 없다. 예를 들어 BitTorrent의 경우 신규 참여자들은 파일 조각이 하나도 없기 때문에 최소한 하나의 파일 조각을 얻을 때까지는 시스템을 위해 공헌할 수 없다. 따라서 신규 참여자들이 자원공유에 동참하기 위해서는 시스템에 의해 최소한의 서비스가 먼저 제공되어야 한다. 기존의 인센티브 메커니즘의 경우 이런 문제를 해결하기 위해 시스템 자원의 일부를 신규 참여자를 위해 할당한다. BitTorrent의 경우는 전체 시스템 자원의 20%를 OU 방식을 통해 신규 참여자들에게 할당하고 있으며, 평판 방식의 인센티브 메커니즘들의 경우도 일정 부분을 평판 정보가 전혀 없는 참여자들을 위해 할당하고 있다. 그러나 주의해야 할 점은 신규 참여자들의 참여를 유도하기 위해 할당되는 자원이 무임승차 공격의 주요 공격 포인트가 된다는 점이다[19, 25, 26]. 그렇다고 무임승차를 막기 위해 신규 참여자를 위한 자원할당을 제한하면 시스템이 경직되고 성능이 급격히 저하된다[23].

위와 같은 딜레마를 해결하기 위해서는 두 가지 해결 방법이 적용될 수 있다. 첫 번째는 신규 참여자를 위해 할당되는 자원의 양을 신규 참여자의 수에 따라 유연하게 조정하는 것이다[15]. 예를 들어 BitTorrent의 경우 OU를 위해 시스템 자원의 20%가 고정적으로 신규 참여자들에게 할당되어 있는데, 이렇게 고정적인 자원할당의 경우 무임승차에 대한 취약성이 해소되기 어렵다. 따라서 FairTorrent[18]처럼 신규 참여자의 비율에 따라 동적으로 자원을 할당하는 방식으로 무임승차에 대한 내성 (tolerance)을 키우는 것이 바람직하다. 두 번째는 네트워크 코딩 (network coding)이나 암호화 (encryption) 방식을 도입하는 방법이다[10, 17, 19, 32].

www.kci.go.kr

이와 같이 네트워크 코딩이나 암호화 방식을 사용하는 경우 신규 참여자에게 할당되는 자원은 서비스 수신자에 의한 보상(reciprocation)이 이루어지기 전에는 전혀 이득이 될 수 없기 때문에 무임승차를 효과적으로 제한할 수 있다.

3. 공평성 (fairness)

대부분의 경우 참여자들은 자신이 시스템에 공헌한 만큼 시스템으로부터 서비스를 받을 수 있다면 공평하다 느낄 것이고 보다 많은, 혹은 양질의 서비스를 받기 위해 자신이 가지고 있는 자원을 적극 공유하려 할 것이다[18]. 비록 공평성 수준이 높은 시스템이 가장 좋은 시스템 성능을 가지는 것은 아니지만[31] 무임승차에 대한 욕구를 효과적으로 차단하기 위해서는 보다 높은 공평성 수준을 강제하는 것이 바람직하다. 따라서 효과적인 인센티브 메커니즘을 갖춘 시스템은 참여자들에게 그들이 제공한 것과 같은 서비스 혹은 자원을 할당받을 수 있도록 보장해야 한다. 이때 중요한 점은 무임승차가 없는 환경에서 뿐만 아니라 무임승차가 이루어지고 있는 상황에서도 무임승차자들에게 제공되는 서비스를 효과적으로 차단하여 모든 참여자들에게 각각의 공헌도에 따라 차별화된 서비스를 제공할 수 있어야 한다는 것이다.

4. 견고성 (robustness)

효과적인 인센티브 메커니즘은 앞서 3장에서 소개된 전략적 우회 기법들에 대한 취약성이 제거되어야 한다. 대체로 평판 방식의 경우 신분세탁, 시빌 공격, 그리고 공모에 취약하고, 호혜주의 방식의 경우 이타주의 공략, 부정행위, 그리고 큰 시야 공략에 취약한 것으로 알려져 있다[3]. 따라서 협조적 분산시스템 환경에 적용할 효과적인 인센티브 메커니즘을 디자인할 때에는 초기 단계에서부터 이런 전략적 우회 기법들이 충분히 고려되어야 하며 시스템에 적용하기 전에 충분한 검증이 필요하다.

5. 비대칭적 이해관계 (asymmetric interest) 해소

호혜주의 방식의 경우 참여자들 간 대칭적 이해관계(symmetric interest)를 기반으로 동작하기 때문에 비대칭적 이해관계에 있는 참여자들 간에 활발한 거래를 유도하기 어렵다는 단점이 있다. 비대칭적 이해관계의 대표적인 예는 참여자 A는 참여자 B가 원하는 것을 가지고 있고, 참여자 B는 참여자 C가 원하는 것을 가지고 있으며, 참여자 C는 참여자 A가 원하는 것을 가지고 있는 경우이다. (물론 이때 B는 A가 원하는 것이 없고, C는 B가 원하는 것이 없으며, A는 C가 원하는 것이 없어야 한다.) 이런 경우 호혜주의 방식을 적용하면 참여자들 간의 어떤 조합도 대칭적 이해관계를 형성하지 않기 때문에 인센티브 메커니즘에 의한 거래가 성립하지 않는다. 비디오 스트리밍 (video streaming) 같은 어플리케이션은 비대칭적 이해관계의 극단적인 예라 할 수 있다. 이런 환경에서는 전방위 보상 (pay-it-forward)[24, 33] 개념을 활용하는 것이 바람직하다. 이때 네트워크 코딩이나 암호화 방식 등을 통해 전방위 보상이 계속 이루어질 수 있도록 강제할 수 있다면 보다 효과적이다.

V. 실험 및 분석

이번 장에서는 4장에서 도출된 인센티브 디자인 고려사항을 성능 척도로 활용하여 다양한 호혜주의 방식의 인센티브 메커니즘들에 대한 비교 실험 및 분석을 실시한다. 실험을 위해 우리는 호혜주의 방식 중에서도 가장 성공적인 협조적 분산시스템의 하나로 알려진 BitTorrent[2, 14]와 그 변종(variant)들인 PropShare[17], FairTorrent[18], 그리고 TBeT[19] 시뮬레이터를 각각의 프로토콜 명세 (protocol specification)에 따라 개발하였다.

기본적으로 BitTorrent[2, 14]의 경우 tit-for-tat (TFT) 알고리즘을 통해 공평성을 강조하고, optimistic unchoking (OU)을 통해 신규 참여자 유도 (bootstrapping)를 구현한다. TFT와 OU를 구현함에 있어 각 리처들은 선택된 5 (TFT=4, OU=1) 명의 이웃들에게 자신의 업로드 대역폭을 균등하게 할당한다.

PropShare는 OU을 구현하는 방식은 BitTorrent와 동일하지만 TFT를 구현하는 방식이 다르다. 즉, BitTorrent가 매 10초마다 자신에게 가장 많은 파일 조각을 보낸 4명의 이웃들을 선택하여 균등한 업로드 대역폭으로 보상하는데 비해 PropShare는 매 10초마다 자신에게 파일 조각을 보낸 모든 이웃들을 선택하여 그들이 보낸 파일 조각을 보낸 양에 비례하여 자신의 업로드 대역폭을 다르게 할당한다. 결론적으로 PropShare는 BitTorrent보다 엄격한 TFT를 적용하고 있다. FairTorrent는 BitTorrent나 PropShare와 전혀 다른 방식으로 TFT를 구현한다.

FairTorrent에서 각 리처는 자신의 모든 이웃들에 대해 부족분 (deficit) 수준을 측정하고 관리하는데, 각 이웃에 대한 부족분 수준은 지금까지 자신이 그 이웃에게 보냈던 파일

3) 금전교환 방식의 경우 중앙집권적 방식으로 구현되기 때문에 이런 전략적 우회 기법에 대한 취약성이 대부분 제거되지만 통화의 창출이나 관리를 위한 별도의 하부구조가 요구되므로 협조적 분산시스템 환경에 적용이 제한된다.

www.kci.go.kr

조각 개수에서 그 이웃이 자신에게 보내온 파일 조각 개수를 차감한 양이다. 따라서 부족분 수준이 (-)라는 의미는 자신이 그 이웃에게 보낸 파일 조각 수보다 그 이웃이 자신에게 보낸 파일 조각 수가 더 많다는 의미이다. 이 부족분 수준을 바탕으로 각 리처는 OU에 대한 별도의 구현 없이 하나의 파일 조각을 부족분 수준이 가장 적은 (즉 지금까지 공헌도가 가장 높은) 이웃에게 자신의 모든 업로드 대역폭을 할당하여 보낸다. 이때 각 이웃에 대한 부족분 수준은 하나의 파일 조각을 주고받을 때마다 갱신된다.

TBeT의 경우는 기본적으로 BitTorrent와 동일한 방식으로 동작하지만 시더가 각 파일 조각들을 암호화하고, 암호에 사용된 키를 다시 비밀 공유 (secret sharing) 기법을 통해 여러 키 조각들로 나눈 뒤 리처들에게 분배하는 점이 다르다. TBeT에서 각 리처는 시더에게 받은 파일 조각과 키 조각을 이웃들과 서로 교환한다. 이때, 모든 키 조각을 다운로드 한 리처들만이 암호화에 사용된 키를 복호할 수 있으므로 파일 조각들을 해독 (decrypt)할 수 있다. 하나의 키 조각은 하나의 파일 조각을 업로드 (upload)할 때에만 얻을 수 있으므로 다른 리처들에게 파일 조각을 업로드 하지 않으면 (즉 시스템에 공헌 없이는) 비록 모든 파일 조각을 다운로드 하더라도 키를 알 수 없으므로 쓸모가 없게 된다.

본 논문에서는 각 메커니즘들의 핵심적인 차이점에 대해서만 설명하였으며 세부적인 사항은 관련 논문들[2, 14, 17, 18, 19]을 참조할 수 있다.

1. 실험 환경 구성

모든 실험은 최초 리처들 없이 하나의 시더로 구성된 스웜 (swarm)에서 시작되며 이 시더는 시뮬레이션이 종료될 때까지 시스템에 남는다. 각 리처는 시스템에 참여함과 동시에 파일 조각 다운로드를 시작하고, 모든 파일 조각을 다운로드할 때까지 시스템을 떠나지 않는다. 하지만 다운로드를 완료한 이후에는 지체 없이 시스템을 떠나는 것으로 가정한다. 모든 리처들은 시뮬레이션이 시작되고 10초 이내에 시스템에 참여하는 것으로 묘사되는데, 이와 같은 형태의 참여자 폭주 (flash crowd)는 최악의 상황에서 시스템 성능을 확인하는 기준이 된다.

시더의 업로드 대역폭은 6,000 Kbps이며 리처들의 업로드 대역폭은 400 Kbps에서 1,200 Kbps 분포[16, 19]를 갖되 각 리처들의 다운로드 대역폭은 제한이 없는 것을 가정한다. 즉, 업로드 대역폭만이 성능 제한 요소 (limiting factor)로 작용한다. 스웜에서 공유되는 파일의 크기는 128MB이며 각 파일 조각의 크기는 전통 BitTorrent에서 통상 사용되는 256KB로 설정되었다. 설명과정에서 별도의 언급이 없으면 앞서 설명한 매개변수 (parameter)가 기본적으로 사용되며, 각 인센티브 메커니즘의 효과는 파일 다운로드 완료시간으로 측정된다. 모든 그래프는 서로 다른 난수 시드 (random seed)를 바탕으로 30번의 실행에 대한 평균값으로 표현된다.

2. 실험결과

본 절에서는 앞서 4장에서 도출된 인센티브 디자인 고려사항을 성능 척도로 활용하여 BitTorrent[2, 14], PropShare[17], FairTorrent[18], 그리고 TBeT[19]에 대한 성능 및 취약점을 비교·분석한다.

2.1 단순성과 확장성 (simplicity and scalability)

효과적인 분산시스템은 단순성과 확장성 (simplicity and scalability)을 보장하여야 한다. 즉, 인센티브 메커니즘의 구현이 간단하여야 하며, 시스템에 참여하는 참여자의 수에 상관없이 참여자당 서비스의 질에는 큰 차이가 없어야 한다. 특히 확장성은 참여자 수가 증가할수록 서비스의 질이 떨어지는 전통적인 클라이언트-서버 모델과 비교하여 협조적 분산시스템이 가지는 큰 장점이라 할 수 있다. 각 인센티브 메커니즘들에 대한 확장성 평가를 위해 우리는 참여자 폭주 상황을 가정한 실험을 수행하였는데, 이 실험에서는 200명에서 1,000명에 이르는 참여자가 동시에 시스템에 참여하며 무임승차자는 없는 것으로 가정하였다.

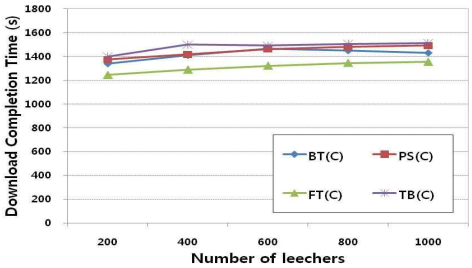


그림 1. 참여자 폭주 환경에서 무임승차가 없는 경우
Fig. 1. No free-riding under a flash crowd

그림 1에서 보듯이 무임승차가 없는 경우 BitTorrent (BT), PropShare (PS), FairTorrent (FT), 그리고 TBeT (TB) 모두 만족할 만한 시스템 확장성을 보이고 있다. 즉, 시스템에 동시에 참여하는 참여자의 수가 증가하더라도 개별적인 리처들이 경험하는 파일 다운로드 완료시간은 별 차이가 없다. 그 이유는 4가지 방식 모두 개별 참여자의 경험에 의거한 호혜주의 방식이므로 시스템이 간단하고, 각 참여자는 시스템에 참여하고 있는 총 참여자 수와 관계없이 일정한 시

www.kci.go.kr

야 크기 (즉 55)만으로도 동작하기 때문이다.

2.2 신규 참여자 유도 (newcomer bootstrapping)

그림 2 결과를 보면 FairTorrent의 경우 다른 시스템들보다 대략 5%정도 좋은 성능을 보이고 있는데, 그 이유는 BitTorrent, PropShare, 그리고 TBeT의 경우 약 20% 정도의 고정된 업로드 대역폭을 OU로 사용하고 나머지 80%를 보상을 위한 TFT로 사용하는데 반해 FairTorrent는 OU와 TFT의 별도 구분 없이 자원 전체를 유연하게 사용하기 때문이다. 즉, FairTorrent의 경우 모든 이웃들에 대한 부족분 (deficit) 수준을 관리하고 있기 때문에 신규 참여자를 포함하여 부족분 수준이 0인 이웃 (즉, 현재까지 주고받은 양이 동일한 이웃)들은 unchoking으로 선택될 확률이 동일하다. 이런 경우 참여자 폭주와 같은 환경에서는 보다 많은 시스템 자원이 신규 참여자에게 할당된다. 하지만 신규 참여자가 적은 환경에서는 공헌도가 높은 이웃을 먼저 선택하여 파일 조각을 보내므로 대부분의 자원이 TFT를 위해 할당된다. 이 결과를 바탕으로 볼 때 신규 참여자 유도를 위해 고정적인 양의 자원을 할당하는 인센티브 메커니즘보다는 상황에 맞게 유연하게 대처할 수 있는 방식이 협조적 분산시스템 환경에 보다 적합하다 하겠다.

2.3 공평성 (fairness)

앞서 4장에서 언급했듯이 대부분의 참여자들의 경우 자신이 시스템에 공헌한 만큼 시스템으로부터 서비스를 받을 수 있다면 공평하다고 느낄 것이고 보다 양질의 서비스를 받기 위해 자신의 자원을 적극적으로 공유할 것이다[18]. 각 인센티브 메커니즘이 제공하는 공평성 정도를 평가하기 위해 1,000명의 참여자가 동시에 참여하는 상황에서의 시스템 순응적인 참여자들이 경험하는 공평성 정도를 측정하였다. 이때 부정행위를 동반하는 무임승차자들의 비율은 25%로 가정하였으며, 공평성 정도는 각 참여자가 다운로드를 완료할 때까지의 평균 다운로드 속도 대비 평균 업로드 속도의 비율로 계산된다. 따라서 공평성 정도가 1이라는 의미는 각 사용자가 업로드 한 양만큼 다운로드할 수 있다는 의미이며, 1보다 큰 경우는 업로드한 양이 다운로드한 양보다 많다는 의미이다.

그림 2는 각 인센티브 메커니즘별 공평성 정도의 누적 분포 함수를 보여준다. 결과에서 보듯이 BitTorrent의 경우 공평성 정도가 1보다 작거나 (즉, 업로드한 양보다 다운로드한 양이 많은 경우) 그 반대의 경우가 다수 발생하는 것을 볼 수 있다. 이에 반해 Propshare, FairTorrent, TBeT의 경우는 보다 강력한 공평성 정도를 보이고 있는데 이는 TFT을 강화한 결과로 볼 수 있다. 이 결과를 바탕으로 보면 부정행위를 동반한 무임승차 공격이 이루어지는 경우 FairTorrent가 가장 강력한 공평성 정도를 제공하며 TBeT, PropShare가 그 뒤를 따르고 있는 것을 알 수 있다. 따라서 다른 시스템의 참여자들보다 FairTorrent 참여자들이 보다 적극적으로 자원을 공유할 것이다.

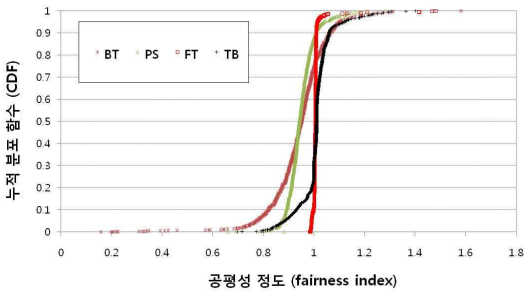


그림 2. 공평성 정도의 누적 분포 함수
Fig. 2. Cumulative Distribution Function of fairness index

2.4 견고성 (부정행위 및 큰 시야 공략)

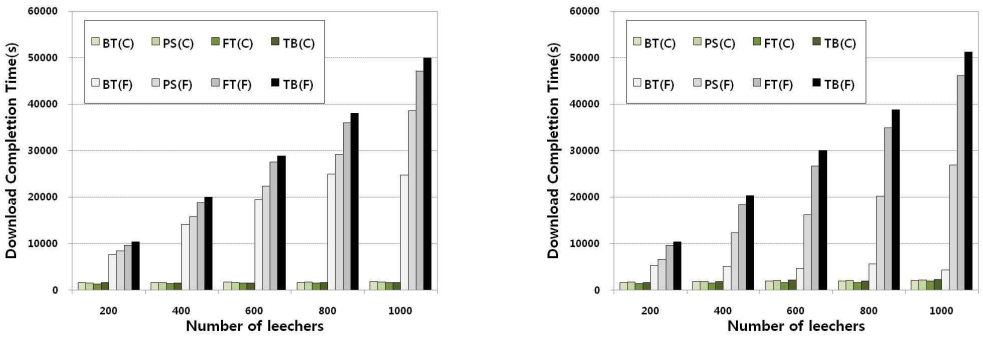
다음으로는 각 메커니즘들의 견고성 (robustness)을 측정하기 위해 기존의 인센티브 메커니즘에 대한 전략적 우회 기법 (3장) 중에 대표적인 방법인 부정행위 (cheating)와 큰 시야 공략 (large-view-exploit)의 영향에 대해 알아본다.

그림 3(a)는 무임승차자들이 파일 조각을 받은 이후 보상을 거부하는 방식의 무임승차 기법인 부정행위 (cheating)가 시스템 성능에 미치는 영향을 보여준다. 이때 전체 참여자의 25%를 무임승차자로 가정하였으며, 무임승차자의 업로드 대역폭을 0으로 설정함으로써 파일 조각을 받을 지라도 보상을 할 수 없도록 하였다. 결과에서 보듯이 무임승차자들 (Free-riders : F)의 평균 다운로드 완료시간은 시스템 순응적인 참여자들 (Compliant participants : C)의 평균 다운로드 완료시간보다 평균 15배 이상 긴 것을 알 수 있다.

이 결과에서 우리는 무임승차자들이 단지 보상을 거부하는 방식의 소극적인 전략적 우회 기법을 선택하는 경우 4가지 인센티브 메커니즘 모두 무임승차를 효과적으로 방지하고 있음을 알 수 있다. 이때 시스템에 동시에 참여하는 참여자의 수가 증가함에 따라 무임승차자들의 평균 다운로드 완료시간이 길어지고 있다. 그 이유는 시스템 순응적인 참여자들이 다운로드를 완료하고 시스템을 떠나고 난 이후에는 남은 무임승차자들은 오로지 시더로부터만 서비스를 받을 수 있기 때문이다.

그림 3(b)는 무임승차자들이 부정행위 기법에 큰 시야 공략을 추가하였을 때 시스템 순응적인 참여자들과 무임승차자들의 평균 다운로드 완료시간을 보여준다. 이때 무임승자자들은 매

www.kci.go.kr



(a) 부정행위 (cheating) (b) 큰 시야 공략 (large-view-exploit)

그림 3. 부정행위와 큰 시야 공략을 동반한 무임승차의 영향
Fig. 3. The effect of free-riding with cheating (a) and large-view-exploit (b)

10초마다 트래커에게 새로운 참여자 정보를 요구하여 받은 정보를 바탕으로 보다 많은 참여자들에게 TCP 연결을 시도한다. 또한 최대 시야 크기인 55를 넘은 이후에도 다른 참여자들로부터의 연결 요구를 거부하지 않는 방법으로 자신의 시야 크기를 최대한 키우는 것으로 가정하였다. 결과에서 보듯 큰 시야 공략을 적용하였을 때 BitTorrent와 PropShare의 경우 무임승차자들의 평균 다운로드 완료시간이 큰 폭으로 줄어들고 있음을 알 수 있다. 특히 BitTorrent의 경우에는 일부 무임승차자들이 아무런 공헌 없이도 시스템 순응적인 참여자들보다 빨리 파일 다운로드를 완료할 수 있었는데 비해 FairTorrent와 TBeT은 큰 시야 공략의 영향이 적었다. 그 이유는 FairTorrent의 경우 보상 없이 받을 수 있는 무료 파일 조각이 이웃 당 하나로 한정되기 때문[4]에 큰 시야 공략으로부터 얻을 수 있는 이득이 적고, TBeT의 경우에는 보상 없이는 키 조각을 받을 수 없으므로 시야 크기가 전체 다운로드 완료시간에 영향을 미치지 않기 때문이다. FairTorrent나 TBeT과는 달리 BitTorrent와 PropShare의 경우에는 파일 조각단위가 아닌 시간단위 (10초)로 unchoking을 하기 때문에 무임승차자가 큰 시야 공략을 통해 받을 수 있는 무료 파일 조각의 수가 상대적으로 많다. 이런 결과를 놓고 볼 때 보상의 단위가 시간이 아닌 일의 단위 (예 파일조각)일 때 무임승차를 보다 효과적으로 제한할 수 있음을 알 수 있다.

2.5 견고성 (신분세탁 및 시빌 공격)

2.4절의 결과를 바탕으로 보면 다양한 전략적 우회 기법으로 무장한 무임승차들을 가장 효과적으로 배제하는 방법은 TBeT임을 알 수 있다. TBeT은 파일 조각에 대한 암호화를 통해 암호화된 파일 조각을 받는 것이 바로 이득 (gain)이 될 수 없도록 하고, 파일 조각을 업로드할 때만 (즉 시스템에 대한 공헌이 있을 때만) 키 조각을 받을 수 있도록 함으로써 리처들로 하여금 시스템에 대한 공헌을 강제하고 있다. 하지만 TBeT의 경우 무임승차가 없는 경우 FairTorrent에 비해 성능이 낮은데, 이는 시간을 정해서 (즉 10초 단위로) 한 번에 여러 이웃들에게 파일 조각을 보내는 BitTorrent 방식의 unchoking이 갖는 고유 문제이다. 반면 한 번에 하나의 파일 조각만을 가장 공헌도가 높은 이웃에게 보내는 FairTorrent는 무임승차도 효과적으로 제한할 뿐만 아니라 무임승차가 없는 경우에 있어서도 가장 좋은 시스템 성능을 보장하고 있음을 알 수 있다. 그러나 FairTorrent의 경우 파일 조각에 대한 암호화가 없기 때문에 근본적으로 무임승차를 완전히 배제할 수 없다. 즉, 암호화가 없는 경우 다른 참여자들로부터 무료로 받을 수 있는 파일 조각이 존재하고, 무임승차자들은 신분세탁이나 시빌 공격을 통해 그 기회를 극대화시킬 수 있기 때문이다.

신분세탁이나 시빌 공격이 FairTorrent의 성능에 미치는 영향을 알아보기 위해 우리는 FairTorrent 내의 무임승차자들이 이웃들로부터 하나의 무료 파일 조각을 받으면 그 이웃과의 연결을 해제하고 다른 ID로 재 연결을 시도하는 방식으로 신분세탁이 가능하도록 설정하였다. 무임승차자가 한 파일 조각을 받으면 파일 조각을 보낸 이웃 입장에서 그 무임승차자의 부족분 수준이 +1이 되어 또 다른 파일 조각을 보낼 확률이 거의 없어진다. 하지만 기존의 연결을 해제하고 다른 아이디로 재접속하면 부족분 수준이 다시 0이 되므로 다른 파일 조각을 받을 확률이 다른 신규 참여자와 동일하게 된다. 따라서 무임승차자들은 신분세탁을 통해 (적절한 보상을 제공하지 않으면서도) 같은 참여자들로부터 계속해서 파일 조각을 받을 수 있게 되는 것이다[5].

4) FairTorrent에서는 무임승차자가 파일 조각을 하나 받고나면 부족분 수준이 (+)가 되므로 다른 모든 이웃들의 부족분 수준이 (+)가 되기 전에는 다시 unchoking되기 어렵다.

www.kci.go.kr

고려사항		BitTorrent	PropShare	FairTorrent	TBeT
단순성과 확장성		●	●	●	●
공평성		×	△	●	△
신규 참여자 유도		△	△	●	△
견고성	이타주의 공략	×	×	×	×
	부정행위	×	△	△	●
	큰 시야 공략	×	△	●	●
	신분세탁 (시빌 공격)	△	●	×	●
	공모	●	●	●	●
비대칭적 이해관계 해소		△	△	△	△

표 1. 인센티브 디자인 고려사항을 통한 취약점 분석 (● : 양호, △ : 보통, × : 미흡)

그림 4는 FairTorrent와 TBeT 시스템 안에서 무임승차자들이 신분세탁을 실시하는 경우 시스템 순응적인 참여자들과 무임승차자들의 평균 파일 다운로드 완료시간을 보여준다. 결과에서 보듯이 FairTorrent 내의 무임승차자들은 신분세탁을 통해 시스템 순응적인 참여자들보다 오히려 좋은 서비스를 받을 수 있음을 보인다. 하지만 TBeT 안에서는 무임승차자들이 시스템에 공헌 없이는 키 조각을 받을 수 없기 때문에 신분세탁이나 시빌 공격을 통해 다운로드 완료 시간을 단축시킬 수 없다. 본 실험을 통해 파일 조각에 대한 암호화가 무임승차에 대한 강력한 방어 수단임을 확인할 수 있다.

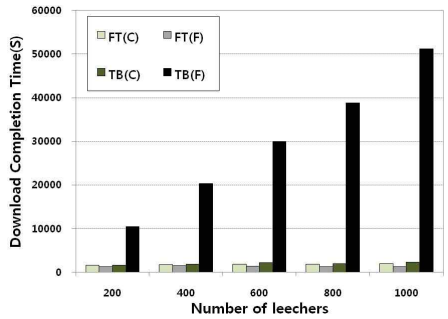


그림 4. FairTorrent에서 신분세탁의 영향
Fig. 4. The effects of whitewashing under FairTorrent

2.6 견고성 (이타주의 공략)

지금까지 살펴본 부정행위, 큰 시야 공략, 그리고 신분세탁이나 시빌 공격에 대한 견고성 이외에도 인센티브 메커니즘을 디자인함에 있어서 간과할 수 없는 부분이 있다. 바로 시더처럼 아무런 보상을 기대하지 않고 시스템을 위해 봉사하는 참여자들이 제공하는 자원에 대한 무임승차, 즉 이타주의 공략이다. 앞서 알아본 BitTorrent, PropShare, FairTorrent, 그리고 TBeT 모두 리처들간의 무임승차에 대한 고려만 하고 있을 뿐 시더에 대한 무임승차는 고려하고 있지 않다. 그 이면에는 시더가 제공하는 서비스는 모든 리처들에게 공평하게 분배된다는 가정이 있다. 하지만 앞의 결과에서 보듯이 무임승차자들이 큰 시야 공략, 신분세탁, 혹은 시빌 공격을 동반하는 경우 시더가 제공하는 서비스에 대한 공평 분배는 깨어질 수밖에 없다. 따라서 효과적인 인센티브 메커니즘을 위해서는 수퍼시딩 (super-seeding)[6]이나 전방위 보상기법과 같은 추가적인 안전장치를 통해 이타주의 공략을 방어할 수 있는 방안이 필수적이라 하겠다.

3. 성능 척도로의 활용

본 절에서는 4장에서 제시되었던 인센티브 디자인 고려사항을 성능 매트릭스로 활용하여 각 메커니즘들의 취약점을 판단한다. 본 논문에서 제시하는 성능 척도를 활용한 취약점 분석은 향후 관련 연구자들이 협조적 분산시스템 환경을 위한 새로운 인센티브 메커니즘을 개발할 때 가이드라인으로 활용할 수 있다.

표 1은 4장에서 도출된 인센티브 디자인 고려사항을 성능 척도로 활용하여 각 인센티브 메커니즘들의 취약점을 분석한 결과이다. 위 결과에서 보듯이 BitTorrent, PropShare, FairTorrent, 그리고 TBeT은 공통적으로 단순성과 확장성 및 공모에 대한 견고성에서 뛰어난 성능을 보이고 있다. 이는 4가지 인센티브 메커니즘들 모두 TFT를 기반으로 한 호혜주의 방식을 채택하고 있기 때문에 얻을 수 있는 장점[7]이다. 비대칭적 이해관계 해소 측면에서도 4가지 메커니즘 모두 부분적인 성공을 거두고 있는 것으로 판단할 수 있다. 하지만 이

5) 시빌 공격도 신분세탁과 동일한 맥락에서 이루어질 수 있으므로 본 논문에서 별도의 분석은 생략한다.

6) http://en.wikipedia.org/wiki/Super-seeding

7) 즉, 개인적인 경험에만 의존해서 의사결정을 할 수 있기 때문에 메커니즘이 단순하고, 무임승차자들이 공모를 통해 얻을 수 있는 장점이 없어진다.

www.kci.go.kr

타주의 공략 부분에서는 4가지 메커니즘 모두 취약성을 보이고 있으므로 이에 대한 보완이 필요하다 하겠다.

파일 다운로드 완료시간 측면에서 보면 FairTorrent가 다른 시스템들에 비해 대부분의 경우에서 우수한 성능을 보였지만 신분세탁이나 시빌 공격에 대한 취약한 단점이 있었다. TBeT의 경우는 FairTorrent보다 약간 성능이 떨어지지만 파일 조각에 대한 암호화를 통해 대부분의 전략적 우회 기법들에 대한 견고성을 제공하고 있다. 따라서 두 메커니즘의 장점을 아우를 수 있는 형태의 새로운 형태의 인센티브 메커니즘을 고려할 수 있을 것이다.

Ⅵ. 결론 및 향후 연구방향

본 논문은 협조적 분산시스템 환경을 위한 인센티브 메커니즘을 디자인 할 때 반드시 염두에 두어야 하는 고려사항들을 도출하고, 도출된 고려사항을 인센티브 메커니즘에 대한 성능 평가의 척도로 활용하는 방안을 제시하였다. 인센티브 메커니즘을 위한 고려사항 도출을 위해 우리는 기존의 인센티브 메커니즘들을 금전교환, 평판, 그리고 호혜주의 방식으로 범주화하여 자세히 조사하였으며, 기존의 인센티브 메커니즘을 우회하기 위해 개발된 전략적 우회 기법들을 조사하고 분석하였다. 또한 이런 일련의 과정을 통해 도출된 고려사항들을 활용하여 가장 성공적인 협조적 분산시스템의 하나로 알려진 BitTorrent 및 그 변종들 (PropShare, FairTorrent, 그리고 TBeT)에 대한 성능평가 및 취약점 분석을 실시함으로써 인센티브 메커니즘에 대한 성능 매트릭스로의 활용 가능성을 점검했다. 본 논문에서 도출한 인센티브 디자인 고려사항들은 향후 관련 연구자들이 협조적 분산시스템 환경을 위한 인센티브 메커니즘을 개발할 때 가이드라인으로 활용할 수 있다. 향후 우리는 본 연구결과로 도출된 인센티브 디자인 고려사항을 바탕으로 협조적 분산시스템에 활용할 수 있는 인센티브 메커니즘을 개발할 것이다.

참고문헌

[1] The bittorrent protocol specification, http://www.bittorrent.org/beps/bep_0003.html, Feburary, 2008.

[2] B. Cohen, "Incentives build robustness in bittorrent", P2PECON'03, 2003.

[3] P. Maymounkov and D. MaziIres, "Kademlia: A peer-to-peer information system based on the xor metric", IPTPS'02, 2002.

[4] Gnutella, http://www.gnutellaforums.com/

[5] Ipoque, "ipoque internet study 2008/2009 finds web and streaming outgrows p2p trac", URL http://www.ipoque.com/userfiles/file/ipoque-Internet-Study-08-09.pdf, 2009

[6] G. Hardin, "Tragedy of the commons", Science 162.

[7] D. Hughes, G. Coulson and J. Walkerdine, "Free riding on gnutella revisited: The bell tolls?", IEEE Distributed Systems Online, 2005.

[8] S. B. Handurukande, A.-M. Kermarrec, F. L. Fessa nt, L. Massoulié and S. Patarin, "Peer sharing beh aviour in the edonkey network, and implications for the design of server-less file sharing systems", Eur oSys conference, 2006.

[9] V. Vishnumurthy, S. Chandrakumar and E. G. Sirer, "Karma: A secure economic framework for peer-to-peer resource sharing", P2PECON'03, 2003.

[10] M. Sirivianos, J. H. Park, X. Yang and S. Jarecski, "Dandelion: Cooperative content distribution with robust incentives", USENIX'07, 2007.

[11] S. D. Kamvar, M. T. Schlosser and H. Garcia-m olina, "The eigentrust algorithm for reputation management in p2p networks", WWW'03, 2003.

[12] M. Piatek, T. Isdal, A. Krishnamurthy and T. Ande rson, "One hop reputations for peer to peer file shari ng workloads", NSDI'08, 2008.

[13] E. Zhai, R. Chen, Z. Cai, L. Zhang, E. K. Lua, H. Sun, S. Qing, L. Tang and Z. Chen, "Sorcery: Could we make p2p content sharing systems robust to deceivers?", P2P'09, 2009.

[14] K. Tamilmani, V. Pai and A. Mohr, "Swift: A syst em with incentives for trading", P2PECON'04, 2004.

[15] M. Feldman, K. Lai, I. Stoica and J. Chuang, "Rob ust incentive techniques for peer-to-peer networks", EC'04, 2004.

[16] M. Piatek, T. Isdal, T. Anderson, A. Krishnamurthy and A. Venkataramani, "Do incentives build robu stness in bittorrent?", USENIX NSDI'07, 2007.

[17] D. Levin, K. LaCurts, N. Spring and B. Bhatta charjee, "Bittorrent is an auction: Analyzing and improving bittorrent''s incentives", SIGCOMM'08, 2008.

[18] A. Sherman, J. Nieh and C. Stein, "Fairtorrent : Bringing fairness to peer-topeer systems", ACM CoNEXT'09, Rome, Italy, 2009.

[19] K. Shin, D. S. Reeves and I. Rhee, "Treat-before-tr ick : Free-riding prevention for bittorrent-like peer-to-peer networks", IPDPS'09, 2009.

[20] M. Zghaibeh and F. C. Harmantzis, "Revisiting free riding and the tit-for-tat in bittorrent: A

www.kci.go.kr

measurement study", Peer-to-Peer Networking and Applications, Vol. 1, No. 2, pp. 162--173, 2008.
[21] H. Wang, J. Liu and K. Xu, "On the locality of bittorrent-based video swarming", 8th International workshop on Peer-To-Peer Systems, 2009.
[22] M. Iza, G. Urvoy-Keller, E. W. Biersack, P. Felber, A. A. Hamra and L. GarcÞ-Erice, "Dissecting BitTorrent: Five Months in a Torrent''s Lifetime", Lecture Notes in Computer Science, Vol. 3015/2004, 2004.
[23] S. Jun and M. Ahamad, "Incentives in bittorrent induce free riding", P2PECON'05, Philadelphia, PA, 2005.
[24] L. Jian and J. K. MacKie-Mason, "Why share in peer-to-peer networks?", International Conference on Electronic Commerce, 2008.
[25] M. Sirivianos, J. H. Park, R. Chen and X. Yang, "Free-riding in bittorrent networks with the large view exploit", IPTPS'07, 2007.
[26] T. Locher, P. Moor, S. Schmid and R. Wattenhofer, "Free riding in bittorrent is 12 cheap", HotNets'06, 2006.
[27] J. R. Douceur, "The sybil attack", IPTPS'02, 2002.
[28] R. Landa, D. Grin and R. G. Clegg, E. Mykoniati, M. Rio, "A sybilproof indirect reciprocity mecha nism for peer-to-peer networks", INFOCOM'09, 2009.
[29] M. Feldman and J. Chuang, "Overcoming free-riding behavior in peer-to-peer systems", ACM Sigecom Exchanges, Vol. 5, 2005.
[30] A. R. Bharambe, C. Herley and V. N. Padmanabhan, "Analyzing and improving a bittorrent network''s performance mechanisms", INFOCOM'06, 2006.
[31] B. Fan, D. ming Chiu and J. Lui, "The delicate tradeoffs in bittorrent-like file sharing protocol design", ICNP'06, 2006.
[32] T. Locher, S. Schmid and R. Wattenhofer, "Rescuing tit-for-tat with source coding", IEEE P2P'07, 2007.
[33] J. J. D. Mol, J. A. Pouwelse, M. Meulpolder, D. H. J. Epema and H. J. Sips, "Give-to-get: free-riding resilient video-on-demand in p2p systems", SPIE Conference Series, 2008.

저 자 소 개

신 규 용

1996년 3월 육군사관학교 전산학 학사.
2000년 2월 한국과학기술원 전산학 석사 (ATM 네트워크).
2009년 12월 노스캐롤라이나 주립대학 전산학 박사 (분산 시스템 보안).
현재 : 육군사관학교 전자정보학과 정보과학 조교수
관심분야 : 컴퓨터 네트워크, 분산 시스템, 인센티브, 네트워크 보안
Email : yessss@gmail.com

유 진 철

1989년 3월 육군사관학교 전산학 학사.
1993년 7월 아이오와 주립대 통계학 석사 (게임이론).
2003년 5월 펜실베니아주립대 컴퓨터공학박사 (고성능/저전력 시스템)
현재 : 육군사관학교 전자정보학과 정보과학 부교수
관심분야 : 고성능 컴퓨팅, 저전력 시스템, 정보 보안
Email : jyoo@kma.ac.kr

이 종 덕

2005년 3월 육군사관학교 전산학 학사.
2009년 5월 버지니아 주립대 컴퓨터과학 석사 (무선 센서 네트워크 전공).
현재 : 육군사관학교 전자정보학과 강사
관심분야 : 무선 센서 네트워크, 보안
Email : jdlee@kma.ac.kr

박 병 철

2001년 3월 육군사관학교 전자공학 학사.
2009년 5월 연세대학교 산업공학 석사 (시뮬레이션 전공).
현재 : 육군사관학교 전자정보학과 강사
관심분야 : Modeling & Simulation
Email : parkbc6457@gmail.com

www.kci.go.kr