P2P 오버레이 네트워크에서의 능동적 공격에 대한 방어

정회원 박 준 철*

Defending Against Some Active Attacks in P2P Overlay Networks

Jun-Cheol Park* ***Regular Member***

요 약

피어-투-피어(P2P) 네트워크는 개방적, 평면적, 자율적 특성으로 인하여 참여 피어들의 악의적인 공격에 근원적으로 취약하다. 본 논문에서는 부트스트래핑(bootstrapping) 단계 및 온라인 단계에서의 악의적 피어들의 공격을 효율적으로 방어하는 문제를 다룬다. 본 논문은 부트스트래핑 단계에서 네트워크의 신뢰성 있는 노드를 이용하여 새로 가입하는 피어에게 ID 관련 정보를 안전하게 부여하는 멤버쉽 처리 프로토콜을 제시한다. 이 신뢰성 있는 노드들은 새로운 피어들이 네트워크에 참여할 때만 사용되고, 그 이외의 P2P 동작에는 관여하지 않는다. 온라인 단계에서의 공격에 대하여 본 논문에서는 P2P 오버레이를 통해 전송되는 메시지의 구조를 제안하여, 메시지 변경, 재생 공격 및 잘못된 정보를 가지는 메시지 공격들의 검출이 용이해지도록 한다. 제안한 기법들은 함께 적용되어 악의적 피어들의 속임수를 억제함으로써 피어들로 하여금 네트워크의 프로토콜을 준수하게 만든다. 제안 기법들은 기본적 P2P 오버레이 모델을 가정하여 비구조적 및 구조적의 다수 P2P 네트워크들에 적용될 수 있다.

Key Words : P2P Overlay Network, Malicious Peer, Defense, Cryptographic Means, Bootstrapping

ABSTRACT

A peer-to-peer(P2P) network is inherently vulnerable to malicious attacks from participating peers because of its open, flat, and autonomous nature. This paper addresses the problem of effectively defending from active attacks of malicious peers at bootstrapping phase and at online phase, respectively. We propose a secure membership handling protocol to protect the assignment of ID related things to a newly joining peer with the aid of a trusted entity in the network. The trusted entities are only consulted when new peers are joining and are otherwise uninvolved in the actions of the P2P networks. For the attacks in online phase, we present a novel message structure applied to each message transmitted on the P2P overlay. It facilitates the detection of message alteration, replay attack, and a message with wrong information. Taken together, the proposed techniques deter malicious peers from cheating and encourage good peers to obey the protocol of the network. The techniques assume a basic P2P overlay network model, which is generic enough to encompass a large class of well-known P2P networks, either unstructured or not.

Ⅰ. 서 론

P2P[1,2,10] 네트워크에서의 보안은 매우 어려운 과제이다. P2P 네트워크는 개방적, 평면적, 자율적 특성으로 인해 이기적이나 악의적인 행위에 대한 책임 소재를 규명하는 부분에 있어 취약점을 드러낸다[3-5, 10-13]. 네트워크에 참여하는 모든 피어가 항상 신뢰성 있게 네트워크 프로토콜을 수행한다고 보장

※ 이 논문은 2004년도 홍익대학교 교내연구비에 의하여 지원되었음.
* 홍익대학교 컴퓨터공학과 컴퓨터네트워킹연구실(jcpark@cs.hongik.ac.kr)
논문번호 : KICS2006-02-063, 접수일자 : 2006년 2월 6일, 최종논문접수일자 : 2006년 3월 13일

하는 것은 불가능하다. P2P 네트워크는 따라서 악의적 의도를 가진 한 피어 또는 피어 그룹의 능동적 공격 가능성에 대해 대비가 되어 있어야 한다. P2P 오버레이 네트워크에서 가능한 능동적 공격으로는 메시지 훼손/재생/폐기, ID 위조/변조, 쿼리에 대해 거짓 응답, 다른 이름으로 위장한 바이러스 파일을 제공하는 것 등을 들 수 있다.

본 논문은 적절한 암호화 기법을 통해 효율적으로 방어할 수 있는 몇 가지 능동적 공격에 대해 다룬다. 우선 공격을 두 가지 유형으로 구분하는데, 첫 번째가 부트스트래핑(bootstrapping) 과정에서의 공격이고, 두 번째가 온라인 단계, 즉, 피어들이 상호 통신하는 단계에서의 공격이다. 제안하는 방어 기법들은 공개 키 기반 인프라에서와 같이 CA (Certificate Authority)라 부르는 믿을 수 있는 노드들의 집합을 가정한다. 이러한 CA들은 피어의 네트워크 가입 시에만 필요하며 따라서 P2P 오버레이의 확장성이나 신뢰성에는 영향을 미치지 않는다. 본 논문은 신규 피어와 CA 사이에 안전한 멤버쉽 처리 프로토콜을 제안하여 피어의 ID 부여 과정을 여러 공격들로부터 보호한다. 온라인 상태에서의 공격들에 대해서는 피어들 간 교환되는 메시지들을 위한 메시지 구조를 제안하여 메시지 변경, 재생 공격, 오류 정보를 포함하는 메시지 생성 공격으로부터의 효율적인 방어가 가능함을 보인다. 제안 기법들은 피어 멤버쉽, 연결, 개체 탐색 등을 관할하는 하위 구조로부터 독립적이기 때문에 비구조적 및 구조적 P2P 네트워크에 모두 적용될 수 있다.

본 논문의 구성은 다음과 같다. 다음 장에서는 관련 연구들이 소개되고, 3장에서는 제안 기법들이 적용될 P2P 오버레이 네트워크 모델을 제시한다. 4장에서는 피어 멤버쉽을 다룰 보안 프로토콜과 이를 통해 부트스트랩 과정에서 어떻게 여러 능동적 공격에 대한 방어가 이루어지는지 다룬다. 5장에서는 네트워크 상의 메시지 구조를 제안하고 여러 공격 유형 및 그 방어 기법들을 제시한다. 6장에서는 본 논문의 결론 및 추후 연구 방향에 대해 언급한다.

Ⅱ. 관련 연구

Sybil 공격[6]은 다수의 서로 다른 ID가 동일 사용자에게 배정됨으로써 각 피어는 고유한 ID를 사용해야 한다는 기본 가정에 기반을 두고 있는 네트워크에 위협을 끼치는 공격 유형을 말한다. 예를 들면, [8]에서 제기된 바와 같이, 다수의 ID를 가진 한 피어가 이들 ID 중 일부를 사용하여 자신의 나머지 ID들을 추천함으로써 아무런 일을 하지 않은 ID 들의 평판(reputation)을 향상시킬 수 있다. 결국 P2P 네트워크에서의 평판 시스템[9,11,12]의 유용성은 이런 공격에 의해 훼손 가능하다. [6]의 연구에 따르면 중앙의 인증 관련 기관이 부재한 상황에서는 어떤 P2P 네트워크라도 이런 공격에 취약하다. [8]에서는 믿을 수 있는 중앙 기관의 필요성을 없애는 자율-인증(self-certification)의 개념을 도입하여 각 피어가 스스로 CA를 운용하여 원하는 만큼의 ID를 만들어 낼 수 있도록 했다. 이 때 다수 ID를 남용할 가능성은 ID 분배와 IP 주소를 연계시키고 악의적 피어가 연속적이지 않은 다수의 IP 주소들을 보유하기가 어려울 것이라는 가정을 통해 완화하려고 했다. 다수 ID 남용 문제의 또 다른 해결책 중 하나는 ID를 사용하는 사용자가 ID 당 일정 금액을 지불하게 함으로써 다수 ID를 배정받는 과정이 부담스럽도록 만드는 것이다. [5]에서는 본 논문과 마찬가지로 믿을 수 있는 노드(CA)들의 존재를 가정하고 ID 분배 문제를 다루었지만 문제 영역이 구조적 P2P 네트워크에서의 보안 라우팅과 포워딩 이라는 점에서 본 논문과 다르다. 본 논문은 부트스트래핑 과정을 위해 가입 피어에게 안전하게 ID 및 관련 정보들을 제공하는 직접적 방법을 제시하였다는 점에서 타 연구들과 차별된다.

다수의 암호화 알고리즘과 프로토콜들이 P2P 네트워크에서 데이터를 안전하게 저장하는 목적으로 개발되었다. 자율-인증(self-certifying) 데이터[5]는 이 데이터를 추출하는 피어에 의해 무결성이 검증될 수 있는 데이터이다. [7] 및 [14]에서는 부분적 정보(파일의 블록 및 키의 부분)를 이용하여 전체 정보를 복원해 내는 암호화 이론을 다루고 있다. 이러한 결과들과 달리 본 논문은 P2P 네트워크 응용에서 필수적인 기본 메시지(요청 및 응답) 전달 과정에서의 보안에 관심을 두고, 기존 연구 결과들이 다루지 못한 문제 영역에 새로운 접근 방법을 제시하였다.

Ⅲ. P2P 오버레이 네트워크 모델

본 장에서는 제안 기법들이 적용될 P2P 오버레이 네트워크 모델을 소개한다. 이 모델은 매우 포괄적이어서 현재까지 알려진 많은 P2P 네트워크들이 이를 따르고 있다. 본 모델은 P2P 오버레이에서 피어의 활동을 부트스트래핑 단계와 온라인 단계로 구분한다. 부트스트래핑 단계는 신규 피어의 네트워

크 멤버 가입과 다른 피어들과의 연결 설정을 통해 P2P 오버레이 토폴로지를 생성하는 과정을 포함한다. 이 과정에서 본 논문은 다수의 믿을 수 있는 노드 - 공개 키 기반 인프라에서와 같이 CA라 부름 - 들의 존재를 가정한다. 어떤 피어가 네트워크에 가입하고자 할 때 이 피어는 먼저 사용하는 IP 주소를 포함하는 임의의 IP 주소 공간을 관할하는 CA에 접근한다. 제안 모델은 오버레이의 각 사용자가 항상 동일한 호스트, 즉 동일한 IP 주소를 사용한다고 가정한다. 따라서 어떤 사용자가 네트워크 접속 지점을 바꾸게 되면, 이 사용자는 새로운 IP 주소를 포함하는 공간을 관할하는 CA로부터 새로운 정보(ID, 키의 쌍, 인증서)를 부여받아야 한다. 가입이 허락되면 새로운 피어는 네트워크의 일원이 되면서 ID 및 관련 정보들을 소유하게 된다. 이 피어는 이어서 네트워크에 연결되기 위한 일을 수행한다. 실제 연결 방법은 오버레이 토폴로지의 구성(비구조적 또는 구조적)과 특정 P2P 네트워크 응용에 따라 달라지며, 본 모델에서는 어떤 가정도 하지 않는다.

어떤 피어가 네트워크를 떠나게 되면 네트워크 상의 다른 피어들이 연결도가 떨어지거나 심한 경우 완전히 나머지 네트워크 피어들과 분리되는 경우가 발생할 수 있다. 이러한 피어들은 계속 온라인 상태에 있는 경우 추가로 새로운 피어들을 선택해 연결되기를 시도할 수 있다. 각 P2P 오버레이 네트워크는 자신의 토폴로지를 이러한 상황에서 즉석으로 변형하는 프로토콜을 가지고 있다. 본 모델은 이 부분에서도 어떤 특정 프로토콜을 가정하지 않는다.

온라인 단계에서 각 피어는 오버레이 상에서 동작하는 응용 프로토콜에 규정된 작업을 수행한다. 본 모델은 요청(request)과 응답(response)의 두 가지 메시지 유형을 가정한다. 예를 들어, 파일 검색을 위해 각 피어는 쿼리(요청)를 발생시키고 쿼리힛(응답)을 기다리게 된다. 쿼리와 쿼리힛 같은 메시지들은 오버레이 상의 피어들을 통해서만 오버레이 네트워크에서 이동한다. 트랜잭션의 마지막 단계(예: 파일 공유에서 파일을 다운로드)에서만 피어는 목적지 피어로의 직접 네트워크 연결을 시도한다.

Ⅳ. 피어의 부트스트래핑 과정 보안

본 장에서는 피어와 CA 간의 보안 프로토콜을 제시하며, 이를 통해 어떻게 멤버쉽 과정에서의 대표적 능동적 공격들이 방어되는지 보인다. 본 논문에서 $K\{message\}$ 표현은 $message$에 키 K로 비밀키 암호화를 적용한 것을, $\{message\}_{Alice}$ 표현은 $message$에 Alice의 공개 키로 공개 키 암호화를 적용한 것을 각각 의미한다.

4.1 보안 피어 멤버쉽 처리 프로토콜

부트스트래핑 과정에서 신규 가입을 원하는 피어는 하나의 키 쌍(공개/개인)과 인증서를 부여받는다. 프로토콜 설명을 위해 사용자 Alice가 IP 주소 IP_{Alice}를 가지는 호스트에서 어떤 P2P 오버레이 네트워크에 가입하고자 한다고 하자. 또한 Alice는 이메일 주소 $email_{Alice}$를 소유하고 있다고 하자. 어떤 사용자든 자신의 IP 주소를 관할하는 CA의 기본 정보(IP 주소 및 포트 번호, 공개 키)를 알고 있으며, 이 정보는 널리 알려져 있어 가짜 정보로 바뀔 가능성은 없다고 가정한다. 이 프로토콜은 CA 자체의 신뢰성을 가정하고 있어서 CA가 거짓 정보를 제공하거나 타인에게 비밀을 누설하는 경우 보안성 제공이 불가능해진다. 하지만 현재 인터넷에서 운용되는 전문 CA(예: VeriSign)의 신뢰성이 매우 높다는 점을 감안한다면 이 신뢰성 가정은 무리한 것이 아니라고 판단한다.

R_1, R_2, R_3는 Alice에 의해 랜덤하게 선택된 한 번만 사용될 키들이고, C는 CA에 의해 선택된 역시 한 번만 사용될 문자열이다. 사용자 Alice에게 부여될 인증서에는 사용자 이름, 이 피어가 수행될 호스트의 IP 주소, 공개 키와 그 유효 기간이 포함되고 이 모든 것이 해쉬 함수에 의해 계산된 결과가 인증서에 그 이름이 명시된 CA의 개인 키에 의해 서명된다. 사용자 Alice의 ID는 hash($public\ key_{Alice}|IP_{Alice}$)이 된다. 이렇게 IP 주소를 ID 계산에 포함시킴으로써 공격자는 부여받은 ID를 장소를 옮겨서 다른 IP 주소를 가지는 호스트에서 사용하는 것이 불가능해진다. 물론 선의의 사용자라 하더라도 동적 IP 할당 (DHCP 등)나 호스트 이동성 때문에 IP 주소가 변경되는 경우 자신에게 부여된 ID 및 인증서가 효력을 잃는다는 점은 감수해야 한다. 어떤 피어의 인증서는 추후 타 피어들에게 공개되겠지만, 인증서에 공개 키가 포함되어 있기 때문에 그 키와 쌍이 되는 개인 키가 인증서와 함께 전달될 때 인증서를 평문으로 전달하는 것은 위험하다. 공격자에게 인증서와 암호화된 개인 키가 노출되는 위험을 방지하기 위해 이 프로토콜에서는 암호화된 개인 키와 인증서를 다시 다른 키로 암호화하는 방법을 택하고 있다(메시지 5). 또한 이 메시지 5를 통해 CA는 피어에게 다른 유용한 정보를 안전하게 전달할 수 있

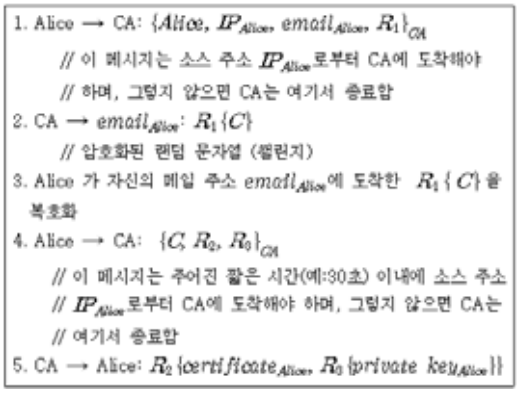

그림 1. 보안 피어 멤버쉽 처리 프로토콜

는데, 그러한 정보로는 네트워크 상의 다른 CA들의 이름과 공개 키의 쌍을 들 수 있다.

4.2 공격과 방어

악의적인 여러 공격에 대해 각각의 방어가 프로토콜을 통해 어떻게 실현되었는지 살펴본다.

4.2.1 복수 ID들의 남용

많은 ID를 가진 사용자가 이 ID들을 부정하게 사용하면서 이들이 모두 한 사용자에게 속해 있다는 사실을 감추기 원한다고 하자. 이런 남용 가능성을 완벽하게 막는 것은 믿을 수 있는 어떤 노드가 있어 이 노드가 피어 ID를 부여하기 전에 해당 사용자의 실생활에서 쓰이는 ID(예: 운전면허, 여권)를 검사하는 것이 강제되기 전에는 불가능하다. 제안한 프로토콜은 피어 ID를 이메일 주소와 IP 주소의 쌍과 연계시킴으로써 이러한 남용의 가능성을 줄인다. 프로토콜에 의하면 사용자는 ID 등을 부여받기 위해 적법한 IP 주소의 위치에서 즉시 사용 가능한 이메일 주소를 가지고 있어야 하며, 이 과정은 종단 간 암호화를 거쳐(사용자 측은 CA의 공개 키를 이용한 암호화, CA 측은 사용자가 선택한 키 값을 이용한 비밀 키 암호화) 이루어지기 때문에 중간 과정에서 도청이나 중간자 공격(man-in-the-middle)이 매우 어렵다. 또한 CA는 ID 관련 요청이 들어온 IP 주소를 기억하고 있어서 동일 주소로부터 다른 요청이 들어올 경우 이를 거부하게 된다. 악의적 피어는 실제 존재하는 IP 주소와 임의의 공개 키(피어 자신이 임의로 생성하였거나 또는 자신을 지나는 메시지로부터 취한 것)를 이용하여 CA가 부여하지 않은 가짜 ID를 만들 수 있다. 그러나 모든 메시지가 그 소스 ID와 ID의 인증서를 포함하도록 한다면, 가짜 ID의 경우 인증서의 서명한 내용으로부터 만드는 ID와 일치하지 않을 것이다. 인증서를 동시에 바꿔치기하는 경우에는 검증하는 피어가 CA의 공개 키를 잘 알고 있다는 가정 하에 역시 인증서 위조의 발각이 가능하다. 물론 어떤 사용자가 다수의 (IP 주소, 이메일 주소) 쌍을 소유하고 있다면, 그만큼에 해당하는 ID를 가질 수 있다. 이메일 주소의 경우 CA들 간에 서로 자료 공유를 하지 않는다면 이미 사용한 것을 다른 CA에게 ID를 부여받을 때 제시하는 것도 가능하다. 이메일 제시를 요구하는 것은 대부분의 이메일 계정의 경우 부여를 위해 소정의 본인 확인 절차를 거쳤을 것으로 판단하여, ID 중복 부여를 완전히 제거하지는 못하더라도 어렵게 하는데 목적이 있다. 사용하는 인증 방식의 강도는 P2P 오버레이 네트워크의 특정 응용에 따라 결정할 수 있다.

4.2.2 메시지의 도청 및 악의적 변경

공격자는 CA와 가입자(또는 이메일 주소) 사이에 교환되는 어떤 메시지도 가로챌 가능성이 있다. 하지만 공격자는 CA의 개인 키나 랜덤하게 선택된 키 들을 알지 못하는 한 어떤 메시지든 그 암호화되기 이전의 내용을 알아내기 매우 힘들다. 그리고 각 메시지는 양 종단에서 선택된 키로 암호화되기 때문에 공격자가 수신자에 적법한 메시지인 것처럼 보이는 메시지를 조작해내는 것이 불가능하다. 결국 공격자는 양 종단 어떤 쪽도 다른 쪽에 발각되지 않으면서 흉내 낼 수 없다. 메시지 내용을 임의로 변경하는 경우는 수신한 메시지의 복호화 결과 의미 없는 내용이 나오므로 수신자에게 발각된다.

Ⅴ. 피어의 온라인 활동들에 대한 방어

본 장에서는 피어들이 오버레이 네트워크 상에서 여러 온라인 활동들을 수행할 때 이들에 대한 다양한 공격과 이런 각각의 공격에 대해 암호화 기법을 이용한 방어 기법을 제시한다.

5.1 온라인 활동과 메시지 구조

오버레이 네트워크의 피어는 네트워크 상의 다른 피어들과 교류하기 위해 온라인 활동들을 수행한다. 이들 중 본 논문에서는 메시지 생성, 전달, 응답의 피어간 메시지 교환에 관련된 활동을 다룬다. 이런 활동들은 어떠한 P2P 응용이든 그 목적을 달성하기 위해 수행하는 가장 기본적 행위들이라 볼 수 있다.

공격과 방어 기법을 서술하기 위해 우선 메시지 내용에 대해 악의적 변경이 가해진 것을 발각할 수

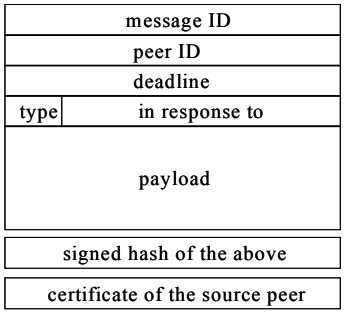

그림 2. 메시지 구조

있는 메시지 구조를 제시한다. 한 피어가 데이터(요청 또는 응답)를 네트워크로 전송할 때 데이터의 해쉬 값에 대한 서명과 피어의 인증서를 첨부하는 것이 필요하다. 그림 2는 전송할 데이터와 부가 정보를 포함한 메시지 구조를 나타낸다.

message ID는 peer ID를 갖는 소스 피어가 메시지에 부여한 유일한 번호이다. 각 메시지는 이 message ID와 peer ID에 의해 구분된다. deadline 값은 메지시의 유효기간을 의미한다. 이 deadline이 지난 후에는 중간 경유 피어는 해당 메시지를 이웃 피어로 전달하지 않는다. type 필드로 메시지가 요청(예: 쿼리)인지 응답(예: 쿼리힛)인지 구분하며, 이 필드의 값에 따라 in response to 필드가 null(메시지가 요청인 경우)이 되거나 또는 이 메시지 응답을 유발한 요청 메시지의 해쉬 값(메시지가 응답인 경우)으로 지정된다. 이 in response to 필드 값은 나머지 데이터 부분과 같이 해쉬 되어 서명된 값을 통해 보호된다. 따라서 어떤 데이터를 다른 요청에 대한 응답인 것처럼 보이게 하는 것은 해쉬 함수의 단일 방향(one-way) 성질에 의해 사실상 불가능하다. payload 부분은 실제 전송할 내용을 포함한다. 이 필드들이 소스 피어가 전송하고자 하는 데이터가 되며, 이에 부가적으로 소스 피어의 개인 키에 의한 전체 데이터 해쉬 값의 서명과 소스 피어의 인증서가 함께 전송된다.

어떤 피어가 자신의 이웃 피어로부터 메시지를 수신했을 때, 이 피어는 메시지를 다음과 같이 테스트한다. 먼저 메시지에 포함된 메시지 소스의 인증서를 테스트한다. 이 과정은 인증서를 발급한 CA의 공개 키를 알고 있으면 쉽게 수행할 수 있다. CA의 개인 키가 노출되지 않는 한 어떤 피어도 이 테스트를 통과할 수 있는 인증서를 만들어낼 수 없을 것이다. 다음으로 이 피어는 수신 메시지의 서명 부분을 테스트하는데, 이 과정에서 인증서에 포함된 소스 피어의 공개 키가 사용된다. 이 공개 키로 서명 부분을 복호화 하여 해쉬 값을 얻어 내고, 이 값이 수신 메시지의 데이터 부분에 대해 해쉬 함수를 적용한 값과 일치되는지를 확인한다. 테스트하는 피어는 어떤 단계이든 테스트가 실패하는 경우 즉시 이 메시지를 폐기한다. 만약 메시지의 deadline이 지났다면 모든 테스트를 통과했다 하더라도 메시지를 더 이상 이웃 피어로 전달하지 않는다.

5.2 공격과 방어

이제 온라인 상태에서의 악의적 피어에 의한 여러 공격과 그 방어 기법들에 대해 설명한다.

5.2.1 전달 메시지의 고의적 변경

어떤 메시지가 악의적으로 변경되었다고 가정하자. 그러면 이 메시지를 검증하는 어떤 피어도 변경 사실을 감지할 수 있다. 메시지의 payload 부분이나 또는 기타 데이터의 어떤 필드 값이라도 만약 변경되었다면 서명에 사용된 해쉬 값은 변경된 데이터에 해쉬 함수를 취한 것과 일치하지 않을 것이다. 물론 이 변경이 기존의 데이터와 동일한 해쉬 값을 만들어 내도록 이루어졌다면 일치가 일어나게 되나 해쉬 함수는 단일 방향 성질을 가지므로 그러한 변경 가능성은 무시할 정도로 작다. 서명된 해쉬 값에 변경이 발생했다면 공격자가 서명에 사용한 소스 피어의 개인 키를 알고 있지 않은 이상 발각될 수밖에 없다. 만약 데이터 부분과 서명된 해쉬 값이 함께 변경되었다면 서명 부분은 인증서의 공개 키로 정확하게 복호화 되지 못할 것이고, 역시 발각될 것이다. 인증서 자체도 물론 변경의 위험에 노출되어 있지만, 인증서의 변조는 인증서를 발급한 CA의 공개 키를 알고 있는 어떤 피어도 속이지 못할 것이다. 이러한 변경 감지가 가능한 이유는 어떤 피어가 생성하는 메시지에 그 피어의 공개 키 대신 인증서를 첨부함으로써 CA의 공개 키를 알고 있는 검증 피어가 인증서 부분부터 순차적으로 메시지 변경을 테스트할 수 있기 때문이다. 인증서 대신 피어의 공개 키가 따라온다면, 공격자는 얼마든지 다른 키가 원래의 공개 키인 것처럼 위장할 수 있다.

자신을 거쳐 가는 메시지마다 변경 여부를 테스트하게 할 것인지는 각 P2P 오버레이 네트워크의 프로토콜에서 결정할 필요가 있다. 이러한 테스트 절차가 필수 요구 사항이라면 메시지의 변경은 그 발생 후 처음 거치게 되는 이웃 피어에게서 발각될 것이고 해당 메시지는 즉시 네트워크에서 폐기될

것이다. 이런 테스트를 강제하는 네트워크에서는 어떤 메시지의 변경을 감지한 피어가 이 메시지를 자신에게 보낸 이웃 피어를 악의적 변경을 가한 또는 프로토콜을 따르지 않은 피어로 판단할 수 있다. 왜냐하면 만약 이웃 피어가 메시지에 변경을 가하지 않았다면 이웃 피어에 메시지가 이미 변경된 상태로 도착했다는 것을 의미하고, 프로토콜에 따르면 이웃 피어는 이 변경된 메시지에 변경 감지 테스트를 수행했었어야 하기 때문이다. 메시지 변경을 감지한 피어가 이러한 악의적 행위를 알리고자 하는 것은 효과를 거두기 어렵다. 그 이유는 각 피어가 스스로 메시지를 변경한 후 이웃 노드를 모함하기 위해 이웃 노드로부터 받은 것이라고 "거짓" 증거를 제시할 수 있기 때문이다. 다만 변경된 메시지를 수신한 피어는 메시지를 보낸 이웃 노드에게 낮은 신뢰도를 부여하고, 향후 해당 이웃 노드로의 통신을 제한하는 등의 차별화를 하는 것은 가능하다.

5.2.2 수신 메시지의 재생 공격

수신한 메시지를 이용한 재생 공격은 메시지 소스 피어의 평판을 깎아 내리거나 네트워크 자원을 고갈시켜 서비스 거부를 유도하는 등의 목적을 가질 수 있다. 예를 들어 어떤 피어가 자신을 거쳐 간 메시지를 저장하였다가 일정 시간이 지난 후 저장 메시지를 브로드캐스팅 함으로써 네트워크 자원을 낭비하도록 하거나, 또는 저장 메시지를 소스와 멀리 떨어진 네트워크 부분에 뿌림으로써 프로토콜의 오동작을 유도, 또는 소스 피어의 평판을 훼손하는 것 등을 재생 공격의 유형으로 볼 수 있다. 재생 공격에 대해 본 논문은 절대 시간을 deadline으로 사용함으로써 그 공격의 영향력을 크게 줄이도록 한다. IPv4나 IPv6 프로토콜에서 사용하는 TTL 또는 hop limit은 매 라우터마다 그 값이 감소하나, 이 deadline 값은 소스 피어에 의해 설정된 후 매 거쳐가는 피어에서 변경되지 않는다. 따라서 deadline 값으로 절대 시간 값을 정하고 소스 피어의 서명으로 이를 보호함으로써 이 deadline 값이 변경되는 경우는 어떤 피어든 그 변경 사실을 감지할 수 있다. 그러나 여러 피어들이 사용하는 클럭 사이에는 시간차가 존재할 수 있기 때문에 이 deadline을 통한 재생 공격 방지가 효과를 내기 위해서는 피어들 간의 클럭 시간 차이가 수용할 수 있는 범위 이내라는 가정이 필요하다. 피어들이 수행되는 호스트 컴퓨터의 시간 차이가 실제로 크지 않은 경우가 일반적임을 감안할 때 이 가정은 현실적이라 볼 수 있다. 소스 피어는 deadline을 설정할 때 피어 간 시간차를 고려하여 약간의 여유를 줄 필요가 있다.

5.2.3 고의적으로 거짓/잘못된 정보를 제공하는 공격

한 피어가 이미 답을 알고 있는 질문(예: 이 피어가 잘 알고 있고, 신뢰하는 어떤 피어에 대한 신뢰도 정보)을 포함한 쿼리를 발생시키면 이 피어는 도착한 응답들을 자신의 기준에 따라 평가할 수 있게 된다. 질문의 성격에 따라 회신을 보낸 피어의 응답이 자신과 단지 "다른" 것인지 또는 "잘못된" 것인지 판정할 수 있다. 여기서 "잘못됨"의 평가를 받는 응답은 같은 질문에 대해 절대 다수의 네트워크 피어들이 응답한 합의된 답과 다름을 의미한다. 이런 잘못된 답을 포함하는 메시지가 도착하는 경우에는 쿼리를 발생시킨 피어가 이 도착 메시지를 증거로 하여 응답 피어의 악의적 행위를 고발할 수 있다. 메시지 내용과 인증서 덕분에 어떤 다른 피어도 이런 거짓/잘못된 정보를 담고 있는 메시지를 위조할 수 없다. 따라서 이 메시지 증거는 매우 강력하게 해당 응답 피어의 악의적 행위를 뒷받침하며, 이런 종류의 공격을 억제하는데 큰 역할을 한다.

Ⅵ. 결 론

암호화 기법을 이용하여 본 논문은 P2P 오버레이 네트워크에서의 악의적 피어들에 의한 여러 공격으로부터의 효율적인 방어 기법을 제시하였다. 우선 가입하고자 하는 피어와 공개 키 기반 인프라에서 CA의 역할을 하는 믿을 수 있는 노드 사이에 보안성을 가지는 멤버쉽 처리 프로토콜을 제안했다. 이 프로토콜은 피어의 부트스트래핑 과정에서 가능한 Sybil 공격을 비롯하여, 메시지 변경과 도청 공격을 방어한다. 다음으로 피어가 오버레이 네트워크 상에서 통신하는 온라인 단계에서 가능한 여러 공격 유형으로부터의 보호를 위해 새로운 메시지 구조를 제안하고 그 방어 기법들을 개발했다. 제안 메시지 구조는 메시지 변경, 재생 공격, 거짓 정보를 포함한 메시지 생성에 대하여 효율적인 대처가 가능하도록 설계되었다. 본 논문에서 제시된 방어 기법들은 피어로 하여금 네트워크의 프로토콜을 준수하도록 독려하는 역할로서 효과적이다. 제안 기법들은 하위 P2P 토폴로지 구조에 독립적이며 비구조적 및 구조적 P2P 네트워크 모두에 적용이 가능하다. 본 논문에서 제안 기법들을 위해 가정한 믿을 수 있는 노드(CA)들은 피어의 멤버쉽 처리 단계에서만

사용되며 피어의 온라인 활동과는 무관하다.

제안 기법들은 P2P 오버레이 네트워크의 피어에 암호화 작업의 부하를 유발하는데, 현재 대부분 P2P 네트워크의 경우 피어가 실행되는 호스트는 일반 PC인 경우가 많기 때문에 이러한 부하가 네트워크 운용에 큰 영향을 미치지 않을 것으로 판단한다. 다만 피어가 자원이 제한된 소형 단말기에서 실행되는 경우 제안 기법들의 부하와 이의 시스템 차원의 영향에 대한 후속 연구가 필요하며, 이를 위해 MANET이나 센서 네트워크의 관련 연구 결과들의 적용 가능성을 분석하고자 한다. 또 다른 과제로 본 논문에서 다루지 않은 유형의 공격에 대한 방어 방법의 개발이 필요하다. 그 공격 유형 중 하나가 피어의 불법적인 메시지 폐기이다. 예를 들어, P2P 온라인 경매에서 어떤 피어는 자신의 잠재적 경쟁자가 될 수 있는 다른 피어들에게 입찰을 요구하는 메시지를 전달하지 않으려 할 수 있다. 이런 종류의 공격은 암호화 기법을 이용하더라도 공격의 결과를 가지고 공격 피어를 찾는 것이 매우 어렵다.

참 고 문 헌

[1] M. Parameswaran, A. Susarla, A.B. Whinston, “P2P Networking: An Information-Sharing Alternative”, *IEEE Computer*, 34(7), July 2001.

[2] S. Androutsellis-Theotokis, D. Spinellis, “A Survey of Peer-to-Peer Content Distribution Technologies”, *ACM Computing Surveys*, 36(4), December 2004.

[3] E. Sit, R. Morris, “Security Considerations for Peer-to-Peer Distributed Hash Tables”, *Proc. Int’l Workshop on Peer-to-Peer Systems*, March 2002.

[4] D. Wallach, “A Survey of Peer-to-Peer Security Issues”, *Proc. Int’l Symp. on Software Security*, November 2002.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, D. Wallach, “Secure Routing for Structured Peer-to-Peer Overlay Networks”, *Proc. Usenix Symp. on Operating Systems*, December 2002.

[6] J. Douceur, “The Sybil Attack”, *Proc. Int’l Workshop on Peer-to-Peer Systems*, March 2002.

[7] M. Rabin, “Efficient Dispersal of Information for Security, Load Balancing and Fault Tolerance”, *Journal of the ACM*, 36(2), April 1989.

[8] P. Dewan, “Countering Identity Farms in Reputation Systems for P2P Networks”, *Arizona State University*, *Technical Report*, 2004.

[9] S. Marti, H. Garcia-Molina, “Taxonomy of Trust: Categorizing P2P Reputation Systems”, *COMNET Special Issue on Trust and Reputation in Peer-to-Peer Systems*, 2005.

[10] J. Risson, T. Moors, “Survey of Research Towards Robust Peer-to-Peer Networks: Search Methods”, *TR UNSW-EE-P2P-1-1*, *Univ. of New South Wales, Australia*, September 2004.

[11] P. Dewan, P. Dasgupta, “Securing P2P Networks Using Peer Reputations: Is there a silver bullet?”, *Proc. IEEE Consumer Communications and Networking Conf.(CCNC2005)*, *USA*, 2005.

[12] A. Blanc, Y. Liu, A. Vahdat, “Designing Incentives for Peer-to-Peer Routing”, *Proc. IEEE INFOCOM*, March 2005.

[13] J. Liang, R. Kumar, Y. Xi, K. Ross, “Pollution in P2P File Sharing Systems”, *Proc. IEEE INFOCOM*, March 2005.

[14] A. Shamir, “How to Share a Secret”, *Communications of the ACM*, 22, 1979.

박 준 철 (Jun-Cheol Park) 정회원

1986년 서울대학교 계산통계학과 (학사)

1988년 KAIST 전산학과(석사)

1998년 미국 Maryland 대학교 전산학과(박사)

현재 홍익대학교 컴퓨터공학과 조교수

<관심분야> Overlay Networks, Network Security