정 보 보 호 학 회 지
제26권 제6호, 2016. 12

정보 중심 네트워킹에서 보안과 프라이버시

김 은 아*, 정 진 환**

요 약

미래인터넷 기술의 하나인 정보 중심 네트워킹은 기존의 호스트 중심 네트워킹 개념을 대체하는 새로운 통신 방식으로, 인터넷과 같은 현재의 통신 방식의 한계를 극복하기 위한 대안으로 제안되었다. 정보 중심 네트워킹은 정보의 근원지 주소가 아닌 정보의 이름을 기반으로 통신하여, 네트워크의 확장성을 높이고 정보의 전송 효율을 높이는 것을 주요 목표로 한다. 이를 위하여 이름 기반 라우팅이나 네트워크 내 캐싱 기능 등을 제공하고, 신뢰성 있는 정보 제공을 위하여 무결성 보장 기능도 제공한다. 이와 같이 설계에서부터 네트워크의 효율과 신뢰성 제공을 고려하여 설계된 네트워킹 개념이지만, 여전히 보안 위협이나 프라이버시 침해 위험이 존재한다.

본 고에서는 정보 중심 네트워킹 구조에서 발생 가능한 보안 위협과 프라이버시 침해에 대응하기 위한 기존의 연구들을 소개하고, 향후 연구 방향을 제시하고자 한다.

Ⅰ. 서 론

최근 모바일 기기와 사물 인터넷(Internet of Things) 기기와 같은 다양한 인터넷 기기들이 증가하면서 인터넷 상의 데이터 전송량이 급증하고 있다. 이러한 데이터 전송의 대부분은 멀티미디어 콘텐츠 서비스로, 동일한 콘텐츠를 다수 사용자에게 반복적으로 전송하는 형태를 보인다. 현재의 인터넷은 효율적인 콘텐츠 서비스를 위하여 CDN(Content Delivery Network)과 같은 기술을 이용하기도 하지만, 수많은 기기들과 이로부터 발생하는 데이터 전송량을 수용하기에 확장성(Scalability) 면에서 한계가 있다.

보다 확장성 있고 효율적인 콘텐츠 서비스를 위한 미래 인터넷 연구의 일환으로 정보 중심 네트워킹(Information-Centric Networking, 이하 ICN)이 있다. 이는 기존 인터넷과 같은 호스트(Host) 중심 네트워킹 개념을 대체하는 새로운 통신 방식으로, 통신의 목적인 정보(다양한 형태의 데이터를 의미, 이하 콘텐츠) 자체가 통신의 기반이 된다.

ICN은 호스트의 IP 주소를 이용하여 콘텐츠에 접근하는 기존 인터넷과 달리 콘텐츠에 부여된 이름을 이용하여 콘텐츠에 접근하는 방식이다. 이를 위하여 각 콘텐츠는 네트워크에서 유일하게 식별 가능한 이름을 가질 수 있어야 하고, 이름 기반 라우팅 방법이 존재해야 한다. 이름 기반 라우팅은 콘텐츠가 네트워크 내 어느 위치에 저장되어도 이름으로 접근이 가능하게 하므로, 네트워크 내 임의 위치에 콘텐츠를 캐싱(Caching)할 수 있도록 하여 콘텐츠 분배 효율을 높일 수 있다. 현재까지 제안된 다양한 ICN 구조들은 앞서 설명한 바와 같이 1) 유일한 이름을 갖는 콘텐츠, 2) 이름 기반 라우팅, 3) 네트워크 캐싱 기능을 특징으로 한다. 이와 함께 신뢰성 있는 콘텐츠 제공을 위하여, 4) 콘텐츠 무결성 보장 기능을 제공하는 구조도 있다.

ICN이 기존과 다른 새로운 통신 방식을 채택하였지만, 보안과 프라이버시는 여전히 중요한 문제이다. 기존 인터넷에 존재하는 보안 위협이 ICN에서도 적용될 수 있고, ICN 고유의 특성을 이용한 보안 위협이나 프라이버시 침해가 발생할 수 있다.

본 고에서는 ICN 구조에서 발생 가능한 보안 위협과 프라이버시 침해에 대응하기 위한 기존의 연구들을 소개하고자 한다. 또한, 이들 연구의 한계점을 통하여 향후 연구 방향을 제시하고자 한다.

본 고의 구성는 다음과 같다. II장에서 대표적인 ICN 구조들을 소개하고, 각각의 특징을 간략히 살펴본다. III장에서 ICN에서 발생할 수 있는 보안 위협과 보안 고

* 삼성전자 (dmsk999@gmail.com)
** SK Telecom (jhjeong.kr@gmail.com)

려사항에 대하여 기존 연구를 통해 알아본다. IV장에서는 ICN에서 발생할 수 있는 프라이버시 침해 가능성과 기존 연구에서 제안된 대응책들을 소개한다. 마지막으로 V장에서 향후 연구 방향을 제시하면서 결론을 맺도록 한다.

Ⅱ. ICN 구조

ICN은 통신 방식에 따라 두 가지로 나눌 수 있다. 콘텐츠 요청자에 의해 통신이 시작되는 소비자 주도(Consumer-driven) 모델과 콘텐츠 생성자나 제공자에 의해 통신이 시작되는 발행-구독(Publish- Subscribe) 모델이다.

두 가지 모델의 ICN 구조들의 세부 통신 방식은 다르지만, 공통적 특징인 1) 콘텐츠 네이밍(Naming), 2) 이름 기반 라우팅, 3) 네트워크 캐싱, 4) 콘텐츠 무결성 보장 기능을 가진다.

2.1. 소비자 주도 구조

대표적인 소비자 주도형 ICN 구조는 Content-Centric Networking(CCN)[1,2]이다. CCN은 2009년 Palo Alto Research Center에서 제안되었고, 2010년 미국 National Science Foundation(NSF)이 지원하는 Future Internet Architecture Program에서 Named-Data Networking(NDN)[3] 과제로 연구를 진행하였다.

CCN에서 콘텐츠 이름은 URI와 같은 계층적인 구조를 갖는다. 이는 콘텐츠 이름에 도메인 개념을 부여할 수 있고, 조건 검색이나 비교가 가능하다. 통신을 위해서 콘텐츠 요청을 위한 Interest 패킷과 응답을 위한 Data 패킷이 이용된다. 콘텐츠 이름을 포함하는 Interest가 네트워크 내에 플러딩(Flooding)되면, 해당되는 콘텐츠를 저장하고 있는 라우터나 콘텐츠 제공자가 Data를 Interest의 역 경로로 전송한다. CCN 라우터는 콘텐츠 캐싱을 위한 CS(Content Store), 콘텐츠 요청 관리와 라우팅을 위한 PIT(Pending Interest Table), 라우팅을 위한 FIB(Forwarding Information Base)를 운용해야 한다. 이러한 라우터의 구조는 기존의 인터넷과 다른 점이고, 이를 이용한 보안 공격이 가능해진다.

2.2. 발행-구독 구조

Data Oriented Network Architecture (DONA)[4]는 2007년 UC Berkeley 대학에서 제안되었다.

DONA에서 콘텐츠 이름은 CCN과 달리 평면 구조를 가진다. 이름을 구성하는 요소는 공개키 기반의 검증 가능한(Self-certifying) 해쉬값들로, 생성자의 공개키 해쉬값과 콘텐츠 자체의 해쉬값으로 이루어진다. 이는 콘텐츠의 무결성을 검증할 수 있도록 한다. 통신을 위해서 콘텐츠 발행을 위한 REGISTER 메시지와 콘텐츠 구독을 위한 FIND 메시지를 사용하고, 이들 메시지는 Resolution Handler(RH)로 구성된 계층적인 네트워크에서 라우팅 된다. RH는 REGISTER에 포함된 콘텐츠 이름과 콘텐츠 발행자 정보를 저장하는 기능, 콘텐츠 구독 요청을 계층 구조 내 다른 RH들에게 전송하는 기능, 요청된 콘텐츠가 저장된 위치를 탐색하는 기능 등을 제공한다.

Publish Subscribe Internet Technology (PURSUIT)[5]는 발행-구독 구조의 네트워크 프로토콜 스택을 연구하는 유럽 FP7 과제이다.

PURSUIT에서 콘텐츠 이름은 DONA와 같은 평면 구조로, 콘텐츠가 속한 그룹을 나타내는 영역 식별자(Scope ID)와 영역 내에서 유일하게 콘텐츠를 식별할 수 있는 랑데부 식별자(Rendezvou ID)로 구성된다. 통신을 위해서 콘텐츠 발행을 위한 PUBLISH 메시지와 콘텐츠 구독을 위한 SUBSCRIBE 메시지를 사용하고, 이들 메시지는 Rendezvous Node(RN)로 구성된 랑데부 네트워크에서 처리된다. RN은 Distributed Hash Table(DHT)를 이용하여 발행된 콘텐츠의 저장 위치를 결정하고, 구독 요청된 콘텐츠 또한 DHT를 이용하여 빠르게 검색할 수 있다.

발행-구독형 ICN 구조에서는 대부분 평면 구조의 검증 가능한 이름을 채용하여, 콘텐츠의 생성자와 콘텐츠에 대한 무결성을 확인할 수 있도록 하였다.

Ⅲ. ICN 보안 위협 및 고려사항

본 장에서는 ICN 구조에서 발생 가능한 보안 공격의 종류와 제안된 대응방안을 살펴본다.

소개하는 서비스 거부 공격, 콘텐츠 포이즈닝 공격, 캐시 폴루션 공격은 주로 CCN과 같이 콘텐츠 라우터

에 의해 콘텐츠가 캐싱되고, 소비자 주도 구조로 통신이 이루어지는 ICN 구조를 대상으로 한다.

3.1. 서비스 거부 공격 (Denial of Service Attack)

서비스 거부 공격은 콘텐츠 라우터나 콘텐츠 제공자에게 지속적이고 다량의 악의적 요청을 시도하여, 정상적인 콘텐츠 요청에 대응하지 못하도록 한다. 이는 CCN과 같은 소비자 주도 구조에서 주로 발생하는데, 콘텐츠 라우터의 PIT를 고갈시키거나[6-9] 콘텐츠 제공자의 리소스를 고갈시키기[9] 위하여 Interest 플러딩을 이용한다. 공격자가 동적으로 생성되거나 존재하지 않는 콘텐츠를 요청하는 Interest를 고속으로 다량 전송하면, 콘텐츠 라우터나 콘텐츠 제공자는 이를 처리하기 위하여 정상적인 서비스를 지연시키거나 제공하지 못하게 된다.

Interest 플러딩 기반 서비스 거부 공격을 대응하기 위한 연구의 다수가 공격으로 의심되는 Interest가 유입되는 인터페이스나 Interest가 요청하는 콘텐츠 이름에 대하여 처리 비율을 제한하는 방법(Rate limiting)을 제안하였다[6-9]. 처리 비율 제한 방법은 하나의 인터페이스로부터 유입되는 Interest를 처리하기 위하여 라우터의 리소스를 모두 사용하는 것을 방지하거나, 콘텐츠 이름으로 Interest를 필터링 하는데 효과적이다. 그러나 실제 공격자와 정당한 요청자의 Interest를 구분하기 어렵고, 이로 인하여 정당한 요청자의 콘텐츠 요청이 제한될 수 있다.

3.2. 콘텐츠 포이즈닝 공격 (Content Poisoing Attack)

콘텐츠 포이즈닝 공격은 콘텐츠 라우터의 캐시를 유효하지 않은 콘텐츠로 채우는 공격이다. 이를 위해 공격자는 하나 이상의 콘텐츠 라우터나 콘텐츠 제공자를 제어하여 네트워크 내에 유효하지 않은 콘텐츠를 주입한다. 공격자가 주입하는 콘텐츠는 기존에 네트워크 내에 캐싱된 유효한 콘텐츠의 이름을 사용하지만, 콘텐츠의 내용이나 서명이 유효하지 않은 정보로 구성된 것으로, 사용자에게 쓸모없는 콘텐츠가 된다. 또한, 이러한 콘텐츠로 라우터의 캐시가 채워지면, 유효한 콘텐츠가 저장되지 못하여 캐시 효율이 낮아진다.

콘텐츠 포이즈닝 공격을 다룬 연구들은 라우터의 서명 검증을 기반으로 하는 방법을 제안하였다. 라우터가 콘텐츠 패킷에 포함된 서명을 검증하거나[9], 요청 패킷에 포함된 콘텐츠 해쉬값과 실제 콘텐츠의 해쉬값을 비교하는 방법[9,10] 등이 있다. 서명 검증 방법은 암호화 연산 비용과 그에 따른 확장성 문제, 서명 검증에 필요한 정보의 공유 문제 등이 뒤따른다. 다른 대안으로 콘텐츠 사용자들의 피드백을 기반으로 콘텐츠에 점수를 부여하는 방법이 있다[11]. 이 방법은 사용자의 피드백에만 의존하기 때문에 신뢰성에 한계가 있다.

콘텐츠 라우터는 적은 비용으로 공격을 탐지할 수 있어야 하므로, 서명 검증 보다는 해쉬 검증과 같은 기능을 갖는 것이 효과적으로 보인다.

3.3. 캐시 폴루션 공격 (Cache Pollution Attack)

캐시 폴루션 공격은 콘텐츠 전송 효율을 높이기 위하여 자주 요청되는 콘텐츠를 캐싱하는 기능을 역으로 이용하여, 공격자가 유용하지 않은 콘텐츠를 계속적으로 요청하여 캐시의 효율을 떨어뜨리는 공격이다. 공격자는 자주 요청되지 않는 콘텐츠를 계속 요청하여 캐시에 저장되도록 하거나(False Locality), 유용하지 않은 여러 콘텐츠를 주기적으로 요청하여 캐시에 저장되는 콘텐츠가 계속 바뀌도록 한다(Locality Disruption). 이는 캐시가 효율적으로 동작하지 못하도록 하여 네트워크 내 콘텐츠 전송을 지연시킨다.

캐시 폴루션 공격을 감지하거나 공격에 강인한 캐시 기법에 대한 연구들이 진행되었으나[12,13], 라우터에서 수행해야 하는 연산 비용이 높은 문제점이 있다. 단일 캐시의 고비용 연산으로 공격에 대응하는 대신, 여러 캐시들이 협력하여 공격을 탐지하는 것도 유용한 방법이다[14]. 그러나 현재까지 협력 캐싱에 대한 효과적인 연구 결과는 나타나지 않았다.

3.4. 시큐어 네이밍 (Secure Naming)

콘텐츠에 이름을 지정하는 것은 ICN의 필수 요소로 특히 라우팅과 보안 기능들을 위해 중요하다. 콘텐츠 이름을 지정할 때, 콘텐츠 제공자와의 신뢰성 있는 바인딩(Binding)이 이루어지지 않으면, 콘텐츠 포이즈닝 공격과 같이 콘텐츠의 신뢰성을 떨어뜨리는 공격이 가능해진다. 안전한 바인딩을 위하여 전자 서명이 이용될 수

있으나, 서명 검증을 위한 비용 문제도 고려되어야 한다. 라우터를 지나가는 모든 패킷에 대한 서명 검증은 라우터의 부하를 가중시키기 때문이다.

CCN에서 신뢰성 있는 이름 생성을 위하여 신원 기반 암호(Identity-based Cryptography)를 이용한 연구에서는 콘텐츠 제공자의 신원이나 콘텐츠의 이름이 공개키로 사용된다[15]. 이 방식은 공개키에 대응되는 개인키 생성을 위하여 제3의 신뢰기관을 이용해야 하고, 가독성이 떨어지는 콘텐츠 이름을 위한 이름 변환 서비스가 추가되어야 한다.

Ⅳ. ICN 프라이버시 침해 및 고려사항

본 장에서는 콘텐츠 라우터, 콘텐츠, 콘텐츠 이름 등의 ICN 구성 요소로부터 정보를 수집하거나 유출시키는 공격의 종류와 제안된 대응방안을 살펴본다.

소개하는 타이밍 공격과 통신 모니터링 공격은 CCN과 같이 콘텐츠 라우터에 의해 콘텐츠가 캐싱되고, 소비자 주도 구조로 통신이 이루어지는 ICN 구조를 대상으로 한다.

4.1. 타이밍 공격 (Timing Attack)

타이밍 공격은 콘텐츠 라우터와 지역적으로 근접한 콘텐츠 요청자의 정보 유출을 목적으로 한다. 공격자는 라우터에 캐싱된 콘텐츠를 조사하기 위하여 다수의 콘텐츠를 요청하고 전송되는 시간을 정확하게 측정한다. 콘텐츠 마다 전송 시간이 차이가 발생하면, 콘텐츠가 대상 콘텐츠 라우터로부터 전송되었는지, 다른 라우터나 콘텐츠 제공자로부터 전송되었는지 구별할 수 있다. 이렇게 대상 라우터에 캐싱된 콘텐츠 목록을 조사하여 해당 라우터에 콘텐츠를 요청하는 사용자들의 콘텐츠 선호도 혹은 요청 패턴을 파악할 수 있다.

타이밍 공격으로 인한 콘텐츠 라우터에 저장된 콘텐츠 목록이나 콘텐츠 요청자들의 정보 유출을 방지하기 위하여, 콘텐츠 라우터에서 인위적으로 전송 시간을 지연시키는 방법들이 제안되었다[16,17]. 이는 공격자로 하여금 시간을 이용하여 정보를 추정하지 못하게 하지만, ICN의 목적인 효율적인 데이터 전송에 반하는 방법이다. 전송 시간 지연은 콘텐츠 서비스의 질을 떨어뜨린다.

4.2. 통신 모니터링 공격 (Communication Monitoring Attack)

통신 모니터링 공격은 타이밍 공격과 같이 콘텐츠 라우터로부터 콘텐츠 요청 정보를 수집하되, 특정 콘텐츠 요청자에 대한 콘텐츠 요청 정보를 수집하는 공격이다. 공격자는 공격 대상과 근접한 위치에 있어, 같은 콘텐츠 라우터를 이용할 수 있고, 사전에 공격 대상에 대한 정보를 보유하고 있는 경우가 많다.

콘텐츠 라우터에 캐싱된 콘텐츠를 조사하여 사용자의 콘텐츠 요청 정보 유출을 방지하기 위하여, 민감한 콘텐츠를 콘텐츠 라우터 캐시에 저장하지 않는 방법들이 제안되었다. 콘텐츠를 캐시에 저장하지 않기 위해 보안 터널링(Secure Tunneling)을 이용한 콘텐츠 전송을 하거나[18], 콘텐츠 요청에 콘텐츠 저장을 방지하는 플래그를 삽입할 수 있다. 또한 선택적으로 콘텐츠를 캐싱하기 위하여 요청 빈도가 특정 임계치 이상인 경우에만 캐싱하는 방법도 제안되었다[19,20].

콘텐츠 라우터와 콘텐츠 요청자 사이에 보안 터널을 이용한 콘텐츠 전송은 통신 복잡도와 비용을 증가시키고, 콘텐츠 라우터의 부하를 가중시킨다. 또한, 일부 콘텐츠 요청자에 의하여 과도하게 사용되는 경우 불필요하게 네트워크의 리소스를 낭비하게 된다. 콘텐츠 요청 빈도에 따른 선택적인 콘텐츠 캐싱 방법은 콘텐츠 요청자들의 요청 빈도에만 의존하기 때문에 신뢰성이 떨어질 수 있다.

4.3. 익명성 (Anonymity)

익명성은 통신 네트워크에서 중요한 요구사항이다. 통신의 익명성이 보장되지 않으면, 콘텐츠 요청자와 콘텐츠 자체에 대한 정보가 유출되고, 통신 검열을 용이하게 한다. 기존의 IP 기반 인터넷과 달리 특히 ICN에서는 통신 패킷에 콘텐츠의 이름이 명시되기 때문에, 이름을 통해 콘텐츠에 대한 정보가 쉽게 유출될 수 있다. 또한 콘텐츠 이름을 이용하여 통신 패킷을 필터링 하거나 검열할 수 있다.

CCN에서 통신 익명성 제공을 위하여 보안 터널링을 이용하는 방법들이 제안되었다[18,21]. 보안 터널링은 콘텐츠 제공자나 콘텐츠 라우터와 콘텐츠 요청자 사이에 콘텐츠를 암호화 하여 전송하는 방식이다. 다른 방법으로 콘텐츠 이름을 난독화 하는 기법도 제안되었다

[22]. 그러나 이들에 적용되는 암호화 연산의 복잡도와 비용은 심각하게 고려되지 않았다.

Ⅴ. 결 론

본고에서는 ICN 구조에서 발생 가능한 보안 위협과 프라이버시 침해에 대응하기 위한 기존의 연구들을 간략하게 소개하였다. ICN은 설계에서부터 네트워크의 효율과 신뢰성 제공을 고려하여 설계된 네트워킹 개념이지만, 소개한 바와 같이 여전히 보안 위협이나 프라이버시 침해 위험이 존재한다. 현존하는 연구에서 보안 위협이나 프라이버시 침해에 대응하기 위한 노력을 기울이고 있으나, ICN의 기본 목적인 확장성과 콘텐츠 전송 효율성을 위배하는 경우를 발견할 수 있었다. 향후 ICN을 위한 보안과 프라이버시를 고려할 때, ICN의 기본 특성을 유지하면서 적은 비용과 공격에 강인한 대응 방안들이 제안되어야 할 것이다.

참 고 문 헌

[1] CCNX. http://www.ccnx.org/

[2] V. Jacobson et al., “Networking named content,” CoNext’09, ACM, 2009.

[3] NDN. http://named-data.net/

[4] T. Koponen et al., “A Data-oriented (and beyond) Network Architecture,” ACM SIGCOMM Computer Communi- cation Review, vol. 37, no. 4, Oct. 2007.

[5] Publish-Subscribe Internet Technology. http://www.fp7-pursuit.eu/PursuitWeb

[6] A. Afanasyev et al., “Interest flooding attack and countermeasures in named data networking,” IEEE IFIP Networking Conference, 2013.

[7] A. Compagno et al., “Poseidon: Mitigating interest flooding ddos attacks in named data networking,” The 38th IEEE Local Computer Networks (LCN), 2013.

[8] H. Dai et al., “Mitigate ddos attacks in ndn by interest traceback,” IEEE Computer Communications Workshops (INFOCOM WKSHPS), 2013.

[9] P. Gasti et al., “Dos and ddos in named data networking,” The 22nd IEEE ICCCN, 2013.

[10] C. Ghali et al., “Elements of trust in named-data networking,” arXiv preprint arXiv:1402.3332, 2014.

[11] C. Ghali et al., “Needle in a haystack: Mitigating content poisoning in named-data networking,” NDSS Workshop on Security of Emerging Networking Technologies(SENT), 2014.

[12] A. Karami and M. Guerrero-Zapata, “An anfis-based cache replacement method for mitigating cache pollution attacks in named data networking,” Computer Networks, 2015.

[13] H. Park et al., “Detection of cache pollution attacks using randomness checks,” IEEE ICC, 2012.

[14] S. Wang et al., “Collaborative caching based on hash-routing for information- centric networking,” ACM SIGCOMM Computer Communication Review, 2013.

[15] X. Zhang et al., “Towards name-based trust and security for content-centric network,” The 19th IEEE ICNP, 2011.

[16] G. Acs et al., “Cache privacy in named-data networking,” The 3rd IEEE ICDCS, 2013.

[17] A. Chaabane et al., “Privacy in content-oriented networking: Threats and countermeasures,” ACM SIGCOMM Computer Communication Review, 2013.

[18] S. DiBenedetto et al., “Andana: Anonymous named data networking application,” arXiv preprint arXiv:1112.2205, 2011.

[19] T. Lauinger et al., “Privacy implications of ubiquitous caching in named data networking architectures,” Technical report, TR-iSecLab-0812- 001, iSecLab, 2012.

[20] T. Lauinger et al., “Privacy risks in named data networking: what is the cost of performance?,” ACM SIGCOMM Computer Communication Review, 2012.

[21] S. Chung et al., “A privacy-preserving approach

in content centric networking," The 11th IEEE CCNC, 2014.

[22] S. Arianfar et al., "On preserving privacy in content-oriented networks," ACM SIGCOMM workshop on Information-centric networking, 2011.

〈저자소개〉

김 은 아 (Kim Eunah)
2003년 : 이화여자대학교 컴퓨터학과 졸업
2005년 : 이화여자대학교 컴퓨터학과 석사
2006년~현재 : 삼성전자 책임연구원
관심분야 : 네트워크 보안, 개인정보보호

정 진 환 (Jeong Jin-Hwan)
1999년 : 고려대학교 컴퓨터학과 석사
2005년 : 고려대학교 컴퓨터학과 박사
2005년~2014년 : 한국전자통신연구원 선임연구원
2014~현재 : SKTelecom 매니저
관심분야 : 모바일 네트워크, 운영체제