정 보 보 호 학 회 지
제26권 제6호, 2016. 12

ICN 해킹 공격 및 대응 방안 연구 동향

허 미 숙*

요 약

ICN은 증가하는 콘텐츠 트래픽을 효율적으로 수용하려는 목적으로 새롭게 제안된 미래 인터넷 기술이다. 기존 host-centric 구조와 다르게 콘텐츠의 경로의 보안성 보다는 콘텐츠 자체의 안전성을 고려한 것이 큰 특징이다. 본 논문에서는 ICN의 naming, routing, caching 및 그 외 특성들을 살펴보고 그와 관련된 공격 유형 및 현재까지 제안된 대응 방안에 대해 살펴본다.

Ⅰ. 서 론

2016년에 발표된 Cisco VNI 2015-2020 글로벌 전망 보고서[1]에 의하면 IP traffic이 2020년까지 월 194 Exabytes 까지 증가할 것으로 전망 되며, 그중 82% 이상이 비디오와 같은 멀티미디어 콘텐츠 일 것으로 예상하고 있다. 이는 2015년의 70% 보다 높은 수치이다. 현재 인터넷 구조에서는 이런 미래 트렌드를 반영하기에는 충분하지 않아 십여 년 전부터 대량의 콘텐츠를 전송하고 분배하는데 적합하도록 개선된 구조의 인터넷 아키텍처가 연구되기 시작했다. 그러한 여러 솔루션들 중 하나가 정보 중심 네트워킹 (ICN, Information Centric Network)이다. ICN은 콘텐츠 cache와 사용자의 콘텐츠 요청에 중점을 두고 설계되었다. 이런 목적들을 성취하기 위해 host location에 독립적인 naming, in-network caching, name-based 라우팅 방법 등이 제안되었다.

ICN은 콘텐츠를 요청자에게 직접 보내는 대신 공유하고 싶은 콘텐츠에 대한 홍보 메시지 (Advertisement Message)를 네트워크을 통하여 게시한다. 또한 특정 콘텐츠를 원하는 사용자는 콘텐츠의 원 저자를 알 필요 없이 원하는 콘텐츠를 네트워크를 통하여 요청한다. ICN은 적당한 라우팅 정책을 이용하여 요청자가 원하는 콘텐츠와 게시된 콘텐츠가 일치 하는 경우, 게시된 콘텐츠를 요청자에게 전송한다. 이는 기존의 P2P, DDB, CDN, cloud computing [2,3] 과 비슷한 목적을 가지고 있으나 그 구조에서는 차이점이 있다. 위에서 언급한 naming, routing 및 caching 방법과 security 특징이 그것이다. 특히 기존 IP 네트워크와는 다르게 설계 초기부터 security를 고려하여 만든 것이 주목할 만하다. IP 기반 네트워크가 data의 경로를 안전하게 설정/관리 하는 것이 주목적인 반면, ICN은 모든 노드에 cache될 수 있는 콘텐츠 자체를 안전하게 하고자 하는데 주안점을 두고 있다. 이와 같은 security 구조 및 아키텍처의 차이점으로 공격 형태 또한 다르게 나타나며 이를 해결하기 위한 솔루션도 기존 IP 기반 네트워크와는 많은 차이점을 가지고 있다.

본 논문에서는 위에 언급한 ICN의 특성들 즉, naming, routing, caching 등에 대해 자세히 알아보고 그와 관련된 공격 즉, ICN 구조의 고유 속성에 의해 생겨나는 공격들, 그리고 현재까지 공개된 솔루션들을 소개하고자 한다.

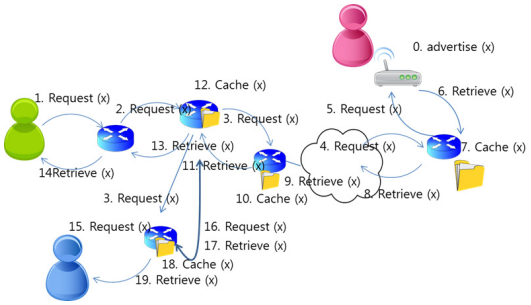
Ⅱ. ICN의 특성

ICN은 기존 네트워크와 다른 구조를 가지고 있으므로 또한 그 공격 방법이 기존 네트워크에서 행해지는 것과 다른 형태의 공격들이 제안되고 있다. 다음 장에서 소개할 ICN 구조의 특징과 관련된 공격 및 솔루션들을 이해하기 위해 먼저 기존 host-centric 네트워크와 ICN 구조의 차이점을 살펴보고자 한다.

두 네트워크 구조의 차이점은 크게 다섯 가지로 나눌 수 있다. 첫째는 naming 체계와 운영 방법이다. 기존 네트워크에서는 네트워크 주소를 이용하여 패킷의 도착

* 삼성전자 (misukhuh@gmail.com)

호스트 주소를 명확히 명시한다. 그러나 ICN에서는 콘텐츠를 대표하는 이름 외에는 어떤 특정 호스트 주소도 갖지 않는다. 이는 ICN이 콘텐츠의 효율적 공유에 그 목적을 두고 있기 때문에, 호스트의 주소보다는 특정 콘텐츠를 네트워크에서 효율적으로 찾는 구조로 설계되었기 때문이다. 콘텐츠를 요구하고 이에 맞는 콘텐츠를 찾아 주는 것이 필요하므로 콘텐츠가 저장되어 있는 주소가 아닌 콘텐츠의 이름이 필요하다. 그러므로 찾고자 하는 콘텐츠의 정보가 포함된 콘텐츠 naming 체계가 필요하고 이를 토대로 ICN 네트워크상에서 패킷을 라우팅을 하게 된다. 이 때문에 특정 호스트 주소를 가지는 기존 네트워크의 라우팅과는 다른 라우팅 기술이 요구된다. 호스트의 위치를 기반으로 하게 되는 IP 주소가 아닌 name- based routing을 사용하는 것이다. 이는 라우터에서 요청된 콘텐츠 이름을 저장하고 cache 된 콘텐츠가 없다면 주변 라우터에 수신된 요청을 재전송한다. 주변 라우터가 요청된 콘텐츠를 찾아 전달해 주면 라우터는 수신된 콘텐츠를 라우터 정책에 따라 cache 후, 요청자 (또는 요청 라우터)에 전달 또는 cache 없이 전달해 주게 된다. 요청된 라우팅의 역방향으로 콘텐츠가 전송 되므로 요청된 콘텐츠를 받을 때까지 일정 시간 요청을 저장 하고 있다가 요청 콘텐츠가 전달돼서 다시 전송해 주거나 일정시간이 지나면 요청 내용을 삭제하게 된다. 셋째는 바로 전에 언급했듯이 전송되는 콘텐츠를 임시 저장하는 것이다. 기존 네트워크는 특별한 목적을 위해, 지정된 서버 등에 콘텐츠가 저장되는 반면 ICN은 콘텐츠가 지나가는 대부분의 라우터에 콘텐츠를 저장할 수 있는 것이 기본 원칙이다[그림 1]. 많이 요청되는 콘텐츠는 이 특징으로 인해 콘텐츠 요청 메시지가 콘텐츠가 최초 게시된 곳까지 가지 않고 그 콘텐츠가 cache된 라우터를 만나면 바로 콘텐츠를 가져 올 수 있어 전체적으로 네트워크 효율성을 높일 수 있다. 네 번째는 security 특성이다. 기존 네트워크에서와 달리 모든 사용자들이 콘텐츠를 게시할 수 있고, 모든 네트워크 노드들이 전송 중의 콘텐츠를 cache 할 수 있으므로 ICN에서는 콘텐츠 자체에도 security를 적용 하는 것이 매우 중요하다. 기본적으로 콘텐츠의 공급자 (Content Owner)의 서명 정책을 사용함으로써 실제 콘텐츠 생성자가 생성한 콘텐츠인지 확인 할 수 있다. 이는 콘텐츠가 여러 노드에서 랜덤하게 cache되는 특성상 실제 시작 주소에 대한 정보가 없어 발생할 수 있는 여러



〔그림 1〕 ICN 아키텍쳐 : routing and caching

security 취약점을 보완하는 중요한 정책이라고 할 수 있다. 마지막으로 ICN의 naming에 의해 발생되는 API의 차이점이다. 기존 네트워크가 특정 주소로 data를 보내는 형식을 지원하는 API를 제공 하는 반면 ICN에서의 API는 콘텐츠를 요청(request)하거나, 요청된 콘텐츠의 전송 및 처음 게시하는 방법들을 제공해야 한다.

Ⅲ. ICN 공격 및 대응 방법

이 장에서는 위에 제시한 ICN 특징들로 인한 공격 유형들을 살펴보고 그에 대응되는 솔루션들을 살펴보고자 한다.

3.1. Naming 공격 및 대응 방법

ICN은 콘텐츠의 이름을 참조하여 패킷을 라우팅 한다. 그림 1에서와 같이 콘텐츠 요청이 수신되면, 그 콘텐츠가 cache 되어 있는 지 확인 하고 cache 되어 있으면 요청 라우터나 요청자에게 전송한다. 그렇지 않은 경우 콘텐츠 이름을 남기고 주변 라우터에 전송하게 된다. 이런 특성 때문에 요청된 콘텐츠의 이름이 전송 경로에 있는 모든 노드들에게 쉽게 노출 될 수 있고, 이것은 ICN의 주요한 공격 포인트 중의 하나가 된다. 요청되는 콘텐츠 이름 중에 미리 공격하고 싶은 콘텐츠 이름의 리스트를 가지고 필터링하는 name watch 공격과 사전 리스트 없이 전송되는 임의의 콘텐츠 이름들을 분석하고 특정 정보들을 얻고자 하는 content-analysis (sniffing) 공격으로 나눌 수 있다[4]. [4]에서는 공격 환경을 다음과 같이 가정한다. data를 저장하는 infrastructure가 특정 admin.에 의해 제어 되는 환경이 아니고, user와 콘텐츠 게시자간에 미리 공유된 secret이 없으며 Tor 같은 익명성을 위한 특정 솔루션이 적용

되어 있지 않고, 공격자는 제한된 자원을 가진다. 이런 환경에서, 제안하는 방법은 실제 사용자와 공격자가 콘텐츠를 제대로 얻기 위해 필요한 계산 량을 다르게 설계하는 것이다. 공격자가 훨씬 많은 양의 계산을 해야 필요한 것을 얻을 수 있도록 하는 방법으로 data block을 mixing하는 방법을 제안하였다. 그러나 이 방법은 프라이버시를 보호 하지 않으며, 매우 많은 사용자들을 가정할 때 비효율적인 방법으로 평가된다.

[5]에서는 Attribute based encryption (ABE)을 이용하여 게시자와 사용자들 간에 key를 미리 공유하지 않고, 콘텐츠에 접근 할 수 있는 속성만을 사용하여 콘텐츠를 암호화 하여 원하지 않는 속성을 가진 사용자는 콘텐츠에 접근하지 못하게 하는 방법이다. 특히 콘텐츠 이름도 같은 방법으로 암호화 하고, 이를 이웃 라우터로의 전송 여부를 결정할 수 있는 broker라는 기능을 둠으로써 사용자들의 프라이버시를 보장하도록 하였다. 그러나 이 방법은 콘텐츠 이름의 암호화로 name- based 라우팅 아키텍처의 ICN에 부담을 주고 실제 방대한 스케일 위에서 효율적으로 운영 될 수 있는지 검증이 필요하다.

3.2. Routing 공격 및 대응 방법

고전적으로 라우팅 공격에는 DDoS와 스푸핑 공격이 있다. DDoS 공격에는 라우터 및 네트워크 등의 리소스를 고갈시키는 방법과 timing 공격 두 개로 나눠지며 네트워크 중간에서 행해지는 스푸핑 공격에는 jamming, hijacking, interception 등이 있다. DDoS는 host- centric 구조와 비슷하게 콘텐츠 요청들을 다량으로 발생 시켜 목표물의 자원을 고갈시키는 공격이다. ICN에서 다량의 콘텐츠 요청은 주변 라우터에 전송되고 이에 대응되는 콘텐츠가 여러 경로를 통해 재전송되면서 라우팅 테이블이 공격자의 요청들로 저장/처리되는 과정을 거치면서 라우터의 프로세서 및 메모리를 고갈 시키고 네트워크 전체를 혼잡하게 하며 합법적 요청자의 응답속도를 지연시킨다. 이런 ICN infrastructure의 특성을 반영한 공격을 infrastructure 공격이라 한다. 자원을 고갈 시키는 또 다른 공격으로 특정 owner가 가지고 있는 콘텐츠를 계속 요청함으로써 콘텐츠 배포자(Content Source)에 부담을 주는 것을 source 공격, 특정 라우터 주변을 돌면서 특정 라우터에 다량의 콘텐츠 요청을 하는 mobile blockade공격 [6] 또한 공격자가 특정 노드를 장악해 제한된 수 이상의 요청을 하도록 하고 특정 개수 이하로만 요청을 받아들여 나머지는 무시하게 함으로써 전체 네트워크에 부담을 주는 flooding 공격 등이 있다. request timeout을 증가 시켜 많은 요청을 하게 하는 timing 공격도 DDoS공격에 포함된다. 또한 공격자와의 공유 link에 많은 request를 보내는 jamming 공격, 거짓 라우팅 정보를 주변에 보내 적법한 사용자의 콘텐츠 요청이 제대로 응답되지 않게 하는 hijacking 공격, 거짓 라우팅 정보를 보내고 그 라우팅 정보에 속한 요청이 들어왔을 때 이웃 라우터에 전달한 후 요청 된 콘텐츠를 받아 실제 요청자에게 콘텐츠를 전송하여 공격자는 요청자가가 모르게 요청자가 원하는 콘테츠 정보를 중간에서 가로채어 정보를 얻어냄으로써 요청자의 프라이버시를 침해하는, interception 공격 등이 있다. 즉 ICN의 특성을 이용한 라우팅 공격은 분산공격, 자원고갈, path infiltration의 원인이 되며 그로 인한 프라이버시 침해에 영향을 끼치게 된다.

DoS/DDoS의 방지를 위해 일반적으로 사용자가 발생 시키는 패킷의 양을 제한하는 방법이 제안되었으나 ICN과 같이 호스트 ID가 없는 환경에서는 이를 적용하기가 쉽지 않다. [7]에서는 각 라우터에서 들어오고 나가는 요청수를 제한하여 flooding으로 인한 성능 저하를 방지 하고 또한 의심되는 name-space를 고립시키고 주변 라우터에 알리는 방법을 제안하고 있다. [8]에서는 expired된 interest(유효하지 않은 콘텐츠에 대한 요청)를 찾기 위해 여러 metric parameter를 사용하기도 한다. [9]에서는 콘텐츠 요청과 이에 응답된 콘텐츠의 기록을 유지함으로써 악의적 요청에 대한 통계적 수치를 구하고 이를 이용하여 요청을 수행하는데 제한을 두는 방법을 이용한다. [10]에서는 ranking 알고리즘을 이용하여 스팸을 걸러내는 방법을 제안하였다. IP 기반의 네트워크에서는 주로 end 단에서의 traffic 혼잡이나 서비스 거부를 야기하지만 ICN에서는 모든 라우터에 무리를 줄 수 있는 특징 때문에 그 해결 방안도 살펴본바와 같이 라우터 단에서 이루어지는 경향이 있다.

3.3. Caching 공격 및 대응 방법

ICN 아키텍처에서는 콘텐츠나 요청이 라우팅 되는

과정에서 노드들에 cache 된다. 이런 특징으로 인한 다양한 공격 형태가 나타나는데 time analysis, bogus announce- ment, cache pollution등이 그 예이다. 어떤 콘텐츠가 source로부터 공격자까지 오는 대략의 시간을 알 때 그 콘텐츠가 실제 도착하는 시간이 source로부터 도착하는 시간보다 작을 때에는 중간에 콘텐츠가 cache 되어 있다고 예측할 수 있으며 근처에 있는 다른 사용자가 그 콘텐츠를 이전에 요청 했을 수 있다고 추정함으로써 일종의 프라이버시 침해를 할 수 있게 된다. 또한 콘텐츠나 cache된 복사본들에 대해 공격자는 가짜 업데이트 알림을 라우팅 convergence 시간보다 자주 보냄으로써 라우터들이 실제 저장된 콘텐츠 update 시도를 하게 되고 이로 인해 합법적 콘텐츠 전송이 제대로 되지 않게 하는 bogus announcement 공격이 있다. 다량의 거짓 업데이트 announcement는 불필요한 콘텐츠 관련 프로세스를 야기 시켜 전체 네트워크에 부담을 주게 된다. 또한 ICN 네트워크 내의 콘텐츠 인기도등을 바꾸기 위한 공격이 가능하다. 요청이 드물 수 있는 콘텐츠에 대한 요청을 다수 내보냄으로서 그런 콘텐츠들로 cache를 채우게 되고 실제 인기 있는 콘텐츠 요청은 다시 source 까지 가서 받아 오게 되는 일들이 생기게 된다. 이렇게 무작위 콘텐츠를 요청하는 공격을 random(unpopular) request 공격이라 한다. 이런 cache 관련 공격에 대한 솔루션으로 현재 단일 cache server를 이용하는 시스템을 위한 것은 많으나 다수의 노드에 cache되는 ICN 구조에는 그대로 적용하기가 쉽지 않다. [11]의 random 공격에 대한 솔루션은 콘텐츠 요청의 분포를 보고 인기, 비인기 콘텐츠를 구별하여 filtering하는 방법을 사용한다. 그러나 이 방법은 scalability면에서 적합한지 검증이 필요하다. time analysis 공격에 대한 대책으로 [12]에서는 중복된 요청들에 대해 random delay를 추가 하여 콘텐츠를 보내는 방법을 사용하여 시간차를 이용한 공격이 어렵게 하였다. 그러나 이는 라우터 마다 다른 caching 정책을 고려하지 않았으며 공격자가 target 사용자와 가까이 있다는 가정을 하고 있다. [13]에서는 콘텐츠를 받은 사용자들에 의해 생성되는 랭킹 알고리즘을 이용하여 cache할 콘텐츠를 선택하는 방법이다. 이를 통해 실제 자주 요청되는 콘텐츠와 그렇지 않은 것을 구별하여 cache하게 된다.

3.4. 그 외 공격 및 대응 방법

그 외 공격으로 packet mistreatment, breaching signer's key, unauthorized access 등의 공격이 있다. Packet Re tran- smission은 공격자가 ICN 네트워크에 접근하여 콘텐츠를 수정하거나 콘텐츠 응답을 여러 번 하거나 합법적 사용자처럼 콘텐츠를 생성하여 ICN네트워크에 혼란을 주는 공격이다. 또한 ICN 콘텐츠의 생성자의 서명 정보를 이용하여 생성자의 서명 key를 훼손하는 것이다. 이는 쉽지 않은 공격이나 공격이 성공 했을 때 ICN에 큰 impact가 될 수 있다. 또한 ICN이 여러 노드에 콘텐츠의 복사본들을 cache하므로 콘텐츠에 접근하는 것이 비교적 쉬어 허용되지 않는 콘텐츠 접근, 또한 가능하게 된다.

현재 나와 있는 많은 security 솔루션들은 IP 네트워크 구조와는 다른 cache 정책 때문에 ICN에 바로 적용하기가 어려운 것들이 많다. 권한이 없는 콘텐츠 접근을 막기 위한 방법으로 [9]에서는 access control provider (ACP)를 두고 콘텐츠 제공자가 원하는 공유자를 등록할 수 있게 하고 사용자는 그 ACP에서 자격을 취득 후 콘텐츠를 얻어 오는 방법을 제안하고 있다. [14]에서는 ICN 구조에서 스마트 그리드 환경의 많은 데이터량을 안전하게 보호하는 방법으로 id-based encryption을 이용한 암호화 방법을 제안하고 있다. 그러나 id- based encryption은 마스터키를 발급하는 서버가 필요하므로 분산 환경의 ICN에 적합한지 검증이 필요하다. 또한 [15][16]에서는 web application attack에 관해 서버 사이드와 클라이언트 사이의 공유되는 secret이 없는 솔루션을 제안하고 있어 ICN에 적용 가능성을 시사 하기도 한다.

Ⅳ. 결 론

미래 인터넷은 결국 매우 많은 콘텐츠들을 어떻게 보급하느냐에 그 승패 여부가 달려있다고 할 수 있다. 이를 위해 ICN으로 대표되는 DONA, NetInf, NDN, PURSUIT 등과 같은 많은 architecture들이 제안되었다. 이들의 큰 특징으로 address 등의 location에 의존하지 않는 naming, network 내의 노드들에 cache하는 in-network caching, 그리고 IP 주소로 잘 정의된 프로토콜에 의해 routing이 되는 것이 아니라 요청된 콘텐츠

이름을 찾아가는 name-based 라우팅 등이 있다. 아래 표 1은 그런 특징과 그에 관련된 security 특성의 연관성을 표시한 것이다.

표 1을 보면 알 수 있듯이 ICN의 security는 특히 가용성과 프라이버시 부분에 취약하다[17]. 가용성 부분이 취약했던 이유는 다량의 불필요한 콘텐츠 요청을 보낼 수 있는 것, 또한 네트워크 노드들에 불필요한 콘텐츠를 cache하게 할 수 있기 때문이었다. 또한 사용자의 콘텐츠 요청에 접근 하거나 timing 분석을 통해 요청자의 일부 정보를 취득해 프라이버시 침해가 생기게 된다. 지금의 ICN 솔루션들은 ICN 고유의 아키텍처 및 그로 인한 공격 방법을 고려하고 있다. 이후로도 ICN의 security는 다음과 같은 점을 고려하여 해법을 찾아야 할 것이다.

- ICN 아키텍처의 특징인 콘텐츠 중심의 구조를 고려하여 콘텐츠 자체의 안전성에 집중해야 한다.
- IP 구조에 비해 프라이버시에 취약한 부분이 있으므로 이를 고려해야 한다.
- 악의적 게시나 요청은 ICN의 security를 위협하는 큰 요소이므로 부적합한 요청을 구별 할 수 있는 방법이 여럿 제안되었으나 앞으로도 이를 고려한 솔루션들이 필요하다.
- ICN은 사용자당 콘텐츠 요청 수를 제한하기가 어려워 이에 의한 대책 또한 필요하다.

〔표 1〕 공격과 security 관계

	기밀성	무결성	가용성	프라이버시
Naming	L		L	H
Routing	L		H	
Caching			L	M

L: 관계 적음 M: 중간 H :높음

참 고 문 헌

[1] Cisco Visual Networking Index: Forecst and Methodology, 2015-2020, white paper

[2] A. M. K. Pathan and B. Rajkumar, “A taxonomy and survey of content delivery networks,” Grid Comput. Distrib. Syst. Lab., Univ. Melbourne, Parkville, Vic, Australia, Tech. Rep., 2007.

[3] E. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, “A survey and comparison of peer-to-peer overlay network schemes,” *IEEE Commun. Surveys Tuts.*, vol. 7, no. 2, pp. 72-93, 2005.

[4] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, “On preserving privacy in content-oriented networks,” in *Proc. ACM SIGCOMM Workshop CN*, Aug. 2011, pp. 19-24.

[5] M. Ion, J. Zhang, M. Schuchard, and E. M. Schooler, “Toward contentcentric privacy in ICN: Attribute-based encryption and routing,” in *Proc. ASIA CCS*, Hangzhou, China, Aug. 2013, pp. 513-514.

[6] G. Tyson, N. Sastry, I. Rimac, R. Cuevas, and A. Mauthe, “A survey of mobility in information-centric networks: Challenges and research directions,” in *Proc. NoM*, New York, NY, USA, Jun. 2012, pp. 1-6.

[7] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, “DoS & DDoS in named data networking,” in *Proc 22nd Int. Conf. Comput. Commun. Netw.*, 2013,pp.1-7.

[8] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, “Poseidon: Mitigating interest flooding DDoS attacks in named data networking,” in *Proc. IEEE 38th Conf. Local Comput. Netw.*, Oct. 2013, pp. 630-638.

[9] N. Fotiou, G. F. Giannis, and G. C. Polyzos, “Access control enforcement delegation for information-centric networking architectures,” in *Proc. 2nd Edition ICN Workshop Inf.-Centric Netw.*, Aug. 2012, pp. 85-90.

[10] N. Fotiou, G. F. Marias, and G. C. Polyzos, “Fighting spam in publish /subscribe networks using information ranking,” in *Proc. 6thEURO-NF Conf. NGI*, Paris, France, Jun. 2010, pp.1-6.

[11] M. Xie, I.Widjaja, andH.Wang, “Enhancing

cache robustness for contentcentric networking," in *Proc. IEEE INFOCOM*, 2012, pp. 2426-2434.

[12] A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "Protecting access privacy of cached contents in information centric networks," in *Proc. SIGCOMM*, Hong Kong, China, May 2013, pp. 1001-1003.

[13] C. Ghali, G. Tsudik, and E. Uzun, "Needle in a haystack: Mitigating content poisoning in named-data networking," in *Proc. SENT*, San Diego, CA, USA, 2014, pp. 1-10.

[14] B. Vieira and E. Poll, "A security protocol for information-centric net- working in smart grids," in *Proc. SEGS*, Berlin, Germany, Nov. 2013, pp. 1-10.

[15] A. Barua, H. Shahriar, and M. Zulkernine, "Server-side detection of content sniffing attacks," in *Proc. 22nd Annu. ISSRE*, Hiroshima, Japan, Nov. 2011, pp. 20-29.

[16] H. Shahriar and M. Zulkernine, "Client-side detection of cross-site request forgery attacks," in *Proc. 21st IEEE ISSRE*, San Jose, CA, USA, Nov. 2010, pp. 358-367.

[17] E. AfAllah, H.Hassanein and M.Zulkernine."A Survey of Security Attacks in Information-Centric Networking", in I*EEE Comm. Survey & Tutorials*, Jan. 2015, pp 1441-1454

〈저 자 소 개〉

허 미 숙 (Misuk Huh)
정회원

1990년 2월 : 서울대학교 수학과 졸업
1992년 2월 : 서울대학교 수학과 석사
2001년 8월 : 서울대학교 수학과 박사
2001년 12월~현재 : 삼성 종합기술원/삼성 전자
관심 분야 : 정보보호