Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.155

콘텐츠 중심 네트워킹 환경에서의 Fake Data Filtering Method 연구*

김 대 엽†‡
수원대학교

A Study on Fake Data Filtering Method of CCN*

DaeYoub Kim†‡
Suwon University

요 약

네트워크 성능 향상을 위하여 콘텐츠 중심 네트워킹(CCN)은 콘텐츠 전송 경로 상에 있는 네트워크 중간 노드들이 중계하는 콘텐츠를 임시로 저장하고, 중간 노드가 임시 저장된 콘텐츠에 대한 요청 메시지 (Interest)를 수신하면, 해당 노드는 Interest를 콘텐츠 제공자에게 전송하지 않고, 임시 저장된 콘텐츠를 응답 메시지 (Data)로 콘텐츠 요청자에게 전송한다. 중간 노드에 의한 Interest 처리 방식은 효율적인 콘텐츠 전송을 가능케 할 뿐만 아니라 콘텐츠 제공자에게 집중되는 Interest를 분산 처리되게 함으로써 콘텐츠 제공자 또는 그 주변 네트워크 노드에서 발생하는 네트워크 병목현상을 효과적으로 해결할 수 있다. 이를 위하여 CCN 노드는 수신된 Data를 임시 저장하는 Content Store와 Data를 요청자에게 전송하기 위해 Interest 유입 경로를 저장/관리하는 Pending Interest Table (PIT)와 같은 자원을 추가적으로 운영한다. 그러나 공격 목표 노드에 대량의 Fake Interest을 전송하여 특정 노드의 PIT 자원을 고갈시켜 네트워킹을 방해하는 서비스 거부 공격에 대한 가능성이 제기 되었다. 본 논문에서는 앞서 제기된 Fake Interest를 이용한 PIT 공격 및 대응 방안을 살펴보고, Fake Data를 이용한 새로운 공격 방법 및 대응 방안을 제안한다. 또한, 제안된 방식을 시뮬레이션을 통하여 그 성능을 평가 한다.

ABSTRACT

To enhance network efficiency, content-centric networking (CCN) proposes that intermediated network nodes on a content-delivery path temporally cache transmitted contents. Then if an intermediated node receives a content request message (Interest) for previously cached content, the node directly transmits the cached content as a response message (Data) to requestors and finishes the transmission of the received Interest. Since Interest is performed by intermediated network nodes, it is possible to efficiently transmit contents and to effectively solve a network congestion problem caused around contents sources. For that, CCN utilizes both content store to temporarily cache content and pending Interest table (PIT) to record Interest incoming Face. However, it has mentioned the possibility of denial service attack using both the limitation of PIT resource and fake Interests. In this paper, we briefly describe the presented PIT flooding attack utilizing fake Interest. Then we introduce new attack possibility using fake Data and propose a countermeasure for the proposed attack. Also we evaluate the performance of our proposal.

Keywords: Future Internet, CCN, DoS/DDoS Attack, Attack Detection

접수일(2013년 11월 5일), 게재확정일(2013년 12월 24일)
* 본 연구는 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구 결과임 (No. NRF-2013R1A1A2008389).
† 주저자, daeyoub69@suwon.ac.kr
‡ 교신저자, daeyoub69@suwon.ac.kr (Corresponding author)

I. 서 론

초기 인터넷은 호스트들 사이의 안전한 네트워크 연결을 제공할 목적으로 제안되었기 때문에 대용량 콘텐츠 전송 시 발생되는 네트워크 병목현상, 취약한 보안 구조로 인한 침해 사고, 호스트의 빈번한 이동으로 발생하는 비효율성과 같은 다양한 문제점들과 그 해결 방안을 사전에 고려하지 못했다 [1]. 이와 같은 문제점들로 인한 인터넷의 비효율성을 개선하고 대용량 멀티미디어 콘텐츠 서비스를 보다 효과적으로 지원하기 위하여 다양한 미래 인터넷 기술 연구가 진행되고 있다 [2-4].

미래 인터넷 기술 중 하나인 콘텐츠 중심 네트워킹 (Content-Centric Networking, CCN)은 사용자 기기 또는 서버와 같은 사용자 노드 (Edge Node) 뿐만 아니라 네트워킹 패킷을 중계해 주는 라우터와 같은 중간 네트워크 노드에 콘텐츠를 임시 저장할 수 있는 기능(Caching)을 구현하고 이를 효과적으로 지원하기 위하여 콘텐츠 이름에 기반 한 패킷 포워딩 기술을 제공함으로써 콘텐츠를 보다 효과적인 전송할 수 있도록 한다[3,4].

CCN은 기본적으로 콘텐츠 요청 메시지 (Interest)와 응답 메시지(Data)를 이용한 네트워킹을 제공하며, 이를 효과적으로 구현하기 위하여 콘텐츠를 임시 저장 메모리 (Content Store, CS)와 Interest 유입 경로를 기록/관리하는 Pending Interest Table (PIT)와 같은 자원을 추가적으로 운영한다. 그러나 추가된 자원 중 하나인 PIT를 Fake Interest를 이용하여 Flooding 시키는 서비스 거부 공격(Denial of Service Attack, DoS Attack)에 대한 가능성이 최근 제기 되었다 [5-7].

본 논문에서는 CCN의 추가 자원인 CS를 대상으로 한 새로운 DoS Attack 방법을 소개하고, 이와 같은 공격을 효과적으로 대응하기 위한 방안을 함께 제안한다.

II. 콘텐츠 중심 네트워킹

효율적인 네트워킹을 위하여 CCN은 라우터와 같은 네트워크 노드가 임시 저장하고 있는 Data를 네트워킹에 활용 한다. 이를 위하여, 네트워크 노드가 Interest를 수신하면, 해당 노드의 CS에 임시 저장된 Data 중에 수신된 Interest에 대응되는 Data가 있는지를 우선 확인한다. 만약 수신된 Interest에 대응하는 Data가 CS에 존재하면, 해당 Data를 요청자에게 전송하고 수신된 Interest의 중계를 완료한다. 이와 같이 중간 네트워크 노드에 의하여 Interest가 직접 처리되기 때문에 콘텐츠 제공자 (Content Source/Provider)에게 집중되는 Interest를 분산처리 할 수 있을 뿐만 아니라 전체 네트워크 트래픽 양을 효과적으로 줄일 수 있다.

중간 네트워크 노드에 임시 저장된 콘텐츠를 네트워킹에 효율적으로 활용하기 위하여 CCN은 IP 주소와 같은 호스트 Identity 대신 계층화된 콘텐츠 이름을 이용하여 Interest와 Data를 처리 한다 [3,4,8]. 또한, 요청자의 프라이버시 보호를 위하여 Interest는 콘텐츠 요청자에 대한 정보를 포함하지 않는다. 그러므로 요청된 Data를 해당 요청자에게 전송하기 위하여, Interest를 수신한 CCN 노드는 Interest의 유입 경로 (Face)를 PIT에 저장/관리한다. 또한, CCN 노드가 Data를 수신하며, PIT를 참조하여 Data에 대응되는 Interest가 유입된 Face를 확인하고, Data를 해당 Face를 통하여 전송 한다. 즉, Interest의 유입 경로를 통하여 Data가 전송될 수 있도록 관리한다.

그림 1는 이와 같은 Interest와 Data 처리 절차를 예를 이용하여 설명한다. (1)~(6)은 Interest 처리 절차를 설명하고, (7)~(10)은 Data 처리 절차를 설명한다.

(1) Face 0을 통하여 Interest가 수신된다.
(2) CS에 수신된 Interest에 대응되는 Data가 저장되어 있는지 확인한다. 만약 저장되어 있다면, Face 0을 통해 해당 Data를 전송한다.
(3) CS에 수신된 Interest에 대응되는 Data가 저장되어 있지 않다면, PIT에 Interest에 대응되는 정보가 있는지 확인한다. 만약 있다면, 해당 정보의 incoming Face 필드에 Face 0을 추가한 후, Interest 처리를 완료한다.
(4) PIT에 대응되는 정보가 없다면, FIB (Forwarding Information based) 테이블을 참조하여 수신된 Interest를 전송할 Face (ex. Face 2)를 선택한다.
(5) PIT에 수신된 Interest의 incoming Face 정보를 기록한다.
(6) FIB에서 선택한 Face를 통하여 수신된 Interest를 전송한다.
(7) Data가 수신된다.
(8) PIT에 수신된 Data에 대응되는 Interest 정

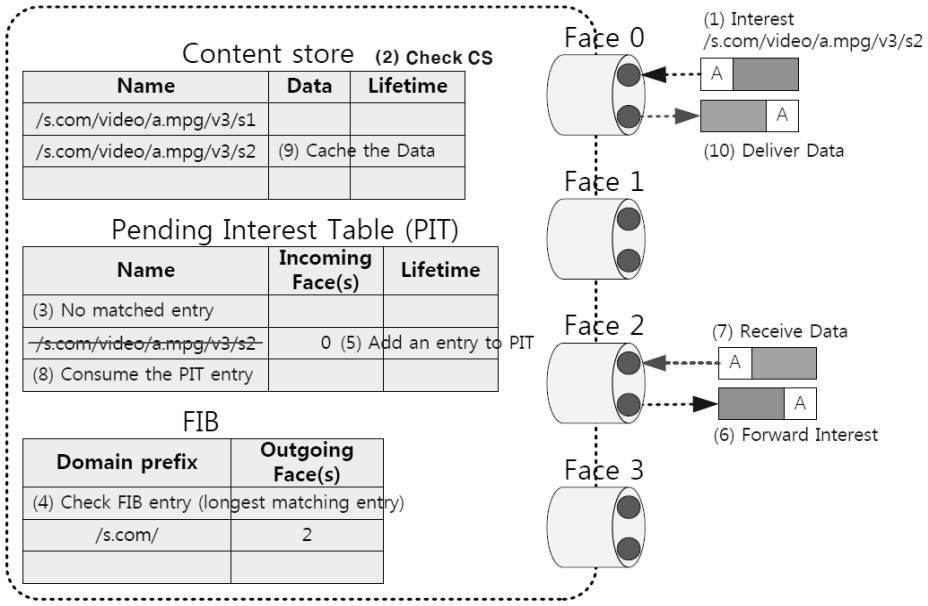


Fig.1. CCN Interest/Data Forwarding Model

보가 있는지 확인한다. 만약 없으면, 해당 Data는 폐기처리 된다.

(9) PIT에 수신된 Data에 대응하는 Interest 정보가 존재하면, CS에 Data를 저장한다.

(10) Data를 PIT의 대응되는 Interest 정보의 incoming Face들을 통해서 전송한다.

III. PIT 취약점을 이용한 CCN 노드 공격

대량의 Interest가 CCN 노드로 유입되어 노드의 PIT 자원이 모두 소모되면, 해당 노드의 PIT에 가용 자원이 생길 때 까지 수신된 Interest를 폐기 하거나 또는, 새로운 Interest를 PIT에 기록하기 위해서 기존의 Interest 정보를 삭제해야 한다. 그러므로 공격 Interest가 대량으로 유입되어 PIT의 자원이 고갈되면, 전자의 경우 수신된 정상 Interest가 폐기 처리되고, 후자의 경우 정상 Interest 정보가 PIT에 기록되었다 할지라도 이후에 공격 Interest가 대량으로 유입되면 이들 공격 Interest 처리를 위하여 PIT에 기록된 정상 Interest가 삭제되기 때문에 대응되는 Data를 수신하더라도 이를 처리하지 못하고 폐기하게 된다. 그러므로 PIT를 어떤 식으로 관리하더라도 정상적인 네트워킹을 방해할 수 있다 [6,7].

그림2는 [6]에서 제안된 Interest를 이용하여 공격 목표 노드의 PIT 자원을 소진시켜 정상적인 네트워킹을 방해하는 시나리오를 설명한다. 공격 Interest를 공격 목표 노드 (CR1)까지 전송하기 위해서 공격에 사용되는 Interest는 다음과 같은 세 가지 조건을 만족해야 한다.

(조건 1) 공격 Interest의 Content Name은 CR1의 Domain Name Prefix을 최상위 Name Component로 사용한다.

(조건 2) 공격 Interest의 Content Name과 같은 Content Name을 갖는 콘텐츠가 중간 노드의 CS에 저장되어 있지 않아야 한다.

(조건 3) 공격 Interest의 Content Name이 중간 노드의 PIT에 저장된 Interest의 Content Name과 같지 않아야 한다.

이와 같은 조건들을 만족하는 공격 Interest를 생성하기 위하여 공격자는 CR1의 Domain Prefix Name '/Domain1'을 Content Name의 최상위 Name Component로 고정하고, 하위 Name Component들을 random하게 바꿔가며 공격 Interest를 생성한다. 이렇게 생성된 공격 Interest들을 수신한 중간 노드들은 CS와 PIT에 수신된 공격 Interest의 Content Name과 같은 정보가 없음을 확인하고, 공격 Interest를 CR1로 전송한다.

공격용 Interest가 CR1에 전송되면, CR1은 해당 Interest를 PIT에 기록하고 처리한다. 그러나 공

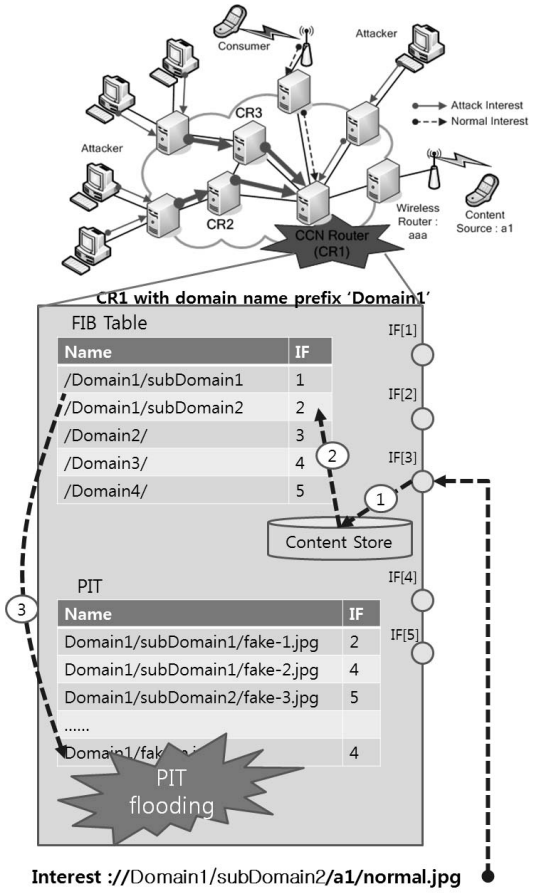


Fig.2. CCN PIT Flooding Attack

격용 Interest는 존재하지 않는 콘텐츠에 대한 요청 메시지이므로 용청된 Data가 전송될 수 없기 때문에 공격용 Interest 정보는 PIT Entry의 생명주기 동안 PIT 자원을 점유한다.

이와 같이 대량의 공격용 Interest가 지속적으로 생성/전송되어 CR1의 PIT 자원이 모두 소진되면, 이 후에 수신되는 Interest를 정상적으로 처리할 수 없게 된다. [6, 7]에서는 이와 같은 공격 시나리오를 바탕으로 정상 Interest의 drop rate을 측정 결과를 제시하였다.

IV. CS 취약점을 이용한 CCN 노드 공격

CS는 네트워킹 성능을 향상시키기 위해 CCN에 새롭게 추가된 자원이다. CCN 노드가 CS에 저장되어 있는 Data에 대응되는 Interest를 수신하면, 해당 Interest를 Content Source로 전송하지 않는 대신에 CS의 Data를 해당 Interest가 유입된 Face로 전송한다. 그러므로 CS는 CCN 성능에 직접적인 영향을 준다.

CS를 공격 목표 자원으로 고려 할 때 두 가지 공격 모델을 제안할 수 있다. 첫 번째 공격 모델은 중간 노드의 CS에 사용자들의 요청이 없는 콘텐츠(Non-popular Content)를 대량으로 저장시킴으로써 실제 요청이 많은 콘텐츠 (Popular Content)가 임시 저장되지 못하도록 한다. 두 번째 공격 모델은 popular content의 Fake Data를 생성/전송하여 실제 Data가 전송 되지 못하도록 한다.

본 논문에서는 첫 번째 공격 모델을 CS Pollution Attack이라하고, 두 번째 공격 모델을 CS Poisoning Attack이라 부르기로 한다. 본 절에서는 새롭게 추가된 자원인 CS에 대한 Pollution 및 Poisoning 취약점에 대하여 살펴보고, CS Poisoning 취약점을 이용한 공격 시나리오를 소개한다.

4.1 CS Pollution Attack

CCN 노드가 Data를 수신 했을 때, 해당 CCN 노드의 CS 저장 공간이 부족할 경우, CCN 노드는 다음과 같은 2가지 방안 중 하나를 선택해서 처리하게 된다.

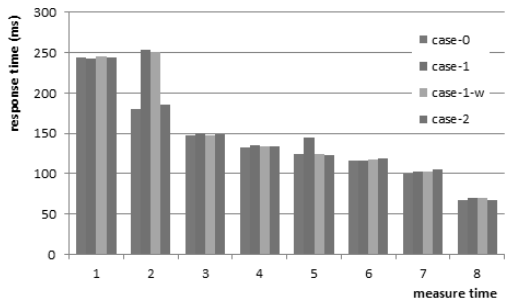
(경우 1) 수신된 Data를 CS에 저장하지 않고 PIT를 참조하여 전송한다.

(경우 2) CS의 entry 중 하나를 정책에 따라 삭제한 후, 수신된 Data를 CS에 저장하고 PIT를 참조하여 전송한다.

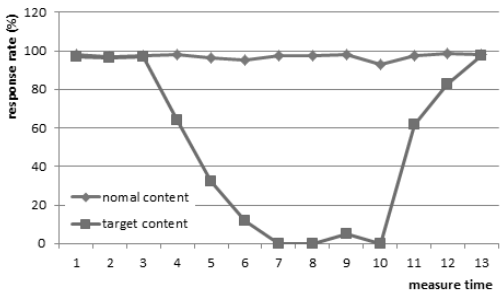
경우 1에서 중간 노드에 Data가 임시 저장 되지 않더라도 Data는 정상적으로 요청자에게 전송된다. 또한 해당 노드 외에 Data 전송 경로 위에 있는 다른 노드의 CS에 저장될 수 있다. 그러므로 해당 Data를 요청하는 Interest는 Data를 저장한 다른 노드에 의해서 처리 될 수 있기 때문에 전체 네트워크 성능에도 큰 차이를 보이지 않을 수 있다.

또한, Data의 요청 빈도에 따라 임시 저장 노드를 결정하는 방법과 같은 다양한 임시 저장 정책(Caching Policy)들이 제안되고 있다 [9]. 이러한 임시 저장 정책을 적용하면, non-popular content가 임시 저장되는 노드를 제한할 수 있다.

경우 2에서 CCN 노드가 수신된 Interest에 대응되는 Data를 CS에서 찾을 수 없으면 CCN 노드는 Interest를 다음 노드로 전송한다. 최악의 경우 전송



(A) CS Pollution Attack



(B) CS Poisoning Attack

Fig.3. CCN CS Attack Impact Evaluation

구간에 있는 모든 노드들이 대응되는 Data를 CS에 저장하고 있지 않아도 Interest는 Content Source로 전송되어 정상적으로 처리된다.

그러므로 두 경우 모두 Interest와 Data의 전송은 정상적으로 운영되기 때문에 CS Pollution 공격의 영향은 매우 적다. 그림 3-(A)은 CS Pollution 공격 시, 정상 Interest에 대한 반응 시간을 나타낸다. 측정에 사용된 네트워크 및 환경 구성은 6절에서 설명한 구성을 따른다. 공격 목표 설정 및 진행은 다음과 같이 수행된다.

(1) 공격 목표가 되는 Domain을 선택한다.

(2) 공격 목표 Domain의 Edge 노드의 parent 노드 하나를 선택하여 해당 노드에 대하여 특정 시각 (measure time 2)에 해당 노드의 CS가 공격 Data로 Flooding 된 상태를 가정한 후 시간에 따른 응답 소요 시간을 측정한다.

(3) 공격 목표 Domain의 Gateway 노드가 measure time 5에 동일한 공격을 받는다고 가정하고 응답 소요 시간을 측정한다.

Case-0는 공격이 진행되지 않는 정상 상태 일 때의 응답 시간을 나타낸다. Case-1은 임시 저장 정책이 적용되지 않은 Basic CCN에서 (경우 1)에서 설명한 공격이 진행될 때의 응답 시간을 의미한다. Case-1-w은 임시 저장 정책으로 WAVE를 적용하였을 때 (경우 1)의 공격이 진행된 상황에서의 응답 시간을 나타낸다. Case-2는 (경우 2)의 공격을 가정했을 때 응답 시간을 의미한다. 그림 3-(A)에서 알 수 있듯이, 공격이 진행되면 일시적으로 응답 시간이 느려지지만, 일정 시간 후에는 정상 상태와 큰 차이를 보이지 않음을 알 수 있다. 이는 CCN의 특성 상 Data를 임시 저장하는 노드의 수가 점진 적으로 증가하기 때문이다.

또한, CCN 노드는 수신된 Data에 대응하는 Interest 정보가 PIT에 기록되어 있을 때에만 CS에 수신된 Data를 저장한다. 그러므로 CS Pollution 공격에 이용하기 위해서는 공격 목표 노드의 Domain 내부에 위치한 노드와 공격자 간의 공모가 필수적으로 요구된다. 이러한 공모는 네트워크 모니터링을 통하여 이상 징후를 감지할 수 있다. 특히, 공격 목표 노드의 특정 Face를 통하여 전송되는 Interest와 Data의 양을 모니터링 함으로써 별도의 모니터링 시스템 구축 없이도 이상 징후를 미연에 감지할 수 있으며, 이러한 경우, 공격에 사용되는 Face로부터 유입되는 Data의 Caching을 금지시키는 CS 정책에 따라 공격을 효과적으로 무력화 시킬 수 있다 [10,11].

4.2 CS Poisoning Attack

Data를 수신한 CCN 노드는 PIT의 Interest 유입 정보를 참조하여 수신된 Data를 전송할 Face를 결정하고 Data를 해당 Face를 통하여 전송한다. Data를 전송한 후, CCN 노드는 PIT에서 대응되는 정보를 삭제한다. CS에 Data가 저장된 후에 해당 Data를 요구하는 Interest를 수신하면, 노드는 CS를 우선 확인하여 저장되어 있는 Data를 전송하고 수신된 Interest의 처리를 종료한다.

이와 같은 Interest와 Data 처리 방식은 CS Poisoning Attack에 대하여 취약점을 갖고 있다. 설명을 위하여 공격자 노드는 Interest 전송 경로 위에 있는 노드와 1-hop distance를 갖는 노드 중 하나로 가정한다. 그러나 FIB Poisoning Attack을 통하여 이와 같은 가정 없이도 공격은 가능하다. 그림 4는 공격 절차를 설명한다.

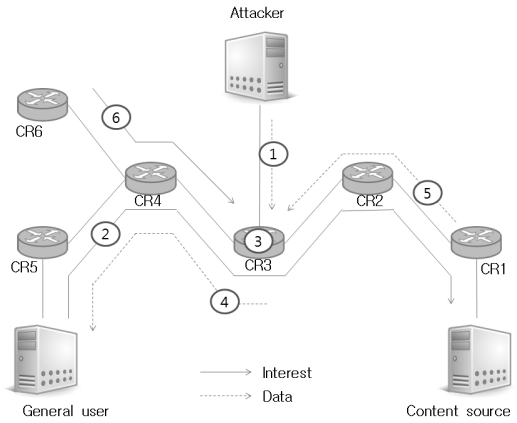


Fig.4. CS Poisoning Attack Scenario

(1) 공격자는 공격 목표가 된 콘텐츠의 Content Name과 같은 이름을 갖는 공격 용 콘텐츠(Fake Data)를 생성한다. 공격자는 생성한 Fake Data를 사용자가 생성한 Interest가 경유하여 전송될 중간 노드 CR3으로 반복하여 전송한다. Fake Data를 수신한 CR3은 PIT를 확인하여 대응하는 Interest 정보가 없으면, 수신된 Fake Data를 폐기한다.

(2) 사용자가 공격 목표 콘텐츠를 이용하기 위하여 Content Source에게 Interest를 전송하면, Interest는 CR3를 경유하여 Content Source에게 전송된다. CR3는 수신된 Interest 정보를 PIT에 저장한다.

(3) CS3가 공격자에 의해 반복적으로 전송된 Fake Data를 다시 수신되면, CR3는 PIT에 대응하는 Interest 정보가 있으므로 수신된 Fake Data를 CS에 저장한다.

(4) CR3는 PIT에서 해당 Interest 정보를 삭제한 후, Fake Data를 사용자에게 전송한다.

(5) 이 후, CR3가 Content Source로부터 Data를 수신하면 PIT에서 해당 Interest 정보가 삭제되었기 때문에 수신된 정상 Data는 폐기 처리 된다.

(6) CR3가 저장한 Fake Data의 Content Name과 동일한 Data를 요청하는 Interest가 다시 수신하면, CR3는 CS에 저장되어 있는 Fake Data를 응답으로 요청자에게 전송한 후, 수신된 Interest 처리를 중단한다.

그러므로 CR3에 Fake Data가 저장되어 있는 동안 실제 Data는 정상적으로 사용자들에게 전송될 수 없다. 또한, CS에 저장되어 있는 Data는 주기적으로 또는 정책에 따라 삭제하는 경우에도 단계 (1)에서 공격자가 계속하여 Fake Data를 전송하기 때문에 반복되는 공격을 처리할 수 없다.

그림 3-(B)은 CS Poisoning 공격 시 콘텐츠 배포 성공률을 나타낸다. 측정에 사용된 네트워크 및 환경 구성은 5절에서 설명한 구성을 따른다. 공격 목표를 특정 콘텐츠로 고정한 후, 해당 콘텐츠의 Content Source가 포함된 Domain의 Gateway 노드를 대상으로 공격을 수행한다. 또한, 노드의 CS에 저장된 Data는 고정된 생명주기 후에 삭제 되도록 설정하였다. 그림 3-(B)에서 공격은 measure time 3에서 시작되어 measure time 8까지 계속되도록 설정했다. 공격 시작 후 일정 시간이 지나면 노드에 저장된 Data가 삭제되고, 이렇게 삭제된 후에는 Fake Data만 전송 되어 응답률이 0에 가깝게 떨어지는 것을 알 수 있다. 또한 공격 중지 이후에도 Fake Data가 노드에서 모두 삭제될 때까지 정상 Data의 응답률이 정상화되지 못함을 알 수 있다.

V. CS Poisoning 공격 대응 방안

Fake Data를 이용하여 정상 Data의 전송을 방해하는 공격이 가능한 이유는 공격 단계 (3)에서 수신된 Data의 검증을 위해 PIT의 entry 중 수신된 Data에 대응되는 정보가 있는지 만을 확인하기 때문이다. 실제 CCN은 Data를 검증하기 위하여 콘텐츠 생성자의 서명을 Data에 첨부하도록 권고하고 있다. 그러나 중간 노드에서 중계하는 모든 Data의 서명을 검증하는 것은 성능 측면에서 매우 비효율적이다. 그러므로 콘텐츠 서명 검증 외에 중간 노드에서 Data를 검사할 수 있는 추가적인 방안이 필요하다.

CCN은 원칙적으로 Interest가 전송된 경로를 따라 역으로 Data가 전송된다. 그러므로 Data를 수신했을 때, Interest가 전송되지 않은 경로를 통해 Data가 수신되며, 수신된 Data는 요청에 의해 전송된 Data가 아닌 임의로 전송된 Data로 간주 할 수 있다.

본 절에서는 이렇게 Interest 전송 경로 외로 부터 전송된 Fake Data를 검사(filtering) 할 수 있도록 PIT의 구조를 개선하고, 개선된 PIT를 이용하여 Fake Data를 검사하는 절차를 제안한다.

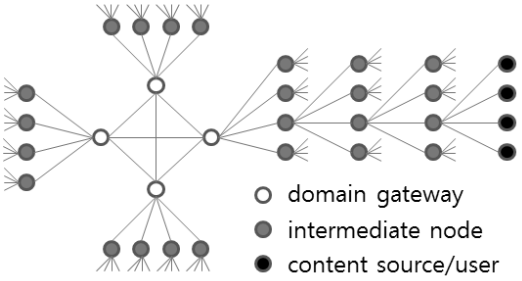


Fig.5. Network Topology for Simulation

5.1 개선된 PIT 구조

Fake Data를 이용한 공격에 대응하기 위하여 CCN 노드가 수신된 Interest의 유입 경로뿐만 아니라 전송 경로도 함께 관리할 수 있도록 PIT의 구조를 다음과 같이 개선한다.

```
PIT_EntryStr := {
 Boolean                          statue;
 String                           interest;
 Struct Face   inFases[_No_FACE];
 Struct Face   outFases[_No_FACE];
}

PIT : = {
 INT  n              umOfEntry ;
 PIT_EntryStr        entry[_No_ENTRY] ;
}
```

PIT.entry는 수신된 Interest의 유입 경로를 저장/관리한다. PIT_EntryStr의 statue는 PIT entry 정보의 상태를 의미한다. interest는 수신된 Interest의 Content Name을 저장한다.

inFases는 Interest가 유입된 Face 정보를 저장한다.

outFases는 FIB (Forwarding Information Base) Table을 참조하여 Interest를 전송한 Face 정보를 저장한다.

5.2 개선된 PIT 기반 Interest 처리 절차

i번째 Face를 통하여 Interest를 수신한 CCN 노드는 개선된 PIT를 이용하여 다음과 같은 절차를 수행한다.

(1) CS와 PIT를 참조하여 수신된 Interest에 대응되는 정보가 있는지 확인한다. 만약 대응되는 정보가 있다면 2절에서 설명된 절차를 따른 후, Interest 처리를 종료한다.

(2) 대응되는 정보가 없다면, FIB 테이블을 참조하여 수신된 Interest를 전송할 Face를 결정한다. 이렇게 결정된 전송 Face를 j번째 Face라고 하자.

(3) PIT에 수신된 Interest 정보를 저장한다. 이때, Interest의 Content Name, 유입 Face i 뿐만 아니라 FIB 참조를 통해 결정된 전송 Face j도 함께 저장한다.

(4) Interest를 Face j를 통하여 전송한다.

5.3 개선된 PIT 기반 Data 처리 절차

CCN 노드가 Face k를 Data를 수신하면, 다음과 같은 절차를 수행한다.

(1) PIT에 해당 Data에 대응하는 entry가 존재하는지를 확인한다. 즉, Data의 Content Name과 일치하는 PIT.entry[i].interest을 찾는다.

(2) PIT.entry[i].outFaces에 기록된 Face 중에 Data가 유입된 Face k와 일치하는 정보가 있는지 확인한다. 만약 기록된 Face 중에 Data 유입 Face와 동일한 정보가 없다면 해당 Data를 폐기한다.

(3) 대응하는 정보가 있다면, CS에 Data를 저장한다.

(4) PIT.entry[i].inFaces를 참조하여 Data를 해당 Face들을 통하여 전송한 후, PIT.entry[i] 정보를 PIT에서 삭제한다.

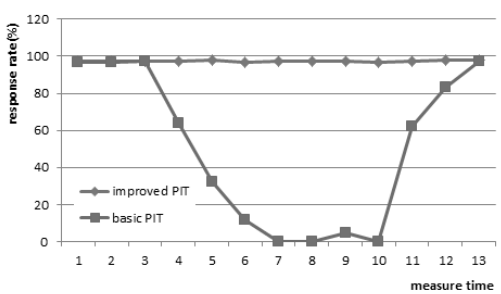


Fig.6. CS Poisoning Attack Countermeasure Result

VI. 성능 평가

그림 5는 성능평가를 위해 구성한 네트워크 구성도를 설명한다. 시뮬레이션을 위하여 4개의 네트워크 도메인에 각각 1개의 Boarder Gateway Node (BGN)가 존재하고, BGN을 root 노드로 하는 depth 4의 tree 형태의 토폴로지를 유지한다. 또한 leaf 노드를 제외한 노드는 각각 4개의 child 노드를 갖는다. root 노드부터 leaf 노드까지 모든 노드는 계층적인 도메인 이름을 할당 받아 사용하며, 콘텐츠는 leaf 노드에 대응하는 기기에서만 생성/배포 한다고 가정한다.

성능 평가를 위하여 leaf 노드들에는 16,000개의 콘텐츠가 존재한다고 가정하고, leaf 노드 중에 random하게 선택된 노드들에서 이들 콘텐츠에 대하여 9996개의 Interest를 순차적으로 생성하여 전송하도록 설정한다. 이 때, 노드 사이의 통신 속도는 BGN 까지의 거리에 반비례 하도록 설정하여 측정하였다. 즉, BGN으로부터 노드까지의 depth가 k일 때 parent 노드와의 통신 속도는 2^k ms/packet 으로 설정한다.

그림 6의 basic PIT는 4절에서 측정한 Basic CCN에 대하여 CS Poisoning 공격 전/후의 공격 목표가 된 콘텐츠의 응답률을 나타낸다. improved PIT는 CS Poisoning 공격 대응을 위하여 개선된 PIT 구조가 적용되었을 때 응답률을 나타낸다. 그림6에서 알 수 있듯이 개선된 PIT 구조와 처리 절차를 적용할 경우, 공격 진행 중에도 응답률이 그림 3-(B)의 정상 응답률과 유사한 성능을 나타냄을 알 수 있다.

VII. 결론

본 논문은 다음과 같은 두 가지 측면에서 CCN 연구 방향에 기여한다. 첫 번째로 CCN 구현을 위하여 새롭게 추가된 PIT 뿐만 아니라 CS도 DoS 공격에 취약점을 갖고 있음을 보였다. 특히, CS Pollution 공격 가능성은 이미 여러 차례 언급되었지만 CS Poisoning 공격에 대한 취약점은 본 논문에서는 처음 지적되었다.

두 번째로 CS Poisoning 공격의 원인을 지적하고, 효과적으로 대응하기 위하 방안으로 중간 노드에서의 Data의 서명 검증이 비효율적이기 때문에 PIT 구성 및 운영 방안의 개선을 제안하였다. 제안된 기법은 PIT의 변경을 최소화 하고 소프트웨어로 구현이 가능하기 때문에 적용이 용이한 방법이다.

특히, 일반적인 DoS 공격이 일정 시간동안 진행된 이후에 공격을 탐지할 수 있는 단점이 있는 반면에 개선된 PIT를 이용한 CS Poisoning 공격 대응 방법은 공격에 이용된 Fake Data를 실시간으로 filtering 할 수 있어 공격을 원천적으로 막을 수 있을 것으로 기대된다.

References

[1] D.D. Clark, "The Design Philosophy of the DARPA Internet Protocols," ACM Sigcomm Comp. Comm. Review, Vol. 18, No. 1, pp. 106- 114, Aug. 1988.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher and B. Ohlmann, "A Survey of Information-Centric Networking," IEEE Communications Magazine, Vol. 50, No. 7, pp. 26-36, July 2012.

[3] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs and R. Braynard, "Networking Named Content," 5th International Conference on Emerging Networking Experiments and Technologies, pp. 1-12, 2009.

[4] The NDN project team, Named Data Networking (NDN) Project, NDN technical Report NDO-0001, 2010.

[5] C. Park, T. Kwon and Y. Choi, "Scalability Problem for Interest Diffusion in Content- Centric Network," NCS, Dec. 2010.

[6] D. Kim, J. Lee, "How to Make Content Centric Network (CCN) More Robust Against DoS/DDoS Attack," IEICE Trans. Commun. Vol. E96-B, No. 1, PP 313-316, January 2013.

[7] D. Kim, "A Study on Countermeasure for CCN Interest Flooding Attack," Journal of Korea Multimedia Society, Vol. 16, No. 8, August 2013, pp. 954-961.

[8] D. Kim, "Content Centric Networking Naming Scheme for Efficient Data

Sharing," Journal of Korea Multimedia Society, Vol. 15, No. 9, September 2012, pp. 1126-1132.

〔9〕 K. Cho, M. Lee, K. Park, T. Kwon, Y. Choi and S. Pack, "WAVE: Popularity-based and Collaborative In-network Caching for Content-Oriented Networks," in Proc. IEEE INFOCOM Workshop on Emerging Design Choices in Name-Oriented Networking (NOMEN), March 2012.

〔10〕 M. Xie, I. Widjaja and H. Wang, "Enhancing cache rebustness for content-centric networks," in: Infocom, 2012.

〔11〕 M. Conti, P. Gasti and M. Teoli, "A lightweight mechanism for detection of cache pollution att만 in Named Data Networking," Computer Networks, 57, PP 3178-3191, 2013.

〈저자소개〉

김 대 엽 (DaeYoub Kim) 종신회원
2000년 2월: 고려대학교 대학원 수학과 이학박사
2000년 3월: (주)텔리맨 CAS팀 책임연구원
2002년 8월: (주)시큐아이 정보보호연구소 PKI실 차장
2012년 2월: 삼성전자 종합기술원 전문연구원
2012년 3월~현재: 수원대학교 정보보호학과 조교수
〈관심분야〉 보안프로토콜, 콘텐츠 보안, 미래 인터넷 보안, 보안 코딩