Journal of Korea Multimedia Society Vol. 16, No. 8, August 2013(pp. 954-961)
http://dx.doi.org/10.9717/kmms.2013.16.8.954

콘텐츠 중심 네트워킹 환경에서의 Interest Packet Flooding 대응 연구

김 대 엽†

요 약

미래 인터넷 기술 중 하나인 콘텐츠 중심 네트워킹(CCN)은 네트워크 성능 향상을 위하여 네트워크 노드들이 수신된 콘텐츠를 임시 저장하고, 해당 콘텐츠에 대한 요청을 수신하면 임시 저장된 콘텐츠를 이용하여 네트워크 노드가 이를 직접 처리한다. 또한, CCN은 IP 주소와 같은 호스트 Identity 대신 계층화된 콘텐츠 이름을 이용하여 패킷을 전송하고, 요청자 프라이버시 보호를 위하여 요청 메시지는 요청자 정보를 포함하지 않기 때문에 콘텐츠 제공자와 네트워크 노드들은 실제 요청자를 식별할 수 없다. 수신된 콘텐츠를 요청자에게 전송하기 위하여 네트워크 노드는 PIT(Pending Interest Table)에 요청 메시지와 해당 요청 메시지의 유입 경로 정보를 기록하고, 콘텐츠를 수신하면 기록된 PIT 정보를 이용하여 해당 콘텐츠를 요청자에게 전송한다. 만약 PIT 저장 공간이 고갈되면, 콘텐츠 요청 메시지와 수신된 콘텐츠를 정상적으로 처리할 수 없다. 그러므로 안전한 CCN 구현을 위해서는 PIT 저장 공간 고갈을 목적으로 하는 공격의 탐지와 대응이 필요하다. 본 논문에서는 PIT 저장 공간에 대한 공격 탐지 및 대응을 위하여 공격 메시지 유입 경로에 따른 공격 탐지/제어 방안을 제안하고, 공격 제어를 위한 메시지 구조를 함께 제안한다. 또한, 제안된 방식을 시뮬레이션을 통하여 그 성능을 평가 한다.

A Study on Countermeasure for CCN Interest Flooding Attack

DaeYoub Kim†

ABSTRACT

To enhance the efficiency of network, content-centric networking (CCN), one of future Internet architectures, allows network nodes to temporally cache transmitted contents and then to directly respond to request messages which are relevant to previously cached contents. Also, since CCN uses a hierarchical content-name, not a host identity like source/destination IP address, for request/response packet routing and CCN request message does not include requester's information for privacy protection, contents-providers/network nodes can not identify practical requesters sending request messages. So to send back relevant contents, network nodes in CCN records both a request message and its incoming interfaces on Pending Interest Table (PIT). Then the devices refer PIT to return back a response message. If PIT is exhausted, the device can not normally handle request/response messages anymore. Hence, it is needed to detect/react attack to exhaust PIT. Hence, in this paper, we propose improved detection/reaction schemes against attacks to exhaust PIT. In practice, for fine-grained control, this proposal is applied to each incoming interface. Also, we propose the message framework to control attack traffic and evaluate the performance of our proposal.

Key words: Future Internet(미래 인터넷), CCN(콘텐츠 중심 네트워킹), DoS/DDoS Attack(분산 서비스 거부 공격), Attack Detection(분산 서비스 거부 공격 탐지)

※ 교신저자(Corresponding Author) : 김대엽, 주소 : 경기도 화성시 봉담읍 와우안길 17 수원대학교 IT 대학 정보보호학과 (445-743), 전화 : 016) 818-6913, FAX : 031) 229-8284, E-mail : daeyoub69@suwon.ac.kr

† 수원대학교 정보보호학과

※ 본 연구는 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구 결과임 (No. NRF-2013R1A1A2008389).

1. 서 론

초기 인터넷은 호스트들 사이의 안전한 연결을 제공하기 위하여 제안되었다. 그러므로 대용량 콘텐츠 전송 시 발생되는 네트워크 병목현상, 취약한 보안 구조로 인한 침해 사고, 호스트의 빈번한 이동 시 발생하는 비효율성과 같은 현재 인터넷이 갖고 있는 다양한 문제점들과 그 해결 방안은 초기 인터넷 설계 시 고려되지 않았다[1]. 이와 같은 인터넷의 문제점들을 해결하고 인터넷을 통한 멀티미디어 콘텐츠 서비스를 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 콘텐츠 이름에 기반 한 패킷 포워딩과 네트워크 기기/노드에 콘텐츠 임시 저장(caching) 기능을 구현하여 콘텐츠의 효과적인 전송을 제공한다[2]. 이와 같은 CCN의 장점을 활용한 다양한 서비스와 함께 CCN 성능 개선을 위한 연구도 계속 진행되고 있다[5,6].

CCN을 구현하기 위하여 각각의 노드는 콘텐츠를 임시 저장하는 Content Store (CS)와 패킷 포워딩을 위한 Pending Interest Table (PIT)을 추가적으로 운영한다. 그러나 CCN에 추가된 이와 같은 새로운 자원에 대한 서비스 거부 공격(Denial of Service Attack, DoS Attack) 가능성이 최근 제기 되었다[7,8]. 본 논문에서는 CS와 PIT를 대상으로 한 DoS Attack의 가능성을 살펴보고, PIT의 제한적인 저장 공간을 이용한 DoS Attack에 대한 효과적인 탐지 및 개선된 대응 방안을 제안한다.

2. 콘텐츠 중심 네트워킹

효율적인 네트워킹을 위하여 CCN은 네트워크 노드들이 수신된 콘텐츠(응답 메시지, Data)를 임시 저장할 수 있다고 가정한다. 또한, CCN 노드는 요청 메시지(Interest)를 수신하면 CS에 임시 저장된 Data 중에서 수신된 Interest에 대응하는 Data가 저장되어 있는지 먼저 확인한 후, 대응되는 Data가 존재하면, 해당 Data를 요청자에게 전송하고 수신된 Interest를 다음 노드로 더 이상 전송하지 않는다. 중간 노드들에 의하여 Interest가 처리되기 때문에 콘텐츠 제공자에게 집중되는 요청 메시지를 분산처리 할 수 있을 뿐만 아니라 전체 네트워크 트래픽 양 또한 효과적으로 줄일 수 있다.

이와 같이 CCN 노드들에 임시 저장된 콘텐츠를 활용하기 위하여 CCN은 IP 주소와 같은 호스트 Identity 대신 계층화된 콘텐츠 이름을 이용하여 Interest와 Data를 전송한다. 또한, 요청자의 프라이버시 보호를 위하여 Interest는 콘텐츠 요청자 정보를 포함하지 않는다. 그러므로 네트워크 노드가 Data를 수신했을 때, 해당 Data를 요청자에게 전송하기 위해서 CCN 노드는 Interest와 Interest의 유입 경로(Face)를 PIT에 저장/관리하고, 이를 참조하여 Data를 전송한다.

그림 1는 이와 같은 Interest와 Data 처리 절차를 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 추가한다.

(4) PIT에 대응되는 정보가 없다면, FIB (Forwarding Information based) 테이블을 참조하여 수신된 Interest를 전송할 Face (ex. Face 2)를 선택한다.

(5) PIT에 수신된 Interest와 incoming Face 정보를 기록한다.

(6) FIB에서 선택한 Face를 통하여 수신된 Interest를 전송한다.

(7) Data가 수신된다.

(8) PIT에 수신된 Data에 대응되는 Interest 정보가 있는지 확인한다. 만약 없으면, 해당 Data는 폐기 처리 된다.

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

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

3. PIT Flooding 공격 탐지

그림 1에서 보여 지듯이, CCN을 구현하기 위하여 새롭게 추가된 자원 중 하나가 CS이다. 수신된

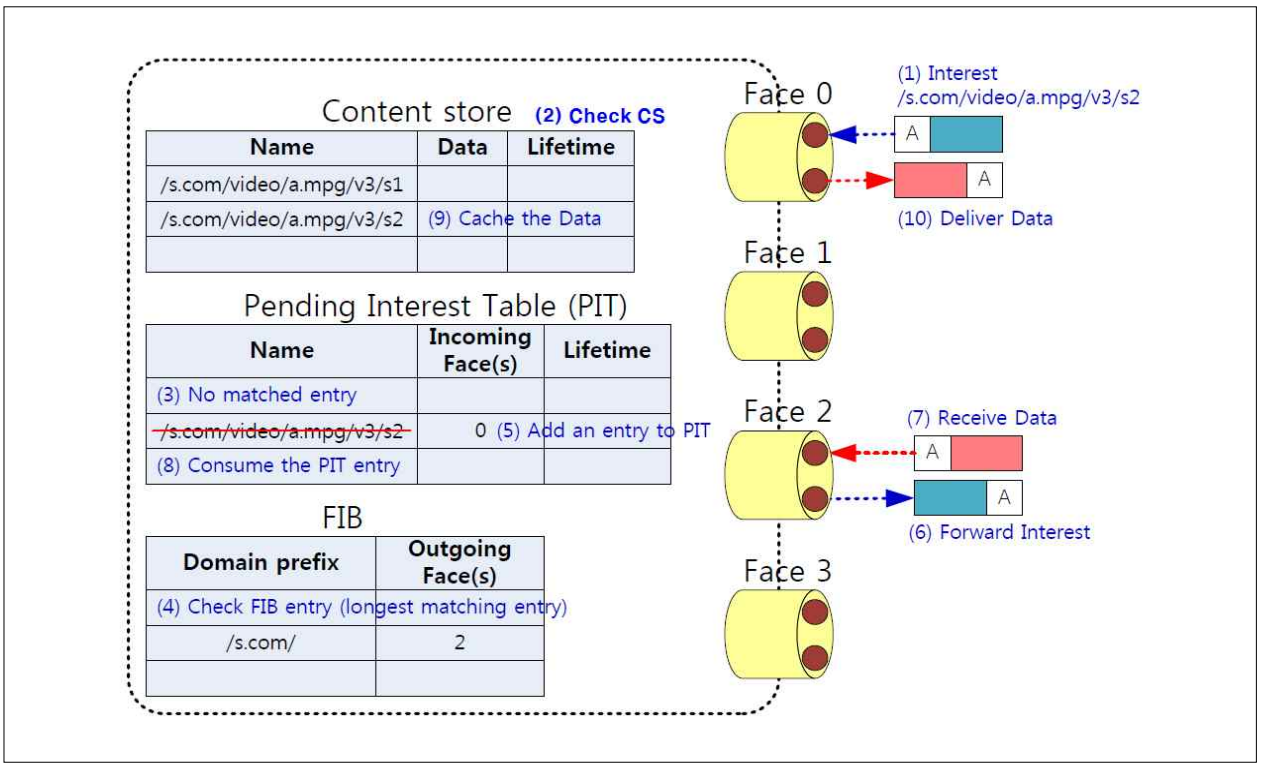

그림 1. CCN Forwarding Model

Interest에 대응되는 Data가 CS에 저장되어 있다면, CCN 노드는 Interest의 incoming Face로 해당 Data를 전송한다. 이와 같이 Interest가 중간 노드에 의하여 처리될 수 있기 때문에 CS에 저장된 Data의 관리는 CCN 성능에 직접적인 영향을 줄 수 있다. 그러므로 CS가 DoS Attack의 목표 자원이 될 가능성이 있다. 그러나 CS 저장 공간이 부족할 경우, CCN 노드는 수신된 Data를 저장하지 않고 포워딩한다. 뿐만 아니라, 수신된 Interest는 대응되는 Data를 CS에서 찾을 수 없으면 CCN 노드는 Interest를 다음 호스트로 포워딩한다. 그러므로 CS를 공격 목표 자원으로 이용하는 DoS Attack이 진행되어 공격 목표가 된 노드의 CS가 공격 Data로 모두 소모되어 정상적인 Data를 저장 할 수 없게 되었어도 Interest와 Data의 전송은 정상적으로 운영되기 때문에 DoS Attack 영향은 매우 적다. 또한, CCN 노드는 수신된 Data에 대응하는 Interest 정보가 PIT에 기록되어 있을 때에만 CS에 저장한다. 그러므로 CS를 DoS Attack의 공격 자원으로 이용하기 위해서는 콘텐츠 요청자와 제공자의 공모가 필수적으로 요구되기 때문에 공격 목표 설정 및 시도가 매우 제한적일 수 있다.

CCN에 새롭게 추가된 또 다른 자원이 PIT이다. 노드의 PIT가 모두 소모된 경우, 해당 노드가 Interest를 수신하면, PIT에 가용 자원이 생길 때 까지 Interest를 폐기한다. 뿐만 아니라, Data를 수신한 CCN 노드가 대응되는 Interest 정보를 PIT에서 찾지 못하면 해당 Data는 폐기 처리된다. 그러므로 PIT를 공격 목표 자원으로 이용하는 DoS Attack는 정상적인 Interest가 PIT에 기록되지 못하게 하거나 또는, 기록된 정상 Interest를 삭제하게 유도하여 정상 Interest에 대한 Data가 폐기 처리 되도록 할 수 있다. 또한, 공격 목표에 공격Interest가 전송되게 Interest의 콘텐츠 이름을 설정하는 것만으로도 공격 목표가 된 CCN 노드의 PIT 저장 공간을 소모시킬 수 있기 때문에 PIT에 대한 공격은 CS에 대한 공격보다 더 효과적이고 간단하다.

그러므로 본 절에서는 PIT를 공격 목표 자원으로 이용한 DoS Attack을 PIT-flooding 공격이라 부르고, 공격 탐지를 위한 절차를 제안한다. PIT-flooding 탐지는 다음과 같은 절차에 따라 수행된다.

3.1 PIT 임계값 설정

PIT-flooding 공격을 탐지하기 위하여 서비스 거부 공격 탐지를 위한 일반적인 방법처럼 PIT의 저장

용량의 임계값(threshold)을 $m\%$로 설정하고, PIT의 저장 공간의 $m\%$ 이상이 소진되면 이를 공격 상황으로 간주한다. 그러나 이와 같은 단순 탐지 기법은 PIT 저장 공간이 일정량 이상 소모된 후에만 탐지가 가능하기 때문에 공격에 효과적으로 대응할 수 없다. 또한, Interest 유입양의 급격한 증가를 모두 공격으로 간주하는 경우, 단순 증가를 공격으로 오판할 수 있다. 그러므로 보다 세밀한 공격 탐지 및 판단 기법이 필요하다.

3.2 PIT 상태 관리

PIT의 기록된 entry (Interest, incoming Faces)는 대응되는 Data가 수신되거나 entry의 생명 주기(lifetime)가 지나도록 대응되는 Data가 수신되지 않으면 자동으로 삭제된다. 그러므로 CCN 노드의 PIT에 최대 N개의 entry를 기록/관리되고, 각각의 entry의 생명 주기를 T초라고 할 때, PIT의 임계값을 $m\%$라 가정하면,

$$t^I v = \lceil \lfloor N \times m \rfloor \times T^{-1} \rceil \tag{1}$$

개 이상의 Interest가 지속적으로 CCN 노드로 유입되면, T초 후에는 PIT의 임계값을 초과할 수 있다. 그러므로 PIT 저장 공간을 효율적으로 관리하기 위하여, T초 동안 유입되는 Interest의 양을 t개의 주기로 나눠서 관찰한다. i번째 관찰 주기 p_i에 유입된 Interest의 양을 $t^I v_i$라고 하고, p_i에 PIT에 기록되어 있는 entry의 총 개수를 pv_i라 하면, pv_i는 다음 두 조건을 동시에 만족 한다:

$$pv_i \geq (pv_{i-1} + t^I v_i) - \sum_{j=1}^{t-1} t^I v_{i-j}, \tag{2}$$

$$pv_i \leq pv_{i-1} + t^I v_i \tag{3}$$

즉, PIT의 생명 주기가 T이므로 p_i에 PIT에 기록되어 있는 entry는 이전 $t-1$개의 주기 p_{i-1}, p_{i-2}, ..., $p_{i-(t-1)}$에 유입된 Interest들이다. 그러므로 p_{i-1}까지 이들 Interest에 대한 응답 Data가 전혀 수신되지 않은 상태에서 p_{i-1}, p_{i-2}, ... , $p_{i-(t-1)}$에 수신된 Interest에 대한 응답 Data가 p_i에 모두 수신된 경우가 pv_i값의 최솟값이 된다. 반대로, 이전에 수신된 Interest에 대한 응답이 p_i에 전혀 수신되지 않는 경우가 최댓값이 된다. 조건식 (2)와 (3)을 관찰하면, pv_i 값에 유입되는 Interest의 양과 대응되는 Data의 유입 양이 영향을 주는 것을 알 수 있다. 본 절에서는 이와 같은 두 가지 요소를 이용한 DoS Attack 탐지 방안을 제안한다.

3.2.1 비정상 상태 탐지

p_{i-1} 관찰 주기에 pv_{i-1}개의 entry가 PIT에 존재한다고 가정할 때, p_i에 $t^I v_i$개의 새로운 entry가 PIT에 추가로 기록된다. 특히, Interest가 PIT에 기록된 후 T초 사이에 대응되는 Data가 수신되지 않으면, 해당 entry는 삭제된다. 즉, p_{i-t}에 유입된 $t^I v_{i-t}$개의 Interest에 대응하는 entry는 PIT에서 모두 삭제된다. 그러므로 p_i에 PIT에 추가로 증가되는 entry의 수 $t^I v_i^*$는 다음을 만족하다:

$$t^I v_i - t^I v_{i-t} \leq t^I v_i^* \leq t^I v_i. \tag{4}$$

그러므로 t개의 연속된 관찰 주기 $p_{i-(t-1)}$, $p_{i-(t-2)}$, ⋯, p_i에 각각 증가 되는 entry의 최소 개수 $t^I v_j - t^I v_{j-t}$ $(i-(t-1) \leq j \leq i)$가 $t^I v$개를 넘는지 확인한다. 만약 p_j에 $t^I v_j - t^I v_{j-t} > t^I v$ 상황이 발생하면, CCN 노드는 해당 상황을 비정상 상황으로 간주한 후, 비정상 상황의 발생 원인을 분석한다.

4.2.2 비정상 상태의 발생원인 분석

CCN 노드는 PIT의 entry에 대응되는 Data를 수신하면, PIT 기록을 확인하여 대응하는 Interest가 수신된 Face로 해당 Data를 전송한 후, PIT에서 해당 entry를 삭제한다. 그러므로 $p_{i-(t-1)}$와 p_i 사이에 기록된 PIT entry에 대응하는 Data가 수신된 수만큼 pv_i 값은 감소한다. 그러므로 Interest의 유입 양이 비정상인 경우라도 대응하는 Data가 정상적으로 수신되면 pv_i가 PIT의 임계값을 초과하지 않을 수 있으며, 이러한 상황은 정상 상태로 간주해야 한다. 그러므로 Interest의 유입 양이 비정상 상태를 나타내면, Data의 응답률을 확인하여 비정상 상태의 실제 원인을 판단한다. 이를 위하여, 정상 상태에서의 Interest에 대한 응답 Data가 수신되는데 소요되는 평균 응답 시간 α와 하고 평균 응답률 β를 측정하고 그 자료를 유지한다. 정상적인 상태에서 p_i에 전송된 Interest에 대응하는 Data는 $p_{i+\alpha}$에 수신된다. $t^D v_i$를 p_i에 수신된 Data의 양이라고 하면 $t^I v_{i-\alpha}$ 와 $t^D v_i$는 $\beta \leq t^D v_i \times (t^I v_{i-\alpha})^{-1} \leq 1$ 을 만족한다. 그러므로 정상

응답률에 대한 임계값을 γ 라 할 때, p_k에 측정한 응답 비율이

$$\frac{t^D v_i}{t^I v_{i-\alpha}} < \gamma \le \beta \le 1 \quad (5)$$

이면, p_i에 발생한 비정상 상황의 원인을 공격에 의한 것으로 간주한다. 즉, p_i에 수신된 Data의 수가 정상 상태와 비교하여 임계값 보다 적게 수신되면 비정상 상황의 원인을 공격으로 간주한다. 그림 2는 DoS Attack 탐지를 위한 절차를 설명한다. $t^p v_{(i,j)}$는 p_j에 추가된 PIT entry 중에서 p_i까지 대응되는 Data가 수신되지 않아 PIT에 남아 있는 entry의 수를 의미한다.

4. PIT Flooding 공격 대응

PIT-Flooding 공격에 대응하기 위해서는 유입되는 Interest의 양을 감소시키는 방안이 필요하다. 이를 위해서는 공격자를 확인하고 해당된 공격자로부터 전송되는 Interest를 차단하는 방안이 가장 효과적이다. 그러나 Interest는 요청자 정보를 포함하지 않기 때문에 유입된 Interest를 분석해서 공격자를 식별하기 어렵다. 또한, PIT entry는 생명 주기에 따라 주기적으로 삭제되기 때문에 네트워크 노드들 간의 공조를 통한 공격자를 식별하기도 어렵다.

```
i←0
While(1) {
  Count t^I v_i and t^D v_i ;
  Manage PIT ;
  Calculate t^P v_(i,i-(t-1)) ;
  t^I v_i^* ← (t^I v_i − t^D v_i − t^P v_(i,i-(t-1))) ;
  If t^I v_i^* > t^I v then {
    ac←(ac+1) ;
    If ac>α and as=1 then {
      ϵ←t^D v_i × (t^I v_(i-α))^-1 ;
      If ϵ<γ then Notify Attack State ;
    }
    Else {
      ϵ←pv_i × (t^I v_i^*)^-1 ;
      If ϵ<α−ac then {
        as←1; Notify Abnormal State;
      }
    }
  }
  Else {
    nc←(nc+1) ;
    If nc>α then {
      ac←0 ; nc←0 ; as←0 ;
    }
  }
  i←(i+1) ;
}
```

그림 2 Pseudo Code for Detection

그러므로 PIT-Flooding 대응을 위해서 공격자를 직접 식별하는 것 보다는 공격을 탐지한 CCN 노드가 주변 노드들에게 공격 탐지 정보를 알리고 주변 노드들의 협력을 통하여 공격에 대응하는 방안이 합리적이다. 이를 위하여 본 절에서는 공격을 탐지한 CCN 노드의 one hop 이웃 노드와의 공조를 통한 공격 대응 기법을 제안한다.

4.1 제어 메시지

CCN은 기본적으로 Interest와 Data 두 개의 메시지만을 정의하고 처리한다. 그러므로 이웃 노드들에게 공격 상황을 전파하기 위하여 별도의 메시지가 필요하다. [7]에서는 공격 상황을 주변 노드들에게 알리기 위하여 공격에 사용된 Interest에 포함된 contents name과 동일한 name을 갖는 packet을 별도로 생성하는 방안을 제안하였다. 이 경우, 이웃 노드들이 공격 Interest 만을 선별하여 제어할 수 있다는 장점은 있으나, CCN이 contents name을 기반으로 패킷 전송을 하기 때문에 이와 같이 제어 메시지를 생성하는 경우, CCN은 해당 제어 메시지를 이웃 노드에게 전송하지 않는다. 그러므로 [7]에서 제안된 메시지를 CCN에 적용하기 위해서는 CCN 네트워킹 구조를 모두 변경해야만 한다.

그러므로 CCN에 적용 시 수정을 최소화 할 수 있는 제어 메시지 구조가 필요하다. Data는 대응하는 Interest 전송 기록이 PIT에 남아 있을 때에만 처리되기 때문에 Interest를 이용한 제어 메시지를 제안하고, 기존 Interest와 구분하기 위하여 새롭게 정의되는 제어 요청 메시지를 Control 이라고 부른다. 그림 3은 Control 처리를 위하여 새롭게 제안하는 Interest의 구조이다. 제안된 Interest 구조는 [9]에 정의된 메시지 구조를 최소한으로 수정하도록 설계되었다. 변경 또는 추가된 항목은 다음과 같다:

- Na: Tag, Name, Command를 sub-field로 갖는다. Tag는 메시지의 종류를 나타낸다. “ccn-in-

```
Interest::=
    Name (Na)
    MinSuffixComponents (Min)
    MaxSuffixComponents (Max)
    PublisherPublicKeyDigest ? (Pd)
    Exclude ? (Ex)
    ChildSelector ? (Cs)
    AnswerOringnKind (Ao)
    Scope (Sc)
    InterestLifetime (Lt)
    Nonce ? (No)
    FaceID (Fi)
    Signature (Sg)
    SignedInfo (Si)
```

그림 3. Interest Message Framework

terest" 값을 갖거나 Tag 항목을 포함하지 않으면 Interest를 나타낸다. Control을 위해서는 "ccn-push" 값을 사용한다. Name은 요청하는 콘텐츠의 name prefixes 또는 Control의 수신 처에 대응하는 name prefixes를 명시한다. Command는 제어 내용을 명시한다. DoS Attack 대응을 위해서는 "interest-traffic-dr?Dr"을 예약 명령어로 정의한다. Dr은 traffic decrease rate을 의미한다.

- Min (5), Max (10)
- Ao (0), Sc (2), Lt (0)
- Sg, Si: Interest에 포함된 모든 항목에 대한 Control 생성자의 서명 및 서명 검증에 필요한 정보를 각각 의미한다. Sg는 Control의 최종 수신자에 의해 검증된다. 항목 구조는 ContentObject의 Sg와 Si를 따른다[10].

4.2 제어 메시지를 이용한 공격 대응

PIT-Flooding 공격을 감지한 CCN 노드는 운영하는 f개의 Face에 대하여 유입된 Interest의 양을 각각 측정한다. 단위 시간동안 i번째 Face로 유입되는 Interest의 수를 f_i라 하자. 유입되는 Interest의 양을 조절하기 위하여 traffic decrease rate (Dr)을 다음과 같이 계산 한다: $\{t^I v_k\}_{k=i-T,\cdots,i}$의 최솟값과 최댓값을 각각 $t^I v_{\min}$과 $t^I v_{\max}$라 할 때,

$$Dr \le \frac{(T \times t^I v) - pv_i + t^I v_{\min}}{T \times t^I v_{\max}} \tag{6}$$

CCN 노드는 $\Omega = Dr \times t^I v_i \times (f \times pv_i)^{-1}$을 계산하여 각각의 Face에 유입된 Interest의 양 f_i가 Ω 보다 큰 Face에 대해서만 Control를 생성한 후, 해당 Face로 전송한다. Control 전송 후, 각각의 Face 별로 Interest 유입량을 측정하여 $(Dr \times f_j \times pv_i^{-1}) \times t^I v_i$ 보다 많은 양이 유입되면, 기준을 초과해 유입된 Interest를 폐기 시킨다.

p_i에 Interest 유입량에 이상이 감지되고 CCN 노드로부터 Control을 전송 받은 이웃 노드들이 Interest 전송 양을 용청 받은 만큼 줄인다면, pv_k $(k > i)$는 $T \times t^I v$를 초과하지 않게 된다. 실제로 p_k에 유입되는 Interest의 양 $t^I v_k$는 다음을 만족 한다:

$$\begin{aligned} t^I v_k &\le \sum_{j=1}^{f} \frac{f_j}{pv_i} \times Dr \times t^I v_i \\ &= \frac{Dr \times t^I v_i}{pv_i} \sum_{j=1}^{f} f_j . \end{aligned} \tag{7}$$

$\sum_{j=1}^{f} f_j \le pv_i$이므로, $\Phi = \frac{(T \times t^I v - pv_i)}{T}$라 하면 식 (7)은 다음을 만족한다.

$$\begin{aligned} & t^I v_k \\ & \le Dr \times t^I v_i \\ & \le \left(\frac{T \times t^I v - pv_i + t^I v_{\min}}{T} \right) \times \frac{t^I v_i}{t^I v_{\max}} \\ & \le \left(\frac{T \times t^I v - pv_i + t^I v_{\min}}{T} \right) \\ & \le \Phi + t^I v_{\min} \\ & \le \Phi + t^I v_{k-T} \end{aligned} \tag{8}$$

공격이 진행 중인 상태라면 일반적으로 $t^I v_k \ge t^I v_{k-T}$라 가정할 수 있다. 그러므로 $i < t \le i + T$에 대하여

$$\begin{aligned} pv_t &\le pv_i + \sum_{j=1}^{t} (t^I v_{i+j} - t^I v_{i+j-T}) \\ &\le pv_i + \sum_{j=1}^{t} \Phi \\ &< pv_i + (t \times \Phi) \\ &\le T \times t^I v \end{aligned} \tag{9}$$

을 만족한다. 또한, $t > i + T$에 대하여, $t^I v_i \le t^I v_{\max}$이고 $t^I v_{\min} \le pv_i$ 이므로, 식 (6)에 의하여

$$\begin{aligned} pv_t &\le T \times (t^I v_i \times Dr) \\ &\le (T \times t^I v_{\max}) \times Dr \\ &\le (T \times t^I v) - pv_i + t^I v_{\min} \\ &\le T \times t^I v \end{aligned} \tag{10}$$

이 만족된다. 그러므로 식 (1)에 의하여 pv_t는

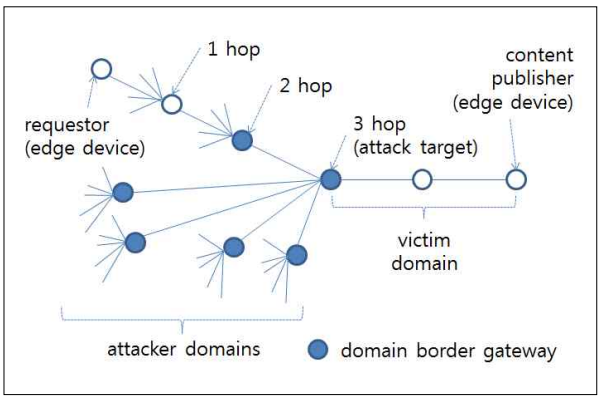

그림 4. 시뮬레이션을 위한 네트워크 구성도

$\lceil N \times m \rceil$을 넘지 않는다.

6. 성능 평가

시뮬레이션을 위하여 각각의 CCN 노드는 6개의 Face를 운영한다고 가정한다. 그림 4는 시뮬레이션을 위한 network 구성을 설명한다. CCN name 구조에 따라 각각의 domain 마다 최상위 name prefix에 대응하는 domain border gateway (D_{BG})가 1대씩 존재 한다고 가정하고, 각각의 domain은 25개의 edge device (D_E)와 5개의 중간 노드들로 구성되어 있으며, D_{BG}에서 D_E 까지 3 hop으로 구성되어 있는 tree 형태의 topology로 구성되어 있다고 가정하자.

공격 대상 노드가 된 D_{BG}의 6개의 노드 중 3개의 Face 로부터는 공격 Interest와 정상 Interest가 섞여서 유입되고 3개의 Face는 정상 Interest만 유입된다고 가정한다. 모든 노드의 PIT는 100개의 entry를 저장할 수 있고 임계값은 70%로 설정한다. 또한, 공격 목표 노드에 유입되는 Interest 중 10%는 정상 Interest라고 가정한다. 탐지와 대응을 위하여 $T=4$, $t=10$, $\alpha=4$, $\beta=95\%$, $\gamma=70\%$로 각각 설정한다. 또한, 공격 Interest는 공격 대상인 D_{BG}의 domain name prefix "/domain_1/"을 최상위 content-name prefix로 사용하고 하위 name prefix를 무작위로 생성하여 Interest가 D_{BG} 까지 전송될 수 있도록 생성한다. 이때, 다음 사항을 유의해서 생성한다.

(1) Interest에 대응하는 Data가 존재하는 경우, 응답 시 PIT에서 해당 entry가 삭제되므로, 항상 존재하지 않는 Data를 요청할 수 있게 생성해야 한다.

(2) PIT에 동일한 Interest가 존재하면 해당 Interest가 더 이상 전송 되지 않으므로 attacker는 Interest의 contents name이 중복되지 않게 생성해야 한다.

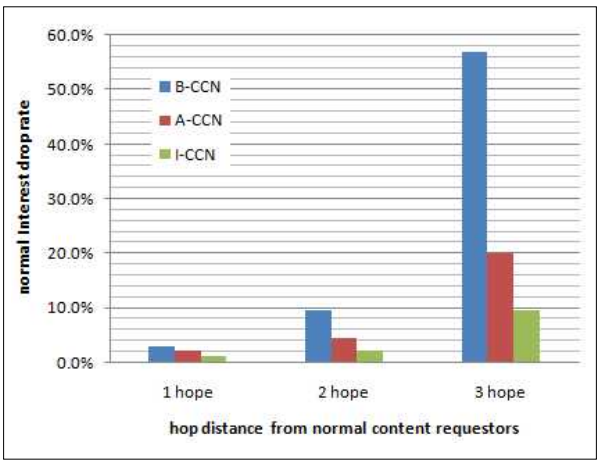

그림 5. Interest drop rate

그림 5는 정상 Interest의 drop rate을 나타낸다. B-CCN은 DoS Attack 대응 기능이 탑재되지 않은 기본적인 CCN을 나타내고, A-CCN은 [7]에서 제안된 대응 방안이 탑재된 CCN을 나타낸다. I-CCN은 본 논문에서 제안된 탐지 및 대응 방안이 탑재된 CCN을 나타낸다. B-CCN의 경우 공격 목표가 된 D_{BG}로 유입되는 Interest에 대하여 정상 Interest와 공격 Interest를 판단하는 절차를 포함하고 있지 않기 때문에 대량의 공격 Interest 정보로 D_{BG}의 PIT가 소모되면 정상 Interest를 처리하지 못하고 모두 폐기했다. A-CCN의 경우, 비정상 Interest가 유입되면 D_{BG}에 연결된 모든 Face에 동일하게 Interest 전송량을 줄이도록 권고하여 PIT 소진을 방지하고, 폐기되는 정상 Interest의 양도 B-CCN에 비하여 65%정도 줄일 수 있다. 그러나 이 경우, 정상 Interest가 유입되는 경로에도 동일한 제어 메시지가 전송되어 처리할 수 있는 정상 Interest 양이 줄어들고 처리 속도 또한 지연되는 단점이 있다. 이에 반하여 I-CCN은 공격 Interest가 유입되는 Face만을 선별하여 제어 메시지를 전송하게 함으로써 공격 Interest가 유입되지 않는 Face는 제어 대상에서 제외시켰다. 이 경우, D_{BG}에서 폐기되는 Interest의 양은 A-CC에 비해 50% 이상 줄었음을 알 수 있다. 더욱이, 공격 대응 시에도 정상 Interest만 유입되는 Face로 유입되는 Interest는 전혀 영향을 받지 않고 처리된다. 이를 통하여 공격 목표가 된 D_{BG}에 전체 Interest 처리 양 및 속도를 개선시키는 효과를 기대할 수 있다.

6. 결 론

본 논문의 결과는 다음과 같은 세 가지 측면에서 그 기여도를 생각할 수 있다. 첫 번째로 CCN에 대한 DoS Attack 가능성에 대하여 처음 문제점을 제기한 [7]에서 제안된 CCN DoS Attack 대응은 탐지 노드와 연결된 모든 노드에게 Interest 전송 양을 일정 비율 (Dr) 이하로 동일하게 감소시키도록 요구한다. 그러나 일률적인 요청은 공격에 이용되지 않는 Face를 통하여 유입되는 정상 Interest의 양도 감소시키는 단점을 갖고 있다. 본 논문에서는 공격에 악용된 Face를 선별하고 대응함으로써 정상 Interest 유입 및 처리를 더 효율적으로 수행할 수 있게 했다.

두 번째로 제어 메시지에 포함된 Name의 경우, [7]에서는 공격 대상의 name prefix를 명시하도록 되어 있다. 그러나 실제 공격 시나리오에서 Interest를 전송할 때 네트워크 큐에 쌓여 있는 Interest의 Name을 기반을 FIB를 검색하여 전송하기 때문에 [7]의 제안을 구현하려면 CCN 네트워킹 프로세스를 수정해야 한다. 본 논문에서는 Control의 Name을 Control을 수신하게 될 CCN 노드의 name prefix로 하여 기존의 CCN 네트워킹 프로세스 수정 없이 구현/적용하도록 하였다.

마지막으로 제어 메시지를 생성, 전송, 처리하기 위하여 Interest 기반의 제어 메시지를 구성하였다. 기존의 Interest를 기반으로 구성되었고, 실제구현 시, Interest의 Name의 첫 번째 prefix 확인 후 일반 Interest와 Control을 구분하여 구현하면 되기 때문에 제안된 절차를 구현 할 때 기존 프로그램의 변경을 최소화 할 수 있다.

참 고 문 헌

[1] D.D. Clark, "The Design Philosophy of the DARPA Internet Protocols," *ACM Sigcomm Comp. Comm. Review*, Vol. 18, No. 1, pp. 106-114, 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, 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] 김대엽, "효율적인 데이터 교환을 위한 Content-Centric Networking 식별자 방안," 멀티미디어학회논문지, 제15권, 제9호, pp. 1126-1132, 2012.

[6] J. Lee and D. Kim, "Device Mobility Management in Content-Centric Networking," *IEEE Ccomm. Magazine,* Vol. 50, No. 12, pp. 28-34, 2012.

[7] D.Y. Kim and J.H. 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, 2013.

[8] C. Park, T. Kwon, and Y. Choi, "Scalability Problem for Interest Diffusion in Content-Centric Network," in Proc. of The 14th Conference on Next Generation Communication Software (NCS), 2010.

[9] CCNx Interst Message, http://www.ccnx.org/releases/latest/technical/InterestMessage.html, 2013.

[10] CCNx Content Object, http://www.ccnx.org/releases/latest/technical/ContentObject.html, 2013.

김 대 엽

1997년 3월~2000년 2월 고려대학교 대학원 수학과 이학박사

1997년 9월~2000년 3월 ㈜텔리맨 CAS팀 연구원

2000년 4월~2002년 8월 시큐아이 정보보호연구소 차장

2002년 9월~2012년 2월 삼성전자 종합기술원 전문연구원

2012년 3월~현재 수원대 정보보호학과 조교수

관심분야 : 보안프로토콜, 콘텐츠 보안, 미래 인터넷 보안