4S-02

Interest Flooding Attackによるルータへの負荷集中に対する考察と対策

篠原　涼希†　　神本　崇史‡　　梅田　沙也華‡　　重野　寛†
慶應義塾大学理工学部†　　慶應義塾大学大学院理工学研究科‡

1. はじめに

コンテンツ名を使用して直接通信を行う Named Data Networking (NDN)[1]では，Interestの情報をルータ内にあるPending Interest Table (PIT)に記録し，その情報をもとにDataを取得する．

NDN において，Interest Flooding Attack (IFA) と呼ばれる攻撃が指摘されている[2]．IFAとは，実在しないコンテンツを要求してネットワークを混乱させる攻撃である．IFA への対策手法としてPushbackがある[3]．Pushbackは，攻撃者がいる方向の Interest を制限する手法である．しかし，Pushback は攻撃者と同様に通常ユーザのInterestも制限されるという問題がある．

本研究では，IFAによって攻撃者のInterest情報が大量にPITに記録されて負荷となることに注目し，PITへのInterest情報の記録を制限することにより攻撃 Interest を制御する攻撃抑制手法を提案する．

2. 関連研究

NDN や IFA について説明し，その対策における関連研究をあげる．

2.1 Named Data Networking

NDNでは，Interestパケットによってコンテンツの要求が行われ，それに対して Data パケットによる応答が返る．NDN において各ルータは PIT を所持している．各ルータは，Interest を受け取るとその情報をPITに記録し，Interestに対応するDataを受け取ると情報を削除する．

2.2 IFAが与えるPITへの影響

IFA とは，攻撃者が実在しないコンテンツを要求する Interest を大量に送信することによって，ネットワークを混乱させる攻撃である．コンテンツが返らない攻撃者の Interest 情報は PIT から削除されずに長く残る．したがって，IFA を受けると攻撃者の Interest 情報によって通常ユーザの Interest 情報が追い出されるという問題が発生する．

2.3 IFAへの対策手法およびその問題点

IFAの影響を軽減する手法としてPushbackがある．Pushback は，充足率に基づいて Interest 量を制限する手法である．充足率とは転送されたInterest数に対する返信Data数の割合である．充足率が低い経路ほど Interest を送信させないことによって Interest 量を制限する．しかし，Pushback は充足率が低い経路上の Interest を一斉に制御するため，通常ユーザの Interest 量も制限されるという問題点がある．そこで，攻撃に使用される Interest のみを制限する手法が必要となる．

3. 提案手法

評価値を用いて Interest 情報の記録を制限するPIT制御手法を提案する．

提案手法では，IFA によって PIT が攻撃者のInterest 情報で埋まるということに注目した．提案手法は，PITに記録するInterest情報を選別することによって，PIT が埋め尽くされないようにすることを目的とする．

3.1 インタフェースの状況把握

Interest が転送されてくるたびに，ルータは各インタフェースから転送された Interest 数に対する返信 Data 数の割合を表す評価値を更新する．さらに，ルータは PIT を参照し，各インタフェースから転送された Interest 情報の記録数を保持する．

3.2 PITに記録するInterest情報の選別

評価値と記録数をもとに，ルータは Interest が転送されてきたときに，送信元のインタフェースと他のインタフェースを比較する．送

Study and Countermeasure against Packet Concentration of Routers caused by Interest Flooding Attack
Ryoki SHINOHARA†, Takashi KAMIMOTO‡,
Sayaka UMEDA ‡ and Hiroshi SHIGENO†
†Department of Science and Technology, Keio University
‡Graduate School of Science and Technology, Keio University

表1　シミュレーション条件

シミュレータ	ns-3 (ndnSIM)
各リンクの帯域	10 [Mbps]
各リンクの最大遅延	10 [ms]
通常ユーザの要求数	1000 [/sec]
攻撃者の要求数	10000 [/sec]
攻撃開始時刻	10 [s]
各ルータの PIT サイズ	275
比較対象	Pushback

信元側の評価値が他の評価値よりも低いかつ送信元側からの Interest 情報数が他からの情報数よりも多い場合，送信元インタフェースは攻撃 Interest を転送している可能性が高いと考え，PIT への記録を止める．この制限をネットワーク内の全ノードで行うことにより，攻撃となりうる Interest をネットワーク全体で制御する．

4. 評価

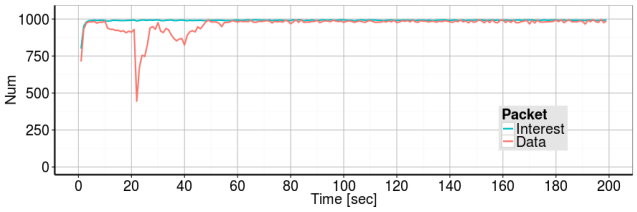
提案手法の有用性を示すため，IFA が発生する環境における通常ユーザの送信 Interest 数と取得 Data 数に関して，シミュレーションにより評価を行った．

4.1 シミュレーションモデル

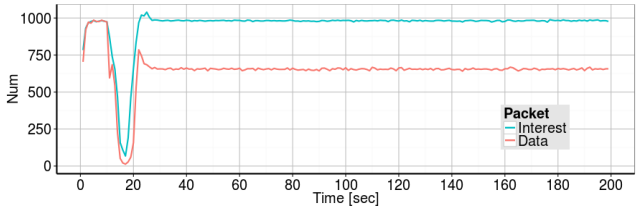
シミュレーション条件を表1に示す．通常ユーザは Zipf の法則に従ってコンテンツを要求し，攻撃者は毎回異なる実在しないコンテンツを要求する．

4.2 攻撃による通常ユーザへの影響

攻撃の影響を調べるため，通常ユーザの Interest 送信数と Data 取得数による比較を行う．図1に時間経過に伴う通常ユーザの Interest 送信数と Data 取得数の変化を示す．(a)は提案手法による結果，(b)は Pushback による結果を表す．図より，提案手法では IFA を受けても Interest 送信数は制限されておらず，Data 取得数に関しても制限開始直後は一時的に低下するが，20 秒ほどで回復して高い値を維持することが確認できる．この結果より，提案手法は全ルータで Interest を制御する手法であるが，実際には末端ルータのみでほぼ制御ができており，通常ユーザの Interest は制限されていないと考えられる．一方で，Pushback では IFA の開始とともに Interest 送信数が制限され，回復した後も Data 取得数が少ないことが確認できる．この結果より，Pushback は全ルータで Interest を制御しており，途中のルータで攻撃者に加えて通常ユーザの Interest も制限されていると考えられる．以上より，提案手法は通常ユーザの Interest を制限せず，攻撃の Interest のみを制限した手法であると言える．



(a) 提案手法



(b) Pushback

図1　通常ユーザの Interest 送信数と Data 取得数

5. おわりに

本研究では，IFA による各ルータの PIT への負荷集中について注目しその対策手法を提案した．

提案手法は，Interest 情報の PIT への記録を制限することにより，攻撃となりうる Interest を制御する．提案手法をシミュレーションによって比較評価し，通常ユーザの Interest 送信数や Data 取得数が回復することを確認した．

以上より，ルータへの負荷集中に注目した手法が IFA による通常ユーザへの影響の抑制に有用であることを示した．

参考文献

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard. Networking named content. In Proc. of ACM CoNEXT, 12 pages, 2009.

[2] Seungoh Choi; Kwangsoo Kim; Seongmin Kim; Byeong-hee Roh, "Threat of DoS by interest flooding attack in content-centric networking," 2013 International Conference on Information Networking (ICOIN), pp.315-319, Jan. 2013.

[3] Afanasyev, A.; Mahadevan, P.; Moiseenko, I.; Uzun, E.; Lixia Zhang, "Interest flooding attack and countermeasures in Named Data Networking," 2013 IFIP Networking Conference, pp.1-9, May 2013.