Vol.2020-DPS-182 No.16
Vol.2020-CSEC-88 No.16
2020/3/12

MANET-NDNにおける キャッシュ検証オーバヘッド削減手法に関する研究

柳谷 遼[1]　重安 哲也[1]

概要：NDN（Named Data Networking）では，中継ルータにおいて悪意を持った攻撃者によるコンテンツの不正改竄に対処するため，コンテンツの真正性を確保する仕組みが必要となる. しかし，MANET（Mobile Ad hoc NETwork）環境下で，ユーザが毎回遠隔のパブリッシャと真正性確認を行うと，大きなオーバヘッドを生じてしまう．本稿では，コンテンツ配送に関わった中継ノードとの協調によって，コンテンツを取得したユーザがコンテンツを自律分散的に周辺ノードと協調検証し攻撃者を検知する手法を提案し評価を行う．評価結果から，提案手法は検証オーバヘッド削減によって効果的に攻撃者を検出できることを報告する．

1. はじめに

現代社会において，多くの情報通信メディアが広く普及し，インターネットは日々の生活と深く関連しているものとなっている．現在，これから更に増加すると考えられるビデオコンテンツの効率の良い配送が課題となっており，ICN（Information Centric Network）[1] の研究が盛んに行われている．その中でも NDN は最も多くの研究が行われているものの一つである．

しかし，NDN では，悪意を持った攻撃者によるキャッシュの汚染などにより，ネットワークの利用効率を低下させるような攻撃が想定されている．そのため，コンテンツの利用において，その真正性の確保が大きな課題となっている．そこで，本稿では MANET に NDN を実装した環境（MANET-NDN）下において，ネットワークのオーバヘッドを増加させずに汚染コンテンツの検知を行うために，各ノードが周辺ノードと自律分散的に協調しコンテンツの検証を行う手法を提案するとともに，本稿で提案する手法を導入することにより検証要求をプロバイダに対して行う場合よりも検証にかかる時間を削減できることを，計算機シミュレーションを用いて明らかにする．

2. ネットワークアーキテクチャ

我々が日々利用するインターネットでは，IP（Interenet Protocol）に基づき通信が行われる．IP は TCP（Transmission Control Protocol）を上位とする TCP/IP モデルのインターネット層に規定される．IP は，データを送信する際に各ノードに割り当てられた IP アドレスで任意のノードを識別し，宛先の IP アドレスを確認することで，ノード間でデータを送信する．

ここで，現在の主要トラフィックである映像の共有やアクセスにおいては host-to-host 型である IP よりも，information-to-user 型である CDN（Content Delivery Network）[2] や P2P（Peer to Peer）[3] の方がふさわしい．

CDN では図 1 のようにオリジナルサーバからコンテンツの複製を配布した複製サーバ群を用い，ユーザはそれらからコンテンツの取得を行うことで，各サーバへのアクセスを分散する．ユーザは 1 つのドメイン名に複数の IP アドレスを割り当てる DNS（Domain Name System）ラウンドロビンや P2P の利用によってコンテンツの所在を意識せずにコンテンツを取得できる．CDN を導入することで，web だけでなく容量の大きいコンテンツやブロードバンドを利用したコンテンツ配信を安定かつ低コストに実現できる．

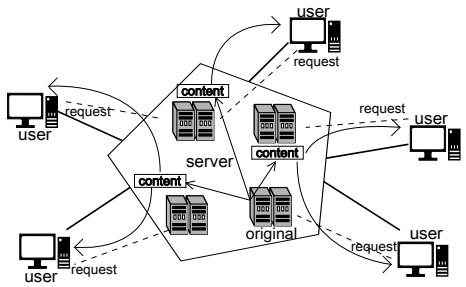

図 1　CDN

[1] 県立広島大学経営情報学科
Dept. of Management and Information Systems. Pref. Univ. of Hiroshima

Vol.2020-DPS-182 No.16
Vol.2020-CSEC-88 No.16
2020/3/12

P2P はネットワークに接続されたコンピュータ同士が末端装置として対等の立場，機能で直接通信するネットワークアーキテクチャである（図 2）．P2P は常に端末がサーバに要求を行うクライアント・サーバ方式と異なり，それぞれの端末がクライアントとサーバ両方の役割を適宜担うことから，端末同士は対等な関係であるといえる．P2P はその構造上，サーバではなく端末と通信するため，端末数が膨大になっても特定端末へのアクセス集中は発生しづらい．P2P の利用例には，Skype[4] などの IP 電話がある．

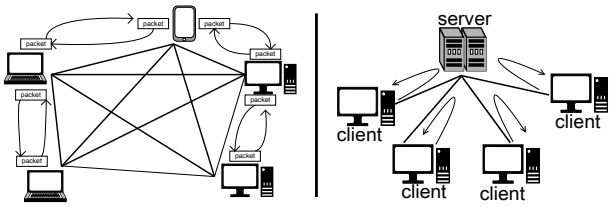

図 2　P2P とクライアント・サーバ方式

しかし，これらはオーバレイ・ネットワークでありコンテンツはサーバのみに存在するため，さらに増加するトラフィックに対応した効率的なコンテンツ配送にはアーキテクチャレベルでの解決が必要である．

そこで，アーキテクチャレベルでこの課題を解決するために ICN の研究が行われている．

代表的な ICN として NDN[5]，NetInf，PURSUIT[6] などの方式があり，その中でも NDN は盛んに研究が行われているものの一つである．NDN はコンテンツ要求を行う Interest パケットとコンテンツ返送を行う Data パケットによりコンテンツを取得する．ここで，Data パケットが返送時に通過したノードにコンテンツの複製をキャッシュすることで，効率的なコンテンツ配送を可能としている．

3. MANET-NDN における セキュリティ問題

NDN では，悪意のある攻撃者によるコンテンツの不正改竄が想定されるため，攻撃の検出にはコンテンツの真正性の確保が必要である．TCP/IP では経路上で攻撃者からのコンテンツの改変を防ぐため，暗号化を用いた通信によって安全性を確保する．

暗号化方式の代表例として公開鍵暗号方式や共通鍵暗号方式 [7] があるが，NDN において暗号を用いた場合，ユーザは安全にコンテンツを得ることが可能だが，コンテンツの配送時に経由したノードではコンテンツは暗号化されており，中継ノードはコンテンツをキャッシュしても復号ができず利用できない．そのため，暗号化によるコンテンツ配送は効率の良いコンテンツ配送を目的とする NDN になじまない．

3.1 有線環境下の NDN

文献 [8] が言及する有線環境下の NDN では，攻撃者は基幹ネットワークの外に存在するためコンテンツ汚染の拡散攻撃の検出には，末端ノードと接続するエッジルータにおいてコンテンツの真正性を確認する（図 3）．そのため，有線環境下では，エッジルータ以外では対策が不要となり，対応は比較的容易となる．

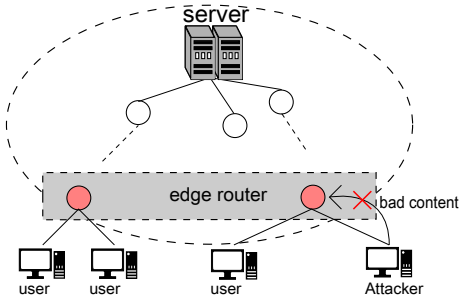

図 3　エッジルータにおける真正性確認

3.1.1 無線環境下の NDN のセキュリティ課題

有線環境下の NDN では，前述のように末端に近いエッジルータで汚染コンテンツの検出を行うと効率よく安全性を確保できるが，MANET 下では末端という考えに基づいた制御は困難である．これは MANET 下ではノードは様々な場所に位置し様々なユーザやサーバとマルチホップ通信を行うため，図 4 のように攻撃者は様々な場所に潜むことが可能であるためである．

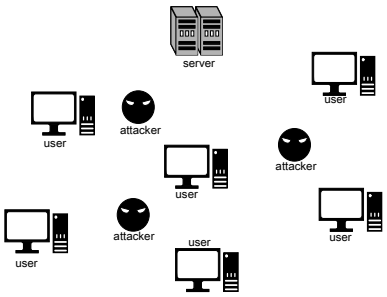

図 4　無線環境下の脅威

様々な場所に潜む攻撃者は，あらゆる場所から汚染コンテンツを差し込むことが可能であり，有線環境下のように単一の場所における対策では意味をなさないため，無線環境独自の対策が必要となる．

ここで，検証を遠隔のパブリッシャと連携して実施すると，多くのオーバヘッドが生じる．また，それよりも近い場所の特定ノードのみと検証を行うと，検証結果の信頼性の問題が生じる．そのため，セキュリティ対策手法は検証オーバヘッドが少なく，信頼性の高い検証が実現されるべきである．無線環境下では，伝送範囲内にいる他ノードの通信の傍受が可能である．有線環境下では中継のないノードとルータ間の通信を経路上で傍受することはできない．

無線環境下における傍受の有効活用によって，有線環境よりも効率の良い攻撃対策ができる可能性がある．

4. 提案手法

本論文では，MANET 環境下に NDN を適用した MANET-NDN におけるコンテンツ汚染攻撃に対して新たな対策手法を提案する．また，提案手法を実装したシミュレータによる性能評価を行うことで，本手法の有効性を示すとともに，提案手法の課題を明らかにする．

提案手法は，NDN をオーバレイによって既存の IP ネットワーク上に実装する環境下でのコンテンツ汚染攻撃に対し効率よく対処可能なコンテンツ検証手法を提案する．提案手法は，

1） 協調検証
2） IP 通信を併用した検証
3） 傍受による精度向上
4） 検証回数の削減

を組み込んだ自律分散的な検証により，オーバヘッドを削減する．

4.1 協調検証

提案手法では，各ノードが周辺ノードと自律分散的に協調しコンテンツの真正性を検証する．検証はユーザが送信した Interest に対応する Data が返送された際に行う．Data を受信したユーザは図 5 のように，自身の伝送範囲内に存在するノードであり，かつ，Data を自身に送信した検証対象ノード以外の複数ノードに検証を要求する．協調検証の結果によって，Data を受信したユーザはコンテンツを利用するか否かを決定する．

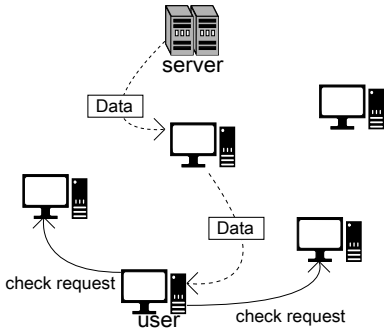

図 5 協調検証

検証要求を受信したノードは，自身がキャッシュするコンテンツの中に検証対象となるコンテンツと同名のキャッシュが存在する場合に検証を受諾する．

ここで不審なコンテンツ同士の検証によって誤った結果が発生する可能性に注意する必要がある．そのため，提案手法では複数のノードに対して同時並行的に検証を依頼することで，不審コンテンツ同士による誤った検証結果の採用を回避できる．

また，自身のキャッシュの中に検証要求コンテンツと同名コンテンツを保持していない場合は，単純にその旨を検証要求を送信したノードへ返送する．

4.2 IP 通信を利用した検証

周辺ノードと協調して実施する検証はオーバーヘッドの削減を可能とするが，要求を受けたノードにキャッシュが存在しない場合はこの手法では検証できない．そのため，協調検証ができなかった場合は代替検証手法が必要となる．

そこで，提案手法では周辺ノードへの協調検証依頼後に，検証不可能という通知を受け取ると，IP 通信を利用してプロバイダとの直接通信で検証する．図 6 は IP を用いてプロバイダ – ノード間に暗号化を用いたセキュアな通信経路を確保し確実な検証を行う例を示している．

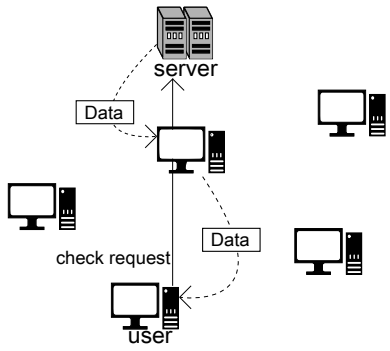

図 6 IP 検証

IP 検証では誤った検証結果を得る可能性が低いという利点があるが，ノードとプロバイダ間の距離に伴って検証に要する時間が増加する．

4.3 傍受検証

CSMA/CA 方式を利用した無線通信では，自身が宛先でなくてもパケットを傍受できる．これを利用して，提案手法では自身が転送する必要のないコンテンツを傍受した際にも自身のキャッシュ内のコンテンツを検証する．

ノードは自身が宛先でない Data を傍受した際に検証を開始する．ここで，提案手法は傍受したコンテンツと同名のコンテンツが自身のキャッシュ中に存在する場合に，それらを比較する．このとき，両者の内容に差異があれば，キャッシュを破棄する．キャッシュを破棄する理由は，この提案手法では検証に用いた 2 つのコンテンツに不審なコンテンツが含まれるという事は判定できるが，どちらが不審なコンテンツかまでは判定できないためである．

4.4 検証の省略

文献 [8] で述べられているように，ネットワーク上で転送されるすべてのコンテンツを検証することは非効率である．そのため，本論文が対象とする無線環境下であっても

必要のない検証を減らすことがオーバヘッド削減に不可欠である．

そのため提案手法では，IP 通信を用いた検証によって安全であると確認できたキャッシュにフラグを立てる．ノードは要求したコンテンツを受信した際，図 7 のようにフラグが立っていると検証の省略を行う．これにより，キャッシュから得られるコンテンツのオーバーヘッドを大幅に削減することが可能である．

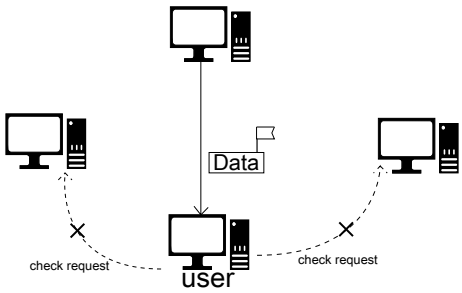

図 7　検証の省略

4.5　攻撃者検知

様々な検証によりコンテンツの汚染を検知する手法をこれまで提案してきたが，コンテンツの汚染が検証によって検知できた場合でも，汚染コンテンツを拡散する攻撃者を検知し攻撃者に対して適切な対処を行わなければ根本的な解決には至らない．

そのため，このプロセスでは今まで提案した手順による様々な検証結果をもとに，周辺ノードを評価するリストを用いた攻撃者の評価を行う．各ノードはそれぞれ，周辺ノードの情報と周辺ノードから流れてきたコンテンツを検証した際の検証不一致率を記録するリストを保持する．各ノードは検証を行うたびにリストの検証不一致率を更新する．ここで検証不一致率が更新され閾値を超えた場合，そのノードは汚染コンテンツを流入させる不審なノードであると判断される．その後，その不審なノードから受信したコンテンツは破棄するとともに，そのノードが自身の FIB に登録されている場合は FIB を変更する．提案手法で用いる不一致率 $D(i)$ は以下の式によって求める．

$$D(i) = \frac{P_{false}}{P_{true} + P_{false} + C} \tag{1}$$

i はノードの ID である．また，P_{true} は検証の結果正しいコンテンツと判断した Data の数であり，P_{false} は不審なコンテンツと判断した Data の数である．加えて，取得コンテンツ中の不審コンテンツの割合だけでなく，ネットワーク稼働初期の母数が少ない状態での誤検知を減らすために定数 C を分母に追加する．

ただし，新たに攻撃者と判定されたノードが FIB（Forwarding Information Base）に登録されていた場合でも，その ID 以外のノードへ FIB の情報を変更できない場合は経路変更を行わない．これは FIB に登録されているノードも攻撃の影響によってそのノード以外のノードが生成した汚染コンテンツを転送しただけである可能性もあるとし，そのノードを転送先に記録するエントリを削除してしまうと，ネットワーク的に孤立が発生する可能性があるためである．

また，リストの更新は検証結果を得たときだけでなく，傍受によるキャッシュ済みコンテンツの検証を行った時も更新を行うことで早期の攻撃者検知を狙う．

4.6　比較手法

提案手法がオーバヘッドをどれだけ削減できているかを評価するために用いる比較手法について述べる．比較手法では，コンテンツ取得後に IP 通信を用いた検証のみを行う．比較手法では攻撃者検知の有効性を調べるため，検証結果を利用した攻撃者検知も行わない．

比較手法の利点は確実な検証結果を得られる点であるが，検証の末に不審なコンテンツであることが判明しても，経路変更を行わないため攻撃者の汚染が終わるまで正しいコンテンツを得ることが出来ない点が欠点である．

4.7　攻撃動作

本論文が想定する環境下でのコンテンツ汚染攻撃について述べる．攻撃者は一般のノード中に混在するとともに，自身を経由して転送される Data を汚染する．また，攻撃者は一般のノードと同様にコンテンツを取得するため Interest を送信する．

4.8　実験環境

提案手法の性能評価に用いたシミュレーション諸元を表 1 に示す．本評価では提案手法と比較手法の 2 つのパターンのデータ計測を行う．比較手法は協調検証や検証結果を利用した攻撃者検知は行わない．攻撃者は自身を経由して転送される Data を汚染する．今回は複数台の攻撃ノードを集中的に配置し攻撃する集中型と，分散配置して攻撃する分散型を考える．

表 1　シミュレーション諸元

条件	値
シミュレーション時間	1000〜5000（sec）
ノード数	16〜64（台）
攻撃者数	0〜2（台）
閾値 S	0.3〜0.7
コンテンツ数	100（個）

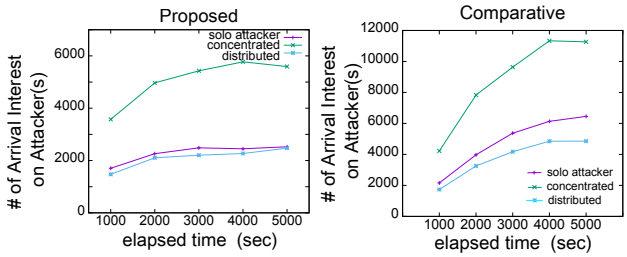

図 8　攻撃者の Interest 受信数

5. 評価結果

5.1 攻撃者の Interest 受信数

図 8 はシミュレーション経過時間と攻撃者の Interest 受信数の関係を示す．同図から分かるように，提案手法では，一定時間が経過するとそれ以降は攻撃者は Interest を受信しなくなる．これは，提案手法の攻撃者検知と適切な経路変更により，一般ノードは Interest を安全な経路で転送することにより，安全なコンテンツを得ることができたためである．

5.2 検証回数

IP を用いた検証で得られたコンテンツをキャッシュヒット時に他ノードに転送した際の検証省略効果を評価する．

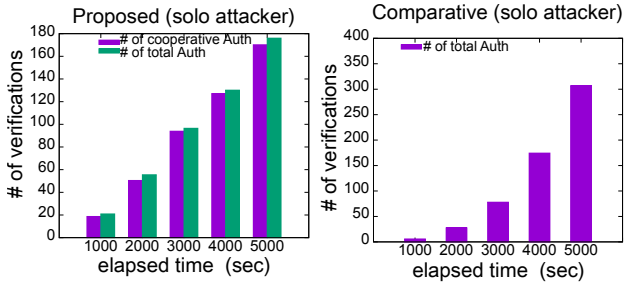

図 9　検証回数 (単一攻撃者)

図 9 の結果から提案手法の検証回数は比較手法の約 55%に低下していることがわかる．これは，提案手法の全検証数の約 90%は協調検証で実施されたことによる．

5.3 検証に要した平均ホップ数

IP を用いた検証は確実にコンテンツの真正性を確認できることが大きな利点であるが，プロバイダとノード間の距離が離れるほど，検証に要するホップ数は増加しオーバヘッドは増加する．しかし，提案手法の協調検証では，コンテンツ要求ノードの周辺ノードのキャッシュを利用することで最短距離である 2 ホップの検証をおこなう．本節では，提案手法はノード数を様々に変化させたトポロジにおいて，協調検証を少ないホップ数で実施できるかを評価する．

表 2 に示すように，提案手法の検証時のホップ数は 2.7〜2.8 であり，比較手法は 3.8〜4 ホップであることがそれぞれわかる．

表 2　手法別の検証時のホップ数

ノード台数	提案手法（hop）	比較手法（hop）
16	2.78	3.40
25	2.76	3.98
36	2.72	3.89
49	2.73	3.88
564	2.71	3.82

提案手法では，ノード数の増加にかかわらず，ほとんどの検証が図 10 の経路①のように 2 ホップでの協調検証によって行われているため少ないホップ数となる．ここで，実際のホップ数が 2 ホップより大きくなったのは，少ない回数ながら IP による検証が発生し経路②のような経路で検証が行われたためである．

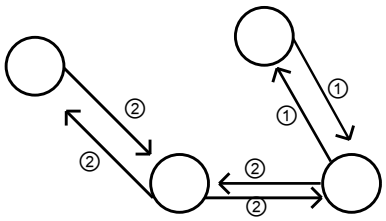

図 10　手法によるホップ数

さて，比較手法においてユーザは 2 ホップ以上先に存在するプロバイダとのみ検証をおこなうため，ノード数が増えた場合，提案手法より大幅にホップ数は大きくなる．しかし，比較手法ではノード数が増加した場合でも，検証に要したホップ数は変化しないこともわかる．

これは隠れ端末問題によって末端ノードのコンテンツ取得率が著しく低下し，末端において検証自体がほとんど発生しないためである．

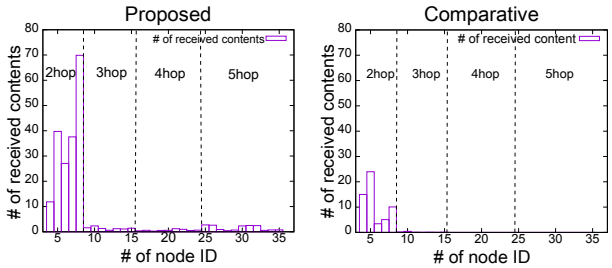

図 11　ノード別コンテンツ取得数

図 11 から，提案手法と比較手法はともに，プロバイダから離れた場所に位置するノードのコンテンツ取得率が著しく低下していることがわかる．よって MANET-NDN 下では，隠れ端末問題によるコンテンツや検証パケットの衝突によって末端ノードへの配送効率が著しく低下するため，隠れ端末問題を解決する制御手法の実装も必要であることがわかる．

5.4 受信コンテンツ数とキャッシュヒット率

図 12 に総受信コンテンツ数と，そのうちキャッシュから返送された数を示す．

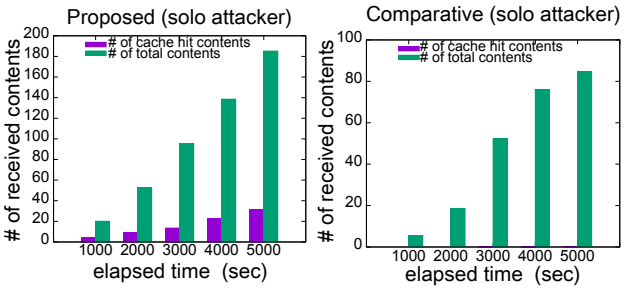

図 12 コンテンツ受信数 (単一攻撃者)

同図に示す結果より，提案手法は攻撃下であってもキャッシュヒット率は約 15%となること，コンテンツの取得量も比較手法の 2 倍の 180 コンテンツとなることがわかる．しかし，同図に示すように比較手法ではコンテンツの取得量は最大 80 コンテンツほどになり，キャッシュヒットはほぼ発生しないことがわかる．

図 9，12 から，提案手法は少ない検証回数でコンテンツ取得数とキャッシュ利用率を向上させることがわかる．

提案手法では，コンテンツ取得時に周辺ノードにランダムに検証要求をおこなう．しかし，自身よりも下流に位置するノードに対して検証を依頼した場合，キャッシュがないために検証できない可能性が高い．そのため，自身が検証を依頼するコンテンツのキャッシュを保持している確率が高い自身より上流のノードに対して検証を依頼するアルゴリズムの実装が必要となる．

5.5 受信コンテンツの人気度分布

ここまで，提案手法は効率的な検証と攻撃の検知により，攻撃下においてもコンテンツの効率的な配送が可能であることを示した．しかし，提案手法には検証依頼を受けたノードのキャッシュの該当コンテンツの有無によってコンテンツの取得効率が変化すると考えられる．

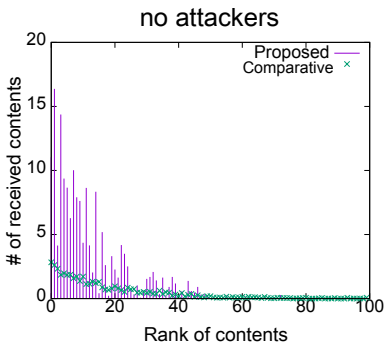

図 13 人気度別コンテンツ取得量

図 13 は検証の結果正しいコンテンツとして判定されたコンテンツの人気度分布である．どちらも Zipf 則に則ったコンテンツ分布となっているが，提案手法の方がばらつきは多く，人気度の低いコンテンツの取得率が低い結果になった．

6. おわりに

本稿では，MANET 環境に NDN を適用した MANET-NDN において，コンテンツ汚染攻撃に対し新たな対策手法を提案した．提案手法は各ノードが周辺と自律分散的に協調しコンテンツの真正性確認を行うことで検証オーバヘッドを削減し，コンテンツ汚染攻撃下でも安全な通信ができることを示した．

参考文献

[1] 朴 容震 : 情報指向ネットワーキングの研究動向 (online), http://gits-db.jp/bulletin/2012/papers/2012-2013.web.8-13.pdf.pdf.

[2] NTT コミュニケーションズ: Content Delivery Network(online), http://cn.ntt.com/jp/services/network/cdn.html.

[3] 森下 民平: P2P アーキテクチャ (online), https://www.cac.co.jp/softechs/pdf/st2501_07.pdf.

[4] Microsoft : Skype(online), https://www.skype.com/ja/.

[5] L. Zhang, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang: Named Data Networking(online), http://www.caida.org/publications/papers/2014/named_data_networking/named_data_networking.pdf.

[6] N. Fotiou, P. Nikander, D. Trossen, G. Polyzos : Developing information networking further: from PSIRP to PURSUIT(online), https://www.researchgate.net/publication/228826668_Developing_information_networking_further_from_PSIRP_to_PURSUIT.

[7] ネットワークエンジニアとして : Common key cryptosystem / Public key cryptosystem(online), https://www.infraexpert.com/study/security4.html.

[8] D. Kim, J. Bi, A. Vasilakos, I. Yeom: Security of Cached Content in NDN, IEEE Trans. on Forensics AND Security, vol.12, no.12, pp. 2933 – 2944, 2017.