パブリックスペース設置型無線APにおけるダウンリンク帯域の不正占有対策

新田 翔平[1,a)]　重安 哲也[1]

概要：スマートフォン等の無線端末の急速な普及に伴い，LTE（Long Term Evolution）方式を用いた携帯電話網へのアクセストラフィックが急激に増加している．そのため，アクセストラフィックを光ファイバ等の有線回線に接続された無線 AP（Access Point）にオフロードすることで，LTE 網への負荷を軽減することが求められている．しかし，不特定多数の人が利用するパブリックスペースに設置される無線 AP では AP を利用するユーザ間に社会的なつながりが存在しないため，他者よりも自端末のみの通信を優先する利己的なユーザの出現が問題となる．そこで，本稿では，無線 AP のダウンロード帯域の獲得を目的とする不正行為への対策として，既存端末との通信の互換性を維持しながら効果的に不正行為の影響を排除できる手法を提案する．また，提案手法を計算機シミュレーションによって評価した結果，1）無線 AP のみに提案手法を導入した場合であっても，ネットワーク端末間の公平性を維持しながら不正行為による影響をほぼ無効化できること，ならびに，2）AP が競合なしに効率的に連続送信することでスループットを不正端末なしのネットワークよりも向上できることの 2 点を明らかにする．

1. はじめに

LTE 回線を利用するスマートフォンやタブレットといった無線端末の急速な普及の結果，大幅に増加したアクセストラフィックに耐えられず，LTE 回線が通信障害を引き起こすなどの事例が報告されている [1][2]．そのため，LTE 回線へのアクセストラフィックを光ファイバに接続される無線 AP にオフロードすることで，LTE 回線の負荷を大幅に軽減することが求められている [3][4]．

しかし，会社や学校のように同じ組織に所属するユーザ間で利用することを前提としたプライベートスペース設置型の無線 AP とは異なり，不特定多数の人が利用するパブリックスペース設置型の無線 AP では，これを利用するユーザ間にはそもそも社会的な関係性が存在しないために，自端末のみの通信を優先し，他の端末よりも多くの帯域を獲得しようとする利己的なユーザの出現が問題となる．

利己的なユーザが複数ユーザで共有すべき通信帯域を独占してしまうと，ユーザ端末間の通信の公平性は大きくくずれることとなり，結果として，そのような無線 AP は LTE 回線のオフロード先としての役目を果たすことができなくなる．そのため，トラフィックオフロードを目的としてパブリックスペース設置型の無線 AP を利用するためには利己的なユーザの不正行為を抑制し，端末間の公平性を維持する手法が必要となる．

利己的なユーザによる不正行為を検出し，これを抑制するためにこれまで多くの議論が行われているが [5][6]，その多くが利己的ユーザが送信元となることを想定したアップリンク帯域の不正獲得を対象とした議論であり，利己的ユーザが受信側になることを想定したダウンリンク帯域の不正獲得を対象とした議論はこれまであまり行われていない．

しかしながら，スマートフォンやタブレットといった現状のスマートデバイスを用いた通信では動画や音声の受信といったダウンリンクトラフィックが主体となる通信が主な利用形態となっている [7]．そのため，これまでにあまり議論されてこなかったダウンリンクでの不正行為に対しても新たに十分な検討を行うことが必要となる．

さて，ダウンリンクの不正には IEEE802.11 規格の ACK（ACKnowledgement）フレームのヘッダに記載されるデュレーション値を操作する方法 [8] がある．同不正手法では，ACK のデュレーション値を 0 以上の値に設定することで，これを傍受した他の端末に対して不正に NAV（Network Allocation Vector）を設定させる．NAV 期間が設定された端末は，同期間が経過するまでの間，新たな送信が禁止されてしまう．そのため，利己的端末のみが，他端末との競

[1] 県立広島大学
Prefectural University of Hiroshima, 1-1-71 Ujinahigashi Minamiku, Hiroshimacity, 734-8558, Japan
[a)] q104033be@pu-hiroshima.ac.jp

合なしに連続的に送信を行うことになる．

ここで，利己的端末が TCP（Transmission Control Protocol）トラフィックを受信している場合は，ACK のデュレーション値の不正をサーバからの TCP セグメント受信後に実施することで，自身の TCP-ACK を即座に返信し，TCP フローのウィンドウサイズを他端末のそれよりも短い期間で増加させることでダウンリンク帯域を独占することができる．不正端末が帯域を独占すれば，通常端末のスループットは大幅に低下し，端末間の公平性は大きく低下する．

この不正行為に対して，無線端末間で不正端末が設定する NAV 期間を破棄することで通常通り通信を行うという対策が提案されているが [8]，これを行うには全ての端末がその手法を実装することが必要となるため，現実的な対策としては考えにくい．そこで，AP 一台のみを変更することで不正行為を抑制する新たな方法が求められる．

本稿では，不正端末が ACK 返信時に設定した NAV 期間の間に AP において受信された不正端末のデータパケットを有線ネットワーク側に中継せずに破棄することでその影響を抑制する方式を提案する．また，計算機シミュレーションによる評価結果から，提案手法を用いることで，不正端末を抑制しない場合と比べて，通常端末のスループットが向上し，公平性が改善することを明らかにする．

以下，2 章ではこれまでに報告されている不正な帯域獲得を目的とした不正行為の概要を，3 章ではこれに対する提案方式についてそれぞれ述べる．4 章は提案方式の性能評価によってその有用性を明らかにし，5 章において本稿のまとめを述べる．

2. 通信帯域の不正獲得手法

通信帯域の不正獲得対象はアップリンクとダウンリンクの 2 種類に大別できる．以下，本章では，それぞれの不正行為の概要について述べる．

2.1 アップリンクでの不正な帯域獲得

IEEE802.11 型の無線 LAN では CSMA/CA（Carrier Sense Multiple Access / Collision Avoidance）方式を採用している．CSMA/CA 方式では，データ送信前に固定長の IFS（Inter Frame Space）時間と CW（Contention Window）以下の乱数で生成されたバックオフ時間の待機をキャリアセンス動作と組み合わせることで，複数端末による同時送信に起因するフレームの衝突を防ぐ．

さて，文献 [6] によって報告されているアップリンクにおける不正行為は AP に対する送信機会をその他の端末よりも多く獲得するために，IFS 時間と CW の設定範囲を通常より小さく設定することで，他の端末よりも短い時間多くのデータフレームを送信する．この不正行為の概要を図 1 に示す．

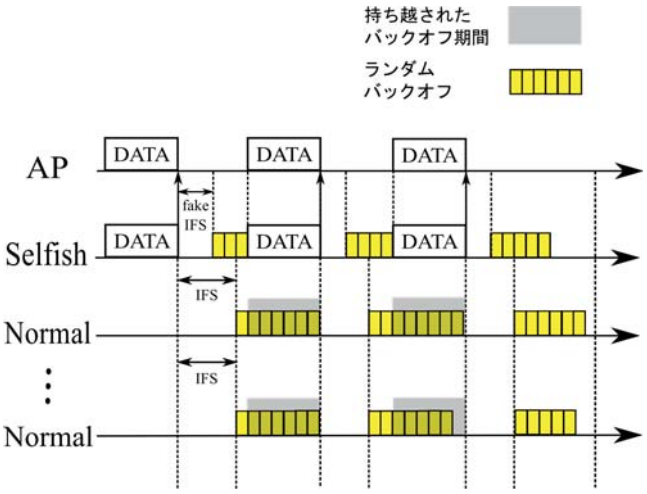

図 1 IFS と CW の不正設定

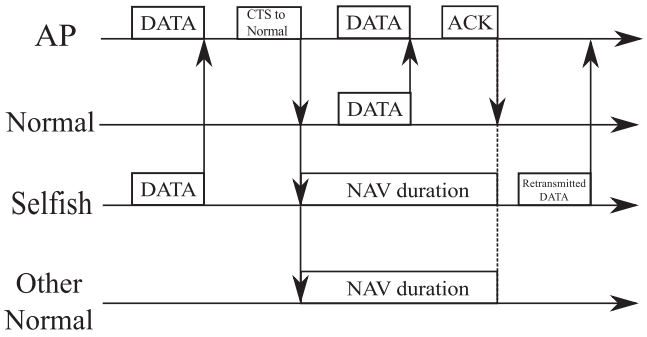

図 2 CTS による不正行為対策

また，これに加えて不正端末では，自身の送信するフレームの衝突が発生した際には本来であれば CW の値を 2 倍に増加させなければならないバイナリバックオフの操作を行わないため，常に他の端末よりも優先して送信を開始することができる．

このバックオフ期間短縮の不正行為に対して，不正端末を検出する手法も検討されている [5]．また，検出された不正行為に対する対策として，AP から送信機会がうばわれた端末に対して CTS（Clear To Send）を送信し，送信権を付与することで端末間の公平性を調節する方式 [6] が提案されている．図 2 は提案方式の概要を示す．

この提案方式では AP が不正端末からのデータフレームを受信した際に，ACK ではなく通信を付与したい通常端末宛ての CTS を返信する．CTS を傍受した不正端末は NAV が設定されるため，通常端末は不正端末に邪魔されることなく送信を行うことができる．このように不正端末の送信を抑制し，通常端末の送信機会が公平になるように通常端末宛てに CTS を送信することで通常端末間の公平性を維持する．

2.2 ダウンリンクでの不正な帯域獲得

以下では，2 種類のダウンリンクでの不正行為について述べる．

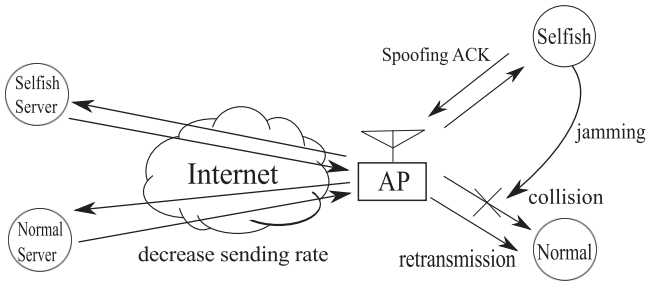

図 3 なりすまし ACK

2.2.1 なりすまし ACK[8]

ダウンリンクでの不正行為の一つになりすまし ACK（Spoofing ACK）がある [8]．図 3 になりすまし ACK の概要を示す．同図において AP が他の端末宛てにデータフレームを送信していることを傍受した不正端末（Selfish）は意図的に他の端末（Normal）が受信しているデータフレームに自身が送信するフレームをぶつける（jamming）ことで，受信を妨害する．ここで，衝突の発生により，Normal からの ACK が返信されなければ AP は同じ端末宛てにフレームの再送を繰り返してしまうため，Selfish は Normal になりすまして AP に ACK を送信することで，AP 側に Normal の受信失敗を検知させることなく AP の再送を回避する．

一方，Normal は DATA の受信に失敗するだけでなく，TCP-ACK をサーバ側に返信することがないため，TCP を使用したセッションでは，ウィンドウサイズが低下することによって使用帯域も減少する．このように自分以外の端末が使用する帯域を減少させる一方で，不正端末は自身の使用可能な帯域を増加させる．

しかし，この不正行為を実装するためには通常の IEEE802.11 とは異なる手順のプロトコルで不正端末の MAC（Media Access Control）動作をさせる必要がある．そのためには，新たなハードウェアの開発が必要な場合がほとんどとなるため，本不正行為が実際に行われる可能性はあまり高くないと考えられる．

2.2.2 ACK-NAV[8]

ACK のデュレーション値を 0 以上の値に設定し，自分以外の端末の送信を禁止するために，不正に NAV 期間を延長する不正行為を ACK-NAV と呼ぶ [*1]．同不正行為の概要を図 4 に示す．ここでは，不正端末を GR（Greedy Receiver），通常端末を NR（Normal Receiver）とそれぞれ表記する．

さて，通常の通信では，任意の端末がデータフレームを送信する際は，フレームのデュレーション値には一連の通信が完了するまでの予定期間が記録されており，同フレームを傍受した他の端末はそのデュレーションに記載された時間だけ NAV 期間が設定され，自身の新たな通信を延期する．

[*1] 文献 [8] において著者らはこの不正行為を ACK-NAV と呼んでいないが，本論文では便宜上これを ACK-NAV と呼ぶ．

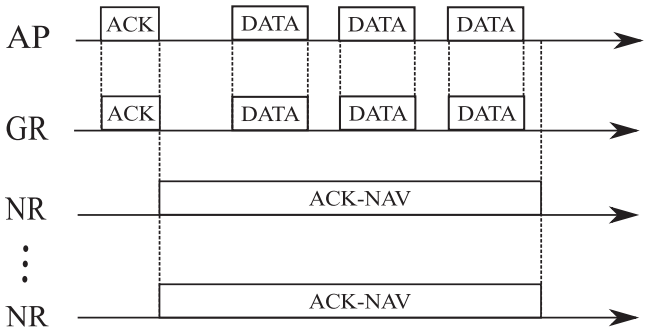

図 4 ACK-NAV

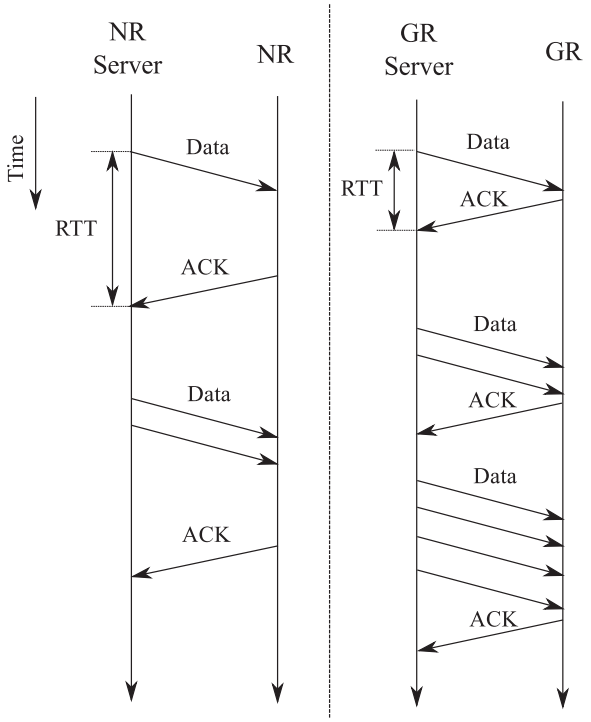

図 5 ACK-NAV による RTT 短縮の影響

これに対して，GR では，ACK を返信する際に通常は 0 の値が設定されるデュレーション値に 0 以上の値を設定し，周囲の端末に不正に NAV 期間を設定する．結果として，自身のみが通信可能な状況を作り出す．また，不正端末は受信した TCP セグメントに対する ACK を即座に返信し，送信側で計測される RTT（Round Trip Time）を小さくすることで，自身を宛先とする TCP フローの輻輳ウィンドウのサイズを増加させていく．このようにして，不正端末は他の通常端末よりも多くの帯域を占有する．その概要を図 5 に示す．

さて，この不正行為は ACK のデュレーション値というパラメータを変更するだけで実施可能な行為であるため，前節の不正手法と比べて実際に実施することは容易となっている．

2.2.3 ACK-NAV による帯域占有

ACK-NAV によるダウンリンクの帯域不正獲得の影響を図 6 に示すネットワークトポロジを用いて評価する．同図

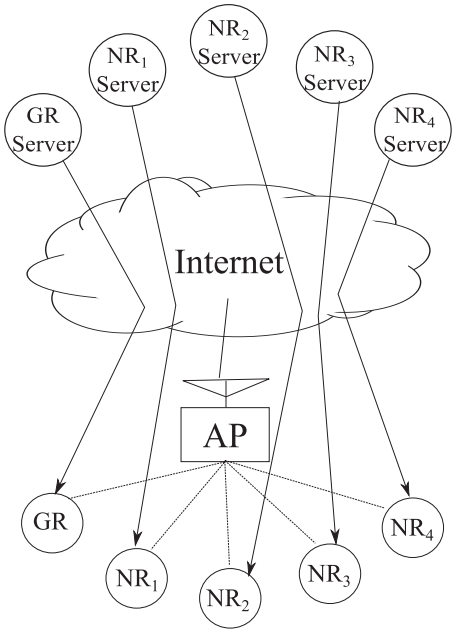

図 6 評価ネットワークのトポロジ

の端末 5 台のうち，1 台は ACK のデュレーション値を不正に大きな値に設定する不正端末（GR），その他の 4 台は通常端末（$NR_i(i \leq 4)$）とする．

次に，不正端末による帯域占有の影響と ACK デュレーション値の大きさとの関係性を確認するために，不正端末の ACK が設定するデュレーションの値を 0.1〜30ms の範囲で変化させた．これらの状況下における通信特性は QualNet6.1 を用いて評価した．表 1 は評価に用いたシミュレーション諸元を示す．

表 1 シミュレーション諸元

項目	設定値
無線規格	IEEE802.11b
アプリケーショントラフィック	FTP
無線伝送速度	11Mbps
有線伝送速度	100Mbps
シミュレーション回数	100 回
シミュレーション時間	100 秒

2.2.4 受信スループット

端末 5 台の受信スループットの合計値を図 7 に示す．同図から不正端末の NAV 値が 15ms 以上の場合は受信スループットが減少していることが分かる．この理由は NAV 値を増加させることで増加した不正端末のスループット値よりも通常端末の減少したスループットの合計値が上回ったためである．

一方，NAV 値が 25ms 以上なると受信スループットは逆に増加していく．これは不正端末が帯域をほぼ占有し，自身のスループットを急激に増加させたためであると考えられる．

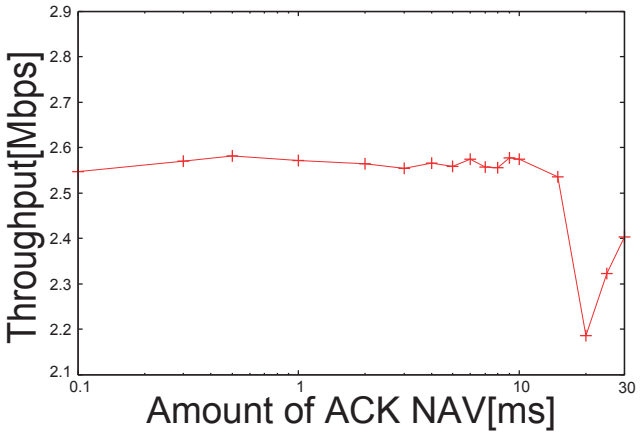

図 7 スループット

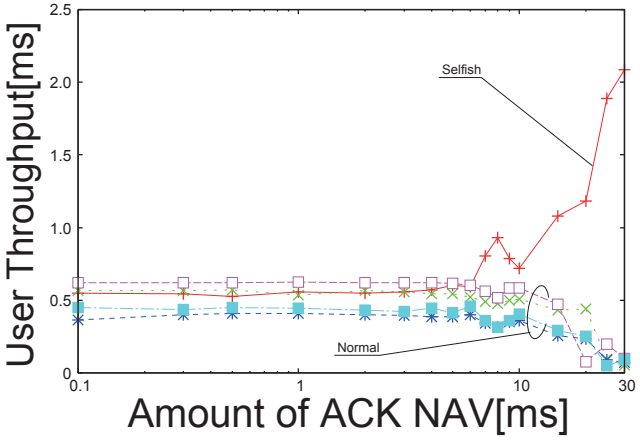

図 8 各端末のスループット推移

2.2.5 ユーザスループット

図 8 に端末ごとの受信スループットを示す．同図から NAV 値が 10ms 以上では，NAV 値の増加に比例して，不正端末のスループットが急激に増加するが，逆に，通常端末のスループットは減少することがわかる．特に，デュレーションとして ACK に設定可能な値の上限値 [9] 付近となる 30ms の付近の NAV 値では，NR_1〜NR_4 はほとんど帯域が獲得できていないことがわかる．

このことから，不正端末が ACK の NAV 値を増加させる一方で，通常端末の帯域が多く奪われ，帯域が不正に使用されることがわかる．

2.2.6 Fairness Index

本節では，ネットワークの公平度を Fairness Index [10] を用いて評価する．Fairness Index とはネットワーク資源の割り当ての公平度を定量的に評価する指標であり，以下の式で算出される．

$$FairnessIndex = \frac{\left(\sum_{i=1}^{n} x_i\right)^2}{n\sum_{i=1}^{n} {x_i}^2} \quad (1)$$

ここで，n は端末数，$x_i(i \leq n)$ は各端末の受信スループットをそれぞれ表す．Fairness Index は 0〜1 の間の値を

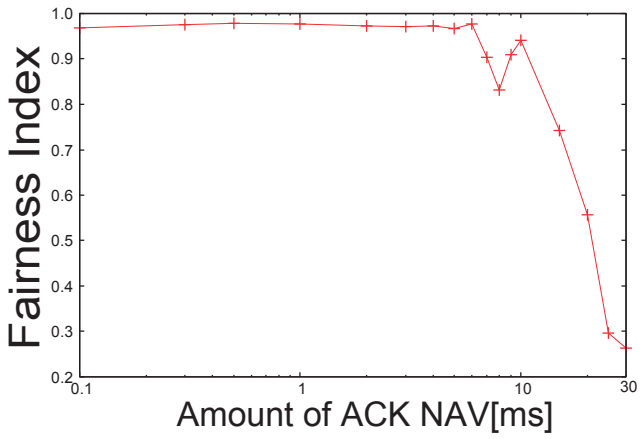

図 9 Fairness Index

とり，この値が 1 に近いほど端末間の受信スループットの公平性が高いことを意味する．

図 9 は図 8 に示した端末 5 台の受信スループットの値を Fairness Index によって評価したものである．同図から NAV 値が増加するにつれて Fairness Index は低下することがわかる．これは，NAV 値の増加とともに不正端末が帯域を占有する量が増加するのに反して，通常端末のそれが減少することで，不正端末と通常端末のスループット差が大きくなったためであると考えられる．

2.2.7 まとめ

本章における議論から，不正端末が設定する NAV 値が大きくなるほど，不正端末が占有する帯域は増加すること，同時に通常端末の帯域が減少することがそれぞれ確認された．また，ACK-NAV の不正行為が実施されてしまうと，無線区間全体の総受信スループットが低下し，公平性が大きくくずれることで，無線 LAN へのトラフィックオフロードの大きな妨げになる．

さて，文献 [8] では，ACK-NAV への対策として，設定された NAV 期間が不正端末によって不正に設定されていた場合，これを端末側で破棄することによってその影響を排除することを提案しているが，このような方法では，全ての端末の設定を変更する必要があり，現在のように非常に多くの端末が普及してしまった状況では，その実現は困難である．そのため，本稿では無線 AP1 台のみの変更で不正端末の影響を抑制する方法を以降の章で検討する．

3. 提案方式

本稿で提案する制御方式の動作について述べる．

3.1 提案方式の動作

不正端末の影響を抑制する方法として，以下 2 方式を提案する．

(1) 不正端末の送信回数増加の抑制（方式 1）：不正に設定された NAV 期間に，AP が受信した不正端末のデータフレームを破棄する．

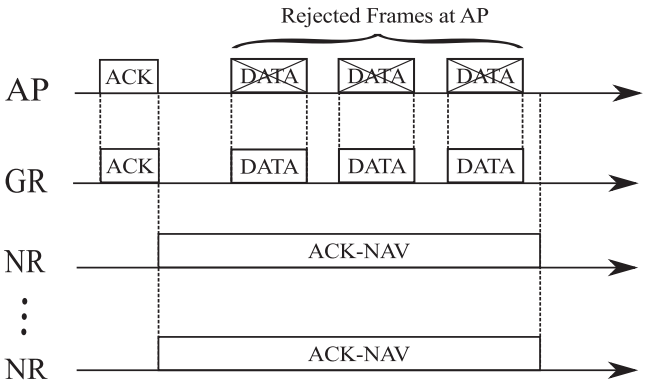

図 10 方式 1 の動作

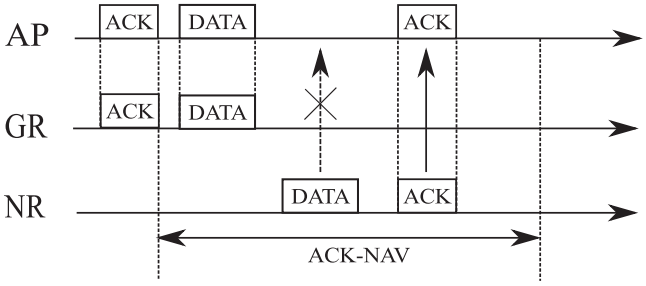

図 11 NAV 期間内の ACK 返信

(2) 全ての端末に向けたダウンリンクスループットの増加（方式 2）：上記の方式に加えて，不正 NAV 期間の間だけ AP のバックオフ値を 0 にする．

以上 2 つの動作の詳細を次節で述べる．

3.1.1 不正端末の送信回数増加の抑制（方式 1）

同方式の動作の概要を図 10 に示す．提案方式では，AP が ACK を受信する際に，デュレーション値の妥当性を検査する．ここで，不正なデュレーション値を持つ ACK の受信を検知すると，AP は ACK の送信元と不正デュレーション期間を記録する [*2]．

次に，AP は不正に設定された NAV 期間において，通常端末のデータフレームを受信した場合は破棄せずに有線ネットワーク側に中継するが，不正端末と判定された端末からのデータフレームは全て破棄する．

このように，不正 NAV 期間中の不正端末のデータフレームを破棄することで，TCP の輻輳制御により不正端末宛ての送信レートは低下するため不正行為の影響を抑制できると考えられる．また，通常端末は NAV 期間内に新たなデータフレームの送信を開始することはできないが，受信したデータフレームに対する ACK は返信することができる [11] ため，AP が NR 宛に送信を行った場合にも ACK のタイムアウトによるスループットの低下は起こらない．その様子を図 11 に示す．

[*2] ここで，IEEE802.11 における ACK フレームのヘッダには，送信元アドレスは記載されていないが，ACK と対応する DATA に記載した送信先アドレスから，ACK の送信元を特定する．

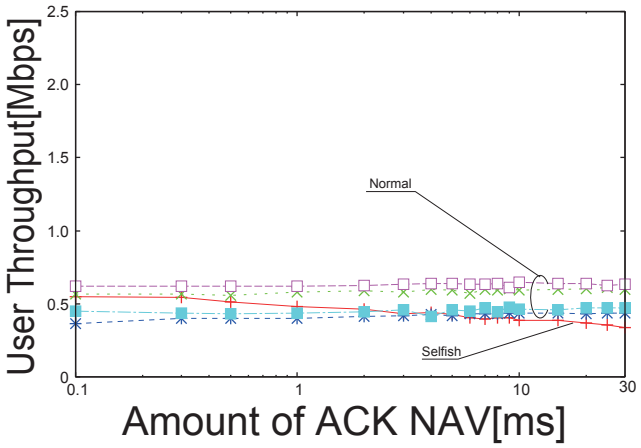

図 12 方式 1 を実装した場合の各端末のスループット

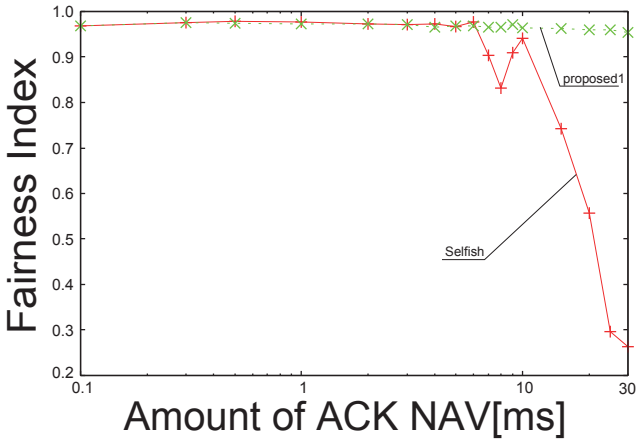

図 13 Fairness Index

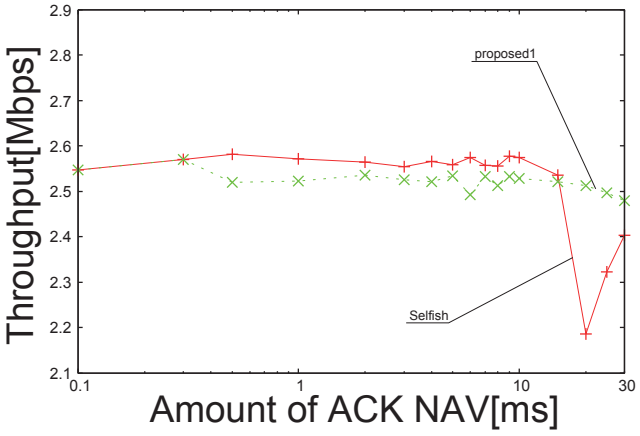

図 14 総スループット

3.1.2 全ての端末に向けたダウンリンクスループットの増加（方式 2）

提案方式では，前述した動作に加えて，不正に設定された NAV 期間において AP のバックオフ値を 0 にする．

これは，不正端末によって設定された NAV 期間に通信を行うことができるのは AP と不正端末の 2 端末だけであるため，AP のバックオフ値を 0 にすることで，AP の送信機会を増やしてもフレーム同士の衝突は発生しにくいためである．結果として，同期間を利用したバックオフ 0 による連続送信によって AP の送信キューにたまっているパケットを効果的に送信することで，全ての端末の受信スループットが向上すると考えられる．

4. 提案方式の評価

本章では，2 章で実施したシミュレーション評価と同じ環境に 3 章で提案した方式を実装した場合の性能を評価する．

4.1 方式 1 のシミュレーション結果

4.1.1 ユーザスループット

図 12 に方式 1（proposed1）を実装した場合の端末ごとの受信スループットを示す．方式 1 を実装することで，不正端末が ACK-NAV の不正を行った場合にも端末の不正な帯域獲得を抑制し，通常端末のスループットの低下も抑制されていることが確認できる．

4.1.2 Fairness Index の向上

次に Fairness Index を図 13 に示す．同図から，ACK-NAV の値が変化しても Fairness Index は 0.96 付近で安定していることが分かる．これは，方式 1 を実装し，不正端末の影響を抑制することで，端末ごとのスループットのばらつきが小さくなり，公平な通信が実現できているといえる．

4.1.3 総スループット

方式 1 を実装したときの端末 5 台の受信スループットの合計値を図 14 に示す．同図から，NAV 値が 10ms 以上になると総スループットは低下していき，30ms では不正端末が存在しない場合と比べて，0.08Mbps 低下することがわかる．これは，不正に設定された NAV 期間に通信を行っているのは AP と不正端末の 2 つのみであるため，NAV 期間が長いほど，帯域がどの端末にも使用されないチャネルのアイドル時間が増加するために，総スループットが低下したと考えられる．

4.2 方式 2 のシミュレーション結果

4.2.1 ユーザスループット

方式 2（proposed2）を実装したときのユーザスループットを図 15 に示す．同図から方式 2 では方式 1 のユーザスループットと比べると，全体的に向上していることが分かる．これは，NAV 期間に AP の送信機会を増やし，AP 内のキューにたまったパケットを送信することで，方式 1 と比べて，無駄なく帯域が使用されているためと考えられる．

4.2.2 Fairness Index

次に，Fairness Index を図 16 に示す．同図から，方式 2 を実装した場合も方式 1 と同様に高い Fairness Index を維持している．このことから，方式 2 の導入後も同様に公平な通信状況が維持されているといえる．

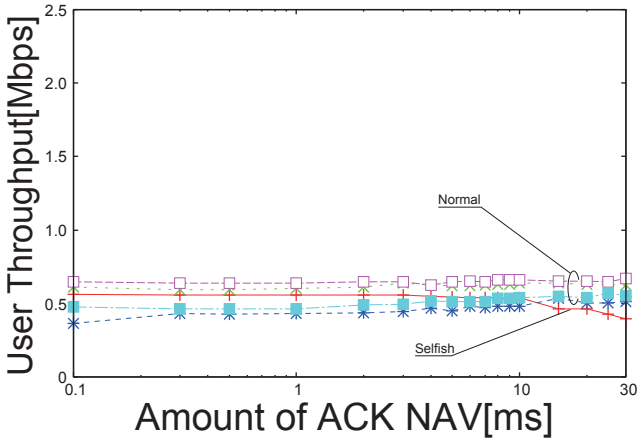

図 15 方式 2 を実装した場合の各端末のスループット

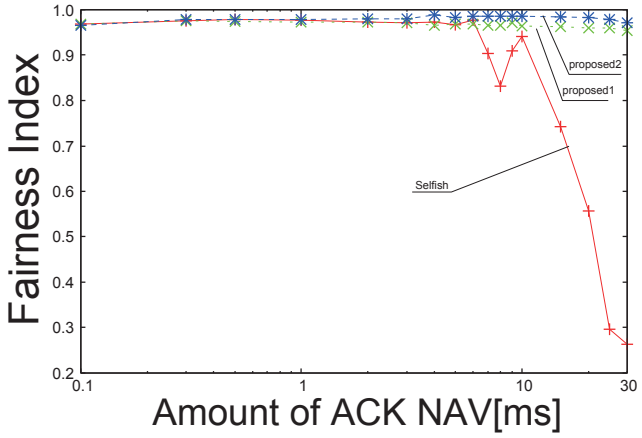

図 16 Fairness Index

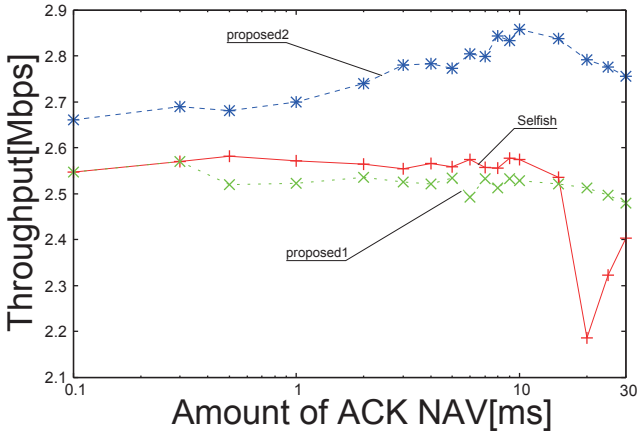

図 17 スループット

4.2.3 総スループット

方式 2 を実装したときの端末 5 台のスループットの合計値を図 17 に示す．不正度合いが大きくなるにつれて，総スループットは低下していくが，最も不正度合いが強い 30ms でも 2.75Mbps であることから，不正端末が存在しない場合の受信スループットの 2.56Mbps よりも高い．これは，方式 2 によって AP 内のキューにたまったパケットを競合なしに，効率的かつ連続的に送信する機会が増えたため，全ての端末の受信スループットが増加したと考えられる．

5. まとめ

本稿では ACK のデュレーション値を 0 よりも大きな値に設定する不正行為の ACK-NAV による帯域使用の不公平状況について報告し，その不正行為の制御方式を提案した．

計算機シミュレーションによる評価の結果，NAV 期間だけ不正端末のデータパケットを AP が全て破棄するという簡単な方式 1 のみでも，不正端末の影響を軽減することはできたが，総スループットの低下を防ぐことはできなかった．しかし，方式 1 に NAV 期間だけ AP のバックオフ値を 0 にして，AP の送信機会を増やす手法を追加した方式 2 では，全ての端末の受信スループットが向上し，不正端末が存在しない場合と比べて，高いスループットを達成できることを明らかにした．

参考文献

[1] 佐藤 仁：海外での通信障害：日本との違い，InfoCom ニューズレター（オンライン），入手先（http://www.icr.co.jp/newsletter/global_perspective/2013/Gpre201311.html）（参照 2014-08-18）.

[2] NTT docomo：ドコモからのお知らせ：一連のネットワーク障害への対策について，NTT docomo（オンライン），入手先（https://www.nttdocomo.co.jp/info/notice/page/120127_00.html）（参照 2014-08-20）.

[3] Wi-Fi オフロードにまい進する 通信事業者，日経コミュニケーション，no.9, pp.84-85 (2011).

[4] 木村龍明，奥田隆史，井手口哲夫，田学軍：公衆無線 LAN によるデータダウンロードサービスにおけるユーザの協調行動の有効性に関する研究，電子情報通信学会技術研究報告 vol. 112, no. 307, pp. 57–62 (2012).

[5] 武次潤平，榊原勝己：IEEE802.11 無線 LAN における不正検出のための正規バックオフ測定値推定法の検討，電子情報通信学会技術研究報告 vol. 111, no. 409, pp. 53–58 (2012).

[6] 世良勇樹，小畑博靖，村瀬勉，石田賢治：WLAN 環境におけるアクセスポイントを用いた MAC 改造端末に対する制御方式，電子情報通信学会技術研究報告 vol. 113, no. 5, pp. 7–12 (2013).

[7] A. Schulman, D. Levin, N. Spring：On the Fidelity of 802.11 Packet Traces, Proc. of Passive and Active Network Measurement (Lecture Notes in Computer Science Volume 4979), pp 132-141 (2008).

[8] M. Han, L. Qiu：Greedy Receivers in IEEE 802.11 Hotspots: Impacts and Detection, Trans. on IEEE Dependable and Secure Computing, vol.7, pp.410–423 (2010).

[9] M. Loukides：802.11 Wireless Networks The Definitive Guide, O'REILLY (2002).

[10] R. Jain, W. Hawe, D. Chiu：A Quantitative measure of fairness and discrimination for resource allocation in Shared Computer Systems, DEC-TR-301 (1984).

[11] IEEE802.11: IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE (2012).