Vol.2011-DPS-149 No.3
2011/11/24

IEEE802.15.4 ビーコンモードにおける完全衝突解決アルゴリズム

伊達仁美[†1]　重安哲也[†1]

環境モニタリングにおけるセンサ間接続のための通信規格として広く利用される IEEE802.15.4 では，ビーコンモードでのチャネルアクセスにスロット化 CSMA/CA を使用する．CSMA/CA では，キャリアセンスとスロット化ランダムバックオフによってデバイス同士のパケット衝突を回避するプロトコルであるが，キャリアセンスが働かないエリアに端末が存在する場合は隠れ端末問題によってパケット衝突が発生する．本稿では，キャリアセンスが機能しないエリアの端末とのパケット衝突も回避するために，デバイスの送信要求に応じてコーディネータが送信権を割当てる手法を提案し，同手法によってパケットの送信成功確率が向上することについて報告する．

A New Solution for Packet Collisions on IEEE802.15.4 Beacon Mode

Hitomi Date[†1] and Tetsuya Shigeyasu[†1]

IEEE802.15.4 which is widely used communication standard to connect sensors for environmental monitoring, employs slotted CSMA/CA on beacon mode. Although CSMA/CA can avoid packet collisions by both slotted random backoff and physical carrier sensing, it can not avoid packet collisions caused by existence of hidden terminals locating outside of carrier sensing range. To reduce packet collisions, this paper proposes a new solution which allocates transmission opportunity on demand from device having transmission request. Simple analytical results confirm that our proposal can improve packet reception ratio than traditional IEEE802.15.4.

†1 県立広島大学 経営情報学部
Faculty of Management and Information Systems, Prefectural University of Hiroshima

1. はじめに

近年の ICT (Information and Communications Technology) 技術を用いたエコ社会の実現に対する希求から，環境モニタリングが盛んに行われるようになってきた．環境モニタリングでは，多種多様なデータを数多く取得する事で質の高い環境制御が実現できる事から，多くのセンサをネットワーク接続することでリアルタイムにデータを収集する仕組みが必要となる．

IEEE802.15.4 は大規模なセンサ群の間を無線接続することを目的に策定された無線 PAN (Personal Area Network) の標準規格であり，最大通信速度は 250kbps と低速ながら，低価格，低消費電力であることが望まれる無線センサネットワーク用の通信規格として，現在，大きな注目を集めている．IEEE802.15.4 では，送信チャネルへのアクセスモードとしてビーコンモードとノンビーコンモードが規定されているが，どちらのモードにおいても，パケット送受信を制御する MAC (Media Access Control) プロトコルには CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) が使用される．CSMA/CA を含む CSMA 系の MAC プロトコルは，キャリアセンスのみで高いスループット性能を達成できることから様々な通信システムにおいて広く使用されている．しかしながら，キャリアセンスのみでは送信端末の通信範囲外に位置する隠れ端末とのパケット衝突を回避できないため，一般的な CSMA 系の自律分散システムでは，RTS/CTS（Request To Send/Clear To Send）交換あるいは，ビジートーンなどの制御をキャリアセンスを組み合わせて用いられることが多い．

ところが，IEEE802.15.4 ではこれらの隠れ端末対策を併用しない CSMA/CA のみで送受信が行われるため，隠れ端末の存在するネットワークでは，高トラフィック時にパケット衝突の増加によって通信性能の低下を引き起こすと考えられ，結果として環境モニタリング性能も大幅に低下してしまう危険性がある．そこで，本稿では，IEEE802.15.4 のビーコンモードに着目し，同モードにおける隠れ端末に起因するパケット衝突を回避する手法として，CSMA/CA による送信権競合をパルス信号を用いる 2 進バックオフアルゴリズムに置換える方式を提案する．提案に引き続き，提案方式のパケット送信成功確率が既存の CSMA/CA に比べて優位である事を簡易な解析によって明らかにする．

2. IEEE802.15.4 におけるチャネルアクセスモード

IEEE802.15.4 を用いたセンサネットワークはコーディネータとデバイスによって構成さ

Vol.2011-DPS-149 No.3
2011/11/24

れる．同ネットワークにおいてコーディネータが定期的に送出するビーコン信号にデバイスが同期することで送受信を実施する方式をビーコンモード，逆にビーコンを用いずに送受信を実施する方式をノンビーコンモードとそれぞれよぶ．

ビーコンモードでは，各デバイスはコーディネータの送信するビーコン信号に含まれる情報からビーコン信号間のスーパーフレーム構造を認識する．スーパーフレームとは，デバイスがアクティブな期間を指しており，16 スロットに分割された CAP (Contention Access Period) と CFP (Contention Free Period) から構成される．デバイスはスーパーフレーム内の両ピリオドに対応した送信制御を実施することで間欠的な動作の実現が可能となる．

ビーコンモードとノンビーコンモードでは共に原則として CSMA/CA によってチャネルアクセスが行われる．特に，IEEE802.15.4 ビーコンモードではスロット化 CSMA/CA 方式が用いられる[1)]．

IEEE802.15.4 のビーコンモードにおける Super Frame 構造を**図 1** に示す．同モードの送信スロットは，スロット化 CSMA/CA で送信を制御する CAP と送信をコーディネータによって保証される GTS (Guranteed Time Slot) 通信を行う CFP から構成されるが[2)]，以下では，本稿がパケット衝突の解決に主眼をおいていることから，CAP のみからフレームが構成される場合のアクセス手順について述べる[⋆1]．

2.1 スロット化 CSMA/CA

ビーコンモードでは，ネットワークはビーコンを送出する 1 台のコーディネータと少なくとも 1 台以上のデバイス群から構成される．**図 2** に示すようにあるデバイスがコーディネータに向けて新たな送信を行う場合を考える．デバイスはまず，コーディネータのビーコンを受信することで同期を確立した後，バックオフとして r スロット待機する．

このとき r には，$[0, 2^{BE} - 1]$ から一様乱数によって 1 つの整数が選択される．r スロット経過後，デバイスは 2 回の CCA（Clear Channel Assesment）期間程チャネルを検査し，どちらもチャネルがアイドルであった場合，新たな DATA の送信を開始する．また，この DATA を正しく受信したコーディネータは ACK（Acknowledgment）を返信することで一連の動作を完了する[3)]．

2.2 CSMA/CA 方式の抱える問題点

前節にも述べたとおり，IEEE802.15.4 におけるスロット化 CSMA/CA では，コーディネータからのビーコンを受信することを契機に送信要求の生じたデバイスはバックオフ手続

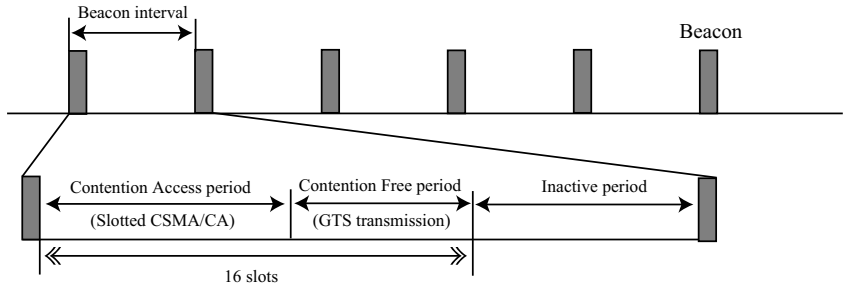

図 1 Super Frame structure of IEEE802.15.4

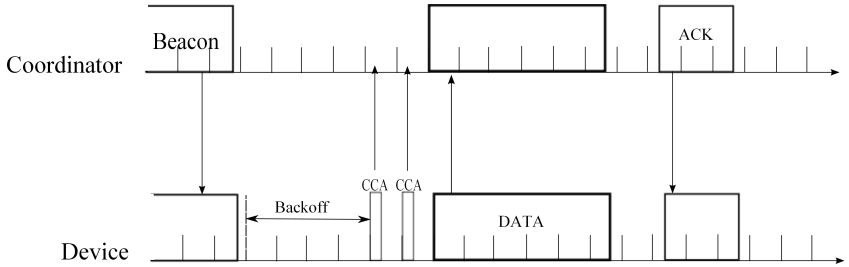

図 2 Slotted CSMA/CA on IEEE802.15.4

きを開始する．ここで，バックオフ期間はランダムに決定されるが，複数のデバイスが同一長のバックオフ期間を選択した場合は，必ずコーディネータ上でこれらの送信する DATA 同士が衝突し消失する．

パケット衝突が発生した場合は，バックオフ期間を長く再設定し再送を試みることになる．一般的に，送信トラフィックの増加に伴って衝突確率も増加し，スループットも低下する．

また，**図 3** に示すように，全てのデバイスがコーディネータの通信範囲内に存在した場合にも，任意の 2 つのデバイス同士が互いの通信範囲外にあった場合は，両端末が同一のバックオフ期間を選択しなかった場合にもコーディネータ上での衝突が発生する（隠れ端末問題）．

3. 2進カウントダウンを用いた完全衝突回避アルゴリズム

IEEE802.15.4 における衝突なしのチャネルアクセス方式として 2 進カウントダウンを用

⋆1 GTS 通信はオプション扱いであるため，CFP の長さを 0 にすることが規格上可能である．

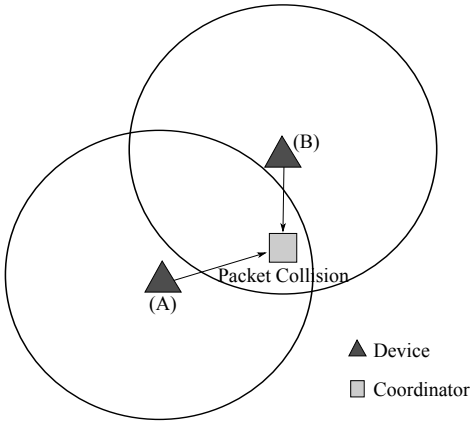

図 3 Hidden terminal problem on beacon mode

いる方式を提案する．同方式では，コーディネータが配下のデバイスに対して識別子をあらかじめ付与することを前提とする．識別子のビット数はデバイス数によって決定し，たとえば n 端末の場合は $\log_2(n+2)$ 以上の最小の整数とする．ここで，n+2 とした理由は，識別子がすべてビット 0 あるいは 1 のいずれかで構成される識別子はデバイスに割当てる事のないように除外するためである．この理由については後述するが，特に全てのビットが 1 であるようなアドレスは本方式ではコントロールアドレスとよぶ．

図 4 に示すように，提案方式における一連の送信手続きは競合期間と送信期間から構成する．競合期間は，ID entry と ID ACK とよぶ 2 つのフェーズの繰り返しで構成される．

まず，コーディネータはスロット化 CSMA/CA と同様に定期的にビーコンを配下のデバイスに向けて送出する．このとき，ビーコン中には配下の端末の識別子の長さの情報を含めて送信する．これに対して，送信要求のあるデバイスはビーコンに引き続き自身の識別子の先頭ビットをパルス信号として送出する（ID entry フェーズ）．ここで，コーディネータは自身のアンテナから一定以上の電力が検出された場合は，返信として同じくパルス信号を送出する（ID ACK フェーズ）．先の ID entry フェーズで自身がパルス信号を送出しなかった端末は，このコーディネータからのパルスを検出することで他の端末の新たな送信開始の可能性を知り，衝突を避けるためにスリープモードへ遷移する．

以上を識別子のビット数と同じ回数だけ繰り返すことで，高々，l つのデバイスのみが新たな送信を開始できることになる[4]．ここで，ビーコンモードではすべてのデバイスはコーディネータの通信範囲内に存在することから，コーディネータからのパルスを傍受することで隠れ端末との衝突も回避できる．

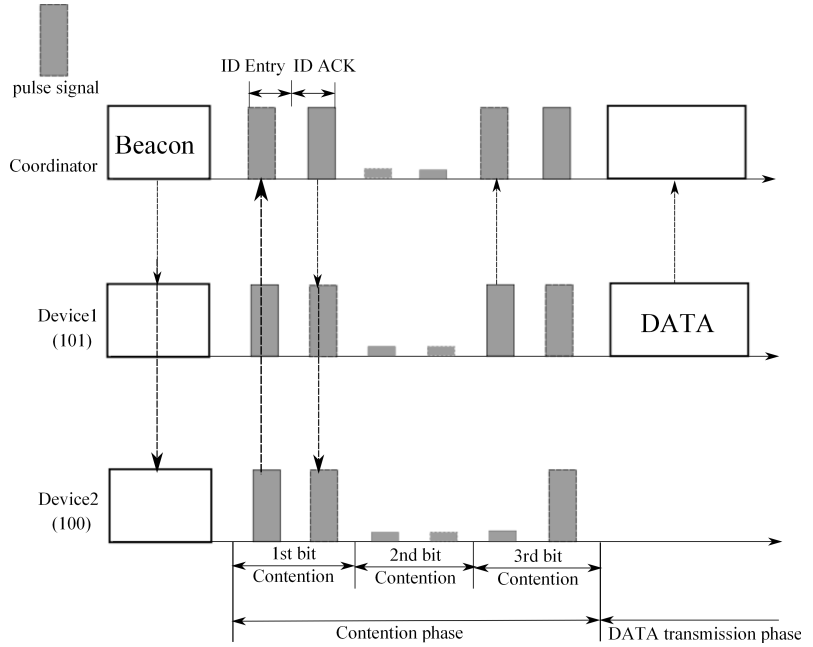

図 4 Proposal Method

さて，前述のように識別子の全てのビットが 0 であるアドレスをデバイスに割当てなかった理由であるが，以上の方式からも分かるように，本提案方式において全てのビットが 0 である端末は，送信要求の有無に関わらず，競合期間において違いをコーディネータ側で判別できないため，これをデバイスに割当てる事を避けるためである．

ところで，同方式において，一回のパルス検出を検出する行為はキャリアセンスと同じ原理で対応可能であると考えられる事から既存の IEEE802.15.4 におけるスロット化 CSMA/CA の CCA と同じでよいと考えられる．従って，l ビットの長さの識別子で競合を実施する場合は競合期間の全長を 2×CCA×l 以上に設定すればよいと考えられる．

3.1 新規デバイスがネットワークに新規参加した場合の動作

前節では，デバイスにすでに識別子が割当てられた状態を前提としたチャネルアクセス方

式について説明したが，本節では，ネットワークの構成後に新たなデバイスがネットワークに参加した場合についての動作を説明する．

まず，ネットワークに新たに参加する端末は，2 進カウントダウンの際の識別子をコーディネータに要求する．このとき，デバイスはコーディネータのビーコンを受信し，現在，ネットワークで使用されている識別子の長さを取得する．その後，全てのビットを 1 に設定されたコントロールアドレスを一時的に自身のアドレスとして使用して送信権を獲得した後に，通常の DATA パケットの代わりに IdRequest パケットをコーディネータに送信する．

コーディネータは IdRequest パケットに応じて識別子をデバイスに付与する．この際，ネットワークの識別子のビット数を増やさなければならない場合は，配下の全てのデバイスに対して 1 ビット識別子をシフトするように併せて指令を出す．

また，複数のデバイスが同時に IdRequest を送信することで衝突が発生した場合には，対応するデバイスは ACK が返信されない事でこの衝突を検知できるため，次回はランダムな値 s を設定し，s 回目のビーコンで同様に IdRequest を再実行する．

4. CSMA/CA と 2 進カウントダウン方式の性能解析

2 進カウントダウン方式によるチャネル競合方式の有効性を評価するために，簡単な解析モデルを定義して性能を比較する．

4.1 ネットワークモデル

4.2 解析モデルのネットワーク構成

本節における解析に使用するモデルを**図 5** に示す．まず，解析モデルは，ネットワークはただ 1 つのコーディネータによって制御されるものとし，このコーディネータの通信範囲内にはデバイスがランダムに配置されているとする．コーディネータとデバイスの通信ハードウェアには全く同じ機能が具備されていることとし，また，通信時に送信電力制御は一切行わず，常に最大電力で送受信を行うものとする．そのため，コーディネータと全てのデバイスの通信可能距離は同じとなり，これを解析では r として取り扱う．

4.3 解析モデルにおける隠れ端末の存在割合

前節において定義したネットワークにおいて任意のデバイスに着目した場合に，他の全てのデバイスのうち，どの程度のデバイスが隠れ端末となるかを導出する．

4.4 解析モデルのネットワーク構成

本節における解析に使用するモデルを図 5 に示す．まず，解析モデルは，ネットワークはただ 1 つのコーディネータによって制御されるものとし，このコーディネータの通信範囲内

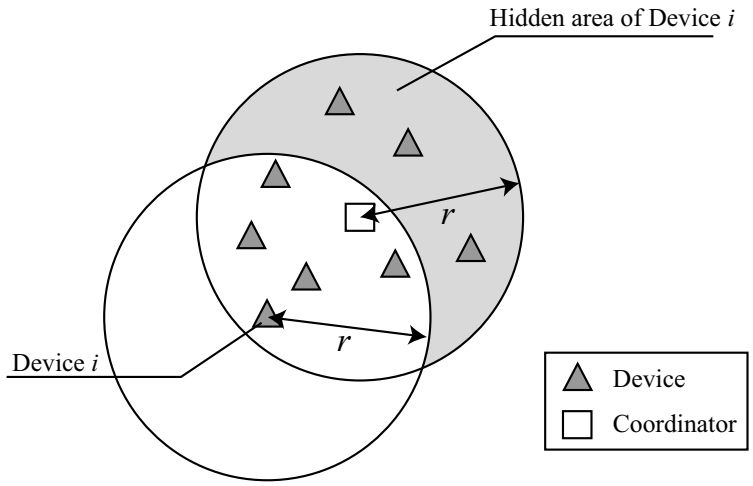

図 5 Analytical Model

にはデバイスがランダムに配置されているとする．コーディネータとデバイスの通信ハードウェアには全く同じ機能が具備されていることとし，また，通信時に送信電力制御は一切行わず，常に最大電力で送受信を行うものとする．そのため，コーディネータと全てのデバイスの通信可能距離は同じとなり，これを解析では r として取り扱う．

4.5 解析モデルにおける隠れ端末の存在割合

前節において定義したネットワークにおいて任意のデバイスに着目した場合に，他の全てのデバイスのうち，どの程度のデバイスが隠れ端末となるかを導出する．例えば，図 5 におけるデバイス i に対する隠れ端末は同図のコーディネータの通信範囲のうち，色付きで示された範囲に存在するデバイスとなる．

着目する任意のデバイスがコーディネータからの距離が x (ただし，$x \leq r$) であるとすると，着目したデバイスとコーディネータの双方と通信が可能な範囲は次式で導出できる．

$$\int_{\frac{\pi}{2}}^{\frac{\pi}{3}} (-16r^2) \sin\theta \cos\theta (\theta - \sin\theta \cos\theta) d\theta \tag{1}$$

従って，上式をコーディネータの通信範囲から除外した面積をコーディネータの通信範囲の面積で割る事で，任意の端末が送信を行った場合にネットワーク中の他のデバイスのうち

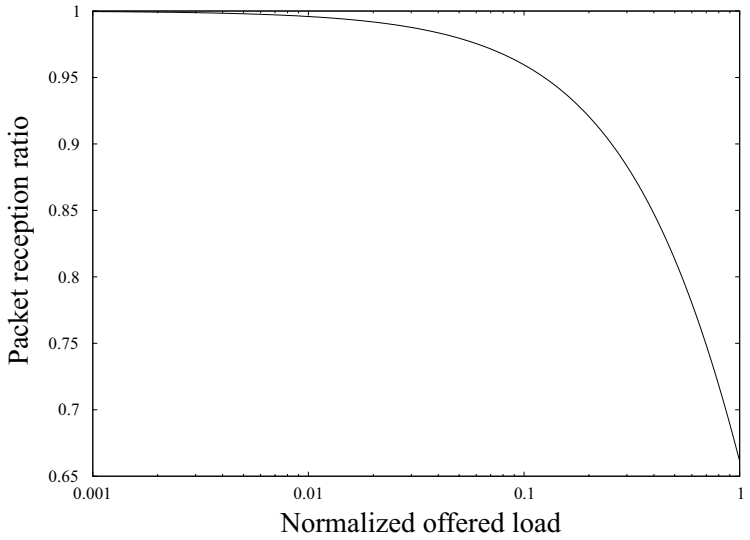

図 6 Packet reception ratio of CSMA/CA

隠れ端末となるデバイスの割合 hr が以下のように算出できる．

$$hr = \frac{1}{\pi r^2}\{\pi r^2 - \int_{\frac{\pi}{2}}^{\frac{\pi}{3}} (-16r^2)\sin\theta\cos\theta(\theta - \sin\theta\cos\theta)d\theta\} \quad (2)$$

$$= \frac{3\sqrt{3}}{4\pi} \quad (3)$$

4.6 CSMA/CA におけるパケット送信成功率

前節において導出した，任意の端末に対する隠れ端末の存在割合を用いて，CSMA/CA におけるパケット送信成功率を概算する．ここでは，あるビーコンに同期して CSMA/CA に従う任意のデバイスが送信する場合のパケット送信が成功する確率を求める．

ここでは，解析を簡単にするために，送信を行うデバイスのビーコン受信直後のバックオフを開始する時点から送信完了後の ACK を受信するまでに要するまでの長さによって時間長を固定長と見なして正規化する．この正規化された時間内にネットワーク中の全てのデバイスには合計で平均 G 回の再送を含むトラフィックがポアソン分布に従ってランダムに生じる事とする．このような条件下で，さらに解析を簡単化するために，着目したデバイスの通信範囲内に存在する他のデバイスに送信供給が発生した場合には，CSMA/CA のキャリアセンスならびにランダムバックオフによって完全に衝突を回避できると仮定する．逆に，着目したデバイスの隠れ端末となるデバイスに送信要求が生じた場合には，衝突により必ずパケットが失われると仮定する．

以上の仮定の下に，CSMA/CA におけるパケット送信成功率を算出した結果を**図 6** に示す．同図から分かるように，トラフィックの増加に反して CSMA/CA のパケット送信成功率が低下することが確認できる．特に，正規化された時間内に平均 1 個のトラフィックが発生する場合，すなわち衝突が発生しなければ，IEEE802.15.4 における通信回線を使い切るトラフィックが発生する場合の CSMA/CA のパケット送信成功率は約 65%程度まで急激に低下する事が確認できる．

4.7 提案方式によるパケット送信成功率の向上効果

本稿で提案を行った 2 進カウントダウンアルゴリズムによる競合方式を用いた場合，ネットワークでの発生トラフィックとは無関係に，常に送信要求発生時にはただ一つのデバイスのみに送信権を与える事ができる．従って，本節で取り扱う解析モデルにおいては，図 6 の値を 1 から差し引いたものが提案方式と CSMA/CA の性能差になると考えられる．

そこで，提案方式の導入による優位性を評価するため，提案方式のパケット送信成功率を図 6 で算出した CSMA/CA の値によって割った値を提案方式によるパケット送信成功率の向上率として**図 7** に示す．

同図からも分かる通り，ネットワークのトラフィックが増加するに従って，提案方式による性能向上幅が大きくなる事が分かる．また，特に，ネットワークの回線とほぼ同等のトラフィックが発生する場合には，提案方式を利用する事で約 1.5 倍に性能が向上することが確認できる．

5. おわりに

本稿では，IEE802.15.4 における隠れ端末に起因するパケット衝突を解決するために，2 進カウントダウンを用いたチャネル競合を行う方式を提案した．

既に述べたとおり，提案方式は隠れ端末とのパケット衝突を完全に解決できるが，一方では，デバイス間の識別子によって送信権獲得の優位性が決定してしまうため，高トラフィック時には送信機会の不公正を招きやすい．そこで今後はこれを改善するために，付与する識別子をスライドさせる等の検討を行なっていくつもりである．

また，本提案方式はコーディネータの ID ACK をネットワークの全デバイスが傍受する

Vol.2011-DPS-149 No.3
2011/11/24

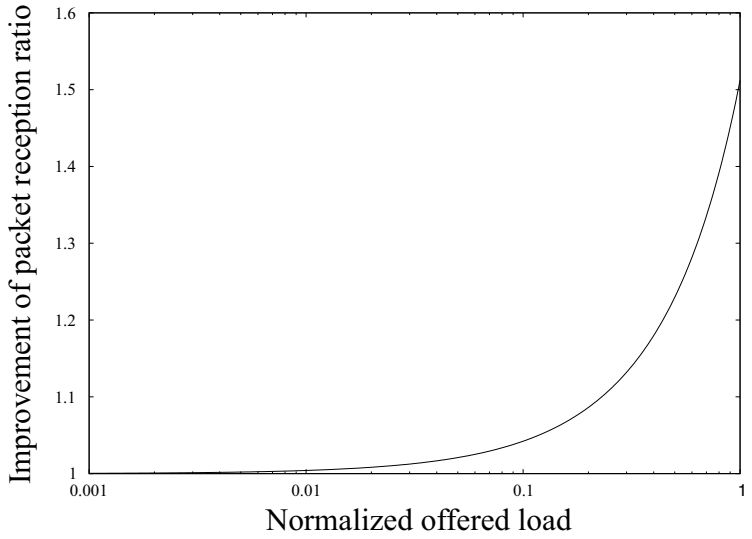

図 7 Improvement of packet reception ratio by proposed method

ことのみでパケット送信を回避しているため，デバイスの送信範囲の影響に提案方式のパケット送信成功率は依存しない．そのため，スロット化 CSMA/CA では，各デバイスが省電力のための送信電力制御を実施するととで自身の送信範囲を制限しているような場合には，キャリアセンス範囲の低下によって隠れ端末問題も発生し易くなるが，本提案方式においては，全く影響を受けないことが利点であると考えられる．

そのため，送信電力制御を実施した場合の本提案方式の優位性を端末の消費電力量やパケット送信成功率の双方から評価することも今後の課題となる．

参 考 文 献

1) 服部武，藤岡雅宣，“ワイヤレス・ブロードバンド教科書 高速 IP ワイヤレス編，”インプレス R & D，pp.90-95，2008.
2) Mario Arzamendia，森香津夫，内藤克浩，小林英雄，“IEEE802.15.4 センサネトワークにおけるトラヒック適用 MAC 制御方式，”電子情報通信学会技術研究報告，WBS，ワイドバンドシステム：IEICE technical report 108(231)，pp.75-80，2008.
3) 高橋淳，阪田史郎，柳原健太郎，福永茂．“センサネットワークにおける QoS を考慮した衝突回避のための適応的バックオフ制御方式，”電子情報通信学会技術研究報告，IN，情報ネットワーク 107(525)，pp.373-378，2008.
4) S.Cooper,“Binary Countdown Protocol，“http://www.ehow.com/facts_7564724_binary-countdown-protocol.html,”2010.