

モバイル PAN における隠れ端末を考慮した動的アドレス割り当てプロトコル

四條雅博[†] 田中希世子[§] 鈴木偉元[§] 石川憲洋[§] 石原進[‡]

[†] 静岡大学大学院理工学研究科 [§] (株) NTT ドコモ [‡] 静岡大学工学部

Dynamic Address Assignment Protocol considering Hidden Node for mobile PAN

Masahiro Shijo[†] Kiyoko Tanaka[§] Hideharu Suzuki[§] Norihiro Ishikawa[§] Susumu Ishihara[‡]

[†] Graduate School of Science and Engineering, Shizuoka University [‡] NTT DoCoMo, Inc. [§] Faculty of Engineering, Shizuoka University

1 はじめに

近年、Linux OS や Symbian OS を搭載した携帯電話の普及に見られるように、携帯電話等の携帯端末の高機能化が進んでいる。また広域無線通信とは別に、Bluetooth や IrDA といった短距離無線通信技術も進歩してきた。一方で、現在における広域無線はメールの送受信、ホームページの閲覧に、短距離無線通信は PC とのデータ同期、ヘッドセットとの無線接続というようにそれぞれ比較的単純な形態での利用しかされてこなかった。このような背景があり、広域・短距離無線通信技術を融合した新たなサービス創出が期待されている。そこで筆者らは新たな PAN 利用形態として mobile Personal Area Network (mPAN) を提案している。mPAN とは、携帯端末が周りに存在する周辺機器と PAN を構築し、移動先でもサービス起動可能なサービスモビリティを実現するためのコントロールポイントとなるネットワークサービスである。

mPAN を実現するためには、周辺機器との通信を可能とするために周辺機器へアドレスを割り当てることでネットワークを構築する必要がある。現在のネットワークでは、ノードに対するアドレス割り当てに DHCP サーバなどのアドレス割り当てサーバが広く用いられている。ところが mPAN では、DHCP サーバの設置場所にかかわらず、周辺機器をユーザのニーズに合わせて設置可能であるべきと考える。そこで本稿では、この mPAN におけるアドレス割り当て方法を述べる。

以降、第 2 章で mPAN の説明を行い、第 3 章で関連研究、第 4 章でアドレス割り当て方法について述べる。そして第 5 章では本プロトコルの考察を行い、第 6 章でまとめを行う。

2 mPAN

2.1 mPAN 概要

mPAN とは、携帯電話等の携帯端末 (Control Point: CP) がユーザの周辺に存在する周辺デバイス (Peripheral Device: PD) と PAN を構築し、ユーザが移動した先々でもサービスを起動したり、起動したサービスを継続することができるサービスモビリティを実現するためのコントロールポイントとなるネットワークサービスである [1]。PD はリッチな入出力機能を持ち、ユーザの持つ CP からのサービス要求に対し、CP に代わって自身の入出力機能を利用することで、CP に対しサービスを提供する。図 1 に mPAN の構成例を示す。ユーザの持つ CP がサービスを実行するために必要となる PD の選択や接続の制御を行うことで PAN を構築し、サービスに応じて PAN 内のローカル通信と CP からの外部ネットワークアクセスを利用する。CP がユーザの移動に伴って変化する PD との間で随時 PAN 構築を制御し、その時々での PAN における必要なサービスの起動や、PAN の変化によらないサービスの継続といったサービスモビリティを実現する。

この mPAN によって、CP がローカルに存在する PD からの直接的な情報取得や、ローカルで取得した情報をトリガとして外部ネットワークにアクセスし、外部サーバとの連携によるサービスを自動的に実行、自分の周辺機器との間で構築される PAN のみでなく、外部ネットワークを介し家族や友人等が構築した他の PAN と接続することで、複数 PAN 間での連携サー

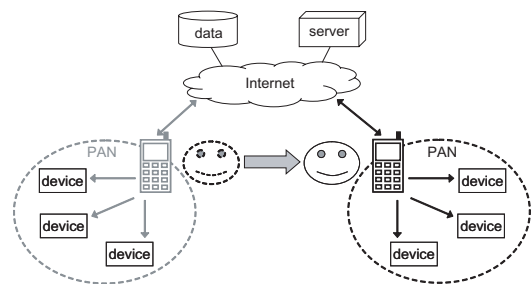


図 1: mPAN の構成

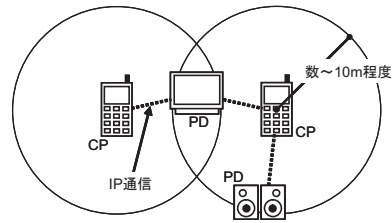


図 2: mPAN の想定環境

ビスを実現することができる。

mPAN 実現の技術課題の 1 つとして、他のノードと PAN を構築し通信を可能とするためのアドレス割り当て方法がある。そこで本稿では、mPAN におけるアドレス割り当て方法の検討を行う。以降、mPAN の想定環境と、目標とする PAN 形態、アドレス割り当てプロトコルの条件を示す。

2.2 想定環境

mPAN では、以下の環境を想定している (図 2)。

- CP と PD の通信可能範囲は数 m ~ 10m 程度とする。
- CP-PD 間通信は 1 ホップ通信に限定する。
- 通信は CP-PD 間でのみ行なわれ、PD どうしでの通信は行なわれないものとする。ただし、アドレス衝突処理等に当たってはその限りではない。
- PD が関与しない CP-CP 間通信は行われないものとする。
- CP を介した PAN 外通信を考慮し、PAN 内の通信プロトコルは IP を使用する。
- アドレス割り当てを行う中央サーバは存在しない。

現在のネットワークでは、ノードに対するアドレス割り当てに DHCP サーバなどのアドレス割り当てサーバが広く用いられている。しかし mPAN では、DHCP サーバの設置場所にかかわらず、ユーザのニーズに合わせて PD を設置可能であるべきと考える。したがって mPAN では、ノードのアドレス割り当てに關する中央サーバは用いないものとする。

2.3 目標とする PAN 形態

mPAN における PAN の目標形態を以下に示す。

- 隠れ端末があっても、アドレスの衝突がなく、通信を維持可能
mPAN では基本的に 1 ホップ通信であるため、各ノードの通信可能範囲内でアドレス衝突がなければ通信が可能に思える。しかし、自身が通信したいノードのさらに 1 ホップ先のノード（隠れ端末）とアドレスが衝突していた場合、ARP の誤作動やノード自体の誤作動を招きかねない。したがって、隠れ端末とのアドレス衝突を回避し通信を維持できるべきである。
- 通信中にノードのアドレスが変わっても通信の復旧が可能
アドレス衝突が発生した際、別のノードとトランスポート層コネクションを確立していた場合にアドレスを変更することでコネクションが破壊される。このとき mPAN ではアドレス変更前後における通信の継続ができることを目指す。
- mPAN 利用に伴う CP の電力消費を最小限にする
CP は携帯電話のような常に起動された状態を想定しており、mPAN を利用することで CP の電力を極端に消費してしまえば CP の使い勝手が悪くなってしまう。したがってアドレス割り当て作業においても CP の電力消費を最小に抑えることを目指す。一方で、本稿においては PD は安定した電源供給が得られることを仮定する。

3 関連研究

これまで IP ネットワークにおける DHCP 等の中央サーバが不要な、様々なアドレス自動設定プロトコルが提案されてきた。以下にそれらアドレス自動設定プロトコルの例を示す。

3.1 AutoIP [2]

IETF Zeroconf WG で提案されている AutoIP では、アドレスをランダムに選択し、ARP を利用したアドレス衝突検出方法を用いる。まず 169.254/16 アドレス空間においてランダムにアドレスを選択する。次に、選択したアドレス（仮アドレス）のネットワーク内の唯一性を確認するために、仮アドレス宛に ARP Probe を送信する。もし ARP Probe に対する応答として ARP Reply が返ってくれば仮アドレスはネットワーク内で既に使用されていると判断できる。しかしこのアドレス衝突検出方法では、ARP メッセージを用いるためにノードから 1 ホップで通信可能なノードとしかアドレス衝突検出が行えない。したがって、2 ホップ以上先のノードとのアドレス衝突検出が行えないという問題がある。

3.2 IPv6 Stateless Address Autoconfiguration [3]

IPv6 Stateless Address Autoconfiguration (IPv6 SAA) では、ネットワークインタフェースが保持するユニークな IEEE EUI-48 の MAC アドレスを利用することで、ユニークなリンクローカルアドレスを生成する。IPv6 SAA では、このリンクローカルアドレスのネットワーク内での唯一性を確認するために、重複アドレス検出 (Duplicate Address Detection: DAD) を行う。AutoIP のアドレス衝突検出方法と同様に、DAD ではノードの生成したリンクローカルアドレス宛に近隣要請メッセージを送信する。もし近隣要請メッセージに対する応答として近隣通知メッセージが返ってくれば、そのリンクローカルアドレスはネットワーク内で既に使用されていると判断する。

IPv6 SAA の一つの問題点は IEEE EUI-48 MAC アドレスをリンクローカルアドレス生成に利用する点である。この MAC アドレスはユニークな識別子であることを保証した規格に基づいているが、同じベンダーから重複した MAC アドレスを保持したネットワークインタフェースが出荷されていた例が報告されている。さらに AutoIP と同様に、IPv6 SAA の DAD 方法においても無線環境では直接通信可能なノードとしかアドレスの衝突検出が行われない。

3.3 MANETconf [4]

R. Prakash らの提案する MANETconf では、モバイルアドホックネットワーク (MANET) に参加して、ノードにユニークなアドレスを割り当てる方法を提供している。MANETconf では、既にネットワークに参加しているノード (initiator) が新たにネットワークに参加するノード (requester) に対してアドレスを割り当てる。initiator はネットワーク内で既に使用されたアドレスのリストを保持し、requester がブロードキャストしたアドレス要求メッセージを受信すると、ネットワーク内で未使用と判断されるアドレスを選択し、そのアドレス (仮アドレス) をいったんネットワーク内にフラディングさせ、仮アドレスが未使

用な状態であるか確かめる。その後、initiator はすべてのノードからアドレス使用許可メッセージが返ってきた場合のみ、仮アドレスを requester にユニキャストで伝え、割り当てる。

MANETconf では、requester が MANET へ参加する際、initiator とのユニキャスト通信にどのようなアドレスを使用するのか規定されていない。もし requester と同じアドレスを使用したノードが initiator と requester のそばに存在した場合、そのノードが誤動作を起こす懸念がある。

3.4 PACMAN [5]

K. Weniger の提案する PACMAN では、proactive 型もしくは reactive 型ルーティングプロトコルパケットの情報を用いてアドレス割り当て・アドレス衝突検出を行う。

各ノードはルーティングプロトコルパケットからネットワーク内のノード数の推定とアドレス割り当てテーブルを作成することで、ネットワーク内でユニークなアドレスを割り当てる。複数のネットワークどうしが近づくことで、それぞれのネットワーク内のノード間で通信が可能な状態になるネットワーク融合によるアドレス衝突に対しては、Passive Duplicate Address Detection (PDAD) により衝突を検出する。proactive 型ルーティングプロトコルを利用したネットワークでは、各ノードは定期的にフラディングされるリンク状態情報に含まれた送信元アドレス、シーケンス番号、近隣ノードのアドレスセットの違いからアドレス衝突を検出する。AODV 等の reactive 型ルーティングプロトコルを利用したネットワークでは、RREQ, RREP の送信元アドレス、それらメッセージに対応する要求アドレスなどの情報を解析してアドレス衝突を検出する。

このように、PACMAN ではアドレス割り当て・アドレス衝突検出にルーティングプロトコルパケットの情報を用いることから、1 ホップ通信が基本となる mPAN では PACMAN の PDAD 機構はそのまま利用できない。また、PACMAN では、すべてのノードが定期的に自身の IP アドレスと 1 ホップ内のノードの IP アドレスからなるリストをブロードキャストするために、CP の電力消費が増大してしまう。

4 mPAN におけるアドレス割り当て

本章では mPAN におけるアドレス割り当てプロトコルを述べる。mPAN のような PAN におけるアドレス衝突を考えた場合、各ノードの通信可能範囲のずれによりそれぞれのノードの通信可能範囲外の隠れ端末とのアドレス衝突が起こり得る。そこで、まず 4.1 で mPAN におけるアドレス衝突発生パターンを整理し、4.2 以降で本アドレス割り当てプロトコルについて述べる。

4.1 mPAN におけるアドレス衝突発生パターン

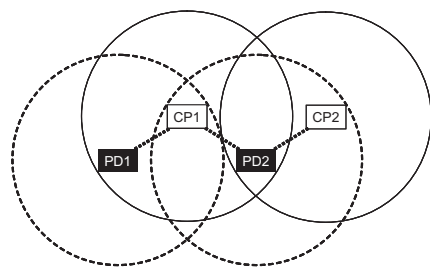
mPAN におけるアドレスの衝突パターンは以下に示す 3 つに大別される。ここでは図 3 中の CP 1 が新たに自身の IP アドレスを設定する場合を考えることとする。

- (1) CP と 1 ホップ圏内の CP または PD (CP1-PD1, CP1-PD2)
- (2) CP の 1 ホップ圏内の隠れ端末間 (PD1-PD2)
- (3) CP と CP の 2 ホップ先の隠れ端末間 (CP1-CP2)

mPAN における通信は CP-PD 間の 1 ホップ通信となるため、それぞれのノードにおいて隣接ノードおよび 2 ホップ先のノードとのアドレス唯一性が確認できればよいことになる。図 3 の例では CP1 が通信可能な PD1 と PD2 がいずれも異なるアドレスを持つていればよい。

4.2 基本方針

以降、CP の送信メッセージを極力減らし、CP の電力消費を最小限に抑えることを可能としたアドレス割り当てプロトコル



CP1: PANの構築を行うCP

図 3: mPAN におけるノードの配置例

を述べる。

本アドレス割り当てプロトコルでは、現行のインターネットとの親和性を確保するため IPv4 アドレスを使用する。アドレス生成は IPv4 通信を想定した MANET で一般に利用される 169.254/16 のアドレス空間からランダムにアドレスを選択することで行う。

mPAN では、通信は CP-PD 間のみで行われ、PD は安定した電力供給が見込まれるのに対し CP のパワーは限られるという、CP と PD 間の非対称性が存在する。この非対称性を利用し、PD のみ自身から 1 ホップで通信可能なノードの IP アドレス、MAC アドレスの対応表 (1 ホップ近隣アドレスリスト) を定期的にブロードキャストさせる。一方で、CP は 1 ホップ近隣アドレスリストを送信しない。したがって CP は PD よりも近隣ノードの IP アドレス、MAC アドレスのデータサイズ分、パケット送信量は少なくなる。

PD の隣接ノードは PD から 1 ホップ近隣アドレスリストを受信することで、自身の 2 ホップ内に存在するノードのアドレス情報 (IP アドレスと MAC アドレス) を取得する。PD の隣接ノードは自身から 2 ホップ内のノードのアドレス情報を 2 ホップ近隣アドレスリストとしてローカルで管理する。各ノードは 2 ホップ近隣アドレスリストを参照することで自身が保持するアドレスと自身の 2 ホップ内のノードとのアドレス衝突を検出することが可能になる。

アドレス衝突が検出された場合、CP、あるいは PD はアドレスの変更を行う。このアドレス変更によるコネクションの破壊を避けるために旧アドレスを用いた IP パケットを新アドレスを利用した IP パケットによりカプセルリングし、アドレス変更前後でコネクションの維持を可能とする。

以下、本プロトコルの詳細を述べる。

4.3 初期アドレスの設定

以下、図 4、図 5 を利用し初期アドレスの設定手順を述べる。図 4 は図 3 における CP1 が PD1 とアドレス衝突している状況から自身の初期アドレスを設定する手順を示す。図 5 は図 3 における PD2 が CP1 とアドレス衝突している状況から自身の初期アドレスを設定する手順を示す。

新たにネットワークに参加する CP、PD は 1 ホップ内に存在する PD から 1 ホップ近隣アドレスリストを受信することで、自身から 2 ホップ内のノードのアドレス情報を取得する。ノードは受信した 1 ホップ近隣アドレスリストから 2 ホップ近隣アドレスリストを作成する。その後ノードは AutoIP で用いられているアドレス空間 (169.254/16 プレフィックスアドレス) において、2 ホップ近隣アドレスリストに含まれていないアドレスをランダムに選択し、自身のネットワークインタフェースに割り当てる。

ノードはアドレス設定後、新しい IP アドレスが 2 ホップ内の他のノードとアドレス衝突していないか確かめるため、自身が割り当てた IP アドレスに対する ARP Request をブロードキャストする (図 4)。各ノードは、自身の持つ IP アドレスと等しいアドレスに対する ARP Request を受け取った場合に ARP Reply を返す。また、自身の隣接ノードに対する ARP Request と、自身の ARP テーブル上の MAC アドレスとは異なるノードから受信した場合、Proxy ARP Reply を返す。これにより ARP Request を送信したノードは、自身から 2 ホップ以内のノードとのアドレス衝突を確認できる。

その後アドレス設定を行ったノードは、1 ホップ近隣アドレスリスト送信元 PD の IP アドレスが自身の 1 ホップ内でユニークであることを確かめるため、この PD に対する ARP Request をブロードキャストする (図 4)。図 3 における PD2 のように、他の PD から 1 ホップ近隣アドレスリストを受信しない状況では、この ARP Request をブロードキャストする必要はない (図 5)。

CP は自身の IP アドレスに有効期限 (TL_{cp}) を設ける。その TL_{cp} が切れた時点で CP は自身の IP アドレスに対する ARP Request をブロードキャストする (図 5 における CP1 と CP2 の動作)。これにより CP がアドレス変更を行わなかった場合でも、その CP の近隣に存在するノードは送信元 CP の存在を知ることができる。この ARP Request の送信元 IP アドレスと MAC アドレスにより、図 3 の PD2 のような、自身の 1 ホップ内に他の PD が存在しない場合でも自身の IP アドレスが他のノードと衝突していることが判断できるので、初期アドレスの設定が可能になる (図 5)。以上の手順によりノードは初期アドレスの設定を終え、以降は次節以降のアドレス管理を行う。

4.4 リンク状態管理

CP、PD は常に、隣接する PD から受信した 1 ホップ近隣アドレスリスト、および隣接ノードからの ARP メッセージ (Re-

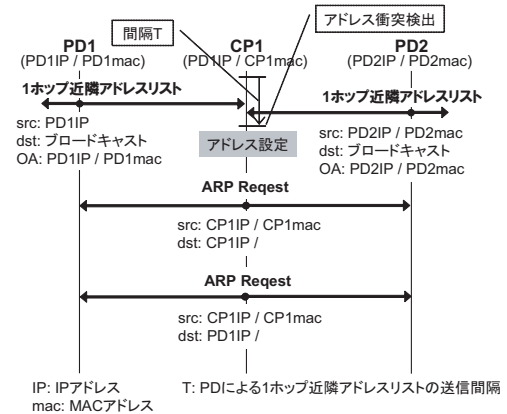


図 4: 図 3 における CP1 の初期アドレス設定

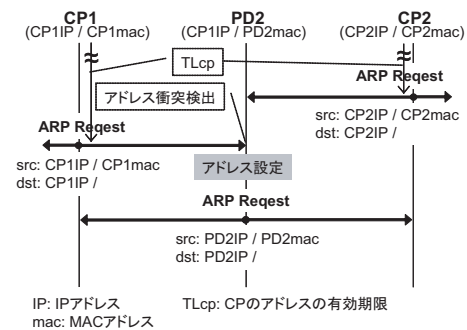


図 5: 図 3 における PD2 の初期アドレス設定

quest/Reply) の送信元アドレスを監視する。これらから得られた自身から 2 ホップ以内のノードのアドレスが、すでに自身の 2 ホップ近隣アドレスリストに含まれていなければ、これを新たに追加する。

PD はノードのアドレス情報を自身の 2 ホップ近隣アドレスリストに記録する際、アドレス情報と共にアドレスの有効期限 (TL_n) を記録する。この TL_n は CP が保持する IP アドレスに対して与えられた有効期限 (TL_{cp}) よりも大きい値とする。PD はこの TL_n が切れるまでに、再びノードの存在を確認できれば、PD はそのノードの有効期限 (TL_n) を初期値に更新する。 TL_n が切れるまでノードの存在が確認できなければ、PD はそのノードのエントリを自身の 2 ホップ近隣アドレスリストから削除する。

4.5 アドレス衝突検出

CP、PD はアドレス設定後、PD の送信する 1 ホップ近隣アドレスリストと、CP、PD がそれぞれ送信する ARP メッセージを利用してアドレス衝突検出を行う。1 ホップ近隣アドレスリストには送信元 PD の IP アドレス、MAC アドレスと、送信元 PD から 1 ホップ内に存在するノードの IP アドレス、MAC アドレスの情報が含まれている。

ノードが複数の異なる PD から 1 ホップ近隣アドレスリストを受信した場合には、それぞれの送信元 PD のアドレス情報により、ノードは 1 ホップ近隣アドレスリストの送信元 PD 間のアドレス衝突を検出できる。なお PD は、自身の起動時に乱数を作成しておき、自身の送信する 1 ホップ近隣アドレスリストにその乱数を付加しておくことで、複数の PD から 1 ホップ近隣アドレスリストを受信したノードにおいて、1 ホップ近隣アドレスリスト送信元 PD の IP アドレスが同じで MAC アドレスも同じ場合の PD 間におけるアドレス衝突を検出することができる。

CP、PD の各ノードは、受信した ARP メッセージの送信元 IP アドレスが自身の IP アドレスと同じで送信元 MAC アドレスが自身の MAC アドレスと異なる場合、アドレス衝突が発生していると判断する。

4.6 アドレス衝突解決

自身のアドレス衝突を発見したら、ノードは 4.3 節のアドレス設定方法に基づき自身のアドレスの再設定を行う。

一方、図 3 の CP1 が PD1-PD2 間のアドレス衝突を発見したときのように、ノードが自身の 1 ホップ内の隠れ端末間における

アドレス衝突を発見した場合、このノードは自身の2ホップ近隣アドレスリストに登録されている衝突を起こした一方のノード宛に、データリンク層においてアドレス衝突報告メッセージをユニキャストする。アドレス衝突報告メッセージを受信したノードは4.3節に基づきアドレスの再設定を行う。

通常、トランスポート層コネクションはIPアドレスを用いて確立されるため、コネクション確立中にアドレスの変更を行なうと、使用していたコネクションは破壊される。この解決法としてはPACMANでとられている手法と同じく旧アドレスを用いたパケットを新アドレスを利用してカプセル化する方法を用いる。各ノードは、旧アドレスと新アドレスの対応付けが記録されたbinding tableを保持し、カプセル化されたデータパケットは通信相手に到達した時点でデカプセル化され、古いアドレスを用いてトランスポート層に伝える。これにより、アドレス変更前後において通信相手とのコネクションの維持を可能とする。

5 考察

5.1 ケーススタディ

本節では、mPANにおいて考えられる様々なトポロジに対するアドレス衝突検出の動作を検証する。以下、図6を用いて説明を行う。

初期状態：
図6はCP1が他のノードの直接通信範囲外からPD1, PD2, CP2と直接通信可能な位置に移動し、PD2はCP3と直接通信可能であり、CP1からCP3は隠れ端末となっている状況を想定している。CP1はアドレス6を保持しており、移動後のトポロジにおいて直接通信可能なPD1とアドレスが衝突している。さらにPD2はCP1が移動してきたことでCP1を介してCP2とアドレスの衝突を起こしている。

CP1による1ホップ近隣アドレスリストの受信：

アドレス6を保持したCP1は移動後、PDの1ホップ近隣アドレスリストのブロードキャスト間隔と同じだけ1ホップ近隣アドレスリストの受信を待つ。CP1は直接通信可能なPD1とPD2から1ホップ近隣アドレスリストを受信し、PD1, PD2それぞれに隣接するノードを自身の2ホップ近隣アドレスリストに加える。

CP1のアドレス変更：

CP1は、自身の2ホップ近隣アドレスリストの情報に登録されたアドレス情報から、自身のアドレス6が2ホップ内のノード(PD1)と衝突していることがわかる。そこでCP1は自身の保持する2ホップ近隣アドレスリストに含まれていないIPアドレス(アドレス5とする)をランダムに選択し、自身のネットワークインタフェースに割り当てる。

CP1による近隣ノードのアドレス衝突の検出：

その後、CP1は自身が割り当てたIPアドレスに対するARP Requestを送信する。CP1が割り当てたアドレス5を使用したノードはCP1の1ホップ内には存在しないので、ARP Replyは返ってこない。次にCP1は受信した1ホップ近隣アドレスリストの送信元PD(PD1, PD2)のIPアドレス(アドレス6とアドレス8)に対するARP Requestを送信する。

CP1の1ホップ内にはPD2が使用しているアドレス8を保持したCP2が存在している。したがってCP1はアドレス8に対するARP Requestの応答としてPD2とCP2からARP Replyを受信する。PD2からのARP ReplyとCP2からのARP Replyにおいて、それぞれの送信元IPアドレスが同じで送信元MACアドレスが異なることから、CP1はPD2が保持するアドレス8がアドレス衝突を起こしているとわかる。

CP1の近隣ノードのアドレス衝突解決：

そこでCP1はアドレス8のアドレス衝突を起こし、CP1の2ホップ近隣アドレスリストに登録されていたPD2のMACアドレス2に対してデータリンク層におけるアドレス衝突報告メッセージを送信する。このアドレス衝突報告メッセージを受信したPD2は先のCP1と同様にアドレスを変更する。以上のような手順により、図6におけるアドレス衝突はなくなる。

CP1が移動後の場所で起動した場合のアドレス割り当て：

CP1が移動後の位置で起動された状況と考えた場合、CP1がもともと保持していたアドレスをアドレス6の代わりに未指定アドレス(0.0.0.0)に置き換えて、アドレス割り当ての手順を考えることができる。

5.2 アドレス確定までの時間

図6のノード配置をもとにアドレス確定に要する時間について検討する。PDのアドレスリスト送信時間間隔を T とすると、

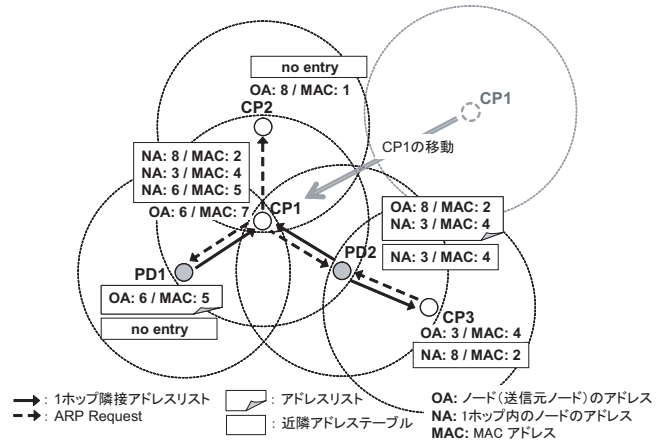


図6: ケーススタディ

新たにアドレスを設定するCP1はPD1, PD2の通信可能範囲内に移動してから、最大 T のうちに1ホップ内のPD1, PD2からアドレスリストを受信することになる。CP1は、受信したアドレスリストに含まれる2ホップ内のノードのアドレス以外のアドレスを選択することから、最大約 T のうちにアドレス割り当てを終える。その後、自身の割り当てたIPアドレスに対するARP Requestと、受信したアドレスリストの送信元PD1, PD2のIPアドレスに対するARP Requestを送信する。この複数のノードに対するARP Requestを連続して送信可能であると考えられる。また、IEEE 802.11無線LANのような少なくとも1Mbpsの伝送速度を持つ無線技術では、応答遅延が約1秒であることから、ARP Requestの送信後ARP Replyが返ってくるまでの時間を1秒とする。したがって、CP2-PD2間のアドレス衝突は1秒間のうちに検出できる。図6ではCP2-PD2間においてアドレス衝突が起きており、5.1で述べたようにCP1はPD2に対してアドレス衝突報告メッセージを送信する。このアドレス衝突報告メッセージも0.5秒でPD2に到達しアドレス変更が行われると考えられると、合計最大時間約 $T + \alpha + 1.5$ 秒でCP1とその2ホップ内のノードのアドレス唯一性が確保される。ここで、 α はCP, PDにおけるネットワークインタフェースのアドレス設定 + アドレス衝突検出の処理時間としている。

6 まとめ

本稿ではmPANにおける隠れ端末を考慮したアドレス割り当てプロトコルについて述べた。本プロトコルでは、CP-PD間の非対称性を利用し、移動端末であるCPのメッセージ送信量を可能な限り少なくしエネルギー消費を抑える。mPANでは、各ノードにおいて隣接ノードおよび2ホップ先のノードとのアドレス唯一性が確保できればよく、本プロトコルではPDに直接通信可能なノードのアドレスをブロードキャストさせることで、CP, PDは2ホップ内の割り当て済みアドレスを取得する。この割り当て済みアドレスの情報を利用することで、各ノードがあらかじめアドレス衝突を回避したアドレスを選択できるようにした。

今後の課題として、実装と実環境におけるプロトコルの有効性の検証、mPANの特徴を生かした更なるプロトコル最適化が挙げられる。

参考文献

- [1] 田中 ほか: “モバイルパーソナルエリアネットワークの提案,” 情報学ワークショップ2004 (WiNF 2004), (Sep. 2004).
- [2] S. Cheshire, B. Aboba and E. Guttman: “Dynamic Configuration of IPv4 Link-Local Addresses,” *Internet-Drafts (draft-ietf-zeroconf-ipv4-linklocal-17.txt)* (Jul. 2004).
- [3] S. Thomson: “IPv6 Stateless Address Autoconfiguration,” *Request for Comments 2462* (Dec. 2004).
- [4] Sanket Nesargi and Ravi Prakash: “MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network,” IEEE INFOCOM (INFOCOM 2002), (2002).
- [5] Killian Weniger: “PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks,” IEEE JSAC, Special Issue on Wireless Ad Hoc Networks, (Jan. 2005).