# アドホック・メッシュネットワークによる災害時通信システム

木下　昌昭 *　　白井　治彦 **　　黒岩　丈介 ***　　小高　知宏 *

# A Disaster Communication System using Ad-hoc Mesh Network

**Masaaki KINOSHITA*, Haruhiko SHIRAI**, Jousuke KUROIWA*** and Tomohiro ODAKA***

(Received February 6, 2015)

In this article, we propose a disaster communication system using ad-hoc network and mesh network. In this system, we use the Etherphone which is new communication technology using only the data link layer and the physical layer. The Etherphone network uses a broadcast for the transmission of a message of data. We produced mobile communication terminal equipment by using Etherphone. We built an alternative communication network at the time of disaster by constructing mobile ad-hoc network which using wireless multi-hop communication. We demonstrated that the mobile communication terminal equipment can take ad-hoc communication in alternative communication network at the time of disaster.

***Key words*** **:** Etherphone, Disaster Communication, Mobile Ad-hoc Network,Routing Protocol

## 1. はじめに

近年のIT技術の発達に伴い, 医療や災害救助においても, 積極的にIT技術が利用されている. 現在利用されている通信ネットワークは, 一般的にユーザの端末と最寄りの電話局あるいは基地局などの間を接続するアクセスネットワークと, 電話局または基地局などを相互に接続する基幹ネットワークにより構成される. このような通信ネットワークは通常時には安定した高速な移動通信サービスを提供可能であるが, 地震等の災害が発生した場合, アクセスネットワークは通信可能であったとしても, 基幹ネットワークが物理的な損壊や停電等により, 通信不能になることがある.

*大学院工学研究科 原子力・エネルギー安全工学専攻
**技術部
*** 大学院工学研究科 知能システム工学専攻
*Nuclear Power and Energy Safety Engineering Course, Graduate School of Engineering
**Dept. of Technology
***Human and Artificial Intelligent Systems Course, Graduate School of Engineering

災害時における通信ネットワークの問題は, 今まで以上に致命的になりうる. 被災状況の確認や適切な救助活動などに必要な情報は, その被害が大きくなればなるほど得難くなる. これらの通信網の復旧は, 破損箇所の明確な特定が困難であることや災害による地形の変動により, 破損箇所に人が足を踏み入れられなくなってしまうなど非常に時間と手間がかかる. 被災時での救助活動は, 迅速な対応が求められることが多く, 既存のシステムの復旧を待たず, 代替的な通信システムを敷設し利用しようとする研究が多くなされている.[1],[2]

本研究では, イーサフォン[3]という通信技術を用いた無線通信端末を製作し, その端末を用いて無線マルチホップ通信によるモバイルアドホックネットワーク[4]を構成することで, 災害時における代替的な通信ネットワークを構築する.

モバイルアドホックネットワークはユーザ端末間の無線通信を基本とする自律分散ネットワークであり, 直接無線通信を行うことのできない端末との通信は, 無線通信が可能な他のユーザ端末が中継を行うことで実現することができる. 基地局を必要とせず, 通信経路は中継端末の負荷の状態や端末自体の通信範囲外への移動に応じて他の通信可能な端末を用いるよう自動的に再

構成されるため, 大規模災害発生時の既存移動通信ネットワークの代替手段として有効であると考えられる.

本稿では, シングルボードコンピュータを用いてイーサフォン無線通信端末を実装し, その無線通信端末を用いてアドホックな通信が行えることを実証した.

## 2. 災害時通信システムの構成

### 2.1 災害時通信システムの概要

本研究における災害時通信システムとは地震, 津波, 洪水, 台風などの広域にわたる大規模災害の影響により, 敷設されているネットワークインフラに障害が発生した際に, それに代替する応急的通信インフラのことである.[5] そして, 災害時通信システムにおいて, 破壊された通信ネットワークに対して, 代替的に構築したネットワークのことを災害時通信ネットワークと呼ぶことにする. この通信インフラは被災地で破壊され利用できなくなった通信インフラの修復ではなく, 通常のインフラ修復までの一時的通信インフラであるため, ネットワーク構築にかかるコストが安価であること, ネットワーク構築や通信に手間がかからないなどの即応性, 二次災害による被害を受けにくいという耐障害性が求められる.

そのような問題から, こういった研究では, 主にメッシュネットワークやアドホックネットワークといった技術が用いられている. アドホックネットワークでは, マルチホップ通信という広くコンピュータ等の無線接続に用いられている IEEE802.11x,Bluetooth 等の技術を用いながら多数の端末をアクセスポイントの介在なしに相互に接続する形態をとっている. しかし, それらの無線マルチホップ通信は, 最適化されたルーティングプロトコルを考案する必要があり手間がかかる. また, 情報の伝達内容や伝達頻度, 利用目的や利用規模によってネットワークの構成方法は様々である. そこで, 設定不要で簡単に通信可能なイーサフォン通信技術を用いて無線通信端末を製作し, 災害時における代替的なネットワークとしてモバイルアドホックネットワークを構築する.

モバイルアドホックネットワーク（mobile ad hoc network,MANET）は, 携帯機器を無線通信でリンクする自己形成型ネットワークの一種である. 図 1 に示すように,MANET 内の各機器は任意の方向に自由に動かすことができ, その際に他の機器とのリンクを頻繁に変化させる. 各機器は自らとは無関係のトラフィックを転送でき, 従ってルーターとしての機能も持っている.MANET 構築において最も重要なのは, 各機器がトラフィックを正しく転送するのに必要な情報を継続的に維持する機能を持つことである.

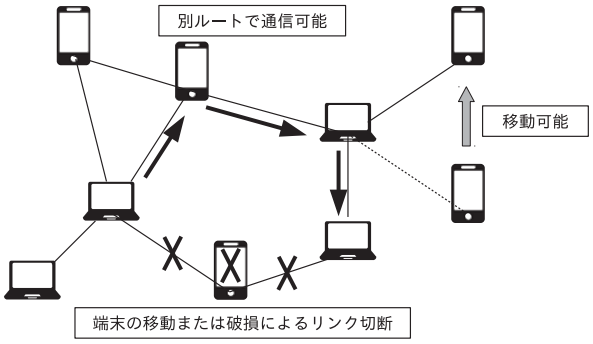


図 1 モバイルアドホックネットワーク

MANET は無線アドホックネットワークの一種であり, 一般にアドホックネットワークの上にルーティングを行うネットワーク環境があるという構成である. また, メッシュネットワークの一種でもあるが, メッシュネットワークは一般に移動体や無線に限定されない.

無線マルチホップ通信を利用する MANET で重要となるのがルーティングである. 通常, 無線端末を用いてネットワークの構築を行う場合には,OLSR や AODV などのルーティングプロトコルを用いて, 無線マルティホップに最適化したルーティングプロトコルを考案する必要がある. しかし, 本研究では通信技術にイーサフォンを用いている. イーサフォンの詳細については次章で説明するが, 通信におけるルーティングは, 細かくルートを設定して通信するのではなく, 周囲にある全ての端末にブロードキャストを行うことで通信を行うので, ルーティングプロトコルの最適化設定に伴う手間を削減することができる.

### 2.2 災害時通信ネットワークの構築

災害時通信ネットワークのネットワーク形態としては, モバイルアドホックネットワークを利用する. モバイルアドホックネットワークでは, 多数の端末をアクセスポイントの介在なしに相互に接続する形態であるマルチホップ通信を行う.

本研究における無線通信の規格として IEEE 802.11 を使用する.IEEE 802.11 は IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が 1998 年 7 月に定めた無線 LAN の標準規格である. クライアント側から見た無線 LAN の接続形態は, アクセスポイントの使用の有無で 2 つのモードに大別できる. インフラストラクチャーモードとアドホックモードである. インフラストラクチャーモードでは, 無線 LAN クライアントはアクセスポイントを介して通信を行う. アクセスポイントが, イーサネットで言うと, ハブに相当する働きをする. アドホックモードはピア・ツー・ピアモー

ドまたはインディペンデントモードとも言う. アドホックモードでは, 無線 LAN クライアント同士が, アクセスポイントを介さず, 直接通信を行う. このため, 無線 LAN クライアント同士が通信する場合, インフラストラクチャーモードに比べて電波使用効率が良い.

2 つの無線 LAN アダプタをアドホックモードで通信させるには, アダプタに設定する ESSID（Extended Sevice Set Identifier）を一致させておく必要がある. 一般的な利用方法は, 無線 LAN インターフェースをもつ PC2 台を通信可能な近さに設置し, 互いにファイルのやりとりなどを行うものである. アドホックモードでの通信を, バケツリレー方式でつないでいくと, 複数の端末を介して無線の到達範囲を超えた通信ができるので, これを応用したアドホックネットワークシステムとしての利用が研究されている. 以上の理由から, 本研究においてもアドホックモードを利用する.

災害時通信ネットワークは, データの送受信と中継の両方の機能を持つイーサフォン無線端末で構成される MANET である.MANET では, ネットワークを構成する端末の移動が想定されており, 端末が破損もしくは移動した場合にも, 物理的に通信路が確保されていれば通信が可能で, 二次災害の発生にも対応できる耐障害性に優れている. 災害時通信ネットワークでの通信は図 2 のようになる. 端末同士の通信には, ブロードキャスト通信により, 通信可能範囲内のすべての端末に対して, ピア・ツー・ピア通信を行う. 発信端末から目的端末までのデータの送信には, 各端末でブロードキャスト通信を行うことにより, バケツリレー方式でデータを転送していくマルチホップ通信を利用する. また, 端末間の無線通信には IEEE 802.11 で取り決められている無線 LAN 規格を用いる.

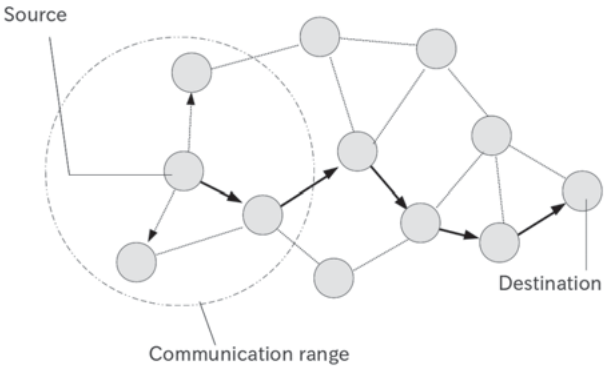


図 2 ネットワークの概要

## 3. イーサフォンによる災害時通信システムの設計と構築

### 3.1 イーサフォン通信技術

イーサフォンとは福井大学が特許を有する通信技術（特許第 4110251 号）のことである.[6] イーサフォン開発における基本コンセプトとして 2 点挙げられる.1 点は従来のアナログデータ通信基盤に代わる通信基盤を開発することである. もう 1 点は, 昨今のインターネット通信環境が複雑になっており, 近距離・閉鎖的な通信網には短所が多いと考えるからである. イーサフォンの特徴を表 1 に挙げる.

表 1 イーサフォンの特徴

| | 説明・特徴 |
|---|---|
| (1) | イーサネットの機能のみを用いる<br>・OSI 参照モデル L1,L2 を使用<br>・イーサネット機器を使用できる<br>・L3 以上は利用不可 |
| (2) | 長距離でもノイズの影響を受けにくい<br>・信号増幅装置は必要なし |
| (3) | 通信設定は必要なし<br>・TCP/IP などのプロトコルを使用しない<br>・電源と LAN インフラがあれば使用可能 |
| (4) | 無線通信も可能<br>・有線 LAN/無線 LAN どちらにも対応<br>・無線でも通信設定は不要 |
| (5) | アナログ/ディジタルデータを伝送可能<br>・通信時はディジタル形式<br>・アナログデータは A/D 変換により対応 |

イーサフォン通信は OSI 参照モデルにおける第 1 層（物理層）と第 2 層（データリンク層）のイーサネットの機能を用いて行われる.OSI 参照モデルとは国際標準化機構である ISO により制定された, 異機種間のデータ通信を実現するためのネットワーク構造の設計方針「OSI」（Open Systems Interconnection）に基づき, コンピュータなどの通信機器の持つべき機能を階層構造に分割したモデルである.OSI 参照モデルを表 2 に挙げる. イーサフォンの様々な特徴の中で一番の利点は通信設定なしにネットワークを構成し, 接続できることである.

### 3.2 イーサフォン無線通信で用いるフレームフォーマット

イーサネットでの通信単位はイーサネットフレームである. イーサネットフレームのデータ形式として代表的なフレームが 2 種類ある. その内の 1 つである Ethernet II フ

表 2 OSI 参照モデル

| 階層 | OSI 参照モデル | プロトコル例 |
|---|---|---|
| 7 | アプリケーション層 | WWW |
| 6 | プレゼンテーション層 | SSL,TLS |
| 5 | セション層 | Socktes |
| 4 | トランスポート層 | TCP，UDP |
| 3 | ネットワーク層 | IP |
| 2 | データリンク層 | CSMA/CD |
| 1 | 物理層 | 100 BASE-TX |

レームは,IEEE で規格化される前に,DEC と Intel,Xerox が策定したため,3 社の頭文字を取って通称 DIX 規格と呼ばれることが多い.Ethernet II フレームのフレームフォーマットを図 3 に示す. 通常, 無線通信でやり取りされるデータのフレームフォーマットは IEEE802.11 無線 LAN 規格のフレームフォーマットを使用している. しかし, イーサフォン無線通信では,IEEE802.11 無線 LAN 規格のフレームフォーマットは用いない.IEEE802.11 フレームの中の「IEEE802.11 ヘッダ」には 7 項目のフィールドがある. そして, その中の Address 1/2/3/4 のフィールドのアドレス情報については, ネットワークの構成により変化する. さらに,TCP/IP での通信では, データ部に IP パケットを用いる. そのため, 設定が複雑になる.

以上の理由からイーサフォン無線通信では,IEEE802.11 無線 LAN 規格のフレームフォーマットは用いない. そして, その代わりにイーサフォン通信技術のフレームフォーマットを使用する. アドホック通信などのイーサフォン無線通信で用いるフレームフォーマットは,Ethernet II フレームを元に構成されている. 図 4 に示すような,Ethernet II フレームのデータ部の先頭からイーサフォンプロトコルヘッダとイーサフォンアドホックネットワークプロトコルヘッダを追加したフレームフォーマットを用いる.[7]

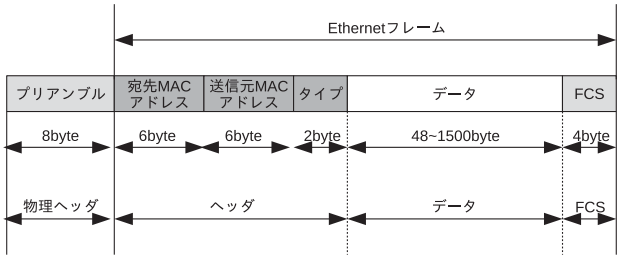


図 3 Ethernet II フレームのフレームフォーマット

フレームフォーマットの各内容について説明する. イーサフォンはブロードキャスト通信を用いるので, 宛先

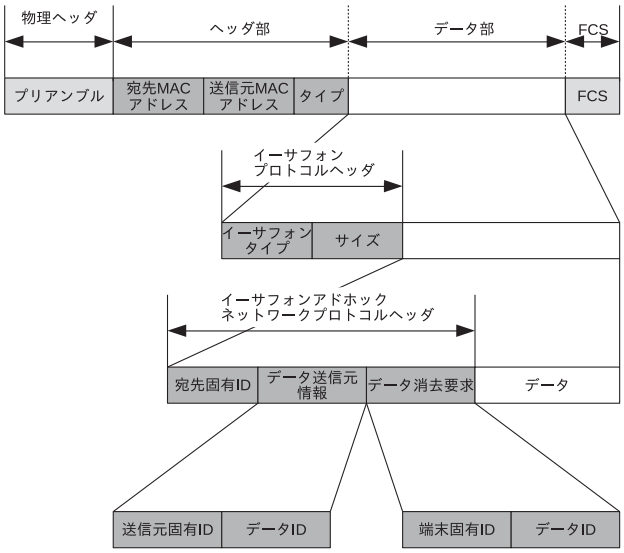


図 4 イーサフォンアドホックネットワークプロトコルのフレームフォーマット

MAC アドレスにはブロードキャストアドレスが挿入される. 送信元 MAC アドレスには自身の MAC アドレスを挿入する. そしてデータタイプフィールドには, イーサフォンプロトコルを示す値を設定する.

イーサフォンプロトコルヘッダ部におけるイーサフォンタイプフィールドの値はイーサフォンを使用したアプリケーションの性質ごとに割り振られる値である. この値を参照することによってどのような系統のアプリケーションかを判別し, アプリケーションは自分で受信したデータを扱うべきかを判断することができる. サイズフィールドにはフレームサイズが挿入される. イーサフォンプロトコルヘッダのフィールド情報を表 3 に示す.

表 3 イーサフォンプロトコルヘッダのフィールド情報

| フィールド名 | バイト数 | 内容 |
|---|---|---|
| イーサフォンタイプ | 2 | 他のイーサフォンシステムとの区別 |
| サイズ | 2 | フレームサイズ |

イーサフォンアドホックネットワークプロトコルヘッダ部は大きく分けて 3 つの領域に分けられる. 宛先固有 ID フィールドとデータ送信元情報フィールド, データ消去要求フィールドである.

まず, 宛先固有 ID フィールドは宛先である端末に付けられている固有 ID が入る. このプロトコルを用いて通信を行う全ての端末にはあらかじめ MAC アドレスとは別に固有の ID が設定されている. 固有 ID は端末一つ一つを識別する固有の ID であるため, フィールドの大

きさは MAC アドレスと同等の 6byte に設定した. ネットワークインターフェースごとに一意に設定されている MAC アドレスも 6byte で表現されているため,MAC アドレスをそのまま固有 ID として使用することも可能である. しかし, 同一ネットワーク内で MAC アドレスをそのまま使用した固有 ID とユーザが設定する重複しない一意な固有 ID を混在させると, 万が一重複した際に正しく通信が行われない可能性があるため, どちらかに使用を限定しなければならない. 本研究で行うような非常に小規模な実験のような環境でなければ,MAC アドレスを固有 ID としてそのまま使用するほうが簡単である.

データ送信元情報フィールドは, 最初に通信を開始する端末によって設定されるフィールドである. このフィールドは送信元固有 ID フィールドとデータ ID フィールドに分けられる. 端末が最終的な宛先まで通信を行う際, 送信元から宛先端末まで複数の端末を中継するが, イーサフォンアドホックネットワークプロトコルのフレーム内の送信元 MAC アドレスを含む送信元の情報は保存されないか書き換えられてしまう. このままでは, さらにそのデータを受け取った端末が同様にデータをリレーし, データが永遠にネットワーク内を循環し続ける事態が起きてしまう. これを防ぐために送信元情報を元に送信済みデータの情報を保存するデータベースを作成し不要な再送を防止する. これをここでは再送防止用データベースと呼ぶこととする.

送信元固有 ID フィールドは宛先固有 ID フィールドと同様に 6byte に設定した. この送信元固有 ID フィールドはデータを作成し, 送信を開始した送信元端末の固有 ID が設定されている. データ ID フィールドにはデータの固有 ID が入る. データ ID はデータを送信する端末が情報を連続して送信する際に何番目のデータであるかを示すようなデータの固有 ID のことである. これは後述に示す受信処理の中の応答メッセージによる処理によって先に送信したデータが削除されないようにするためのものである. データ ID フィールドの大きさは 1 日に情報を送信する回数等を考慮し, 大きめに設定し,2byte とした.

データ消去要求フィールドは, 各端末の再送防止用データベースに対する消去要求フィールドである. データ送信元情報と同様に 8byte で, 端末の固有 ID とデータ ID を入力する. 一つの端末が送信可能なデータの個数は, データ送信元情報フィールドのデータ ID で設定されている 2byte 分である 65536 個である. データベースに登録された端末固有 ID とデータ ID からなる送信済み情報を元に受信したデータを転送するかしないかを判断するため, 送信済み情報は重複して使用することはできない. そのため, 前述した限界個数である 65536 個以上の通信は不可能になってしまう. そこで, 目標端末に対して確実に情報が伝わった後に各端末の再送防止用データベースの情報をクリアする必要がある.

データ消去要求フィールドには通常何もデータが入力されていないが, 各端末の再送防止用データベースの情報をクリアする際に, 端末固有 ID とデータ ID が入力され送信される. このフィールドの情報を元に各端末は再送防止用データベースから適切に送信済み情報を削除し, 再びその ID を用いて通信を行うことができるようになる.

イーサフォンアドホックネットワークプロトコルヘッダのフィールド情報を表 4 に示し, データ送信元情報のフィールド情報を表 5 に示す. データ消去要求のフィールド情報に関してはデータ送信元情報をほぼ同じであるため省略する.

表 4 イーサフォンアドホックネットワークプロトコルヘッダのフィールド情報

| フィールド名 | バイト数 | 内容 |
|---|---|---|
| 宛先固有 ID | 6 | データを送信する宛先の固有 ID |
| データ送信元情報 | 8 | データを一番最初に送信する送信元の情報 |
| データ消去要求 | 8 | 再送防止用記憶 ID の削除要請 |

表 5 データ送信元情報のフィールド情報

| フィールド名 | バイト数 | 内容 |
|---|---|---|
| 送信元固有 ID | 6 | データを送信した送信元の固有 ID |
| データ ID | 2 | 送信したデータの固有 ID |

## 4. 災害時通信システムにおける通信の概要

システムを初めて動作する際はデータ ID を全て利用可能状態にしてスタートさせる. ここで前提条件は以下のようにまとめられる.

- 各ノードの無線通信端末は固有の ID を持つ
- 全てのノードはお互いの MAC アドレスと固有 ID を把握している
- データ ID はデータに付けられた固有 ID
- データ ID を全て利用可能状態にしてシステムをスタートさせる

また, 通信方式及び通信におけるフレームフォーマットはイーサフォンプロトコルをベースに設計されたイーサフォンアドホックネットワークプロトコルを用いる.

まず, 通信の全体的な流れについて説明する. ある端末がデータを送信すると, その他の端末はネットワークを常に監視していて, 受信したデータが自分宛のデータではなく, 一度も転送したことがない場合, ブロードキャストによって周囲の全ての端末に対して受信したデータを転送する. また, 受信したデータが自分宛ではないが, 転送したことがある場合はそれ以上転送せず, 受信したデータを破棄する. そして, 受信したデータが自分宛であったならば, 受信したデータを受け取り, そこで通信を終了し, 受信したデータに基づいた動作を行う. 通信における各行程の詳細については以下の節で述べる.

### 4.1 データの送信

まず, データを送信する際の処理について説明する. 送信側は, データを伝える宛先である端末の固有 ID を, 送信するデータの宛先固有 ID フィールドに挿入する. データ送信元情報のフィールドに自身の固有 ID とデータ ID を挿入する. 使用したデータ ID を利用不可能状態にする. 具体的には, データ ID は 1 から開始して, データを送信するためにイーサフォンフレームを作成するたびに 1 ずつ加算していく. そのため, 通信を行う際にデータ ID が重複することはない. 初めてデータを送信する際はデータ消去要求フィールドには何も挿入しない. 受信している応答メッセージがある際は, その応答メッセージのデータ送信元情報の内容を送信するデータのデータ消去要求のフィールドに挿入する. そして, データに災害情報や避難情報のような伝えたい情報（伝達事項）を入力して送信する. ここで送信処理は図 5 のようにまとめられる.

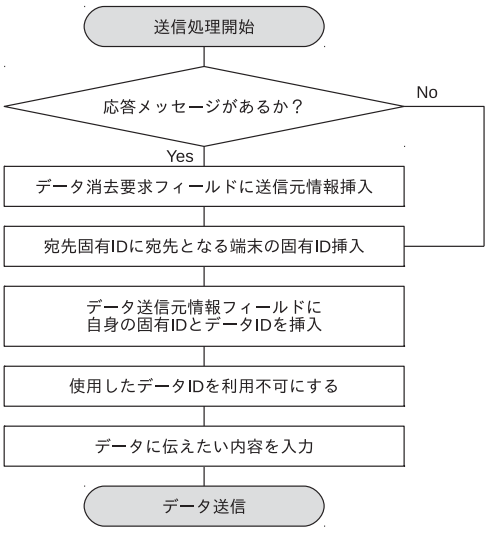


図 5 送信処理のデータフロー図

応答メッセージは受信したデータに対する返事ではなく, データの送信側が, 指定した宛先にデータが届いたのかを確認するものである. 応答メッセージにはデータ消去要求のフィールドに受信したデータのデータ送信元情報の内容を挿入しておく. これは中継処理の初期化処理やデータの送信によって利用不可状態になっているデータ ID を利用可能状態にするためなどに用いる. 応答メッセージ送信時にも送信処理を行うが, データには受理成功を示すメッセージだけで, 返事や新たな情報は入力できない.

また, 応答メッセージは自分で作成して返すものではなく, 自動で送信するように設定されている.

### 4.2 データの中継

次に, データを中継する際の処理について説明する. 全ての端末はデータを受信すると, まずデータ消去要求フィールドの中身を確認する. データ消去要求フィールドに情報が入っている場合には, そのデータ消去要求フィールドの中の固有 ID とデータ ID が自身の再送防止用データベースに記憶されているか照合し, 記憶されている場合, その情報に対応した固有 ID とデータ ID を消去する. それから, 受信したデータの宛先固有 ID と自身の固有 ID を比較する. その際, 自身の固有 ID と一致しなければ, そのデータを自分宛ではないデータであると判断する. そして, そのデータの送信元情報フィールドの送信元固有 ID とデータ ID を, 自身の再送防止用データベースと照合して転送すべきかそうでないかを判断する. 照合した結果, 再送防止用データベース内にすでに保存されていると判断された場合は, 受信したデータのブロードキャストを行わず, 受信した情報を破棄して処理を終了し, そうでない場合には, データ送信

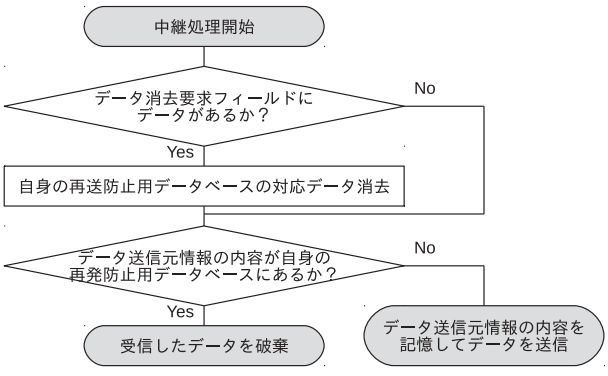


図 6 中継処理のデータフロー図

元情報を自身の再送防止用データベースに登録し, 送られてきたデータを周囲の端末にブロードキャストして送信する. ここで中継処理は図 6 のようにまとめられる.

### 4.3 データの受信

最後に, データを受信した際の処理について説明する. まず, 受信したデータのデータ送信元情報の固有 ID と自身の固有 ID とを照合し, 一致した場合は, そのデータを破棄する. 一致しなかった場合は次のステップに進む. 受信したデータの宛先固有 ID と自身の固有 ID とを照合する. 一致しなかった場合は, 受信したデータが自分宛でないということなのでデータの中継処理を行う. 一致した場合は, 再送防止用データベースをチェックし, そのデータを受け取ったことがあるか否かを判断する. 受け取ったことがあればデータを破棄し, 受け取ったことがなければ, 再送防止用データベースに登録して残りの処理を開始する. ここでの再送防止用データベースの役割は, データの宛先端末が別々の経路を経由してきた同一データを複数回受信し, 同じ処理を複数回実行しないようにすることである. そして, 受信端末はデータを受信した後に応答メッセージを送信元端末に対して送信する. データ消去要求フィールドの固有 ID が自身の固有 ID と一致した場合は, 自身の利用不可能状態にあるデータ ID とデータ消去要求フィールドのデータ ID とを照合し, 一致した場合はそのデータ ID を利用可能状態にする. ここで受信処理は図 7 のようにまとめられる.

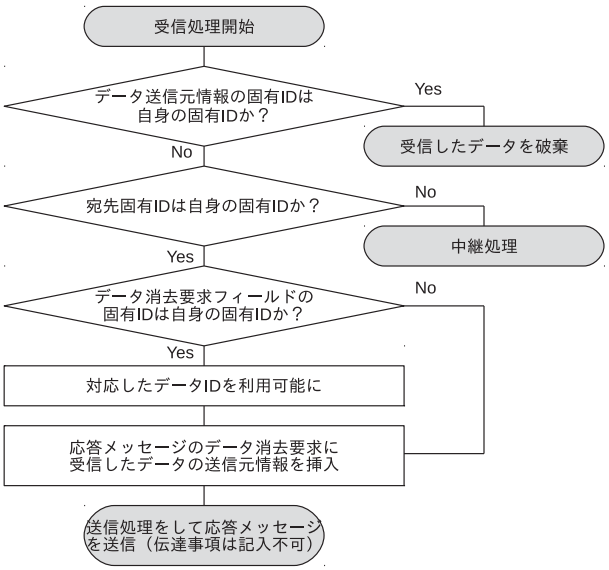


図 7 受信処理のデータフロー図

## 5. 災害時通信ネットワークを構成する無線通信端末の実装

### 5.1 無線通信端末の構成

イーサフォンはアナログデータの通信基盤として提案された通信モデルであり, 特に音声通信を対象に考えられた. そこで本研究で製作するイーサフォン無線通信端末では, 主な処理を BeagleBone Black で行う. 端末間の通信には, インターフェース変換ドングルである USB 無線 LAN アダプタを用いた通信を利用する. そして, マイクなどの音声入力用デバイスとスピーカーなどの音声出力用のデバイス, データ送受信用のデバイスで構成されている. イーサフォン無線通信端末をブロック図で表すと図 8 のように表せる.

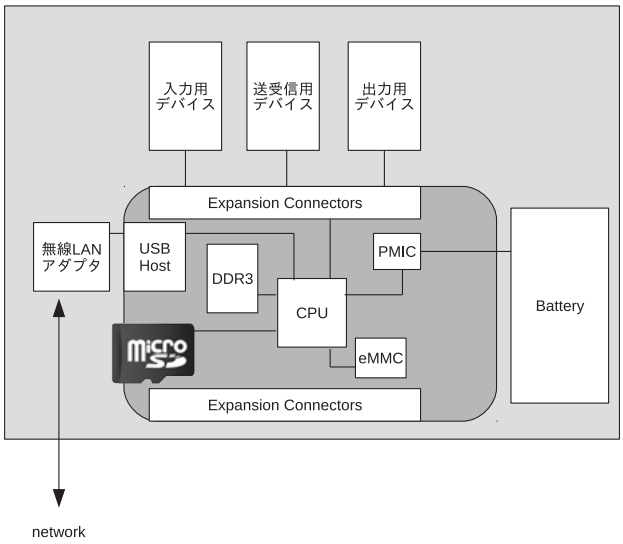


図 8 イーサフォン無線通信端末のブロック図

BeagleBone Black は,5000 円以下で購入できる名刺サイズのシングルボードコンピュータである.beagleboad.org によって, オープンソースハードウェアとして開発されており, 日本でも簡単に入手できる.SoC（System-on-a-chip）に ARM Cortex-A8 1GHz の TI AM335x を採用していて,DRAM も 512MB 搭載されている.

SoC というのは, ある装置やシステムの動作に必要な機能の全てを, ひとつの半導体チップに実装する方式である. ターゲットとなる装置により構成は異なるが, マイクロプロセッサを核に各種のコントローラ回路やメモリなどを統合したチップが多い. 一般的には, 半導体チップは機能ごとに提供されるため, プラスチック基板上に複数のチップを実装して相互に接続する必要があるが,SoC では複数のチップに分かれていた機能を統合し, ひとつのチップとして提供する. これにより, 装置の小型化や製造コストの低減, 配線の省略による高速化,

部品点数の削減による消費電力の節減などのメリットが期待できる.

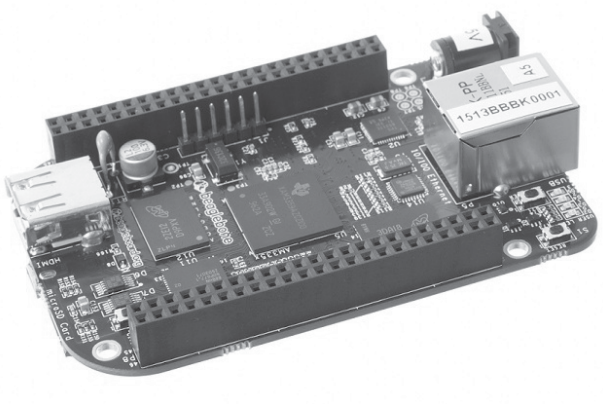

図 9 BeagleBone Black

図 9 に示している BeagleBone Black は, 手のひらに乗るような, とても小さなボードであるが,Android だけでなく,Ubuntu や Debian などの Linux 環境も動作させることもできる.BeagleBone Black の主な機能をまとめると表 6 のようになる.

表 6 BeagleBone Black の主な機能

| 機能 | 内容 |
|---|---|
| CPU | TI Sitara AM3359AZCZ100 1GHz ARM Cortex-A8 |
| 主記憶 | 512MB DDR3L 800MHz |
| 補助記憶 | 4GB eMMC(オンボード Flush),microSD,USB |
| ネット | 100M イーサ x1 |
| USB | 1 port + OTG port |
| 画像出力 | micro HDMI port |
| 音声 | HDMI 出力 |
| コンソール | ピンヘッダー 3.3V 経由接続 |
| 電源 | 5V 電源アダプタ, または USB 給電 |
| 消費電力 | 210〜460mA |
| サイズ | 86.36 x 53.34[mm] |

本研究では, 無線 LAN アダプタとして,WLI-UC-GNM（BUFFALO 社製）を用いることとした.WLI-UC-GNM を図 10 に示す.

図 10 WLI-UC-GNM

WLI-UC-GNM の仕様を表 7 に示す.

表 7 WLI-UC-GNM の仕様

| 機能 | 内容 |
|---|---|
| 準拠規格 | IEEE802.11b/g/n, ARIB STD-T66（2.4GHz） |
| 伝送方式 | DS-SS 方式, OFDM 方式, 単信（半二重） |
| データ転送速度 | IEEE802.11n : 最大 150Mbps |
| | IEEE802.11g : 最大 54Mbps |
| | IEEE802.11b : 最大 11Mbps |
| アクセス方式 | インフラストラクチャーモード, アドホックモード |
| 動作電圧 | 5.0V |
| 消費電力 | 最大 2.5W |
| 動作環境 | 温度 0〜40 ℃, 湿度 20〜80 % |

BeagleBone Black をイーサフォン無線通信端末として利用するためにしなければならない設定としては,microSD への OS のインストール, 無線 LAN アダプタの ESSID の変更と通信モードの変更がある. 本研究では,microSD に Ubuntu をインストールしたが, その方法については本稿では省くことにする. 無線 LAN アダプタの ESSID の変更と通信モードの変更については, 変更方法としては, コマンドを入力して変更する一時的に設定が反映される方法と, 設定ファイルを編集して変更する永続的に設定が反映される方法があるが, 本研究では後者を実行した. 今回,ESSID は etherphone-network, 通信モードはアドホックモードに設定した. 設定を行うには,`/etc/network/interface` を書き換える.16 行目の `iface wlan0 inet dhcp` の `dhcp` を `static` に書き換える. そして, その下の行に以下の内容をを挿入する.

```
netmask 255.255.255.0
wireless-essid etherphone-network
wireless-channel 5
wireless-mode ad-hoc
wireless-power on
```

以上の編集が終わったら BeagleBone Black を再起動することで設定が反映される.

## 6. 実験

### 6.1 パケットキャプチャリング

パケットキャプチャとは, 通信回線を流れるパケットを捕獲（キャプチャ）して中身を表示したり, 解析・集計などを行うことをいう. 主に, ネットワークを流れるデータの通信量（トラフィック）やその変化を調べたり, 障害発生時に原因を調査するのに使われる. 例えば, サーバとクライアントがどのようなパケットをやり取りしているか, 機器の故障などで異常なパケットが大量

に送出されていないかなどを調べられる. そのためのハードウェアやソフトウェアをパケットキャプチャツールあるいはネットワークプロトコルアナライザ, パケットアナライザ,LAN アナライザ, スニッファなどと呼ぶ.

ネットワークカードは通常, パケットの宛先などを読んで自分に関係がなければこれを破棄するが,「プロミスキャスモード」と呼ばれる特殊な設定にすることで, 自分の属するセグメントを流れる全てのパケットを受信することができる. パケットキャプチャではこれを取得して, パケットの中身を表示したり各種の統計を取ったりする. 通信量を記録して時間帯や曜日による変化を表示したり, パケットの送信元や宛先, プロトコルの種類などによる統計を表示することができる.

専用のハードウェアをネットワークに接続して解析するタイプの製品もあるが, 多くの製品はソフトウェアで提供されており, コンピュータのネットワークカードが受信したパケットを解析する.

今回の実験では, イーサフォン無線通信端末からパケットが発信され, そのパケットがイーサフォンアドホックネットワークプロトコルのフレームフォーマットになっていることをまず確認する. そして, 送信されたパケットが他のイーサフォン無線通信端末で受信できることを確認する. この実験において, 発信されたパケットがイーサフォンアドホックネットワークプロトコルのフレームフォーマットになっているかどうかを確認するためにパケットキャプチャツールを用いる. 本研究では, パケットキャプチャツールとして,「Wireshark」を用いる. そして, イーサフォン無線通信端末がパケットを受信したかどうかは, その端末で直に確認する.

### 6.2 前準備

イーサフォン無線通信端末を 3 台とパケットキャプチャ用の PC を 1 台用意する. イーサフォン無線通信端末のうち, データ送信用の端末を端末 A, データ受信用の端末を端末 B, その他の端末を端末 C とする. イーサフォン無線通信端末とパケットキャプチャ用の PC の無線通信の方式を「アドホックモード」に設定する. 次に, アドホックモードに設定した端末間で通信を行うために, 無線 LAN アダプタに設定する ESSID を一致させておく. そして, 端末 A から端末 B へのデータの送信をパケットキャプチャ用の PC でパケットキャプチャする. 以上のパケットキャプチャの概要を図示すると図 11 のようになる. ここで, 各端末の無線 LAN アダプタの MAC アドレスは表 8 に示した通りである. 今回はこの MAC アドレスを各イーサフォン無線通信端末の端末固有 ID として用いる. 図 12 は端末 A で無線 LAN アダプタの設定を確認した際のものである. 図 12 を確認すると, 無線通信の動作モードが「アドホックモード」になっていて,ESSID が「etherphone-network」になっていることがわかる.

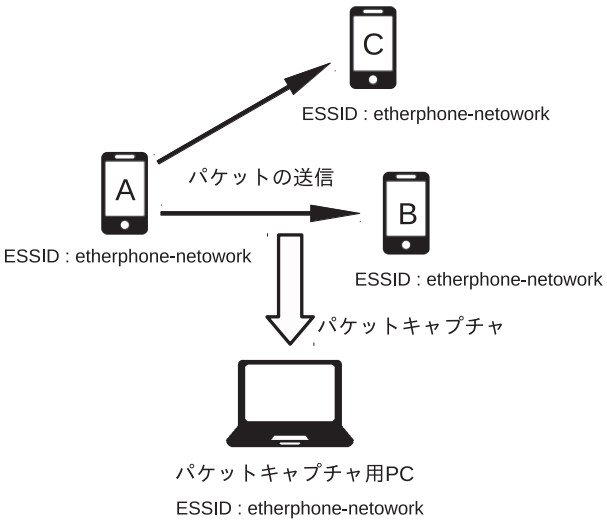


図 11 パケットキャプチャ

表 8 各イーサフォン無線通信端末の無線 LAN アダプタの MAC アドレス

| 端末 | MAC アドレス | 端末固有 ID |
|---|---|---|
| 端末 A | B0:C7:45:A9:44:1E | B0:C7:45:A9:44:1E |
| 端末 B | B0:C7:45:A9:18:D9 | B0:C7:45:A9:18:D9 |
| 端末 C | B0:C7:45:AA:2F:32 | B0:C7:45:AA:2F:32 |

### 6.3 パケットキャプチャ

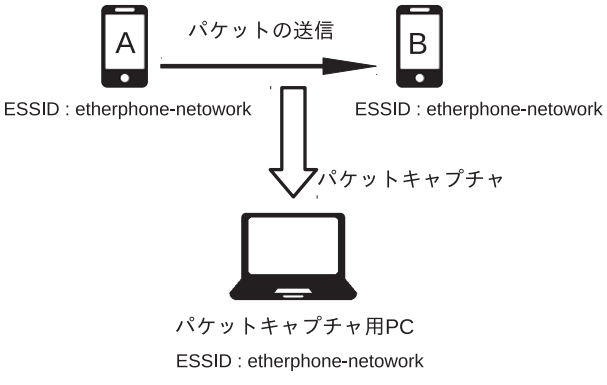


図 13 端末 A から端末 B 宛にデータを送信

まずは, 図 13 のような端末 A と端末 B, そしてパケットキャプチャ用の PC がある状態を用意する. そして, 端末 A から端末 B 宛にイーサフォンアドホックネットワークプロトコルのフレームフォーマットでデータを送信する. 送信するパケットの概要は表 9 のようになる.

```
ubuntu@BeagleBoneBlack:~$ ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr b0:c7:45:a9:44:1e
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::b2c7:45ff:fea9:441e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2871 (2.8 KB)

ubuntu@BeagleBoneBlack:~$ iwconfig wlan0
wlan0     IEEE 802.11bgn  ESSID:"etherphone-network"
          Mode:Ad-Hoc  Frequency:2.432 GHz  Cell: 5E:96:BF:F1:C2:8D
          Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

図 12 ESSID と通信モードの確認

表 9 送信するパケットの概要

| 名称 | | 内容 | 説明 |
|---|---|---|---|
| 宛先 MAC アドレス | | FF:FF:FF:FF:FF:FF | ブロードキャストアドレス |
| 送信元 MAC アドレス | | B0:C7:45:A9:44:1E | 端末 A の MAC アドレス |
| タイプ | | 1234 | イーサフォンのプロトコルタイプ |
| イーサフォンタイプ | | 1011 | 本研究のイーサフォンアプリケーションのタイプ |
| サイズ | | 116 | フレームサイズ |
| 宛先固有 ID | | B0:C7:45:A9:18:D9 | 端末 B の端末固有 ID |
| データ送信元情報 | 送信元固有 ID | B0:C7:45:A9:44:1E | 端末 A の端末固有 ID |
| | データ ID | 1 | |
| データ消去要求 | 端末固有 ID | 00:00:00:00:00:00 | 今回はデータ消去要求は出さない |
| | データ ID | 0 | 今回はデータ消去要求は出さない |
| データ | | announce:this packets are test data by running the program of etherphone.exe | 文字列 |

イーサフォン無線通信では通信方式としてブロードキャスト通信を用いるので宛先 MAC アドレスはブロードキャストアドレスを指定する. 送信元 MAC アドレスは今回送信元である端末 A の MAC アドレスを指定する. タイプというのは上位層のプロトコルを識別するための番号のことであり,16 進数で表示される. 本研究ではイーサフォンのプロトコルタイプ番号を 1234 とした. イーサフォンタイプはイーサフォン通信技術を用いたアプリケーションを識別するための番号であり, 本研究では, イーサフォンタイプ番号を 1011 とした. サイズは送信するパケットのフレームサイズを表している. 宛先固有 ID は今回宛先としている端末 B の端末固有 ID を指定する. データ送信元情報は一番最初にデータを送信した端末の端末固有 ID とそのデータの ID を管理するための情報である. そのため, 送信元固有 ID は今回送信元である端末 A の端末固有 ID を指定する. そして, 一回目の送信なのでデータ ID に 1 を指定する. データ消去要求は受信処理で挿入されるフィールドであるので今回は何も指定しない. そして, 最後に送信したいデータを指定する. 今回は文字列を指定した.

実際に端末 A から端末 B 宛にイーサフォンアドホックネットワークプロトコルのフレームフォーマットでデータを送信する. 送信したパケットを Wireshark でキャプチャすると図 14 のようなる. 送信したフレームは 16 進数 (Hex) で表記される.

### 6.4 実験結果

今回, 端末 A から端末 B に向けてイーサフォン無線通信でデータを送信した. イーサフォン無線通信ではイーサフォンアドホックネットワークプロトコルのフレームフォーマットを利用し, 送信したパケットの内容は表 9 のとおりである. このパケットの内容と Wireshark で

```
Hex                                                     Text
--------------------------------------------------------------------------------
ff ff ff ff ff ff b0 c7 45 a9 44 1e 12 34 10 11  ........E.D..4..
00 74 b0 c7 45 a9 18 d9 b0 c7 45 a9 44 1e 00 01  .t..E.....E.D...
00 00 00 00 00 00 00 00 61 6e 6e 6f 75 6e 63 65  ........announce
3a 74 68 69 73 20 70 61 63 6b 65 74 73 20 61 72  :this packets ar
65 20 74 65 73 74 20 64 61 74 61 20 62 79 20 72  e test data by r
75 6e 6e 69 6e 67 20 20 74 68 65 20 70 72 6f 67  unning  the prog
72 61 6d 20 6f 66 20 65 74 68 65 72 70 68 6f 6e  ram of etherphon
65 00 00 00 00                                   e....
```

図 14 Wireshark でキャプチャしたパケット

キャプチャしたパケットを比較し, 送信したパケットがイーサフォンアドホックネットワークプロトコルのフレームフォーマットとなっていることが確認できた. また, 端末 B の標準出力から端末 B 宛に送信したパケットを受信したことを確認できた.

## 7. 考察

本研究では, イーサフォン無線通信を利用してモバイルアドホックネットワークを構築した. そして, イーサフォン無線通信端末でのモバイルアドホック通信によるデータ通信を行った. 実験結果から, 送信したパケットがイーサフォン無線通信で利用するイーサフォンアドホックネットワークプロトコルで指定したフレームフォーマットになっていることが確認した. また, 端末 B の標準出力から端末 B 宛に送信されたパケットを受信したことを確認した. このことから今回製作したイーサフォン無線通信端末がイーサフォン無線通信用のプロトコル通りに挙動していることがわかる.

## 8. まとめ

本研究では, イーサフォン無線通信端末を用いて災害時における代替的な通信システムを構築するためにイーサフォン無線通信端末でのモバイルアドホック通信によるデータ通信を行い, イーサフォン無線通信端末がイーサフォン無線通信用のプロトコル通りに挙動しているかの検証を行った. パケットキャプチャリング実験を行った結果, 今回製作したイーサフォン無線通信端末が正しく動作することがわかった. また, イーサフォン通信技術を用いることで, 通信に関する設定の手間を省け, 安価にネットワークを形成することが可能であることがわかった.

このことから, 本研究で製作したイーサフォン無線通信端末が災害時の代替的通信システムに求められるコストが安価・即応性・耐障害性という 3 つの要求を満たしつつ簡単に通信を行うことができることを示すことが出来たと考えられる. 今後の課題としては, シミュレーション実験とイーサフォン無線通信端末の動作実験の比較検討や, モバイルアドホックネットワークを利用する際に解決しなければならない問題点であるセキュリティや電力効率などの解決及び検証を行う必要があると考えられる.

## 参考文献


[1] 大和田泰伯, 照井宏康, 間瀬憲一, 今井博英: マルチホップ無線 LAN の提案と実装, 電気情報通信学会論文誌, J89-B, 11, 2092-2102 (2006).

[2] Yao-Nan Lien, Hung-Chin Jang and Tzu-Chieh Tsai: A MANET Based Emergency Communication and Information System for Catastrophic Natural Disasters. Distributed Computing Systems Workshops, 2009. ICDCS Workshops '09. 29th IEEE International Conference on, 412-417 (2009).

[3] 吉岡正博, 白井治彦, 黒岩丈介, 小高知宏, 小倉久和: イーサネットの機能のみを用いた通信モデルの提案と実装-ブロードキャスト機能を利用したイーサフォン, 情報処理学会全国大会講演論文集, 69(2007).

[4] Ms.Ruchia A.Kale and Prof.Dr.S.R.Gupta. AN OVERVIEW OF MANET AD HOC NETWORK: International Journal Of Computer Science And Applications, 6, 2, 223-227 (2013).

[5] 神谷将樹, 白井治彦, 黒岩丈介, 小高知宏, 小倉久和: イーサフォンを用いたアドホックネットワークによる災害時通信システムの構築, 日本知能情報ファ

ジィシステムシンポジウム講演論文集, 27, 969-972 (2011).

[6] 福井大学:通信装置, 及び, 通信方法, 特許出願 2004-217916, 特許公開 2006-041842, 特許番号（特許第 4110251）.

[7] 袴田暁人, 白井治彦, 黒岩丈介, 小高知宏, 小倉久和: 災害時復旧支援ネットワーク用の新しいプロトコルの提案, 福井大工報, 59, 17-24 (2011).