

地域情報の流通基盤となる大規模多目的情報ネットワーク構成技術の研究

研究代表者 山本 尚生 東京都市大学 知識工学部 教授

1 はじめに

無線メッシュネットワークと無線センサーネットワークの融合、連携により、アクセスネットワーク機能、多目的情報センシング機能、および地域内情報の流通機能を、常設の環境として提供する多目的情報流通基盤の構築を目指し、主に、広域（市区町村レベル）への適応性と管理の柔軟化を可能とする技術を追求してきた。課題を主に、スケーラビリティ上の問題の解消およびトラフィック制御法の確立に絞り、次の2項目、

課題A 運用時における品質維持およびセキュアなソフトウェア管理技術（2章、3章）

課題B 大規模化に備えたオーバーレイバイパス網の構成法およびゲートウエイ最適配置法（4章）

に関する技術提案とその検証を行った。以下その検討状況を報告する。

2 災害時における長期品質維持技術

2-1 検討の背景

災害における人命救助に関しては、救助を待つ人たちの生存率が、72時間をこえると急激に低下すると言われている。つまり、災害当日こそ通信インフラを利用できるようにすべきであり、災害当日から通信途絶を回避できるネットワークが必要である。このようなネットワークとして自律分散制御により柔軟なルーティング機能を有する無線メッシュネットワーク（WMNs: Wireless Mesh Networks）が注目されている[2-1] [2-2] [2-3]。

しかし、WMNsは商用電源での利用が想定されていたため、これまでバッテリー駆動での長期運用の検討がほとんどなされていない。

本研究では、インターネットと接続されたGWの存在するバッテリー駆動のWMNsを想定し、ネットワークの運用長期間化技術の検討を目的とする。主に次の2つの方策について検討する。

1 WMNsにおいて利用が想定されるCSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

[2-4] [2-5]の制御パケットの送信回数を削減することで、ノードの消費電力を軽減する方式

2 ノードの残電力量をメトリックとしたルーティングによりノード間の電力平準化を行う方式

2-2 提案手法

大別して運用上の対策と設計上の対策がある。災害時には設計上のノード配置等が変化し制限されることも想定されるので、ここでは運用上の対策としての提案を行う。

(1) ノードの送受信回数削減による省電力化

WMNsではパケットのデータ量が大きいいため通常のデータアグリゲーションによるパケット数の削減効果は期待できない。そこで、擬似的なデータアグリゲーションを提案する。本手法では物理的にパケットを集約しなくても、CSMA/CA制御パケットのオーバーヘッドを削減する方法を提案する。

図1にWMNsにおいてCSMA/CAに擬似的なデータアグリゲーションを導入した場合の通信シーケンスを示す。

詳細説明は省略するが、同じ方向へ連続で転送するデータフレームの個数に基づいて、通常データフレームごとに個別に行うCSMA/CAプロセスをまとめて行う。最初のパケット送信におけるRTS内のDurationフィールドの値をそれに応じて増加させる。これにより、ノードがRTS/CTSを送受信

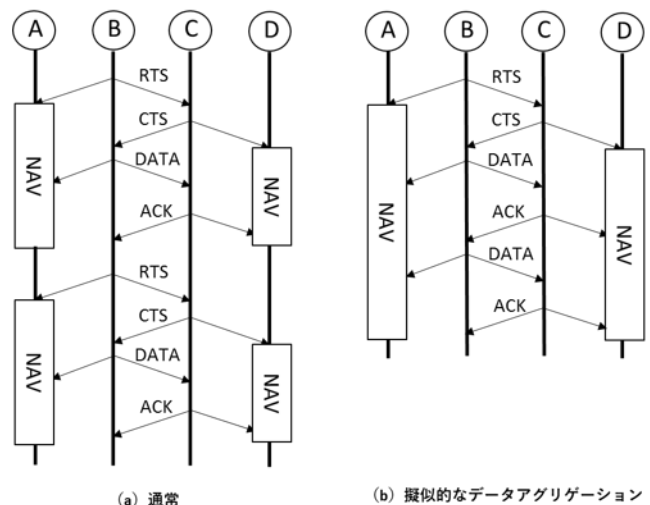


図2-1 WMNsにおいてCSMA/CA(RTS/CTS/DATA/ACK)

する回数が減り、個々のパケットに要する電力消費を削減できる。また、物理的にアグリゲーションしているわけではないので、再送が発生した場合も誤りの発生したパケットのみの再送で済む。

(2) 電力消費の平準化

WSNsに適した代表的なルーティングプロトコル LEACH (Low-Energy Adaptive Clustering Hierarchy) [2-6]では、負荷の集中するクラスタヘッドを一定期間ごとに交代させることにより、多数のノードに負荷を分散させ電力平準化を行う。本検討ではWMNsへこの考え方を援用する。ノードの残電力量をメトリックとしてルーティングを行うことで、全ノードが均等に送受信を行い電力消費の偏りを減らし、特定のノードの電力が早期に枯渇することを防ぐ。ノードの残電力量を反映するメトリックの式を(1)に示す。

$$[\text{metric}]_{\text{new}} = \text{metric} \times 1/E^2 \quad (1)$$

metricはメトリック値であり、Eは残電力量である。

2-3 シミュレーションによる性能評価と今後の課題

比較は、①通常のCSMA/CAの動作で最短ホップを経路とした場合、②CSMA/CAに擬似的データアグリゲーションを加えた場合、③通常のCSMA/CAの動作で電力平準化の経路とした場合、④CSMA/CAに擬似的データアグリゲーションを加え、電力平準化の経路とした場合、の4パターンで行う。表2-1にシミュレーション諸元を。ノードは9×9の格子状に300m間隔で配置し、格子状の頂点の内、1つをGWとする。各ノードに発生するパケットは単位時間あたりの平均発生パケット数λのポアソン分布に従うものとする。また、全てのパケットはGWを宛先とする。発呼率λを7~14まで変化させ、ネットワークの負荷を変化させる。パケットのデータサイズを1000byteとし、RTSのサイズを20byte、CTS、ACKのサイズを14byteとする。1byte当たりの送信電力を式2に示す。送信電力23dBm=200nWであり、72.2Mbps=9025kbyteであることから、1byte当たりの送信電力(mW)は0.00002216(mW/byte)となる。これから算出されるRTS/CTS/DATA/ACKの送信電力を表2-2に示す。なお、本検討では受信にかかる電力は考慮しない。

評価結果を図2-2, 2-3に示す。①の場合を「normal」、②の場合を「hs_agg(hand-shake aggregation)」、③の場合を「ene_eff(energy efficient)」、④の場合を「hs_agg+ene_eff」として、比較する。

表2-1 シミュレーション諸元

seed	1~5
発呼率(λ)	7~14
発呼間隔	平均1/λの指数分布に従う
ノード配置	9台×9台を格子状に配置 (300m間隔)
GW位置	格子状の頂点の内1つ
伝送レート	72.2[Mbps]
送信電力	23[dBm]
受信閾値	-82[dBm]
利得	0[dB]
伝達係数	2.45
Data size	1000[byte]
RTS size	20[byte]
CTS size	14[byte]
ACK size	14[byte]

表2-2 消費電力

	size(byte)	送信(mW)
Data	1000	0.02216000
RTS	20	0.00044320
CTS	14	0.00031024
ACK	14	0.00031024

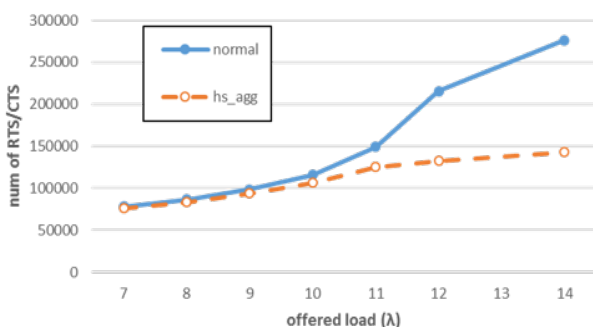


図2-2 RTS/CTS送信回数

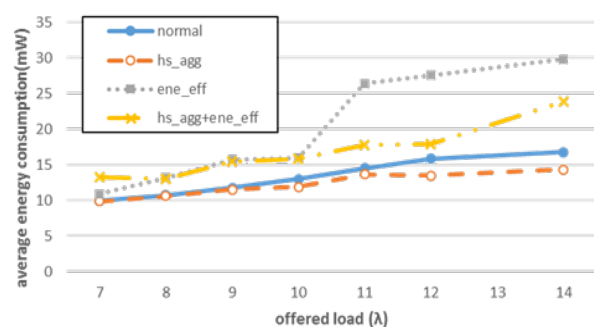


図2-3 平均消費電力(mW)

図2-2にnormalとhs_aggのオフロードに対するRTS/CTSの送信回数を示す。図2-2より、低負荷時はあまり変化が見られないが、高負荷になるに連れてnormalよりもhs_aggの方がRTS/CTSの送信回数を削減できていることがわかる。これは、低負荷時はアグリゲーションの機会が少なく通常と同じ動作となるが、高負荷時はアグリゲーションの機会が多くなり、提案手法が有効に機能したためである。図2-3にオフロードに対する消費電力の平均(mW)を示す。図2-3より、normalと比べhs_aggの消費電力が小さいことがわかる。これは、RTS/CTSの送信回数が削減されたことによって消費電力もまた削減されたためである。

今後の課題として、より実環境に即したシミュレーションを行う必要があり、ネットワークシミュレーター Qualnet 等に提案手法を実装していく。

3 運用時におけるセキュアな管理技術

3-1 検討の背景

MANET(モバイルアドホックネットワーク: Mobile Ad-hoc Networks) や WMNs のような無線マルチホップ環境上の通信において、暗号化せずに通信した場合、通信経路上でデータが盗まれたり中間者攻撃(Man-In-The-Middle attack)にあう危険性が高い[3-1] [3-2] [3-3]。本検討では、従来有線系で使われてきた IPsec と呼ばれる暗号化通信の仕組みを用いてこのような脅威から守る技術の提案を行う。まず関連技術を説明する。

(1) IPsec の仕組み

IPsec はデータを送信する際に、認証情報を付加して送信をする。受信側は、受信したデータとこの認証情報を比較することによって、通信経路上でデータが改ざんされていないかどうかを確認する [3-4]。MANET に IPsec を適用する際には、移動通信のため途中で特定フェーズが途切れてしまう可能性がある。その際には再度フェーズを実行しなければならないため時間がかかってしまうという問題点がある(図 3-1)。

(2) IKEv2 とは

IKEv2 は、共有秘密鍵と SA(Security Association) の折衝と管理を自動で行うプロトコルである。

IKEv2 は、IKEv1 と比較して、各機能のシンプル化とリモートアクセス VPN 機能(ユーザー認証機能等)が強化されている。

(3) MOBIKE とは

MOBIKE(Mobility and Multihoming Protocol) [3-5]は、通信の途中で IP アドレスが変更されるような場合でも SA を再生成することなく、新たな IP アドレスを通知するだけで、既に確立された SA を継続して利用できるプロトコルである。IPsec で行われる、ネゴシエーションしたセッション情報の変更、コネクションの再構築の必要がなくなるため、コネクション再生成の時間を短縮できる。

3-2 性能評価環境と実験

本研究では、無線 LAN インターフェースを持つ

PC を端末とした実機による実験環境を構築して提案方式の性能を評価する。図 3-2 に実験環境を示す。下記の実験を上記環境にて行った。

1. VPN 接続(IKEv1 および IKEv2)がされている状態において 1GB のファイルをダウンロードする時間を計測する。MANET は経路を変更しないものとする
2. VPN 接続(IKEv1 および IKEv2)状態において MANET の通信経路を切り替える。切り替えた際にどの程度の早さで VPN 接続が切り替わるか測定する。

本実験では、IKEv2 を構築するためにマイクロソフト社製の Windows Server 2012 に搭載されている DirectAccess を利用した。DirectAccess では、リモート ユーザーは仮想プライベート ネットワーク (VPN) に接続しなくても、社内共有フォルダー、Web サイト、およびアプリケーションに安全にアクセスできる。また、IKEv1 を構築するためにソフイーサ社製の PacketiX VPN を使用した。PacketiX VPN は、L2TP/IPsec, OpenVPN, MS-SSTP, L2TPv3, EtherIP などの VPN プロトコルに新たに対応し、iPhone や Android などのスマートフォンや Cisco などの VPN ルータからの VPN 接続を受付けることができたようになった VPN ソフ

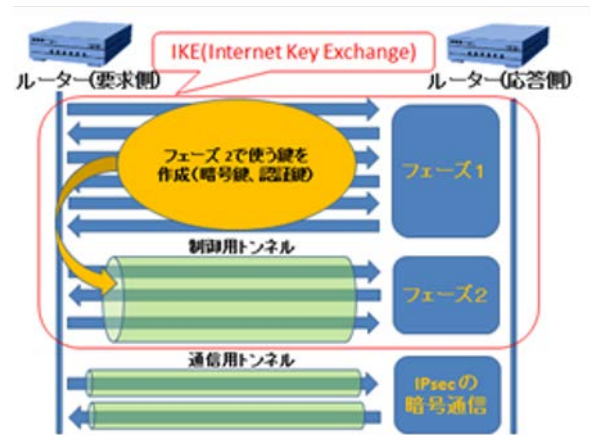


図3-1 IPsecにおける通信手順

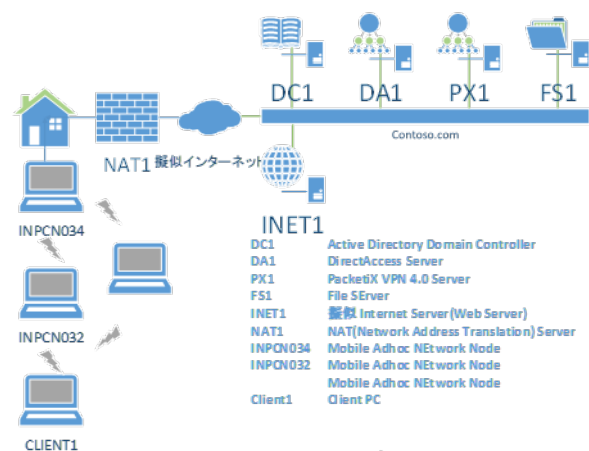


図3-2 実験環境

トウェアである。こちらは、IKEv1 なので再接続の際には手動にて操作して接続する必要がある

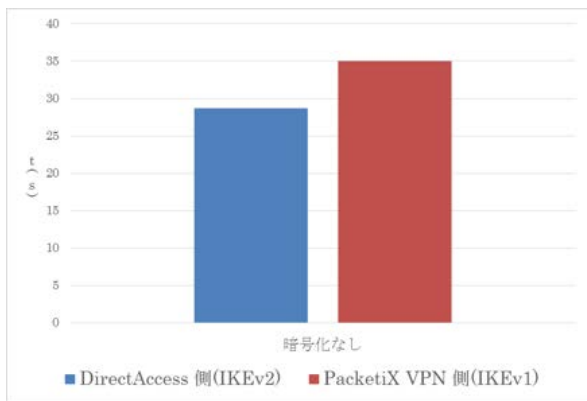


図3-3 実験(1)の結果

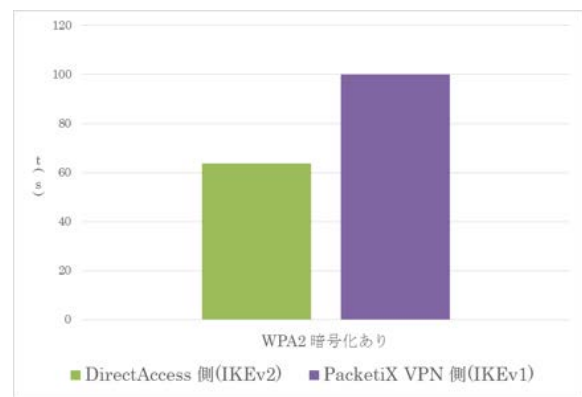


図3-4 実験(2)の結果

本実験では、図 3-3 に示すようにファイルのダウンロードは IKEv2 の方が早いことが分かる。これは、IKEv2 の方がパフォーマンス良いことが分かる。

また、図 3-4 より、経路切り替え時の接続に関しても IKEv2 の方が優位であることがわかる。これは、IKEv2 ではコネクションを再度生成するためと考えられる。以上より、IKEv2 の方が優位であることが判明した。

4 大規模化に備えたオーバレイバイパス網の構成法およびゲートウェー動的配置法

4-1 検討の背景

WMNs の大規模化に伴い中継ホップ数の増加や、輻輳の発生のパケット損失の増加など、ネットワーク性能が劣化してしまうことが考えられる。

本検討では、メッシュ機能を持たせた自律飛行体 (UAV) をバイパス経路の入り口として機能させ、GW と UAV 間にバイパス経路を構築し、このバイパス経路 [4-1] [4-2] へ、UAV が接近した地上ノードのトラフィックを動的に分散する経路構築法を提案する。地上ノードのトラフィックを効率的に軽減させることで輻輳を回避し、ネットワーク性能劣化の抑制を期待する。

UAV は自在に移動できるので、災害によるノード破損や一時的な通信集中などの動的なトラフィック変化に対して、柔軟に対応することが可能となる。この特性を活かし、トラフィックの変化に対して効率的に経路を構築するためには、

1. 移動ノードの接近を検知して経路を迅速に更新する経路変更アルゴリズム

2. 経路接続が不安定な領域を探索する移動ノードの行動アルゴリズム

が必要と考えられる。ここでは主に①についての検討結果を示す。

4-2 提案方式—空中バイパス経路構築法

GW と通信可能な範囲内を飛行する UAV をバイパス経路の入り口となる空中ノードとして機能させ、地上ノードから見て、UAV を移動する疑似 GW として機能させる (図 4-1)。本提案では、IEEE802.11s タスクグループにおいて標準のルーティングプロトコルとして定義されている HWMP (Hybrid Wireless Mesh Protocol) を用いる [4-3] [4-4]。

(1) 経路変更の提案アルゴリズム

HWMP では周期的にプロアクティブ PREQ を送信することで、ネットワーク内の GW と全 MP 間の経路をプロアクティブに構築する。このプロアクティブツリー経路構築モードにを利用し、UAV との通信が可能になった地上ノードが GW を宛先とする通信を行う場合に、UAV ノードを中継ノードとして選択する機能を追加する。以下にその制御プロセスを記述する。

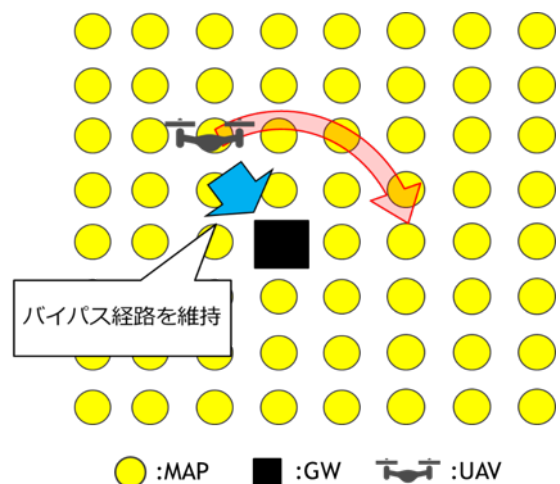


図4-1 ネットワーク構成と UAV の動作

(2) バイパス経路選択手順

UAV ノードは GW との通信が途切れないよう、GW との通信可能範囲内を移動する (図 4-2)。UAV ノードは自ノードの MAC アドレスを含むノード情報が記述されたビーコン信号を一定間隔で信号到達範囲内に存在する地上ノードに送信する。ビーコンを受信した地上ノードは、自身の持つ宛先が GW の経路表からネクストホップアドレスに設定されているアドレス情報を UAV ノードの MAC アドレスに書き換える。書き換えた後に PREQ メッセージを受信し、シーケンス番号やメトリックによって経路が再度変更されないように、ビーコンの送信間隔は PREQ メッセージが届くよりも短い間隔で設定する必要がある。

UAV ノードには、自ノードが GW 以外のノードをネクストホップに設定しないようにするために、UAV ノードが GW から定期的な送信されるビーコン信号を受信したときネクストホップアドレスを GW の MAC アドレスに書き換える。UAV ノードをネクストホップに設定していた地上ノードとの通信可能範囲から UAV ノードが離れてしまうことがある。このような事態を想定して、更新した経路表に beacon Life time を追加し、一定時間 UAV ノードからのビーコン信号を受け取らなければ、再度経路表の更新を行う動作を追加する。

バイパス経路を地上ノードに利用させる機能によって、かえって UAV ノードに通信が集中してしまい通信性能が低下してしまうことを避けるため、UAV ノードが中継ノードとして選択される回数を制限する必要がある。ホップ数に制限値を設け宛先ノードまでのホップ数が少ない経路に関してはバイパス経路を利用しないように設定する。以上の動作によって、UAV を用いたバイパス経路を効率的に利用することが可能となり、輻輳を回避しネットワーク性能劣化の抑制が期待できる。

4-4 評価実験 (シミュレーション) と課題

ネットワークモデルを図 4 に示す。UAV は GW と 1 ホップで通信が出来る距離を保ち、一定の速度で円状に移動する。上記の環境においてバイパス経路を併用できているか確認するため、ホップ数制限値を変化させ UAV ノードの中継ノード被選択率を変化させた場合 (シナリオ 1) と、ネットワーク内のセッション数を変化させた場合 (シナリオ 2) の二通りの評価を行った。経路変更のホップ数制限は、各地上ノードが持つ GW までのホップカウントを参照し、設定したホップ数制限値を下回ったノードは UAV を中継ノードとして選択しないように設定する。

評価方法として、遅延時間とパケット損失率の比較を行う。表 4-1 にシミュレーション条件を示す。

図 4-3, 4-4 は、ホップ数制限の値を 2~6 の間で変化させた場合の平均パケット損失率, 最大パケット損失率, 平均遅延時間, 最大遅延時間である。図 4-3 の平均パケット損失率より、ホップ数制限値が 2~6 の中間である 3,4 の値のときにパケット損失を抑制できていることが分かる。また、最大パケット損失率の値より、ホップ数制限値が 4 よりも大きい値の場合、UAV ノードを使わない場合以上にパケット損失が発生することがわかる。同様に、図 4-4 の最大遅延時間の結果についても同様に、ホップ数制限値が大きい値のときに遅延時間が長くなっていることがわかる。

以上の結果より、ホップ数制限により UAV ノードを中継ノードとして選択し GW までのバイパス経路を選択的に用いることで、輻輳によるネットワーク性能の劣化を抑制できることがわかった。しかし、バイパス経路を効果的に利用するためには UAV ノードが中継ノードに選択される回数を適切に制限する必要がある。また、UAV が移動することで通信している経路が断絶してしまいネットワーク性能に影響を与えてしまうため、beacon Life time とは別に経路情報を更新する動作を考案する必要があることがわかった。

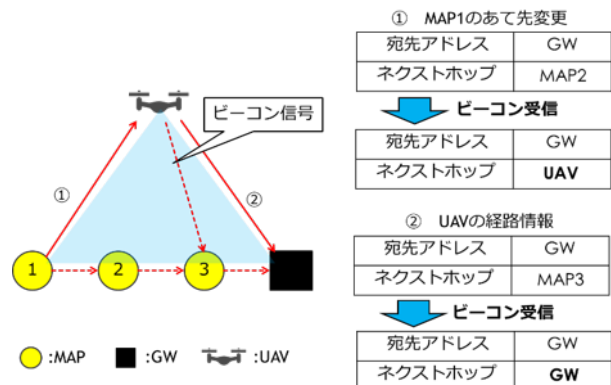


図4-2 あて先アドレスの変更

表4-1 シミュレーション条件

シミュレータ	Qualnet 6.1
シミュレーション時間	330[s]
地上ノード数	64
GW 数, 空中ノード数	1
ノード配置	8 台×8 台を格子状に配置 (300[m]間隔)
GW-空中ノード間距離	450[m]
ネットワークプロトコル	IPv 4
MAC プロトコル	IEEE802.11s
通信方式	IEEE802.11a/g
周波数	2.4[GHz]
伝送速度	Auto Rate Faillback (6~54Mbit/s)
パケット送信間隔	0.1[s]

今後、UAV ノードが中継ノードとして選択される回数を制限する方式にホップ数制限だけではなく、メトリック値を変化させることで動的に UAV に流れるトラフィック量を制限する方式を用いた場合のネットワーク性能評価を行っていく。また、バイパス経路を用いた通信と地上ノード間における通信との無線干渉の影響を避けるため、バイパス経路において地上ノード同士の通信とは異なるチャネルを用いる方式についても検討していく。

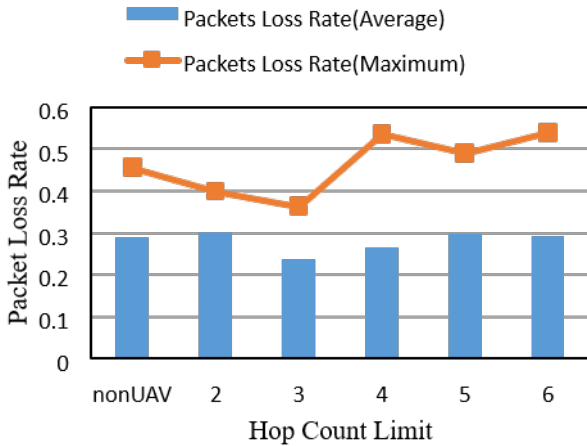


図4-3 パケット損失率の平均と最大値

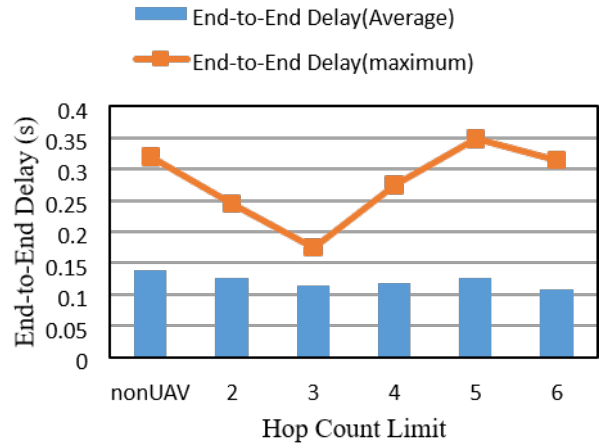


図4-4 遅延時間の平均と最大値

5 まとめ

無線メッシュネットワークと無線センサーネットワークを融合、連携することにより、多目的情報流通基盤の構築を目指し、広域への適応性と管理の柔軟化、セキュア化を可能とする技術を追求し、以下の検討を行った。

災害時における長期品質維持技術として、無線メッシュネットワークにおける長期運用のための省電力化の検討を行い、制御パケット (CSMA/CA) の削減とノード消費電力平準化技術を提案した。運用時におけるセキュアな管理技術としては、有線系の通信網で使われている IPsec の無線マルチホップ環境での適応性を確認するためにモバイルアドホックネットワーク上での実験により性能評価を行った。また、無線メッシュネットワークの大規模化に備えたオーバレイバイパス網の構成法およびゲートウエー動的配置法として、移動型中継端末を利用した輻輳回避経路構築法を提案し性能評価を行った。

【参考文献】

- [2-1] 総務省, “東日本大震災における情報通信の状況,”平成 23 年版 情報通信白書,
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h23/pdf/n0010000.pdf>.
- [2-2] 遊橋裕泰, “ケータイから見た 3.11 東日本大震災,”
https://www.nhk.or.jp/bunken/book/media/pdf/2014_c1.pdf.
- [2-3] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey,” Comput. Network. ISDN Syst., vol.47, no.4, pp.445-487, Mar. 2005.
- [2-4] P. Karn, “MACA – a new channel access method for packet radio,” ARRL/CRRL Amateur Radio 9th Computer Networking Conference, pp. 134-40, ARRL, 1990
- [2-5] IEEE Std. 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1997.
- [2-6] Ngo Thuan, Nishiyama Hiroki, Kato Nei, Sakano Toshikazu, and Takahara Atsushi. “A spectrum- and energy-efficient scheme for improving the utilization of mdru-based disaster resilient networks,” IEEE Transactions on Vehicular Technology - Special Section on Green Mobile Multimedia Communications, 32(2):345–355, February 2014.
- [3-1] Cisco Visual Networking Index

http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

- [3-2] 上口 優太, 井上 慎一郎, 菅谷 直史, 石井 方邦, 笹瀬 巖, ” MANET における匿名通信のための経路構築を必要としない Onion Routing”, 情処研報, 2010-CSEC-49(6), 1-6, May 2010.
- [3-3] 川端 秀明, 末田 欣子, 水野 修, 石井 啓之, ” MANET におけるユーザ信頼度を考慮した公開鍵分散管理方式の提案”, 信学技報, 87-92, Dec. 2009.
- [3-4] ITpro, 攻略編:全体をつかんで逆から見る, 日経 NETWORK 流で理解しよう
<http://itpro.nikkeibp.co.jp/article/COLUMN/20071012/284162/>
- [3-5] IKEv2 Mobility and Multihoming Protocol (MOBIKE) 4555, <http://www.ietf.org/rfc/rfc4555.txt>
- [4-1] 今井清隆, 山本尚生, “外部高速ネットワークを併用した無線 LAN メッシュネットワークの大規模化の研究—大規模化によるネットワーク性能低下の抑制—”, 信学技法, Vol.109, No.145, pp.43-48, Jul.2009.
- [4-2] 岡宏典, 岡田啓, 間瀬憲一, “気球と地上ノードを用いた緊急時のアドホックネットワーク構築システム”, 信学論(B), Vol.J94-B, No.7, pp.822-832, Jul.2011.
- [4-3] 西沢耕太郎, 山本尚生, “無線メッシュネットワークにおけるふくそう制御用シグナリングと連携した迂回経路構築アルゴリズム”, 信学論(B), Vol.J92-B, No.9, pp.1500-1512, Sep.2009
- [4-4] M. Bahr, Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s, IEEE, 2007.

〈発表資料〉

題 名	掲載誌・学会名等	発表年月
発展途上国における通信ネットワークを対象とした信頼性評価尺度とその評価法の検討	電子情報通信学会論文誌 Vol. J99-A No. 9	2016年9月
無線メッシュネットワークにおける災害時長期運用のための省電力化の検討	電子情報通信学会、信学技報, vol. 116, no. 323, CQ2016-86, pp. 71-76	2016年11月
無線メッシュネットワークにおける移動型中継端末を利用した輻輳回避経路構築法の研究	電子情報通信学会、信学技報, vol. 116, no. 323, CQ2016-85, pp. 65-70	2016年11月
無線センサネットワークにおけるデータ収集遅延時間を短縮する自律飛行体移動スケジューリング手法の研究	電子情報通信学会 2017 総合大会	2017年3月