「マルチメディア，分散，協調とモバイル
(DICOMO2018)シンポジウム」 平成30年7月

データ送信量解析によるアドホックネットワークの動作推定方式の提案

福岡宏一† 齋藤正史‡1 横谷哲也‡2 寺島美昭†

概要：自動車の自動制御運転（自動運転）では，自動運転のための情報の交換を車車間や路車間で直接通信を行う無線アドホック通信を用いることが想定されている．その際，無線通信に対する攻撃による通信途絶や通信遅延は，自動運転の安全性を脅かすと考えられ，この無線アドホックネットワークにおいてジャミングなどの攻撃による通信途絶の検知や通信途絶からの迅速な回復といった高信頼化は重要である．そこで本研究では，攻撃による通信途絶の検知を目的とした．本稿は，将来の攻撃検知への前段階として，送信電波から抽出したデータ送信量の解析のみを用いることによってネットワークの動作を推定し，ネットワーク監視を行う方式を提案する．本方式は，送信電波のみを用いるため，無線の不安定性や帯域の細さに適した方式となり，ネットワークのプロトコルや各種設定に依存しないブラックボックスなネットワーク監視が可能となる．また，提案方式の理論検証のための実験手順の考案を行い，ネットワークシミュレータによって実験と検証を行う．

Proposal of Motion Estimation Method of Wireless Ad Hoc Network by Data Transmission Amount Observation

KOUICHI FUKUOKA† MASASHI SAITO‡1 TETSUYA YOKOTANI‡2
YOSHIAKI TERASHIMA†

1. はじめに

昨今話題となっている自動車の自動制御運転（以下自動運転と呼称）では，自動での加減速やステアリング操作を行う運転のための情報の交換を，車車間や路車間で直接通信を行う無線アドホック通信を用いて行うことが想定されている[1]．その際，無線通信に対するジャミング攻撃やサイバー攻撃等による通信途絶や通信遅延のネットワーク異常は，死角に存在する車両等との接触事故や隊列走行の乱れなどの自動運転の安全性を脅かすと考えられている．この攻撃への対策には，攻撃の検知と，ネットワーク異常の修復が必要である．本研究では自動車の無線通信に対する攻撃の検知部分について着目し，ネットワーク監視によって攻撃検知を行うことを目的とする．

本研究では，各端末の電波からデータ送信量を抽出し，これを用いて傾向解析や他端末と比較解析することによって，ネットワーク状況を外部から推定してネットワークを監視する方式を提案する．提案方式では，無線通信の際に発せられている電波のみを利用するため，ネットワークのプロトコルや各種設定に依存しないブラックボックスなネットワーク監視が可能となる．

本稿は，攻撃検知の前段階として，ネットワークの基本的な機能の動作推定方式の提案を行い，提案手法の理論検証のための実験設定の考案と，ネットワークシミュレータによる実験で検証を行う．

2. 課題設定

本研究では，自動運転を行う自動車に使用される無線アドホックネットワークに対する攻撃の検知を目標としている．しかし，現時点ではデータ送信量解析による外部からの動作推定の可否が不明である．そのため，攻撃検知の前段階として，単純なネットワークモデルにおいてデータ送信量解析によってアドホックネットワークの基本的な動作を推定し，ネットワークを管理する技術を開発する．この技術を発展させ，将来的に自動車のネットワークにおける攻撃検知手法の開発を行う．

無線ネットワークでは，有線と比較して帯域幅が細く通信リソースが乏しい．また，有線よりも通信が不安定である．無線ネットワークの管理方式は，これらに考慮した方式でなくてはならない．

3. 関連研究

アドホックネットワークでは，従来のトランシーバで用いられていた一方向の簡易的な無線通信から，より高機能化して有線と遜色ない通信が可能になりつつある．それに伴って物理層に対するジャミング攻撃と，上位層に対するサイバー攻撃の連携した攻撃が想定されるなど，攻撃の多様化も進んでおり，攻撃のリスクが増加している．そのため，これらの攻撃に対する施策は急務である．[2]

従来の有線環境におけるネットワーク動作推定方式として，パケットキャプチャを用いたネットワーク動作推定方式が存在する．パケットキャプチャでは，通信回線を流れるパケットをキャプチャしてパケットの中身を表示する[3]．これを解析することによってネットワークを流れるデータの通信量やその変化の推定，障害発生時の原因の推定が可能となる．しかし，無線ネットワークでは通信が不安定であるため，実用に耐える精度でのパケットキャプチャ

† 創価大学大学院 工学研究科
‡1 金沢工業大学 情報フロンティア学部
‡2 金沢工業大学 工学部

が困難である．また，有線と比較して周波数やルーティングプロトコル等各種パラメータが多様であり，対象のネットワークのパラメータへ合わせたキャプチャが必要不可欠になってしまう．以上のような特性があるため，無線ネットワークに適さない推定方式である．

一方，ネットワーク管理の面では，有線環境において Simple Network Management Protocol(以下 SNMP)が用いられている．SNMP は，ネットワーク監視，ネットワーク管理を行うためのプロトコルであり，各端末の状態やリソース，トラフィック等様々な項目の監視が可能となっている[4]．しかし，SNMP はこれらの情報交換のために通信を行うため，ネットワークのトラフィックに負荷をかける．無線ネットワークでは，帯域幅が細く通信リソースが少ない．そのため，SNMP を用いたネットワーク管理は無線ネットワークには適さない管理方式である．

4. 提案

4.1 動作推定フローと推定項目

提案方式では，図 1 に示すように通信を行う際に確実に発せられている各端末の送信電波を利用し，これを観測機によって観測する．観測機では，この送信電波から各端末のデータ送信量を抽出し，1 秒毎にデータ送信量を累積（次項にて詳述）する．観測者は，累積したデータを各端末内での解析や，他端末との比較解析を行うことで，無線ネットワークの動作を推定し，ネットワーク管理を行う．

本方式では，各種情報交換のための通信を用いずに動作推定を行うことや，無線通信の際に確実に発せられている電波を用いて動作推定を行うため，不安定で帯域の細い無線ネットワークの特性に適したネットワーク管理方式となる．

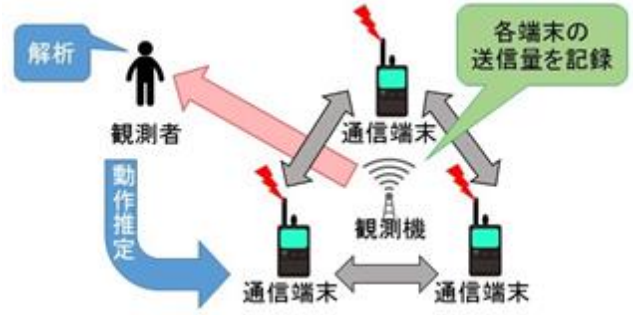

図 1　想定システム図

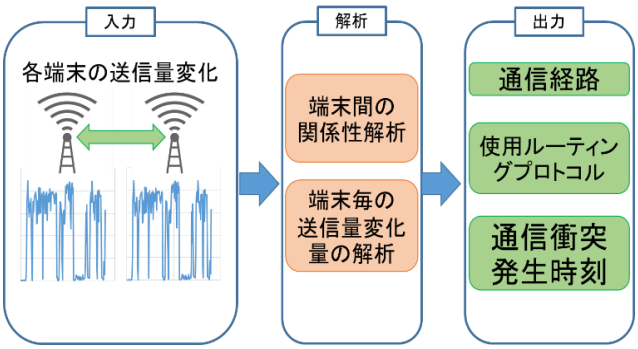

図 2　動作推定フロー

本研究の現段階では，ネットワークの基本的な動作の推定を目的とし，将来的に自動運転のネットワークにも応用できる推定項目として，以下の 3 項目の動作推定を行う．

推定 1 ネットワークで使用されている通信経路の推定
推定 2 使用されているルーティングプロトコルの推定
推定 3 通信衝突を発生時の衝突発生時刻の推定

図 2 のように，ネットワーク内の各端末の送信量変化に対して解析を行うことで，上記 3 項目の動作推定を行う．動作推定を行う際，観測者はネットワークの端末の位置と各端末の番号，そして送信量がどの端末のものであるのかを把握しているものとする．

4.2 累積

各端末の送信量の変化を明確にする目的で，観測機では 1 秒毎にデータ送信量を合計し，これを累積と呼称する．端末番号を N，1 秒毎の秒数を t とした時，累積値 T_{Nt} は以下の通りとなる．

$$T_{Nt} = \sum_{n=t-1}^{t} (P_n)$$

Pn は n 秒におけるパケットサイズ(byte)を示す．

4.3 推定 1 通信経路推定

アドホックネットワークでは，アクセスポイントが存在せず，端末間同士で通信を行う特性上，送信元から宛先までいずれかの端末を経由して情報伝達が行われる．この際，管理者側から通信経路の把握が可能であるということは，セキュリティやネットワーク保全の面からも必要不可欠であると考え，本項目を推定項目とした．

アドホックネットワークでは送信元から宛先までいずれかの端末を中継して通信を行うため，図 3 のように通信を中継する関係にある端末間において，それぞれの送信量変化を比較した際，送信量の変化傾向が一致する．また，これをネットワーク全体に拡大して比較した際，同様に送信元に対してパケットを中継する各端末の送信量の変化傾向が一致する．

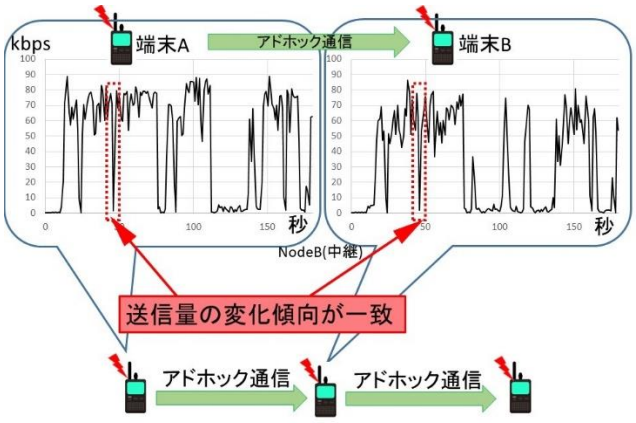

図 3　隣接端末間送信グラフ比較

提案手法では変化傾向の一致度に着目し，それぞれの端末の一致度を比較するため，送信元と各端末の相関係数を計測することとした．相関係数が高い端末は送信元との一致度が高く，中継している端末である可能性が高い．

端末番号 N における相関係数 C_N は以下のようになる．

$$C_N = \frac{\frac{1}{x}\sum_{t=1}^{x}((T_{St}-\overline{T_S})(T_{Nt}-\overline{T_N}))}{\sqrt{\frac{1}{x}\sum_{t=1}^{x}(T_{St}-\overline{T_S})^2}\sqrt{\frac{1}{x}\sum_{t=1}^{x}(T_{Nt}-\overline{T_N})^2}}$$

x は送信量の計測を終了した時間，T_{St} は送信元端末 S における t 秒の累積値を示す．$\overline{T_S}$ は累積値 T_S の平均値を示す．同様に T_{Nt} は端末 T における t 秒の累積を，$\overline{T_N}$ は累積値 T_N の平均値を示す．

中継端末の相関係数 C_N の値が閾値以上であった場合，相関が強く存在すると判断し，端末 N は通信経路に使用されている端末であると判断する．

4.4 推定 2 ルーティングプロトコル推定

現在，アドホックネットワークで使用されるルーティングプロトコルは，図 4 のように通信要求後に経路探索を行い，経路を構築するリアクティブ型と，ネットワーク起動時にあらかじめ経路探索を行い，経路を構築するプロアクティブ型の 2 種のプロトコルに大別される．将来的には，これらを組み合わせたハイブリッド型のプロトコルの利用が想定されており，その際にネットワーク管理者からのプロトコル種別の把握は必要不可欠と考え，本項目を推定項目とした．

上記 2 種のプロトコルの最大の差は，経路探索のタイミングにある．ネットワーク内の通信アプリケーションが 1 つの場合，リアクティブ型では，経路探索を行う送信元端末と，要求毎に返答を行う宛先端末の相関関係が強くなる．それに対し，通信要求と関係なくあらかじめ経路探索を行うプロアクティブ型では，データ送信時に送信元端末が経路探索を行わず通信をすることが可能となっており，送信元端末と宛先端末の相関関係が弱くなる．

提案手法ではこの傾向に着目し，宛先端末 D とした場合，前項の相関係数の式にこれを当てはめ，宛先端末の相関係数 C_D が閾値以上であればリアクティブ型，C_D が閾値未満であればプロアクティブ型であると判断する．

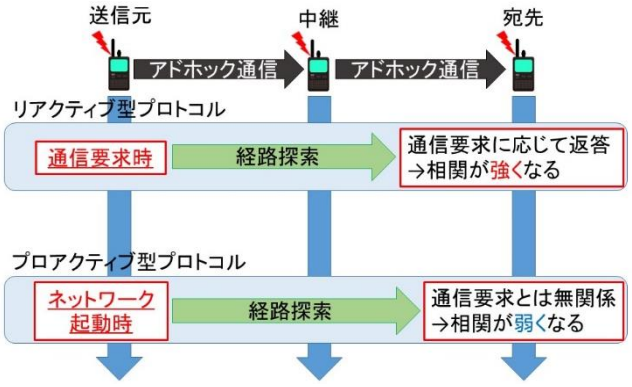

図 4　プロトコルによる経路探索の差異

4.5 推定 3 通信衝突発生時刻推定

ネットワークにおいて通信衝突が発生した際，必要な情報交換が行えない弊害が発生してしまう．これを回避するために観測者から通信衝突発生を把握することは必要不可欠と考え，本項目を推定項目とした．

通信衝突が発生した際，通信が重なり合う端末において，図 5 のように 100 秒以降で送信量変化量の増減が大幅に増加するという結果が予備実験によって得られた．特に一時的に送信量が送信量平均よりも非常に多くなる現象は衝突発生後に顕著に確認された．これは，衝突によってパケットの中継が困難になり一時的に通信が遅延した後，遅延していた分のパケットの送信を一度に行うことによってバースト的にパケットが発せられてしまい，送信量変化の増大が発生してしまうためである．

提案手法では，衝突発生によって送信量変化の増大が増大する傾向に着目し，この増大部分を抽出する手段として偏差値計算を用いた．端末 N において全体の送信量平均に対する 1 秒毎の秒区間 t の偏差値 D_{Nt} は以下の式になる．

$$D_{Nt} = \frac{10(T_{Nt}-\overline{T_N})}{\sqrt{\frac{1}{x}\sum_{t=1}^{x}(T_{Nx}-\overline{T_N})^2}} + 50$$

x は送信量の計測を終了した時間，$\overline{T_N}$ は累積値 T_N の平均値を示す．偏差値 D_{Nt} が閾値以上であった場合，該当端末の該当時刻で衝突が発生しているものと判断する．

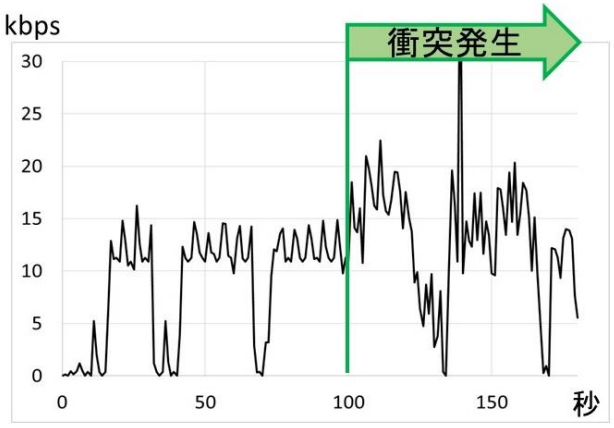

図 5　衝突による送信量変化

5. 実験

5.1 実験手順

本研究では，提案手法の理論的な検証と動作推定の可否の検証を第一に考え，実機環境ではなくネットワークシミュレータ QualNet[5]を実験環境として用いた．このネットワークシミュレータによって生成されたデータを解析することによって提案手法の検証を行う．今回の実験では，各端末から観測機までの電波の劣化は考慮しない．

今回の実験では，表 1 の設定を用いてシミュレーション

Simulation Time	180s
Radio Type	802.11b
Data Rate	2Mbps
Frequency Band	2.4GHz
Application	Constant Bit Rate(CBR)

表 1　実験用パラメータ設定

実験番号	推定項目	プロトコル
実験 1-1	推定 1 通信経路	OLSR
実験 1-2	推定 1 通信経路	AODV
実験 2	推定 2 ルーティングプロトコル	AODV/OLSR
実験 3	推定 3 通信衝突発生時刻	OLSR

表 2　実験項目

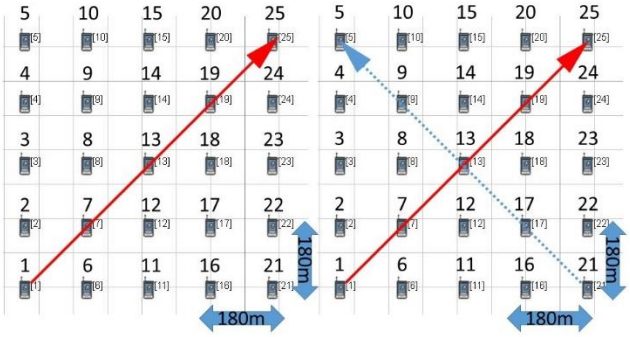

図 6　実験に用いたネットワークトポロジー

番号	送信方向	送信間隔	開始	送信量
App1	端末 1-25	0.1 秒	0 秒	1024Byte
App2	端末 1-25	0.1 秒	0 秒	128Byte
App3	端末 21-5	0.1 秒	100 秒	128Byte

表 3　アプリケーション設定

を行った．各推定項目とその際の実験番号，その際に用いたルーティングプロトコルを表 2 に示す．ルーティングプロトコルは，リアクティブ型の代表的なプロトコルである Ad hoc On-Demand Distance Vector(以下 AODV)[6]，プロアクティブ型の代表的なプロトコルである Optimized Link State Routing INRIA(以下 OLSR)[6]をそれぞれ用いた．

検証で用いたネットワークトポロジーは，図 6 に示す単純で他端末への影響が明瞭に確認できる Grid トポロジーを用いた．端末上の数字は各端末の端末番号を示す．端末間の距離は，縦方向横方向ともに 180m で，この距離は斜め方向に 1 ホップで通信が出来ない距離を実験的に導き出したものである．

よりシンプルな条件での理論検証のため，通信経路推定・ルーティングプロトコル推定では，アプリケーションを左下の端末 1 から右上の端末 25 へ一方向のみの通信とした．図 6 左側の赤矢印がこれに該当し，いずれかの端末を経て端末 1 から端末 25 へ到達する．このアプリケーションの設定は表 3 の App1 を用いた．同様に，通信衝突発生時刻推定では左下の端末 1 から右上の端末 25 へ表 3 の App2 の設定で通信を行い，これに対して 100 秒以降に右下の端末 21 から左上の端末 5 へ表 3 の App3 の通信を衝突させ，検証を行った．これらはそれぞれ図 6 右側の赤矢印，青矢印が該当する．

今回，通信経路推定で使用する相関係数 C_N の閾値は 0.3 を用いた．また，ルーティングプロトコル推定で使用する相関係数 C_D の閾値は 0.3 を用いた．そして，通信衝突発生時刻推定で使用する偏差値 D_{Nt} は 60 を用いた．これらは全て予備実験によって得た値である．

5.2 実験結果

5.2.1 実験 1 通信経路推定

ルーティングプロトコルを OLSR INRIA で実験した際，各端末に対し 4.2 項の累積式 T_{Nt} を適用した後，4.3 項の相関係数 C_N を算出したグラフが以下の図 7 となる．縦軸が相関係数，横軸が端末番号である．相関係数 C_N が 0.3 以上の中継端末は端末 2・端末 7・端末 8・端末 13・端末 14・端末 19・端末 20 となる．次に，図 6 のトポロジー順に送信量変化グラフを並べたものが図 8 である．各端末それぞれ横軸に秒数，縦軸に送信スループットを配置したものである．図 7 と図 8 を比較すると，活発に送信が行われていて，中継をしている各端末の部分と一致した．

同様に，ルーティングプロトコルを AODV に変更して相関係数 C_N を算出したグラフが図 9，図 6 のトポロジー順に送信量変化グラフを並べたものが図 10 である．相関係数 C_N が 0.3 以上の中継端末は，端末 2・端末 6・端末 7 が該

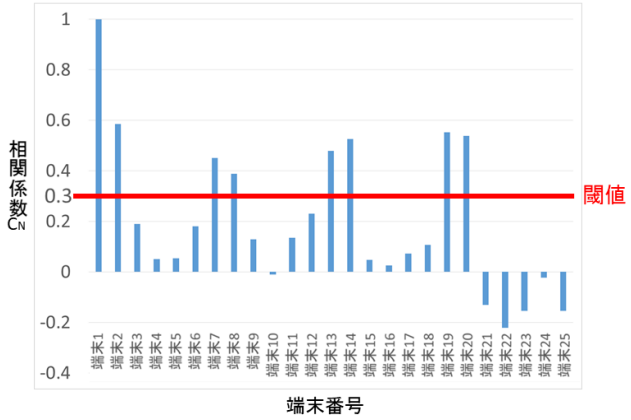

図 7　実験 1-1 OLSR INRIA における相関係数 C_N

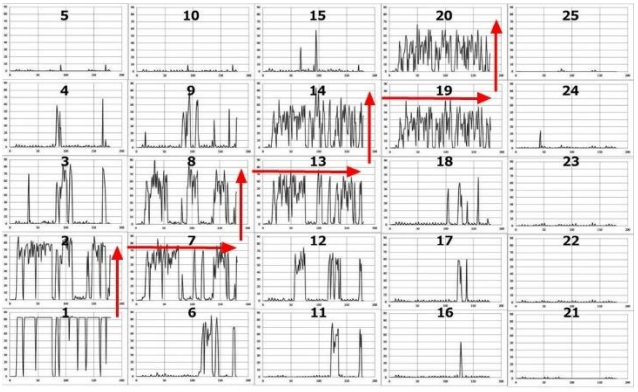

図 8　実験 1-1 OLSR INRIA の各端末の送信量変化

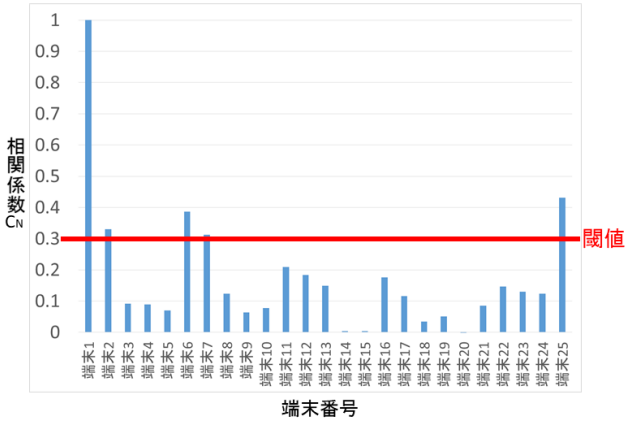

図 9　実験 1-2 AODV における相関係数 C_N

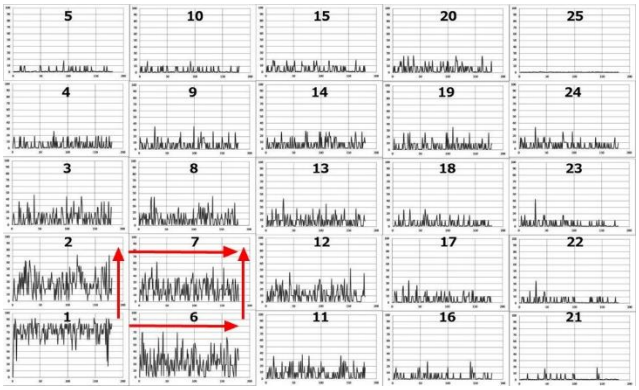

図 10　実験 1-2 AODV の各端末の送信量変化

当する．これらの端末は，発信元である端末 1 の近接端末であり，OLSR INRIA で実験した場合と違い，宛先までの経路を追うことが出来なかった．

5.2.2 実験 2 ルーティングプロトコル推定

次に，通信経路推定のそれぞれの宛先の相関係数を比較したグラフが図 11 となる．今回の実験では，右端の端末 25 が宛先端末に該当する．これらを比較した場合，AODV では相関係数 C_D が 0.3 以上の強い相関を示しているのに対し，OLSR では相関係数 C_D が負の相関を示している．その

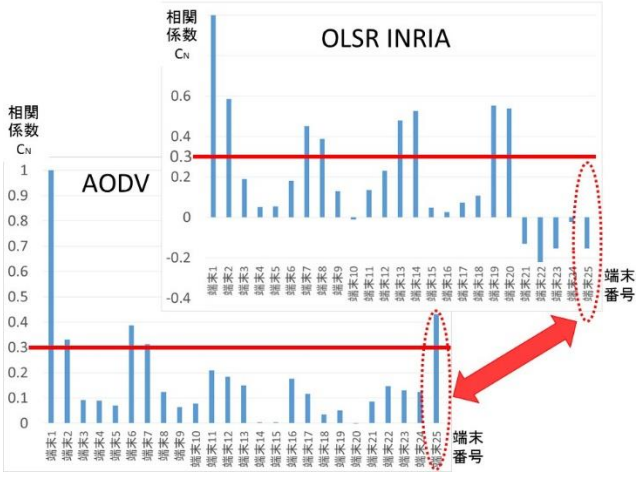

図 11　実験 2 AODV・OLSR の宛先相関係数比較

ため，提案手法によって宛先の相関係数を比較することでルーティングプロトコルの種別を判別することが可能であった．

5.2.3 実験 3 通信衝突発生時刻推定

次に，通信衝突発生時刻推定の実験を行い，各端末をトポロジー順に配置したグラフが図 12 となる．それぞれのグラフは縦軸に送信スループット，横軸に秒数を配置したものとなる．特に影響の大きい中心部の端末 13 について着目し，このグラフを拡大したものが図 13 となる．

この実験では 100 秒以降に衝突が発生しているが，図 13

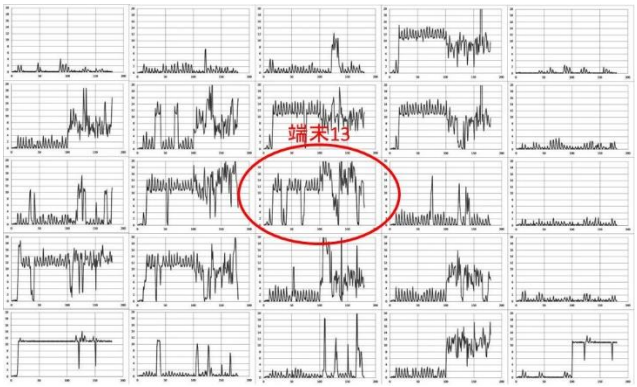

図 12　実験 3 通信衝突実験の各端末の送信変化量

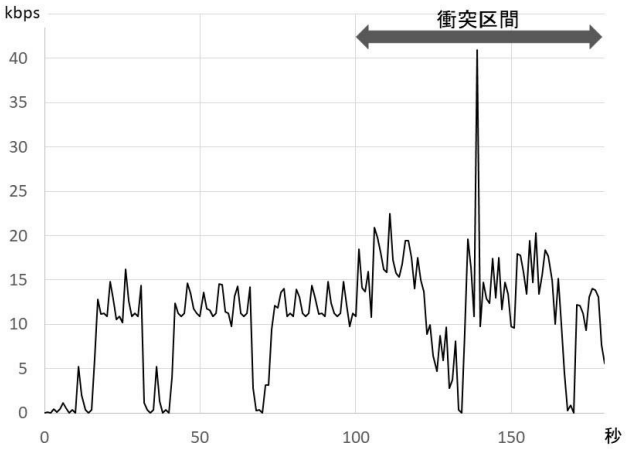

図 13　実験 3 端末 13 送信量変化グラフ

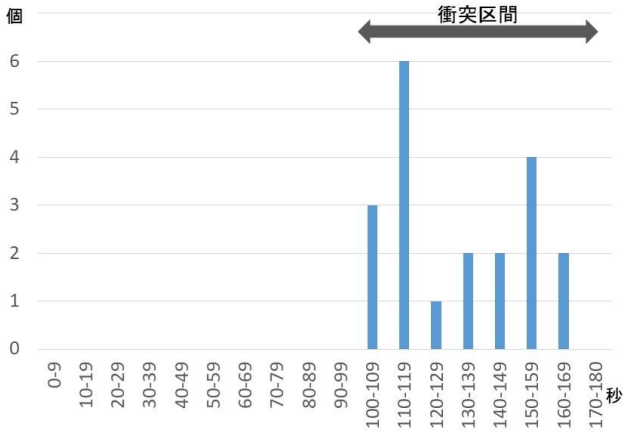

図 14　実験 3 偏差値 D_N60 以上出現個数

ではその衝突によって送信スループットが乱高下していることが確認できる．この中心部の端末に対し，4.5 項の偏差値 D_{Nt} を算出し，10 秒毎に偏差値 60 以上の秒区間が発生した個数を並べたグラフが図 14 となる．偏差値 60 以上が出現した場所は衝突発生後の 100 秒以降となっており，提案手法により通信衝突の発生を推定することが可能であった．

5.3 考察

今回の実験により，データ送信量解析によってネットワークの動作推定が可能であることが確認できた．

通信経路推定に関して，OLSR INRIA で実験した際には，提案手法によって通信に使用されている主経路を問題なく抽出することが出来た．しかし，AODV で実験した際には送信元である端末 1 の隣接端末のみしか抽出することが出来なかった．これは，ルーティングプロトコルの特性上通信が拡散してしまい，送信元との関係性が宛先端末に近づくにつれて希薄になってしまっているためだと予想される．今後は，この点を克服できるよう，今回使用した相関係数 C_N の閾値を見直すことや，送信元だけでなく中継端末とその他の中継端末の相関係数を比較する等，手法を改良していく必要がある．

ルーティングプロトコル推定に関して，今回の実験では提案手法によってプロトコルを推定することが可能であることが確認できた．今後は，より精度を向上させるために閾値についての再検討を進めていく．

通信衝突発生時刻推定では，今回の実験では提案手法を用いて通信衝突の発生区間を推定することが可能であった．しかし，衝突発生区間である 170 秒から 180 秒の間では該当偏差値が出現せず，通信衝突が発生していない時刻と同等の反応を示してしまっている．今後は，閾値の精度を向上させて誤検知や検知抜けの無いように改良する．

6. おわりに

本稿では，無線環境に適したネットワーク管理方式としてデータ送信量解析を用いたネットワーク動作推定手法を提案した．また，これらの手法の理論検証のための実験設定の考案を行い，ネットワークシミュレータを用いた検証によってネットワークの基本動作である無線アドホックネットワークにおける通信経路推定，ルーティングプロトコル推定，通信衝突発生時刻推定の 3 項目の推定について達成をすることが出来た．しかし，全体的に検証回数が少なく，結果の信頼性が不十分であるため，今後は検証回数を増加させてより信頼性のある推定手法にしていく必要がある．また，今回は理論検証を目的に，実環境で発生する各端末から観測機への電波の劣化を考慮しない理想的な環境で実験を行ったため，今後は実環境での電波の劣化を考慮して検証を進めていく必要がある．そして，今回の実験によってデータ送信量解析によるネットワーク動作推定が可能であることを検証できたため，これらの手法を発展させ，自動車のネットワークにおける攻撃検知を開発する．

参考文献

[1] 松井進：アドホックネットワークの実用化に向けた課題と実用化動向，日本信頼性学会誌 第 34 巻，pp.532-539，2012.
[2] Kanika Grover：Jamming and anti-jamming techniques in wireless networks: a survey，International Journal of Ad Hoc and Ubiquitous Computing vol.17 Issue4，pp197-215，2014.
[3] 竹下恵：パケットキャプチャ無線 LAN 編，リックテレコム，2016
[4] ダグラス・R.マウロ：入門 SNMP，O’Reilly Japan，2002
[5] QualNet Network Simulator Software SCALABLE Networks (https://web.scalable-networks.com/qualnet-network-simulator-software)
[6] 小菅昌克 他：アドホックネットワークが開く新しい世界(前編)，情報処理学会誌 44 巻第 10 号， pp1052-1055，2003.