

L_016

映像ストリーム収集のためのマルチホップ無線ネットワーク におけるフレーム衝突検出に基づく通信スケジュール制御法

A Communication Scheduling Method based on Frame Collision Detection
in Multi-hop Wireless Network for Video Stream Aggregation

枯成光樹 三津橋 晃文 野田 潤 小西 勇介 中尾 敏康 田口 大悟
Teruki SUKENARI Akitake MITSUHASHI Jun NODA Yusuke KONISHI Toshiyasu NAKAO Daigo TAGUCHI

NEC インターネットシステム研究所
Internet Systems Research Laboratories, NEC Corporation.

1. はじめに

近年、空港/港湾/地下鉄における犯罪・災害・テロ活動の増大を背景として、カメラによる広域監視システムが注目されている。しかし、従来の CCTV(Closed-Circuit-Television)カメラや IP ネットワークカメラを広い範囲に配置した場合、通信インフラの敷設コストが問題となった。我々は通信インフラを必要とせず、ノードのみでネットワークを構築できるマルチホップ無線ネットワークを用いた広域監視システム「ユビキタス・カメラネットワーク」の研究開発に取り組んでいる。

無線通信ネットワークにおいて、互いにキャリアセンスできない複数のノードが、同時に映像ストリームなどのデータ送信を実行した場合、データフレーム衝突(以下、フレーム衝突)が発生する。これは、「隠れ端末問題(HTP: Hidden Terminal Problem)」と呼ばれ、スループットといった無線通信性能を著しく劣化させる^[1]。

本稿では、隠れ端末が存在するマルチホップ無線ネットワークにおける無線通信性能と無線特性値(SN 比, CRC エラーフレーム率, MAC 再送フレーム率)の関係を実機により検証する。また、検証結果に基づき、ノードが計測する無線特性値の変化から、フレーム衝突を検出し、コマンドパケットを用いて通信スケジュールを制御することでフレーム衝突を回避する方式を提案し、その評価実験結果について述べる。

2. ユビキタス・カメラネットワーク

ユビキタス・カメラネットワーク(図 1)は、クラスタ型ネットワーク・トポロジ(以下、クラスタ型 NWT)およびチェーン型ネットワーク・トポロジ(以下、チェーン型 NWT)の組合せによって構成される。広域監視を実現するために、無線到達距離と同じ間隔でノードが配置されるユビキタス・カメラネットワークでは、クラスタ型 NWT およびチェーン型 NWT 上で 2 ホップ以上離れて配置されたノード同士はキャリアセンスできない。このため、無線 LAN などの無線通信ネットワークと比較して、隠れ端末問題が多く発生する。

ユビキタス・カメラネットワークでは、カメラセンサおよび無線通信機器を搭載したノードが、撮影した映像ストリームを複数のノードを経由するマルチホップ無線通信により、中央モニタリングサーバに送信する。「幹」と呼ぶ通信経路上に配置されたノードは、幹から分離した「枝」上に自身が管理するノードを保有できる。幹上に配置されたノードをクラスタヘッドと呼び、枝上に配置されたノード

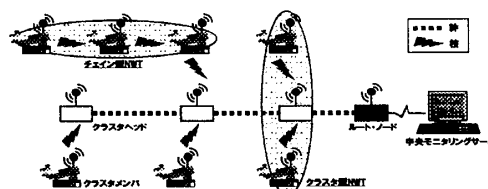
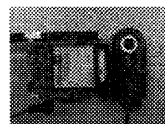


図 1: ユビキタス・カメラネットワーク



(L*W*H) [mm]: 69.5*80.0*51.5

ノード	Linux Machine (Intrinsyc) ・ Intel PXA255 400MHz ・ SDRAM 64[MByte]
カメラセンサ	CCD, USB I/F (Logicool)
無線通信機器	IEEE802.11b CF (symbol)

図 2: ノード 諸元

ドをクラスタメンバと呼ぶ。クラスタメンバは、中央モニタリングサーバから映像ストリームを要求する指令信号を受けた後、映像ストリームをマルチホップ送信する。この時、隠れ端末が存在すると、中央モニタリングサーバで監視する映像ストリームの品質低下、フレーム落ちおよび伝送遅延が発生し、適切な監視ができない。

フレーム衝突を回避する MAC(Media Access Control)プロトコルとして、RTS/CTS 制御がある。しかし、マルチホップ無線ネットワークでは、フレーム衝突を完全に回避できないことが知られている^[1]。参考文献[2]では、ノードが計測する SN 比に基づき、フレーム衝突を検出する方法が提案されている。しかし、互いにキャリアセンスできる状態(以下、非隠れ端末状態)にあっても、SN 比が大きく変動することがあり、SN 比だけでは、隠れ端末によるフレーム衝突を高精度に検出できない。また、CRC エラーフレーム率、MAC 再送フレーム率を利用するためには、ノードが継続的に無線特性値を計算しなければならずノードの処理負荷が大きくなる。そこで本稿では、非隠れ端末状態において計測した無線特性値を基準に、SN 比が低下した場合だけ、さらに CRC エラーフレーム率および MAC 再送フレーム率を計測するように構成し、低リソースのノードでも高精度に、隠れ端末によるフレーム衝突を検出できる方法を提案する。さらには、フレーム衝突を検出したノードが、直接通信可能なノードに対して、送信許可時間を指定するコマンドパケットを送信することで、フレーム衝突を回避する通信スケジュール制御法を提案する。また、隠れ端末が存在するクラスタ型 NWT およびチェーン型 NWT において、CSMA/CA 制御と比較して良好な無線通信性能を得られることを述べる。

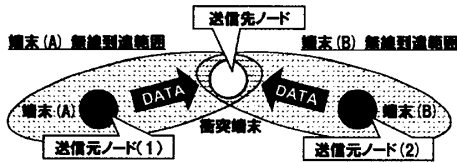


図 3: クラスタ型 NWT

表 1: MPEG ストリーム 諸元

NWT	BitRate [kbps]	Resolution [pixel]	FrameRate [fps]
Cluster	1800	VGA (640*480)	30
Chain	1200	VGA (640*480)	30

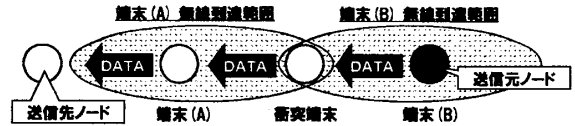


図 4: チェイン型 NWT

3. 無線通信性能と無線特性値の関係

隠れ端末が存在するクラスタ型 NWT およびチェイン型 NWT における無線通信性能と無線特性値の関係を検証するために、小型 Linux マシンをノードとして使用するユビキタス・カメラネットワークを構築した(図 2)。ノード上では、オープンソースの動画配信ソフトウェア VLC-0.8.4(Video LAN Client)^[3]が稼動しており、MPEG-4 形式で符号化された映像ストリームを、UDP によって送受信できる。無線通信には IEEE802.11b を使用し、5200[kbps]の無線通信帯域が得られることを確認した。

実験は、隠れ端末が存在するクラスタ型 NWT(図 3)およびチェイン型 NWT(図 4)で行った。いずれの NWT においても送信元ノードが送信するデータは、他のノードを経由して送信先ノードに到達する。

CSMA/CA 制御では、各ノードがデータ送信を開始する場合、事前にキャリアセンスを行い、無線チャネルの使用状況を確認する。他のノードの送信信号が存在する間は送信を待機し、フレーム衝突を回避する。しかし、端末(A)と端末(B)は、互いにキャリアセンスできない状況にあり、CSMA/CA 制御が正常に動作せず衝突端末上でフレーム衝突が発生する。

実験では、表 1 に示す MPEG ストリームを使用した。これは送信元ノードおよび送信先ノードを含む全ノードが互いにキャリアセンスできる非隠れ端末状態において、全無線通信帯域(5200[kbps])の 70% (3600[kbps])を使用するように、MPEG ストリームのビットレートを調整したものである。

送信先ノードでは、受信した MPEG パケットのサイズを 500[msec]毎に集計し、スループットの時間変化を計算する。一方で、衝突端末は、受信信号の無線特性値である「SN 比[dB], CRC エラーフレーム率, MAC 再送フレーム率」を計測する。CRC エラーフレーム率は、FCS(Frame Check Sequence)フィールドに基づき、ビットエラーが存在すると判断され、廃棄されたデータフレームの割合である。MAC

表 2: 無線通信性能と無線特性値 (クラスタ型 NWT)

Status	SNR [dB]	CRC Error Frame	MAC Retry Frame	Throughput avg. [kbps]
A only	39.1	0.004	0.044	1840.2
B only	31.7	0.007	0.056	1845.5
w/o HTP	29.0	0.051	0.101	1749.8 / 1761.1
w HTP	24.1	0.225	0.301	1084.6 / 216.1

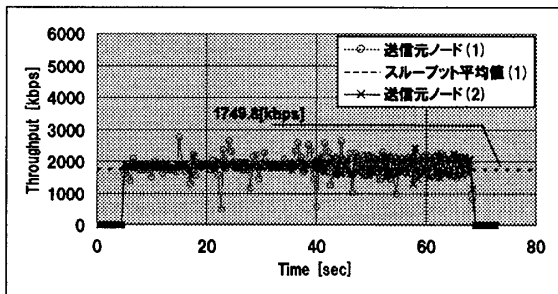


図 5: スループット 時間変化 (クラスタ型 NWT w/o HTP)

表 3: 無線通信性能と無線特性値 (チェイン型 NWT)

Status	SNR [dB]	CRC Error Frame	MAC Retry Frame	Throughput avg. [kbps]
A only	34.0	0.026	0.022	1250.4
B only	36.2	0.006	0.082	1244.9
w/o HTP	33.5	0.128	0.224	1196.8
w HTP	32.1	0.249	0.374	506.6

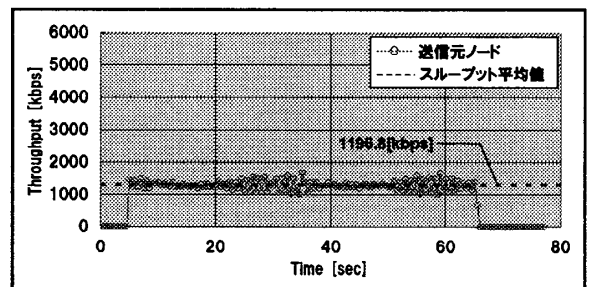


図 6: スループット 時間変化 (チェイン型 NWT w/o HTP)

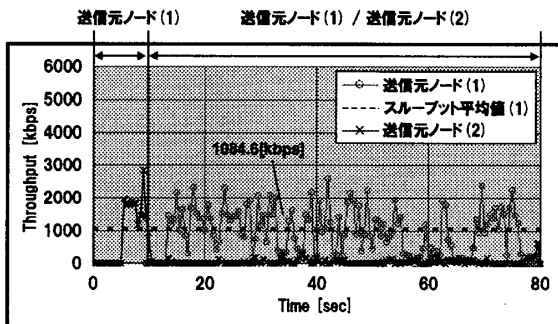


図 7: スループット 時間変化 (クラスタ型 NWT w HTP)

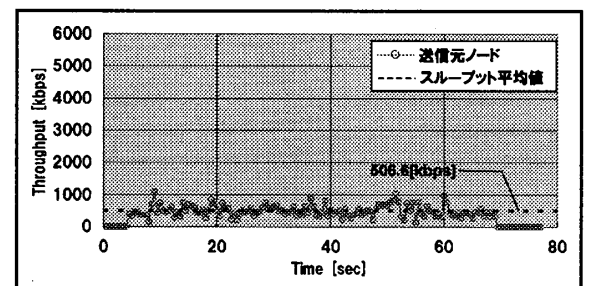


図 8: スループット 時間変化 (チェイン型 NWT w HTP)

再送フレーム率は、フレーム制御フィールドで Retry ビットが有効となっているデータフレームの割合である。図 5, 図 6, および図 7, 図 8 に、非隠れ端末状態および隠れ端末状態で計測したスループットの時間変化を示す。

■ クラスタ型 NWT

クラスタ型 NWT において計測した無線特性値を表 2 に示す。表 2 において、端末(A)が単独で MPEG ストリームを送信した場合に計測された無線特性値を「端末(A)単独送信 (A only)」, 同様に端末(B)のみが送信した場合を「端末(B)単独送信 (B only)」, 非隠れ端末状態で計測された値を「非隠れ端末状態 (w/o HTP)」, さらに、隠れ端末状態での計測値を「隠れ端末状態(w HTP)」として記載している。

隠れ端末状態では、8[sec]以降で 2 台の送信元ノードが同時に MPEG ストリームを送信するため、端末(B)のスループットが著しく低下している(図 7)。端末(A)および端末(B)の単独送信時の SN 比の条件を変更し実験を行った。その結果、環境による SN 比の変動があった場合でも、両者の SN 比に 6[dB]の差異が存在すると、SN 比の良好なノードが無線チャンネルを占有する傾向を確認した。この時、無線チャンネルを占有した端末(A)でも、フレーム衝突を原因として、CRC エラーフレーム率および MAC 再送フレーム率が悪化しており、スループット平均値は、1084.6[kbps]まで低下している。

■ チェイン型 NWT

クラスタ型 NWT と同様に、無線通信特性値は、「単独送信→非隠れ端末状態→隠れ端末状態」の順に悪化している。その結果、隠れ端末状態では、506.6[kbps]までスループット平均値が低下している。図 9 は、チェイン型 NWT において、60[sec]期間に 1[sec]毎に計測した SN 比の時系列データである。複数のノードが同時通信する場合、非隠れ端末状態および隠れ端末状態に共通して、SN 比が大きく変動している。

以上より、次の 2 点が検証できた。

- ・ フレーム衝突が発生すると、無線特性値が悪化し、その結果、パケット損失を原因として無線通信性能が劣化する。
- ・ 複数のノードが同時通信する場合、SN 比が大きく変動する。そのため SN 比だけで隠れ端末によるフレーム衝突を検出することは困難である。

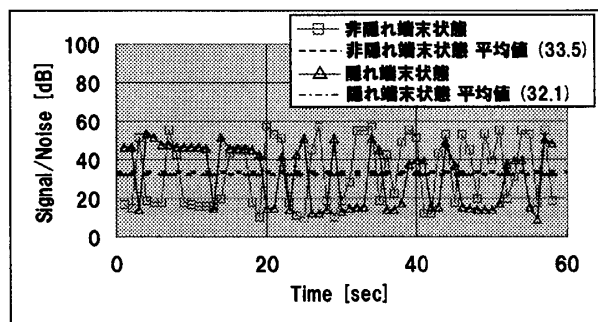


図 9 : SN 比 時間変化

4. フレーム衝突回避方式

4.1 提案方式

前章で説明した検証結果から、我々はフレーム衝突検出法と通信スケジュール制御法から構成されるフレーム衝突回避方式を提案する。

フレーム衝突検出では、単独送信および非隠れ端末状態で計測した SN 比, CRC エラーフレーム率, MAC 再送フレーム率を電波特性基準値として使用する。基準 SN 比に対して、ノードが計測した SN 比が下回った場合だけ、CRC エラーフレーム率および MAC 再送フレーム率の計測を開始する。そして、計測した CRC エラーフレーム率および MAC 再送フレーム率から算出する評価関数値が、基準 CRC エラーフレーム率および基準 MAC 再送フレーム率から算出する評価関数値よりも悪化した場合、フレーム衝突が発生したと判断する。これにより、低リソースのノードが、継続的に CRC エラーフレーム率および MAC 再送フレーム率を計算する処理負荷を低減でき、SN 比が大きく変動する環境でも、高精度に隠れ端末によるフレーム衝突を検出できる。

通信スケジュール制御は、フレーム衝突が検出された場合だけ実行される。通信スケジュール制御では、フレーム衝突を検出したノードが、送信許可時間を指定したコマンドパケットを直接通信可能なノードに送信し、コマンドパケットを受信したノードは指定された送信許可時間だけ無線チャンネルを使用する。通信スケジュール制御は、アプリケーション層で実装され、既存の CSMA/CA 制御を改造する必要がないことを特徴とし、クラスタ型 NWT およびチェイン型 NWT に共通して適用できる。以上より、フレーム衝突を原因とした無線通信性能の劣化を防止する。

4.2 フレーム衝突検出法

衝突端末は、単位ステップ時間 Δt 毎に SN 比の平均値 $\overline{SN}(s)$ (s は表 2 の「Status」に相当)を計測する。 $\overline{SN}(s)$, および単独送信時に計測した基準 SN 比 $\overline{SN}(A \text{ only})$ および $\overline{SN}(B \text{ only})$ が, 【Condition.1】を満たせば、CRC エラーフレーム率, MAC 再送フレーム率の計測を開始する。

【Condition.1】

$$\text{if } \overline{SN}(s) < \min(\overline{SN}(A \text{ only}), \overline{SN}(B \text{ only}))$$

次に、衝突端末は、次の単位ステップ時間 Δt で計測する CRC エラーフレーム率 $Pe(s)$ および MAC 再送フレーム率 $Pr(s)$ を用いて【Condition.2】を評価する。評価関数 $G(s1, s2)$ は、CRC エラーフレーム率 Pe および MAC 再送フレーム率 Pr を用いたユークリッド距離で与えられる。計測した $Pe(s)$, $Pr(s)$ および予め計測した無線特性基準値 $Pe(w/o \text{ HTP})$, $Pr(w/o \text{ HTP})$, $Pe(A \text{ only})$, $Pr(A \text{ only})$, $Pe(B \text{ only})$, $Pr(B \text{ only})$ が, 【Condition.2】を満たせば、隠れ端末によるフレーム衝突が発生したと判断する。

【Condition.2】

$$\text{if } \max(G(s, A \text{ only}), G(s, B \text{ only})) > \min(G(w/o \text{ HTP}, A \text{ only}), G(w/o \text{ HTP}, B \text{ only}))$$

$$G(s1, s2) := \sqrt{\alpha(Pe(s1) - Pe(s2))^2 + \beta(Pr(s1) - Pr(s2))^2}$$

4.3 通信スケジュール制御法

チェーン型 NWT における通信スケジュール制御フローを図 10 に示す。コマンドパケットは TCP 通信によって送信する。衝突端末は、送信許可時間情報「Stream Period」を含むコマンドパケットを、直接通信可能なノード(端末(A)および端末(B))に対して送信する。コマンドパケットを受信したノードは、コマンドパケットで指定された Stream Period[msec]間だけ MPEG ストリーム送信を実行し、その後、次のコマンドパケットを受信するまで MPEG ストリーム送信を待機する。

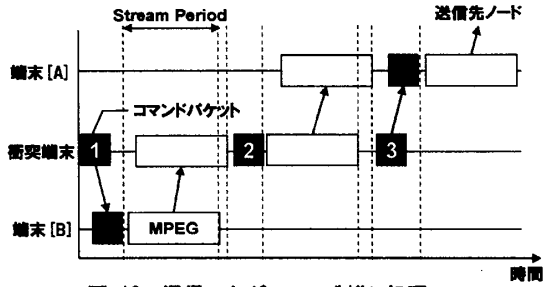


図 10: 通信スケジュール制御 処理フロー

5. 評価実験

提案手法の有効性を確認するための評価実験結果を説明する。

フレーム衝突検出法を非隠れ端末状態に適用し、誤検出率を計測することで性能評価を行った。単位ステップ時間 $\Delta t=3[\text{sec}]$ として、SN 比のみを用いた場合(【Condition.1】)のフレーム衝突検出では、誤検出率が 36%であった。それに対して、SN 比、および CRC エラーフレーム率、MAC 再送フレーム率を用いた場合(【Condition.1】および【Condition.2】)では、誤検出率を 8%に抑えられることを確認した。

通信スケジュール制御法による無線通信性能の改善効果は、隠れ端末が存在するクラスタ型 NWT およびチェーン型 NWT に提案方式を適用することで求めた。具体的には、衝突端末から端末(A)および端末(B)に対して、図 11 に示すスケジュールに従いコマンドパケットを送信する。この時、コマンドパケット内で指定する送信許可時間情報「Stream Period」は、送信元ノードへの伝送遅延が、1[sec]以内になるよう設定した。通信スケジュール制御を適用した場合(Scheduling)と、適用しない場合(CSMA/CA)とで、計測したスループットの時間変化(図 12, 図 13)および無線特性値(表 4)を示す。送信元ノードからの MPEG ストリーム送信が、スケジュールに従って時分割で実行されていることが確認できる。これにより、クラスタ型 NWT, チェーン型 NWT それぞれで無線特性値が改善され、クラスタ型 NWT で 37.6%, チェーン型 NWT で 45.6% の無線通信性能の向上が得られた。

6. おわりに

本稿では、フレーム衝突検出法と通信スケジュール制御法から構成されるフレーム衝突回避方式を提案した。提案方式によって、SN 比が大きく変動する環境でも、高精度に隠れ端末によるフレーム衝突を検出でき、CSMA/CA 制

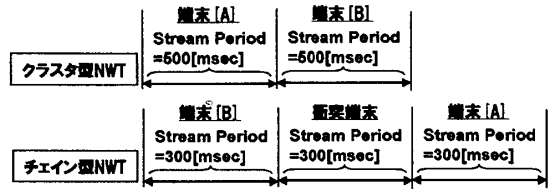


図 11: 通信スケジュール制御 評価実験

表 4: 無線通信性能と無線特性値

Status	SNR [dB]	CRC Error Frame	MAC Retry Frame	Throughput avg. [kbps]
CSMAC/CA				
w HTP (Cluster)	24.1	0.225	0.301	1084.6 / 216.1
w HTP (Chain)	32.1	0.249	0.374	506.6
Scheduling				
w HTP (Cluster)	33.3	0.066	0.224	1762.2 / 1776.5
w HTP (Chain)	34.8	0.102	0.212	1054.2

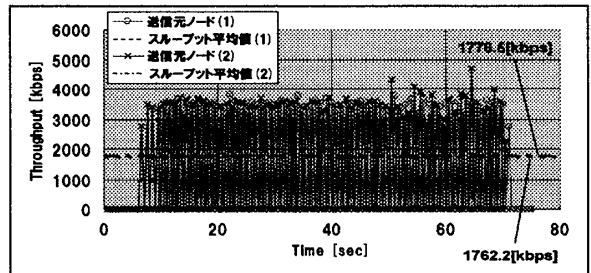


図 12: スループット 時間変化 (クラスタ型 NWT)

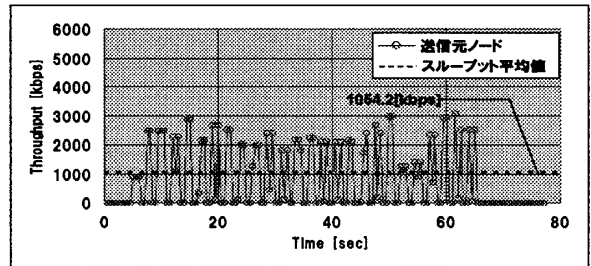


図 13: スループット 時間変化 (チェーン型 NWT)

御と比較して、無得通信性能の劣化を防止できることを実験により確認した。今後は、無線通信性能と無線特性値の相関性に関する理論解析を課題とする。

謝辞

本研究は、独立行政法人 新エネルギー・産業技術総合開発機構(NEDO)の助成事業「半導体アプリケーションチッププロジェクト」の一環として支援を受けて行われたものです。

参考文献

[1] Y. Chen, Q-A. Zeng, and D. P. Agrawal: "Performance of MAC Protocol in Ad Hoc Networks", In Proc. of Int'l Conf. on Communication Networks and Distributed Systems Modeling and Simulation, pp.55-61 (Jan. 2003).
 [2] 間博人, 田村陽介, 徳田英幸: "SN 比を考慮した無線スケジューリング方式", 第 61 回情処全大論文集, Vol.61, No.3, pp.467-468 (2000-10).
 [3] VideoLan.org, URL: <http://www.videolan.org/>.