アドホックネットワークを用いた駐車場における 防犯カメラシステムの提案と評価*

植村 渉[†]・村田 正[†]

A Proposal and Evaluation of Security Camera System at a Car Park in an Ad-Hoc Network*

Wataru UEMURA[†] and Masashi MURATA[†]

In recent year, ad-hoc network technology has gained attention, which consists of not access points and base stations but of wireless nodes. In this network, it is difficult to maintain the whole data flow because of the absence of access points as the network administrator when nodes share the data. This paper proposes the security camera system which has only nodes sharing the taken pictures and has the robustness against the data destroying. The sender node cannot know whether packets are received or not by neighboring nodes in broadcasting because of a unidirectional communication. So in our proposed method, the sender node selects the receiver node from neighboring nodes, and they communicate with each other. On the other hand, neighboring nodes listen to packets between the sender node and the receiver node. After that, this method guarantees nodes of more than 1 which receive a data in broadcasting. We construct the security camera system using wireless nodes with the IEEE 802.15.4 specification and show the performance for security. At last, using the simulator we show the efficiency in the large environment, and conclude this paper.

1. はじめに

2010 年の警察白書によると, 駐車車両内の物品の窃盗発生件数は 143,863 件である [3]. さらに, 車内の物品だけでなく, 自動車そのものを盗む窃盗も発生しており, 自動車は 25,815 件, オートバイは 82,116 件が認知されている. これらの窃盗に対して, さまざまな防犯監視システムが提案されているが, ここでは防犯カメラシステムに注目する.

駐車場の防犯カメラシステムはいくつかの項目で分類できるが, 重要な項目として設置目的が挙げられる. 犯罪の発見のために設置する場合と, 犯罪証拠の確保のために設置する場合である. 前者はリアルタイムに情報を得る必要があり, 監視カメラシステムとよべる. 後者は犯罪が起こった後に証拠を確保することが目標である.

リアルタイムに監視するカメラシステムでは, 監視センタにて監視者がカメラ映像を見て, 危険性の判断をすることが多く, いかに監視者が簡単に異常を発見できる

かが重要である [9]. また, 一つのカメラですべてのエリアを監視するのは不可能であり, 複数のカメラを使って監視すべきである. この条件は, 証拠確保が目的の場合も同様である. これら撮影したカメラ画像は, 監視センタへと送信されるが, 一極集中型であるため, 一般に経路が 1 箇所に限ることが多い. とくに無線ネットワークを構築した場合は, データは基地局を経由するため, データが集中している部分にトラブルが発生すると, 監視情報を消失する可能性がある.

証拠確保のためのカメラシステムの場合, プライバシーの確保が必要になる. たとえば, 複数の端末が撮影した写真から, 個人の行動の流れを得ることがないように注意する必要がある [10].

本論文では, これらの動向を踏まえ, アドホックネットワークの技術を用いた無線端末のみで構築する新しい防犯カメラシステムを提案する. 通常無線ネットワークでは, 無線端末はアクセスポイントのような基地局を経由して通信を行う. そのため基地局のないエリアでは無線端末はネットワークに接続できない. この問題に対して, アドホックネットワークの技術が注目されている [1,2]. 通常, 無線端末は, 自分の電波が届く範囲内の端末にし

* 原稿受付 2011 年 3 月 23 日

[†] 龍谷大学 理工学部 電子情報学科 Faculty of Science and Technology, Ryukoku University; Seta 1-5, Otsu city, Shiga 520-2194, JAPAN

Key Words: ad-hoc network, security camera system, IEEE802.15.4.

接端末とよぶ。アドホックネットワークでは、電波の届かない離れた端末に対しては、間の端末がパケットを中継し、それを繰り返すことで、通信経路を確立する。このとき、どの端末が中継するかを決めるために経路構築の機能が重要となる。経路構築においてそれぞれの端末は対等であり、基地局と端末という親子関係は存在しない。すべての端末が基地局の役割を担うともいえる。そのため端末の追加や離脱にも適応でき、またネットワークトラフィックがある基地局に集中することもない。

提案するシステムでは、駐車場をリアルタイムに監視するのではなく、犯罪が起こった後に証拠を確保することを目的とする。撮影した写真の画像を管理するセンタを置かず、各無線端末がお互いの撮影した写真を共有しあう無線ネットワークを構築する。写真データを集中管理しないため、データの破壊が困難になる。さらに、センタまでの通信経路を確立しなくてもよいメリットがある。そのため工事現場や災害現場などのように一時的に防犯システムが必要となる場面に有効である。また、無線端末を車内や車外の色々な場所に設置できるため、防犯力を高めるために目立つ場所への設置や、逆に死角を見つけにくくするために目立たない場所に設置して、どこから監視されているのかわからないようにもできる。また、駐車場の敷地内に設置した無線端末により、ネットワークの最低限の維持と画像の確保をより確実なものとする。さらにその端末を人の手の届かない壁の中などに設置することで、ネットワーク内の端末の完全な破壊を防ぎ、犯罪情報の確保が可能となる。

1台の基地局で無線ネットワークを構築する場合、設置が手軽であるが駐車場全エリアをカバーする必要がある。広い駐車場や屋内駐車場では適用が困難である。カバーできるエリアを広げるには、複数の基地局を用いることになるが、それぞれの基地局間をつなぐ必要がある。基地局間を有線でつなぐ場合は、ケーブルの敷設のコストがかかるため、基地局間も無線でつなぐ方が望ましい。これに対して本提案システムは、全端末が無線ネットワークでつながるため、これらの煩わしさが無い。なお、盗難や車上荒らしといった犯罪が起こった時には、当該の車両だけでなく他の車両の撮影画像を確保する必要があるため、駐車場の種類としては、利用者が特定できる駐車場である必要がある。不特定多数の人間が利用するショッピングセンタなどの駐車場は対象としていない。具体的には、月極駐車場や職場の駐車場、マンションの駐車場、そして工事現場や災害現場での駐車場や作業場を想定しており、この場合、駐車台数は多くても2~3百台程度までと考えられる。

アドホックネットワークを車同士の通信に用いる方法がすでに研究されている。車の安全な運行を目的としたVSC(Vehicle Safety Communications)[11,13]では、P2P(Peer To Peer)ネットワークが一般的であり、移動体のグループをどのように作るかが課題である[12]。そ

れに対して本論文は駐車場における防犯カメラシステムを議論するため、動いている車はほとんどなく、端末間のリンクの変化は緩やかである。そのためグループを作らず、隣接端末への一斉配信を繰り返すだけで、十分な情報の共有が可能であると考えられる。この有効性に関しては、3.にて実験とシミュレータにて確認する。

複数の車で構築したネットワーク内での情報の共有には、BitTorrent[16]に基づいたFSP(File Swarming Protocol)を使ったコンテンツ共有方法が提案されている[14,15]。FSPでは、ファイルをダウンロードすると同時に他の端末にもアップロードすることで、ファイルを効率よく分散させる。本論文の実験で構築したシステムでは、8ビットマイコンを用いたため複雑なプロトコルの利用は難しく、また搭載メモリが少ないため複数の端末と同時に通信を行うのは困難である。そのため、ファイルの共有には周辺端末への一斉配信を繰り返すフラッディングを採用した。このとき離れた端末と直接通信する必要がないので、ルーティングプロトコル[5,6]は不要である。

以下、2.では、新しい防犯カメラシステムを提案し、その特徴について議論する。3.にて、実機を用いた実験とシミュレーションによる性能評価を通して、システムの有効性を検証する。最後に4.にて、本論文をまとめる。

2. 新しい防犯カメラシステムの提案

この節では、端末のみで構成する新しい防犯カメラシステムを提案する。このシステムでは、2種類の無線端末を用意する。カメラのついている無線端末(以後、カメラあり端末と表記)と、カメラのついていない無線端末(以後、カメラなし端末と表記)である。車の中や外にカメラあり端末を設置し、カメラなし端末は駐車場の壁や柱などに設置する。これら2種類の端末は、ネットワークを構成するうえでは性能に違いがなくてもよく、基地局を用いる場合のように親子関係を意識する必要はない。このシステムでは、これらの端末で構成された無線ネットワークを用いて、撮影した写真を共有する。以下、2.1では端末の動作について説明する。また、2.2ではこのシステムにより生まれる犯罪抑止力を2点挙げ、システムの有効性を議論する。そして、2.3にてプライバシーの保護について確認し、最後に2.4にてセンサネットワークを用いた監視カメラシステムとの比較により、端末の移動性に対する優位性を議論する。

2.1 カメラあり端末とカメラなし端末の動き

本節では、システムで用いる2種類の無線端末の動作について説明する。カメラあり端末は車の中や外に設置し、カメラなし端末は駐車場の敷地に設置するため、それら端末で構成される無線ネットワークはFig.1のような接続となる。2種類の端末はカメラの有無の違いだけで、それ以外の無線通信機能や画像保管能力などは簡単

Fig. 1 Location of cars and nodes at a car park and its wireless network area

のため同等であると想定している．ただし実際には偏りがあっても問題ない．とくにカメラなし端末は、敷地の電源からの電力が期待できるため、通信範囲を広くすることも可能である．

システムのフローチャートを Fig. 2 に示す．メインループでは、他端末からの写真の送信の有無の確認や、行動選択の備えた待機を行う．ここで行動選択とは、写真の撮影や配信のことで、その行動を開始するきっかけは端末の性能によっていろいろな方法が考えられる．撮影した複数の写真の時間的差分を取り、変化が大きいときに配信する方法、加速度センサなどの各種センサが変化したときに撮影する方法、そして一定時間ごとに行動選択を行う方法などが挙げられる．本論文では、簡単のため、一定時間ごとに行動選択する方法でシステムを構築し、評価をした．具体的には30秒に一度、写真の撮影か転送かを選択する方法を用いた．このときの写真撮影を行う確率を写真撮影率とする．なお30秒とは、予備実験にて適度に通信の衝突が発生する時間として選んだものであり、これは通信装置としてIEEE802.15.4に準じた無線端末を用いたことに起因している．他の通信装置、たとえば無線LANであるIEEE802.11を用いた場合は通信速度が速いため、行動選択の間隔をこれより短くすることも可能である．

カメラあり端末は写真を撮影すると、その写真を自分の端末に保管する．その際、自分の端末番号に加えて写真を区別する識別子（たとえば時間や通し番号など）を情報として付加する．もっとも簡単な付加方法は、その情報をそのままファイル名にする方法である．また、行動選択として写真の送信を選んだ場合は、保管している写真の中から1枚選び、隣接端末へ送信する．通信帯域に余裕がある場合は隣接端末1台1台に対して1対1通信にて写真を送信することが可能であるが、帯域が狭い場合は隣接端末全体に対して一斉配信しないと、1枚あたりの写真送信時間が行動選択の間隔を超えるため、システムが有効に働かない．以後、帯域が狭い場合を検討する．このとき、送信した回数を記録しておき、送信回数の少ない写真から順に送信すると、効率よくネットワークに写真を分散できる．

情報配信方法は周辺端末への一斉配信を繰り返すフラッシングであり、写真を受け取った端末がその写真を転送するのは、行動選択時に写真転送を選び、かつそ

Fig. 2 The flowchart of our proposed system

の写真を選択した場合である．一般に1対多の通信方法である一斉配信は送信側から受信側への一方向通信のため、受信側で通信エラーが起こっても送信端末側でそれを把握できない問題が生じる．通常の送信端末と受信端末の間の1対1通信であれば、受信側から再送を要求することでこの問題は回避できる．そこで、本研究では1対多の一斉配信において、受信端末を1台決定し、その端末と通信を行う形で確実な通信を実現する．すなわち通信相手を選定する方法である．受信端末は、送信端末に対して同じデータを持つパケットを送り返す (Fig. 3)．ここで受信端末は、送信端末に対して返信するため、目的端末 (Target ID) と送信端末 (Sender ID) を入れ替えて、自身を送信端末としたパケットを用意する．状態番号 (StateNum) は、パケットの状態を表す番号で、送信端末による隣接端末の呼び出しや、それを受け取った隣接端末から送信端末への返事といったパケットの状態の識別に用いる．パケットの受信失敗を確認するために通し番号 (Seq Num, Ack Seq) を付加しており、このパケット自身の番号と最後に受信した相手パケットの番号を通知する．送信端末はこの情報を用いて再送の可否を決めるが、受信端末はすでに送信端末からのパケットを正しく受けているため再送は行わない．サイズ (Size) とデータ (Data) は、送信パケットと同じものを送り返す．待ち時間 (WaitTime) は、送信・受信端末間の時間同期のための調整値が入っている．隣接端末は、これらの通信のやり取りを受信し、データを受け取る．隣接端末は、

Fig. 3 The packet format of sender and receiver nodes

送信端末からと受信端末からの同じデータの packets を 2 回受け取る機会があり、もし伝送路上でエラーが生じても受信端末が再送要求を行えば正しい packets を受信しエラーを回避できるため、従来の 1 対多の一斉配信と比べてエラーへの耐性が高い配信が期待できる。

受信端末の選定は色々な方法が考えられるが、今回は車同士の通信のため移動する可能性があり、通信中に圏外になることをできる限り避けるため、送信端末に近い端末を受信端末として選ぶこととした。具体的には、送信端末が受信端末選定のための packets を送信し、それを受信した隣接端末はその packets 受信時の電界強度に応じた時間¹を待った後、送信端末に返事をする。最初に packets を返信した端末を、送信端末に近い端末とみなし、受信端末として扱う。

隣接端末は写真を受信すると、自分の端末で保管していない写真であれば自分の端末に保管する。これを繰り返すことで、撮影写真がネットワーク上の各端末に分散し、共有される。カメラなし端末は写真の撮影を行わないだけで、それ以外はカメラあり端末と同じ動作をする。

2.2 犯罪抑止力について

提案する防犯カメラシステムに生ずる新しい二つの犯罪抑止力について、この節で説明する。

まず一つ目は、どこから撮影されているかわからないという点である。カメラが車に設置されており、車の出入りに伴いカメラの設置位置が変化するため、通常の固定されたカメラと比べ、カメラの撮影範囲の予想が困難となり死角を見つけるのが難しい。そのため、犯罪抑止力が働くと考えられる。これは、カメラが固定されたシステムに対するメリットである。

つぎに、撮影した写真を多数の端末で共有するため、写真をネットワーク内の端末からすべて消去するのが難しいという点である。端末に写真を保管する従来のセキュリティシステムでは、端末が破壊や盗難に遭うと情報が残らない。また、センタに写真を保管するセキュリティシステムでは、データが集中している部分を破壊されると、監視情報を消失する危険がある。それに対して提案システムでは、隣接端末に写真を送るため、破壊される直前といった犯罪者の写っている写真がどこかの端

末に保存される可能性が高い。犯罪者が自分の写った写真を削除するには、写真が転送された隣接端末すべてを破壊する必要がある。ここで、カメラなし端末が重要となる。カメラなし端末は通信できる範囲であればどこにでも設置できるため、壁の中など犯罪者の手の届かない場所に設置できる。そのため、すべての端末の破壊は不可能である。加えて、端末の破壊行為は自分の写真を残すことにつながるため、犯罪に対する抑止力が期待できる。これは、端末に写真を保管するシステムに対するメリットである。

これら二つの犯罪抑止力により、従来のカメラが固定されたシステムや端末に写真を保管するシステムに対して強い犯罪抑止効果が期待できる。

2.3 プライバシについて

カメラあり端末は、ある一定の時間間隔や動作検知により自動的に写真を残す。そのため、犯人でない人物を撮影する可能性がある。その写真を他端末に転送するにはその人物のプライバシーを考慮する必要がある。他の端末で写真の再生をできなくするために、撮影写真の暗号化について議論する。また、Zimmer[10]で提案されている道義的な項目について検討する。

カメラあり端末は、撮影写真を暗号化して保存する。簡単な方法としては、写真のデータ長以上の長さのランダム文字列を所有し、撮影した写真と排他的論理和を計算して、暗号化画像情報として保存する。隣接端末には、この暗号化された画像情報を送信する。鍵となるランダム文字列は、自分の端末以外には管理者のみが保管する。それ以外の端末には、この鍵が何であるかわからない。管理者は、この防犯カメラネットワークとは物理的に接続しない計算機に鍵を保管し、有事の際にのみ取り出して復号に用いる。これにより、もし端末を盗まれても、その盗まれた端末のカメラが撮影した写真しか見ることができず、他の端末が撮影した写真のプライバシーを守ることができる。また無線通信において、第三者に通信を傍受される可能性はあるが、送信する写真データが暗号化されているため問題にはならない。ここでは鍵を用いた排他的論理和による暗号化について述べたが、それ以外の暗号化を用いても問題ない。搭載するマイコンの計算能力との兼ね合いで、実用的な方法を用いれば十分である。

Zimmer は、車車間通信、路車間通信にて満たすべきいくつかの道徳について述べている。ここでは、以下の三つの項目について検討する。1) 誰がこれらのデータにアクセスできるのか。2) 運転手はこのシステムを無効にすることを選べるか。3) 誰がこの情報を所有するのか。すなわち、1) はプライバシー確保による道徳的な信頼性を意味し、2) はシステムに対する拒否が認められているか否かという点で道徳的な有効性を意味し、3) は情報の流出に対する保障であり道徳的な安全性を意味する。

¹ 受信時の電界強度が強いほど短い待ち時間とする。

まず、最初の項目について検討する．それぞれの端末に対して暗号化の鍵を用いるため、撮影した写真は撮影した端末自身と鍵を管理する管理者のみがアクセスできる．たとえば、自分の車に搭載している端末が保管している写真を見ようとしても、その端末が撮影した写真しか復号できず、他の端末の画像は確認できない．そのため、プライバシーは確保できている¹．

二つ目の項目は、システムに対する拒否権である．運転手は無線端末の電源を切ることで、システムから離脱することができる．もし、すべての車載端末の電源を切っても、その場合は駐車場に車が一台もないときと同じ状態となり、敷地に設置した無線端末のみで構築したネットワークと等価になる．転送端末の数が多い方がネットワークは安定するため、その状態は望ましくはないが、その場合でも、システムが稼働するように無線端末を設置しておけばシステムとしては問題がない．

最後に三つ目の項目に対しては、隣接端末に写真データを送信するため、最終的に情報を所有するのはすべての端末である．しかしながらその写真データは暗号化されているため、見ることができる写真を所有するのは、それを撮影した端末だけである．そのため、このシステムを利用するには、写真情報を皆で共有することに同意する必要がある．そのうえで、情報の暗号化により、道徳的な安全性を満たしていると考えられる．

以上より、本提案システムはZimmerにおける道徳的な信頼性、有効性、そして安全性の要求を満たしている．

2.4 センサネットワークによる監視カメラシステムとの比較

ユビキタスマニタリングシステム[4]では、センサネットワークを用いて監視カメラシステムを構築している．監視カメラに無線端末をつけ、その端末同士でネットワークを構築し、監視センタに向けて画像情報を送信している．このネットワーク形態の場合、インフラの敷設が容易であるが、監視センタによる集中監視であるため、その近隣のネットワークトラフィックが混雑する問題がある．これは、経路構築の際に目的地が監視センタに限定されるために生じる偏りである．

それに対して提案手法の場合は各端末が写真データを保持するため、経路によるトラフィックの偏りが生じないぶん、ネットワークを効果的に使えると考えられる．ただし、いずれの手法も、端末の配置によるトラフィックの偏りは生じる．また提案手法では端末が車に設置されているので、車の駐車状況に応じて監視範囲が変わってくる．そのため、どこから監視されているかの把握が困難になる．これらの点で、従来のセンサネットワークに

よる監視カメラシステムよりも優位である．ただし、提案手法ではネットワークに属する全端末に写真画像を送るには何度か転送する必要があるため、通信トラフィックの総量の観点ではセンサネットワークによる監視カメラシステムよりも効率が悪い．

3. 実験

この節では、実機を用いた実験とシミュレータによる実験を通して、システムの有効性を確認する．まず、実世界での性能評価として、IEEE802.15.4に準ずる無線端末SS-1[7]を用いて実験を行う．ここでは、ノイズなどの外乱やマイコンの処理の遅れなどの影響による受信失敗の確率を測定する．この受信確率を考慮したシミュレータを作成し、実際の駐車場での端末の配置による写真画像の分散をシミュレートする．端末数を1,000台まで増やし、そのうちの1割の車が同時に駐車場に出入りするように動く環境を用意し、システムの有効性を確認する．

まず実験にあたり、性能評価の指標について説明する．本論文では、同じ写真を多数の端末が保持することで破壊に対する耐性を高めることを目的としている．そのため、ある端末 n のある m 番目の写真を保持している端末の台数 $l_{n,m}$ を考えたとき、 $l_{n,m}$ が大きければ大きいほど、耐性が高いと考えられる．最悪の場合を考慮すると、 $\min_m l_{n,m}$ が最も分散していない写真を意味するが、この場合、撮影した直後の写真に対して低い数字が出ることは明らかで、評価軸としては不適切である．そこで、ここでは写真の分散の状況を、ある瞬間における状況を示す指標と、ある特定の写真に注目した状況を示す二つの指標の合計三つの指標を提案する．前者を瞬間分散率とし、後者を写真の分散数とする．

ある時刻 t において、端末 n の撮影した写真 M_n 枚に対するネットワーク内の他の端末がそれらの写真を保持している平均端末台数 $\sum_{m=1}^{M_n} l_{n,m}/M_n$ を、端末 n の瞬間分散率とする．ここで全端末の写真の瞬間分散率は、それぞれの端末が持つ写真の枚数に応じた重み付けをした瞬間分散率の総和であり、

$$\begin{aligned}
 & \text{全端末の写真の瞬間分散率} \\
 &= \sum_{n=1}^N \frac{M_n}{\sum_{n'=1}^N M_{n'}} \sum_{m=1}^{M_n} (l_{n,m}/M_n) \\
 &= \sum_{n=1}^N \frac{1}{\sum_{n'=1}^N M_{n'}} \sum_{m=1}^{M_n} l_{n,m} \\
 &= \sum_{n=1}^N \sum_{m=1}^{M_n} \left(l_{n,m} / \sum_{n'=1}^N M_{n'} \right) \\
 &= \text{全端末の写真受信枚数} / \text{全端末の写真撮影枚数}
 \end{aligned} \tag{1}$$

となり、全端末の写真撮影枚数に対する全端末の写真受信枚数の比率と等しくなる．防犯カメラシステムが有効

¹ここでは簡単のため共通鍵暗号方式を採用しているが、暗号化鍵と復号化鍵が異なる暗号化方式（たとえば公開鍵暗号方式）を採用し、復号化鍵を管理者だけが保管すれば、自端末が撮影した第三者に対するプライバシーも確保できる．

に働くためには、ある端末が撮影した写真を、少なくとも 1 台以上の他の端末へ受け渡す必要があり、そのとき全端末の瞬間分散率は 1 を超える。ただし、これはある時間における写真の分散状況を示しているため、個別の写真がどれくらい分散しているかはわからない。

そこで、個別の写真に着目し、実験終了時に何台の端末が保持しているかを写真の分散数とする。具体的には、実験時間の半分の時点で端末が撮影した写真が、実験終了時点で何台の端末が保持しているかを各端末ごとに数え、その平均値とする。また、その写真がどれだけ広範囲に分散しているかを表すために、写真の分散距離を考える。これは、写真撮影時の座標から、実験終了時点でその写真を保持している端末の座標までの距離である。写真の分散には、端末の移動と別の端末への通信という二つの要素が関係する。どれだけ広範囲に分散しているかを知るためには、写真の分散の平均値よりも最大値を用いる方が状況を把握できる。

これらの指標を用いて実験を行う。

3.1 無線端末の仕様

本研究では、無線端末としてサイレントシステム社の 8 ビットマイコンつき無線モジュール SS-1 を用いる。このモジュールは二つのシリアルポートを持っており、一つ目のポートを使って JPEG カメラを接続する。無線モジュール SS-1 の仕様を Table 1 に示す。ただしこのマイコンの記憶容量は 4kB と小さいため、二つ目のポートを経由して外部モジュールに接続し、写真データを MicroSD へ書き込む。端末を Fig. 4 に示す。

SS-1 の無線の物理層は、IEEE 802.15.4 に準じている。これはセンサネットワークで一般に用いられる ZigBee[8] と同じである。しかし、SS-1 には ZigBee の通信プロトコルが搭載されていないため離れた端末とパケットをやりとりするための経路構築の機能はない。なお本システムでは、撮影した写真データは隣接端末への送信を繰り返すことでネットワークに分散するため離れた端末と直接通信する必要がなく、経路構築の機能がなくても問題ない。また、通信パケットの衝突検知や ACK などの通信を制御する機能がないため、端末が密集していると送信が困難になりやすい。

3.2 通信相手を選定する一斉配信の効果

今回構築したシステムでは隣接端末への一斉配信のために、まず通信相手を選定する方法を提案した。そこで、この方法の効果を確認するために、通信相手を選定せずに配信する場合と選定して配信する場合の配信成功率の比較を行う。端末 10 台をそれぞれの電界強度が Fig. 5 となるように配置し、30[s] ごとに写真撮影と写真データの送信を繰り返す。なお、写真データのサイズは平均して 10k[byte] である。写真撮影時は、他の端末からの写真データは受け取れない。実験は屋内にて最小電力 (Transmitter power = Min.) で送信したが、

Table 1 Specifications of SS-1 wireless module

Size	32 [mm] × 32 [mm] × 9 [mm]
Voltage	3.3 [v]
Electric Current	2 [μ A] for waiting 40 [mA] for sending
Modulation	2.4 [GHz] spread spectrum (IEEE 802.15.4)
Speed	250 [kbps]
Sensor	Acceleration sensor Temperature sensor
Serial Port	2 ports
g-Range = 1.5g	800 [mV/g]
g-Range = 2g	600 [mV/g]
g-Range = 4g	300 [mV/g]
g-Range = 6g	200 [mV/g]
Acceleration Modes	Dynamic Acceleration Static Acceleration
Supply Voltage(V_{DD})	-0.3 to +3.6

Fig. 4 Prototype of a wireless node: a camera node with JPEG camera and the uALFAT module for a MicroSD storage

送信電力は 16 段階で設定でき、屋外における最大電力 (Transmitter power = Max.) の送信時の電界強度と距離の関係は Fig. 6 である。なお、Fig. 6 はパケットが正常に受信できたときの電界強度を表しているため、パケットの衝突はこれよりも遠くのところでも生じる。

ここでは、3 種類の送信方法を比較する。まず、送信端末が通信相手を選定せずに配信する方法 (Broadcasting only) である。他の方法と公平性を保つために、同じパケットを 2 回ずつ送信し、冗長性を持たせている。この方法では、隣接端末の状態を確認せずに送信するため、周りの端末すべてが写真撮影中の場合などが起こりえる。そこで、写真を一斉配信する前に周りの端末に状態の問合せを行い、端末の存在を確認したときのみ一斉配信する方法 (Broadcasting using receiver's check) も用意した。この方法では、問合せを受けた端末は提案手法と同様に受信強度に応じて時間をずらして返事を行う。送信端末は受信可能な端末が近隣にいることを確認してから、Broadcasting only と同様に同じパケットを 2 回ずつ一斉配信する。Broadcasting only では、受信端末

Fig. 5 The signal powers that mean link quality between nodes in the experiment

Fig. 6 The relationship between signal powers and node distances

Fig. 7 The experimental result of 3 methods: Broadcasting only, Broadcasting using receiver's check, and our proposed method

がいなくても送信を開始するが、この方法ではそれを回避できる。一斉配信を始めた後は Broadcasting only と同様に、他の端末からのパケットとの衝突が生じる可能性が残っている。そして、それら周りの受信端末からパケットの受信強度が一番強い端末を通信相手として選定する提案手法 (Proposed method) の三つの手法を用意し、写真の瞬間分散率の比較を行った。

結果が Fig. 7 である。一つの端末の通信範囲内に存在

する隣接端末の数が多くパケットの衝突が頻繁に起こるため、通信相手を選定しない方法では瞬間分散率が 1 を下回っている。これに対して、通信相手を選定する提案手法では、確実に 1 台以上の端末に送信できるため、瞬間分散率が 1 より大きい。実験開始直後に提案手法の瞬間分散率が 1 に近づいているが、これは各端末の行動選択のタイミングが近くパケットの衝突が起こりやすいためであり、その後、お互いのタイミングがずれていくことで、性能が向上している。

この実験において電界強度ごとにパケットを正常に受信できた場合を数え、パケットの送信回数に対する受信できたパケットの数の比率を Table 3 の写真配信成功率としてまとめた。この表と Fig. 6 より、送信出力に対する写真配信成功率と通信距離の関係がわかる。また、この実機による電界強度と写真配信成功率の関係に基づき、次節のシミュレータを作成する。シミュレータでは写真の配信に 10 秒を要するため、1 秒あたりの成功率 p に対して 10 秒あたりの成功率 p^{10} が写真配信成功率に近づくよう p を決定する。それぞれの値をシミュレータにおける成功率として Table 3 に示す。

3.3 シミュレータによる実験

今回構築したシステムでは、無線端末は 30[s] ごとに写真撮影率に従って写真撮影が写真データの送信かを選択する。この写真撮影率が高いと、多数の写真を撮影するがネットワークへの写真の分散は遅くなる。とくに 0.5 を超えると、送信する写真よりも撮影する写真の枚数の方が多くなる。単位時間当たりの写真撮影枚数が多いため、防犯システムとしてはよいが、ネットワークで写真を共有するシステムとしては望ましくない。一方、写真撮影率が低いと、同じ写真を何度も送信するため、端末間での写真の共有率は高くなるが、冗長なシステムとなる。

そこで、実際の駐車場での利用を想定し、どのくらいの写真撮影率が適切かを知るために、シミュレータを作成し実験を行った。なお、個別の写真の分散状況を確認するため、ここでは写真の分散数を評価の指標とする。

まず、シミュレータの条件について説明する。無線の通信範囲として半径 40[m] を想定し、駐車場の敷地は 160[m]×160[m] の広さとする。これは、端末数が少ない場合にも、お互い通信するための広さである。車は敷地内に偏りなく設置するために、Fig. 8 のように敷地を $1, 4, 16, \dots, 2^{2(n-1)}$ 個に分割して順に配置点を決める。簡単のために 1 台の車につき、一つのカメラ付きの無線端末を想定する。この駐車場において、車が入り出す様子をシミュレートし、撮影した写真が端末間で共有される様子を確認する。ここではカメラなし端末を敷地内に設置する代わりに、車の移動台数を制限することで、駐車場内のネットワークの維持を試みた。ある時間 $t[s]$ において、全台数に対して最大 1 割の車が、同時に移動す

Table 2 The specifications for three methods in experiments

	Broadcasting only	Broadcasting using receiver's check	Proposed method
Sends a packet to check receivers	No	Yes	Yes
Replies a packet to the sender	No	No	Yes
Selects a target from reply nodes	No	No	Yes
How to send a data packet to neighbors	Two unidirectional packets	Two unidirectional packets	Two bidirectional packets
How to corrects an error	Sends the same packet twice	Sends the same packet twice	Requests to retransmit using a sequence number

Table 3 The relationship between the signal power and packet error

電界強度 [dBm]	写真配信成功率	シミュレータにおける	
		1 秒あたりの成功率	10 秒あたりの成功率
-35 ~	1.000	1.000	1.000
-50 ~ -35	0.867	0.986	0.868
-60 ~ -50	0.750	0.972	0.753
-75 ~ -60	0.688	0.963	0.686
-90 ~ -75	0.520	0.937	0.522
-110 ~ -90	0.417	0.916	0.416
~ -110	0.000	0.000	0.000

Fig. 8 The location of nodes on cars

る．移動する車 n は現在地を $(x(n), y(n))$ とすると，駐車場から出るために上へ進み， $(x(n), 0)$ の点を経由して出入り口とみなす $(0, 0)$ の点へ向かう．そして，駐車場に入るために，同じ経路を逆にたどり $(x(n), y(n))$ へと戻る．そのときの移動距離は $1[s]$ に $1[m]$ とし，簡単のために他の車と同じ座標に重なることを許している．端末間の通信は，Table 3 の写真配信成功率に基づき， $1[s]$ あたりの成功率を決定した．なお，写真の撮影と配信にはそれぞれ $10[s]$ かかるものとし，各端末は $30[s]$ ごとに行動選択を行う．写真を配信している端末の隣接端末は， $1[s]$ ごとに Table 3 の成功率に基づいて受信状況が決まり， $10[s]$ 続けて受信が成功した場合に，その写真がその端末に保管される．

3,000[s] 後の写真撮影率に対する写真の分散数を端末

数ごとに示したものを Fig. 9 に示す．ここでは写真撮影率に対する変化を確認するため，端末数は 100 台までとした．Fig. 8 の分割数に応じた端末数として，5，21，そして 85 台のときと，それぞれの間の状況を把握するために 10，50，そして 100 台のときを調べた．分散数が 2 より小さい場合，写真が分散できていないことを意味する．端末数が 21 台より少ないときは，隣接端末と通信できない端末が存在するため，分散数が 2 以下になりやすいが，端末数が増えるにつれて，分散数も大きくなることがわかる．また，他の端末から受信した写真を転送する場合があるため，写真撮影率が 0.5 であっても分散数は 2 に達していない．端末数が 21 台以上のときに，分散数が 2 を超えるのは，写真撮影率が 0.3 より小さい場合であることがわかる．

また，写真の最大分散距離を Fig. 10 に示す．端末数が増えるほど，最大分散距離が長くなるが，写真撮影率にはあまり依存しないことがわかる．なお，今回のシミュレーションは $160[m] \times 160[m]$ の正方形の空間であるため，分散距離の最大値は約 $226[m]$ である．端末数が 21 台以上のときに， $140[m]$ 以上の分散距離を示しており，1 箇所に偏っていないことがわかる．

つぎに，写真撮影率と端末の台数の関係性を調べるため，端末の台数を増やしたシミュレーションを行う．写真撮

Fig. 9 The number of nodes which share the one picture

Fig. 10 The maximum distance of picture distributions that means the maximum distance between taken place and stored place in one picture

Fig. 11 The number of picture distributions by changing the rate of pictures taken

影率として0.20, 0.25, そして0.30を用い, 端末数すなわち車の台数を1,000台まで増やした結果がFig. 11である。いずれの写真撮影率においても, 端末数が300台を超えると分散数が2を下回った。これは, 5[m]に1台の間隔で端末を配置している状態であり, 一般のセダンタイプの車の全長とほぼ一致するため, 駐車場としてはこれ以上密接する場合を考慮する必要はない。そのため, 提案システムは駐車場において有効に働くことがわかる。また, 1台の車に二つ以上の端末を設置する場合など端末数を300台よりも増やすには, 送信出力を下げるなどして通信範囲を抑えれば, 通信圏内の端末の密度を下げる事が可能である。

4. おわりに

本論文にて, アドホックネットワークを用いた駐車場における新しい防犯カメラシステムを提案した。カメラ付きの無線端末を車に設置して駐車場内のあらゆる所を監視し, カメラのない無線端末は駐車場の敷地に設置してネットワーク構築を助ける。このシステムでは, 2点の犯罪抑止力が期待できる。犯罪者は, どこから撮影されているかわからず, 死角を見つけられない。また, 犯罪者が端末を破壊するとき, このカメラのない端末を破壊することは不可能なため, 犯罪者は撮影した画像を完全に消去できない。これら2点の犯罪抑止力により, 従来よりも防犯能力が高まると考えられる。

これら提案システムの効果を確認するために, 実機による実験とシミュレータによる実験を行った。実機においては写真を周りの端末へ一斉配信する際に, 受信端末を一つ決め, その端末との1対1通信をもとにそれ以外の隣接端末はその通信を受信する方法を提案した。これにより, 必ず一つ以上の端末への送信が保証される。シミュレータにおいて, 車が密接した状態である端末の台数が300台の状態まで, 撮影した写真が他の端末に送られることを確認し, 平均2台以上の端末が各画像を保持していることを確認した。これにより, 車上荒らしなどの犯罪が起こり, ある端末が破壊されても, 必ず画像を確保できることが確認できた。

今回用いたシミュレータでは, カメラの撮影範囲は考慮していない。そのため, 死角がどのように変化するか確認できていない。今後は, 1台の車に複数台の端末を搭載する場合を確認し, 死角をなくす方法を検討する必要がある。また, 立体駐車場における通信状況を確認し, 立体的なシミュレートをする必要もある。

本論文では基地局を用いず, 端末だけで防犯カメラシステムを構築した。今後は基地局を用いた防犯カメラシステムとの融合を検討する必要がある。とくに, 壁に固定しているカメラなし端末から, 監視センタへデータを転送することができれば, 基地局を用いた防犯カメラシステムと提案する防犯カメラシステムの両方のメリットを活かすことができ, より頑強なシステムになると考えられる。また, 実験では1箇所の駐車場の場合の性能評価を行ったが, 実用化に向けて, 本システムを適用している他の駐車場の車との通信を考慮し, 最終的には不特定多数の人が用いる駐車場への適用を検討する必要がある。

謝 辞

本研究は文部科学省のハイテク事業による私学助成と科研費(21710188)の助成を得て行われた。

参考文献

- [1] M. Kenichi: Communications supported by ad hoc networks in disasters; *The Journal of the Institute of Electronics, Information, and Communication Engineers*, Vol. 89, No. 9, pp. 796–800 (2006)
- [2] M. Kenichi: Inter-vehicle communications and mobile ad hoc networks; *The IEICE Transactions on Communications*, B, Vol. 89, No. 6, pp. 824–835 (2006)
- [3] 主な街頭犯罪の認知件数の推移 (平成 12 ~ 21 年), 平成 22 年版警察白書; <http://www.npa.go.jp/hakusyo/h22/honbun/html/m1120000.html>
- [4] 江端: どこにいても安全・安心を見守るユビキタスマニタリングシステム; http://www.hitachi.co.jp/rd/sdl/people/ubiq_monitoring/index.html (2006)
- [5] C. Perkins, E. Belding-Royer and S. Das: Ad hoc On-Demand Distance Vector (AODV) routing; *Internet Engineering Task Force(IETF)*, RFC3561: <http://www.ietf.org/rfc/rfc3561.txt> (July, 2003)
- [6] T. Clausen and P. Jacquet: Optimized Link State Routing protocol (OLSR); *Internet Engineering Task Force(IETF)*, RFC3626: <http://www.ietf.org/rfc/rfc3626.txt> (October, 2003)
- [7] SilentSystem: 2.4GHz wireless module SS-1; <http://silentsystem.jp/ss-1.htm>
- [8] ZigBee Alliance: <http://www.zigbee.org>
- [9] R. Collins, A. Lipton, H. Fujiyoshi and K. Takeo: Algorithms for cooperative multisensor surveillance; *Proceedings of IEEE*, Vol. 89, No. 10, pp. 1456–1477 (2001)
- [10] M. Zimmer: Surveillance, privacy and the ethics of vehicle safety communications; *Ethics and Information Technology*, Vol. 7, No. 4, pp. 201–210 (2005)
- [11] G. Korkmaz, E. Ekici, F. Ozguner and U. Ozguner: Urban multi-hopbroadcast protocol for inter-vehicle communication systems; *Proceedings of VANET*, (October, 2004)
- [12] C. Wai and C. Shengwei: Ad hoc peer-to-peer network architecture for vehicle safety communications; *IEEE Communications Magazine*, Vol. 43, No. 4, pp. 100–107 (April, 2005)
- [13] S. Ahmed and S. S. Kanhere: VANETCODE: Network coding to enhance cooperative downloading in vehicular ad hoc networks; *Proceedings of IWCMC* (July, 2006)
- [14] U. Lee, J. Park, J. Yeh, G. Pau and M. Gerla: CodeTorrent: Content distribution using network coding in VANET; *Proceedings ACM Mobishare* (2006)
- [15] S. Das, A. Nandan, G. Pau, M. Y. Sanadidi and M. Gerla: SPAWN: A swarming protocol for vehicular ad hoc networks; *Proceedings of the 1st ACM VANET* (October, 2004)
- [16] J. A. Pouselse, P. Garbachi, D. H. J. Epema and H. J. Sips: The bittorrent p2p File-sharing system: Measurements and analysis; *Proceedings of the IPTPS '05* (February, 2005)

著者略歴

うえむら
植村わたる
渉 (正会員)

2000 年大阪市立大学工学部応用物理学科卒業, 2005 年同大学大学院工学研究科電子情報系専攻博士課程修了。同年龍谷大学理工学部助手。現在, 同助教。博士(工学)。2009 年計測自動制御学会 システム・情報部門学術講演会 奨励賞受賞。人工知能学会, 電子情報通信学会, IEEE などの会員。

むらた
村田まさし
正

1965 年信州大学工学部通信工学科卒業, 1970 年大阪大学大学院工学研究科通信工学専攻博士課程修了。同年大阪大学助手。同講師, 同助教授, 大阪産業大学教授, 大阪市立大学教授を経て, 2005 年龍谷大学教授。2011 年退職。電子回路, 通信方式, 無線通信に関する研究に従事。工学博士。