

# 基地局不要の防犯カメラシステムの構築

\* 植村 渉, 村田 正

龍谷大学 理工学部 電子情報学科

〒520-2194 滋賀県大津市瀬田大江町横谷 1-5

E-mail : {wataru, murata}@rins.ryukoku.ac.jp

**Abstract:** 近年, 日本では駐車場における窃盗事件が増加している. 2007 年の警察白書によると車内の物品の窃盗発生件数は約 17 万件であり, 自動車そのものの窃盗は約 3 万件, オートバイは約 8 万件が認知されている[1]. これらの窃盗に対して, さまざまな防犯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. カメラシステムは, 大きく 2 種類に分けられる. 犯罪行為の発見のためにリアルタイムに監視する方法と, 犯罪証拠の確保のために画像を記録する方法である. リアルタイム監視のためには, 撮影した画像を監視センタのサーバに集める必要がある. それに対して証拠確保の場合には, サーバで保管しても良いし, 各端末で画像を保管しても良い. ここでは, 証拠画像確保を目的とし, アドホックネットワークとファイル分散管理の技術を用いた新しい防犯カメラシステムを提案する.

## 1 はじめに

駐車場の監視カメラシステムは, いくつかの項目で分類できる. 重要な項目のうちの一つとして, 設置目的がある. 設置目的として, 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がある. 前者はリアルタイムに情報を得ることが重要であり, 後者は犯罪が起こった後に証拠を確保できればよい. リアルタイム監視では, 監視センタにてオペレータ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[3]. また, 1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[3]. この条件は, 証拠確保の目的の場合も同様である.

証拠確保のための監視の場合, プライバシの確保が必要になる[4]. 例えば1枚の写真だけでなく, 複数の写真による情報の流れから, 個人のプライバシーを得ることがないように警告している. それ以外にも, 車の安全通信技術の道德について述べている.

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, アクセスポイントのような基地局が端末の管理をし, 無線端末はそれらを経由して通信を行う. その場合, 無線ネットワークを提供するためには必ず基地局を用意する必要があり, 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, 近年, 基地局を用いず無線端末だけでネットワークを構築するアドホックネットワークの技術が注目されている. 端末は, 自分の電波が届く範囲内の端末にしか情報を送ることができない. これを**隣接端末**と呼ぶ. そのため, 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の中継をし, それを繰り返すことで, 通信経路を確立する.

車に無線端末を搭載し、アドホックネットワークを用いた VSC (Vehicle Safety Communications) が提案されている[5, 7]. VSC には P2P 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ポイントとなる[6]. それに対して本論文は駐車場における監視カメラシステムを議論するため、動いている車はわずかであるため、ネットワークの変化は緩やかである. しかし、静的なネットワークではない. そこで本論文では、データの配信を何度も繰り返すことで、情報の共有を目指す.

車両間での情報の共有には、BitTorrent[10]に基づいた FSP(File Swarming Protocol)を使ったコンテンツ共有が提案されている[8, 9]. FSP では、自端末が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、ファイルを分散させる. 今回作製した端末では、8 ビットマイコンを用いているため複雑なプロトコルの搭載は不可能であり、異なる端末と複数の通信のセッションを持つのは無理である. そこで、ブロードキャストを用いて持っているファイルを周りの端末へ一斉配信し、それを繰り返すことで、ネットワークの端末全部が同じファイルを共有するシステムを構築する. そのため、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.

## 2 新しい防犯カメラシステムの提案

本発表では、サーバを使わず端末のみで構成する新しい防犯カメラシステムについて提案する. 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端末と、カメラのついていない端末である. 移動体である車にはカメラあり端末を設置し、駐車場の壁や柱などには両方の端末を設置することを想定している. 提案システムでは、これらカメラあり端末とカメラなし端末で構築された無線ネットワークを用いて、ネットワークに属する端末間で撮影画像を共有する. このシステムの端末の動作について紹介し、生じる犯罪抑止力を 2 点挙げ、システムの有効性を議論する.

このシステム用いる 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同等であると想定している. カメラあり端末は画像を撮影すると、その撮影データを自端末に保管すると共に隣接端末へ配信する. 配信方法は、端末の出入りがある環境を考慮して、受信端末を指定しないブロードキャスト配信を用いる. つまり、電波の受信可能範囲内にいる全ての端末が、同時に画像情報を受け取る. 隣接端末において通信エラーが起これば正常に画像を受信すると、自端末に保管し、その後さらに自身の隣接端末へとブロードキャスト配信する. これを繰り返すことで、撮影画像がネットワーク上の各端末に分散し、共有される.

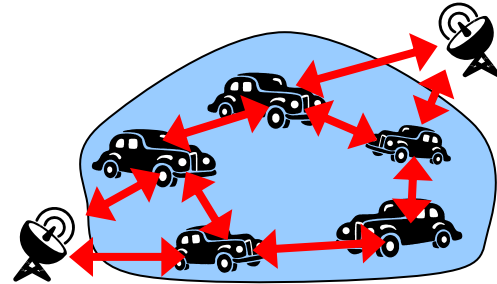


図 1 提案する監視システムの概要

### 2.1 犯罪抑止力について

提案する防犯カメラシステムには、従来の防犯システムにはない新しい 2 つの犯罪抑止力がある. 1 つ目の抑止力は、カメラが多数の車に設置されており車の出入りに伴い設置場所が変化するため、どこから撮影されているかわからないという点である. すなわち、カメラの撮影範囲の予想が困難なため、死角を見つけるのが難しい. 2 つ目の抑止力は、撮影画像を各端末で共有するため、全ての画像情報の消去が難しいという点である. 犯罪者が撮影された画像を削除するには、情報が配信された全ての端末を破壊しなければならない. ここで、カメラなし端末が重要となる. カメラなし端末は無線で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、全ての端末の破壊は不可能である. 加えて、カメラ端末の破壊は自分の画像を残すことにつながるため、車上荒らしの犯罪に対する抑止力が期待できる.

これら 2 つの犯罪抑止力により、従来の防犯カメラシステムよりも強い犯罪抑止効果が期待できる.

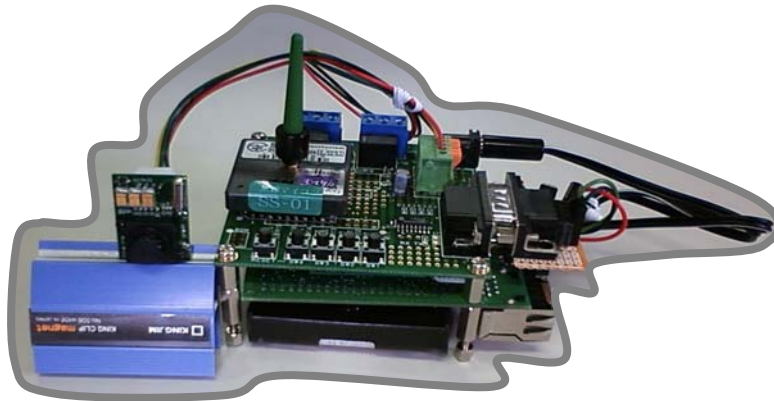


図 2 作製した防犯カメラ端末

## 2.2 プライバシについて

提案する防犯カメラシステムは、ある一定の時間間隔や動作検知により自動的に写真を撮影する。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しないといけない。そこで、他の端末では画像を再生できないようにするために、撮影画像の暗号化について議論する。また、Zimmer[4]に議論されているいくつかの道義的な項目について検討する。

ここでは鍵を用いた排他的論理和 XOR による暗号化について議論するが、それ以外の暗号化を用いても問題ない。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。

カメラあり端末は、撮影画像と同等の長さのランダム文字列を所有し、撮影した画像と排他的論理和を計算し画像情報として保存する。この暗号化された画像情報を隣接端末に送信する。鍵となるランダム文字列は、自端末以外には管理者のみが保管する。それ以外の端末は、この鍵を知ることができない。管理者は、この監視カメラネットワークとは物理的に異なる場所に鍵を保管し、有事の際にのみ取り出す。これにより、もし端末を盗まれても、その端末のカメラが撮影した画像しか見ることができず、他の端末が撮影した画像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、送信する画像情報が暗号化されているため問題にはならない。

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德について述べている。誰がこれらのデータにアクセスできるのか？運転手はこのシステムを無効にすることを選べるか？誰がこの情報を所有するのか？これら3つのポイントについて検討する。

まず、提案システムではそれぞれのノードで鍵を用いて画像情報を暗号化している。ノードと管理者のみがキーを保持しており、他のノードは暗号化された情報を保管するため、元の画像を見ることはできない。次に、車の持ち主はシステムの電源を切る場合を考える。全ての車に搭載しているカメラ端末の電源を切った場合、駐車場に車がない場合と同じ状況になる。駐車場にはネットワークの維持のために最低限の無線端末を置いているので、この状況でも防犯システムとしては成立する。ただし、一台でも多くの車が参加している方が、ネットワーク的にもデータ共有的にも良い。最後に情報の所有に関しては、全てのノードが所有する可能性がある。しかし、鍵を用いて暗号化するので、他のノードからは守られている。

よって、提案システムは、信頼性、有効性、そしてセキュリティの要求事項を満たしている。

## 2.3 ネットワークの形態について

車に無線端末を搭載し、アドホックネットワークを用いた VSC(Vehicle Safety Communications)が提案されている[5, 7]。VSC には P2P 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ポイントとなる[6]。それに対して本論文は駐車場における監視カメラシステムを議論するため、動いている車はわずかであるため、ネットワークの変化は緩やかである。しかし、静的なネッ

トワークではない．そこで本論文では，データの配信を何度も繰り返すことで，情報の共有を目指す．

車両間での情報の共有には，BitTorrent[10]に基づいた FSP(File Swarming Protocol)を使ったコンテンツ共有が提案されている[8, 9]．

FSP では，自端末が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，ファイルを分散させる．今回作製した端末では，8 ビットマイコンを用いているため複雑なプロトコルの搭載は不可能であり，異なる端末と複数の通信のセッションを持つのは無理である．そこで，ブロードキャストを用いて持っているファイルを周りの端末へ一斉配信し，それを繰り返すことで，ネットワークの端末全部が同じファイルを共有するシステムを構築する．そのため，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．

### 3 センサネットによる監視カメラシステムとの比較

ユビキタスモニタリングシステム[2]では，監視カメラをセンサネットにより構築している．各端末が無線により監視カメラ情報を中継し，基地局へつながるゲートウェイまで情報を転送する．この場合，インフラの敷設が容易であるが，最終的に監視センタによる一箇所集中監視であるため，それに至る経路の破損には弱い．例えば，ゲートウェイ近隣で妨害電波を出すと，無線端末は監視センタから孤立してしまい，情報を伝えられない．

提案手法の場合は各端末が画像情報を保持するため，妨害電波によりネットワークが分断されてもそれぞれの分断されたネットワークで監視機能を維持することができる．

### 4 おわりに

本研究にて，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．カメラ付きの端末は車に設置し，駐車場内のあらゆる所を監視する．このシステムでは，2つ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．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．画像撮影と画像転送の行動選択のバランスについて調べ，実環境下での性能評価を行う．今後は実際に車に設置し，運用上での問題点を検討する必要がある．

### 参考文献

- [1] 主な街頭犯罪の認知件数の推移（平成10～19年），平成20年警察白書，p.56, 2008.
- [2] 江端 智一，どこにいても安全・安心を見守るユビキタスモニタリングシステム，[http://www.hitachi.co.jp/rd/sdl/people/ubiq\\_monitoring/index.html](http://www.hitachi.co.jp/rd/sdl/people/ubiq_monitoring/index.html), 2006.
- [3] Collins, R., Lipton, A., Fujiyoshi, H., and Kanade, T: Algorithms for cooperative multisensor surveillance, Proceedings of IEEE 89, 10, 1456-1477 (2001).
- [4] Z. Michael: Surveillance, Privacy and the Ethics of Vehicle Safety Communications, Ethics and Information Technology 7(4): 201-210 (2005).
- [5] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner: Urban multi-hopbroadcast protocol for inter-vehicle communication systems, in Proceedings of VANET, (October, 2004).
- [6] Chen Wai and Cai Shengwei: Ad hoc peer-to-peer network architecture for vehicle safety communications, IEEE Communications Magazine, 43(4):100-107, (April, 2005).
- [7] S. Ahmed and S. S. Kanhere: VANETCODE: Network Coding to Enhance Cooperative Downloading in Vehicular Ad Hoc Networks, in Proceedings of IWCMC, (July, 2006).
- [8] U. Lee, J. Park, J. Yeh, G. Pau and M. Gerla: CodeTorrent: Content Distribution using Network Coding in VANET, in Proceedings ACM Mobishare, (2006).
- [9] S. Das, A. Nandan, G. Pau, M.Y. Sanadidi, M. Gerla: SPAWN: A Swarming Protocol for Vehicular Ad Hoc Networks, in Proceedings of the 1st ACM VANET, Philadelphia, PA, (October, 2004).
- [10] Pouwelse, J., Garbacki, P., Epema, D., and Sips, H.: The bittorrent p2p File-sharing system: Measurements and analysis: in Proceedings of the IPTPS '05 Ithaca, NY, (February, 2005).