

Mobile IPv6 を利用したコミュニティセキュリティシステム におけるトラフィック分析

勝 将万 井手口 哲夫 奥田 隆史 田 学軍

愛知県立大学大学院 情報科学研究科

近年、ユビキタスネットワークの実現に向けた、各種無線通信技術の開発競争とユビキタス環境下アプリケーションの提案と議論が盛んに行われている。そこで本論文では、ユビキタス環境下アプリケーションの一例として、モバイル通信技術により実現される地域社会の防犯アプリケーション“コミュニティセキュリティシステム”を提案する。システムの構成要素間で利用されるモバイル通信技術には特に Mobile IPv6 を適用し、システムの定義を行う。さらにシステムを通信ネットワークシミュレータ上にモデリングし、トラフィック分析を行うことにより、基本的なシステム特性の定量的評価を行う。

An Analysis of Traffic in Community Security System Using Mobile IPv6

Masakazu Katsu Tetsuo Ideguchi Takashi Okuda Xuejun Tian

Graduate School of Information Science and Technology, Aichi Prefectural University

Recently there has been considerable interest in a competition for various wireless communications for ubiquitous networks and proposals to many kinds of application in ubiquitous networks. This paper discusses “community security system” using technologies of mobile wireless network intended for the safety of local community and residents. One of the technologies of mobile wireless network is Mobile IPv6. We define the system and simulation-modeling using a communications network simulator. Then, we analyze network traffic in the simulation model and evaluate basic properties.

1. はじめに

近年、ユビキタスネットワーク社会を実現するモバイル通信技術の開発競争が盛んに行われている。これに伴い、様々な分野においてユビキタスネットワーク環境下で実現される、多種多様なアプリケーションの提案と議論がなされている。我々はその一例として、人々の地域社会における実生活の安全性に関する問題に着目し、人々が生活する地域社会“コミュニティ”の防犯を目的とした、「コミュニティセキュリティシステム」の提案・検討を行っている[1][2]。従来の研究[1]においては、システムのアプリケーションレイヤの挙動のみに着目している。システムの評価ツールとしてコンピュータ上に多数の主体(=エージェント)の相互作用からなる社会モデルを構築する環境を提供する MAS(Multi Agent Simulator)[3]を利用している。

ユビキタスコンピューティング環境下のアプリケーションの実現性に関する提案と議論は、種々の無線通信ネットワーク技術・規格を利用することが前提とされている。これらの提案と議論は、それぞれのアプリケーションが実行されるエリアの規模や通信トラフィックパターンを鑑みて、種々の技術や規格の中から最適なもの

を選択し、組み合わせることによってなされるべきである。さらにアプリケーションの特性評価はネットワークレイヤや物理レイヤを考慮して、実装によるテストベッド評価や通信ネットワークシミュレータによるシミュレーション評価を行うべきである。

そこで本論文では、以下のステップで構成する。

- ① セキュリティシステムの現状と展望を述べる。
- ② コミュニティセキュリティシステムに求められる機能と構成の定義を行う。
- ③ 定義から鑑みた種々の無線通信技術・規格の導入(プロトコルスタック)の前提を行う。
- ④ システムの具体的な構成要素と挙動を述べる。
- ⑤ 評価ツールとして通信ネットワークシミュレータを利用し、モデリングを行う。これから得られたシステムの構成要素間トラフィックの分析を行うことにより、通信ハンドオーバー時の伝送リンクの再接続等の特性評価を行う。

2. セキュリティシステム

人々の生活する地域社会における防犯システムの例としてホームセキュリティシステム[4]がある。以下にホ

ームセキュリティシステムと、我々が提案しているコミュニティセキュリティシステムの特性の違いを述べる。

2. 1 ホームセキュリティシステム

我々の日常生活の安全性を保障するシステムとして、現状では警備保障会社等によって提供されるホームセキュリティシステムが代表的なものとして挙げられる。これは人々が生活する建築物等の閉空間を対象としており、ID カード認証や暗証番号認証、及び監視カメラによる防犯などが代表的な機能である。“ホーム”は“コミュニティ”に比べ、システムの実行エリアの規模が小さく、機能の管理及び連携が容易であることから、現在の社会においても広く浸透している。また、人々の防犯意識の向上と情報保護の観点から、今後も警備業界の技術の進展が期待できる。

将来のホームセキュリティシステムの展望を考えると、ユビキタスコンピューティング技術の利活用・連携も考えられる。現状の無線通信ネットワーク技術の普及の進展状況[5]とシステムの実行エリアの規模から考えると、UWBやZigBeeなどが属するIEEE802.15系の無線PAN(Personal Area Network)技術、もしくはIEEE802.11系の無線LAN技術との親和性が高いと考えられる。さらにこれらによって実現されるセンサネットワーク技術なども利活用の推進が期待できる。

2. 2 コミュニティセキュリティシステム

コミュニティ向けセキュリティシステムといえるものとして、ホームセキュリティと同様に警備保障会社等によって提供されているシステム[6]などがある。しかし、これらはコミュニティ内を移動する対象(=子供)に専用の端末を持たせ、その位置情報をサービス利用者(=保護者)に提供するという簡易的な機能に留まっている。このような機能に留まる背景には、“コミュニティ”はシステムの実行エリアの規模が“ホーム”に比べ大きく、機能の管理が困難であることによる。さらに、無線通信システムに従属する課題である、通信端末の計算資源と電源不足などに関連することも考えられる。しかし、根本的な問題として、将来的に有用なシステムや機能そのものに対する抽出や議論が不十分であるといえる。

コミュニティセキュリティシステムにおいても、ホームセキュリティと同様にユビキタスコンピューティング技術の連携・利活用が想定できる。現状の無線通信ネットワーク技術の普及の進展状況とシステムの実行エリアの規模から考えると、IEEE802.11系の無線LAN技術、WiMAXに代表される無線MAN(Metropolitan Area Network)技術、第4世代携帯電話などの広域通信網を司る無線WAN(Wide Area Network)技術との相性が良いと考えられる。これらの無線通信技術の特徴から鑑みたコミュニティセキュリティシステムへの適用については、4章で詳細に考察を行う。

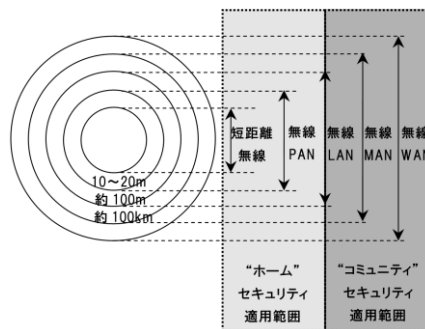


図1: 各種無線ネットワーク規模とシステム適用範囲

3. システムに求められる機能と構成

本章では、システムに求められる機能と構成を[7]を参考に考察する。また、導入する技術の課題と関連技術を示す。

3. 1 共通プラットフォームの構成

共通プラットフォームを導入する。その上に前述した「予防機能」、「通報機能」、「追跡機能」の3機能をアプリケーションとして実現する。このような構成にすることにより、機能の追加や拡張が容易となる。モデルを図3に示す。

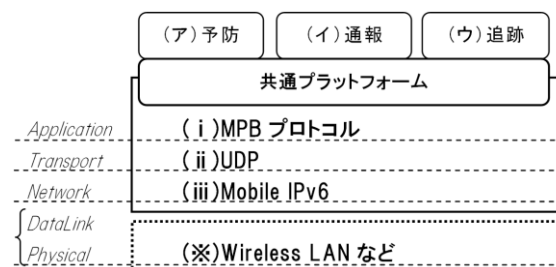


図3: 共通プラットフォームの構成

(ア) 予防機能

システムの執行者がコミュニティ内を巡回する機能である。これによりトラブルの発生を抑制し、防犯の役割を果たす。

(イ) 通報機能

システムの利用者であるコミュニティ内の住民とシステム執行者間の通信を実行する機能である。トラブルの発生を通知し、迅速に解決に導くための機能である。

(ウ) 追跡機能

トラブルの発生者を追跡し、捕捉する機能である。これによりコミュニティの安全を脅かす発生源を取り除き、トラブルの頻発を防ぐ。

(i) MPB(Mobile Police Box)プロトコル

コミュニティセキュリティシステムを実現するアプリケーション層プロトコルとして定義する。システ

ムの中で特に「通報機能」を扱うプロトコルである。
(ii) UDP

通報機能においては、特に迅速かつリアルタイムなデータの送受信機能が求められる。したがってトランスポート層プロトコルには転送速度が高いUDPを採用する。TCPと比較した場合の信頼性の低さなどの種々の機能の不足は、MPBプロトコルで補うものとする。

(iii) Mobile IPv6 [8]

現在のIPv4とIPv6の普及状況を鑑みた場合、IPv4をベースとしてIPv6が混在する環境を考慮すべきだが、将来性とモデリングの簡略化の目的からIPv6のみの環境を前提とする。

さらに、システムの執行者が3機能によってコミュニティ内を移動する過程で、異なるネットワーク間を移動する場合を考慮する。すなわち、通信(通報)の移動透過性を求め、ローミング(roaming)/ハンドオーバー(handover)を考慮する。また、本論文では移動元・移動先で異なるネットワークアドレスを与えたサブネット間を移動する広域ローミングとハンドオーバーについて考える。

広域ローミングとハンドオーバーの実現には様々なアプローチのしかたが議論されているが、本論文においてはモバイル環境に特化したIPv6技術のMobile IPv6を利用する。

3. 2 導入技術の課題と関連研究

Mobile IPv6は、ネットワーク間移動を考慮する関連研究において、参考一般技術として挙げられるものの、実際の利用や実装面では普及が停滞している。理由の1つとしては、Mobile IPv6に関するレイヤ3と無線LANなどに関するレイヤ2がそれぞれ独立してハンドオーバーを行ってしまう問題が挙げられる。つまり、無線LANの関連シーケンスとMobile IPv6の関連シーケンスが独立してなされるため、ハンドオーバー時の必要ステップが多く、結果としてオーバーヘッドを増大させてしまう。このようなレイヤ間の円滑な連携の不備により、結果として数秒間の通信途絶が起こるとされる。また、HA(Home Agent)という特殊な機構が必要な点もデメリットとされる。

さらに、IPv6ではステータレスアドレス自動生成によってIPv6アドレスが逐次自動生成できるようになったため、Mobile IPv6特有のHoA(Home Address)という永続的なアドレスを持つ必要がないとする見方もある。また、近年の無線MAN・WAN技術の通信速度向上により、広範囲通信エリアかつ広帯域のメディア利用を前提とする場合も想定できるようになりつつある。これにより、ネットワーク間移動ケース自体を考慮する必要が少ない環境となり、普及停滞の一因となっていくことも考えられる。

関連研究[9][10][11]などにおいては、複数ネットワー

クインタフェースの同時利用や、レイヤ2の制御情報抽象化とレイヤ3の主導的利用によってレイヤ間連携の円滑化を試みている。

しかし、本論文では4章でも述べるが、着想段階のシンプルな構成を前提としているため、課題とこれに対する議論はここまでにとどめる。

4. システムの前提

システムの前提を以下のように定める。

- ① IEEE802.11系の無線LANのみの環境とする。
- ② ネットワーク環境は無線LANアクセスポイントの通信エリアが一部オーバーラップするように複数設置し、メッシュ形態をなすように構成する。さらにローミング/ハンドオーバーを考慮する。
- ③ 着想段階のシンプルなハンドオーバー機構として、Mobile IPv6を利用する。

前提として3点を挙げた根拠を以下に述べる。

4. 1 前提①—無線通信技術の選定

序論でもふれたように、近年は無線通信技術の開発競争が熾烈である。特に次世代携帯電話の超高速データ通信の通信速度向上の競争が盛んである。総務省[12]によると、2010年をめどに100Mbps超~1Gbpsの無線通信の実現を目指すという。こういった状況を鑑みると、従来の研究においてIEEE802.11系の無線LANを前提としたために発生した論点が消滅してしまう可能性も想定できる。

しかし2008年現在の時点では開発は進行しているものの、実装面では先行きが不透明な部分も多い。したがって本論文では、通信速度の優位性、現状の普及度、シミュレーションモデリングの簡易性の観点から、IEEE802.11系の無線LANのみの環境を前提とする。

4. 2 前提②—コミュニティの実体

我々がコミュニティと呼ぶ実地域社会の実体は、数百m²の規模をもつ空間である。具体的には駅や大通り界隈の歓楽街区などを想定している。ここで問題となるのが、コミュニティの規模:数百m²に対して、IEEE802.11系の無線LANの一般的な通信距離が100m程度と小さいということである。これには、無線LANアクセスポイントの複数設置によるメッシュ化構成によって解決する。さらに3.1節で前述したように、ローミングとハンドオーバーを考慮する。

4. 3 前提③—Mobile IPv6

Mobile IPv6はIETFで“Mobility Support in IPv6”として提案されている、IPv6における広域ローミングをサポートする基本的技術である。本論文におけるローミング/ハンドオーバーの手法としては、着想段階のシンプルなモデルとして、Mobile IPv6のみの導入でシステムの実行を試みることにする。

5. システムの構成要素と挙動

5. 1 構成要素

コミュニティセキュリティシステムの具体的な構成要素について述べる。

(i) コミュニティ (Community) :

人々が活動するエリアである。前述したように数百 m² の規模を、駅や大通り界隈の歓楽街区などの形態を想定する。さらにこの中に、公衆無線 LAN アクセスポイントが通信エリアをオーバーラップするようにメッシュ構成を成している環境を想定する。VCS の集合として表現できるものとする。

(ii) VCS (Virtual Closed Space) :

コミュニティの部分集合である。無線 LAN 環境における、同一 ESSID の範囲と考えることができる。つまり、1 台以上の公衆無線 LAN アクセスポイントからなる通信エリアである。コミュニティの構成要素である。

(iii) MPB (Mobile Police Box) :

コミュニティ内を移動しながら、予防・通報 (受信)・追跡の 3 機能を実行するノードである。Mobile IPv6 における MN(Mobile Node)である。

(iv) VPS (Virtual Police Station) :

固定ノードであり、MPB を管理するノードである。Mobile IPv6 における HA(Home Agent)になり得る。

(v) 住民 (LR: Local Residence) :

コミュニティ内に複数存在し、コミュニティ内で発生したトラブルに関する情報を通報として、MPB もしくは VPS に送信する。Mobile IPv6 における CN(Correspondent Node)である。

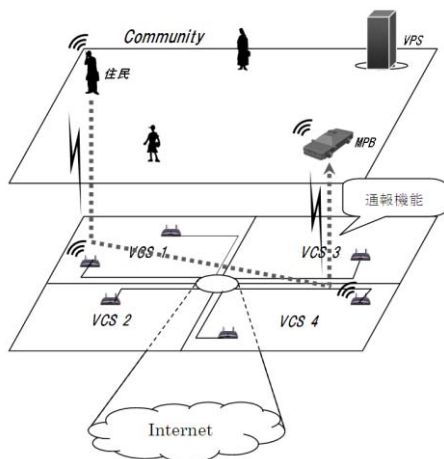


図 4 : MPB システムの構成要素

5. 2 挙動

MPB システムの動作過程を時系列的にみると、以下の 3 ステップに切り分けることができる。

(1) トラブル発生前

予防機能が実行される。MPB はコミュニティ内を巡回し、トラブルの発生を抑止による防犯を行う。

(2) トラブル発生後

トラブル発生場所の最も近接にいた住民が通報を行う。このときの通報情報の内容としては、トラブル発生場所の位置情報、動画像/音声情報として記録したトラブルの内容とったものを想定している。MPB は移動しながらこれを受信し、通報場所に向かう。

(3) トラブルへの対処とトラブル発生者捕捉

MPB はトラブルの発生場所 (=通報の発生場所) に到着後、トラブルの対処にあたる。トラブルの発生者を捕捉できる場合は捕捉する。

6. シミュレーションモデリング

想定するシミュレーションの環境と評価項目について述べる。本稿では特に 5.2 節で述べた動作の中から特に (2) トラブル発生後の時点に着目し、通報機能のみをモデリングすることを考え、予防機能、追跡機能に関してはモデリングを行わない。

5.2 節にて前述したように、通報機能においてやり取りされる通報は動画像/音声情報を想定している。さらに、これらをリアルタイムに住民 - MPB 間で送受信することを想定する。そして、セッションが確立され、通報の送受信の最中に MPB は VCS 間を移動する。このときの MPB の VCS 間ローミング/ハンドオーバーの挙動を考察する。

これらを実現するために、通信ネットワークシミュレーションソフトウェア OPNET Modeler[13][14]を利用する。std_model ライブラリの Mobile_IP プロジェクトの mipv6_route_optimization_enabled シナリオをベースにモデリングを行う。

6. 1 シミュレーション環境

(i) 空間の定義

図 5 のように 4 範囲の無線 LAN アクセスポイント通信エリア (一部オーバーラップ) からなる形状とする。数度のハンドオーバータイミングに着目したいと考え、このような規模とする。各パラメータは以下のようである。

- Wireless LAN > 通信距離 : 100m 相当 (Packet Reception-Power Threshold(dBm) : -73)
- Wireless LAN > Physical Characteristics : Extended Rate PHY(IEEE802.11g (54Mbps))
- Internet_cloud > Packet Latency : 0.1(sec)
- 隣接アクセスポイント間距離 : 160m
- 各アクセスポイント-Internet_cloud 間リンク : T1 (1.544Mbps)

(ii) 各構成要素の定義

(ア) MPB

Mobile IPv6 の MN として動作させる。4 範囲の無線 LAN アクセスポイント通信エリアを図 5 の矢

印に示すような軌跡で移動する。また、住民 (CN) から 1Mbps 相当の通報 Constant Bit Rate パケット (application_damand を利用) を受信し続ける。

- Ground Speed : 30km/h
- Wireless LAN > BSS-ID : 0
- IPv6 > Global Address : 2001:193::2 (= HoA)
- Mobile IPv6 > Node Type : Mobile Node
- Mobile IPv6 > Route Optimization : Enabled

(イ) HA

- Wireless LAN > BSS-ID : 0
- Mobile IPv6 Router Parameters > Interface Type : Home Agent

(ウ) 住民

固定とし、Mobile IPv6 の CN として動作させる。MPB (MN) へ向けて 1Mbps 相当の通報 Constant Bit Rate パケット

(application_damand を利用) を送信し続ける。

- Wireless LAN > BSS-ID : 1
- IPv6 > Global Address : 2001:192::27
- Mobile IPv6 > Node Type : Correspondent Node
- Mobile IPv6 > Route Optimization : Enabled

(エ) CN_Router

- Wireless LAN > BSS-ID : 1

(オ) Foreign_Router_0

- Wireless LAN > BSS-ID : 3

(カ) Foreign_Router_1

- Wireless LAN > BSS-ID : 2

(※) VPS は明確に定義しない。

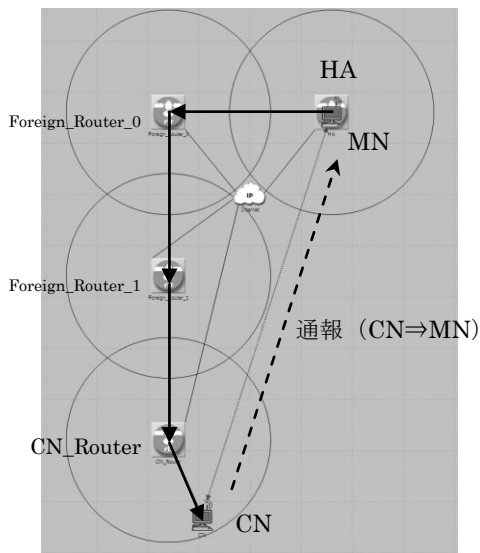


図 5 : シミュレーションモデル

6. 2 シミュレーション結果

シミュレーション結果を以下に示す。シミュレーション時間は 120(sec) である。図 6 は MN でのアプリケーション

オンデマンドトラフィック (= 通報トラフィック) 受信量である。単位 : bytes/sec、Capture Mode : Bucket、統計値総数 : 1200、Bucket Mode : sum/time である。ハンドオーバー時の通信途絶時間以外で約 1Mbps の通報受信を維持している。通信途絶時間は、HA → Foreign_Router_0 間ハンドオーバー時で約 3.8sec、Foreign_Router_0 → Foreign_Router_1 間ハンドオーバー時で約 5.8sec、Foreign_Router_1 → CN_Router 間ハンドオーバー時で約 4.1sec である。

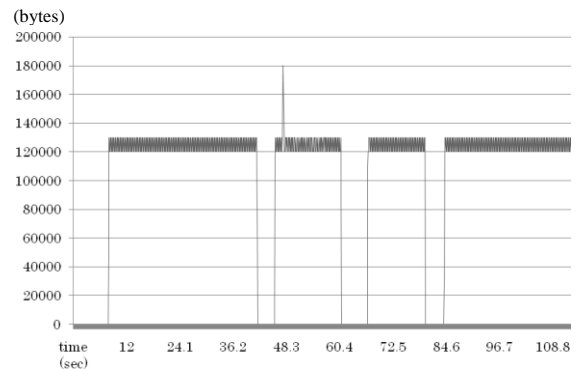


図 6 : シミュレーション結果
Application Demand Traffic Received (bytes/sec)
<CN ↔ MN>

図 7 は 3 系列のデータを同時にプロットしている。3 系列とは以下である。

- MN の Access Point Connectivity (BSS-ID 値)
- MN が送信した Mobile IPv6 Control Traffic [※ バインディングメッセージ、ルータビリティメッセージを含む、単位 : bkts/sec、Capture Mode : Bucket、統計値総数 : 1200、Bucket Mode : sum/time]
- MN が送信した Mobile IPv6 Route Optimization Traffic (pkts/sec) [※ 単位 : bkts/sec、Capture Mode : Bucket、統計値総数 : 1200、Bucket Mode : sum/time]

マーカのない縦線の系列が Access Point Connectivity である。線の上端値が発見したアクセスポイントの BSS-ID 値を表す。-1 はどのアクセスポイントともつながっていないことを表す。最初は HA と同じ 0 である。その後 41.94075sec で途絶する。42.09075sec で BSS-ID : 3 の Foreign_Router_0 をスキャンする (図 7・①の時点)。次に②の時点に注目する。これは MN が送信した Mobile IPv6 Control Traffic (◆マーカの系列) の中で一番最初に送信されたものである。これは MN が移動先ネットワークで CoA を生成し、これを HA へ伝えるためのバインディングアップデートであると考えられる。このときの時刻は約 45.6sec である。つづく③の時点は MN が送信した Mobile IPv6 Route Optimization Traffic (■マーカの系列) の中で最初に送信されるものである。これは、リターンルーティが完了し、経路最適化がなされた最初のトラフィック

を表すと考えられる。このときの時刻は約 47.3sec である。以上をまとめると、最初の HA → Foreign_Router_0 間ハンドオーバは通信が途絶してから L2 コネクションが確立するのに 45.6-41.94075≒3.65925sec の時間を要し、さらに経路最適化を適用した通信を行うまでには 47.3-41.94075≒5.35925sec もの時間を要することがわかる。

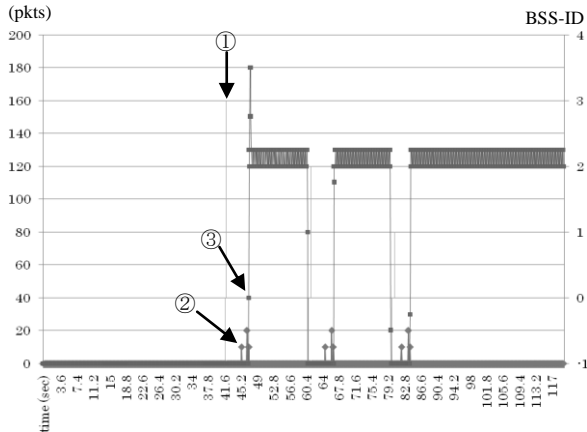


図 7：シミュレーション結果
MN. Wireless Lan. AP Connectivity、
MN. Mobile IPv6. Control Traffic Sent (pkts/sec)、
MN. Mobile IPv6. Route Optimization Traffic Sent (pkts/sec)

以上より、Mobile IPv6 を単体で使用した場合は約 4～5sec の通信途絶時間が発生してしまうということが定量的にわかり、この時間をカバーできるアプリケーションレベルでの通信バスの保持機能が必要となる。また、シームレスなハンドオーバの実現には、やはり基本の Mobile IPv6 の機能拡張を前提としなければならないといえる。

6. まとめと今後の課題

本論文では、ユビキタスネットワーク環境下アプリケーションの一例として、人々が生活するコミュニティの防犯アプリケーション「コミュニティセキュリティシステム」を提案し、前提と定義について考察した。さらに、通信ネットワークシミュレータの活用による定量的評価例を示した。

今後の課題としては、よりシームレスなハンドオーバ（＝円滑な通報機能）を実現するシステムを熟慮し、シミュレータ上で機能拡張をしていきたい。また、同時並行で実装についても検討し、提案アプリケーションの総合的な評価をしていきたい。

謝辞

本研究の一部は平成 19 年度科学研究補助金（基盤研究(C)）の支援を受けて行った。

参考文献

- [1]勝将万,井手口哲夫,奥田隆史,田学軍：コミュニティセキュリティにおけるエージェント間相互作用のモデリングとその評価,電子情報通信学会技術研究報告,Vol.106,No.524,pp.53-58,愛知県立大学(2007-2)
- [2]勝将万,井手口哲夫,奥田隆史,田学軍：Mobile IPv6 を利用したコミュニティセキュリティシステムの特性評価,情報学ワークショップ 2007 (WiNF2007),論文集,pp.43-46,名古屋大学(2007-9)
- [3]MAS コミュニティ「<http://mas.kke.co.jp/>」
- [4]ホームセキュリティ「<http://www.secom.co.jp/service/hs/>」
- [5]無線ネットワークの規格、IEEE802 の全貌「<http://www.atmarkit.co.jp/fnetwork/rensai/ieee01/01.html>」
- [6]ココセコム「<http://www.855756.com/>」
- [7]油原直弘：安全学の構築に向けて,電子情報通信学会論文誌,平成 17 年 5 月 Vol.88 No.5 pp.379-386
- [8]D.Johnson, C.Perkins, J. Arkko, Mobility Support in IPv6, RFC3775, June 2004「<http://www.ietf.org/rfc/rfc3775.txt>」
- [9]金本綾子,鈴木秀和,渡邊晃：Mobile PPC におけるパケットロスレスハンドオーバの提案,マルチメディア,分散,協調とモバイル (DICOM2007) シンポジウム,論文集,pp.866-872,鳥羽(2007-7)
- [10]妙中雄三,榎原茂,塚本和也,門林雄基,尾家祐二：VoWLAN における無線 LAN 再送回数を用いたハンドオーバ制御機構の実装,電子情報通信学会技術研究報告,Vol.106,No.358,pp.79-84,熊本大学(2006-11)
- [11]寺岡文夫,IPv6 インターネットにおける高速ハンドオーバ手法～IP モビリティが拓く次世代 IT～「<http://www.ipc.keio.ac.jp/event/pdf/teraoka20051222.pdf>」
- [12]総務省 電波利用ホームページ「<http://www.tele.soumu.go.jp/j/system/ml/fourth.htm>」
- [13]OPNET Technologies, Inc 「<http://www.opnet.com>」
- [14](株)情報工房・ネットワークシミュレーションソフトウェア OPNET「<http://www.johokobo.co.jp/opnet/index.html>」
- [15]ユビキタス技術 無線 LAN,阪田史郎 編著,オーム社,ISBN4-274-03629-4
- [16]田村大輔,石原進：無線 LAN ハンドオーバー直後の複数ビデオストリームの品質への影響に関する検討,電子情報通信学会技術研究報告,Vol.106,No.498,pp.7-12,広島市まちづくり市民交流プラザ(2007-1)
- [17]大塚裕太,田村大輔,石原進：無線 LAN ハンドオーバーに伴う接続不能期間に着目した TFRC 性能評価,情報処理学会研究報告,Vol.2007,No.44,pp.15-20,沖縄青年会館(2007-5)
- [18]マスタリング TCP/IP IPv6 編,IRI・ユビキタス研究所共著,オーム社