修 士 論 文

アドホックネットワークを応用した電子投票の提案

Proposal of Electric Voting Sytem
over Ad-hoc Network

2008 年　1 月 29 日

指導教員　　相田　仁　教授

東京大学大学院
新領域創成科学研究科 基盤情報学専攻

66328　　杉 谷　心

内容梗概

近年、投票において、開票の迅速性や確実性、資源の節約といった点から、電子投票が注目されてきた。しかし、電子投票の機器はの導入には、投票機代や開票機代、技術料といった多額の費用がかかる。特に、投票の規模が小規模になるほど、費用対効果が悪くなる。

こういったことから、百人程度の人数が一堂に会し、一斉に投票を行う。と、いった投票のモデルを想定した際に、ネットワークのインフラストラクチャを必要としない、安価で手軽にネットワークが構築できるアドホックネットワークが有効であると考えられる。しかし、アドホックネットワークをこのモデルに適応するには、大きく分けてセキュリティ面と無線通信面の2つの問題が挙げられる。(1). 電子投票特有のセキュリティの保持、(2). 一斉に通信を行った場合のコリジョンの多発による通信確度の低下と遅延時間の増大、といった問題である。

そこで本研究では、投票を行う際、セキュリティを維持しつつ通信回数とデータ量の少ない暗号方式の提案と、一斉投票が行われた際に効率よく投票を回収するための通信方式として、リング型の通信プロトコルを提案する。

結論として、投票する端末が、直接サーバに投票データを送信できない場合、つまり、マルチホップ環境下で、投票を行った際、提案手法が投票にかかる時間の面から有効であることが示された。

目次

図目次

表目次

第1章

序論

1.1　はじめに

電子投票という言葉、一度は耳にしたことがあるのではないか。近年、政府において急速にIT化が進展されてきた。そのような中で、選挙事務における投開票等各段階への電子機器の導入は、一度に大量の投票を処理することが困難である現状に対応し、開票の迅速化により選挙の結果を有権者に速やかに知らせるという要請を満たすものであった。

ここでいう電子投票とは、狭義の意味ではタッチパネルや押しボタンを用いて投票を行うことを指す。また、広義の意味では、さらにマークシートやパンチカードによる投票や自宅からのインターネット投票を含むものとする。

電子投票普及協業組合によると、現在、タッチパネルや押しボタンなどを用いて投票を行うといった電子投票は、各地方でTable.1.1のように実施されてきた。

Table 1.1: 選挙の実績

実施年月日	実施場所機関	投票者数(電子投票分)
2005年6月12日	青森県六戸町長選挙	7,193人
2004年11月28日	四日市市長選挙・市議会議員補欠選挙	95,059人
2004年10月24日	新見市岡山県知事選挙・県議会議員補欠選挙	9,798人
2004年2月8日	京都市長選挙（京都府東山区）	15,343人
2004年1月18日	青森県六戸町長選挙	7,118人
2003年7月6日	鯖江市議会議員選挙	34,922人
2003年2月2日	広島市長選挙(広島市安芸区)	29,122人
2002年6月23日	岡山県新見市長選挙・市議会議員選挙	15,066人
2000年6月29日	英国ノーリッジ市　コミュニティパワー選挙	687人

また、インターネット投票については、試験的に米国大統領選挙のアリゾナ州民主党予備選挙で、自宅のパソコンを用いたインターネット投票が実施され、投票率が驚異的にアップしたと報道された。しかし、インターネット投票には、選挙人が自由意志によって投票したかわからないという根本的な問題が存在する。密室での投票は、買収や脅迫の温床になりかねないためである。そのことから、インターネット投票が実現困難であることがうかがえる。

こういった面を踏まえて、総務省は三段階に分けての電子投票の全国的な普及の計画を立てている[13]。そして当面、地方選挙で第一段階での導入をすべきとの見解を示している。

第一段階　選挙人が指定された投票所において電子投票機をもちいて投票する段階

第二段階　指定された投票所以外の投票所においても投票できる段階

第三段階　投票所での投票を義務付けず、個人の所有するコンピュータ端末を用いて投票

する段階

しかし、現状として、投票専用のインタフェースは、購入すると一台四十万円、レンタルで一台十万円前後と高価で、開票機や技術費、さらにはネットワークのインフラストラクチャまで合わせると莫大な費用がかかってしまう。特に、大学の役員選挙といった小規模な投票には、従来の電子投票は不向きである。

そこで、本論文では、コストのかからない投票方式として、個人が所有するコンピュータ端末を持ち込んで、数百人程度規模で一堂に会し投票する場面を想定する。その際に、コストのかからない無線通信技術として、ネットワークのインフラストラクチャを必要としないアドホックネットワークを応用し、セキュリティを維持した電子投票の手法を提案する。

また、アドホックネットワークという無線通信のプロトコルを採用することによるセキュリティ面での不安や、一斉に投票した際の通信の混雑などの問題点が予想されるので、そのような問題点に本論文での提案手法で解決策を提示していく。

1.2　本論文の構成

本論文は、6つの章から構成されている。以下に各章の構成を示す。

第1章

序論として、背景及び研究の動機を説明し、本論文の構成について述べる。

第2章

現在使用されている暗号化についての技術や、無線通信技術の現状について述べる。また、無線通信プロトコルについての関連研究を述べる。

第3章

本論文で提案する暗号化アルゴリズムについて、その詳細を述べる。

第4章

本論文で提案するリング型通信プロトコルについて、その詳細を述べる。

第5章

シミュレーションによる実験を行い、提案手法の有効性を考察する。

第6章

本論文のまとめを行い、今後の課題について述べる。

第2章

研究の背景

2.1　暗号技術

本節では研究の背景として、通信のセキュリティの保持に必要不可欠であり、かつ、電子投票の提案において核となる暗号技術について述べる。

2.1.1　共通鍵暗号

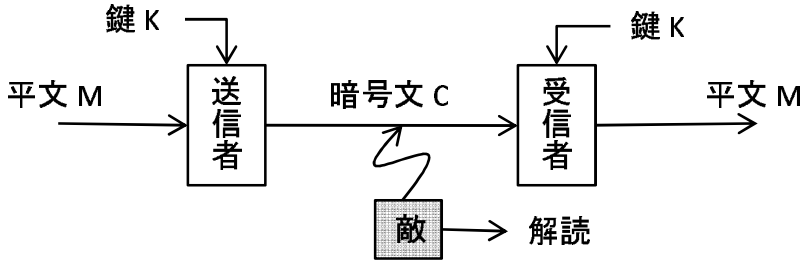

Fig. 2.1: 共通鍵暗号のモデル

送信者と受信者が同じ鍵を秘密に共有する暗号系を共有鍵暗号系という。共通鍵暗号系のモデルを Fig.2.1 に示す。

共通鍵暗号には大きく分けて二種類存在し、ビット単位やバイト単位で暗号化を行う「ストリーム暗号」、ブロックと呼ばれる固定長のデータを単位として暗号化復号を行う「ブロック暗号」が存在する。

ストリーム暗号

平文のビット列 $\mathrm{M} = (b_1, b_2, \cdots)$ を、鍵のビット列 $\mathrm{K} = (k_1, k_2, \cdots)$ を用いて

$c_1 = b_1 \oplus k_1, c_2 = b_2 \oplus k_2, \cdots$

と暗号化する暗号系をストリーム暗号という（Fig.2.2)。ここで、$\mathrm{C} = (c_1, c_2, \cdots)$ が暗号文となる。

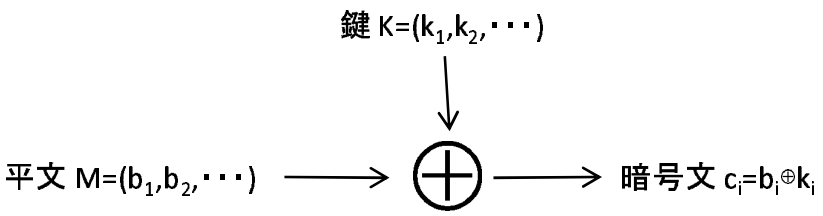

Fig. 2.2: ストリーム暗号のモデル

鍵系列Kを完全なランダムシーケンスとして採用すると、ワンタイムパッド（One Time Pad, OTP）となって情報理論的安全性を持つ。このことは、[9] にて情報理論の考案者で

あるクロード・シャノンが解読不可能であることを数学的に証明している。

また、このワンタイムパッドは、平文と同じ長さの乱数が必要であり、名前の通り通信の度に共通鍵を切り替えなければならないので、通信量と通信回数が大きくなり効率的ではない。特にソフトウエアでは、平文の安全な処理や伝送、真にランダムな鍵、その鍵の一度だけの使用といった、ワンタイムパッド実装の補助的な部分に多くの困難を伴う。

そのため、ワンタイムパッドは広くは採用されていない。

ブロック暗号

ブロック暗号とは、平文のビット列をブロック長と呼ばれるある一定の長さ n ごとに分割し、そのブロック単位で暗号化を行う暗号方式である。

ブロック長と呼ばれる長さ n bit の平文 m をまとめて暗号化する共通鍵暗号系をブロック暗号という。Fig.2.3 に示すように、ブロック暗号の暗号化アルゴリズム E_K は、鍵長と呼ばれる κ bit の共通鍵 K と、n bit の平文 m を入力とし、n bit の暗号文 c $= E_K(m)$ を出力する。平文 m は次式によって計算する。

$D_K(c) = D_K(E_K(m)) = m$

ここで、DK は共通鍵が K の時の復号アルゴリズムである。

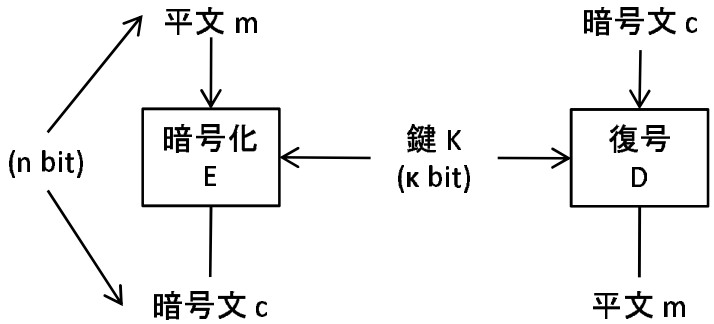

Fig. 2.3: ブロック暗号のモデル

また、ブロック長は 64bit や 128bit が代表的である。暗号アルゴリズムによっては、ブロック長をパラメータで指定でき、ブロック長を変えられるものもある。鍵長は 40/56/64/80/128/192/256bit などがある。

代表的なブロック暗号として、米 NIST が制定した DES (Data Encryption Standard, FIPS PUB 46) や AES (Advanced Encryption Standard, FIPS PUB 197) がある。日本産のブロック暗号としては、MISTY1 や Camellia などが知られている。

2.1.2　公開鍵暗号

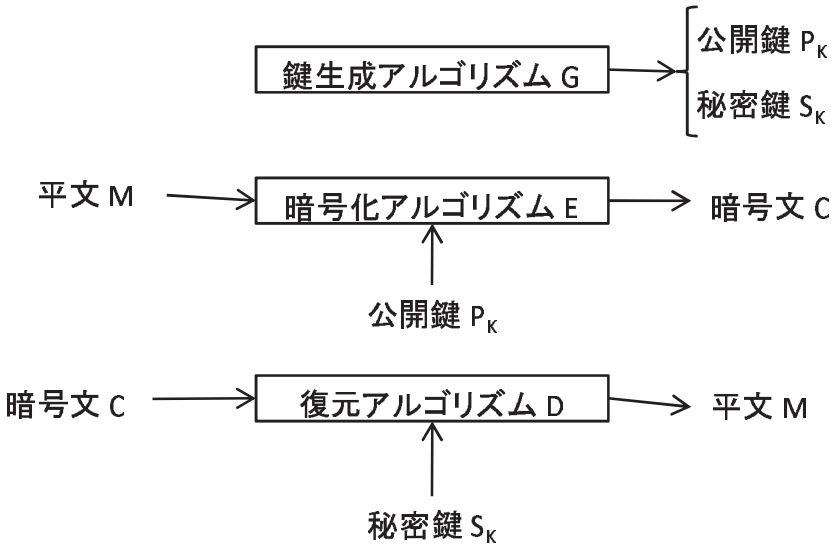

Fig. 2.4: 公開鍵暗号のアルゴリズム

2.2　無線通信技術

本節では研究の背景として、無線通信技術について述べる。

2.2.1　アドホックネットワーク

アドホックネットワークとは、有線通信のインフラストラクチャーや、無線 LAN のようなアクセスポイントを必要としない、無線で接続できる端末 (パソコン、PDA、PHS、携帯電話など) のみで構成されたネットワークのことである。別称として、「無線アドホックネットワーク」、「自立分散型無線ネットワーク」とも呼ばれている。アドホックネットワークでは、広くコンピュータ等の無線接続に用いられている IEEE 802.11x、Bluetooth などの技術を用いながら多数の端末をアクセスポイントの介在なしに相互に接続する形態 (マルチホップ通信 Fig.2.5) を取っている。

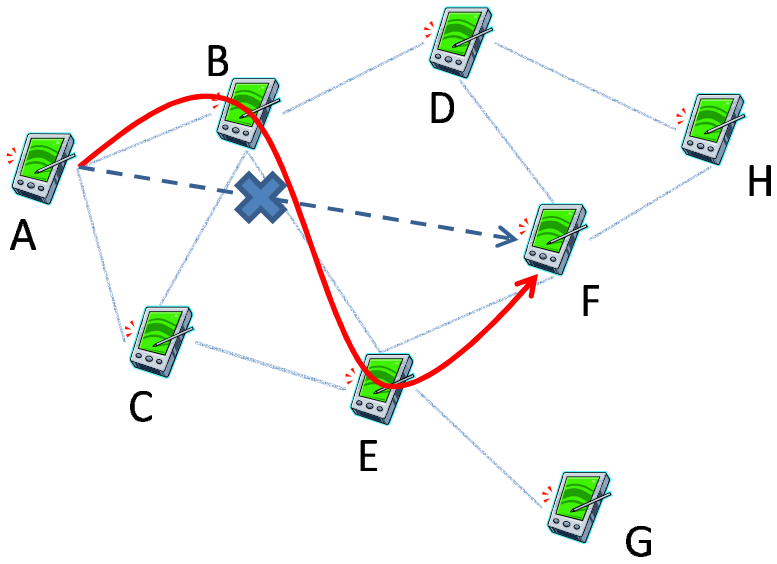

Fig. 2.5: アドホックネットワークにおけるマルチホップ通信

このため、アドホックネットワークでは基地局やアクセスポイントが不要となり、このようなインフラを持たない場所で安価にネットワークを構築することができ、ある限られた域内での簡易なネットワークの構築の手段として有効である。

しかし、現在のところアドホックネットワークの構築には技術的課題がいくつか残されている。アドホックネットワーク内では端末は常に移動し、端末相互間のリンク確実なものではないため、そのような環境でいかに効率よく安定した経路を動的に検出できるか、また、ネットワークの規模と使用する無線の周波数帯域や出力の程度はどう設定すべきか、といった点である。

また、アドホックネットワークに関する研究の歴史は長く、1970 年代当時では、パケット無線ネットワークと呼ばれ、ARPA プロジェクトの一環として軍事利用の観点から研究

が開発されてきた。当時は、ネットワーク全体を集中管理する固定局が使用されていた。

このように、元々インターネットと同じ源から研究が発しており、インターネットの技術標準化を行う組織であるIETFでは、現在アドホックネットワークに関するワーキンググループ(MANET [8])が活動している。特に、ルーティング、マルチキャストに関して各種の方式が提案されている。一方、アドホックネットワーク実現の別の例として、PHSの子機間通信を利用するものがあり、近年、研究開発が行われている。

ルーティング

大きくはテーブル駆動方式（プロアクティブ型）とオンデマンド方式（リアクティブ型）に分類される（Fig.2.6）。

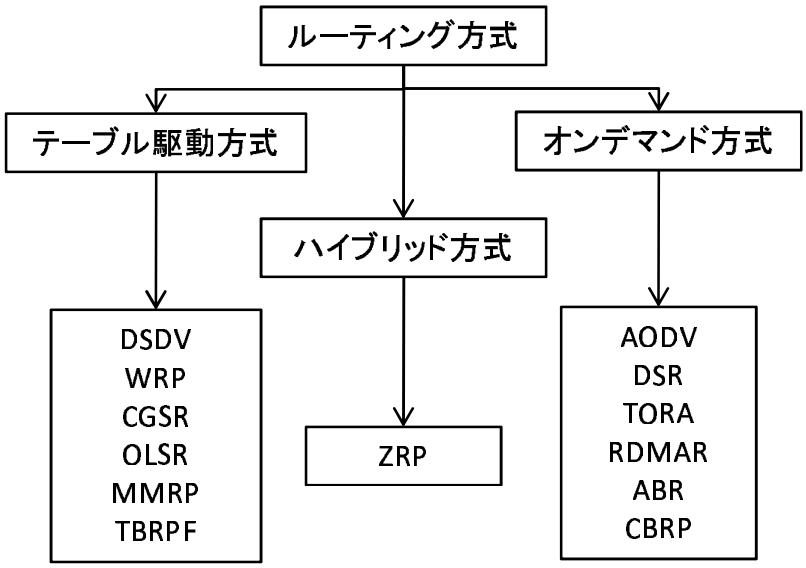

Fig. 2.6: アドホックネットワークにおけるルーティングの分類

2.2.2　IEEE 802.11

IEEE 802.11 とは、無線 LAN（Local Area Network）の標準規格群であり、現在、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g が広く普及している。物理レイヤ規格と MAC レイヤ規格から主に構成され、一つの MAC レイヤ規格で複数の物理レイヤ規格をサポートするのが特徴である。

物理レイヤ

まずは、物理レイヤの各規格について利用周波数帯、伝送速度及び標準化年を Table 2.1 に示す。

IEEE 802.11 は、Local Area とあるように、通信可能距離は約 100m 程度であり、もともとは屋内の一部屋または一フロアなど限られた範囲における通信を対象にした方式である。

Table 2.1: IEEE 802.11

	周波数帯	伝送速度	標準化年
IEEE 802.11b	2.4GHz 帯	11Mbps	1999
IEEE 802.11a	5GHz 帯	54Mbps	1999
IEEE 802.11g	2.4GHz 帯	4Mbps	2003

MAC レイヤ

フレーム衝突の回避のために、CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance) 方式を採用している。CSMA/CA とは、「話す前に聞け」という原理に基づく、アクセス制御方式である。すなわち、自分がパケット信号を送信する際に、まずはアンテナで他の装置がパケット信号を出していないかどうかを、良く確かめてから送信するという極めて単純な機構を採用したアクセス制御方式である。以下に詳しく説明する。

CSMA では、フレーム送信を試みようとするそれぞれの送信局が聞き耳をたてて、無線チャンネルの使用状況を確認し、他の送信局による通信が終わるのを待ってから送信を開始しようとする。このとき、他の送信局との衝突を避けるため、無線チャンネルの使用が終わってから、ある時間だけ待ち時間をおき、送信を開始する。その待ち時間は、最低限の送出間隔である IFS（Inter Frame Space:フレーム間隔）と、乱数により決定されるバックオフ時間 (Table.2.2) 和で決定する。

CSMA/CA 方式は 2.4GHz 帯のように干渉を互いに与えない範囲での独立なチャネルが 4 チャネルしか取れない場合に、自分以外のアクセスポイントが自律分散的に動作させる上で、実際的なアクセス制御方式である。また、この後に繋がる一連の無線 LAN 発展の基礎をなす概念となっている。

Table 2.2: バックオフアルゴリズム

順序	処理内容
1	衝突の検知
2	ジャム信号の発生
3	乱数 r の発生
4	2^r 時間沈黙
5	再送（再度衝突した時は前回の 2 倍沈黙）

2.3　関連研究

2.3.1　無線 LAN におけるトークンパッシング方式の適応

従来、無線 LAN アクセス制御方式として、CSMA 方式 [10] や、ポーリング方式 [11] などが提案されてきた。しかし、これらの手法はいずれも伝送効率や遅延時間の面でいくつかの問題点を抱えている。そこで、無線 LAN におけるトークンパッシング方式が提案されている。

トークンパッシング方式とは、有線 LAN のアクセス制御方式の一つであり、トークンと呼ばれる「送信権」データがネットワークを常に周回し、これを取り込んだ端末がデータを送信する方式である。

IEEE 802.4 におけるトークンバス方式や、IEEE 802.5 におけるトークンリング方式なので利用されている技術である (Fig.2.7)。これは、有線 LAN の MAC 層でのアクセス制御方式において、IEEE 802.3 における CSMA/CD 方式と並んで広く採用されてきた。

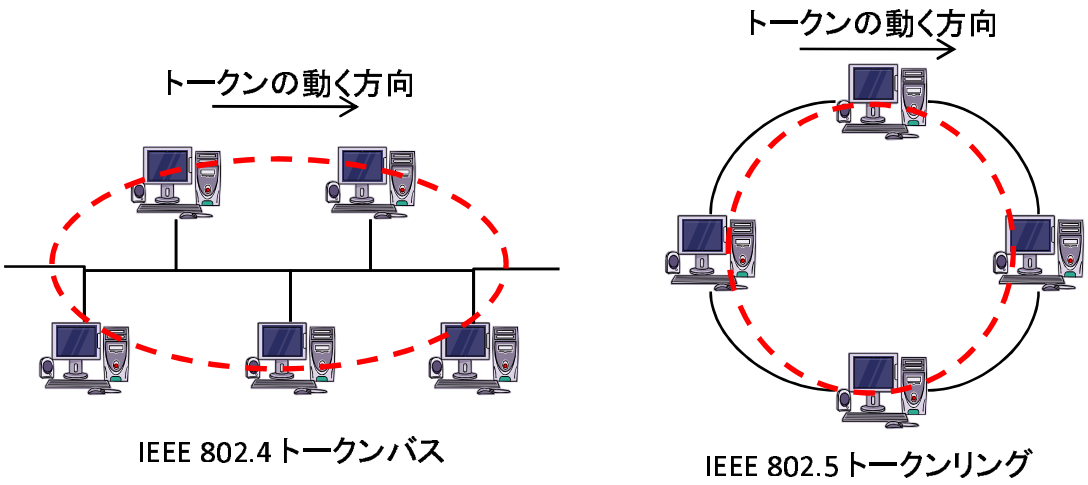

Fig. 2.7: IEEE 802.4 & IEEE 802.5

ここで、無線 LAN におけるトークンパッシング方式と基準となっている IEEE 802.11b で採用されている CSMA/CA を比較し、考えられる無線 LAN におけるトークンパッシング方式のメリットデメリットを以下に示す。

メリット

- 原理的に隠れ端末問題が発生しない
- 高負荷時にも安定した性能が得られる

デメリット

- トークン紛失に伴う制御が複雑

- 障害が大きくなると遅延時間が指数関数的に増加する

ここで問題点として挙げられることは、無線LANにおけるトークンパッシング方式は、前述したように元来有線LAN用のアクセス制御方式であるため、トークンがほとんど紛失しないことを前提としていることである。このため、トークン紛失時にはトークン再構成処理やノード離脱処理など複雑な制御が必要となる [12]。

無線伝送路では、一時的な通信路障害が頻繁に発生するため、トークンの紛失確率は有線LANと比較するとはるかに高い。したがって、このような環境下で有線LAN用のトークンパッシング方式を適用すると、スループット、遅延などの面で大きな性能の劣化を生じることが予想される。そのため、無線LANにおけるトークンパッシング方式の実現には、トークンの紛失にたいする制御が必要不可欠なものと考えられる。

以下に、トークン紛失の際の性能向上について述べた論文を挙げる。

DTP (Direct Token Passing) 方式の提案

トークン紛失の際の制御として、[5] にて DTP (Direct Token Passing) 方式が提案されている。この DTP とは、以下の 2 つの手法が用いられていることが特徴である。

(1) 論理予備リングによるトークン巡回手法

(2) データ代送依頼によるデータ中継手法

(1) 論理予備リングによるトークン巡回手法

トークンの巡回経路を固定化せず、複数パターンの論理予備リングを用いてトークンを巡回させる方式である。つまり、論理リング（トークンの巡回経路）初期化の段階であらかじめ複数パターンの論理リングを作成しておき、論理リング内でトークンの障害が発生した場合には、あらかじめ用意してある予備のリングに切り替えることにより、トークンの巡回を再開する。

Fig.2.8 に示すように障害発生時に論理リング自体が形を変えるため、論理リングが障害物を避けることができることから、トークン巡回経路固定の既存トークンパッシング方式と比較して障害物の影響を大幅に低減することができる。

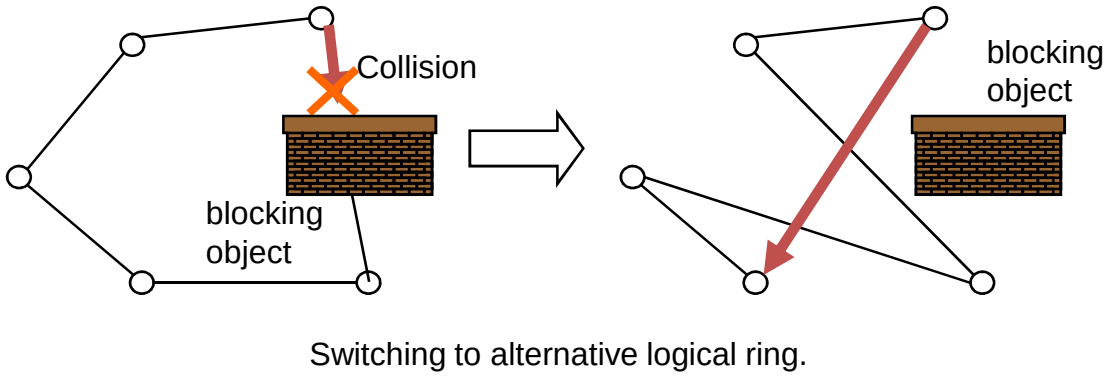

Fig. 2.8: 動的な論理リングの変更

(2) データ代送依頼によるデータ中継手法

Fig.2.9 に示すように、データが障害物に衝突して紛失した場合、宛先のノードと通信できる他のノードにデータの代送を依頼する方式である。

無線 LAN では、あるノードがデータを伝送するとき、そのデータは原理的に論理リングに加入するすべてのノードにブロードキャストされ、各ノードはすべてのデータを一時的にバッファに保存する。紛失したデータの送信元ノードはトークンにデータ代送依頼の情報を付加して送信し、データ代送依頼を受け取ったノードはバッファより代送するデータを取り出すことにより代送を行う。

この手法を用いることで、障害物のない伝送路にデータを中継することができ、障害物によるデータ再送の回数を大幅に減少させることができる。

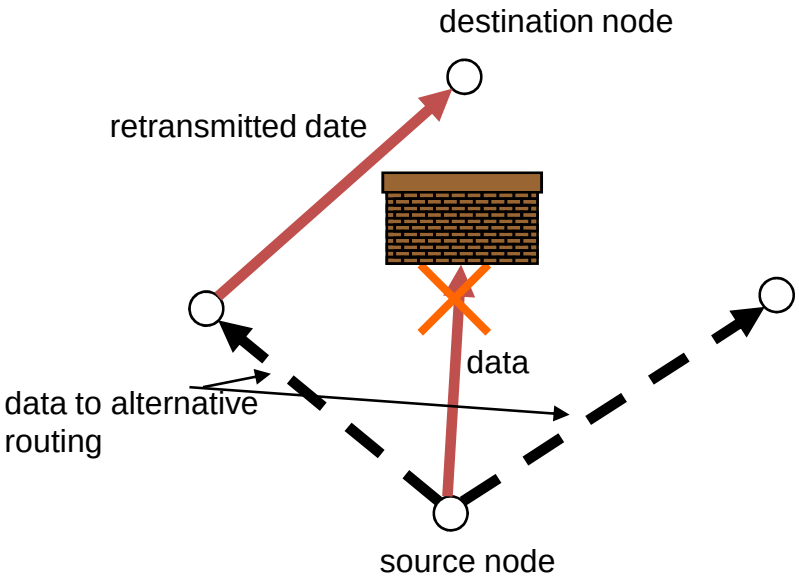

Fig. 2.9: データ中継

この手法の問題点は、あらかじめ複数の予備リングを用意するということは、端末の加入・離脱時に全端末で同期を取る必要があり、端末台数が固定でないと実現が困難な点である。これでは、端末の加入・離脱に伴うトークン巡回路の変更ができない。

無線トークンパッシングLANの提案

有線トークンパッシングLANの無線への適応として、[6]にて無線トークンパッシングLANが提案されている。この提案手法では、以下の2つの対応が述べられているのが特徴である。

(1) トークンリングへの端末の加入

(2) トークンリングからの端末の離脱

(1) トークンリングへの端末の加入

第3章

無線端末での電子投票向け
セキュリティ方式の提案

3.1　求められるセキュリティ条件

一般的に、電子投票でのプロトコルは、以下の6つの条件を持つことが理想とされている。

1. 有権者しか投票できない
2. みんな2回以上は投票できない
3. 他の誰が誰に投票したかは、誰にもわからない
4. だれも他人の票を複製できない
5. だれにも見つからずに他人の票を書き換えられない
6. すべての投票者は、自分の票が最終的な表決で考慮されたことを確認できる

して、各要所で提案するセキュリティ技術について詳しく述べる。最後に、セキュリティプロトコルを上記の6つの条件と比較し、評価する。

なお、前提条件として、各投票者の公開鍵とサーバの公開鍵は公開されているものとし、サーバは各投票者のIDのリストを所持しているものとする。

3.2　投票の流れ

投票の流れを Fig.3.1 に示す。

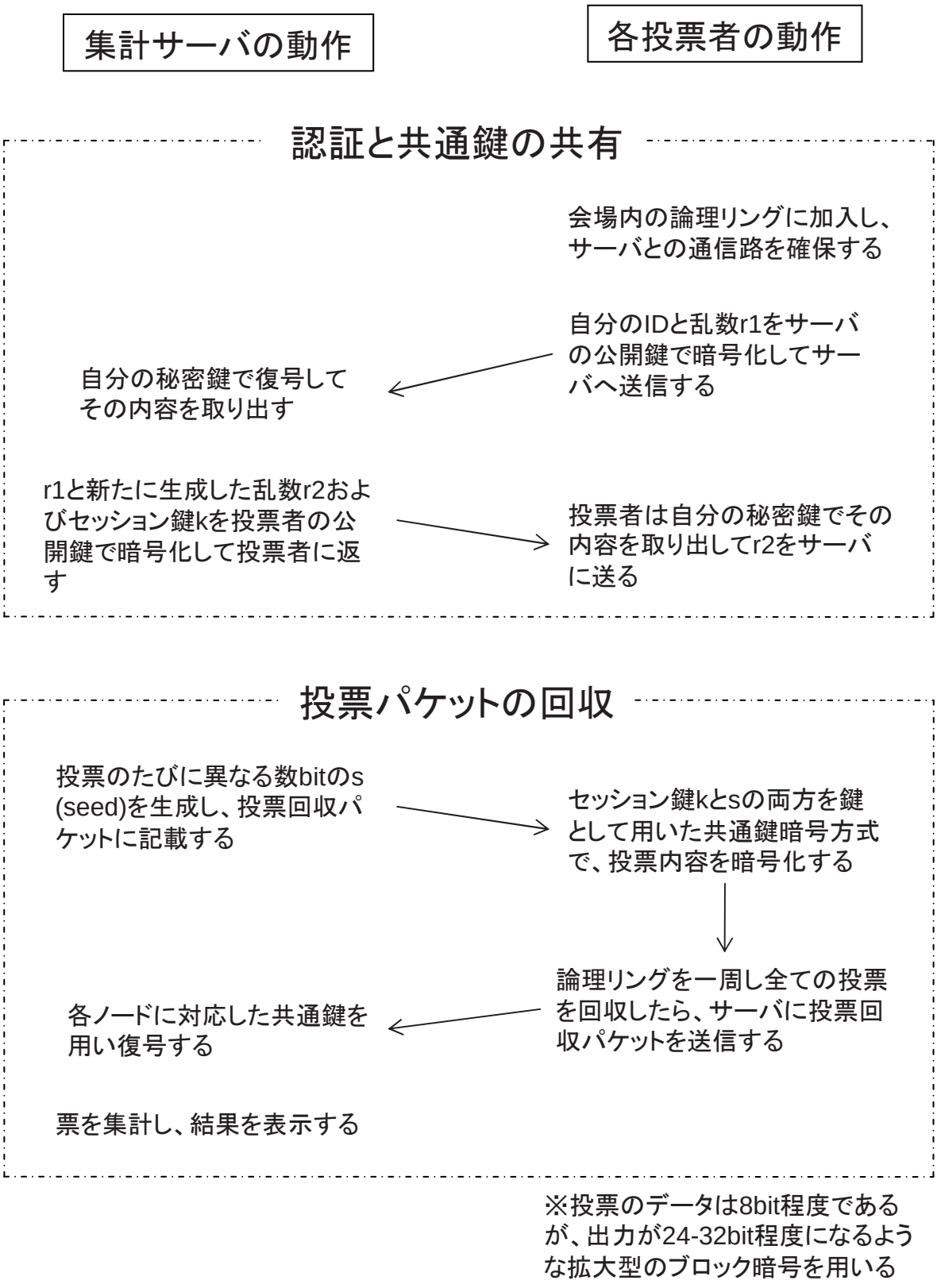

Fig. 3.1: 投票の流れ（セキュリティ）

3.3　セキュリティプロトコルの提案

本節では、前節で提案された投票の流れで、要となるセキュリティプロトコルの詳細を説明する。

3.3.1　ユーザ認証

投票者の端末は会場内の論理リングに加入し、サーバとの通信路を確保する。投票者は、有権者であることをサーバに示すための自身の ID と、投票を暗号化するために用いる乱数 r1 を、サーバの公開鍵で暗号化してサーバへ送信する。サーバは、有権者に対して、セッション鍵を共有するため、自分の秘密鍵で復号してその内容を取り出し、r1 と新たに生成した乱数 r2 およびセッション鍵 k を投票者の公開鍵で暗号化して投票者に返す。投票者は自分の秘密鍵でその内容を取り出して r2 をサーバに送ることで、有権者とサーバが相互に認証するとともにセッション鍵を共有する。

こうして、有権者であることの認証と、投票の暗号化で用いるセッション鍵を共有することができる。

3.3.2　seed 組み込みによる共通鍵暗号方式の改善

投票のパケット自体は、とても小さく 1 オクテット程度である。各有権者の投票を回収する際には、リング型のプロトコルで行う。また、サーバは投票のたびに異なる数 bit の s (seed) を生成し、票回収パケットに記載する。クライアントは、セッション鍵 k と s の両方を鍵として用いた共通鍵暗号方式で、投票内容を暗号化する。この際、投票のデータは 8bit 程度であるが、出力が 24-32bit 程度になるような拡大型の暗号を用いる。

3.4　セキュリティプロトコルの評価

本節では、3で提案されてきたセキュリティプロトコルについて、3.1で書かれた条件と照らし合わせ、評価していく。

1. 有権者かどうかは、最初に有権者の公開鍵基盤を用いて確認されているので、条件を満たす。
2. サーバがどの端末を誰が使用しているか把握しているため一つの端末からは一度しか投票ができない。また、一人の投票者が複数の端末より投票しているのも容易に検出できる。よって条件を満たす。
3. 投票者一人一人の共通鍵は違うので、他の有権者の投票を見ても、復号ができない。また、毎回サーバより送られてくるsは毎回違うので、前回と同じ投票をしたとしても検出できない。よって条件を満たす。
4. 投票者一人一人の共有鍵は違うので、複製しても同じ票にならず、サーバがエラーを認識する。よって条件を満たす。
5. 8bitの投票内容を24〜32bitに拡大しているので、書き換えが行われたときにサーバがそれを見逃す確率は$2^(16)$〜$2^(24)$である。これは、実用的には十分と思われる。よって条件を満たす。
6. 投票されたパケットを集計後サーバがもう一度回すことによって、各投票者は自分の投票がサーバに正しく届いたことは確認できる。ただし、集計結果に正しく反映されているかどうかはこれだけでは判断できない。

第4章

投票回収パケットの通信方式の提案

4.1　提案手法の概要

従来の通信プロトコルでは、数百人単位で一斉に投票が行われた場合に、コリジョンが多発し、遅延時間の増加やスループットの低下、パケトロスレートの増加といった障害を招くと考えられる。

そこで、Fig.4.1 のように、リング型に経路を構築し、アクセスを制御することにより、通信効率を向上させる。

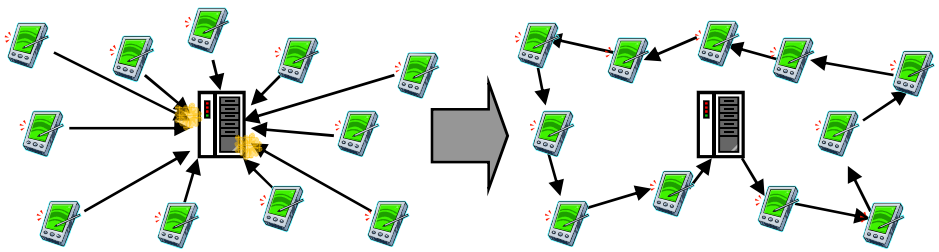

Fig. 4.1: 従来手法との比較のイメージ

サーバが投票回収パケットを次ノードに送信し、受け取ったノードは自分の投票を投票回収パケットに反映させ、次のノードに送信する。このようにして、全てのノードの投票を反映させた投票回収パケットをサーバが受信し、投票完了となる。ノード数が投票ノードが 5 つの場合を Fig.4.2 に示す。

4.2　リング型経路構築アルゴリズム

この節では、リング型経路構築のアルゴリズムを説明する。

4.2.1　フローチャート

巡回セールスマン問題の解決策の一つである、最近追加法を応用したアルゴリズムである。経路構築における、ループ加入希望のノードの動きをフローチャート Fig.4.3 に示す。

4.2.2　各場面での動き

各ノードにおける、次ノードを successor、前ノードを predecessor と呼ぶこととする。

4.2.3

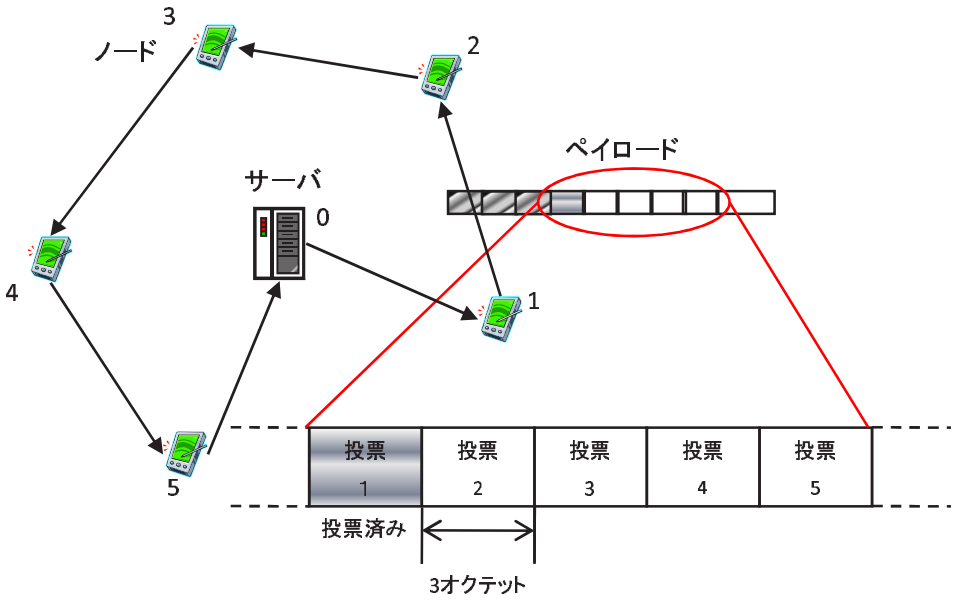

Fig. 4.2: ノードが 5 つの場合

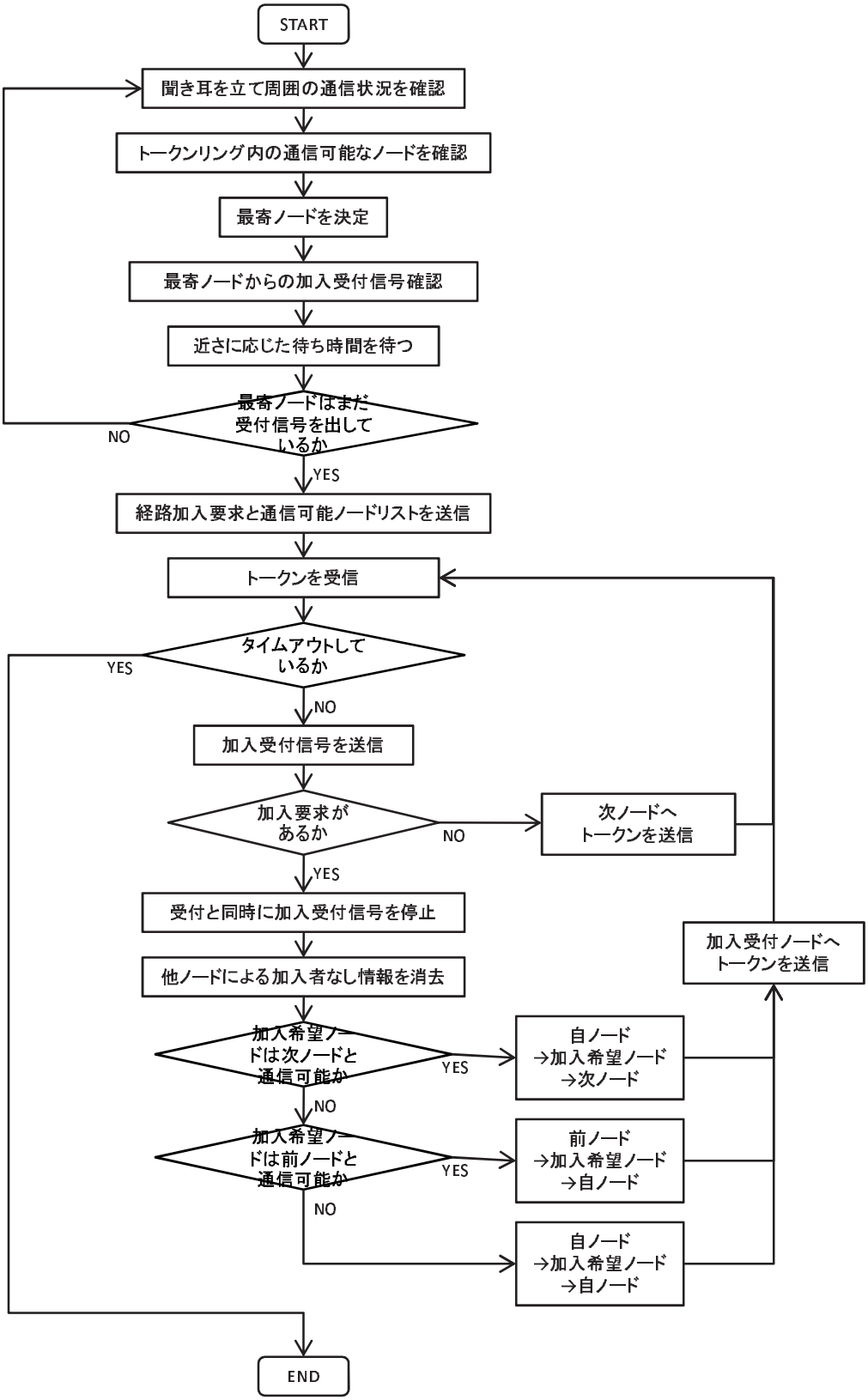

Fig. 4.3: 経路構築のフローチャート

第5章

シミュレーションによる提案手法の評価

従来手法として、ルーティングは、プロアクティブ型のルーティングである Bellman-Ford 方式を用いてシミュレーションを行う。提案手法は、静的なルートを設定した。

ノードが一斉に経路構築要求を開始した場合、コリジョンが多発し経路が構築できない。具体的にはノード数が 36-49 で通信経路の構築ミスが発生する。

そのため、経路構築は、1 秒ごとに端末が経路構築要求を出すものとする。

5.1　ノード数と投票にかかる時間

Table 5.1: シミュレーションパラメータ

シミュレーションエリア	20m × 20m
ノード数	25, 36, 49, 64, 81, 100
通信可能距離	30m
シミュレーション時間	300s
最大通信速度	11Mbit/s
データパケットサイズ	24
経路構築パケット送信間隔	1s
MAC プロトコル	802.11

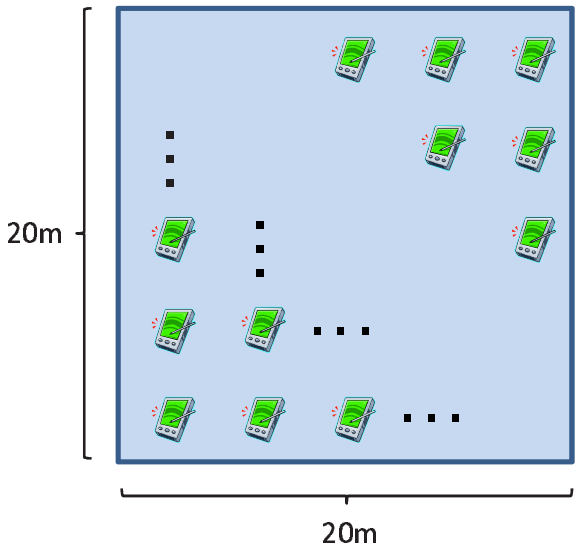

Fig. 5.1: ノードの配置

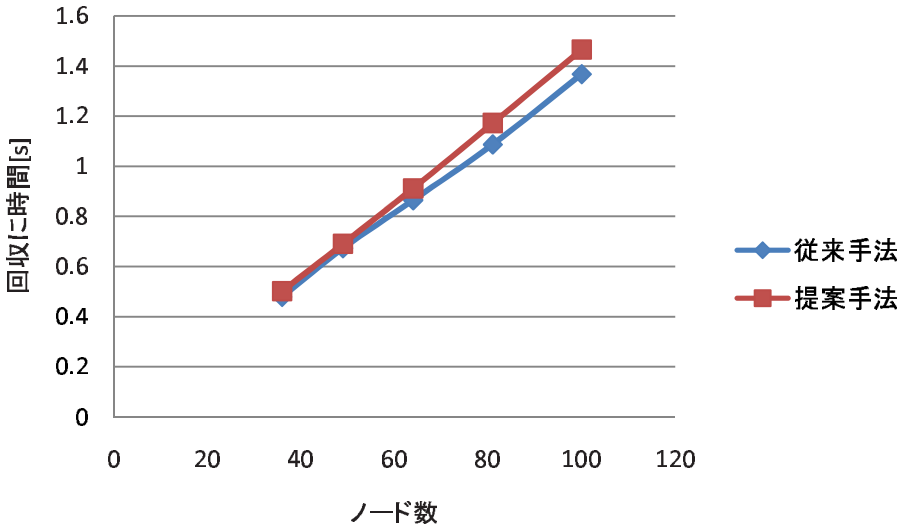

Fig. 5.2: ノード数と通信完了にかかる時間の関係

5.2　ホップ数と投票にかかる時間の関係

5.2.1　メッシュ状の配置

Table 5.2: シミュレーションパラメータ 2

シミュレーションエリア	20m × 20m, 50m × 50m, 〜
ノード数	100
通信可能距離	30m
シミュレーション時間	300s
最大通信速度	11Mbit/s
データパケットサイズ	24
経路構築パケット送信間隔	1s
MAC プロトコル	802.11

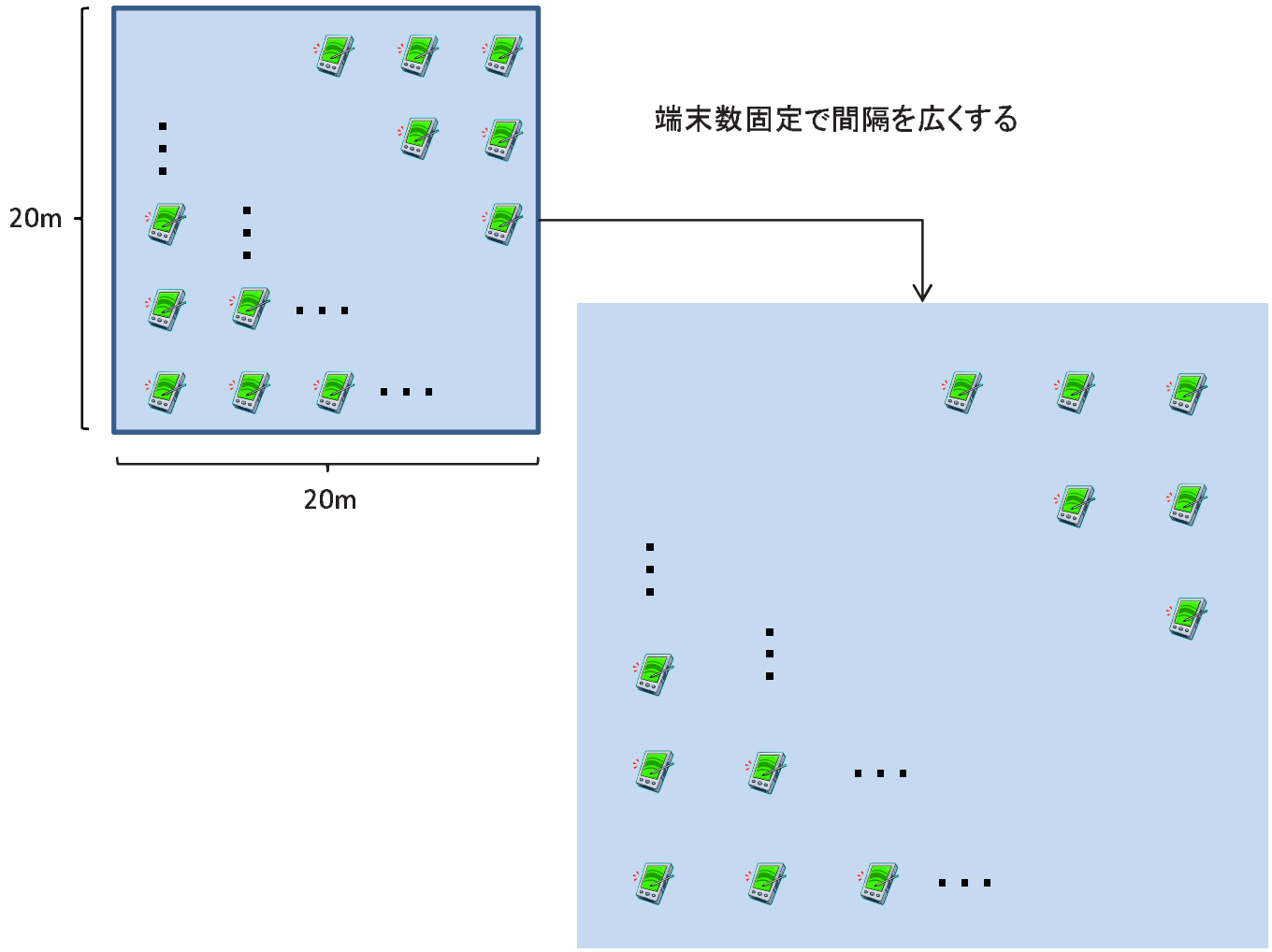

Fig. 5.3: マルチホップ時の投票にかかる時間

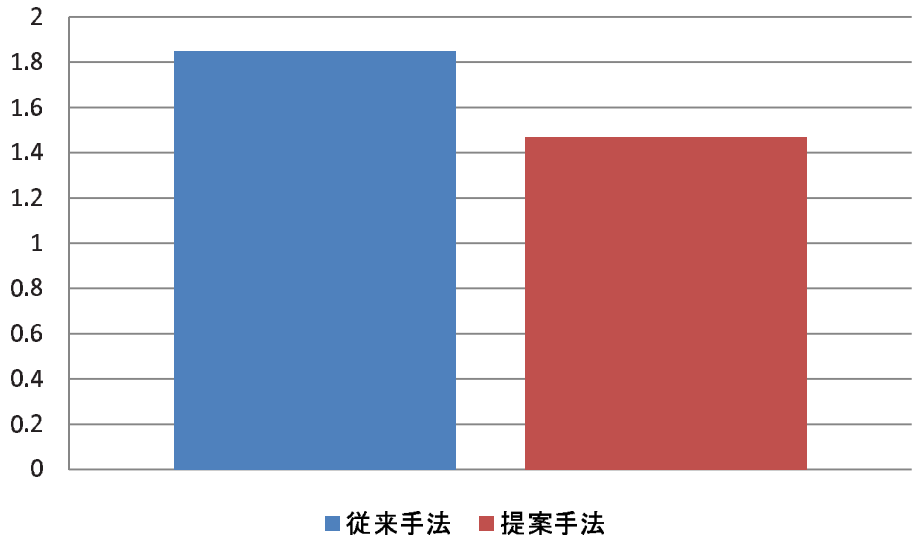

Fig. 5.4: 50m 四方の時の投票にかかる時間の対比

5.2.2　ランダム配置

5.3　通信が集中するノードが存在する場合の動作

Table 5.3: シミュレーションパラメータ 3

シミュレーションエリア	20m × 20m の二部屋
ノード数	100 × 2
通信可能距離	30m
シミュレーション時間	300s
最大通信速度	11Mbit/s
データパケットサイズ	24
経路構築パケット送信間隔	1s
MAC プロトコル	802.11

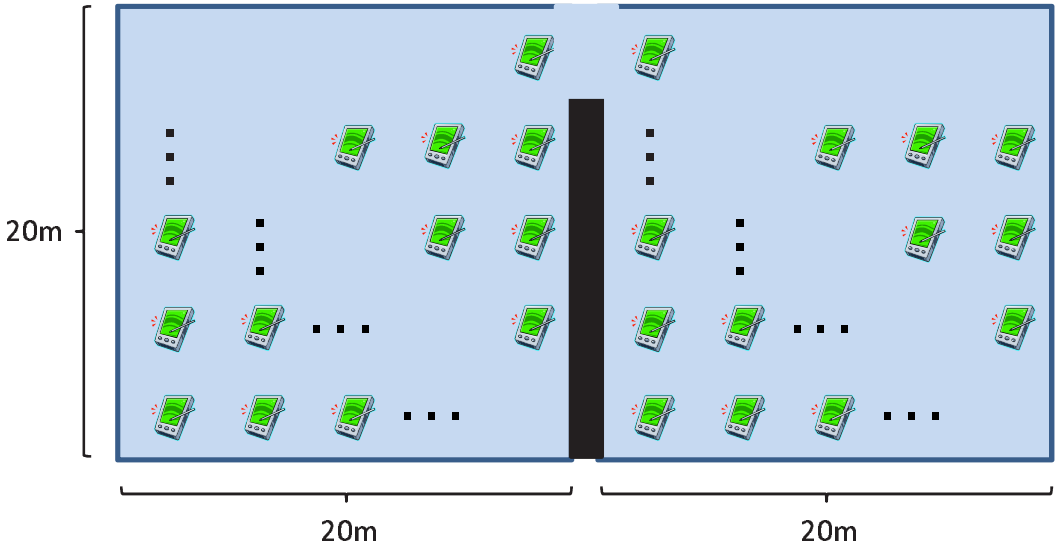

Fig. 5.5: 二部屋での投票

第6章

結論

6.1　まとめ

すべてのノードがシングルホップでサーバへ通信が届かないような場合、提案手法は従来手法より、投票の回収にかかる時間が短くなる。

高密度での通信にも対応できるが、すべてシングルホップで通信できるなら、通常のトークンバスのような方式の方が有利である。

6.2　今後の課題

6.2.1　提案したルーティングのシミュレータへの実装

謝辞

本論文は、非常に多くの方のお力を借りることにより、書き上げる事ができました。

相田 仁教授には、本研究のテーマの立案から、提案手法の検討、結論にいたるまで、貴重な意見やアドバイスを多数いただきました。また、研究を行う素晴らしい環境も与えていただきました。深く御礼申し上げます。

技術職員の千葉 新吾氏、秘書の中山 早百合女史、助教の藤枝 俊輔氏、博士課程の神堀 真也氏におかれましては、研究を行う上での生活面について特にお世話になりました。感謝いたします。

同期のアピラックウィリヤ ウィッタヤー氏、佐伯 嘉康氏、藤原 直弘氏におきましては、互いに切磋琢磨し研究に対するモチベーションを高めてきました。また、それだけでなく、私の研究が行き詰った時に、解決策をともに考察してもらい、打開することができました。感謝するとともに、嬉しく思います。

最後に、研究室の皆様、同期の友人達、様々な面で支えてくれた家族に、感謝いたします。

本当に、ありがとうございました。

2008 年 1 月 29 日

参考文献

[1] ブルース・シュナイアー 著，山形 浩生訳, “暗号技術大全,” ソフトバンクパブリッシング，2005.

[2] 黒沢 馨, 尾形 わかは 著, “現代暗号の基礎数理,” 電子情報通信学会, 2004.

[3] Andrew S. tanenbaum 著, 水野 忠則, 相田 仁, 東野 輝夫, 太田 賢 訳, “コンピュータネットワーク,” ピアソン・エデュケーション, 1996.

[4] C.-K. Toh 著, 構造計画研究所 訳, “アドホックモバイルワイヤレスネットワーク,” 2003.

[5] 齊藤 忠夫, 相田 仁, 青木 輝勝, 日高 宗一郎, トラナウィカライ トリデージ, 橋本 昭則, “無線 LAN におけるシャドーイングを考慮した分散型アクセス方式,” 電子情報通信学会論文誌 B, vol.J83-B, no.2, pp.175-184, 2000.

[6] 首藤 敏, “無線 LAN アクセス制御方式の研究,” 研究報告, 情報制御 第 59 号, 日立京浜工業専門学院, 1999.

[7] Scalable Network Technologies,Inc - QualNet, http://www.scalable-networks.com/.

[8] Mobile Ad-hoc NETwork - MANET, http://www.ietf.org/html.charters/manet-charter.html

[9] Shannon, Claude. “Communication Theory of Secrecy Systems,” Bell System Technical Journal, vol. 28(4), pp. 656-715, 1949.

[10] B.P. Crow, I. Widjaja, J.G. Kim, and P.T. Sakai, “IEEE 802.11 wireless local area networks,” IEEE Commun., pp.116-126, Sept.1997.

[11] K.-C. Chen, “Medium Access Control of Wireless LANs for Mobile Computing,” IEEE Network, vol.8, no.5, pp.50-63, Sept./Oct. 1994.

[12] IEEE, “IEEE Recommended Practice for Use of Unshelded Twisted Pair Cable (UTP) for Token Ring Data Transmission at 4Mb/s,” IEEE Std. 802.5b 1990, 1991.

[13] 総務省: “電子機器利用による選挙システム研究会報告書,” Feb. 2002.

[14] 片下 敏宏, 前田 敦司, 山口 喜教, “電子情報通信学会余剰 FF と位相シフトロックを利用した FPGA 回路の低消費電力実装手法,” 電子情報通信学会論文誌 D-I, Vol.J88-D-I, No.7, pp.1132-1142, 2005.

[15] Ting-Chao Hou, Chien-Yi Wang, and Ming-Chieh Chan, “A Token-based Distributed Sceduling for Mesh Networks with Chain Topologies,” IEEE AINA, 2006.

発表文献

[16] 杉谷 心, 相田 仁, “アドホックネットワークにおける電子投票向け通信プロトコル,” 電子情報通信学会ソサイエティ大会, B-7-74, 2007.

[17] 杉谷 心, 相田 仁, “アドホックネットワークにおける電子投票向けデータ形式の提案,” 電子情報通信学会総合大会, 2008（予定）.