Vol.2011-CSEC-55 No.6
2011/12/5

Ad-hoc Network における マルチパーティプロトコルを用いた 匿名通信方式

上口　優太[††]　　笹瀬　巌[†]

概要: 本論文では，Ad-hoc Network において電波強度を用いたルーティングによって木構造 DC-net (Dining Cryptographers network)を構築し，マルチパーティプロトコルを適用することで，各ノードの投票内容を秘匿にすることが可能な匿名通信方式を提案する. 本方式では, 木構造 DC-net を用いることで，段階的な処理が可能となり，参加者が増加した場合に計算量が増大するというマルチパーティプロトコルの問題点を緩和することが可能となる．また，木構造化により中間ノードは末端ノードの総計に加算する形になるため，中間ノードは自身の保有する情報を直接他のノードへ知らせる必要がなくなり，匿名性を保証することが可能となる．しかしながら，末端ノードが全て同じ票数を持った場合など，特定の条件下で匿名性を保証できない場合がある．そこで，末端ノードの票にダミー情報を付け加えることで，この問題を解決する．また，匿名性およびノードの処理時間について評価を行い，本提案の有効性を示す.

Anonymous Communication with Multi Party Protocols in Ad-hoc Network

Yuta Kamiguchi[††] and Iwao Sasase[†]

In this paper, we propose an anonymous communication with multi party protocols in ad-hoc network to keep secret of vote's contents at each node. In our proposal, we use a tree-structured DC-net (Dining Cryptographers network), and computerize in stages to solve the problem of multi party protocols that amount of calculation grows with the participants swell. We can keep secret of interlevel nodes, because each node knows only total value of under nodes. However it can't keep a secret in some cases where all tail end nodes have same values. We solve this problem with adding dummy information. Anonymity and processing time evaluation show the availability of our proposal.

1. はじめに

近年，ユビキタス社会を支える技術として，ノード同士が協調しあい自律分散的に柔軟なネットワークを構築するアドホックネットワーク(Ad-hoc Network)が注目されている1)．自立分散制御に基づくAd-hoc Networkは，拡散性や耐障害性に優れ，例えばノード数が常時変化している場合においてもネットワークの維持が可能であり，また，中継ノードとして選択されていたノードが電力不足で使用できなくなる場合においても，他のノードが新たな中継ノードとなることにより通信の再開が可能である，といった特徴を持つ．これらの特徴を生かし，Ad-hoc Networkは基地局などのインフラがない災害現場やイベント会場において，ノード同士が即興でネットワークを構築し，情報の収集や管理を行う，といった使用方法が期待されている．

また，インターネットの普及に伴い，近年個人情報の流出などプライバシーの確保が重要となりネットワークユーザの匿名性を保護するために様々な匿名通信の研究が行われている2)．匿名通信は，電子投票やネット上でのアンケートなどにおいて利用が期待されており，様々な暗号技術やルーティング方式を組み合わせることで実現されている．従来，足し算のみを用いて実現することが可能な匿名通信路としてDC-net (Dining Cryptographers network)3)4)が，自身の保有する情報を秘匿にしたまま情報の共有，計算を可能にする匿名通信プロトコルとしてマルチパーティプロトコル5)6)が注目されてきた．

DC-netはユーザ同士が協調することで票数を共有し，その値をサーバへ送ることで送信元の匿名性を保証することが可能となる．DC-netは，足し算のみで実現することが可能なため構築が容易であることや，送信元匿名性を保証することができるという利点がある反面，ユーザ同士で協調が必要なため，ユーザ間の匿名性が保証されないという欠点がある．

マルチパーティプロトコルは，匿名通信プロトコルの一種であり，参加者が自身の保有する情報を秘匿にしたまま他の参加者と保有する情報を共有し，その共有した情報を秘匿にしたままその情報を用いて4. 1章で述べるような計算を可能にするプロトコルである．マルチパーティプロトコルは，自身の持つ情報を直接協調する相手に知らせることを防止する紛失通信や，自身の持つ情報の中身を秘匿にしたまま，情報を持っている証明を可能とするゼロ知識証明の上に成り立つプロトコルであり，強度の匿名性を持つプロトコルとされている．しかし，参加者が増える事により計算量が増大することから，大規模な通信には不向きであり，数人規模の小さな通信での利用が期待されている．

一方でAd-hoc Networkは，教室やイベント会場でも即興で構築されるネットワーク

† 慶應義塾大学理工学研究科開放環境科学専攻
†† kamiguchi@sasase.ics.keio.ac.jp

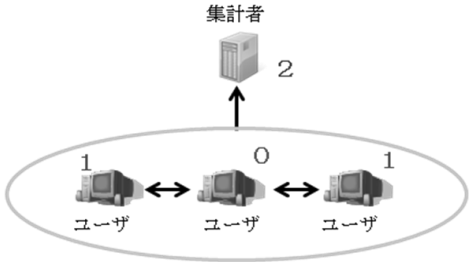

図1 DC-netの動作例

であり，Ad-hoc Networkを用いてその場でアンケートを取るといった使用方法も十分に考えられる．しかしながら，Ad-hoc Networkはノード同士が協調し合うことで構築されるネットワークであるがために，他のノードによるアンケート結果の盗聴やアンケートの送信者がどのノードであるか特定されてしまう恐れがある．そこで，Onion Routing2)7)8)やMix-net9)10)，Clique Net4)，Crowds11)など暗号化やルーティングにより通信内容を秘匿にすることで，上記の問題を解決するAd-hoc Networkにおける匿名通信が注目されている．Ad-hoc Networkとインターネットでは，ルーティングや有線/無線など様々な点で異なるため，Ad-hoc Networkに適した形で匿名通信方式を考える必要がある．DC-netをAd-hoc Network上で実現するには，最終的に票を回収する集計ノードを起点として木構造をとることが望ましいと考えられる．しかし，木構造DC-netにおいても協調による匿名性の問題や，末端ノードで票数が偏った場合に匿名性が保証されないといった問題がある．

そこで本論文では，Ad-hoc Networkにおいて中継ノードの匿名性を保証するために，電波強度を利用したルーティングによって木構造DC-netを構築し，マルチパーティプロトコルを利用することで，各ノードの投票内容を秘匿にすることが可能な匿名通信方式を提案する．本方式では，木構造DC-netを用いることで，段階的な処理が可能となり，参加者が増加した場合に計算量が増大するといったマルチパーティプロトコルの問題点を緩和することができる．また，中間ノードは末端ノードの総計に加算する形になるため，中間ノードは自身の保有する情報を直接他のノードへ知らせる必要がなくなり，匿名性を保証することが可能となる．しかしながら，末端ノードが全て同じ票数を持った場合など，特定の条件下で匿名性を保証できない場合がある．そこで，マルチパーティプロトコルを木構造DC-netに適する形で利用する．本提案では，木構造化により部分木ごとの段階的な処理を可能とし，末端ノードのみが自身の保有する情報にダミー情報を付け加えることにより，全てのノードの匿名性の保証を可能とする．

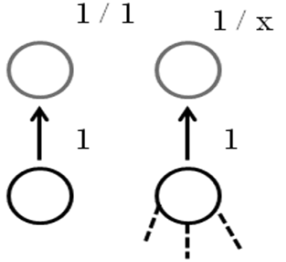

図2 末端ノードと中間ノードの違い

以降，2 章では DC-net の動作，マルチパーティプロトコルの動作について説明をする．3 章では Ad-hoc Network における木構造 DC-net を取り上げ，その問題点を述べる．4 章では提案方式について述べる．5 章では提案方式の評価を行い，最後に 6 章で本稿をまとめる．

2. 関連研究

2.1 DC-net3)4)

本章では，DC-net の動作について説明する．DC-net は元々インターネット上で利用されている匿名通信路である．DC-net では基となる集計者がユーザのルーティングを行い，そのルーティングに基づいたグループを用いてユーザは自身の持つ情報を他のノードと相互に通信を行い共有する．その後，共有した値を加算し，集計者と直接繋がったユーザが集計者へと送信することとなる．図 1 に DC-net の動作例を示す．図 1 のように，各ユーザは自身の保有する値を他のユーザと相互に通信を行い共有する．その後足し算を行い，算出された 2 という値を集計者へと送信する．これによって集計者が知りえる情報は 2 という値のみであり，誰が 1 という値を持ち，誰が 0 という値を持っていたのかを知ることはできない．しかしながら，この方式では集計者に対するユーザの匿名性は保証されるが，ユーザ同士で票の共有を行うため，ユーザ間での匿名性は保証されていないこととなる．

2.2 マルチパーティプロトコル 5)6)

マルチパーティプロトコルは，匿名通信プロトコルの一種であり，参加者が自身の保有する情報を秘匿にしたまま他の参加者と保有する情報を共有し，その共有した情報を秘匿にしたままその情報を用いて 4.1 章のような演算を可能にするプロトコルである．マルチパーティプロトコルでは，参加者が保有する情報を秘密分散を用いて分

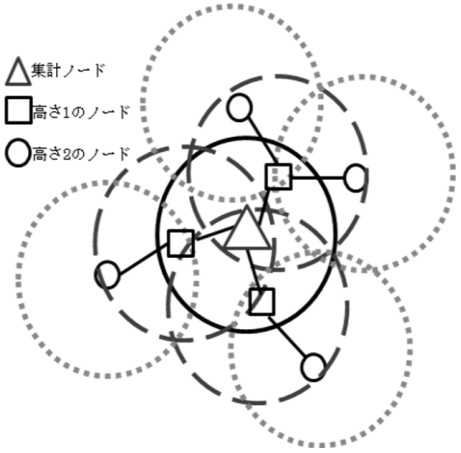

図 3 木構造化の手順

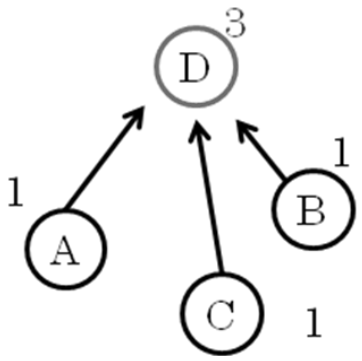

図 4 末端ノードの

割し，分割された情報を他の参加者と共有する．その後，分割されたままの情報を用いて演算を行うことで，誰にも真の情報を露呈することがなくなる．マルチパーティプロトコルは，自身の持つ情報を直接協調する相手に知らせることを防止する紛失通信や，自身の持つ情報の中身を秘匿にしたまま，情報を持っている証明を可能とするゼロ知識証明の上に成り立つプロトコルであり，情報理論的安全性を持つことから強度の匿名性を持つとされている．しかし，マルチパーティプロトコルは参加者同士での情報の分散や共有を行っているため，参加者が増える事により計算量や通信量が増大することとなり，大規模な通信には不向きとされている．しかし，大規模な通信を匿名性が保証されない場合の例仮想的に小規模化したり，分割することで，大規模な通信にも適用可能だと考えることが可能である．3 章において，木構造 DC-net の概要について述べるが，これにより段階的な処理を行い仮想的に通信を小規模化することで，ある程度規模の大きな通信においてもマルチパーティプロトコルの適用が可能となる．

3. Ad-hoc Network における木構造 DC-net

本章では，中間ノードの匿名性を保証し，部分木ごとの段階的処理を可能にするため，Ad-hoc Networkにおける木構造DC-netを提案する．基本的なDC-netではノード同士での値の共有により，ノード同士の匿名性が保証されないという問題がある．この問題を解決するためには，ノード同士が自身の持つ値を直接的に相手に知らせてはいけないこととなる．そこで，ノードの配置を木構造化することにより，中間ノードは末端ノードの値の総計に加算していくこととなるため，中間ノードは自信の持つ値を直接的にやり取りする必要が無くなる. 図2に末端ノードと中間ノードにおける違いについて示す．図2のように，末端ノードから1という値が送られてきた場合，その末端ノードが1という値を持っていると特定可能であるが，中間ノードの場合，1という値が送られてきたとしても, その下にいくつもノードがいるため, 特定は不可能である．このことから，木構造にすることにより中間ノードの匿名性が保証されることが分かる． 次に，木構造化する方法について説明する．図3に木構造化の手順について説明する． 図3に示すように，まず集計ノードを基点とし，集計ノードからの電波を任意の電波強度で受信可能なノードを高さ1のノードとする．同様に，高さ1のノードからの電波を任意の電波強度で受信可能なノードを高さ2のノードとする. この手順を繰り返すことで，木構造化することが可能となる．

3.1 問題点

Ad-hoc Network において，木構造DC-net を用いることで，中間ノードは下位のノードの総計値に自身の値を加えていく形になるため，中間ノードの匿名性を保証することが可能となる．しかし，この方式では末端ノードでは自身の持つ値を直接的にやり取りしているため，末端ノード同士での匿名性を保証することは不可能である．また， 末端ノードの1 つ上のノードから見ると，末端ノードがある条件を満たした場合に限り，匿名性が保証されないという問題がある．例として，賛成を1，反対を0 とする．

末端ノード全てが 1 もしくは 0 の値を持った場合に，全ての末端ノードが 1 ならば末端ノード N 人に対して上位ノードに送られてくる値も N となる．同様に全ての末端ノードが 0 ならば末端ノード N 人に対して上位ノードに送られてくる値は 0 となり，どちらの場合においても匿名性が保証されないこととなる．図 4 は全ての末端ノードが 1 の値を持った場合の例である．

4. Ad-hoc Network におけるマルチパーティプロトコルを用いた匿名通信方式

本章では，3.1 で述べた末端ノードの匿名性が保証されない問題を解決するため，マルチパーティプロトコルを適応的に用いた匿名通信方式を提案する．

4.1 木構造 DC-net におけるマルチパーティプロトコルの適用

木構造 DC-net では，木構造化し，末端ノードから集計ノードへと値を順に受け渡して行くため，一般的なマルチパーティプロトコルとは異なり，本方式では部分木ごとでの計算，上位ノードへの受け渡しが必要となり，最後に集計ノードが結果を算出することとなる．以下に文献 12)を基に，計算方法について示す．

投票参加人数を I 人，立候補者数を J 人とし，立候補者を $C_1C_2,\ldots,C_J$ とする．票

Vol.2011-CSEC-55 No.6
2011/12/5

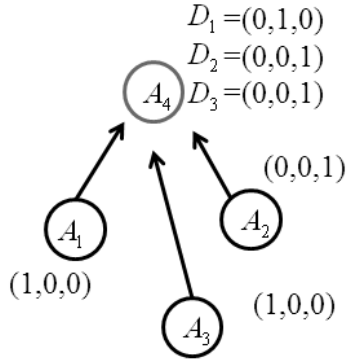

図 5 マルチパーティプロトコルの計算例

$B_i = (b_i^{(1)}, b_{i,}^{(2)} \ldots b_i^{(J)})$ に対し，投票者は自身が投票する立候補者に対応する bit を 1 とし，それ以外を 0 とする．得票数 D_j は関数 g を $g(x_1,\ldots x_m) = x_1 + \cdots + x_m$ とすると $D_j = g(b_1^{(j)} + \cdots + b_I^{(j)})$ となり， $D_j = (d_j^{(1)},\ldots,d_j^{(L)})$ と表記する． L は D_j のビットの最大値で，$\lceil \log_2 I + 1 \rceil$ で算出される．図 5 に例を示す．図 5 は A_1 が(1,0,0), A_2 が(0,0,1)， A_3 が(1,0,0)， A_4 が(0,1,0)という票を持った場合の D_j の値である．ここまでは，一般的なマルチパーティプロトコルと同等の動作を行う．しかし，本提案では木構造 DC-net を用いるため，この後の動作には一般的なマルチパーティプロトコルの動作とは異なる．本提案では，上記で算出した D_j を木構造の上位のノードへと受け渡していくこととなる．上位のノードは D_j を受け取った後，自身の持つ票を D_j に加え，更に上位のノードへと受け渡していくこととなる．これを繰り返していくことで集計ノードに票が集まり，その後当選者の選出を行う． D_j より， $V_l(d_1^{(l)},\ldots,d_J^{(l)})$ となり， $l = (1,\ldots,L)$ である．ここで，全ての bit が 1 である W を用意し，$S_i = W \wedge V_l$ と $d = \{W(1) \wedge V_{(j)}(1)\} \vee \cdots \vee \{W(L) \wedge V_{(j)}(L)\}$ を計算する．ここで $d = 1$ の時，W の値を S_i の値に置き換える．$W = (w_1,\ldots w_j)$ において $w_j = 1$ の時， C_j が当選者となる．

4.2 ダミー情報の適用

4.1で述べた方式では，まだ末端ノードの匿名性が保証されない問題を解決することはできない．そこで，ダミー情報を付け加えることで，末端ノードの匿名性の保証を可能とする．ダミー情報を加えることで，末端ノードの保有する値が1または0になることがなく，仮に末端ノードが全て1 という値を持っていたとしても，上位ノードからはそのことを知ることはできない．ダミー情報を加えるのは4.1 章の D_j 部分であり，末端ノードのみがダミー情報を加え，中間ノードは4.1 章と同じ動作をすればよい．ダミー情報はbit 数を考慮して付与する必要があり，桁上げや特定を防ぐために(1,1,1)や(0,0,0)を除外する．末端ノードは加えたダミー情報を投票とは別に集計サーバへと送信し，集計サーバは集計した総計からこのダミーを引くことで，結果を得ることが可能となる．

5. 評価

本章では，本提案の匿名性に関する評価を行う．本方式では，木構造 DC-net を用いることで，中間ノードの匿名性を保証することが可能となる．また，マルチパーティプロトコルを用い，ダミー情報を加えることで，末端ノードの匿名性を保証することも可能となる．ただし，投票者同士が結託しないことが前提となり，匿名性に関する安全性はマルチパーティプロトコルの安全性に帰着するものとする．

続いて，計算量に関する評価を行う．マルチパーティプロトコルでは参加者の増加に伴い，計算量が増加する．しかし，本方式では，木構造 DC-net を用い，段階的な処理を行うため，参加者の増加による計算量の増加は抑えることが可能となる．表 1 にノード数に応じた平均処理時間を示す．ここで平均処理時間とは，各ノードが 4.1 章で述べた演算処理を開始してから終わるまでの時間を計測したもので，その平均値をとっている．表 1 に示すように，木構造 DC-net による段階的な処理により，ノード数の増加に伴う平均処理時間の増加は増加量の小さな線形となり，増加量は少ないといえる．このことから，ノード数増加による計算量の増加は少ないものと判断することが可能である．

表 1 ノード数に応じた平均処理時間

ノード数	10	30	50
平均処理時間(s)	0.02823	0.04797	0.06386

6. 結論

本論文では，Ad-hoc Network において中継ノードの匿名性を保証するために，電波強度を利用したルーティングによって木構造 DC-net を構築し, マルチパーティプロトコルを利用することで，各ノードの投票内容を秘匿にすることが可能な匿名通信方式を提案した. 本方式では, 木構造 DC-net を用いることで, 段階的な処理が可能となり, 参加者が増加した場合に計算量が増大するといったマルチパーティプロトコルの問題点を緩和することを可能とした．また，中間ノードは末端ノードの総計に加算する形になるため，中間ノードは自身の保有する情報を直接他のノードへ知らせる必要がなくなり, 匿名性を保証することが可能となる. また, ダミーの値を混ぜることにより, 末端ノードの匿名性も保証することが可能となる．評価により，本提案の安全性，および効率を示した.

参考文献

1) Bangnan Xu, Hischke S and Walke B, “The role of ad hoc networking in future wireless communications” Communication Technology Proceedings, 2003, *ICCT 2003*, Vol 2, pp.1353-1358, Apr. 2003.
2) Lui Yang, Markus Jakobsson and Susanne Wetzel, “Discount anonymous on demand routing for mobile ad hoc networks” *Securecomm and Workshops*, pp.1-10, Aug. 2006.
3) G..Bleumer,``DCnetwork,' available at http://www.win.tue.nl/~henkvt/GBl.DCNetwork.pdf, 2003.
4) Emin Gun Sier, Milo Polte, Mark Robson, “CliqueNet: A self-organizing, scalable,peer-to-peer anonymous communication substrate”, at http://www.cs.cornell.edu/People/egs/papers/cliquenet-iptp.pdf, 2001.
5) 黒沢 馨, 岡本 龍明, “ゼロ知識証明とマルチパーティプロトコル”, Information Processing Society of Japan, Vol.32, No.6, pp.663-672, Jun. 1991.
6) 遠藤 つかさ, 越前 功, 吉浦 裕 “小規模投票の匿名性を維持する得票数秘匿型電子投票方式” , IEICE, Vol.107, pp.37-44, Jul. 2007.
7) Xiaoqing Li, Hui Li, Jianfeng Ma and Weidong Zhang, “An efficient anonymous routing protocol for mobile ad hoc networks” , *Fifth International Conference on Information Assurance and Security*, Vol 2, pp.287-290, Aug, 2009.
8) Imad Aad, Claude Castelluccia and Jean-Perre Hubaux “Packet coding for strong anonymity in ad hoc networks”, *Securecomm and Workshops*, pp.1-10, Sept, 2006.
9) Mayako Okubo and Masayuki Abe, “A length-invariant hybrid mix”, IEICS Trans. Fundamentals, Vol. E84-A, No.4, pp.931-940, Apr 2001.
10) Masayuki Abe, “Universally verifiable mix-net with verification work independent of the number of mix-servers”, IEICS Trans. Fundamentals, Vol.E83-A, No.7, pp.1431-1440, Jul. 2000.
11) S. Kitazawa, S. Nagano, M. Soshi, and A. Miyaji, “Anonymous communication with elementary cyclic routes”, Information Processing Society of Japan, Vol. 41, No.8, pp.2148-2160, Aug. 2000.