4-4-2　分散型台帳技術を用いた自律型モビリティ利活用データ集配信技術の研究開発

4-4-2　Distributed-ledger-enabled Data Collection and Dissemination Technology by Autonomous Mobility

渡辺良人　荘司洋三
WATANABE Yoshito and SHOJI Yozo

ソーシャル ICT システム研究室では、主に構内で活躍するサービスロボットのすれ違い通信を用いたデータ集配信プラットフォームの構築を推進している。本稿では、各々のサービスロボットによって取得されるセンシングデータ（映像ファイルなど）をプラットフォーム内の全ロボットに拡散させるための、効率的なデータ管理機能を紹介する。具体的には、各ロボットの活動記録を他のロボットと共有し、どのロボットがどのセンシングデータを所有しているかを把握することを目的として分散型台帳技術を用いる。本プラットフォームに適した台帳の構造として、我々は有向非巡回グラフ（DAG: Directed Acyclic Graph）構造を持った台帳構造を提案する。シミュレーションにより、代表的な台帳であるブロックチェーンと比較して、提案する DAG 型台帳を用いることで、センシングデータ及びロボット活動記録が全ロボットに拡散されるまでの遅延が抑えられることを確認した。

NICT Social ICT Systems Laboratory has been promoting the construction of a data collection and dissemination platform using opportunistic proximity communication among service robots that are mainly active in the premises. In this paper, we propose an efficient data management technique to disseminate the sensing data (e.g., video files) acquired by each service robot to all robots in the platform. Specifically, we use distributed ledger technology to share the activity records of each robot with other robots and to keep tracking which robot owns which sensing data. As a suitable ledger for this platform, we propose a directed acyclic graph (DAG) structure. Through computer simulations, we confirmed that the proposed DAG-based ledger reduces the delay until the sensing data and robot activity records are disseminated to all robots, compared to the blockchain, a conventional ledger.

1　まえがき

1.1　背景

COVID-19 パンデミック下での非接触型サービスのニーズの高まりに伴い、セキュリティ、清掃、消毒、配送などの幅広い分野における自律移動型サービスロボットが急速に社会に普及してきている。我々は、これらのサービスロボットがサービスロボット本来のタスクを遂行しながら、見廻（みまわ）りを目的とした動画撮影などのセンシングを行い、センシングデータを配信するネットワークである“Piggy-back Network”の構築を推進している。Piggy-back Network ではロボット間で確率的に発生するすれ違い通信に基づく Store-Carry-Forward（SCF）技術 [1] を用いることで、インターネットやクラウドに頼らずに大容量データを高速で転送することが可能である [2][3]。この仕組みを用いて、ネットワーク内のロボットが自律的に各々のセンシングコンテンツを拡散・共有し合えれば、ネットワーク管理者や外部ユーザが最寄りのロボットにアクセスするだけでネットワーク内のあらゆるセンシングデータを入手可能となる。しかしながら、SCF 技術によるデータ転送を成功させるには、ロボット本来の作業ルートから逸脱して転送相手と接近する必要も出てくる。そこで、もし、各ロボットが所有するセンシングデータ一覧情報がロボットの作業ルート逸脱前に入手でき、ロボット間で転送すべきデータの有無、つまりロボット間すれ違い通信の必要性の有無を事前に判断できれば、効率的な運用につながることとなる。

1.2　提案手法

本稿では、ミリ波帯無線通信規格と 920 MHz 帯無線通信規格をそれぞれデータプレーン、制御プレーンとして用いた異種無線すれ違い通信に基づく Piggy-back Network 上で、センシングデータの集配信を行うためのロボット間情報共有手法を紹介する。具体的には、Piggy-back Network のような分散システム上で、データの完全性を維持しつつ高い耐改竄(かいざん)性・耐障害性を達成する記録の管理手法として分散型台帳技術を用いる。各ロボットは自身を含むネットワーク内の全ロボットの活動記録を表すトランザクション履歴を台帳で管理しロボット間で共有される。このトランザクション履歴をトレースすることで各ロボットの最新のデータ所有状況の把握が可能となる。台帳は、データ転送の事前に制御プレーンを介してロボット間で共有・同期され、その後台帳から算出されるセンシングデータ所有状況に基づいたセンシングデータ転送の必要性の有無に応じて接近しデータプレーンによるセンシングデータ転送を行う。

なお、本稿では、例えばセルラーネットワークの電波の届きにくい災害地や屋内などにおける低コスト運用を目的として、無線局の免許不要で中距離での情報共有が可能な Wi-SUN を制御プレーンの通信規格として想定する。したがって、制御プレーンの通信は確率的に発生することとなり、そのネットワークモデルは遅延耐性ネットワーク（DTN: Delay Tolerant Network）となるが、DTN 上で分散型台帳を動作させるために、有向非巡回グラフ（DAG: Directed Acyclic Graph）構造を持つ台帳を採用している。

1.3　技術的な挑戦

我々は、ネットワーク内のロボットの過去・現在を含む全てのトランザクション履歴と全センシングデータにネットワーク外の管理者やユーザが容易にアクセスできるプラットフォームの構築を目指している。このようなシステムは、管理者やユーザが容易にアクセスできるサーバを用意し、そこでデータを一極集中管理することでも実現可能であるが、耐障害性を継続的に担保するためには費用がかさむであろう。また、たとえ信頼できる機関によってサーバが管理されているとしても、データを直接扱うことが可能な者によって（故意でなくても）データが改竄されることを完全に防ぐことは技術的には難しい。同様の問題は既存のコンソーシアム型の分散型台帳を採用したとしても生じ得ることが分かっている [4]。

一方、全ロボット間でトランザクション履歴とセンシングコンテンツを複製して所有するような分散システムを構築できれば、管理者やユーザは最寄りのロボットにアクセスするだけで、上記の仕組みを実現することが可能になる。

具体的には、時刻 t におけるネットワーク内の全トランザクション履歴と全センシングデータを、時刻 $t+\tau$（τ は遅延時間）に全ノードが保有した状態としたい。上述したように、本稿で考える Piggy-back Network では、データプレーンに加えて制御プレーンの特性についても DTN となることを想定している。よって、τ はノードの移動速度や通信距離にも依存することになる。

このような環境下で、τ を可能な限り最小化しつつ、更に高い耐障害性・耐改竄性を実現する方法として、我々は DAG 構造の分散型台帳を使ったトランザクション履歴管理手法を提案する。

2　異種無線 Piggy-back Network

2.1　システム概要

図 1 に検討対象とするシステムの概要図を示す。ネットワークは自律移動ロボット（以下、「ノード」とする。）で構成されている。各ノードは自律的に移動しながら定期的にセンシングを行っている。センシングタスクは例えば動画撮影などであり、センシングされた各データコンテンツは大容量のファイルとなり、ノード内のデータベースに保存される。

各ノードは数メートル間での数 Gbps の近距離高速通信が可能なミリ波帯無線規格と、数十～百メートルで約 100 kbps の中距離中速通信が可能な 920 MHz 帯無線規格である Wi-SUN を利用可能である。前者はデータプレーン、後者は制御プレーンで利用する。それぞれの通信可能距離をここでは D_d と D_c とする。

また、各ノードは台帳を管理している。台帳は「ブロック」の集合であり、ブロックには、あるノードから別のノードへのデータ生成及びデータ移行に関する

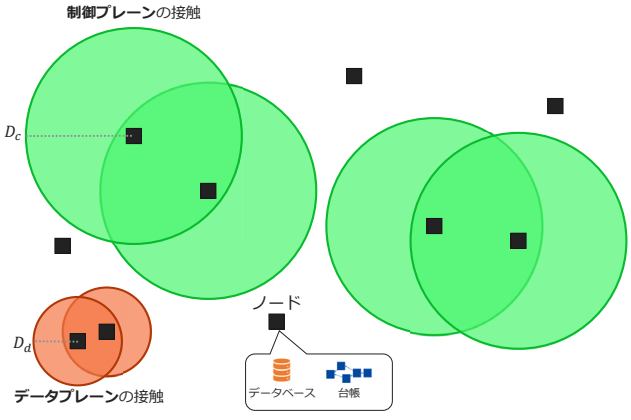

図 1　システム概要

活動履歴を表す複数の「トランザクション履歴」が格納される。台帳の詳細については後の節で解説する。

2.2　トランザクションとネットワーク状

本研究ではトランザクションとして管理するノードの活動内容として、「センシングデータの生成」と「センシングデータの転送」の二つのみを扱う。いま、ネットワーク内に存在するノード v_1, v_2, v_3 について、時刻 $t_1 < t_2 < t_3 < t_4$ において以下のトランザクションが発生したとする。

- 時刻 t_1 に v_1 がデータ d_1 を生成
- 時刻 t_2 に v_1 がデータ d_2 を生成
- 時刻 t_3 に v_1 から v_2 にデータ d_1 を転送
- 時刻 t_4 に v_1 から v_3 にデータ d_2 を転送

これらのトランザクション履歴の集合から表１のネットワーク状態が導ける。なお、括弧内は各データを入手した時刻を示している。つまり、トランザクション履歴を辿ることで各ノードのコンテンツ保有状況を把握することが可能となる。

2.3　ノードの動作フロー

図２に示すとおり、各ノードはデータプレーン・制御プレーンの通信状況やコンテンツ所有状況に応じて以下の４つのフェーズを遷移する。

1）自律活動フェーズ：初期フェーズ。各ノードの本来のタスクをこなすために自律活動を行いながら、動画撮影などのセンシングを行う。

2）台帳同期フェーズ：自律活動フェーズ中の２台のノードが距離 D_c 内に入り制御プレーンの接続が確立されたら、各々の台帳の同期を行う。これにより、二つのノード間で同じ台帳の複製を所有することになる。その後、台帳内のトランザクション履歴をトレースすることでネットワーク状態を導出することでお互いに所有しているデータを把握し、いずれかのノードで足りていないセンシングデータがあれば、データ交換が必要と判断する。

3）接近フェーズ：台帳同期フェーズでデータ交換が必要と判定された場合にこのフェーズに移行する。ここでは、データプレーンの通信を確立するために２台のノードが、本来のルートを外れて接近する。

4）データ交換フェーズ：接近フェーズにより２台のノードが距離 D_d 内に入った後、足りていないデータを補完するためにデータプレーンを介してデータ交換を行う。データ交換が終了した後は、各ノードは自律活動フェーズに戻る。

表１　ランザクションから導出されるネットワーク状態の一例

全コンテンツリスト	$[d_1, d_2]$
v_1 が所有するコンテンツリスト	$[d_1(t_1), d_2(t_2)]$
v_2 が所有するコンテンツリスト	$[d_1(t_3)]$
v_3 が所有するコンテンツリスト	$[d_2(t_4)]$

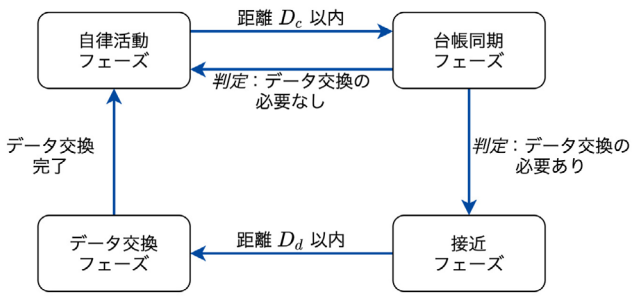

図２　ノードのフェーズ遷移図

3　DAG 構造の分散型台帳

本節では、Piggy-back Network 上で動作させることを目的とした分散型台帳の詳細について、従来の台帳技術であるブロックチェーンと比較しながら説明する。

3.1　台帳の構造

分散型台帳の代表的な例に、ブロックチェーン [5][6] がある（図 3）。ブロックチェーンはブロックとそこに含まれるトランザクションが大きな構成要素である。各ブロックの内容から一意のハッシュ値が導出され、その値を次に生成されるブロック内に含めることで、ブロック同士を鎖状に繋(つな)いだ構造で台帳を表現できる。この単一チェーン構造の台帳をネットワーク全体で複製し共有することで耐障害性を担保している。

我々が提案する台帳もブロックチェーンと同様に、一つのブロックに対して複数のトランザクションが含まれる構成とし、同じ台帳をネットワーク内で共有することで耐障害性を担保する。しかし、本稿で考える Piggy-back Network では、そのネットワーク特性はすれ違い通信に基づく DTN となるため、従来型のブロックチェーンを動作させると、ブロックの伝搬遅延により、チェーンの枝分かれ（フォーク）が大量に発生してしまうという問題が生じる。

そこで我々はフォークを許容した形である DAG 構造により半順序集合（Partially Ordered Set）として台

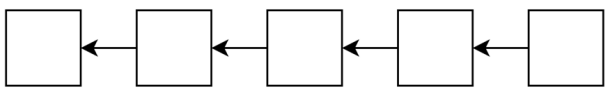

図３　ブロックチェーン構造

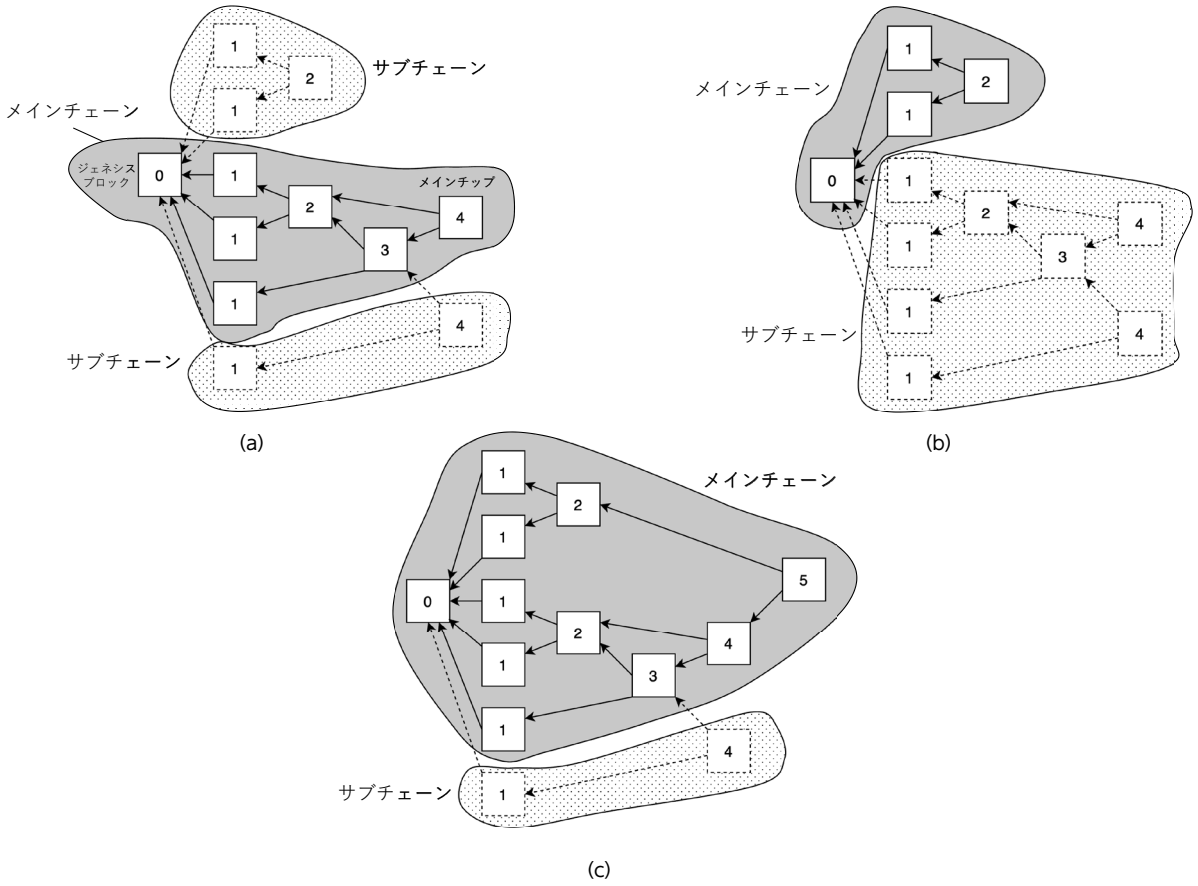

図 4　台帳構造の例　(a) と (b) は 2 ノード間で同期されたものであり、台帳構造は同じであるが、その構成要素であるメインチェーンとサブチェーンが異なる。これら 2 ノード間でブロック生成が行われると、共通した (c) の構造となる。

帳を表現する。我々が提案する DAG 型台帳の構造を図 4 に示す。ブロックチェーンとは異なり、一つのブロックは二つの親ブロックを参照している。従って、台帳全体では枝分かれを含む構造となることが分かる。

各台帳はメインチェーンとサブチェーンで構成されている（図 4 (a)）。メインチェーンは、以下で説明するブロック生成方法により、自身がブロック生成に関わった最新ブロック（以下、「メインチップ」とする。）を含むその全ての親ブロックの集合から成り、サブチェーンはそれ以外のブロックの集合から成る。サブチェーンに含まれるブロックは「台帳同期フェーズ」で対向するデバイスから受け取る。つまり、「台帳同期フェーズ」が行われた 2 ノード間でも図 4 (a) と図 4 (b) で示すように、メインチェーンとサブチェーンの構成は異なるのが通常である。

3.2　ブロック生成方法

台帳技術において耐改竄性を高めるブロックの生成手段として、達成困難・再現困難なタスクを実行するという条件が必要となる。Bitcoin[5] や Ethereum[6] などのブロックチェーンでは、2021 年 9 月現在、Proof-of-Work（PoW）と呼ばれる方法でブロックの生成が行われている。つまり、ブロックを生成するために多量の計算により一定条件を満たすハッシュ値（Nonce）を導出するという達成困難なタスクを実行する。しかし、文献 [7] にもあるとおり、その計算を実行させるための電力の生成に伴い排出される二酸化炭素が地球環境に悪影響を及ぼすという指摘がある。

一方、我々の台帳技術では、Piggy-back Network の特性を大いに活かしたブロック生成手法を用いる。Piggy-back Network においては、近距離無線通信を用いた「データ交換フェーズ」がある。本フェーズに移行するには、ノード同士が物理的にデータプレーンの通信距離 D_d 内まで移動し、さらに大容量データを転送する必要がある。これは、容易には達成困難であるというブロックを生成するタスクの条件を満たしている。そこで、我々は「データ交換フェーズ」の完了をもってブロックの生成を行う Proof-of-Forwarding（PoF）を提案している [8]。ここでは PoF により、データ交換完了時に、対向する 2 ノードが所有する未保存トランザクション履歴と、お互いのメインチップのハッシュ値を含めたものを最新ブロックとして生成する。

いま、「台帳同期フェーズ」を終了した図 4 (a) の台帳を所有するノード v_i と図 4 (b) の台帳を所有する

ノード v_j が「データ交換フェーズ」を完了し PoF によりブロックを生成したと仮定する。このとき v_i と v_j の台帳構造は、双方で同じ図 4 (c) のようになる。図 4 (c) のメインチップは、図 4 (a), (b) のメインチップを参照していることが分かる。なお、提案手法では同一の 2 ノード間で連続してブロックは生成できない制約を与えている。これにより、少なくとも 2 台の悪意のあるノード間で無制限にブロックが生成されることを防ぐことができる。

4 計算機シミュレーション

Piggy-back Network における、トランザクション履歴の拡散とデータの拡散にかかる遅延 τ (**1.3** で説明) について、トランザクション履歴の管理に従来型台帳の代表例である単一枝から成るブロックチェーンと、提案する DAG 型台帳を用いた場合の比較を行ったので結果を紹介する。

4.1　シミュレーション諸元

シミュレーション諸元を表2に示す。ここで、$U(a,b)$ は、$[a,b]$ の一様分布を表す。自律活動フェーズでは、各ノードは二次元空間をランダムウェイポイントモデルに基づいて移動する。センシングデータは毎回ランダムに選ばれたノード上で、ポアソン過程に基づいてランダムな時間に生成されると仮定する。一つのセンシングデータの転送には10秒かかると想定する。これは、例えば 50 Gbit (6.25 Gbyte) のサイズのデータを 5 Gbps で伝送することに相当する。

なお、比較対象であるブロックチェーンを用いたシステムにおいてもブロック生成には PoF を用いるものとする。ブロックチェーンシステムにおいて、もしチェーンのフォークが発生した場合は、Bitcoin[5] や Ethereum[6] などにおける対処方法と同様に、短い方のチェーンに含まれていたトランザクションのうち、長いチェーンに含まれているもの以外は再度未保存のトランザクションとして取り出し、最新のブロック生成時に改めてこれらを含めることとする。

4.2　シミュレーション結果

ブロックチェーンと DAG 型台帳をそれぞれ用いた場合について、K 番目のコンテンツが生成された時点でのネットワーク内の全トランザクション履歴とセンシングデータの拡散までにかかる遅延 τ を図 5 に示した。K は 50 と 100 としている。なお、拡散済みトランザクション履歴としては、ブロックに取り込み済みのもののみを観測している。

図5より、DAG 型台帳よりもブロックチェーンを用いた場合のほうが τ が大きいことが分かる。これは、前述しているとおり、台帳がフォークを許容するかどうかの違いによる影響である。すれ違い通信に基づく DTN では、フォークが頻繁に発生してしまう。つまり、一度ブロックに取り込まれたトランザクション履歴が再度未保存トランザクションとして扱われるという現象が同時多発的に発生するため、ブロックに取り込まれた形で全ノードにトランザクション履歴が拡散されるまでに多くの遅延が発生してしまっている。

次に、図 6 にネットワーク上で最初のコンテンツが生成されてからの各時間における、全ノードに拡散済

表 2　シミュレーション諸元

フィールド面積	300 × 300 m
ノード数	10
移動速度の分布	$U(0.2,1)$ m/s
1 コンテンツ当たりのデータ転送時間	10 秒
D_c	100 m
D_d	5 m
データ生成の平均時間間隔	1 分

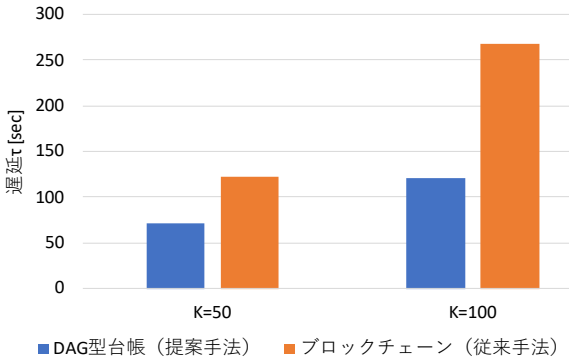

図 5　K 番目のコンテンツが生成された時点の全トランザクション履歴と全コンテンツが拡散されるまでの遅延 τ

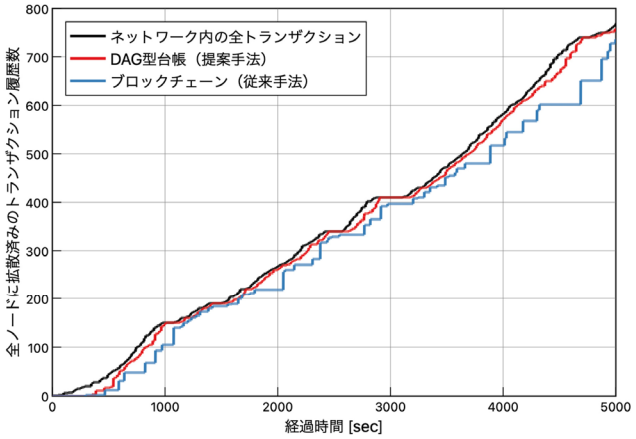

図 6　各時刻における全ノードに拡散済みのトランザクション履歴数

みのトランザクション履歴の累積数を示す。ここでも、トランザクション履歴はブロックに取り込み済みのもののみを観測している。なお、参考値として、ネットワーク内で発生している全トランザクションの累積数も示している。

図から分かるように、DAG 型台帳システムの結果は、ネットワーク内で発生している全トランザクションの累積数によく近接している。しかし、ブロックチェーンシステムでは、その特性が階段状になっており、特に 4,500 秒付近では約 800 個の拡散済みトランザクション履歴数で停滞しており、全体の 15 % のトランザクション履歴が拡散されていない状態になっていることが分かる。それに伴い、500 秒以上の拡散遅延も発生している。

実はブロックチェーンシステムには上記の結果では見えてこない深刻な問題も潜在している。フォーク発生時に既に取り込まれた過去のトランザクション履歴を未保存トランザクションとして扱う都合上、トランザクション履歴の発生順序がブロック間で一貫性が無いのである。これは、例えば時刻同期が行えていない機器がネットワーク内に存在していた場合に、トランザクションの順序を保証できないという課題が生じてしまう。一方、提案する DAG 型台帳を用いることで、少なくともブロック単位でのトランザクション発生順序は保証可能である。

以上より、Piggy-back Network のような IoT 機器で構成される DTN 環境下でトランザクション履歴を管理する手法として DAG 型台帳が有効であることが示された。

5　まとめ

本稿では、DAG 構造を持った分散型台帳による、データプレーンと制御プレーンからなる Piggy-back Network 上でのトランザクション履歴管理の手法を提案した。各ノードのセンシング履歴とそのデータ転送履歴、そしてセンシングデータを全ノードに拡散・共有するという問題を扱い、DAG 型台帳がブロックチェーンに比べて少ない遅延を達成することを示した。

分散型台帳を導入するメリットとして耐障害性・耐改竄性の向上がある。前者は提案手法で達成の見込みがあるものの、後者についてはまだ十分な検討ができていない。PoF は未完成の技術である。PoF により真に耐改竄性を保証するには、2 ノード間でデータ交換が行われた事実を何らかの方法で記録・検証できる仕組みが必要であると考えており、今後の研究課題とする。また、効率的に 2 ノード間で台帳を同期する方法についても今後の検討課題とする。

謝辞

分散型台帳技術について建設的なコメントや提案をしてくださった早稲田大学斉藤賢爾教授に感謝申し上げます。

【参考文献】

1 L. Pelusi, A. Passarella, and M. Conti, “Opportunistic networking : Data forwarding in disconnected mobile ad hoc networks,” IEEE Communications Magazine, vol.44, no.11, pp.134–141, Nov. 2006.
2 Y. Shoji, W. Liu, and Y. Watanabe, “Community-based ‘Piggy-back Network’ utilizing Local Fixed Mobile Resources supported by Heterogeneous Wireless AI-based Mobility Prediction,” Proceedings of 2020 IEEE 91 st Vehicular Technology Conference (VTC2020-Spring), pp.1–5, May 2020.
3 Y. Watanabe, W. Liu, and Y. Shoji, “A Demonstrative Study on the Potential of Store-Carry-Forward-Based Contents Delivery by a Beverage Supplier’s Logistics Network,” Proceedings of 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp.65–70, Oct. 2019.
4 K. Saito, A. Shiseki, M. Takada, H. Yamamoto, M. Saitoh, H. Ohkawa, H. Andou, N. Miyamoto, K. Yamakawa, K. Kurakawa, T. Yabushita, Y. Yamada, G. Masuda, and K. Masuda, “Requirement Analyses and Evaluations of Blockchain Platforms per Possible Use Cases,” arXiv:2103.03209 [cs], March 2021.
5 S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,”, 2008. https://bitcoin.org/bitcoin.pdf
6 V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014. https://github.com/ethereum/wiki/wiki/White-Paper
7 M. J. Krause and T. Tolaymat, “Quantification of energy and carbon costs for mining cryptocurrencies,” Nature Sustainability, vol.1, no.11, pp.711–718, Nov. 2018.
8 Y. Watanabe, W. Liu, A. Abbas, Y. Andreopoulos, M. Hasegawa, and Y. Shoji, “Verifiable Event Record Management for a Store-Carry-Forward-Based Data Delivery Platform by Blockchain,” Proceedings of 2020 IEEE 31 st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp.1–6, Aug. 2020.

渡辺良人　（わたなべ　よしと）
総合テストベッド研究開発推進センター
ソーシャル ICT システム研究室
テニュアトラック研究員
博士 (工学)
無線通信、符号理論、マルチメディア信号処理
ブロックチェーン

荘司洋三　（しょうじ　ようぞう）
総合テストベッド研究開発推進センター
ソーシャル ICT システム研究室
室長
博士 (工学)
ミリ波通信システム、光通信システム