

次世代 IoT に向けたマシン-クラウド間 大量データ転送技術に関する研究

吉村 太一 †1,a)

小川 猛志 †1,b)

概要 近年では従来の LTE などの WAN に比べ、大幅な低コスト化や低消費電力化を実現した Low Power Wide Area Network(LPWAN)が注目され、実用化されている。一方で LPWAN は狭帯域であり、1 日の通信回数の制限が存在することからマシンの異常時におけるログデータの収集などといった大量データの転送に対応できないといった課題が挙げられる。そのため、クラウド制御による Wi-Fi すれちがい通信によりマシンとスマートフォン間でデータを転送させる事で、通信時のコストや消費電力を増大させずに大量データを転送できる手法について研究している。同手法は端末間の分散制御でデータを転送する既存技術と異なり、クラウド内の管理サーバが集中制御して端末間のマルチホップ通信を実施させる。このため、事前に信頼関係のない任意の端末間で安全、低消費電力でかつ通信品質の高いデータの転送が可能である。本稿では、実際のサービスを想定したデータ転送実験の結果を示し、マシンとクラウド間でデータを分割・冗長化する技術が必要であることを報告する。また従来の Forward Error Correcting(FEC)技術の適用時の課題を示すとともに、同課題を解決する手法を提案する。

1. はじめに

マシンが収集する膨大な量のデータを全てクラウドに転送しクラウドで処理すると、ネットワークやクラウドの負担が増大する。このため、マシンまたはマシン近辺の装置でデータを一次処理し、その結果をクラウドで処理するエッジコンピューティング[1]が提案されている。エッジコンピューティングによってマシンとクラウド間の通信量を大幅に削減できると考えられている。

また、近年では従来の LTE などの WAN に比べ、大幅な低コスト化や低消費電力化を実現した Sigfox[2]や LoRa[3]、NB-IoT[4]などの Low Power Wide Area Network(LPWAN)が注目され、実用化されている。LPWAN では端末あたりの通信データ量を極めて少なく抑制でき(Sigfox では 1 日最大 1kB 程度)、無通信時に通信回路をスリープする事で、人口の 10~100 倍の端末を経済的に収容できる。この事から、マシンとクラウド間の通信に LPWAN を適用する事で屋外に設置するマシンの低コスト化が期待される。

ただし、マシンのソフトウェアの更新やマシンの異常時におけるログデータの収集などといった保守を考慮すると、マシンとクラウド間でそれらデータを転送できる必要がある。数日程度の遅延時間で転送できれば十分だと考えているが、LPWAN の帯域では一度に大量データを転送できない。そのため保守者の出張により更新を実施すると、人件費の負担によってビジネスモデルが破綻する。この事からマシンとクラウド間の通信に LPWAN を適用する場合、マシンから大量データを経済的かつ確実に転送する技術が必要になる。

上記について、我々はクラウドからの制御による Wi-Fi すれちがい通信によりマシンとスマートフォン(以下、端末)間でデータを転送させる事で、通信時のコストや消費電

力を増大させずに大量データを転送できる手法について研究している[5]。端末がすれ違う際にデータを転送し宛先まで届ける技術に、Delay Tolerant Networks(DTN)技術[6][7]やアドホック通信がある。提案手法ではそれらの分散制御型の既存技術と異なり、クラウド内の管理サーバが各端末の位置情報や過去の移動履歴などを活用してデータの転送を実施させる端末を選択する。また、端末間で 1 回のみ使用可能な相互認証情報を管理サーバから端末に転送して相互接続を実施させる。すなわち、集中制御型の端末間マルチホップ通信を実施させる。このため、事前に信頼関係のない任意の端末間で安全、低消費電力でかつ通信品質の高いデータの転送が可能である。

本稿では、第一に提案手法について実施したマシンと端末間のデータ転送実験の結果を示す。本実験では、現状の IoT 端末の実装[8]から最大で 20MB のデータ転送を目標としたが、すれちがい通信距離の確保が難しい場合や第三者による電波の遮蔽等がある場合は、データを 1 端末に転送できず、複数の端末に分割して転送する必要がある事が分かった。このためデータが部分的にしかクラウドまで到達しなくとも再送を要求せずにデータ全体の復元を可能とする技術が必要であると考えられるが、従来の Forward Error Correcting(FEC)技術を適用すると消費電力の増大などの課題が発生することが分かった。そこで、本稿ではさらに同課題を解決する手法を提案する。

本論文の残りの章では、以下を説明する。2 章で保守以外の用途で大量データの転送が必要になる例を挙げる。3 章で一般ユーザの端末を利用した大量データを転送する手法を示す。4 章ですれちがい通信時のデータ転送量の実験結果とその考察を示す。5 章で FEC 技術の概要を、6 章で従来 FEC を提案手法に組み合わせた時に発生する課題を説明する。7 章で課題解決の方法を提案し、定性的に評価する。最後に 8 章でまとめと今後の予定を示す。

†1 東京電機大学大学院 情報環境学研究所
Graduate School of Information Environment, Tokyo Denki University
a) 18jkm30@ms.dendai.ac.jp
b) togawa@mail.dendai.ac.jp

2. 大量データの転送例

アプリケーションによってはマシンの保守以外の用途でも、マシンとクラウド間にて大量データの送信が非同期で必要になる。転送例を以下に示す。

2.1. 橋や道路などの建築物監視

建築物内部に多数設置したセンサ端末において、センサ間の距離や応力を測定し建築物の正常性の一次判定を行う。確実に正常、または異常と判定できた場合、LPWAN を利用しクラウドに「正常/異常」と通知する。異常の予兆を検出した場合、見逃し防止のために提案手法により詳細なデータをクラウドに転送し、クラウドで最終判定を行う。

2.2. 街角カメラによる不審者監視

カメラにストレージを内蔵させ、過去の撮影画像を保管する。HD 動画、30 フレーム標準画質(2.5Mbps 程度)で、1月で0.9TB 程度である。通常の Web カメラと異なり動画をインターネットに転送しない。提案手法により必要に応じてカメラに不審者の特徴を示す情報をダウンロードし、カメラ内の処理によって過去の画像やダウンロード後の撮影画像と比較する。合致する可能性を検出した場合、クラウドに LPWAN で通知するとともに、根拠となる画像データを提案手法でクラウドにアップロードする。

3. 一般ユーザの端末を利用した提案手法

3.1. 大量データ転送方式

表 1 に本文中で使用する用語の定義を、図 1 に提案するデータ転送方式の概要を示す。前提条件として各端末が 1 日以内にフリースポットに接続する確率(以下、FS 接続率)を 0.5 以上 0.95 以下、平均 0.8 以上とする。なお、フリースポットへ接続したら必ずクラウドにデータを転送可能であると仮定する。

本サービス専用のデータ配送アプリケーションを一般ユーザの端末に事前に配布する。当該アプリケーションは端末が徒歩に相当する速度で移動している時に、LTE を経由して GPS から得た位置情報を周期的にクラウドに通知する。大量データのアップロードが必要になるとマシン内に大量データを発生させ、LPWAN を経由してデータの発生をクラウドに通知する。クラウドはアプリケーションを搭載した端末からマシン近辺の端末を選択し、LTE を経由してデータの回収を委託する。端末は徒歩に相当する速度でマシンとすれちがう際に自動で Wi-Fi を経由してマシンからデータを回収する。フリースポットへ移動後に無線 LAN を経由してクラウドへデータを転送する。

従来のすれちがい通信と異なり、クラウドからの制御で

マシンと端末間の Wi-Fi 通信を開始させるため、消費電力を抑制できる。また、フリースポットからアップロード時に追加の通信費用の不要な無線 LAN を経由するため、端末の通信費用も増大しない。図 1 ではアップロード例を示したが、データ転送手順を入れ替える事でクラウドからマシンへの大量データのダウンロードも可能である。

表 1 本文中で使用する用語の定義

FS 接続率	<ul style="list-style-type: none"> 各端末が 1 日以内にフリースポットへ接続する確率 接続したら必ずクラウドにデータを転送可能 0.5 以上 0.95 以下、平均 0.8 以上
すれちがい通信距離	端末が遠方から徒歩でマシンに徐々に近づき、通信を開始した時点のマシンと端末間の距離
繰り返し送信	データブロックの転送が未完了の時、転送できる端末が到達するまで送信
データ到達率	データ全体のクラウドへの到達率
ブロック到達率	マシンからデータブロックを受け取った端末の FS 接続率

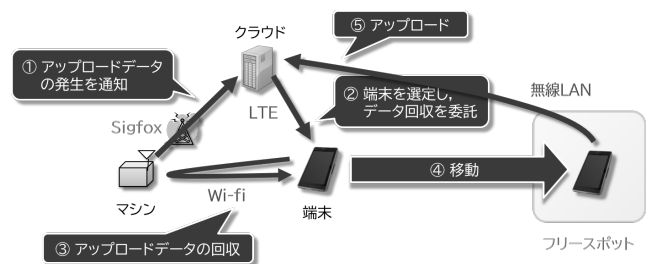


図 1 提案するデータ転送方式 | アップロード例

3.2. マシンと端末間の相互認証方法

図 2 に従来の認証規格である IEEE802.1X を提案手法に適用した場合の認証手法の例を示す。認証サーバと各端末が相互認証で使用するマスターキーを事前に共有する事で、例えば無線 LAN 基地局と端末間で事前に認証情報を共有せず、任意の無線 LAN 基地局と端末間の相互認証が可能となる。端末が Wi-Fi によりマシンと自動接続時に、端末はマスターキーから生成した認証データをマシン(基地局相当)に送信する。マシンは LPWAN を経由してクラウドに認証データを転送し、クラウドは当該端末と事前に共有しておいたマスターキーを利用して当該認証データを検証する。検証結果をもとにクラウドからマシンへ接続許可を通知し、マシンと端末間で無線リンクを確立する。その後、端末がマシンからデータを回収する。正常な端末間であれば適切に相互認証が可能であるが、例えば第三者がなりす

もし複数の端末でマシンに認証を要求すると、マシンは要求された分だけクラウドに認証データを転送し、クラウドは受け取った認証データの分だけ接続判定を通知する事になる。無線 LAN 基地局と認証サーバ間であれば一般に広帯域な IP 網が使用されるため問題にはならないが、提案手法では認証データが極めて狭帯域な LPWAN により転送されるため、マシンとクラウド間で帯域消費や通信制限が発生し、DoS 攻撃の手段となり得る可能性が生じると考えられる。

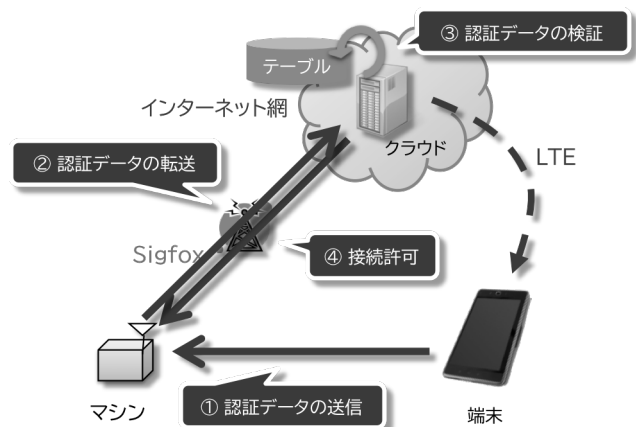


図2 IEEE802.1X を適用した通信例

図3に提案する認証手法の概要を示す。事前にマシンと管理サーバ間でマスターキーを共有しておき、データ転送が必要になるとカウンタ同期等といった手法によって当該マスターキーから1回のデータ転送に限り有効な共有秘密情報(PSK)をそれぞれ生成する。クラウドはLTEを経由してPSKを端末に送付する。当該端末はマシンとWi-Fiで通信可能な範囲に到達すると、既存のWPA2-PSK認証手順を使用し、当該PSKから生成した認証データをマシンに送付する。マシンは受け取った認証データを当該PSKで検証し、認証データが一致したならばデータを当該端末に送付してWi-Fi回路をスリープする。

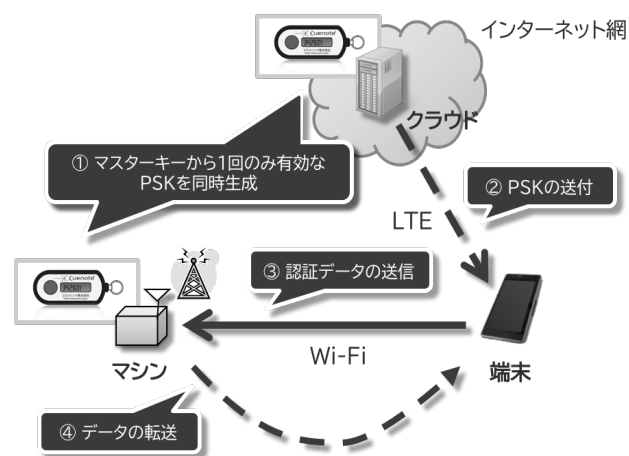


図3 提案するマシン-端末間の認証手法

この手法により、悪意者がマシンに接続を試みても正当な認証データを持たないため、悪意者の接続を拒否できる。また、従来技術と異なりマシンは端末から受信した認証データの正当性をクラウドに問い合わせずに判定できるため、LPWAN への DoS 攻撃を回避できる。

図4に提案認証手法の適用時におけるデータ転送方式のアップロードシーケンス図について示す。

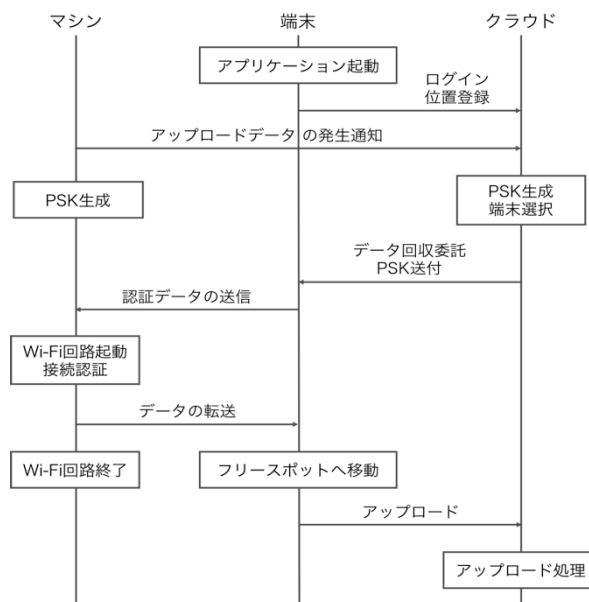


図4 提案認証手法の適用時におけるシーケンス図 | アップロード例

4. データ転送量の評価

本提案の実現性を評価するために、RaspberryPi 3(マシン側)と MacBook Pro(端末側)で動作するプロトタイプを開発し、すれちがい通信でアップロードできるデータ量を測定した。無線リンクで802.11nを使用した。1回のデータの転送量の目標を20MBとし、電柱の間隔程度の見通しを仮定してすれちがい通信の距離を最大30mとした。実験ではマシンと端末間の距離を10mまでは2m間隔、20mまでは5m間隔、60mまでは10m間隔に変化させ、各間隔でマシンと端末の双方を静止させて、データ転送速度を測定した。また、実験環境によってデータ転送速度に差異が生じる可能性もあるため、データ転送速度を比較するために見通しが悪い屋内の研究棟3F廊下、見通しが良く障害物の無い屋外の研究棟裏広場の2箇所を実験場所を選定した。測定結果から距離とデータ転送速度の関係を線形近似で導出し、徒歩で移動する端末が静止するマシンに徐々に近づき離れるまでにマシンから受信できるデータ量を推定した。

図5にデータ転送速度とマシンと端末間の距離の関係を示す。横軸Mはマシンと端末間の距離を示し、縦軸MB/sはマシンから端末におけるデータ転送速度を示す。

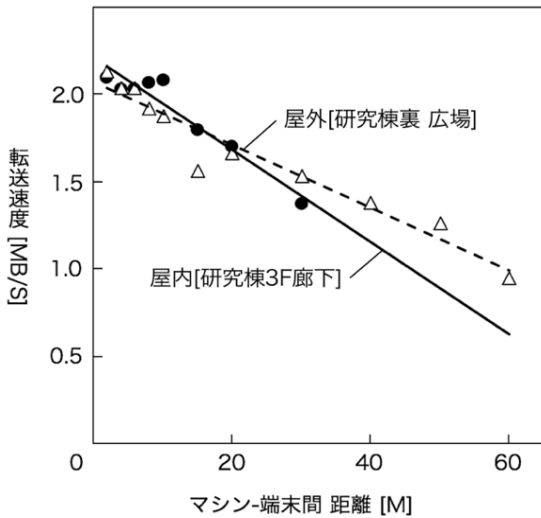


図5 データ転送速度とマシン-端末間の距離の関係

また、図6にすれちがい通信を行う距離(以下、距離L)とデータ転送量の関係を、図7に距離Lの定義を示す。距離Lとは端末が遠方から徒歩でマシンに徐々に近づき、通信を開始した時点のマシンと端末間の距離を示す。その後、端末はマシンのすぐ横(距離0)を通過しマシンからの距離が再びLになるまでデータを受信すると仮定した。

また、端末は直線上を5km/h(徒歩に相当する速度)で移動すると仮定した。それらの仮定に基づき、図5の結果をすれちがい通信距離とデータの転送量総量の関係に換算して、目標の20MBの転送を達成するか評価した結果が図6である。

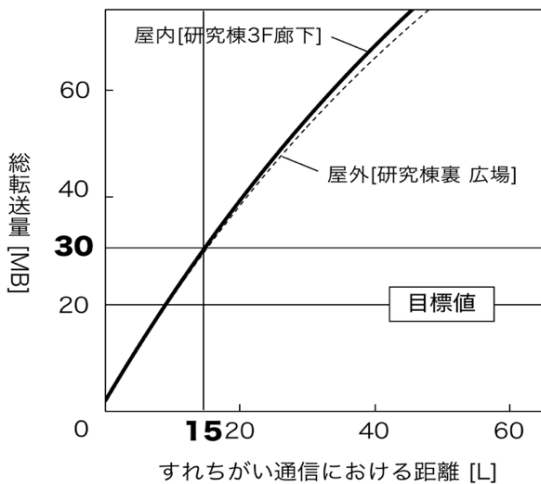


図6 総転送量とすれちがい通信における距離の関係

図6の縦軸MBは端末がマシンとLm離れた地点から通信を開始し、距離0でマシンとすれちがってLm離れるまでに受信したデータの総量(図4からの換算値)を示す。実験場所に関わらず、すれちがい通信距離が30m(L=15)の時に約22秒の移動時間で約30MBのデータを転送でき、目標の20MBの転送を達成した事を確認した。ただし実際のサ

ービスを想定すると、すれちがい通信距離が実験より確保できない事や第三者による電波の遮蔽の影響、使用する無線デバイスの種類による性能低下も考えられるため、総転送量が20MBを下回る可能性も見込める。そのため、確実にデータを転送するためにはデータを少量のブロックに複数に分割し、複数の端末にブロックを転送させる技術が必要と考えた。

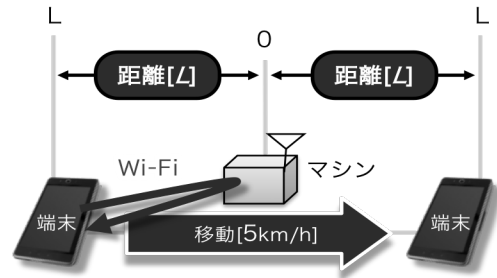


図7 すれちがい通信における距離L

5. 従来 FEC 技術の概要

4章よりデータを複数のブロックに分割し、複数の端末にブロックを転送させる事が必要だと考えた。一方で一部のブロックがクラウドに到達しない場合、クラウドからマシンに再送を要求すると遅延が増大する。このため、データを分割するだけでなく、クラウドからのデータの送達確認が不要な技術の適用が必要である。データの送信者が送信するメッセージに冗長性を付与する事により、データの受信者が追加情報を送信者に要求せずに誤りを検出し訂正する事を可能にする技術として、FEC(前方誤り訂正)が挙げられる。

FECには様々な方式があるが、IoTに適用するため演算量を極力抑制する事や想定するデータ到達率に適用可能である事から、5.1にてXOR(排他的論理和)[9]を、5.2にて冗長化を利用した方式について説明する。

5.1. XOR方式

図8にXORを利用したデータブロックの復元例を示す。例として3個のデータブロックに分割したとする。始めに送信者が1つのデータをビット長の均等な3個のデータブロックに分割し、各データブロックのXORを計算した冗長ブロック(以下、XORブロック)を生成する。合計4個のブロックを送信するが、伝送エラー等で3個目のデータブロックを損失したとする。正常に受信した1,2個目のデータブロックとXORブロックのXORを計算する事で、損失した3個目のデータブロックを復元できる。XOR方式では単純な演算で再送を要求せずにデータブロックを復元できるが、ブロックを2個以上損失するとデータの復元が不可能になる特徴を持つ。

- ① データを3つのブロックに分割し、
[1]～[3]のXORを計算したブロックを生成



- ③ [1][2][XOR]からXORを計算し、[3]を復元

図8 XOR を利用したデータブロックの復元例

5.2. 冗長化方式

図9にデータの冗長化を利用した例を示す。受信者へのデータ全体のクラウドへの到達率(以下、データ到達率)が低い領域では、誤りを検出し訂正するよりもデータを繰り返し送信する方法が一般的であり、処理量の少なさが特徴である。例えば Sigfox では常時同一データを3回送信している[2]。一方で データ到達率を事前に把握する必要があり、データ到達率が不明だと適切な送信数を設定できず、データを過剰に冗長化し無駄を発生させる可能性が生じる。

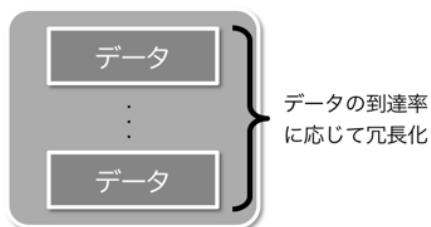


図9 冗長化を利用したデータの繰り返し送信

6. 従来 FEC 技術の適用時における課題

6.1. に従来の XOR 方式を、6.2. に従来の冗長化方式を適用した時に発生する課題について説明する。

6.1. XOR 方式の適用時における課題

表2にデータ分割数とデータの到達率・繰り返し送信数の関係を示す。マシンの1度に端末に転送できるバイト数は障害物の有無などの状況により様々である。ブロックの転送が完了しない場合は、転送できる端末が到達するまで当該ブロックを繰り返し送信する必要がある。

データ分割数が少ないと、1個あたりのブロックのサイズが増加する。サイズが大きすぎると端末がマシンとすれちがい時にブロックの受信を完了できない可能性が高くなるため、マシンから端末への送信数が増加し、マシンの消費電力が増大する。一方で、データの分割数が多いと1個あたりのブロックのサイズが減少するが、分割数が少ない時と比べてブロックを2個以上損失しやすくなるため、データを復元できずに到達率も低下する。すなわち、従来の XOR 方式を適用すると、データの到達率とマシンからのデータ繰り返し送信数の両立が困難と考えられる。

表2 データ分割数とデータの到達量・送信数の関係

データ分割数	少	多
1個あたりのブロックサイズ	大	小
データの到達量	○	△(低下)
マシンから端末への繰り返し送信数	△(増加)	○

6.2. 冗長化方式の適用時における課題

表3にデータの繰り返し送信数とブロック到達率の関係を示す。提案するサービスでは各端末が1日の間にフリースポットに接続する確率にばらつきが大きいと見込んでいる。また、マシンの近辺をどの端末が通過するか Wi-Fi 通信前には判断できない。そのため、適切なデータの繰り返し送信数を設定できないと考えられる。

マシンからデータを受け取った端末が1日以内にフリースポットに接続する確率(以下、ブロック到達率)が低い時にデータの繰り返し送信数が少ないと、クラウドまでデータが到達しない。一方で、ブロック到達率が高い時にデータの繰り返し送信数が多いとマシンの通信消費電力の無駄が発生する。このことから従来の冗長化技術では適切なデータの繰り返し送信数を設定できず、データ到達率とマシンの消費電力の両立が困難と考えられる。

表3 データの繰り返し送信とブロック到達率の関係

データ送信数	少	多
ブロック到達率(低)	△(不到達)	○
ブロック到達率(高)	○	△(消費電力の無駄)

7. 課題解決方法

7.1. に従来の XOR 方式の課題解決方法を、また、7.2. に従来の冗長化方式の課題解決方法を示す。

7.1. 可変長ブロック方式

図 10 に既存方式(上段)と提案方式(下段)を示す。提案方式では、1つのデータの転送の前にマシンが1つのデータをビット長 K の均等な N 個のデータブロックに分割し、XOR データ(ビット長 K)を生成する。マシンは端末とデータリンクを接続すると、端末にデータの先頭から順に最大 K ビット送信する。データリンクが切断されると、マシンは次の端末とデータリンクを接続して、未転送のバイト位置から転送する。最後に XOR ブロックを転送する。端末はデータリンクが切断すると、受け取ったバイト列に先頭バイト位置情報を付与して可変長ブロックを生成し、フリースポット接続時にクラウドに転送する。

既存技術では送信元(マシン)がデータを固定長に分割して XOR データを作成し、固定長のブロック単位で転送する。一方で提案方式では XOR データは送信元(マシン)が作成するが、データの転送は可変長であり可変長ブロック化を端末が行う。このため、既存技術ではブロックの送信途中でデータリンクが切断すると当該ブロックの全体を他の端末に再度送信する必要があったが、提案方式では一旦送信できたバイトの繰り返し送信が不要になった。

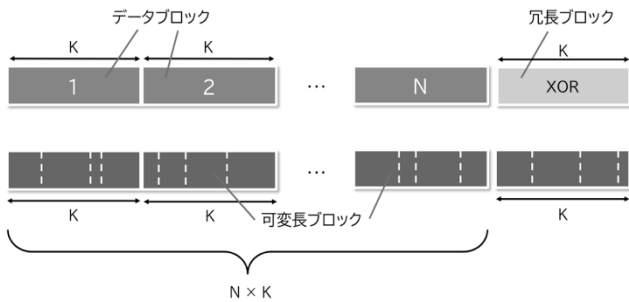


図 10 可変長ブロック方式 概要

また、従来の XOR 方式ではデータブロックにした単位で XOR ブロックを付与するため、ブロックが2個以上未到達の場合クラウドでのデータの復元が不可能だった。それに対して本提案では複数の可変長ブロックが未到達な場合でも、状況によってはクラウドによるデータ復元が可能となった。

図 11 に可変長ブロックを複数損失しても復元できる例について示す。クラウドは受信した各可変長データブロックを、XOR 計算で用いた長さ K バイトで折り返して2次元化し、損失した可変長ブロックを含む列について XOR 計算を行う。XOR の特徴より、縦軸内の可変長ブロックの損失箇所が1箇所以内であれば、データ全体の復元が可能である。

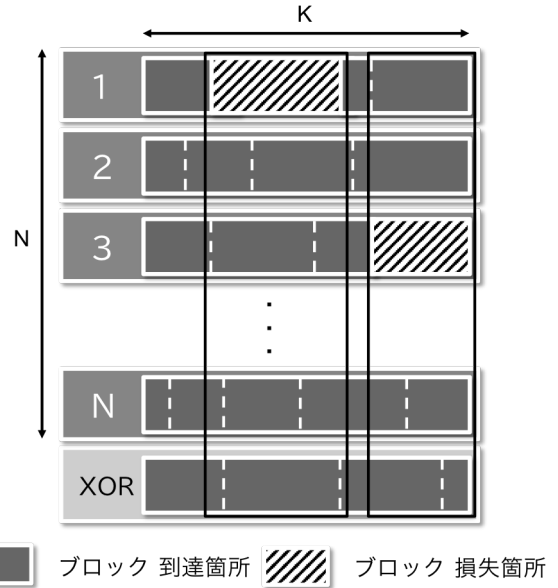


図 11 可変長ブロック損失時のデータ復元例

7.2. 部分再送方式

図 12 に提案方式を示す。始めにデータ1組分である N 個の可変長データブロックと XOR ブロックを複数の端末に転送する。端末がマシンへ接続する時に、マシンは端末の FS 接続率を認知できるため、データ到達率の算出が可能である。算出結果からデータ到達率の不足が予測される場合、FS 接続率の低い端末に転送したブロックのみを繰り返し送信する。繰り返し送信数が必要数のみであり、送信データ量も最小限になるため、消費電力を抑制しつつ十分なデータ到達率を実現できると考えている。

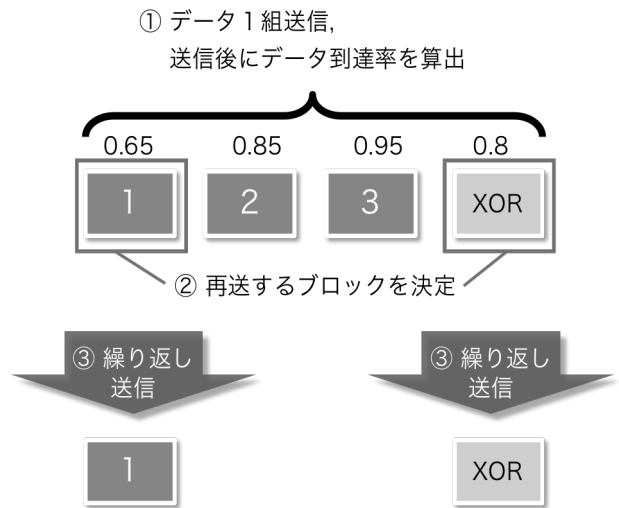


図 12 可変長ブロック方式 概要

8. まとめ

本稿では、IoT マシンとクラウド間の大量データ転送手法を示した。同手法は端末間の分散制御でデータを転送する既存技術とは異なり、クラウド内の管理サーバが集中制御して端末間のマルチホップ通信を実施させる。このため、事前に信頼関係のない任意の端末間で安全、低消費電力でかつ通信品質の高いデータ転送が可能である。また、同手法におけるマシンと端末間のデータ転送実験の結果を示しマシンの消費電力を抑止するためにはマシンとクラウド間でデータを分割・冗長化する技術が必要であることを報告した。そして従来の FEC 技術を適用時の課題を示すとともに、同課題を解決する可変長ブロック方式や部分再送方式を提案した。今後は提案方式を詳細化しレートレス符合など[10][11]最新の FEC 技術との定量評価を行う予定である。

謝辞

本論文の作成にあたり、京セラコミュニケーションシステムの池内賢治様から Sigfox のサーバや基地局を提供いただきました。また、機器の取り扱いや事業展開に関する講習会を定期的に関講いただき、細部にわたるご指導をいただきました。ここに感謝いたします。

参考文献

- [1] NTT, "高レスポンスやビッグデータ処理が要求される新たなアプリケーションの開拓を推進する「エッジコンピューティング構想」策定," NTT(オンライン),
[Online]www.ntt.co.jp/news2014/1401/140123a.html
- [2] Sigfox, [Online]www.sigfox.com
- [3] LoRa, [Online] www.lora-alliance. org/
- [4] NB-IoT, [Online] www.3gpp.org/images/PDF/R13_IOT_rev3.pdf
- [5] Takeshi Ogawa, Taichi Yoshimura, and Noriharu Miyaho, "Cloud Control DTN Utilizing General User' Smartphones for Narrowband Edge Computing," IEEE World Forum on Internet of Things 2018, pp. 19-24, Feb. 2018.
- [6] M. Liu, Y. Yan, and Q. Zhiguang, "A survey of routing protocols and simulations in delay-tolerant networks," International Conference on Wireless Algorithms, Systems, and Applications. Springer Berlin Heidelberg, 2011.
- [7] A. Lindgren, D. Avri, and S. Olov, "Probabilistic routing in intermittently connected networks," Service assurance with partial and intermittent resources, Springer Berlin Heidelberg, 2004, 239-254.
- [8] M. Opdenacker. "Embedded Linux size reduction techniques," "Embeded Linux Conference 2017.
- [9] 会津宏幸, 権藤俊一, and 辻雅史. "インターネットコンテンツ配信における前方誤り訂正技術," 東芝レビュー 65.6(2010): 36-39.
- [10] 西田昇平, 山崎景太, 石橋功至, 猿渡俊介, and 渡辺尚. "Spinal 符号を用いた重畳符号化伝送による無線通信の効率化について," 情報処理学会第 76 回全国大会, 357-358, Mar. 2014.
- [11] 佐々木力, 小林修, 長谷川輝之, 阿野茂浩, and 長谷川亨. "LT 符号を用いたマルチキャストコンテンツ配信における追加要求方式の検討," 情報処理学会研究報告, 2006, 139-146.