Vol.2020-CDS-29 No.2
2020/12/3

LPWA へ暗号技術を適用したセキュア農業 IoT システムの提案と性能評価

内山仁[1]　原田貴史[2]　田村桜子[3]　永井彰[2]　峰野博史[4]

概要：近年，Internet of things（IoT）技術と人工知能技術の急激な発展に伴い，データ収集と収集データに基づいたアクチュエーションを行う，IoT システムの開発が取り組まれている．特に，農業分野においては，農業従事者の高齢化に伴う作業負担の増加に対し，気温や湿度などの環境データに基づいた作物への灌水制御など，農作業効率化の研究が行われている．しかし，農業 IoT 実用化にはハードウェアやネットワークなど，様々な分野の課題が存在する．本研究では，農業 IoT の課題の一部であるネットワークの配線コスト及びセキュリティの課題解決のため，LPWA の一種である ZETA と ZETA 環境下で動作可能な公開鍵ベースの暗号プロトコルを用いた農業 IoT システムを提案と実環境における性能検証を実施した．毎分の灌水制御を想定したシステムにおいて，ZETA を用いたリアルタイムな通信の成功率は 99%以上であり，実運用に十分な性能であることを示した．

キーワード：IoT, LPWA, ZETA，農業, ID ベース認証鍵交換

1. はじめに

近年，農業分野における農業従事者の高齢化に伴う作業負担の増加や後継者不足による栽培技術の喪失という課題[1]に対し，IoT 技術を用いた労働負担の軽減や義栽培技術の形式知化を行う取り組みが進められている．農業における IoT システムでは，センサデバイスから農場の気温や湿度などの環境データを取得し見える化を行うサービスに加えて，取得したデータの分析を行い，分析結果に基づいた作物の灌水制御，農場の環境制御などを行うサービス（図 1）が想定される．

本研究では農業 IoT の実用化における課題の中から 2 つに着目した． 1 つ目はネットワーク配線コストの課題である．農業 IoT では環境データ取得のためのセンサ，農作物への灌水や農場の環境制御を目的としたアクチュエータなど，複数の IoT 端末が設置される．また，農場には農作物や栽培に必要な農業資材が配置されているため，IoT 端末を全て有線ネットワークで接続することは非常に困難であり，無線通信は農業 IoT の展開に最も重要な課題の 1 つである[2]．2 つ目はセキュリティの課題である．農場の環境の制御や灌水制御を行う端末に対して悪意をもったユーザがアクセスすることで，作物の成長を阻害する様な灌水などが可能であり，農家への金銭的損害などが危惧される．また，センサデータがアップロード中に改ざんされた場合，データの分析に基づいた制御が正しく行われず，間接的に作物への被害につながることが予想される．そのため，農業 IoT の運用には認証や暗号化などのセキュリティ機能が必要であると考えられる．

本研究では，農業 IoT 実用化にむけた課題解決のため，

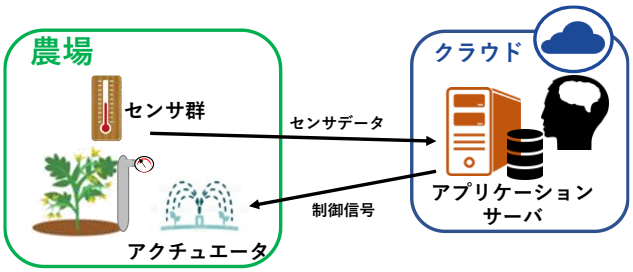


図 1 農業 IoT システムの例

LPWA の一種である ZETA[3]と ZETA 環境下で動作可能な ID ベース認証付き鍵交換プロトコル[4]を用いた，セキュアな IoT システムを提案する．提案したシステムは様々な用途での使用が予想されるが，本稿では農業 IoT を想定した．提案手法に関して毎分の灌水制御を目的とした栽培補助システムのプロトライプを構築し，実際の農場での栽培を通して動作検証を実施することで実用性の検討を行う．

以下，本論文の構成を述べる．第 2 章で関連技術についてまとめ，第 3 章で想定する農業 IoT と提案手法に関して述べる．第 4 章で提案手法の評価実験の内容と結果及び考察，第 5 章でまとめと今後の課題を述べる．

2. 関連技術

2.1 LPWA

LPWA(Low Power Wide Area) とは長距離のデバイス間の通信に用いられる通信規格の一つであり，通信レートが低く遅延が大きいものの，低消費電力かつ高いカバーエリアの通信を低コストで実現可能なことが特徴である．そのため，LPWA は長距離通信を必用とし，遅延のニーズが限られているアプリケーションに適しており[5]，スマートシティ，個人用 IoT アプリケーション，野生生物の監視など様々

1 静岡大学大学院総合科学技術研究科
2 NTT セキュアプラットフォーム研究所
3 株式会社 NTT ドコモ
4 静岡大学学術院情報学領域

表 1 ZETA と他 LPWA 規格の比較

	ZETA[3]	LoRaWAN[6]	SigFox[6]
周波数帯	920MHz・429MHz	920MHz	920MHz
エリア範囲	～10km	～10km	
通信速度	300bps(～2.4kbps)	100bps(～2.4kbps)	100bps
データサイズ	50byte	11byte	12byte
下り方向通信制限	特になし	10 メッセージ	4 メッセージ/日 データサイズは 8byte

なアプリケーションで機能することが期待されている．主な LPWA の規格として NB-IoT, LORAWAN, SigFox,, ZETA などが挙げられ，各通信規格で通信速度や一度に送信可能なデータサイズなどが仕様として定められている．

2.2 ZETA

ZETA は 2018 年に ZiFiSense 社が開発した LPWA 規格の一つである．ZETA は他の LPWA に比べて低コストであることや一度に送信可能なデータサイズが大きく比較的通信速度が高速であること，中継器を介した安定性の高い通信が可能であることが特徴である．また，下り方向への通信の回数や通信帯域等の制限が少なく双方向通信に適した規格である（表 1）．ZETA を用いる際のシステム構成を図 2 に示す．ZETA での通信は ZETA-MS，ZETA-AP，ZETA サーバの 3 つの要素を経由して通信を行われる．ZETA-MS は ZETA での長距離通信が可能なモジュールである．ZETA-MS には UART 通信インターフェースが備わっており，センサやアクチュエータ端末からシリアル通信で送られてきたデータを ZETA-AP まで送信する．ここで，ZETA-AP へのデータ送信には ZETA が用いられ，ZETA 独自のプロトコルでの通信が行われる．ZETA-AP は ZETA を構成する要素のうち基地局の役割をする要素である．ZETA-MS と通信可能な距離にユーザが設置することで，ZETA-MS から受信したデータの集約と ZETA サーバへの送信を行う．ZETA サーバへのデータ送信は LTE や家庭用の回線などを用いインターネットを介して行われる．ZETA サーバは ZETA-MS や ZETA-AP の接続監視や制御などのデバイス管理と，ZETA-AP から受信したデータを保存する役割の要素である．ZETA-MS と接続された端末と外部の端末から通信を行う場合は ZETA サーバを経由する必用がある．ZETA サーバと通信を行う際に用いられるプロトコルは二種類あり，ZETA サーバからデータを受信する上り方向の通信には MQTT，ZETA サーバへデータを送信する下り方向の通信

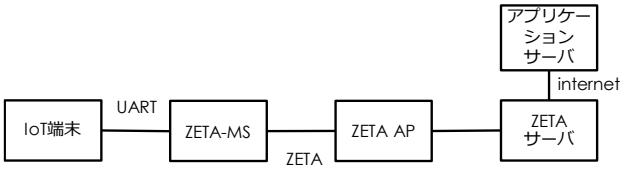


図 2 ZETA を用いたシステムの構成

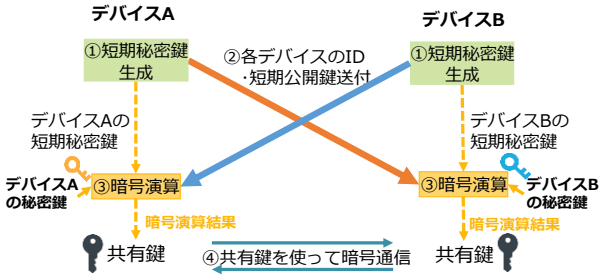


図 3 ID ベース認証付き鍵交換プロトコル

には ZETA サーバに用意された REST のインターフェースを用いて HTTP で通信を行う．

2.3 ID ベース認証付き鍵交換

ID ベース認証付き鍵交換は公開鍵暗号の発展形であり，ID ベース暗号を用いた認証付き鍵交換技術である．本プロトコルは認証と暗号化の両方が可能な暗号方式であり，PKI ベースの公開鍵暗号よりも通信量が少ないことが挙げられ[7]，通信量に制約がある LPWA などの環境において有効な手法である[8]．デバイス A とデバイス B で相互認証を行い，セキュアな通信を行うための共通鍵を交換するまでの動作を図 3 に示す．準備として KGC(KeyGeneration Center)より各デバイスの ID を元に作成した長期秘密鍵をデバイス A とデバイス B に配布しておく．各デバイスではセッションごとに短期秘密鍵と短期公開鍵を配布された長期秘密鍵を用いて生成し，通信相手の端末に対して自身の ID と短期公開鍵を送付する．このとき，短期鍵の計算に用いられる 楕円曲線上の群$E(\mathbb{F}_p)$ における部分群と$E(\mathbb{F}_{p^k})$の部分群の構成は 128 ビット安全である BN 曲線上の Optimal Ate ペアリング(BN462) が用いられる．共通鍵は自身の長期秘密鍵と短期秘密鍵，通信相手の ID と短期公開鍵を元に生成される．生成された共通鍵を用いることでデバイス間の認証と暗号化された通信が可能となる．

3. 提案手法

3.1 想定する農業 IoT

本研究では栽培補助を目的とし，農場とクラウド上に存在するサーバ間でデータのやり取りを行い，データのセンシングと農場のアクチュエータ機器の管理を遠隔地から行うクラウド型の IoT システムを想定する（図 1）．農場に設

置されたセンサ端末は，温度や湿度などの環境を示すデータや栽培されている農作物の状態を表すようなデータを収集し，クラウド上へアップロードする．アップロードされたデータはクラウド上のアプリケーションサーバにて処理や分析が行われ，農作物の栽培に適切なアクチュエータの動作を決定する．アクチュエータの動作決定には機械学習などの高度なデータ分析技術を頭脳部として用いることを想定している．収集されたデータはリアルタイムなアクチュエータ制御のためだけではなく，クラウド上のデータベースなどに蓄積された後に頭脳部の性能向上を目的とした学習に用いられる．学習やデータ蓄積のためには高い処理能力をもつ端末と大きなストレージが必要となるため，クラウド上へのシステム構築を想定する．頭脳部が決定したアクチュエータの動作は農場に設置されたアクチュエータ端末に送信され，アクチュエータ端末が命令に基づいた動作を行うことで栽培の補助を行う．ここでアクチュエータ端末や農作物に水やりをおこなう灌水機器，農場の環境制御を行うような送風機や暖房器などが予想される．アクチュエータ端末の動作結果はセンサ端末同様にクラウド上にアップロードされ，次回以降のアクチュエータ動作決定に利用される．

クラウド型のシステムのメリットとしては，農場のみで完結するエッジシステムに比べて，ストレージや処理能力の高いシステムを構築することが可能な点である．近年，IoT に用いられる小型端末の性能は向上しており，画像処理や機械学習の推論などの処理であれば農場に設置される端末内で実施することができる．しかし，機械学習のモデル更新のための学習などを行う際には農場の端末で行うことは難しい．そのため，動作決定を行う頭脳部分の更新が必要となるシステムではクラウド型で構築することが望ましい．また，収集されたデータへのアクセスが容易な点もメリットとして挙げられる．熟練農家の栽培技術を完全に自動化することは現在では難しく，栽培補助システムを利用している場合であっても人間が監視を行う必要がある．また，農作業すべてを機械化することも困難であるため，栽培補助システムと人間が協力して農作業を行う必要があり，その際農場のデータをリアルタイムに監視する機能は必要となる．農場のデータ取得の際にはアクセス可能な場所に制限が少ないクラウド型のシステムが適している．一方で，クラウド型のシステムではクラウドと農場の端末間でデータをやり取りする必要があり，データ通信のためのネットワークを整備する必要があることがデメリットとして挙げられる．また，通信によってシステム全体の処理時間が増加するため高いリアルタイム性を要求されるシステムには適さないことが予想される．

3.2 提案手法の概要

本稿では LPWA の一種である ZETA と ZETA 環境下で動作可能な公開鍵ベースの暗号プロトコルを用いた，セキュアなクラウド型の栽培補助システムを提案する（図 4）．提案システムはセンサ端末，アクチュエータ，ZETA-MS，ZETA-AP，ZETA サーバ，アプリケーションサーバの 6 つの要素で構成されている．センサ端末で収集された農場のデータは ZETA-MS を通じて ZETAAP, ZETA サーバまでアップロードされる．クラウド上に存在するアプリケーションサーバは ZETA サーバへアクセスし MQTT プロトコルを用いることでセンサ端末より収集されたデータを取得する．また，現場のアクチュエーション端末をアプリケーションサーバ上から操作する場合には，ZETA サーバに対して REST を用いて命令を送信することで ZETAAP と ZETA-MS を介してアクチュエータ端末まで命令が届けられる．ZETA を用いた通信は農場の端末に接続された ZETA-MS から ZETAAP までの通信に用いられ，センサ端末やアクチュータ端末が増加した際の配線コスト増加を低減できる．また，ZETA は 920MHz 帯などの比較的低い周波数帯を用いて通信を行うため，農場に存在する障害物の影響を受けづらいというメリットがある[9]. ID ベース認証付き鍵交換を用いた認証と暗号化はセンサ端末とアプリケーションサーバ間及びアクチュエータ端末とアプリケーションサーバ間で行われ，セキュアな通信が保障される．

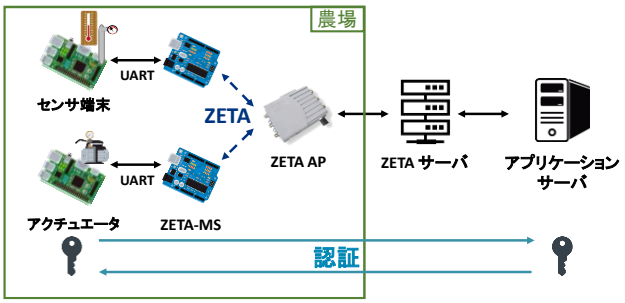


図 4 提案する農業 IoT システム

4. 実験

提案手法の実用性を検証するため栽培補助システムのプロトタイプを作成し，実際の農場において運用実験を行った．実験は静岡県袋井市のトマト栽培ハウスにて，6 月 23 日から 8 月 10 日にかけて行い，トマトの栽培補助を通してシステムの性能を調査した．

4.1 実験アーキテクチャ

実験で用いたシステム（以降は実験用システムと呼ぶ）は農作業のうち灌水の補助を行うことを目的とした灌水制御システムである（図 5）．実験用システムはセンサ端末として農場の温度，湿度，散乱光量を取得する環境センサと植物の状態を取得するカメラデバイスを利用する．ZETA のような通信速度に制限のある通信方式は画像をアップロードすることに適していないため，農場に設置されたデバイス内で画像の特徴のみを抽出し，数値データとしてサーバへアップロードする．実験用システムでは環境センサと

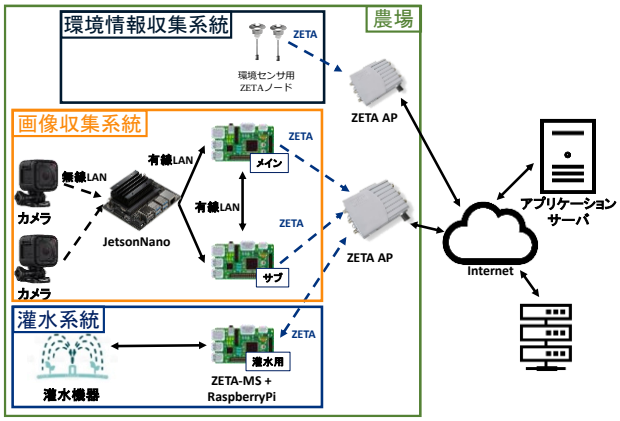


図 5 実験用システムの構成

図 6 画像収集系統のメッセージ

図 7 灌水系統のメッセージ

カメラデバイス用のセンサ端末をそれぞれ 2 台利用する今回の実験用システムアクチュエータ端末は灌水制御のみとなっている．センサ用端末とアクチュエータ端末には RaspberryPi を利用し，それぞれに ZETA-MS が接続されている．画像の特徴量抽出には JetsonNano を用いた．ZETA-AP は農場に 2 台設置し，環境センサとそれ以外の端末で接続先が別となっている．センサ端末から収集したデータ及び灌水制御の結果は ZETA-AP を介して ZETA サーバ，クラウド上のアプリケーションサーバまでアップロードされる．アプリケーションサーバではアップロードされたデータを元に植物の萎れ状態を推定し，適切な灌水タイミングを判断する．判断結果に基づいてアクチュエータ端末に対して灌水命令を送信し，アクチュエータ端末は命令を元に灌水を行う．実験用システムは毎分の灌水制御を目的としており，環境センサとカメラデバイスによるデータ収集及びサーバ上での灌水判断と灌水制御はそれぞれ 1 分周期で行われる．環境センサとカメラデバイスは共に 2 台ずつ設置されており，制御のためのデータをアップロードするメイン機とメイン機が不具合によって停止した時を想定して予備用のデータをアップロードするサブ機に分かれている．今回の実験においてはカメラデバイス用の 2 台の端末は ZETA での通信の衝突を防ぐため，ZETA でのアップロードタイミングを数秒程度ずらすようになっており，アップロードは基本的にメイン機がサブ機よりも先に行われるようになっている．

実験用システムにおいて画像収集系統と灌水系統からアプリケーションサーバへアップロードされるメッセージをそれぞれ図 6，図 7 に示す．画像収集系統のメッセージには画像から抽出した画像特徴量に加え，画像の撮影時刻を示すデータ収集時刻と撮影場所を示す処理区情報が含まれる．どのフィールドも固定長であり，メッセージ長は合計で 93byte となる．灌水系統のメッセージにはアプリケーションサーバからの命令が灌水用の RaspberryPi に到着した時刻，灌水が実施された時刻，灌水が行われた理由が含まれ，末尾には可変長の処理区名が付随する．本稿で示す実験において処理区名は数文字程度であり，灌水系統のメッセージ長は 16byte 程度であった．また，メッセージのアップロードの際には暗号通信用のヘッダが付け加えられる．そのため，画像収集系統からのメッセージに関しては ZETA で一度に送信可能なデータ長である 50byte を上回り，メッセージを複数回に分けてアップロードを行っている．

4.2 実験結果

実験システムのうち ZETA を用いた通信が多く通信の負荷が大きい画像収集系統に関して動作結果を分析し，システムの可動率と ZETA 及び処理の時間に関しての結果を評価した．

(1) 可動率

画像収集系統のデータアップロードに関する可動率を調査した．調査の対象となったのはデータアップロードのうちセンサの故障やシステム改善のための故意の停止を除いた動作を対象とした．また，処理の不具合に加えて処理時間が毎分の灌水制御に適していない時間となった割合に関しても調査を行った．

システムの可動率に関する実験結果を表 2 に示す．”総通信回数”は ZETA を用いて画像の特徴量のアップロード

表 2 システムの可動率

	総通信回数	エラー発生回数	可動率
メイン	45886	104	99.77%
サブ	46915	150	99.68%

可動率 = エラー発生回数/総通信回数

表 3 システムの処理時間

	50 秒時点での完了割合	60 秒時点での完了割合
メイン	97.02%	99.61%
サブ	92.48%	97.88%

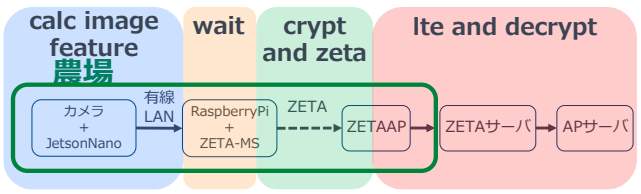
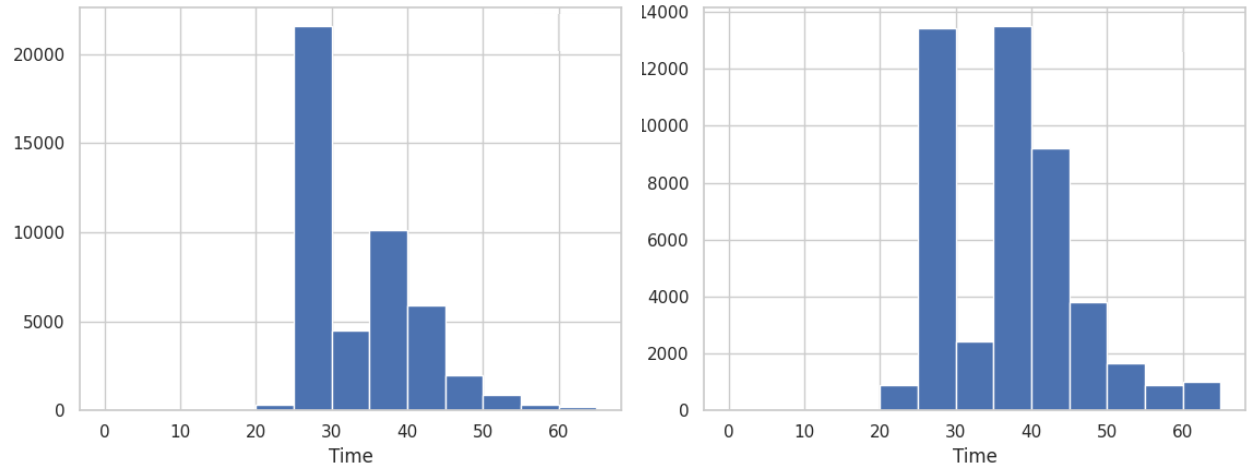
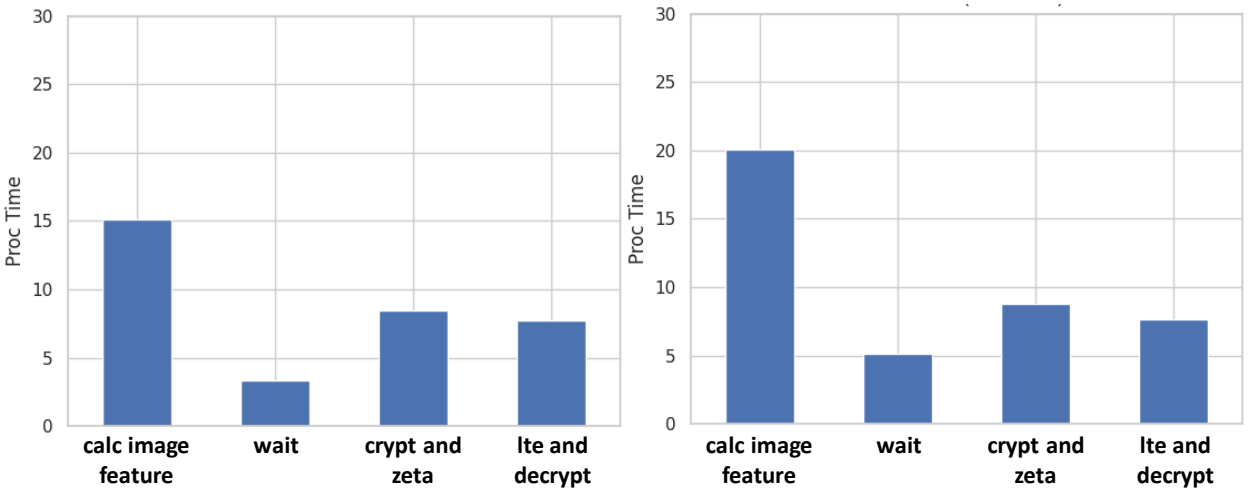


図 8 実験用システムの処理区分



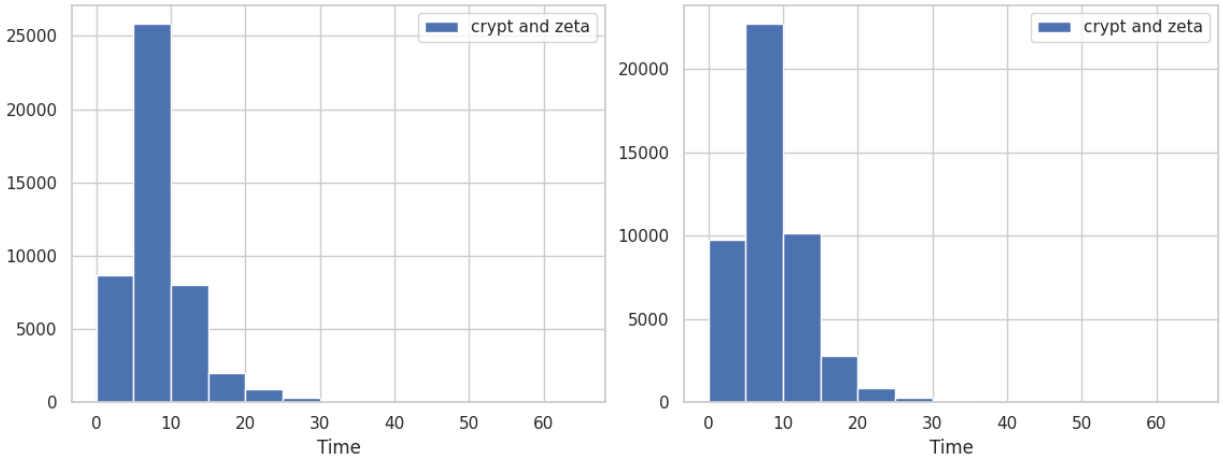
(a) メイン機 **(b) サブ機**

図 9 全処理時間の分布



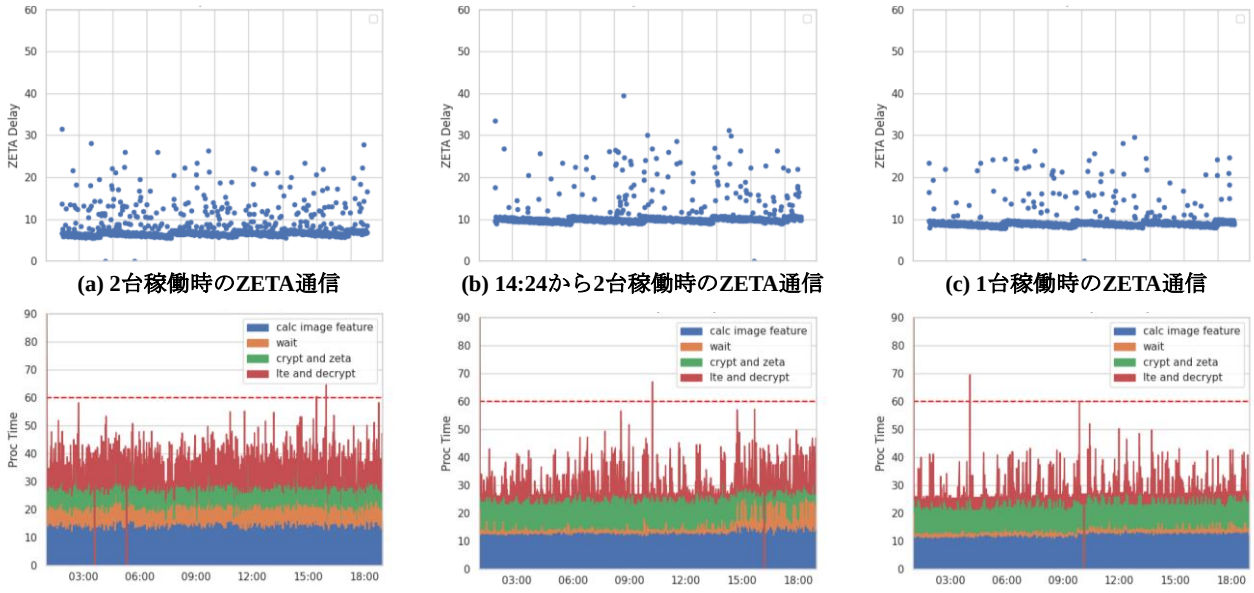
(a) メイン機 **(b) サブ機**

図 10 実験用システムの処理別所要時間平均



(a) メイン機 **(b) サブ機**

図 11 crypt and zeta 処理時間の分布



(a) 2台稼働時のZETA通信　(b) 14:24から2台稼働時のZETA通信　(c) 1台稼働時のZETA通信

(d) 2台稼働時の全処理　(e) 14:24から2台稼働時の全処理　(f) 1台稼働時の全処理

図 12 zeta and crypt と全処理の処理時間と時刻の関係

を試みた回数であり，そのうち ZETA-MS より先へデータが到達しなかった回数を”エラー発生回数”とした．画像収集系統に関してはどちらもエラー発生回数が少なく，可動率は 99%を超える高い数値となっている．また，正常にアップロードが完了した処理がどの程度時間を要したかの分布を図 9 に，50 秒及び 60 秒時点での全体の処理完了割合を表 3 に示す. まず, メイン機に関して 60 秒以内に 99%以上の処理が完了している．50 秒以内を対象とした場合であっても 97%以上の処理が完了しており，ほとんどの処理が毎分の灌水制御に必要なリアルタイム性を保持しているといえる．サブ機に関してはメイン機に比べて全体的に処理の時間が長い傾向にあることが図 9 より見て取れる．これはメイン機のアップロードタイミングよりも遅れてアップロードを開始する場合が多く，待ち時間が全体の処理に含まれることが多いためである．しかし，処理の時間が長い傾向にあるサブ機の場合であっても 98%程度が処理を完了している．これらの結果より，ZETA を用いたシステムは通信速度に制限がある環境において暗号化の処理を加えた通信を行った場合であっても毎分の栽培制御に実用可能な性能であることが示された．

(2) 処理時間に関する調査

提案手法に関して，性能の向上や ZETA に関する詳細な性能を調査するため，画像収集からクラウド上へのアップロードまでを 4 つの処理に区分して詳細な検証を行った．処理の区分を図 8 に示す．処理の区分は，画像データの収集と画像特徴量の算出を”calc image feature”，通信の衝突を避けるための待ち時間を”wait”，暗号化と ZETA を用いた通信を”crypt and zeta”，ZETAAP からクラウド上までの通信と復号を”lte and decrypt”とした．

各処理の時間を比較すると画像の特徴量を算出する”calc image feature”が最も長く，”crypt and zeta”が”lte and decrypt”よりもわずかに長く次点の処理の長さであった（図 10）．各処理時間と時刻のグラフを示した図 12(d)(e)(f)を見ると”calc image feature”は処理時間のばらつきが小さい事がわかる．また，画像の特徴量算出は灌水判断に利用するデータを変更しない限り大きく処理時間を短縮できないと考えた．一方で処理時間も長くばらつきも大きい”crypt and zeta”に関してその傾向を分析することでシステムの改善につながると考え，システムの詳細な処理時間に関して ZETA の通信処理を中心に分析することとした．

ZETA の通信処理である”crypt and zeta”に関する処理時間の分布を図 11 に示す．メイン機とサブ機両方に関して通信のほとんどが 15 秒以内に完了していることがわかる．わずかにサブ機の方が ZETA での通信に時間を要しているのは wait の時間が十分でないために通信の衝突が発生し，遅れて通信を開始した場合に通信の性能が低下するためであると予想される．

ZETA の通信衝突に関する影響について更に分析を行った．図 12 はカメラデバイスが通常通り 2 台稼働している場合と 1 台のみ稼働している場合と 1 台稼働から 2 台稼働に切り替わった場合の処理時間と時刻の関係を，ZETA の通信と全処理に関してそれぞれ示したグラフである．全処理に関して 1 台稼働時と図 12(d)と 2 台稼働時図 12(f)を比較すると，どちらも 60 秒以内に処理が完了している場合がほとんどであるものの，2 台稼働時は処理時間のばらつきが大きくなっていることが見て取れる．これは衝突回避のための”wait”の時間が含まれるようになったことが主な原因であることが図 12(e)より分かるが，”crypt and zeta”のばらつきが衝突によって大きくなったことも一因であると考える．実際に 1 台稼働時（図 12(a)）と 2 台稼働時（図

12(c)）の”crypt and zeta”の処理時間を見ると，2 台稼働時の方がわすかにばらつきが大きくなっていることが見て取れる．これらの結果から，ZETA 通信は通信タイミングによっては衝突が発生し通信性能を低下させるが，実験環境のような同時に通信を行う ZETA-MS が 2 台程度のシステムであれば毎分の制御に影響を与えるほどの性能低下は発生しないことが示された．

5. おわりに

本研究では農業 IoT の実用化に関する課題のうちネットワークの配線コストとセキュリティの問題に着目し，LPWA の一種である ZETA 及び ZETA 環境下での利用に適した ID ベース認証付き鍵交換プロトコルを用いた栽培補助システムを提案した．また，提案システムのプロトタイプを作成し実際の農場における灌水制御に利用することで実用性の検証を行った．性能検証の結果システムのデータ収集系統の可動率は 99%を超え高い安定を示した．また，処理時間に関しても，99%以上が 60 秒以内，97%以上が 50 秒以内に終了しており毎分のリアルタイムな灌水制御に必要な十分な性能をもつ事がわかった．また，処理時間に関して更に詳細な分析を行った結果, 2 台程度の ZETA-MS であれば衝突の影響を受けながらも大きく性能が低下しないことがわかった. 今後は ZETA-MS の台数を増やすことで，ZETA の通信衝突の影響を大きくした場合の性能を調査する予定である．

謝辞 本研究の一部は，JSPS 科研費 17H01730 の助成を受けたものである．また，実験環境を提供していただいた株式会社 Happy Quality の宮地様，サンファーム中山株式会社の玉井様に深い感謝の意を表する．

参考文献

[1] 農林水産省,農村の現状に関する統計:農林水産省, “ http://www.maff.go.jp/j/tokei/sihyo/data/12.html ”, (参照 2020-03-19).
[2] Muhammad Shoaib Farooq et al.,” A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming”,IEEE Access,pp156237-156271(2019)
[3] Techsor Inc.次世代 LPWAN 規格 ZETA の紹介, ”http://www.jasa.or.jp/TOP/download/technical/ZETA_2018-06-29_printed.pdf”,(参照 2020.03.19)
[4] J.Tomida, A. Fujioka, A. Nagai, and K, Suzuki,” Strongly Secure Identiry-Based Key Exchange with Single Pairing Operation ”, ESORICS2019(2019).
[5] Franck Muteba, Karim Djouani, Thomas Olwal,” A comparative Survey Study on LPWA IoT Technologies: Design, considerations, challenges and solutions ”, Procedia Computer Science,pp 636-641 (2019)
[6] 鄭立,” IoT ネットワーク LPWA の基礎-SIGFOX ”，LoRa, NB-IoT- ，リックテレコム(2017).
[7] 木下 魁，永井 彰，鈴木 幸太郎,” TLS1.3 への ID ベース認証鍵交換の適用と実装評価 ”，CSS2019(2019)
[8] Sakurako Tamura, Manami Ito, Akira Nagai, and Kan Yasuda,” A Study of Cryptographic Protocol Feasibility when Using TrustZone for Cortex-M and ZETA Environment”,CSS2019,pp25-32(2019)
[9] Hirofumi Ibayashi, Yukimasa Kaneda, Jungo Imahara, Naoki Oishi, Masahiro Kuroda, and Hiroshi Mineno,” Reliable Wireless Control System for Tomato Hydroponics”, Sensors (Basel). (2016)