(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7574930号
(P7574930)

(45)発行日　令和6年10月29日(2024.10.29)

(24)登録日　令和6年10月21日(2024.10.21)

(51)国際特許分類

Ｈ０４Ｗ　8/26　(2009.01)	Ｈ０４Ｗ	8/26
Ｈ０４Ｗ　4/38　(2018.01)	Ｈ０４Ｗ	4/38
Ｈ０４Ｗ　8/24　(2009.01)	Ｈ０４Ｗ	8/24
Ｈ０４Ｗ　76/10　(2018.01)	Ｈ０４Ｗ	76/10
Ｈ０４Ｗ　60/00　(2009.01)	Ｈ０４Ｗ	60/00

ＦＩ

請求項の数　7　（全13頁）　最終頁に続く

(21)出願番号　特願2023-529410(P2023-529410)
(86)(22)出願日　令和3年6月25日(2021.6.25)
(86)国際出願番号　PCT/JP2021/024157
(87)国際公開番号　WO2022/269906
(87)国際公開日　令和4年12月29日(2022.12.29)
審査請求日　令和5年11月16日(2023.11.16)
特許法第３０条第２項適用　令和３年に学会で発表

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100119677
弁理士　岡田 賢治
(74)代理人　100160495
弁理士　畑 雅明
(74)代理人　100115794
弁理士　今下 勝博
(72)発明者　椎名 亮太
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内
(72)発明者　玉置 真也
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】　データを収集するシステム、方法、装置及びプログラム

(57)【特許請求の範囲】

【請求項１】

標準規格化された無線通信プロトコルを用いて、収集対象の情報を端末からデータ収集部に収集するシステムであって、

前記端末は、

自装置を識別するための端末識別情報の履歴を保持し、

前記端末識別情報の履歴に保持されている少なくとも一つの端末識別情報、及び前記収集対象の情報以外のメタデータを、前記無線通信プロトコルで規定される制御系フレーム内の拡張領域に格納し、当該制御系フレームを前記データ収集部に送信し、

前記データ収集部は、

前記端末識別情報の履歴を前記端末ごとに保持し、

前記制御系フレームを受信すると、前記端末識別情報及び前記メタデータを前記制御系フレームから読み出し、

保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている端末識別情報に一致する端末を特定し、前記制御系フレームに格納されている前記メタデータを、特定した端末の前記収集対象の情報に紐づける、

システム。

【請求項２】

前記端末識別情報の履歴は、前記端末で生成された疑似ＭＡＣアドレスの履歴であり、

前記データ収集部は、

前記端末識別情報の履歴に、前記端末から受信した疑似ＭＡＣアドレスの履歴を前記端末ごとに保持し、
前記制御系フレームを受信すると、疑似ＭＡＣアドレスを前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている疑似ＭＡＣアドレスに一致する端末を特定する、
請求項１に記載のシステム。
【請求項３】
前記端末から送信された制御系フレームを前記データ収集部に転送する無線基地局を備え、
前記データ収集部は、
前記端末識別情報の履歴に、前記制御系フレームを転送した前記無線基地局の情報を前記端末ごとに保持し、
前記制御系フレームを受信すると、前記無線基地局の情報を前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記無線基地局の情報前記無線基地局の情報に一致する端末を特定する、
請求項１又は２に記載のシステム。
【請求項４】
前記メタデータは、前記端末の場所の特定が可能な情報を含み、
前記データ収集部は、
前記端末識別情報の履歴に、前記端末の場所の特定が可能な情報を前記端末ごとに保持し、
前記制御系フレームを受信すると、前記端末の場所の特定が可能な情報を前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記端末の場所に一致する端末を特定する、
請求項１から３のいずれかに記載のシステム。
【請求項５】
標準規格化された無線通信プロトコルを用いて、収集対象の情報を端末からデータ収集部に収集するシステムが実行する方法であって、
前記端末は、自装置を識別するための端末識別情報の履歴を保持し、
前記データ収集部は、前記端末識別情報の履歴を前記端末ごとに保持し、
前記端末は、前記端末識別情報の履歴に保持されている少なくとも一つの端末識別情報、及び前記収集対象の情報以外のメタデータを、前記無線通信プロトコルで規定される制御系フレーム内の拡張領域に格納し、当該制御系フレームを前記データ収集部に送信し、
前記データ収集部は、
前記制御系フレームを受信すると、前記端末識別情報及び前記メタデータを前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている端末識別情報に一致する端末を特定し、前記制御系フレームに格納されている前記メタデータを、特定した端末の前記収集対象の情報に紐づける、
方法。
【請求項６】
標準規格化された無線通信プロトコルを用いて、収集対象の情報を端末からデータ収集部に収集するシステムに備わる前記データ収集部として機能する装置であって、
前記端末を識別するための端末識別情報の履歴を前記端末ごとに保持し、
前記端末識別情報の履歴に保持されている少なくとも一つの端末識別情報、及び前記収集対象の情報以外のメタデータを、前記無線通信プロトコルで規定される制御系フレームを受信すると、前記端末識別情報及び前記メタデータを前記制御系フレームから読み出し、

保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている端末識別情報に一致する端末を特定し、前記制御系フレームに格納されている前記メタデータを、特定した端末の前記収集対象の情報に紐づける、
装置。
【請求項７】
請求項６に記載の装置に備わる各機能部としてコンピュータを実現させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、ＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）向け通信技術に関する。
【背景技術】
【０００２】
無線ＬＡＮシステムを使ったＩｏＴのデータ収集システムにおいては、端末識別のためにＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスとメタデータ、センサデータと合わせて、上位サーバへと送信し、メタデータ及びセンサデータと端末との紐づけを行っている。
【０００３】
これまでの無線ＬＡＮシステムでは、端末識別情報として送信しているＭＡＣアドレスは一般的に端末固有のものであり、複数存在しないといった前提があった。一方、近年、セキュリティ意識の高まりから、Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔをキャプチャすることで端末が一意に特定されてしまうことが問題となり、ＭＡＣアドレスをランダム化する機能が実装され、多くの端末（Ａｎｄｒｏｉｄ、ｉＯＳなど）において利用されつつある。
【０００４】
非特許文献１及び２では、機器情報格納処理部を設けて、端末識別のためにＭＡＣアドレスとメタデータ、センサデータと合わせて、上位サーバへと送信し、端末とメタデータ及びセンサデータとの紐づけを行っている。しかしながら、例えば、端末の移動や持ち出しによって接続先基地局を変更する場合など、ＭＡＣアドレスのランダム化を実施してしまうと、基地局を跨いだ端末の追跡ができず、連続した端末管理が難しい。
【先行技術文献】
【非特許文献】
【０００５】
【文献】ＩｏＴデータ信頼性向上に向けた無線ＬＡＮメタデータ収集方式における端末負荷と消費電力の評価、椎名亮太・玉置真也・鈴木徹也・木村康隆・谷口友宏、信学総大、Ｂ－８－１１　、２０２１年３月
【文献】低レイヤメタデータ収集方式を用いたＩｏＴ機器の論理／物理構成一致管理システムへの適用例、玉置真也・椎名亮太・鈴木徹也・木村康隆・黄　掣・秦野智也・山田崇史・谷口友宏、信学総大、Ｂ－８－１２　、２０２１年３月
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本開示は、ＭＡＣアドレスのランダム化を実施した場合においても、基地局を跨いだ端末の追跡を可能にすることを目的とする。
【課題を解決するための手段】
【０００７】
本開示は、低レイヤの通信プロトコルを活用し、センサデータやメタデータを収集しつつ、端末を一意に特定できる真のＭＡＣアドレスを用いることなく、端末の識別を行う。端末、基地局、管理サーバを連携し、端末によって生成される疑似ＭＡＣアドレスや、端末と基地局間のネットワーク接続情報から端末識別を実施する。また、収集するメタデータの種類によっては、メタデータのみで、端末識別を実施してもよい。これらにより端末

の移動元を推定可能にし、端末移動履歴を作成する。
【０００８】
具体的には、本開示のシステムは、
標準規格化された無線通信プロトコルを用いて、収集対象の情報を端末からデータ収集部に収集するシステムであって、
前記端末は、
自装置を識別するための端末識別情報の履歴を保持し、
前記端末識別情報の履歴に保持されている少なくとも一つの端末識別情報、及び前記収集対象の情報以外のメタデータを、前記無線通信プロトコルで規定される制御系フレーム内の拡張領域に格納し、当該制御系フレームを前記データ収集部に送信し、
前記データ収集部は、
前記端末識別情報の履歴を前記端末ごとに保持し、
前記制御系フレームを受信すると、前記端末識別情報及び前記メタデータを前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている端末識別情報に一致する端末を特定し、前記制御系フレームに格納されている前記メタデータを、特定した端末の前記収集対象の情報に紐づける。
【０００９】
具体的には、本開示の方法は、
標準規格化された無線通信プロトコルを用いて、収集対象の情報を端末からデータ収集部に収集するシステムが実行する方法であって、
前記端末は、自装置を識別するための端末識別情報の履歴を保持し、
前記データ収集部は、前記端末識別情報の履歴を前記端末ごとに保持し、
前記端末は、前記端末識別情報の履歴に保持されている少なくとも一つの端末識別情報、及び前記収集対象の情報以外のメタデータを、前記無線通信プロトコルで規定される制御系フレーム内の拡張領域に格納し、当該制御系フレームを前記データ収集部に送信し、
前記データ収集部は、
前記制御系フレームを受信すると、前記端末識別情報及び前記メタデータを前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている端末識別情報に一致する端末を特定し、前記制御系フレームに格納されている前記メタデータを、特定した端末の前記収集対象の情報に紐づける。
【００１０】
具体的には、本開示の装置は、
標準規格化された無線通信プロトコルを用いて、収集対象の情報を端末からデータ収集部に収集するシステムに備わる前記データ収集部として機能する装置であって、
前記端末を識別するための端末識別情報の履歴を前記端末ごとに保持し、
前記端末識別情報の履歴に保持されている少なくとも一つの端末識別情報、及び前記収集対象の情報以外のメタデータを、前記無線通信プロトコルで規定される制御系フレームを受信すると、前記端末識別情報及び前記メタデータを前記制御系フレームから読み出し、
保持している前記端末識別情報の履歴のなかから前記制御系フレームに格納されている端末識別情報に一致する端末を特定し、前記制御系フレームに格納されている前記メタデータを、特定した端末の前記収集対象の情報に紐づける。
【００１１】
具体的には、本開示のプログラムは、本開示に係る装置に備わる各機能部としてコンピュータを実現させるためのプログラムであり、本開示に係る装置が実行する通信方法に備わる各ステップをコンピュータに実行させるためのプログラムである。
【発明の効果】
【００１２】
ＩｏＴのデータ収集システムにおいて、メタデータに加えて、疑似ＭＡＣアドレスや、

端末と基地局間のネットワーク接続情報から、端末移動履歴を作成し管理に用いることで、ＭＡＣアドレスのランダム化を実施した場合においても基地局を跨いだ端末の管理がプロトコル改変なしで実現できる。

【図面の簡単な説明】

【００１３】

【図１】データ収集システム構成の一例を示す。

【図２】本開示のシステムの構成例を示す。

【図３】本開示のシステムの構成例を示す。

【図４】端末が無線基地局に接続する際の動作の一例を示す。

【図５】本開示のシステムの構成例を示す。

【図６】本開示の端末の構成例を示す。

【図７】メタデータを格納する領域を説明する例である。

【発明を実施するための形態】

【００１４】

以下、本開示の実施形態について、図面を参照しながら詳細に説明する。なお、本開示は、以下に示す実施形態に限定されるものではない。これらの実施の例は例示に過ぎず、本開示は当業者の知識に基づいて種々の変更、改良を施した形態で実施することができる。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。

【００１５】

（データ収集システム）

図１に、データ収集システムの構成の一例を示す。データ収集システムは、端末１１が管理サーバ１３と通信ネットワーク１４で接続されている。

【００１６】

端末１１は、収集対象の情報、メタデータ及び端末識別情報を、データ収集部として機能する管理サーバ１３に送信する。収集対象の情報は、例えばセンサ２０から取得したセンサデータである。メタデータは、端末１１で取得されるデータであり、センサデータ以外の任意の情報を含む。端末識別情報は、端末１１を識別可能な任意の情報であり、例えば、ＭＡＣアドレスである。

【００１７】

センサデータは、標準規格化されたプロトコルで規定されるデータフレームを用いて送信される。データフレームには、端末識別情報であるＭＡＣアドレスが格納される。一方、センサデータ以外のメタデータは、標準規格化された無線通信プロトコルで規定される制御系フレームを用いて送信される。制御系フレームにも、端末識別情報であるＭＡＣアドレスが格納される。

【００１８】

ここで、標準規格化されたプロトコルで規定されるデータフレームは、例えばＴＣＰ／ＩＰのデータフレームである。制御系フレームは、例えばＷｉ－Ｆｉ（ＩＥＥＥ８０２．１１）で定められているプローブ要求である。プローブ要求は、レイヤ２の信号であり、センサデータを送信するためのＴＣＰ／ＩＰのデータ通信が確立する前に、端末１１と無線基地局１２＃Ａ及び１２＃Ｂとの間で送受信する。このため、管理サーバ１３は、ＴＣＰ／ＩＰのデータ通信が確立する前にプローブ要求で送られてくる情報を得ることができ、例えば、ＩＰアドレスの設定などにプローブ要求で送られてくる情報を利用することができる。

【００１９】

管理サーバ１３は、データフレームからセンサデータ及び端末識別情報を読み出し、センサデータ及び端末識別情報の紐づけを行う。管理サーバ１３は、制御系フレームからメタデータ及び端末識別情報を読み出し、メタデータ及び端末識別情報の紐づけを行う。センサデータ及びメタデータは端末識別情報と紐づけられている。これにより、管理サーバ１３は、メタデータ及びセンサデータと端末１１との紐づけを行うことが可能になる。

【００２０】
ここで、端末識別情報の隠蔽処理を行い、ＭＡＣアドレスがＡ０：Ｂ２：Ｄ５：７Ｆ：８１：Ｂ３からＤ０：Ｃ２：Ｄ５：９Ｆ：１０：Ｃ５に変わってしまうと、管理サーバ１３のデータベース上では無線基地局１２＃Ａの端末１１が消え、無線基地局１２＃Ｂに新規の端末１１が設置されたと見えてしまう。このため、管理サーバ１３での端末１１の管理が困難になる。
【００２１】
本開示では、端末１１、無線基地局１２＃Ａ及び１２＃Ｂ、管理サーバ１３を連携し、端末１１から端末識別情報として送信されたＭＡＣアドレスだけでなく、端末１１と無線基地局１２＃Ａ及び１２＃Ｂ間のネットワーク接続情報などに基づいて端末１１の識別を行う。また、収集するメタデータの種類によっては、メタデータのみで、端末１１の識別を行う。これらにより、ＭＡＣアドレスのランダム化を実施した場合においてもプロトコル改変なしで、無線基地局１２＃Ａ及び１２＃Ｂを跨いだ端末１１の管理を可能とする。
【００２２】
本開示の「収集対象の情報」は、端末１１に備わる任意の機器情報など、端末１１で取得可能な任意の情報とすることができるが、以下ではその一例として、センサ２０で取得されたセンサデータである例について説明する。
【００２３】
（第１の実施形態）
図２を参照しながら、本実施形態のシステムについて説明する。本実施形態では、端末識別情報として疑似ＭＡＣアドレスを用いた端末１１の管理を行う。
端末１１は、センサ２０に加え、疑似ＭＡＣアドレス履歴テーブルを備える。端末１１は、センサデータ、メタデータ、及び疑似ＭＡＣアドレスを、管理サーバ１３に送信する。無線基地局１２＃Ａは、接続端末情報として、端末接続数、接続端末ＭＡＣアドレス（疑似）、接続開始時刻、接続断時刻を管理サーバ１３に送信する。
【００２４】
管理サーバ１３は、センサデータ及びメタデータと端末１１との紐づけを行う。これに加え、管理サーバ１３は、疑似ＭＡＣアドレス履歴テーブル及び端末移動履歴を、個別の端末１１ごとに管理する。疑似ＭＡＣアドレス履歴テーブルは、端末識別情報に、疑似ＭＡＣアドレスの履歴を紐づけて、端末１１を管理する。端末移動履歴は、個別の端末１１ごとに、端末移動履歴を更新する。
【００２５】
端末１１の基地局移動時には、端末１１は、疑似ＭＡＣアドレス履歴テーブルの一部の情報を、制御系フレームの一種であるプローブ要求フレームで管理サーバ１３に送信する。すなわち、端末１１は、真のＭＡＣアドレスは送信せず、過去の疑似ＭＡＣアドレスを管理サーバ１３に送信する。この制御系フレームには、メタデータを格納してもよいが、メタデータは格納されていなくてもよい。無線基地局１２＃Ｂは、端末１１の接続端末情報として、過去の疑似ＭＡＣアドレスを管理サーバ１３に送信する。
【００２６】
管理サーバ１３は、端末識別情報として送信された疑似ＭＡＣアドレスと接続端末情報をマッチングし、過去の無線基地局１２＃Ａや端末識別情報を特定し、個別の端末１１ごとに、端末移動履歴を更新する。これにより、端末識別情報として疑似ＭＡＣアドレスを用いた場合であっても、端末１１の管理が可能になる。
【００２７】
（第２の実施形態）
図３を参照しながら、本実施形態のシステムについて説明する。本実施形態では、端末識別情報として端末１１と無線基地局１２間のネットワーク接続情報を用いた端末１１の管理を行う。以下、ネットワークを（ＮＷ）と称する場合がある。
端末１１は、センサ２０に加え、ＮＷ接続情報を備える。端末１１は、センサデータ、メタデータ及びＮＷ接続情報を、管理サーバ１３に送信する。ＮＷ接続情報は、端末１１

が無線通信に用いた任意の情報であり、例えば、接続先基地局ＭＡＣアドレス、接続開始時刻、接続断時刻、ｃｈ／周波数／送受信信号電力の少なくともいずれかを含む。無線基地局１２＃Ａは、接続端末情報として、端末接続数、接続端末のＭＡＣアドレス（疑似）、接続開始時刻、接続断時刻のほか、ｃｈ／周波数／送受信信号電力などのＮＷ接続情報を、管理サーバ１３に送信する。

【００２８】

管理サーバ１３は、センサデータ及びメタデータと端末１１との紐づけを行う。これに加え、管理サーバ１３は、疑似ＭＡＣアドレス履歴テーブル、端末移動履歴及び接続端末情報を保持する。

【００２９】

基地局移動時には、端末１１は、移動前のＮＷ接続情報を、制御系フレームの一種であるプローブ要求で管理サーバ１３に送信する。この制御系フレームには、メタデータを格納してもよいが、メタデータは格納されていなくてもよい。無線基地局１２＃Ｂは、端末１１の接続端末情報として、移動前のＮＷ接続情報を管理サーバ１３に送信する。

【００３０】

管理サーバ１３は、保持しているＮＷ接続情報と、無線基地局１２＃Ｂから送信される接続端末情報をもとに、端末識別情報を特定し、個別の端末１１ごとに、端末移動履歴を更新する。すなわち、端末１１と無線基地局１２間のＮＷ接続情報を用いた端末管理を行う。

【００３１】

図４に、第１及び第２の実施形態において、端末１１が無線基地局１２に接続する際の動作の一例を示す。

端末１１の無線基地局１２を移動しない場合（ステップＳ１１においてＹｅｓ）、メタデータを制御系フレームに挿入し（Ｓ１２）、制御系フレームを送信する（Ｓ１３）。

端末１１の無線基地局１２を移動した場合（ステップＳ１１においてＮｏ）、端末識別情報を制御系フレームに挿入し（Ｓ１５）、メタデータを制御系フレームに挿入し（Ｓ１６）、制御系フレームを送信する（Ｓ１７）。

【００３２】

（第３の実施形態）

図５を参照しながら、本実施形態のシステムについて説明する。本実施形態では、メタデータのみを用いた端末１１の管理を行う。

端末１１は、センサデータ及びメタデータを、管理サーバ１３に送信する。無線基地局１２＃Ａは、接続端末情報として、端末接続数、接続開始時刻、接続断時刻のほか、ｃｈ／周波数／送受信信号電力などのＮＷ接続情報を、管理サーバ１３に送信する。

【００３３】

端末１１は、メタデータ履歴テーブルを備える。メタデータ履歴テーブルは、無線基地局１２＃Ａに接続していたときのメタデータをテーブルとして保持する。メタデータ履歴は、端末１１の収集している任意のデータであり、位置や設置者、環境などの情報が例示できる。

【００３４】

管理サーバ１３は、センサデータ及びメタデータと端末１１との紐づけを行う。これに加え、管理サーバ１３は、接続端末情報（無線基地局）及び端末移動履歴を、個別の端末１１ごとに管理する。

【００３５】

端末１１の基地局移動時には、端末１１は、メタデータ履歴に格納されている、過去のメタデータの少なくとも一部を管理サーバ１３に送信する。この制御系フレームには、メタデータを格納してもよいが、メタデータは格納されていなくてもよい。無線基地局１２＃Ｂは、端末１１の接続端末情報を管理サーバ１３に送信する。

【００３６】

管理サーバ１３は、収集したメタデータ履歴をもとに、管理サーバ１３上の、これまで

収集したメタデータから端末識別情報を特定し、個別の端末１１ごとに、端末移動履歴を更新する。すなわち、メタデータのみを用いた端末管理を行う。

【００３７】

本実施形態では、メタデータとして、位置や設置者、環境などの情報から、場所の特定が可能な場合、疑似ＭＡＣアドレス履歴テーブルやＮＷ情報などは送信しなくてもよい。例えば、端末１１は、無線基地局１２の移動時に、メタデータとして、位置や設置者、環境などの情報から、場所の特定が可能な場合、疑似ＭＡＣアドレス履歴テーブルやＮＷ情報などは送信せず、移動前の無線基地局１２＃Ａに接続していたときのメタデータの少なくとも一部を管理サーバ１３へ送信してもよい。

【００３８】

（第４の実施形態）

図６に、端末１１の構成例を示す。端末１１は、無線送受信処理部２１、通信プロトコル動作処理部２２、端末識別情報格納処理部２３、各種メタデータ格納処置部２４、センサデータ格納処理部２５、位置情報検出部２６、設置者検出部２７、環境情報検出部２８、センサ２０を備える。

【００３９】

位置情報検出部２６は、センサ２０の位置情報を検出する任意の手段であり、例えば、ＧＰＳを含む衛星測位システム、加速度センサ、ジャイロ、Ｗｉ－Ｆｉ信号やＢＬＥビーコン信号などのＲＳＳＩ（Ｒｅｃｅｉｖｅｄ　Ｓｉｇｎａｌ　Ｓｔｒｅｎｇｔｈ　Ｉｎｄｉｃａｔｏｒ）受信である。

【００４０】

設置者検出部２７は、端末１１のユーザの情報を検出する任意の手段である。例えば、以下が例示できる。

・設置者の識別を行う情報：

指紋センサ、静脈センサ、カメラ（顔／虹彩認識）、マイク（声紋検出）

・設置者の状況の情報：

設置者が身に着けているセンサの出力値（例：血圧、心拍、移動速度、発言／会話）を、通信手段を介して受信する。

【００４１】

環境情報検出部２８は、センサデータ以外の情報（メタデータ）を取得する。いずれか１つでもよいし、全てでもよい。

【００４２】

端末識別情報格納処理部２３は、端末１１を識別するための、疑似ＭＡＣアドレス履歴テーブル、ＮＷ接続情報などを格納する。

センサデータ格納処理部２５は、センサ２０からのセンサデータを格納する。

【００４３】

無線送受信処理部２１は、データフレーム及び制御系フレームを送受信する。例えば、無線送受信処理部２１は、制御系フレームの独自拡張領域に、各種のメタデータの格納されている制御系フレームを送信する。センサデータについては、データフレームのペイロード領域に格納して送信する。

通信プロトコル動作処理部２２は、制御系フレームを送受信する。

【００４４】

各種メタデータ格納処置部２４は、位置情報検出部２６、設置者検出部２７及び環境情報検出部２８からのデータを、それぞれ、無線通信プロトコルの制御系フレームの独自拡張領域に格納する。ここで、制御系フレームとは、無線通信プロトコルがＷｉ－Ｆｉ（ＩＥＥＥ８０２．１１）であれば、データフレーム以外の管理フレーム及び制御フレームである。

【００４５】

管理フレームには、

Ｂｅａｃｏｎフレーム（ネットワーク情報を報知するフレーム）、

Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔフレーム（ネットワーク情報を要求するフレーム）、
Ｐｒｏｂｅ　Ｒｅｓｐｏｎｓｅフレーム（Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔに対する応答）、
Ａｓｓｏｃｉａｔｉｏｎ　Ｒｅｑｕｅｓｔフレーム（接続を要求するフレーム）、
Ａｓｓｏｃｉａｔｉｏｎ　Ｒｅｓｐｏｎｓｅフレーム（Ａｓｓｏｃｉａｔｉｏｎ　Ｒｅｑｕｅｓｔに対する応答）、
Ｄｉｓａｓｓｏｃｉａｔｉｏｎフレーム（通信の切断を行うフレーム）、
Ａｕｔｈｅｎｔｉｃａｔｉｏｎフレーム（相手を認証するフレーム）、
Ｄｅ－Ａｕｔｈｅｎｔｉｃａｔｉｏｎフレーム（切断（認証中止）するフレーム）、
Ａｃｔｉｏｎフレーム（追加の機能全般用のフレーム）、
が含まれる。

【００４６】
　また、制御フレームには、
ＲＴＳフレーム（これからデータ送信をしてもいいか確認するフレーム）、
ＣＴＳフレーム（これからデータ送信をするというフレーム）、
Ａｃｋフレーム（データを正常に受信したという確認フレーム）、
Ｂｌｏｃｋ　Ａｃｋ　Ｒｅｑｕｅｓｔフレーム（確認フレーム（Ｂｌｏｃｋ　Ａｃｋ）を要求するフレーム）、
Ｂｌｏｃｋ　Ａｃｋフレーム（複数のＭＡＣフレームに対する確認フレームをまとめたもの）、
が含まれる。

【００４７】
　各種メタデータ格納処置部２４は、独自拡張領域の様式／制限に適合するように、データを、ある短縮コードに変換したり、複数フレームに分ける（フラグメンテーション）するなど、加工した上で格納してもよい。格納タイミングは、データ更新の都度、逐次格納してもよいし、データを一定期間蓄積した上で格納してもよい。格納するデータは、記録（ログ）を含んでいてもよいし、特定の計算／統計処理をした結果を格納してもよい。格納するメタデータ種別及びタイミングは、一定に限らず、端末１１側、もしくは、データ分析部やデータ収集部からの指示で動的に変更してもよい。格納するデータは、データ分析部や収集部からの指示または端末側に予め設定された暗号鍵を用いて暗号化して格納してもよい。

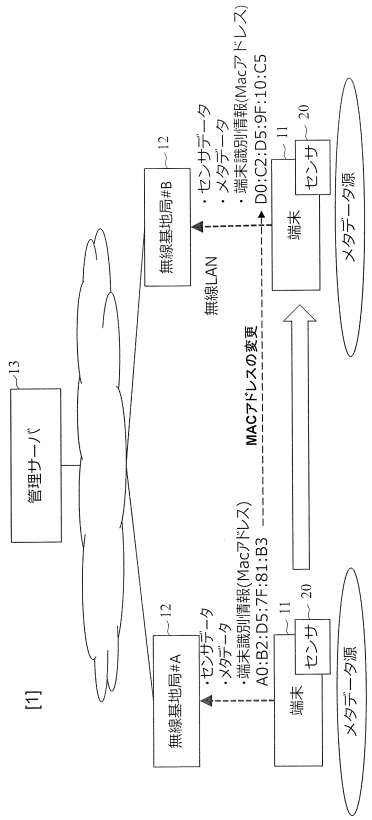
【００４８】
　図７は、ＩＥＥＥ８０２．１１無線ＬＡＮの制御系フレームの中の、メタデータを格納する領域を説明する例である。図７（Ａ）は、制御系フレームがプローブ要求フレームである場合の例である。メタデータは、“Ｖｅｎｄｏｒ　Ｓｐｅｃｉｆｉｃ”領域ＥＸＰに格納される。図７（Ｂ）は、制御系フレームがプローブ応答フレームである場合の例である。メタデータは、“Ｖｅｎｄｏｒ　Ｓｐｅｃｉｆｉｃ”領域ＥＸＰに格納される。なお、図７の出典は次である。
ＩＥＥＥ　Ｓｔｄ　８０２．１１－２０１６，ｐ．７０８－７１２，
ＩＥＥＥ　Ｓｔａｎｄａｒｄ　ｆｏｒ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｅｃｈｎｏｌｏｇｙ．
Ｌｏｃａｌ　ａｎｄ　Ｍｅｔｒｏｐｏｌｉｔａｎ　Ａｒｅａ　Ｎｅｔｗｏｒｋｓ．
Ｓｐｅｃｉｆｉｃ　Ｒｅｑｕｉｒｅｍｅｎｔｓ，
Ｐａｒｔ　１１：　Ｗｉｒｅｌｅｓｓ　ＬＡＮ　ＭＡＣ　ａｎｄ　ＰＨＹ　Ｓｐｅｃｉｆｉｃａｔｉｏｎｓ，

【００４９】
　本開示のデータ収集システムは、センサデータの収集に用いる通信プロトコルの拡張機能又はオプション機能を用いて、センサデータ以外のメタデータを収集する。これにより、ＩｏＴのデータ収集システムにおいて、高い性能を要求しない低レイヤの通信プロトコルを活用して、センサデータに加えて、メタデータを一括して収集することができるため、コスト向上や運用の煩雑化、および、センサデータとメタデータの関連付けの際のエラー発生を回避して、経済的かつ信頼性の高いシステムを実現できる。

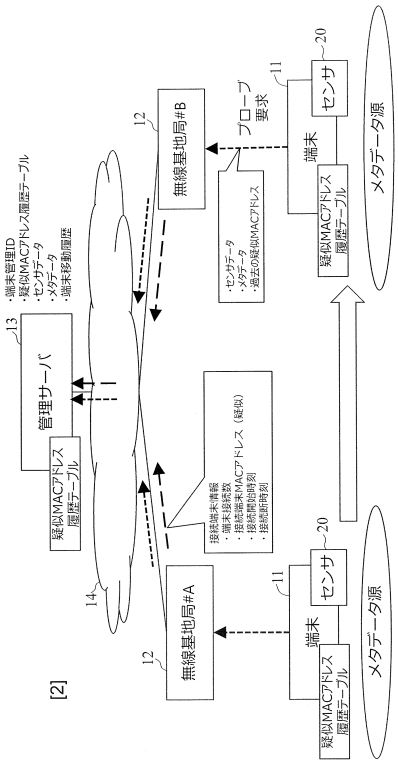
【００５０】
なお、上述のシステムでは管理サーバ１３がセンサデータを収集する例を示したが、本開示はこれに限定されない。例えば、センサデータに代えて又はセンサデータと共に、端末１１の機器情報を収集してもよい。また、本開示の装置はコンピュータとプログラムによっても実現でき、プログラムを記録媒体に記録することも、ネットワークを通して提供することも可能である。
【産業上の利用可能性】
【００５１】
本開示は情報通信産業に適用することができる。
【符号の説明】
【００５２】
１１：端末
１２：無線基地局
１３：管理サーバ
２０：センサ
２１：無線送受信処理部
２２：通信プロトコル動作処理部
２３：端末識別情報格納処理部
２４：各種メタデータ格納処置部
２５：センサデータ格納処理部
２６：位置情報検出部
２７：設置者検出部
２８：環境情報検出部

【図面】

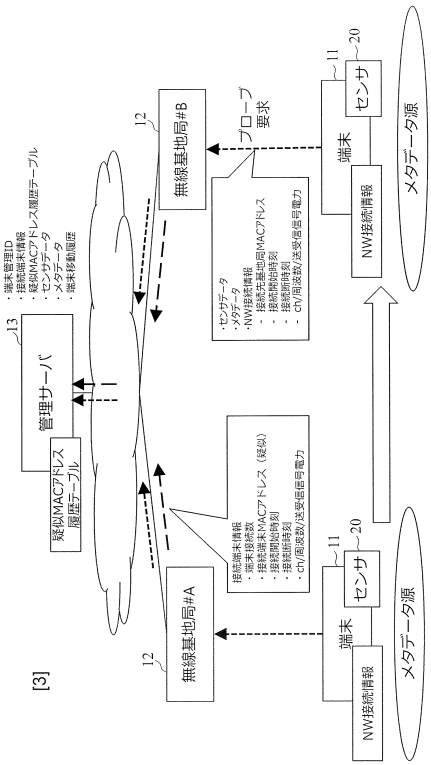
【図１】


[1]
管理サーバ
13
無線基地局#A
無線基地局#B
12
無線LAN
・センサデータ
・メタデータ
・端末識別情報(Macアドレス)
A0:B2:D5:7F:81:B3
D0:C2:1D5:9F:10:C5
MACアドレスの変更
端末
センサ
11
20
メタデータ源

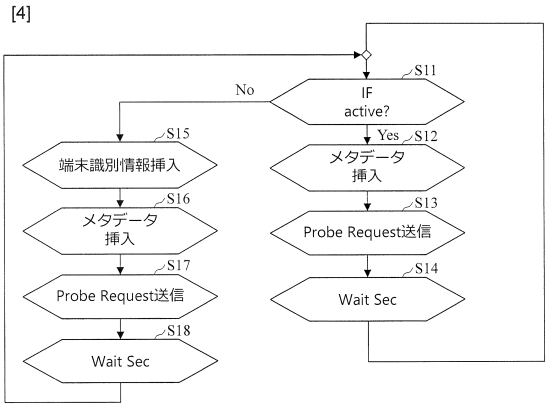
【図２】


[2]
・端末管理ID
・疑似MACアドレス履歴テーブル
・センサデータ
・メタデータ
・端末移動履歴
管理サーバ
疑似MACアドレス履歴テーブル
13
無線基地局#A
無線基地局#B
12
14
プローブ要求
・センサデータ
・メタデータ
・過去の疑似MACアドレス
端末
センサ
11
20
疑似MACアドレス履歴テーブル
メタデータ源

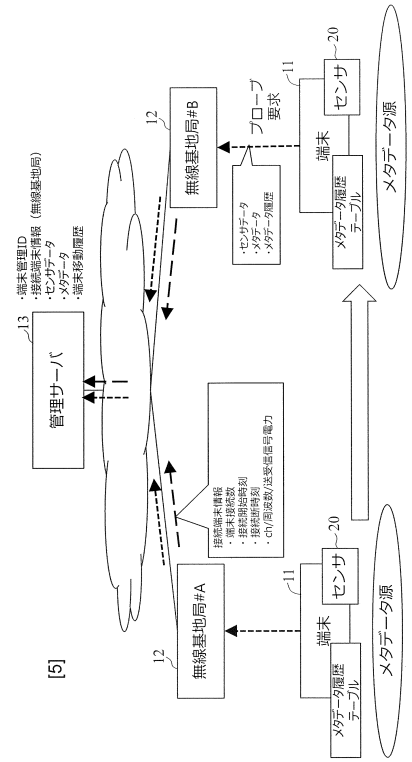
【図３】


[3]
・端末管理ID
・接続端末情報
・疑似MACアドレス履歴テーブル
・センサデータ
・メタデータ
・端末移動履歴
管理サーバ
疑似MACアドレス履歴テーブル
13
無線基地局#A
無線基地局#B
12
プローブ要求
・センサデータ
・メタデータ
・NW接続情報
・接続先基地局MACアドレス
・接続開始時刻
・接続終了時刻
・ch/周波数/送受信信号電力
・接続端末情報
・端末移動履歴
・接続先基地局MACアドレス（疑似）
・接続開始時刻
・接続終了時刻
・ch/周波数/送受信信号電力
端末
センサ
11
20
NW接続情報
メタデータ源

【図４】

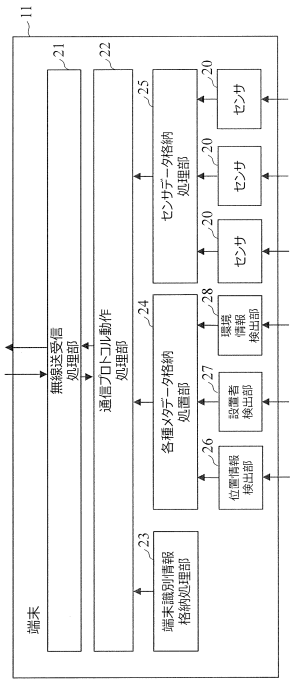

[4]
IF active?
No
Yes
S11
S12
S13
S14
S15
S16
S17
S18
メタデータ挿入
Probe Request送信
Wait Sec
端末識別情報挿入
メタデータ挿入
Probe Request送信
Wait Sec

【図５】



[5]

【図６】



[6]

【図７】

[7]

(A)

Table 9-33—Probe Request frame body *(continued)*

Order	Information	Notes
19	Extended Request	The Extended Request element is optionally present if dot11RadioMeasurementActivated is true.
Last	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements.

EXP

(B)

Table 9-34—Probe Response frame body *(continued)*

Order	Information	Notes
64	Quiet Channel	Either one Quiet Channel element containing an AP Quiet Mode field equal to 0 or, in an infrastructure BSS, one or more Quiet Channel elements each containing an AP Quiet Mode field equal to 1 are optionally present if dot11VHTOptionImplemented is true, and either dot11SpectrumManagementRequired or dot11RadioMeasurementActivated is true.
65	Operating Mode Notification	The Operating Mode Notification element is optionally present if dot11OperatingModeNotificationImplemented is true.
66	Reduced Neighbor Report	The Reduced Neighbor Report element is optionally present if dot11TVHTOptionImplemented is true.
67	TVHT Operation	The TVHT Operation element is present for a TVHT STA when the dot11TVHTOptionImplemented is true; otherwise it is not present.
68	Estimated Service Parameters	The Estimated Service Parameters element is optionally present if dot11EstimatedServiceParametersOptionImplemented is true.
69	Relay Capabilities	The Relay Capabilities element is present if dot11RelayActivated is true; otherwise not present.
Last–1	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements, except the Requested elements.
Last	Requested elements	Elements requested by the Request element or Extended Request element(s) of the Probe Request frame are present if dot11MultiDomainCapabilityActivated or dot11EstimatedServiceParametersOptionImplemented is true. See 11.1.4.3.2 and 11.46.

EXP

フロントページの続き

(51)国際特許分類　　ＦＩ
Ｈ０４Ｗ　84/12　(2009.01)　　Ｈ０４Ｗ　84/12

(72)発明者　谷口 友宏
東京都千代田区大手町一丁目５番１号 日本電信電話株式会社内
(72)発明者　鈴木 徹也
東京都千代田区大手町一丁目５番１号 日本電信電話株式会社内
(72)発明者　木村 康隆
東京都千代田区大手町一丁目５番１号 日本電信電話株式会社内
審査官　松野 吉宏

(56)参考文献
国際公開第２０２０／２３５６４１（WO，Ａ１）
米国特許出願公開第２０２０／０４０３９６７（ＵＳ，Ａ１）
玉置真也、椎名亮太、鈴木徹也、木村康隆、谷口友宏、黄撃 、秦野智也、辻幸嗣，ＩｏＴデータ信頼性向上に向けた無線ＬＡＮメタデータ収集方式の実装，電子情報通信学会２０２０年通信ソサイエティ大会講演論文集２，日本，一般社団法人電子情報通信学会，2020年09月01日，第59頁
伊藤智稀、野口博史、山登庸次、村瀬勉，ＩｏＴデータの短寿命・ローカリティを考慮したメタデータ管理のための負荷分散制御，電子情報通信学会技術研究報告 Ｖｏｌ．１１７ Ｎｏ．４６０，日本，一般社団法人電子情報通信学会 ，2018年02月22日，第117巻，第315-320頁

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４ － ７／２６
Ｈ０４Ｗ　４／００ － ９９／００
３ＧＰＰ　ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４