

明 細 書

発明の名称：遠隔制御システム

技術分野

[0001] 本開示はデータ処理技術に関し、特に、対象となる装置を遠隔から制御する技術に関する。

背景技術

[0002] 集合住宅等には、住人に配達された荷物を一時的に預かる宅配ボックスが設置されることがある。以下の特許文献1では、宅配ボックスの利用者の携帯電話を利用して認証を行い、宅配ボックスを解錠するシステムが提案されている。

先行技術文献

特許文献

[0003] 特許文献1：特開2013-142916号公報

発明の概要

発明が解決しようとする課題

[0004] 近年、スマートフォン等の情報端末に不正な動作を行わせるマルウェアが出回っており、ユーザが気付かないうちに自身の情報端末がマルウェアに感染することもある。このような状況下、ユーザの情報端末を利用して外部の装置を遠隔制御する場合のセキュリティの確保が求められている。

[0005] 本開示はこうした状況に鑑みてなされたものであり、1つの目的は、ユーザの情報端末を利用して外部の装置を遠隔制御する場合のセキュリティを向上させる技術を提供することにある。

課題を解決するための手段

[0006] 上記課題を解決するために、本発明のある態様の遠隔制御システムは、遠隔制御の対象となる被制御装置と、被制御装置と無線通信を行う移動可能な通信端末と、を備える。被制御装置は、遠隔制御を受け付ける際に、第1データを通信端末へ送信し、通信端末は、第1データへの応答として、遠隔制

御の内容を含む第2データを被制御装置へ送信し、被制御装置は、第1データを送信してから第2データを受信するまでの時間が予め定められた閾値未満である場合、第2データに含まれる遠隔制御の内容に応じた処理を実行する。

[0007] なお、以上の構成要素の任意の組合せ、本開示の表現を、装置、方法、コンピュータプログラム、コンピュータプログラムを記録した記録媒体などの間で変換したものもまた、本開示の態様として有効である。

発明の効果

[0008] 本開示によれば、ユーザの情報端末を利用して外部の装置を遠隔制御する場合のセキュリティを向上させることができる。

図面の簡単な説明

[0009] [図1]宅配ボックス解錠の動作例（正常時）を示す図である。
[図2]宅配ボックス解錠の動作例（攻撃時）を示す図である。
[図3]第1実施例の遠隔制御システムの構成を示す図である。
[図4]第1実施例の宅配ボックスの機能ブロックを示すブロック図である。
[図5]第1実施例のユーザ端末の機能ブロックを示すブロック図である。
[図6]第1実施例のサーバの機能ブロックを示すブロック図である。
[図7]第1実施例の遠隔制御システムにおける各機器の動作を示す図である。
[図8]第2実施例の宅配ボックスの機能ブロックを示すブロック図である。
[図9]第2実施例のユーザ端末の機能ブロックを示すブロック図である。
[図10]第2実施例のサーバの機能ブロックを示すブロック図である。
[図11]第2実施例の遠隔制御システムにおける各機器の動作を示す図である。

発明を実施するための形態

[0010] 本開示における装置または方法の主体は、コンピュータを備えている。このコンピュータがプログラムを実行することによって、本開示における装置または方法の主体の機能が実現される。コンピュータは、プログラムにしたがって動作するプロセッサを主なハードウェア構成として備える。プロセッ

サは、プログラムを実行することによって機能を実現することができれば、その種類は問わない。プロセッサは、半導体集積回路（IC）、またはLSI（large scale integration）を含む1つまたは複数の電子回路で構成される。ここではICやLSIと呼んでいるが、集積の度合いによって呼び方が変わり、システムLSI、VLSI（very large scale integration）もしくはULSI（ultra large scale integration）と呼ばれるものであってもよい。LSIの製造後にプログラムされる、フィールド・プログラマブル・ゲート・アレイ（FPGA）、又はLSI内部の接合関係の再構成又はLSI内部の回路区画のセットアップができる再構成可能な論理デバイスも同じ目的で使うことができる。複数の電子回路は、1つのチップに集積されてもよいし、複数のチップに設けられてもよい。複数のチップは1つの装置に集約されていてもよいし、複数の装置に備えられていてもよい。プログラムは、コンピュータが読み取り可能なROM、光ディスク、ハードディスクドライブなどの非一時的記録媒体に記録される。プログラムは、記録媒体に予め格納されていてもよいし、インターネット等を含む広域通信網を介して記録媒体に供給されてもよい。

[0011] まず実施例の概要を説明する。図1は、宅配ボックス解錠の動作例（正常時）を示す。宅配ボックスの解錠時、サーバは、ノンスおよび解錠用の制御データ（コマンド等）をユーザ端末（スマートフォン等）へ送信する。ノンスは、1回限りのランダム値であり、リプレイ攻撃への対策である。ユーザ端末は、ノンスおよび解錠用の制御データを宅配ボックスへ転送する。宅配ボックスは、制御データに応じて、扉の電気錠を解錠する。

[0012] 図2は、宅配ボックス解錠の動作例（攻撃時）を示す。図2は、中間者攻撃の例を示している。ここでのユーザ端末は、マルウェアに感染しており、マルウェアにより制御データが攻撃者端末へ転送されてしまう。攻撃者は、宅配ボックスが解錠されないためユーザが宅配ボックスから離れたことを確認すると、攻撃者端末からノンスおよび制御データを宅配ボックスに送信させ、宅配ボックスを解錠させる。この結果、宅配ボックス内の物品が攻撃者

により不正に取得されてしまう。

[0013] このように、スマートフォン等のユーザ端末には、OSや無線通信における脆弱性が存在する。そのため、攻撃者は、ユーザ端末の脆弱性を利用してマルウェアを感染させることによりユーザ端末の制御を乗っ取り、遠隔制御の対象装置に対する制御データを遅延再送し、不正に対象装置を動作させてしまうことが懸念される。そこで実施例では、ユーザ端末を経由した対象装置（実施例では宅配ボックス）の遠隔制御に対して、遅延再送による攻撃を防御する仕組みを導入した遠隔制御システムを提案する。

[0014] （第1実施例）

図3は、第1実施例の遠隔制御システム10の構成を示す。遠隔制御システム10は、宅配ボックス12a、宅配ボックス12b、宅配ボックス12c（総称する場合「宅配ボックス12」と呼ぶ。）と、ユーザ端末14と、サーバ16を備える。遠隔制御システム10は、通信システムまたは情報処理システムとも言え、ユーザ端末14を利用して宅配ボックス12に対する安全な遠隔制御を実現する。

[0015] 宅配ボックス12は、遠隔制御の対象となる被制御装置とも言える。ユーザ端末14は、宅配ボックスのユーザ、実施例では宅配ボックスから荷物を取り出すユーザにより操作される移動可能な通信端末である。ユーザ端末14は、スマートフォンまたはタブレット端末であってもよく、宅配ボックス12と無線通信を行う。サーバ16は、クラウド上に設けられた情報処理装置である。サーバ16は、複数の宅配ボックス12に対する制御を集約して実行する情報集約装置とも言える。

[0016] ユーザ端末14と宅配ボックス12は、近距離通信網18を介して接続される。一方、ユーザ端末14とサーバ16は、広域通信網20を介して接続される。近距離通信網18は、近距離無線通信を含み、実施例では、Bluetooth Low Energy（「Bluetooth」は登録商標）（以下「BLE」とも呼ぶ。）とする。広域通信網20は、広域無線通信を含み、例えば、第4世代移动通信システムやインターネットを含んでもよい。

- [0017] 図4は、第1実施例の宅配ボックス12の機能ブロックを示すブロック図である。本開示のブロック図において示される各ブロックは、ハードウェア的には、コンピュータのCPU・メモリをはじめとする素子や機械装置で実現でき、ソフトウェア的にはコンピュータプログラム等によって実現されるが、ここでは、それらの連携によって実現される機能ブロックを描いている。これらの機能ブロックはハードウェア、ソフトウェアの組合せによっていろいろなかたちで実現できることは、当業者には理解されることである。
- [0018] 宅配ボックス12は、操作部30、通信部32、電源部34、扉部36、電気錠38、MAC鍵記憶部40、制御部42を備える。実施例では、複数の宅配ボックス12のそれぞれが、図4に示す複数の機能ブロックを備えることとする。変形例として、複数の機能ブロックのうち少なくとも一部の機能ブロック（例えば操作部30、電源部34等）は、複数の宅配ボックス12により共用されてもよい。
- [0019] 扉部36は、宅配ボックスの荷物取り出し口に設けられた開放可能な扉である。電気錠38は、施錠状態と解錠状態を電氣的に切替可能な扉部36の鍵である。電源部34は、宅配ボックス12の各部に電力を供給する。実施例の電源部34は、電池式の電源である。後述するスリープ制御部46によりサスペンド状態（言い換えればスリープ状態）に移行された場合、電源部34は、電力の供給を通常時よりも抑制する。例えば、電源部34は、サスペンド状態では、通信部32に対する電力の供給を抑制する。
- [0020] 操作部30は、ユーザによる操作が入力される部品であり、例えば、宅配ボックス12の筐体上に設けられたボタンである。実施例では、電気錠38を解錠するための所定操作（遠隔制御を受け付けるよう指示する所定操作とも言え、以下「解錠処理開始操作」とも呼ぶ。）が操作部30に入力される。例えば、解錠処理開始操作は、操作部30としての所定のボタンに対する押下操作であってもよい。後述の制御部42は、解錠処理開始操作が入力されると、電気錠38の解錠を指示する遠隔制御を受け付けるためのデータ処理および通信処理を実行する。

- [0021] 通信部 32 は、所定の通信プロトコル（実施例では B L E）を用いて外部装置と通信する。後述の制御部 42 は、通信部 32 を介して、ユーザ端末 14 とデータを送受信する。通信部 32 は、電源部 34（実施例では電池）から供給された電力により駆動する。通信部 32 は、通常状態とサスペンド状態を備え、サスペンド状態では通信機能を制限（例えば停止）することにより電力の使用量を抑制する。
- [0022] M A C 鍵記憶部 40 は、メッセージ認証用のコード（以下「M A C」とも呼ぶ。）を生成するための鍵（以下「M A C 鍵」とも呼ぶ。）を記憶する。なお、M A C 鍵記憶部 40 に記憶される M A C 鍵と同じ M A C 鍵がサーバ 16 にも記憶される。
- [0023] 制御部 42 は、安全な遠隔制御を受け付けるための各種データ処理を実行する。制御部 42 は、操作検出部 44、スリープ制御部 46、チャレンジ設定部 48、チャレンジ送信部 50、レスポンス受付部 52、認証部 54、解錠部 56 を含む。これら複数の機能ブロックの機能が実装されたコンピュータプログラムが、宅配ボックス 12 の記憶領域（記録媒体）にインストールされてもよい。宅配ボックス 12 の C P U は、上記のコンピュータプログラムをメインメモリに読み出して実行することにより、各機能ブロックの機能を発揮してもよい。
- [0024] 操作検出部 44 は、解錠処理開始操作が操作部 30 に入力された場合、そのことを検出する。スリープ制御部 46 は、遠隔操作を受け付ける一連の処理、実施例では、電気錠 38 の解錠に係る一連の処理が終了すると、通信部 32 をサスペンド状態に移行させることにより、電力の消費量を低減させる。また、スリープ制御部 46 は、解錠処理開始操作の入力が検出された場合、通信部 32 をサスペンド状態から通常状態へ復帰させ、無線通信を開始させる。
- [0025] チャレンジ設定部 48 は、解錠処理開始操作の入力が検出された場合、所定の乱数発生器により生成された乱数値（チャレンジとも呼ばれる）を含む第 1 データ（以下「チャレンジデータ」とも呼ぶ。）を設定する。チャレン

ジデータは、(1) ノンス、(2) 乱数値、(3) MACを含む。チャレンジ設定部48は、MAC鍵記憶部40に記憶されたMAC鍵（すなわちサーバ16と共有されたMAC鍵）と上記乱数値とをもとにMACを生成する。チャレンジ送信部50は、チャレンジ設定部48が設定したチャレンジデータをユーザ端末14へ送信する。実施例では、チャレンジデータに乱数値を設定するが、変形例として、チャレンジ設定部48は、乱数値とは異なるデータであって、生成毎に異なるカウンタ値など、一意性を持つ値のデータをチャレンジデータに設定してもよい。

[0026] レスponse受付部52は、チャレンジデータへの応答としての第2データであって、ユーザ端末14から送信されたレスponseデータを受け付ける。レスponseデータは、(1) ノンス、(2) 乱数値、(3) 制御データ、(4) MACを含む。レスponseデータの乱数値は、宅配ボックス12とサーバ16の間で予め定められた規則にしたがってチャレンジデータの乱数値を変換したものであり、宅配ボックス12により検証される検証値とも言える。実施例では、チャレンジデータの乱数値に「1」を足したものとする。変形例として、宅配ボックス12とサーバ16の間で予め定められた規則は、特定の値に対して特定の四則演算を行うことでもよい。

[0027] レスponseデータの制御データは、宅配ボックス12に対する遠隔制御（言い換えれば遠隔操作）の内容を含む。実施例での制御データは、電気錠38の解錠を指示するデータを含む。レスponseデータのMACは、サーバ16に記憶されたMAC鍵（すなわち宅配ボックス12と共有されたMAC鍵）、乱数値および制御データをもとにサーバ16により生成されたものである。

[0028] 認証部54は、レスponse受付部52により受け付けられたレスponseデータをもとに認証処理を実行し、レスponseデータが正当なものか否かを判定する。宅配ボックス12は、認証部54によりレスponseデータが正当なものと判定された場合、レスponseデータに含まれる遠隔制御の内容に応じた処理を実行する。実施例では、遠隔制御の内容に応じた処理として、解錠

部56が、レスポンスデータに含まれる制御データにしたがって電気錠38を解錠する。

[0029] 認証部54の処理を詳細に説明する。認証部54は、チャレンジデータが送信されてからレスポンスデータが受信されるまでの経過時間（以下「応答時間」とも呼ぶ。）を計測する。認証部54は、応答時間が予め定められた閾値（上限応答時間とも言え、例えば20秒）未満である場合、第1条件が満たされたと判定する。上記閾値は、遠隔制御システム10の開発者の知見や、遠隔制御システム10を用いた実験（実際の通信を含む）により適切な値が決定されればよい。

[0030] また、認証部54は、レスポンスデータに含まれる乱数値が、チャレンジデータに含まれる乱数値に対応するか否かを確認する。言い換えれば、認証部54は、レスポンスデータに含まれる乱数値が、予め定められた規則にしたがってチャレンジデータに含まれる乱数値を変換したものに一致するか否かを確認する。実施例では、認証部54は、チャレンジ送信部50により送信されたチャレンジデータに含まれる乱数値を記憶し、レスポンスデータに含まれる乱数値が、チャレンジデータに含まれる乱数値+1であるか否かを確認する。認証部54は、レスポンスデータに含まれる乱数値が、チャレンジデータに含まれる乱数値に対応する場合、第2条件が満たされたと判定する。

[0031] また、認証部54は、レスポンスデータに含まれるMACを用いたメッセージ認証の成否を確認する。具体的には、MAC鍵記憶部40に記憶されたMAC鍵、レスポンスデータに含まれる乱数値および制御データをもとにMACを生成し、生成したMACがレスポンスデータに含まれるMACと一致する場合、メッセージ認証に成功したと判定する。認証部54は、メッセージ認証に成功した場合、第3条件が満たされたと判定する。認証部54は、第1条件、第2条件、第3条件のいずれもが満たされた場合、レスポンスデータが正当なものであると判定する。一方、第1条件、第2条件、第3条件の少なくとも1つが満たされない場合、認証部54は、レスポンスデータが

正当でないと判定する。

- [0032] すなわち、認証部54は、チャレンジデータが送信されてからレスポンスデータが受信されるまでの応答時間に応じて、レスポンスデータに含まれる遠隔制御の内容に応じた処理の実行を制限（実施例では禁止）する。また、認証部54は、レスポンスデータに含まれる乱数値に応じて、レスポンスデータに含まれる遠隔制御の内容に応じた処理の実行を制限する。また、認証部54は、レスポンスデータに含まれるMACを用いたメッセージ認証の結果に応じて、レスポンスデータに含まれる遠隔制御の内容に応じた処理の実行を制限する。
- [0033] 図5は、第1実施例のユーザ端末14の機能ブロックを示すブロック図である。ユーザ端末14は、操作部60、表示部62、通信部64、制御部66を備える。操作部60は、ユーザによる操作が入力される部品である。表示部62は、画面を含み、ユーザに対して種々の情報を提示する。操作部60と表示部62は、例えばタッチパネル機能を備える液晶ディスプレイとして一体化されてもよい。
- [0034] 通信部64は、所定の通信プロトコルを用いて外部装置と通信する。実施例では、通信部64は、BLEにより宅配ボックス12と通信し、また、広域無線通信（例えば第4世代移動通信システム）によりサーバ16と通信する。制御部66は、各種データ処理を実行する。制御部66は、通信部64を介して宅配ボックス12およびサーバ16とデータを送受信する。
- [0035] 制御部66は、チャレンジ転送部68、レスポンス転送部70、表示制御部72を備える。これら複数の機能ブロックの機能が実装されたコンピュータプログラム（例えば遠隔制御用のクライアントアプリケーション）が記録媒体に格納され、その記録媒体を介してユーザ端末14の記憶領域にインストールされてもよい。または、上記コンピュータプログラムがネットワークを介してダウンロードされ、ユーザ端末14の記憶領域にインストールされてもよい。ユーザ端末14のCPUは、上記のコンピュータプログラムをメインメモリに読み出して実行することにより、各機能ブロックの機能を発揮

してもよい。

[0036] チャレンジ転送部 68 は、宅配ボックス 12 から送信されたチャレンジデータを受信し、受信したチャレンジデータをサーバ 16 へ転送する。レスポンス転送部 70 は、サーバ 16 から送信されたレスポンスデータを受信し、受信したレスポンスデータを、チャレンジデータへの応答として、宅配ボックス 12 へ転送する。

[0037] 表示制御部 72 は、サーバ 16 および宅配ボックス 12 との通信時に、通信中であることを表示部 62 に表示させる。また、表示制御部 72 は、宅配ボックス 12 の解錠までしばらく待つことを促す内容を表示部 62 にさらに表示させてもよい。変形例として、表示制御部 72 は、少なくともサーバ 16 との通信時に、通信中であることを表示部 62 に表示させてもよい。

[0038] 図 6 は、第 1 実施例のサーバ 16 の機能ブロックを示すブロック図である。サーバ 16 は、制御部 80、記憶部 82、通信部 84 を備える。制御部 80 は、複数の宅配ボックス 12 と連携するとともに、複数の宅配ボックス 12 の遠隔制御（実施例では解錠）を集約して実施するためのデータ処理を実行する。記憶部 82 は、制御部 80 により参照または更新されるデータを記憶する。

[0039] 通信部 84 は、所定の通信プロトコルを用いて外部装置と通信する。実施例では、広域通信（例えばインターネットや第 4 世代移動通信システム）によりユーザ端末 14 と通信する。制御部 80 は、通信部 84 を介してユーザ端末 14 とデータを送受信する。

[0040] 記憶部 82 は、制御データ記憶部 86 と MAC 鍵記憶部 88 を備える。制御データ記憶部 86 は、宅配ボックス 12 を遠隔操作するためのデータを記憶し、実施例では電気錠 38 の解錠を指示する制御データ（コマンド等）を記憶する。MAC 鍵記憶部 88 は、宅配ボックス 12 と共有する MAC 鍵を記憶する。なお、MAC 鍵記憶部 88 は、複数の宅配ボックス 12 のそれぞれと共有する MAC 鍵であって、宅配ボックス 12 毎に異なる MAC 鍵を記憶してもよい。

- [0041] 制御部80は、認証部90、レスポンス設定部92、レスポンス送信部94を備える。これら複数の機能ブロックの機能が実装されたコンピュータプログラムが、サーバ16の記憶領域（記録媒体）にインストールされてもよい。宅配ボックス12のCPUは、上記のコンピュータプログラムをメインメモリに読み出して実行することにより、各機能ブロックの機能を発揮してもよい。
- [0042] レスポンス設定部92は、ユーザ端末14から送信（転送）されたチャレンジデータを受け付け、そのチャレンジデータもとにレスポンスデータを設定する。既述だが、レスポンスデータは、（1）ノンス、（2）乱数値、（3）制御データ、（4）MACを含む。レスポンス設定部92は、宅配ボックス12とサーバ16の間で予め定められた規則にしたがってチャレンジデータの乱数値を変換した値であり、実施例では、チャレンジデータの乱数値に「1」を足した値をレスポンスデータの乱数値として設定する。
- [0043] また、レスポンス設定部92は、制御データ記憶部86に記憶された制御データ（実施例では解錠指示）をレスポンスデータの制御データとして設定する。また、レスポンス設定部92は、MAC鍵記憶部88に記憶されたMAC鍵と、乱数値および制御データをもとにMACを生成して、制御データに設定する。レスポンス送信部94は、レスポンス設定部92により設定されたレスポンスデータを、チャレンジデータへの応答としてユーザ端末14へ送信する。
- [0044] 認証部90は、チャレンジデータに含まれるMACを用いたメッセージ認証の成否を確認する。具体的には、MAC鍵記憶部88に記憶されたMAC鍵と、チャレンジデータに含まれる乱数値とをもとにMACを生成し、生成したMACがチャレンジデータに含まれるMACと一致する場合、メッセージ認証に成功したと判定する。認証部90は、メッセージ認証に成功した場合、レスポンスデータの送信を許可する。一方、メッセージ認証に失敗した場合、レスポンスデータの送信または送信を抑制させる（言い換えれば禁止する）。

[0045] 以上の構成による第1実施例の遠隔制御システム10の動作を説明する。

図7は、第1実施例の遠隔制御システム10における各機器の動作を示す図である。同図の12は、図1に示す宅配ボックス12a、宅配ボックス12b、宅配ボックス12cのうちユーザが解錠しようとする（すなわち遠隔制御の対象となる）特定の宅配ボックスを意味する。宅配ボックス12a、宅配ボックス12b、宅配ボックス12cのいずれが解錠される場合も同様の動作となる。

[0046] サーバ16と宅配ボックス12には、共通のMAC鍵が予め記憶されている。ユーザは、宅配ボックス12に対して所定の解錠処理開始操作を入力する。宅配ボックス12の操作検出部44は、解錠処理開始操作の入力を検出し、宅配ボックス12のスリープ制御部46は、通信部32をサスペンド状態から通常状態へ復帰させる（S10）。宅配ボックス12のチャレンジ設定部48は、チャレンジデータを設定し、宅配ボックス12のチャレンジ送信部50は、チャレンジデータをユーザ端末14へ送信する（S12）。

[0047] 宅配ボックス12との通信が開始されると、ユーザ端末14の表示制御部72は、表示部62における「通信中」の表示を開始する。ユーザ端末14のチャレンジ転送部68は、チャレンジデータをサーバ16へ転送する（S14）。サーバ16の認証部90は、チャレンジデータに含まれるMACをもとにメッセージ認証を実行する（S16）。メッセージ認証によりチャレンジデータの正当性（言い換えれば非改竄性）が確認されると、サーバ16のレスポンス設定部92は、チャレンジデータをもとにレスポンスデータを生成する。サーバ16のレスポンス送信部94は、レスポンスデータをユーザ端末14へ送信する（S18）。

[0048] ユーザ端末14のレスポンス転送部70は、レスポンスデータを宅配ボックス12へ転送する（S20）。宅配ボックス12との通信が終了すると、ユーザ端末14の表示制御部72は、表示部62における「通信中」の表示を終了させる。

[0049] 宅配ボックス12のレスポンス受付部52は、レスポンスデータを受け付

ける。宅配ボックス12の認証部54は、(1)チャレンジデータ送信からレスポンスデータ受信までの応答時間 t 、(2)レスポンスデータの乱数値、(3)レスポンスデータのMACをもとに、レスポンスデータが正当なものか否かを認証する(S22)。レスポンスデータが正当と判定された場合、宅配ボックス12の解錠部56は、電気錠38を解錠する(S24)。ユーザは、宅配ボックス12の扉部36を開けて、宅配ボックス12に格納された物品を取り出すことができる。レスポンスデータが正当と判定された場合、S24をスキップする。

[0050] 第1実施例の遠隔制御システム10では、サーバ16からの制御データをユーザ端末14が中継して宅配ボックス12に渡す。そのため、宅配ボックス12は、広域通信網20と接続する必要がなく、ユーザ端末14と近距離通信を行えばよい。そのため、宅配ボックス12のコストの増加を抑制できる。

[0051] また、第1実施例の遠隔制御システム10では、チャレンジデータ送信からレスポンスデータ受信までの応答時間に制限を設けた。これにより、攻撃者(言い換えれば中間者攻撃)によるレスポンスデータの窃取と遅延再送による不正な遠隔制御(例えば不正な解錠)を防止することができる。

[0052] また、遠隔制御システム10では、チャレンジデータに乱数値を設定し、レスポンスデータにチャレンジデータの乱数値に対応する検証値を設定させる。これにより、宅配ボックス12は、自機が送信したチャレンジデータに対応するレスポンスデータであるか否かを確認でき、宅配ボックス12のセキュリティを一層高めることができる。

[0053] また、遠隔制御システム10では、複数の宅配ボックス12の遠隔制御(解錠)の指示をサーバ16が一括して実行する。これにより、遠隔制御システム10における認証等の管理を簡素化でき、例えば、ユーザ端末14における処理を簡素化できる。

[0054] また、遠隔制御システム10では、チャレンジデータおよびレスポンスデータにMACを設定することで、宅配ボックス12とサーバ16間でのメッセージ認証(例えば非改竄性の確認)を実現でき、宅配ボックス12のセキュリティを高めることができる。

セキュリティを一層高めることができる。

[0055] また、宅配ボックス１２の通信部３２や制御部４２等は、宅配ボックス１２の設置後、後付で設けられることが多いと考えられる。そこで、宅配ボックス１２の通信部３２や制御部４２等は、電池駆動とすることが望ましい。一方、電池駆動の場合、電池の消耗を極力低減することが望まれる。そこで、遠隔制御システム１０では、宅配ボックス１２の通信部３２は、解錠処理開始操作が入力されたことを契機に、サスペンド状態から復帰して無線通信を行う。これにより、宅配ボックス１２における電池の消耗を抑制できる。

[0056] また、遠隔制御システム１０では、ユーザ端末１４は、宅配ボックス１２およびサーバ１６との通信時に通信中の旨を表示する。これにより、ユーザが通信圏外へ移動してしまうこと、言い換えれば、ユーザが宅配ボックス１２から離れてしまうことを防止し、攻撃者による物品の不正な取得を一層確実に防止できる。

[0057] （第２実施例）

第２実施例の遠隔制御システム１０の構成は、図１に示す第１実施例の遠隔制御システム１０の構成と同様である。ただし、第２実施例の遠隔制御システム１０は、宅配ボックス１２がユーザ端末１４をピンニングする機能、および、サーバ１６がユーザ端末１４をピンニングする機能をさらに備える。以下、第１実施例とは異なる構成を主に説明し、第１実施例と重複する内容は説明を適宜省略する。

[0058] 図８は、第２実施例の宅配ボックス１２の機能ブロックを示すブロック図である。第２実施例の宅配ボックス１２は、第１実施例の機能ブロックに加えて、アドレス取得部１００を備える。

[0059] 操作検出部４４により解錠処理開始操作の入力が検出された場合、通信部３２は、所定のアドバタイズメントパケットを周囲にブロードキャストする。アドレス取得部１００は、アドバタイズメントパケットに対する応答としてユーザ端末１４から通知されたユーザ端末１４のアドレス（以下「ユーザ端末アドレス」と呼ぶ。）を取得する。実施例のユーザ端末アドレスは、Ｂ

LE通信でのアドレス（アクセスアドレス）である。

[0060] 第2実施例のチャレンジデータは、ユーザ端末14から通知されたユーザ端末アドレスに対応するデータを含む。具体的には、チャレンジ設定部48は、チャレンジデータの乱数値の項目に、乱数値とユーザ端末アドレスとを合成した（例えば連結した）データを設定する。なお、チャレンジ設定部48は、ユーザ端末アドレスそのものをチャレンジデータに設定するのではなく、予め定められた規則にしたがってユーザ端末アドレスを変換した値をチャレンジデータに設定してもよい。

[0061] 後述するように、第2実施例のレスポンスデータには、チャレンジデータに含まれるユーザ端末アドレスに対応するデータが含まれる。認証部54は、レスポンスデータに含まれるユーザ端末アドレスに対応するデータが、宅配ボックス12のチャレンジ送信部50に記憶されたチャレンジデータの送信先アドレスに不整合の場合、レスポンスデータに含まれる遠隔制御の内容に応じた処理の実行を制限する。

[0062] 具体的には、認証部54は、レスポンスデータの乱数値の項目に含まれるユーザ端末アドレスと、宅配ボックス12のチャレンジ送信部50に記憶されたチャレンジデータの送信先アドレス（具体的にはBLE通信のパケットに含まれるアクセスアドレス）とが一致するか否かを確認する。両者が一致する場合、認証部54は、第4条件が満たされたと判定する。認証部54は、第1実施例に記載の第1条件、第2条件、第3条件と、上記の第4条件のいずれもが満たされた場合、レスポンスデータが正当なものと判定する。

[0063] また、少なくとも第4条件が満たされない場合、認証部54は、レスポンスデータが正当なものでないと判定する。この結果、レスポンスデータに含まれる遠隔制御の内容に応じた処理（実施例では解錠）の実行が抑制される。

[0064] 図9は、第2実施例のユーザ端末14の機能ブロックを示すブロック図である。第2実施例のユーザ端末14は、第1実施例の機能ブロックに加えて、記憶部102、認証部106、アドレス通知部108を備える。

- [0065] 記憶部102は、制御部66により更新または参照されるデータを記憶する。記憶部102は、証明書記憶部104を含む。証明書記憶部104は、認証局により発行されたユーザ端末14の証明書であるクライアント証明書を記憶する。
- [0066] 認証部106は、サーバ16との相互認証を実行する。認証部106は、サーバ16との相互認証時、証明書記憶部104に記憶されたクライアント証明書をサーバ16へ送信する。それとともに、認証部106は、サーバ16から提供されたサーバ16の電子証明書、実施例ではSSL (Secure Sockets Layer) サーバ証明書をもとにサーバ16を認証する。
- [0067] アドレス通知部108は、宅配ボックス12から送信されたアドバタイズメントパケットが通信部32により受信された場合、BLE通信におけるユーザ端末14のアドレス（アクセスアドレス）を宅配ボックス12へ送信する。
- [0068] 図10は、第2実施例のサーバ16の機能ブロックを示すブロック図である。第2実施例のサーバ16は、第1実施例の機能ブロックに加えて、証明書記憶部110を備える。証明書記憶部110は、認証局により発行されたサーバ16の電子証明書であるSSLサーバ証明書を記憶する。SSLサーバ証明書は、SSL/TLS (Transport Layer Security) サーバ証明書とも言える。
- [0069] 認証部90は、ユーザ端末14との相互認証を実行する。認証部90は、ユーザ端末14との相互認証時、証明書記憶部110に記憶されたSSLサーバ証明書をユーザ端末14へ送信する。それとともに、認証部90は、ユーザ端末14から提供されたクライアント証明書をもとにユーザ端末14を認証する。すなわち、認証部90は、ユーザ端末14に対するクライアント認証を実行する。
- [0070] 認証部90は、クライアント認証の結果に応じて、ユーザ端末14との通信を制限し、例えば、ユーザ端末14との通信を禁止する。通信部84は、クライアント認証が失敗した場合、ユーザ端末14とのSSLセッションを

確立せず、また、ユーザ端末14との通信を切断してもよい。また、認証部90は、レスポンス設定部92によるチャレンジデータの受信を禁止してもよく、または、レスポンス送信部94によるレスポンスデータの送信を禁止してもよい。

[0071] レスポンス設定部92は、レスポンスデータの乱数値の項目に、チャレンジデータに含まれる乱数値を変換した値（実施例ではチャレンジデータの乱数値+1）と、チャレンジデータに含まれるユーザ端末アドレスとを合成した（例えば連結した）データを設定する。

[0072] 以上の構成による第2実施例の遠隔制御システム10の動作を説明する。

図11は、第2実施例の遠隔制御システム10における各機器の動作を示す図である。第1実施例と同様に、サーバ16と宅配ボックス12には、共通のMAC鍵が予め記憶されている。サーバ16の認証部90と、ユーザ端末14の認証部106は、クライアント認証を含む相互認証を実行する（S30）。ここでは、相互認証に成功し、サーバ16とユーザ端末14は、暗号トンネル（「SSLトンネル」とも言える）内での通信、言い換えれば、暗号化およびトンネリングによる通信が可能になったこととする。

[0073] ユーザは、宅配ボックス12に対して所定の解錠処理開始操作を入力する。宅配ボックス12の操作検出部44は、解錠処理開始操作の入力を検出し、宅配ボックス12のスリープ制御部46は、通信部32をサスペンド状態から通常状態へ復帰させる（S32）。宅配ボックス12の通信部32は、アドバタイズメントパケットを周囲にブロードキャストする（S34）。ユーザ端末14のアドレス通知部108は、アドバタイズメントパケットの受信を契機に、ユーザ端末アドレスを示すデータを宅配ボックス12へ送信する（S36）。

[0074] 宅配ボックス12のチャレンジ設定部48は、ユーザ端末アドレスを含むチャレンジデータを設定し、宅配ボックス12のチャレンジ送信部50は、チャレンジデータをユーザ端末14へ送信する（S38）。宅配ボックス12との通信が開始されると、ユーザ端末14の表示制御部72は、「通信中

」を表示部62に表示させることを開始する。ユーザ端末14のチャレンジ転送部68は、暗号トンネルを介して（言わばSSL通信により）チャレンジデータをサーバ16へ転送する（S40）。

[0075] サーバ16の認証部90は、チャレンジデータに含まれるMACをもとにメッセージ認証を実行する（S42）。メッセージ認証によりチャレンジデータの正当性が確認されると、サーバ16のレスポンス設定部92は、チャレンジデータをもとにレスポンスデータを生成する。サーバ16のレスポンス送信部94は、暗号トンネルを介して（言わばSSL通信により）、レスポンスデータをユーザ端末14へ送信する（S44）。ユーザ端末14のレスポンス転送部70は、レスポンスデータを宅配ボックス12へ転送する（S46）。

[0076] 宅配ボックス12の認証部54は、（1）チャレンジデータ送信からレスポンスデータ受信までの応答時間t、（2）レスポンスデータの乱数値、（3）レスポンスデータのMAC、（4）レスポンスデータのユーザ端末アドレスをもとに、レスポンスデータが正当か否かを認証する（S48）。レスポンスデータが正当と判定された場合、宅配ボックス12の解錠部56は、電気錠38を解錠する（S50）。ユーザは、宅配ボックス12の扉部36を開けて、宅配ボックス12に格納された物品を取り出すことができる。

[0077] 第2実施例の遠隔制御システム10でも、第1実施例の遠隔制御システム10と同様の効果を奏する。また、第2実施例の遠隔制御システム10では、宅配ボックス12は、ユーザ端末14のアドレスを事前に取得し、制御データの送信者のアドレスとの同一性を確認する。これにより、攻撃者の端末によるユーザ端末14へのなりすまし攻撃（例えば中間者攻撃）を一層確実に防止できる。

[0078] また、第2実施例の遠隔制御システム10では、サーバ16は、クライアント認証によりユーザ端末14の正当性を確認する。これにより、攻撃者の端末によるユーザ端末14へのなりすまし攻撃（例えば中間者攻撃）を一層確実に防止できる。

[0079] 以上、本開示を第1実施例と第2実施例をもとに説明した。これらの実施例は例示であり、各構成要素あるいは各処理プロセスの組合せにいろいろな変形例が可能で、またそうした変形例も本開示の範囲にあることは当業者に理解されるところである。

[0080] 第1実施例および第2実施例の遠隔制御システム10は、宅配ボックス12、ユーザ端末14、サーバ16を備えた。変形例として、遠隔制御システム10は、宅配ボックス12とユーザ端末14を備えるが、サーバ16を備えなくてもよい。この場合、ユーザ端末14は、実施例のサーバ16のレスポンス設定部92の機能を備えてもよい。例えば、ユーザ端末14が、制御データを含むレスポンスデータを生成し、生成したレスポンスデータを宅配ボックス12へ送信してもよい。この変形例においても、第1実施例および第2実施例と同様の効果を奏する。例えば、チャレンジデータ送信からレスポンスデータ受信までの応答時間に制限を設けることで、レスポンスデータの窃取と遅延再送による不正な遠隔制御を防止することができる。

[0081] 第1実施例および第2実施例の遠隔制御システム10では、遠隔制御の対象となる被制御装置として宅配ボックス12を例示した。しかし、第1実施例および第2実施例に記載の技術を適用可能な被制御装置は宅配ボックス12に制限されない。被制御装置は、スマートフォン等の通信端末を利用して遠隔制御される様々な装置であってよい。例えば、被制御装置は、スマートロック装置、車両のキーレスエントリー装置、LPS (Local Positioning System) を使用したマンロケーションシステム、RFID (Radio Frequency Identifier) を使用したキャッシュレス購買システムであってもよい。

[0082] 上述した実施例および変形例の任意の組み合わせもまた本開示の実施の形態として有用である。組み合わせによって生じる新たな実施の形態は、組み合わせられる実施例および変形例それぞれの効果をあわせもつ。また、請求項に記載の各構成要件が果たすべき機能は、実施例および変形例において示された各構成要素の単体もしくはそれらの連携によって実現されることも当業者には理解されるところである。

[0083] 実施例および変形例に記載の技術は、以下の項目によって特定されてもよい。

[項目 1]

遠隔制御の対象となる被制御装置（１２）と、

前記被制御装置（１２）と無線通信を行う移動可能な通信端末（１４）と

、

を備え、

前記被制御装置（１２）は、遠隔制御を受け付ける際に、第１データを前記通信端末（１４）へ送信し、

前記通信端末（１４）は、前記第１データへの応答として、遠隔制御の内容を含む第２データを前記被制御装置（１２）へ送信し、

前記被制御装置（１２）は、前記第１データを送信してから前記第２データを受信するまでの時間が予め定められた閾値未満である場合、前記第２データに含まれる遠隔制御の内容に応じた処理を実行する、

遠隔制御システム（１０）。

[項目 2]

前記第１データは、前記被制御装置（１２）により決定された乱数を含み

、

前記第２データは、前記第１データに含まれる乱数をもとに決定された検証値を含み、

前記被制御装置（１２）は、前記第２データに含まれる検証値に応じて、前記第２データに含まれる遠隔制御の内容に応じた処理の実行を制限する、

項目 1 に記載の遠隔制御システム（１０）。

[項目 3]

ネットワークを介して前記通信端末（１４）と接続されるサーバ（１６）をさらに備え、

前記通信端末（１４）は、受信した第１データを前記サーバ（１６）へ転送し、

前記サーバ（１６）は、前記第１データへの応答として、前記第２データを前記通信端末（１４）へ送信し、

前記通信端末（１４）は、受信した第２データを前記被制御装置（１２）へ転送する、

項目１または２に記載の遠隔制御システム（１０）。

[項目４]

前記第１データは、メッセージ認証コードを含み、

前記サーバ（１６）は、前記第１データに含まれるメッセージ認証コードを用いたメッセージ認証の結果に応じて、前記第２データの送信を抑制する、

項目３に記載の遠隔制御システム（１０）。

[項目５]

前記第２データは、メッセージ認証コードを含み、

前記被制御装置（１２）は、前記第２データに含まれるメッセージ認証コードを用いたメッセージ認証の結果に応じて、前記第２データに含まれる遠隔制御の内容に応じた処理の実行を制限する、

項目３または４に記載の遠隔制御システム（１０）。

[項目６]

前記サーバ（１６）は、前記通信端末（１４）に対するクライアント認証を実行し、前記クライアント認証の結果に応じて、前記通信端末（１４）との通信を制限する、

項目３から５のいずれかに記載の遠隔制御システム（１０）。

[項目７]

前記サーバ（１６）は、前記通信端末（１４）に対するクライアント認証を実行し、前記通信端末（１４）は、前記サーバ（１６）のサーバ認証を実行することにより、前記サーバ（１６）と前記通信端末（１４）は、相互認証を実行し、

前記サーバ（１６）は、前記相互認証の結果に応じて、前記通信端末（１

4) との通信を制限する、

項目 3 から 5 のいずれかに記載の遠隔制御システム (10)。

[項目 8]

前記通信端末 (14) は、自端末のアドレスを前記被制御装置 (12) へ通知し、

前記第 1 データは、前記通信端末 (14) のアドレスに対応するデータを含み、

前記第 2 データは、前記第 1 データに含まれる前記通信端末 (14) のアドレスに対応するデータを含み、

前記被制御装置 (12) は、前記第 2 データに含まれる前記通信端末 (14) のアドレスに対応するデータが、前記第 1 データの送信先アドレスに不整合の場合、前記第 2 データに含まれる遠隔制御の内容に応じた処理の実行を制限する、

項目 1 から 7 のいずれかに記載の遠隔制御システム (10)。

[項目 9]

前記被制御装置 (12) は、前記通信端末 (14) と無線通信を行う通信部 (32) を備え、

前記通信部 (32) は、前記被制御装置 (12) に設けられた電池で駆動し、

前記通信部 (32) は、遠隔制御を受け付けるよう指示する所定の操作が前記被制御装置 (12) に入力された場合に、サスペンド状態から復帰して無線通信を行う、

項目 1 から 8 のいずれかに記載の遠隔制御システム (10)。

[項目 10]

前記被制御装置 (12) は、前記通信端末 (14) と無線通信を行う通信部 (32) を備え、

前記通信部 (32) は、遠隔制御を受け付けるよう指示する所定の操作が前記被制御装置 (12) に入力された場合に、無線通信を行う、

項目 1 から 8 のいずれかに記載の遠隔制御システム（１０）。

[項目 1 1]

前記通信端末（１４）は、前記サーバ（１６）との通信時、または、前記サーバ（１６）および前記被制御装置（１２）との通信時に、通信中であることを表示する、

項目 3 から 7 のいずれかに記載の遠隔制御システム（１０）。

[項目 1 2]

前記被制御装置（１２）は、電気錠（３８）を備え、

前記第 2 データは、前記遠隔制御の内容として、前記電気錠（３８）の解錠を指示するデータを含む、

項目 1 から 1 1 のいずれかに記載の遠隔制御システム（１０）。

産業上の利用可能性

[0084] 本開示は、対象となる装置を遠隔から制御するシステムに利用可能である。

符号の説明

[0085] １０ 遠隔制御システム、 １２ 宅配ボックス、 １４ ユーザ端末、
１６ サーバ、 ３２ 通信部、 ３８ 電気錠。

請求の範囲

- [請求項1] 遠隔制御の対象となる被制御装置と、
前記被制御装置と無線通信を行う移動可能な通信端末と、
を備え、
前記被制御装置は、遠隔制御を受け付ける際に、第1データを前記通信端末へ送信し、
前記通信端末は、前記第1データへの応答として、遠隔制御の内容を含む第2データを前記被制御装置へ送信し、
前記被制御装置は、前記第1データを送信してから前記第2データを受信するまでの時間が予め定められた閾値未満である場合、前記第2データに含まれる遠隔制御の内容に応じた処理を実行する、
遠隔制御システム。
- [請求項2] 前記第1データは、前記被制御装置により決定された乱数を含み、
前記第2データは、前記第1データに含まれる乱数をもとに決定された検証値を含み、
前記被制御装置は、前記第2データに含まれる検証値に応じて、前記第2データに含まれる遠隔制御の内容に応じた処理の実行を制限する、
請求項1に記載の遠隔制御システム。
- [請求項3] ネットワークを介して前記通信端末と接続されるサーバをさらに備え、
前記通信端末は、受信した第1データを前記サーバへ転送し、
前記サーバは、前記第1データへの応答として、前記第2データを前記通信端末へ送信し、
前記通信端末は、受信した第2データを前記被制御装置へ転送する、
請求項1または2に記載の遠隔制御システム。
- [請求項4] 前記第1データは、メッセージ認証コードを含み、

前記サーバは、前記第1データに含まれるメッセージ認証コードを用いたメッセージ認証の結果に応じて、前記第2データの送信を抑制する、

請求項3に記載の遠隔制御システム。

[請求項5]

前記第2データは、メッセージ認証コードを含み、

前記被制御装置は、前記第2データに含まれるメッセージ認証コードを用いたメッセージ認証の結果に応じて、前記第2データに含まれる遠隔制御の内容に応じた処理の実行を制限する、

請求項3または4に記載の遠隔制御システム。

[請求項6]

前記サーバは、前記通信端末に対するクライアント認証を実行し、前記クライアント認証の結果に応じて、前記通信端末との通信を制限する、

請求項3から5のいずれかに記載の遠隔制御システム。

[請求項7]

前記サーバは、前記通信端末に対するクライアント認証を実行し、前記通信端末は、前記サーバのサーバ認証を行うことにより、前記サーバと前記通信端末は、相互認証を実行し、

前記サーバは、前記相互認証の結果に応じて、前記通信端末との通信を制限する、

請求項3から5のいずれかに記載の遠隔制御システム。

[請求項8]

前記通信端末は、自端末のアドレスを前記被制御装置へ通知し、

前記第1データは、前記通信端末のアドレスに対応するデータを含み、

前記第2データは、前記第1データに含まれる前記通信端末のアドレスに対応するデータを含み、

前記被制御装置は、前記第2データに含まれる前記通信端末のアドレスに対応するデータが、前記第1データの送信先アドレスに不整合の場合、前記第2データに含まれる遠隔制御の内容に応じた処理の実行を制限する、

請求項 1 から 7 のいずれかに記載の遠隔制御システム。

[請求項9]

前記被制御装置は、前記通信端末と無線通信を行う通信部を備え、
前記通信部は、前記被制御装置に設けられた電池で駆動し、
前記通信部は、遠隔制御を受け付けるよう指示する所定の操作が前記被制御装置に入力された場合に、サスペンド状態から復帰して無線通信を行う、

請求項 1 から 8 のいずれかに記載の遠隔制御システム。

[請求項10]

前記被制御装置は、前記通信端末と無線通信を行う通信部を備え、
前記通信部は、遠隔制御を受け付けるよう指示する所定の操作が前記被制御装置に入力された場合に、無線通信を行う、

請求項 1 から 8 のいずれかに記載の遠隔制御システム。

[請求項11]

前記通信端末は、前記サーバとの通信時、または、前記サーバおよび前記被制御装置との通信時に、通信中であることを表示する、

請求項 3 から 7 のいずれかに記載の遠隔制御システム。

[請求項12]

前記被制御装置は、電気錠を備え、
前記第 2 データは、前記遠隔制御の内容として、前記電気錠の解錠を指示するデータを含む、

請求項 1 から 11 のいずれかに記載の遠隔制御システム。