(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4759373号
(P4759373)
(45)発行日　平成23年8月31日(2011.8.31)　(24)登録日　平成23年6月10日(2011.6.10)

(51)Int.Cl.　　F I
H04W 84/12 (2009.01)　　H04L 12/28 300Z
H04L 9/36 (2006.01)　　H04L 9/00 685

請求項の数 9　(全 14 頁)

(21)出願番号　特願2005-336005 (P2005-336005)
(22)出願日　平成17年11月21日 (2005.11.21)
(65)公開番号　特開2007-142958 (P2007-142958A)
(43)公開日　平成19年6月7日 (2007.6.7)
審査請求日　平成20年11月18日 (2008.11.18)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　森友　和夫
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　中木　努

最終頁に続く

(54)【発明の名称】通信装置及び通信方法、並びにコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
（１）前記通信装置を含むネットワークの構成が基地局を介して通信するネットワークか、基地局を介さずに通信するネットワークか、と（２）前記ネットワーク上の装置の数、とのうち少なくともいずれか一方を判定する判定手段と、
受信したデータパケットに含まれるパケット番号と前記通信装置が管理するパケット番号とを比較することにより、前記受信データパケットが改ざんされたか否かの改ざん検出を行う改ざん検出手段と、を有し、
前記改ざん検出手段は、前記判定手段による判定結果に基づいて、前記改ざん検出を実行することを特徴とする通信装置。
【請求項２】
前記改ざん検出手段は、前記ネットワーク上の装置の数が３台以上の場合は、前記改ざん検出を行わないことを特徴とする請求項１に記載の通信装置。
【請求項３】
前記改ざん検出手段は、前記ネットワークの構成が基地局を介さずに通信するネットワークであり、かつ、前記ネットワーク上の装置の数が３台以上の場合は、前記改ざん検出を行わないことを特徴とする請求項１に記載の通信装置。
【請求項４】
前記改ざん検出手段は、前記ネットワークの構成が基地局を介して通信するネットワー

クの場合は、前記ネットワーク上の装置の数に拘らずに、前記改ざん検出を行うことを特徴とする請求項１に記載の通信装置。
【請求項５】
受信した暗号化されたデータパケットを、前記受信した暗号化されたデータパケットのパケット番号に基づいて復号する復号手段を有し、
前記改ざん検出手段は、前記判定手段による判定結果に基づいて、前記復号手段が復号したデータを改ざんされていないデータとして扱うことを特徴とする請求項１に記載の通信装置。
【請求項６】
前記改ざん検出手段は、前記通信装置と通信する装置の数と前記ネットワークの構成とに基づいて、前記改ざん検出を実行するか否かを切替えることを特徴とする請求項１に記載の通信装置。
【請求項７】
前記判定手段は、前記ネットワークの構成がＩｎｆｒａｓｔｒｕｃｔｕｒｅネットワークか、Ａｄ　ｈｏｃネットワークかを判定することを特徴とする請求項１に記載の通信装置。
【請求項８】
通信装置の通信方法であって、
（１）前記通信装置を含むネットワークの構成が基地局を介して通信するネットワークか、基地局を介さずに通信するネットワークか、と（２）前記ネットワーク上の装置の数、とのうち少なくともいずれか一方を判定する判定工程と、
受信したデータパケットに含まれるパケット番号と前記通信装置が管理するパケット番号とを比較することにより、前記受信データパケットが改ざんされたか否かの改ざん検出を行う改ざん検出工程と、を有し、
前記改ざん検出工程では、前記判定工程における判定結果に基づいて、前記改ざん検出を実行することを特徴とする通信方法。
【請求項９】
請求項８記載の通信方法をコンピュータに実行させるためのコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信する際のセキュリティ技術に関する。
【背景技術】
【０００２】
無線通信では、通信の傍受を防ぐために暗号化通信が行われる。近年広く普及しているＩＥＥＥ８０２．１１規格に基づく無線ＬＡＮ通信では、ＷＥＰ、ＴＫＩＰ、ＡＥＳなどの暗号方式が利用されている。なお、ＷＥＰはＷｉｒｅ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ、ＴＫＩＰはＴｅｍｐｏｒａｌ　Ｋｅｙ　Ｉｎｔｅｇｒｉｔｙ　Ｐｒｏｔｏｃｏｌ、ＡＥＳはＡｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄの略である。
【０００３】
また、ＩＥＥＥ８０２．１１ｉでは、ＡＥＳの改ざん検出方式として、ＣＣＭＰを用いる。ＣＣＭＰは、Ｃｏｕｎｔｅｒ　ｍｏｄｅ　ｗｉｔｈ　ＣＢＣ－ＭＡＣ（Ｃｉｐｈｅｒ－Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ－Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）Ｐｒｏｔｏｃｏｌの略である。
【０００４】
ＣＣＭＰでは、パケット毎にインクリメントされるパケット番号を利用して暗号化を行う。そして、データの受信側では、そのデータの暗号化に利用されたパケット番号を用いて、受信パケットの復号化及び改ざん検出を行う（非特許文献１）。
【０００５】
また、ＩＥＥＥ８０２．１１規格では、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードと、Ａｄ

ｈｏｃモードの２つの通信モードが規定されている。Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードは、アクセスポイント（以後ＡＰ）を介して通信するモードである。Ａｄ　ｈｏｃモードは、ＡＰを介さずに無線通信装置同士が直接相手と通信するモードである。
【非特許文献１】改訂版　８０２．１１高速無線ＬＡＮ教科書　第３１１頁～第３１６頁／発行　株式会社インプレス　ネットビジネスカンパニー
【発明の開示】
【発明が解決しようとする課題】
【０００６】
上述したようにＣＣＭＰは、パケット番号を利用して暗号処理を行う。つまり、パケット毎に暗号鍵が異なることになる。
【０００７】
ＩｎｆｒａｓｔｒｕｃｔｕｒｅモードにおいてはＡＰがネットワーク下の無線通信装置と各々のパケット番号を管理することでデータ通信が成立している。各無線通信装置においては直接の通信相手はＡＰとなるのでＡＰのＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）Ａｄｄｒｅｓｓに対してのみパケット番号を関連付けして管理すればよい。
【０００８】
しかし、Ａｄ　ｈｏｃモードにおいてはＡＰが存在しない。そのため、各無線通信装置が、ネットワーク下に存在する各通信相手と関連付けたパケット番号を管理する必要がある。従って、各無線通信装置が、ネットワーク下に存在している全ての通信相手の存在を把握し、さらに各通信相手に関連付けしてパケット番号を管理しなければならない。これは非常に複雑な処理を必要として、負荷がかかってしまう。
【０００９】
本発明は、セキュリティの低下を極力少なくしつつも、処理の負荷増大を軽減して通信できるようにすることを目的とする。
【課題を解決するための手段】
【００１０】
上記課題を解決するために、本発明は、通信装置であって、（１）前記通信装置を含むネットワークの構成が基地局を介して通信するネットワークか、基地局を介さずに通信するネットワークか、と（２）前記ネットワーク上の装置の数、とのうち少なくともいずれか一方を判定する判定手段と、受信したデータパケットに含まれるパケット番号と前記通信装置が管理するパケット番号とを比較することにより、前記受信データパケットが改ざんされたか否かの改ざん検出を行う改ざん検出手段と、を有し、前記改ざん検出手段は、前記判定手段による判定結果に基づいて、前記改ざん検出を実行することを特徴とする。
【００１１】
また、通信装置の通信方法であって、（１）前記通信装置を含むネットワークの構成が基地局を介して通信するネットワークか、基地局を介さずに通信するネットワークか、と（２）前記ネットワーク上の装置の数、とのうち少なくともいずれか一方を判定する判定工程と、受信したデータパケットに含まれるパケット番号と前記通信装置が管理するパケット番号とを比較することにより、前記受信データパケットが改ざんされたか否かの改ざん検出を行う改ざん検出工程と、を有し、前記改ざん検出工程では、前記判定工程における判定結果に基づいて、前記改ざん検出を実行することを特徴とする。
【発明の効果】
【００１４】
本発明によれば、セキュリティの低下を極力少なくしつつも、処理の負荷増大を軽減して通信できる。例えば、Ａｄ　Ｈｏｃネットワークにおいて通信相手が１台の場合には、暗号通信及び改ざん検出を実行し、２台以上の場合には、暗号通信は行うが改ざん検出は行わないようにすることで、セキュリティの低下を極力少なくでき、複数の通信相手毎の管理内容を少なくすることで負荷の増大を軽減できる。
【発明を実施するための最良の形態】
【００１５】

はじめに、図９を用いてＣＣＭＰ方式について簡単に説明する。

【００１６】

図９の（ａ）にＣＣＭＰ方式の暗号化処理のブロック図を示す。ＣＣＭＰ方式では、パケット番号インクリメント部９０２によりパケット毎にパケット番号をインクリメントして管理する。図９の（ａ）において入力された平文ＭＰＤＵのＭａｃ　Ｈｅａｄｅｒ、ＭＡＣ　ＨｅａｄｅｒのＡｄｄｒｅｓｓの値（送信元アドレス）と、ユーザーにより設定される一時鍵、パケット番号を用いてデータ部をＣＣＭ暗号化部９０１にて暗号化する。なお、ＭＰＤＵは、ＭＡＣ　Ｐｒｏｔｏｃｏｌ　Ｄａｔａ　Ｕｎｉｔの略である。ＣＣＭＰヘッダ生成部９０３では、暗号化データ、データの整合性をチェックするＭＩＣ、平文より抽出したＭＡＣ　Ｈｅａｄｅｒ、パケット番号と暗号処理に使用する鍵の番号を指定するＫｅｙ　ＩＤよりＣＣＭＰヘッダを生成する。ＭＩＣは、Ｍｅｓｓａｇｅ　Ｉｎｔｅｇｒｉｔｙ　Ｃｈｅｃｋの略である。そして、暗号化ＭＰＤＵ組立部９０４において、それらを組み合わせることにより暗号化されたＭＰＤＵを組み立てる。以上がＣＣＭＰ方式による暗号化処理である。

【００１７】

次に図９の（ｂ）にＣＣＭＰ方式の復号化処理のブロック図を示す。ＣＣＭＰ復号化部９０５では、受信した暗号化ＭＰＤＵのＭＡＣ　Ｈｅａｄｅｒ、ＭＩＣ、ＭＡＣ　ＨｅａｄｅｒのＡｄｄｒｅｓｓの値、パケット番号と、ユーザーにより設定される一時鍵を用いて暗号化されたデータ部を復号する。平文ＭＰＤＵ組立部９０６は、暗号化されたＭＰＤＵから抽出したＭＡＣ　Ｈｅａｄｅｒと復号化されたデータ部から平文ＭＰＤＵを組み立てる。各無線通信装置は通信相手のＭＡＣ　Ａｄｄｒｅｓｓとパケット番号を関連付けして管理している。この「自装置が管理しているパケット番号」と「受信した暗号化ＭＰＤＵのパケット番号」を比較する。その結果「自装置が管理しているパケット番号」が「受信した暗号化ＭＰＤＵのパケット番号」よりも小さい場合、もしくは同じ場合は受信した暗号化ＭＰＤＵは正常なデータとして判定する。

【００１８】

一方、もし「自端末が管理しているパケット番号」が「受信した暗号化ＭＰＤＵのパケット番号」よりも大きい場合は、受信した暗号化ＭＰＤＵは改ざんされているとみなす。この処理を「Ｒｅｐｌａｙ　Ｃｈａｃｋ」と呼び、Ｒｅｐｌａｙ　Ｃｈｅｃｋ処理部９０７にて実行する。

【００１９】

以上がＣＣＰＭ方式による暗号処理、復号処理、改ざん検出の仕組みである。

【００２０】

以下、添付図面に従って本発明に係る実施例を説明する。

【００２１】

図１では、撮像装置としてのデジタルスチルカメラ（以後ＤＳＣ）１０１と、出力装置としてのプリンタ１０２が、ＩＥＥＥ８０２．１１規格のＡｄ　ｈｏｃモードで無線通信するものとする。

【００２２】

また、ＤＳＣ１０１とプリンタ１０２は、ＣＣＭＰ方式によりデータを暗号化し、ＣＣＭＰにより復号処理及び改ざん検出を行う。

【００２３】

図２に、本実施例におけるＤＳＣ１０１の機能ブロック図を示す。操作部２１０は、システムコントローラ２１１を介してＣＰＵ２１５に接続されており、操作部２１０にはＤＳＣ１０１のシャッタースイッチや各種キーが含まれる。撮像部２０２は、シャッターが押下されたときに画像を撮影するブロックで、撮像処理部２０３によって処理される。表示部２０６は、ＬＣＤ表示、ＬＥＤ表示、音声表示等、ユーザーに対する情報を表示するブロックであり、表示処理部２０７によってその表示内容の制御処理が行われる。また表示部２０６に表示された情報から選択するなどの操作は操作部２１０と連動して行われることになる。すなわち、表示部２０６と操作部２１０とがユーザーインタフェース（Ｉ／

Ｆ）を構成することになる。無線通信機能部２０４は無線通信を行うブロックであり、ＲＦ部２０５は、他の無線通信機器との間で無線信号の送受信を行う。無線通信機能部２０４とＲＦ部２０５によりＤＳＣ１０１の無線部を構成する。メモリカードＩ／Ｆ２０８は、メモリカード２０９を接続する為のインタフェースである。ＵＳＢ　Ｉ／Ｆ２１２は、外部機器とＵＳＢを用いて接続する為のインタフェースである。オーディオＩ／Ｆ２１４は、音信号を外部機器と接続する為のインタフェースである。これらのブロック図に示される機能部分は、ＣＰＵ２１５からの制御によって処理され、後述する各種制御を含め、ＣＰＵ２１５によって制御されるプログラムは、ＲＯＭ２１６、もしくは、フラッシュＲＯＭ２１３に格納されることになる。また、ＣＰＵ２１５によって処理されるデータは、ＲＡＭ２１７、もしくは、フラッシュＲＯＭ２１３に対して、書き込み、読み込みが行われる。フラッシュＲＯＭ２１３は不揮発性の記憶領域であり、ここに無線通信の設定情報などを記憶する。なお、撮像した画像データは圧縮処理を経てメモリカードＩ／Ｆ２０８を介し、メモリカード２０９に書き込まれる（保存される）。

【００２４】

図３に、本実施例におけるプリンタ１０２の機能ブロック図を示す。操作部３１０は、システムコントローラ３１１を介してＣＰＵ３１５に接続されている。プリントエンジン３０２は、用紙に画像をプリントする機能ブロックであり、プリント処理部３０３によって処理される。表示部３０６は、ＬＣＤ表示、ＬＥＤ表示、音声表示等、ユーザーに対する情報を表示するブロックであり、表示処理部３０７の制御によりその表示内容が制御される。また表示部３０６に表示された情報から選択するなどの操作は操作部３１０を介して行われる。つまり、表示部３０６及び操作部３１０がプリンタ１０２のユーザーＩ／Ｆを構成することになる。無線通信機能部３０４は無線通信を行うブロックであり、ＲＦ部３０５は、他の無線通信機器との間で無線信号の送受信を行う。無線通信機能部２０４とＲＦ部２０５によりプリンタ１０２の無線部を構成する。メモリカードＩ／Ｆ３０８は、脱着可能なメモリカード３０９を接続する為のインタフェースであり、ＤＳＣ１０１に搭載されたメモリカードを差し込むことで、撮像画像を印刷することも可能にしている。ＵＳＢ　Ｉ／Ｆ３１２は、外部機器とＵＳＢを用いて接続する為のインタフェース、パラレルＩ／Ｆ３１４は、外部機器（主としてホストコンピュータ）とパラレル通信を用いて接続する為のインタフェースである。これらのブロック図に示される機能部分は、ＣＰＵ３１５からの制御によって処理され、後述する各種制御を含め、ＣＰＵ３１５によって制御されるプログラムは、ＲＯＭ３１５、もしくは、フラッシュＲＯＭ３１３に格納される。ＣＰＵ３１５によって処理されるデータは、ＲＡＭ３１７、もしくは、フラッシュＲＯＭ３１３に対して、書き込み、読み込みが行われる。フラッシュＲＯＭ３１３は不揮発性の記憶領域であり、ここに無線通信の設定情報などを記憶する。

【００２５】

図４に、本実施例におけるＣＣＭＰ方式の復号ブロック図を示す。ＤＳＣ１０１、プリンタ１０２の無線通信機能部２０４、３０４もしくはＲＦ部２０５、３０５は、図４に示す複号ブロックを具備する。

【００２６】

図４の示すＣＣＭＰ方式の復号ブロックは、図９の（ｂ）にて説明した復号ブロック図に対してＲｅｐｌａｙ　Ｃｈｅｃｋ制御部４０１が追加されている。Ｒｅｐｌａｙ　Ｃｈｅｃｋ制御部４０１は、通信路の切り替え機能を具備し、平文ＭＰＤＵ組立部９０６からの出力を、出力端子４０２もしくは端子４０３へ切り替える。端子４０３に切り替えた時は、Ｒｅｐｌａｙ　Ｃｈｅｃｋ処理部９０７にて「Ｒｅｐｌａｙ　Ｃｈｅｃｋ」を実行し、パケット番号を用いた改ざん検出を行う。改ざんが検出された場合は、受信したデータを破棄し、改ざんが認められない場合は、正常なデータとして上位アプリケーションに引き渡す。また、端子４０２へ切り替えた時は「Ｒｅｐｌａｙ　Ｃｈｅｃｋ」を実行せずに、平文ＭＰＤＵ組立部９０６の出力を受信データとして上位アプリケーションに引き渡す。

【００２７】

次に、ＤＳＣ１０１、プリンタ１０２における無線パラメータを図５に示す。図５に示す各種パラメータは、操作部２１０、３１０の操作によりユーザーにより設定される。または、ＤＳＣ１０１にて設定したパラメータをＵＳＢメモリ等にコピーし、そのＵＳＢメモリ等のパラメータをプリンタ１０２にコピーする方法がある。さらに、無線パラメータのデータ交換のためにＤＳＣ１０１、プリンタ１０２間でＡｄ　ｈｏｃネットワークを構築し、自動的に無線パラメータ交換、設定する方法などもある。

【００２８】

図５の「Ｎｅｔｗｏｒｋ　Ｍｏｄｅ」は、無線ネットワークの構成が「Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ」、または「Ａｄ　ｈｏｃ」なのかを指定するための項目である。ここでは「Ａｄ　ｈｏｃ」が設定されている。

【００２９】

「ＳＳＩＤ」はネットワーク識別子を示す。

【００３０】

「ＣＨ　Ｎｕｍｂｅｒ」は使用する周波数チャネルを指定するものであり、この項目はＡｄ　ｈｏｃモードで自機がネットワークを構成する際に使用する。

【００３１】

「Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｔｙｐｅ」はＩｎｆｒａｓｔｒｕｃｔｕｒｅモードでネットワークが構成される際に適用される認証方法を指定する。具体的には、Ｏｐｅｎ　Ｓｙｓｔｅｍ、Ｓｈａｒｅｄ　Ｓｙｓｔｅｍ、ＷＰＡ、ＷＰＡ－ＰＳＫのいずれかをユーザーが選択する。Ａｄ　ｈｏｃモードを用いる場合は、本項目は意味をなさない。なお、ＷＰＡは、ＷｉＦｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ、ＷＰＡ－ＰＳＫはＷｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　Ｐｒｅ－ｓｈａｒｅｄ　ｋｅｙの略である。

【００３２】

「Ｅｎｃｒｙｐｔｉｏｎ　Ｔｙｐｅ」は無線ネットワークにて適用される暗号化方法を指定する。具体的には、ＷＥＰ（４０ｂｉｔ）、ＷＥＰ（１０４ｂｉｔ）、ＴＫＩＰ、ＣＣＭＰなどがあり無線機器において初期設定としていずれかを選択及び自動的に選択、またはユーザーが選択する。ここでは暗号方式として、ＣＣＭＰを選択している。

【００３３】

「Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ」は暗号化時に用いられる鍵を指定する。暗号鍵は、無線機器が自動的に生成、またはユーザーが直接入力することで設定してもよい。ここでは暗号方式としてＣＣＭＰを選択したので「８文字以上６３文字以下」で構成される暗号鍵をユーザーが設定するものとする。

【００３４】

さらにユーザーはネットワークを構成する機器の台数を指定する。ここでは、ＤＳＣ１０１とプリンタ１０２の２台である。従ってネットワーク構築台数を２台と指定する。無線通信機能部２０４、３０４は、このネットワーク構築台数により、Ｒｅｐｌａｙ　Ｃｈｅｃｋ部９０７によるＲｅｐｌａｙ　Ｃｈｅｃｋを実行するか否かを決定する。

【００３５】

図６にＲｅｐｌａｙ　Ｃｈｅｃｋ制御フローチャートを示す。なお、図６に示す制御は、ＣＰＵ２１５、３１５が、ＲＯＭ２１６、３１６もしくは、フラッシュＲＯＭ２１３、３１３に格納されたプログラムに従って実行する。また、ＣＰＵ２１５、３１５からの指示により図４の復号ブロックを後述のように制御する。または、無線通信機能部２０４、３０４が制御部を有する場合は、この制御部が図４の復号ブロックを制御してもよい。

【００３６】

以下、図６の制御をＣＰＵ２１５、３１５が実行するものとして説明する。

【００３７】

図６において、ＣＰＵ２１５、３１５は、図５のＥｎｃｒｙｐｔｉｏｎ　ＴｙｐｅがＣＣＭＰに設定されたかどうかを判定する（ステップＳ６０１）。ＣＣＭＰでない場合は、ステップＳ６０５に進み、ＣＣＭＰに設定されている場合は、ステップＳ６０２においてＮｅｔｗｏｒｋ　ＭｏｄｅがＡｄ　Ｈｏｃモードに設定されているかを判定する。Ａｄ

Ｈｏｃモードでない場合は、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードであるので、Ｒｅｐｌａｙ　Ｃｈｅｃｋを実行するために、平文ＭＰＤＵ組立部９０６からの出力を端子４０３に接続する（ステップＳ６０４）。Ａｄ　Ｈｏｃモードに設定されている場合は、ステップＳ６０３においてネットワーク構築台数が２台となっているかを判定する。ネットワーク構築台数が２台の場合は、通信相手が１台だけであり、複数の通信相手毎の管理を行う必要が無いので、Ｒｅｐｌａｙ　Ｃｈｅｃｋを実行するために、平文ＭＰＤＵ組立部９０６からの出力を端子４０３に接続する（ステップＳ６０４）。つまりネットワーク構築台数が２台と指定されると、パケット番号によるＲｅｐｌａｙ　Ｃｈｅｃｋを行うようにする。

【００３８】

また、ネットワーク構築台数が２台でない場合は、ステップＳ６０５に進む。ステップＳ６０５では、Ｒｅｐｌａｙ　Ｃｈｅｃｋを実行しないようにするために、平文ＭＰＤＵ組立部９０６からの出力を端子４０２に接続する。

【００３９】

以下、Ａｄ　ｈｏｃモード（中継局を介さない直接通信するモード）による無線通信機器の接続方法を図７を用いて説明する。図１において、ＤＳＣ１０１、プリンタ１０２は無線通信機能を搭載している。該機能では、「Ｂｅａｃｏｎ」と呼ばれる無線通信に必要な情報を周辺無線装置へ報知する信号を各機器でランダムに持ち回りで発することで同期をとる。

【００４０】

ここではＤＳＣ１０１、プリンタ１０２には予め同一の無線パラメータが設定されているものとしてＡｄ　ｈｏｃネットワークを構築する方法を説明する。

【００４１】

まずプリンタ１０２の無線通信機能の電源部をＯＮにする。プリンタ１０２は予め設定されているＡｄ　ｈｏｃモードの無線パラメータに基づいて構成されているＡｄ　ｈｏｃネットワークを検索する。その方法は「Ｂｅａｃｏｎ」を検索する方法、「Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔ」という制御信号をブロードキャストに発信し、「Ｐｒｏｂｅ　Ｒｅｓｐｏｎｓｅ」という応答を待つ方法などがある。ここでは後者を採用する。プリンタ１０２は、「Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔ」を発信し（Ｓ７０１）、「Ｐｒｏｂｅ　Ｒｅｓｐｏｎｓｅ」の応答を待つ。ここではプリンタ１０２が検索しているＡｄ　ｈｏｃネットワークには、他の機器が存在しないため、ある一定回数の「Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔ」を送信しても「Ｐｒｏｂｅ　Ｒｅｓｐｏｎｓｅ」を受け取れない。従って自らネットワークを構築し、「Ｂｅａｃｏｎ」の発信を開始する（Ｓ７０２）。

【００４２】

次にＤＳＣ１０１の無線通信機能の電源部をＯＮにする。プリンタ１０２と同様に予め設定されているＡｄ　ｈｏｃモードの無線パラメータに基づいて構築されているＡｄ　ｈｏｃネットワークを検索するために「Ｐｒｏｂｅ　Ｒｅｑｕｅｓｔ」を発信する（Ｓ７０３）。ＤＳＣ１０１が検索しているＡｄ　ｈｏｃネットワークはすでにプリンタ１０２によって構築されている。従ってプリンタ１０２はＤＳＣ１０１に対して「Ｐｒｏｂｅ　Ｒｅｓｐｏｎｓｅ」を応答し、ＤＳＣ１０１は該応答を受信する（Ｓ７０４）。「Ｐｒｏｂｅ　Ｒｅｓｐｏｎｓｅ」を受信したＤＳＣ１０１はプリンタ１０２が構築したＡｄ　ｈｏｃネットワークの同期情報等を取得し、Ａｄ　ｈｏｃネットワークへ参加できる。

【００４３】

以上の方法によりＡｄ　ｈｏｃネットワークに参加したＤＳＣ１０１はＡｄ　ｈｏｃネットワーク上の機器を検索し、印刷処理を指示するプリンタ１０２を選択する。この無線通信で扱うデータはＣＣＭＰ方式によって暗号化されている（図９（ａ）参照）。その際のパケット番号の制御を図８にて説明する。

【００４４】

ＤＳＣ１０１、プリンタ１０２においてパケット番号は、図８に「送信番号」の値として示す様にパケットの送信毎にインクリメントされていく。また図８に「受信番号」とし

て示される各々の機器が受信時に期待するパケット番号の値もパケット受信毎に受信処理後にインクリメントされる。ＤＳＣ１０１、プリンタ１０２は、受信したデータのパケット番号（図８では「Ｐａｃｅｋｔ　Ｎｕｍ」）と、各機器（ＤＳＣ１０１、プリンタ１０２）が管理している受信番号とを比較する。そして、図９（ｂ）において説明したように、この比較により受信パケットが改ざんされているかどうかを判定する。

【００４５】

ここで図８に示すように仮にユーザー想定外の第３の無線通信機能を搭載したＤＳＣ（図１には図示せず）が過去に送信された正しいパケットの一部を借用して送信元を偽って偽造パケットを送信してきたとする。しかし図に示すように第３の装置の送信パケットに含まれるパケット番号はＤＳＣ１０１、プリンタ１０２のパケット番号より小さい。従ってユーザー想定外の第３の装置からＤＳＣ１０１、プリンタ１０２がＣＣＭＰ方式によって暗号化されたデータを受信しても「Ｒｅｐｌａｙ　Ｃｈｅｃｋ」により正常なパケットでないことが判明するため不正なアクセスを防ぐことを可能とする。

【００４６】

以上よりＡｄ　ｈｏｃモード時におけるＣＣＭＰ方式によるデータ通信を容易にかつ負荷を増大させることなく実現することを可能とする。

【００４７】

次に、図１０に示すように２台のＤＳＣ１００１、１００２、１台のプリンタ１００３の３台の機器によってネットワークが構成される場合について説明する。ＤＳＣ１００１、１００２、プリンタ１００３の構成は図２、３において説明した構成と同様である。

【００４８】

ＤＳＣ１００１、１００２、プリンタ１００３における無線パラメータは「ネットワーク構築台数」以外のパラメータは図５と同様とし、「ネットワーク構築台数」は「３台」とする。図６のフローチャートに従うと、ネットワーク構築台数が「３台」であれば「Ｒｅｐｌａｙ　Ｃｈｅｃｋ」は「Ｏｆｆ」となる。つまりネットワーク構築台数が３台と指定されると図４のＲｅｐｌａｙ　Ｃｈｅｃｋ制御部４０１はスイッチを端子４０２側に切り替え、パケット番号のＲｅｐｌａｙ　Ｃｈｅｃｋを行わない。

【００４９】

従って、Ａｄ　ｈｏｃモード時に、ネットワークを構築する機器が３台以上の場合には、複数の通信相手毎にパケット番号を管理するという複雑な制御を行う必要がなくなり、各機器の処理の負荷を軽減することができる。また、その場合であっても、ＣＣＭＰ方式による暗号化通信は行うので、セキョリティの低下を少なくすることができる。特に、ＣＣＭＰ方式による暗号通信は暗号強度がＷＥＰと比較して強いため、Ｒｅｐｌａｙ　Ｃｈｅｃｋを実施しない場合においても、全体としてセキュリティレベルの向上に繋がる。

【００５０】

次に、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードにおける通信について説明する。

【００５１】

図１１は、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードにおけるシステム構成であり、ＤＳＣ１１０１、プリンタ１１０２、無線アクセスポイント１１０３（以下ＡＰ）によってネットワークが構成される。ＤＳＣ１１０１、プリンタ１１０２の構成は図２、３において説明した構成と同様である。

【００５２】

ＡＰ１１０３はＩＥＥＥ８０２．１１系の無線通信を制御する無線アクセスポイントである。

【００５３】

ＤＳＣ１１０１、プリンタ１１０２における無線パラメータは無線ネットワークの構成方法に依存する。Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードの場合は、図５の「Ｎｅｔｗｏｒｋ　Ｍｏｄｅ」を「Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ」とする。また、「ＳＳＩＤ」、「Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｔｙｐｅ」、「Ｅｎｃｒｙｐｔｉｏｎ　Ｔｙｐｅ」、「Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ」においてはＡＰ１１０３に設定されている設定値と同様の

値を設定する。ここでは特に「Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｔｙｐｅ」を「ＷＰＡ－ＰＳＫ」、「Ｅｎｃｒｙｐｔｉｏｎ　Ｔｙｐｅ」を「ＣＣＭＰ」と設定する。「ＣＨ　Ｎｕｍｂｅｒ」はＡＰ１１０３が使用する動作チャネル、「ネットワーク構築台数」はＡＰが管理する台数であるので本項目の指定はしなくて良い。

【００５４】

図６のフローチャートに従うと、「Ｎｅｔｗｏｒｋ　Ｍｏｄｅ」が「Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ」であるので、「Ｒｅｐｌａｙ　Ｃｈｅｃｋ」は「Ｏｎ」となる。つまり図４のＲｅｐｌａｙ　Ｃｈｅｃｋ制御部４０１はスイッチを端子４０３側に切り替え、パケット番号を用いたＲｅｐｌａｙ　Ｃｈｅｃｋを行う。なお、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードの場合は、各通信装置は、ＡＰ１１０３に対してのパケット番号を管理すればよい。

【００５５】

なお、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモードにおける無線接続のためのパラメータは、例えばＤＳＣ１１０１にＡＰ１１０３に設定されている値と同様の無線パラメータを設定する。そして、そのパラメータをＵＳＢメモリ等にコピーし、そのＵＳＢメモリ等のパラメータをプリンタ１１０２にコピーする方法がある。または、各機器がＡＰ１１０３と無線パラメータのデータ交換のためのネットワークを構築し、そのネットワーク下で無線パラメータ交換をする方法などでよい。

【００５６】

「Ｎｅｔｗｏｒｋ　Ｍｏｄｅ」が「Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ」の場合はＤＳＣ１１０１、プリンタ１１０２はＩＥＥＥ８０２．１１及びＩＥＥ８０２．１１ｉで規定される手順に則りそれぞれＡＰ１１０３との接続処理を行う。このネットワークでは、ＣＣＭＰ方式によって暗号化通信が行われ、ＣＣＰＭ方式による復号処理及び改ざん検出も行われる。

【００５７】

なお、上記説明では、ネットワーク構築台数はユーザーが設定するものとしたが、Ａｄ　Ｈｏｃネットワークに参加している機器の数を自動的に判別し、この数により図６の制御を行うようにしてもよい。この場合、各機器は、Ａｄ　Ｈｏｃネットワークにおいて受信されるＢｅａｃｏｎに含まれる送信元のＭＡＣ　アドレスを管理することにより、Ａｄ　Ｈｏｃネットワークに参加している機器の数を判別することができる。

【００５８】

以上のように、上記説明によれば、ネットワークの構成、通信相手の数によらずＣＣＭＰ方式による暗号化通信を行え、ＷＥＰによる暗号化通信よりもセキュリティを強化することができる。また、Ａｄ　Ｈｏｃモード時に、ネットワークを構築する機器が３台以上の場合には、改ざん検出を行うためにネットワーク化の全ての通信相手を把握する必要がなくなる。また、複数の通信相手毎にパケット番号を管理するという複雑な制御を行う必要がなくなる。従って、各機器の処理の負荷を軽減することができる。また、その場合であっても、ＣＣＭＰ方式による暗号化通信は行うので、セキョリティの低下を少なくすることができる。特に、ＣＣＭＰ方式による暗号通信は暗号強度がＷＥＰと比較して強いため、Ｒｅｐｌａｙ　Ｃｈｅｃｋを実施しない場合においても、全体としてセキュリティレベルの向上に繋がる。

【図面の簡単な説明】

【００５９】

【図１】Ａｄ　Ｈｏｃモード時に機器が２台の場合のシステム構成図。

【図２】デジタルカメラの機能ブロック図。

【図３】プリンタの機能ブロック図。

【図４】ＣＣＭＰ復号ブロック図

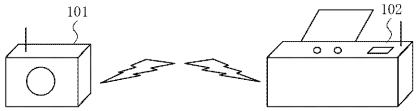
【図５】無線パラメータの項目

【図６】各通信装置が行うＲｅｐｌａｙ　Ｃｈｅｃｋ制御フローチャート図。

【図７】Ａｄ　ｈｏｃネットワークの参加シーケンス

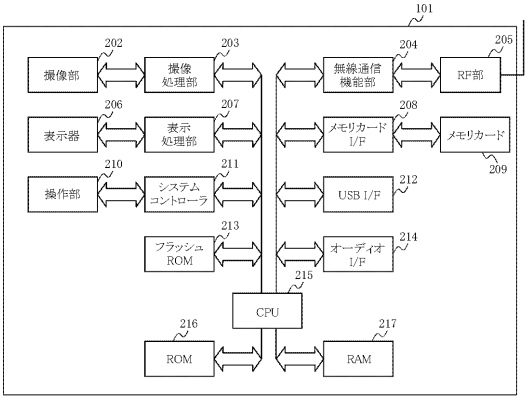
【図８】ＣＣＭＰ方式におけるパケット番号制御図
【図９】ＣＣＭＰ方式による暗号及び復号を説明する図
【図１０】Ａｄ　Ｈｏｃモード時に機器が３台の場合のシステム構成図。
【図１１】Ｉｎｆｒａｓｔｒｕｃｔｕｒｅモード時のシステム構成図。
【符号の説明】
【００６０】
１０１　デジタルカメラ
１０２　プリンタ
９０５　ＣＣＭ暗号化部
９０６　平文ＭＰＤＵ組立部
９０７　Ｒｅｐｌａｙ　Ｃｈｅｃｋ部
４０１Ｒｅｐｌａｙ　Ｃｈｅｃｋ制御部
４０２、４０３　出力端子

【図１】



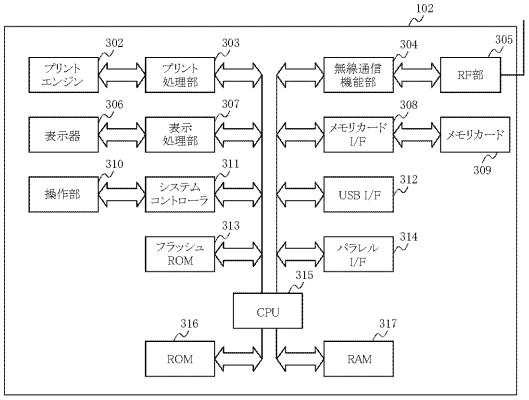
無線接続によるDSCとプリンタのシステム構成

【図２】



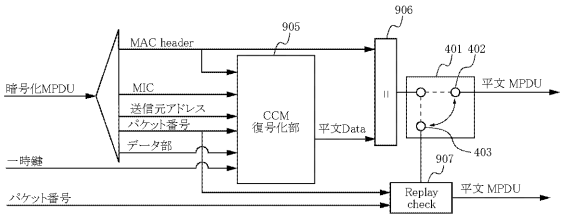
無線通信機能を具備するDSCの機能ブロック図

【図３】



無線LANダイレクトプリントシステム対応プリンタの機能ブロック図

【図４】



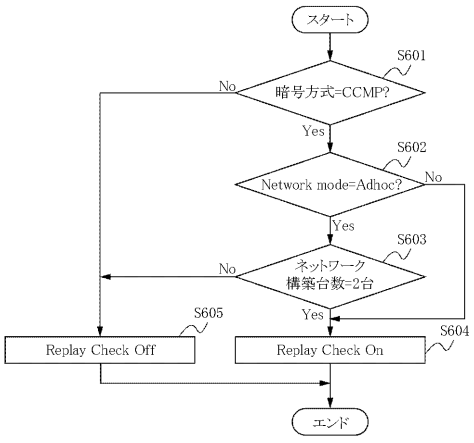
CCMP復号ブロック図

【図５】

無線通信項目	データ詳細
Network Mode	Adhoc
SSID	adhoc_dsc_printer
CH Number	7
Authentication Type	–
Encryption Type	CCMP
Encryption Key	dsctoprinter
ネットワーク構築台数	2台

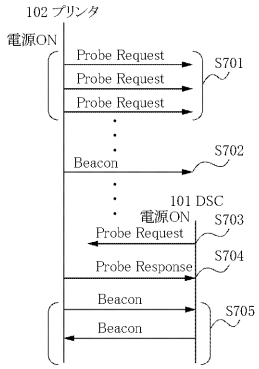
無線パラメータ

【図６】



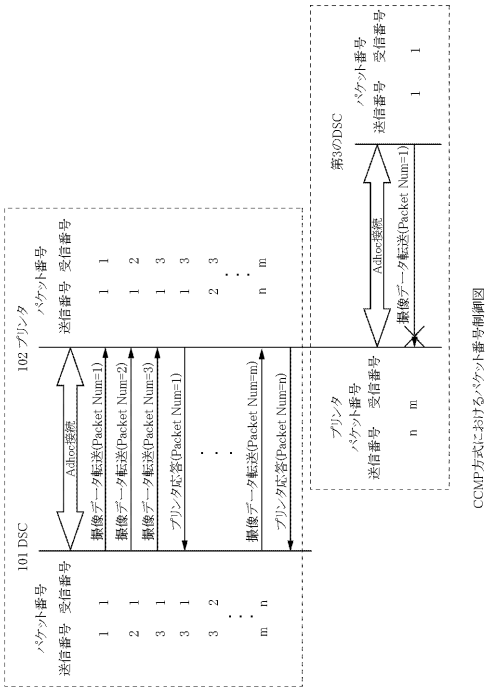
Replay Check制御フローチャート

【図７】



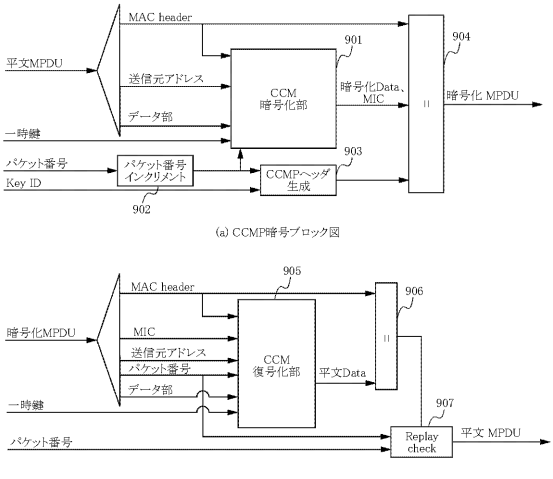
Adhocネットワーク参加シーケンス

【図８】

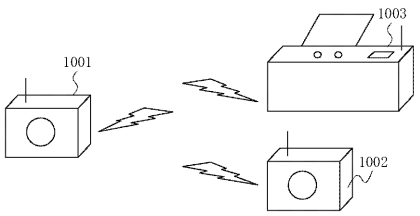


CCMP方式におけるパケット番号制御図

【図９】

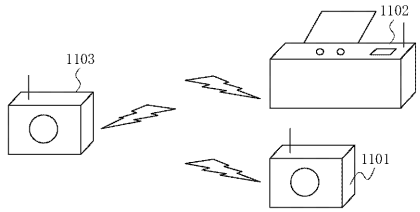


【図１０】



2台のDSCとプリンタによる無線システム構成

【図１１】



APとDSCとプリンタによる無線システム構成

フロントページの続き

(56)参考文献 特開２００７－１１０４８７（ＪＰ，Ａ）
特開２００７－１１６５０９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　８４／１２
Ｈ０４Ｌ　１２／２８－４６
Ｈ０４Ｌ　９／３６