(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7108616号
(P7108616)

(45)発行日　令和4年7月28日(2022.7.28)

(24)登録日　令和4年7月20日(2022.7.20)

(51)国際特許分類

H04W 12/06 (2021.01)		H04W	12/06
H04W 84/18 (2009.01)		H04W	84/18
H04W 4/30 (2018.01)		H04W	4/30

FI

請求項の数　9　（全14頁）

(21)出願番号　特願2019-535929(P2019-535929)
(86)(22)出願日　平成29年12月29日(2017.12.29)
(65)公表番号　特表2020-507240(P2020-507240A)
(43)公表日　令和2年3月5日(2020.3.5)
(86)国際出願番号　PCT/EP2017/084798
(87)国際公開番号　WO2018/122367
(87)国際公開日　平成30年7月5日(2018.7.5)
審査請求日　令和2年12月18日(2020.12.18)
(31)優先権主張番号　A51196/2016
(32)優先日　平成28年12月30日(2016.12.30)
(33)優先権主張国・地域又は機関
オーストリア(AT)

(73)特許権者　398055255
アー・ファウ・エル・リスト・ゲゼルシャフト・ミト・ベシュレンクテル・ハフツング
オーストリア国、８０２０グラーツ、ハンス－リスト－プラッツ、１
(74)代理人　100069556
弁理士　江崎 光史
(74)代理人　100111486
弁理士　鍛冶澤 實
(72)発明者　プリラー・ペーター
オーストリア共和国、８１１１ グラートヴァイン－シュトラーセンゲル、アム・ハング、９
審査官　青木 健

最終頁に続く

(54)【発明の名称】　データネットワーク内におけるネットワークノードの通信

(57)【特許請求の範囲】
【請求項１】
データネットワーク（６）内でネットワークノード（１）と通信パートナー（１０）との間で通信接続を構築するための方法であって、
前記ネットワークノード（１）が、少なくとも１つのメッセージ（Ｍ）をワイヤレスインタフェース（３）経由で前記通信パートナー（１０）から受信し、
照合データ（９）が、前記メッセージ（Ｍ）に添付されている当該方法において、
前記照合データ（９）が、先行する記録周期中に所定の期間内に前記通信パートナー（１０）によって把握された測定データ（７）を示す送信機測定データマップ（８）を含み、
当該受信された照合データ（９）中に含まれている送信機測定データマップ（８）が、前記ネットワークノード（１）にとって既知である相関関係に基づいて、及び／又は前記通信パートナー（１０）によって前記ネットワークノード（１）に通知された相関関係に基づいて、前記送信機測定データマップ（８）に関係なく作成された、前記ネットワークノード（１）のデータメモリ（５）内に記憶されている受信機測定データマップ（８′）と比較されることによって、前記ネットワークノード（１）が、前記通信パートナー（１０）を照合し、
前記送信機測定データマップ（８）と前記受信機測定データマップ（８′）とが一致することは、前記通信パートナー（１０）が、前記ネットワークノード（１）と同じ測定環境（１３）内に存在することを裏付けることを特徴とする当該方法。
【請求項２】

前記ネットワークノード（１）と通信パートナー（１０）とは、互いに独立した計測機器（１１）又は測定環境（１３）のオートメーションシステム（１２）であることを特徴とする請求項１に記載の方法。
【請求項３】
前記ネットワークノード（１）は、前記送信機測定データマップ（８）に基づいて、前記通信パートナー（１０）との暗号化された通信のための暗号鍵を作成することを特徴とする請求項１又は２に記載の方法。
【請求項４】
前記ネットワークノード（１）は、前記受信機測定データマップ（８′）に基づいて、前記通信パートナー（１０）との暗号化された通信のための暗号鍵を作成することを特徴とする請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記ネットワークノード（１）は、前記通信パートナー（１０）の照合後に前記相関関係に基づいて少なくとも１つの仮想ネットワークノード（１１ｃ）を作成することを特徴とする請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記データネットワーク（６）は、アドホックネットワークであることを特徴とする請求項１～５のいずれか１項に記載の方法。
【請求項７】
少なくとも１つの測定トランスデューサ（２）、少なくとも１つのワイヤレスインタフェース（３）、少なくとも１つのプロセッサユニット（４）、及び少なくとも１つのデータメモリ（５）を有するネットワークノード（１）であって、
前記ネットワークノード（１）によって実行可能なプログラム論理が、前記ネットワークノード（１）内に実装されている当該ネットワークノード（１）において、
前記ネットワークノード（１）が、前記プログラム論理の実行時に請求項１～５のいずれか１項にしたがう方法を実行することを特徴とするネットワークノード（１）。
【請求項８】
前記ネットワークノード（１）は、測定環境（１３）用の計測機器（１１）であることを特徴とする請求項７に記載のネットワークノード（１）。
【請求項９】
前記ネットワークノード（１）は、計測機器（１１）又はエンジンテストベンチ（１４）用のオートメーションシステム（１２）であることを特徴とする請求項７に記載のネットワークノード（１）。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データネットワークネット内のネットワークノードと通信パートナーとの間における通信接続構築のための方法に関する。このネットワークノードは、少なくとも１つのメッセージを、通信パートナーからワイヤレスインタフェースを介して受信し且つ、このメッセージには、照合データが添付されている。
【背景技術】
【０００２】
最近では、例えば無線リンクを介するワイヤレスの接続手段によって、数多くの多様な機器が装備されている。データネットワークを設置する度々に面倒な仕事をユーザから引き取るために、そのような機器は、他の互換性のある機器との通信接続を、頻繁に自ら自動的に構築し得、結果として、これら機器の複数個が、アドホックネットワークを形成し、結果として、これら機器が、能動的に、且つ相互の受信領域にある。このような応用分野からのネットワークの例は、公知のブルートゥース規格等を介して、オーディオシステムを自動車用ハンドフリー電話装置として使用する等のために、スマートフォンを車両のオーディオシステムと自動的に連結するなどである。この能力は、「モノのインターネット

」（Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎｇｓ）として公知である開発の一環で、日用品に拡大され、結果として、およそ家庭用品、スマートフォン、ＨｉＦｉ機器、屋内装置、センサ、屋内気候などのための制御器、及び類似の機器が相互に連絡し得、これが、ユーザに絶対に意識される必要はない。

【０００３】

つまり、これによって、ユーザにとって多大な利点が、実現されるが、およそサイバー攻撃の形での悪用の可能性も、さらなるネットワーキングに伴って顕著に増加する。ワイヤレスの通信との組み合わせにおけるモノのインターネット（Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎｇｓ）によって、攻撃者が、見せかけの身元を使用することで、技術的システムへの通信を受容し得、且つ、これによってデータへの不正なアクセスを場合によって獲得し、又は機能を起動し、又は不正な変更を実行し得る危険（ｓｅｃｕｒｉｔｙ ｅｘｐｌｏｉｔ）が存在する。故に、データ通信の自動的な構築の前に、通信パートナーが、信頼できることが、各機器によって確保されなくてはならない。

【０００４】

この信頼できることの確認又は検査は、本開示との関係において、一般的に「照合」として記載される。この照合の作業は、例えば通信パートナーが、同一システムの一部であるかどうかについての検査を含み得る。上記の例において、このシステムは、車両内のほぼ全ての通信パートナーを含み得、車両外部における危機、又は隣接する車両内で機器が、アドホックネットワークに組み込まれることは除外されなくてはならない。現在、この照合は、車両システムとスマートフォンの間に接続が生成される前に、およそスマートフォンのユーザが、車両の表示器に表示されたコードを入力するように要求されることによって、大抵「手で」行われる。

【０００５】

安全上の危惧は、産業上の領域における、且つ増大した安全性要件を有するシステムの領域における独自に連絡する機器の使用が、なぜ問題性を有し得るかの理由でもある。故に、この際においても各機器間のデータ連絡のための資格は、使用者によって定義されなくてはならない。接続は、より高い安全性要件において、暗号化されても構築され得、この際、特に暗号鍵（ｅｎｃｒｙｏｐｔｉｏｎ ｋｅｙｓ）の交換は、攻撃に対して脆弱である。

【０００６】

例えば試験台に存在する計測機器といった産業用途における計測機器が、アドホックに構築されたワイヤレスの通信を介して接続することで、及び場合によってオートメーションシステムへの測定データの本来の伝導からも独立して、データを交換し得ることで、追加的特徴が、実装され得、且つ顧客のための付加利用価値が創出される。上に示された安全配慮の他に、機器が、実際に同一の試験台において、内設されていて、ワイヤレスの通信が、空間境界を越えても可能であるので、且つ、こうして非帰属の機器（およそ他の試験台内の隣接空間内に建造されている機器）にも到達し得ることが、確保されなくてはならない。さらに、通信パートナーが、信用され得、同様に実際、能動的な計測機器のことであり、及び不正な、同じ空間内又は隣接空間内に存在し、及び／又は隠された機器によって、単に見せかけられないことが、確保されなくてはならない。この安全予防措置は、試験台が、多様な企業に賃貸され、結果として、ライバル企業が、隣接する空間内で同時に検査を実行することが起こり得る時に、特に関連し得る。ワイヤレスのセンサネットワークにおいても、この問題性が生起し、これらネットワークにおいて、測定データが、ワイヤレスでオートメーションシステムに伝達される。故に、一定の試験台又は被検体への機器の帰属は、現在、試験台技術者などの手によって、コンフィグされなくてはならない。これは、例えばシリアル番号の入力、又は他の特徴の申告によって行われ得、又は完全自動化が不可能な他の行動も含み得る。この手動の作業によって、入力するヒトが、この作業の一環において、機器の正真性も既に検査したと想定され、ここでも安全性リスクが生じる。現在、この作業は、完全自動化が可能ではなく、且つ正真性の申告におけるエラーは、事後的に検査され得ない。

【０００７】
別の実施例は、可動の測定システムとの関連における試験目的のために、又は大量生産される車両のために、車両内で配分された（ワイヤレスの）相応するシステム（制御器、センサ等）の既に言及されたネットワーキングであって、この実施例において、上記の安全上の問題が、関連している。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明の課題は、アドホックネットワークの接続構築を、さらに確実に及び同時に、さらに容易に成形することであり、特に上に解説された先行技術の欠点が、回避されなくてはならない。
【課題を解決するための手段】
【０００９】
この課題は、請求項１に記載の：
データネットワーク（６）内でネットワークノード（１）と通信パートナー（１０）との間で通信接続を構築するための方法であって、
前記ネットワークノード（１）が、少なくとも１つのメッセージ（Ｍ）をワイヤレスインタフェース（３）経由で前記通信パートナー（１０）から受信し、
照合データ（９）が、前記メッセージ（Ｍ）に添付されていている当該方法において、
前記照合データ（９）が、先行する記録周期中に所定の期間内に前記通信パートナー（１０）によって把握された測定データ（７）を示す送信機測定データマップ（８）を含み、
当該受信された照合データ（９）中に含まれている送信機測定データマップ（８）が、前記ネットワークノード（１）にとって既知である相関関係に基づいて、及び／又は前記通信パートナー（１０）によって前記ネットワークノード（１）に通知された相関関係に基づいて、前記送信機測定データマップ（８）に関係なく作成された、前記ネットワークノード（１）のデータメモリ（５）内に記憶されている受信機測定データマップ（８′）と比較されることによって、前記ネットワークノード（１）が、前記通信パートナー（１０）を照合し、
前記送信機測定データマップ（８）と前記受信機測定データマップ（８′）とが一致することは、前記通信パートナー（１０）が、前記ネットワークノード（１）と同じ測定環境（１３）内に存在することを裏付けることによって解決される。
この方法において、照合データが、送信機測定データマップを含み、この送信機測定データマップが、先行する記録周期中において通信パートナーによって把握された測定データにとって代表的であり、このネットワークノードが、通信パートナーを照合する。これは、追加的な手動の相互作用なしに、ネットワークノードによる通信パートナーの自動的な認識及び照合を可能にする。この際、関与する機器が、共通の同期的時間情報を駆使し、これは、例えば無線時計信号の受信を介して、又はローカルにワイヤレスで送信されたタイムスタンプによって確保され得る。本発明にしたがって、通信パートナーは、同じ測定環境に属することを単に申告しているのかどうかが、又は通信パートナーは、実際に存在しているかどうかが区別され得る。
【００１０】
本発明に係わる方法は、例えば車両内で使用され得る。この方法は、例えば利用者のスマートフォンが、車両内にあり、且つ同行したか否かを認識し得る。「同行した」場合においてのみ、信頼できる接続が（例えばブルートゥースを介して）構築される。例えば、Ｖ２Ｖ（Ｃ２Ｃ）を介して連絡する車両の識別と確実な認証と固有の車両の環境に対する配置といった、さらに広い文脈におけるアプリケーションが、本発明に係わる方法を利用し得る。
【００１１】
受信機測定データマップは、例えばネットワークノードによって、自ら把握された測定データの代表として作成され得、このことは、およそネットワークノードが、計測機器であ

る時、ネットワークノードが、測定データ把握を駆使することを前提とする。しかし、受信機測定データマップは、ネットワークノードによって作成された測定データマップでもあり得、この測定データマップは、測定データに基づいて生成され、この測定データは既に信頼できるとして等級付けられた第三ユニットによって獲得されている。これは、例えばネットワークノードが、オートメーションシステムである時、起こり得て、このオートメーションシステムは、複数個の計測機器の測定データを受信し、且つ記憶する。

【００１２】

本発明に関し、ネットワークノードと通信パートナーは、相互に独立して、測定場所又は、測定環境のオートメーションシステムであり得る。これは、例えば個々の製造者の全ての機器が、アドホックネットワークにおいて相互に連絡し、これら全ての機器が、試験台の測定に関与していて、且つ多様な機器組み合わせの依存において、追加の機能性を提供することを可能にする。測定推移に基づく照合によって、実際に同一の試験台において起動している機器とのみ接続されることが確保されている。通信は、（例えば他の製造者による）他の計測機器が、試験システムに組み込まれている時、又はオートメーションシステムが使用され、このオートメーションシステムが、このアドホックネットワーク構築を支持しない時、相当する機器間でも構築され得る。

【００１３】

本発明に関し、有利な手法で、ネットワークノードが、送信機測定データマップは象に基づいて、通信パートナーとの暗号化された通信のための暗号鍵を作成し得る。この際、ネットワークノードは、通信パートナーによって伝達された送信機測定データマップのデータを使用し得る。

【００１４】

他方で、暗号化情報の伝達は、ネットワークノードが、暗号鍵の作成ために記憶された測定データを使用する時、回避され得る。ネットワークノードは、故に有利な手法で、通信パートナーとの暗号化された通信のための暗号鍵を、受信機測定データマップに基づいて作成し得る。例えば、ネットワークノードは、受信機測定データマップにおいて、送信機測定データマップに相当する時間周期を求め得、且つ暗号鍵を、受信機測定データマップの時間的にずれた時間周期に基づいて作成する。通信パートナーは、送信機測定データマップの時間的にずれた同一の時間周期に基づいて、暗号鍵を作成する。つまり、暗号化されたデータ送達は、送信機測定データマップと受信機測定データマップが、相互に相当し、つまり同一の試験台に関する測定に基づいて、既に生成されていて、この際、暗号鍵のためのデータベースが、データネットワークを介して伝達される必要がない時にのみ機能する。

【００１５】

「暗号鍵」という概念は、この暗号鍵が、メッセージの暗号化又は復号化に役立ち、及び対称的、又は非対称的な暗号化方法のことであるかどうかから独立して、本発明との関係において、一般的に暗号キーのために使用される。

【００１６】

受信機測定データマップと送信機測定データマップとの間における差異は、ネットワークノードと通信パートナーとの間において判明している相関関係によって算出され得る。この相関関係は、例えば時間遅延又は、プラスの、又はマイナスの増大であり得、この増大は、容易に算出され得る。但し、ネットワークノードと通信パートナーの属性が判明している時、より複雑な相関関係も考慮され得る。場合によって、パラメータは、施設でもあり得、この施設に、ネットワークノードと通信パートナーが内設され、相関関係を求めるために使用される。試験台の場合において、例えば被検体の、及び／又は、ダイナモメータの仕事率データ及び／又は、材料データは、考慮され得る。相関関係は、例えば施設の構築によって生じる。例えば駆動歯車において、伝動装置を介して被駆動回転数が、駆動回転数に相関する。

【００１７】

有利な実施例において、ネットワークノードが、通信パートナーの照合後に、相関関係に

基づいて、少なくとも１つの仮想ネットワークノードを作成し得る。例えば第一測定値及び第二測定値から、第三測定値が算出される時、ネットワークノード（このネットワークノードが例えば第一測定値を測定する時）は、通信パートナーの測定データをリアルタイムで受信し、そこから第三測定値を算出するために、通信パートナー（この通信パートナーが、例えば第二測定値を測定する時）との通信を利用し得、及びオートメーションシステムに第三測定値を提供し得る。オートメーションシステムは、第三測定値のデータを、そうして固有のチャネル内で、仮想ネットワークノードが、リアルな計測機器であるかのように、さらに処理し得る。ネットワークノードは、オートメーションシステムである時、１つ以上の通信パートナーの１個以上の測定値に基づいても、第三測定値を作成し得る。

【００１８】

有利な実施例において、データネットワークは、アドホックネットワークであり得る。データネットワークは、アドホックネットワークとして記載され、このデータネットワークは、関与する機器（又はネットワークノードと通信パートナー）のユーザが、コンフィグレーションすることなく、自動的に構築され、結果として、これら機器は、ワイヤレスインタフェースのカバレッジ内に存在する。これと異なり、ユーザによって予設定された定義による従来の手法で、データネットワークを構築することも可能である。その時、本発明に係わる方法は、追加のセキュリティレベルを提供し得る。

【００１９】

本発明は、別の観点において、少なくとも１つの測定トランスデューサ、少なくとも１つのワイヤレスインタフェース、少なくとも１つのプロセッサユニット及び少なくとも１つのデータメモリを有するネットワークノードに関し、このネットワークノード内に、ネットワークノードによって実施可能なプログラム論理が、実装されていて、及びネットワークノードが、プログラム論理実施の際に、上に解説された本発明に係わる方法を実施する。この際、ネットワークノードは、任意の機器であり得、この機器は、アドホックネットワークの構築に好適である。測定トランスデューサは、センサ、又は他の測定データを生成するユニットであり得る。可動のアプリケーションのために、測定トランスデューサは、例えば、位置座標を求めるためのセンサ、特に地理座標を求めるための、例えばＧＰＳチップであり得る。

【００２０】

有利な手法において、ネットワークノードは、測定環境のための計測機器であることが可能である。本発明との関係において、例えば可動の又は定置のラボ、可動の又は定置の試験台、航空機、陸上車両及び／又は船舶、又は一般的に不動産、又は土地範囲といった試験課題及び／又は、分析課題及び／又は制御課題のために定義された領域は、測定環境として記載されていている。

【００２１】

別の有利な実施例において、ネットワークノードは、計測機器、又はエンジンテストベンチのためのオートメーションシステムであることが可能である。

【００２２】

本発明は、下記に図１～４に関連しつつ、一層詳細に解説され、これら図は、例示的、概略的、且つ非減縮的な本発明の優れた発展形を示す。

【図面の簡単な説明】

【００２３】

【図１】本発明に係わる方法を利用するアドホックネットワークの概略図である。

【図２】エンジンテストベンチの概略図であり、このエンジンテストベンチ内に、本発明に係わる方法が実装されている。

【図３】測定信号のグラフによる対比であり且つ、そこから導き出された測定データマップである。及び

【図４】複数個の測定信号のグラフによる対比である。

【発明を実施するための形態】

【００２４】

図１は、測定環境１３を概略的に示し、この測定環境内に、複数個の計測機器１１が配置されていて、これら計測機器が、各々にワイヤレスインタフェース３を介して、相互にデータを交換し得る。各計測機器１１は、測定トランスデューサ２、データメモリ５及びプロセッサユニット４を有する。タイミング信号発生装置１５が、全ての計測機器１１に、合致する時間情報を提供し、結果として、計測機器１１が、必要に応じて、データメモリ５内に記憶されたデータを、相応する時間情報で実装し得る。タイミング信号発生装置１５が、ローカルに、ワイヤレスでタイムスタンプを送信し得る。代替的に、計測機器１１の同期化のために、無線時計信号が利用され得る。

【００２５】

理解しやすいように、下記において、特に試験台環境における本発明に係わる方法と装置の実装について関連が記述され、しかし当業者は、この中に開示された考え方を、他の実施例にも支障なく応用し得る。実施例として、特にシステムが、考慮の対象になり、これらシステムにおいて、複数個の機器が、アドホックネットワークを構築し、且つ使用することができる。

【００２６】

図１において、３つの計測機器１１が、測定環境１３の領域内に配置されていて、これら測定環境は、其々に測定トランスデューサ２を介して、測定データ７を生み出し、且つデータメモリ５内に保存し、及び／又は任意のデータリンクを介して、オートメーションシステムへ伝達する。測定データの伝達は、ワイヤレスインタフェース３を介して、又は他の（図１に不図示の）データリンクを介して行われ得る。

【００２７】

加えて、計測機器１１は、相互に連絡し、且つ、そうしてアドホックネットワークを構築することが可能である。このアドホックネットワーク（このアドホックネットワークは、図１中にデータネットワーク６として概略的に示されていて）は、測定環境１３において、例えば製造者の全ての機器を有し得、これら機器のプログラム論理は、本発明にしたがう方法を支持する。アドホックネットワークを支持しないより古い計測機器１１、又はアドホックネットワークに関与すべきでない他の製造者のコンポーネントは、さらに測定環境１３に組み込まれ得、但しアドホックネットワークの構築の際に考慮されないままである。

【００２８】

２つの計測機器１１間における接続構築は、下記において、ネットワークノード１のために解説され、このネットワークは、通信パートナー１０との通信接続を構築する。ネットワークノード１と通信パートナー１０は、同様に、示された場合において、各々に１つの測定環境１３の計測機器１１である。

【００２９】

「ネットワークノード」と「通信パートナー」という名称は、本願明細書との関係において、単に明細書の明瞭性及び機器の識別可能性、且つ機能的差異を含意する。観察の仕方によって、各機器は、アドホックネットワーク内において、ネットワークノード１又は通信パートナー１０として、見なされ得る。信用できるとして証明しようとする機器が、本願明細書との関係において、通信パートナー１０として記載され、且つ通信パートナー１０の照合を行う機器が、ネットワークノード１として記載される。

【００３０】

全ての計測機器１１は、常時、これら計測機器の測定トランスデューサ２によって記録された測定データ７の測定データマップを、これら計測機器のデータメモリ内に記憶し、通信パートナーの測定データマップが、下記に、送信機測定データマップ８として、及びネットワークノード１の測定データマップが、受信機測定データマップ８′として記載される。測定データマップは、こうして測定データの推移を代表し且つ、定義可能なタイムスパン（例えば最近の１時間）を経て、データメモリ５内に記憶され得る。

【００３１】

計測機器１１は、既に判明しているプロトコールを介し、無線通信範囲内に存在する他の

機器の常時の認識を行い得、且つ既に判明しているアルゴリズムに基づいて、見出された機器とのリンクが構築されるべきかどうかを決定し得る。

【００３２】

図示された状況では、通信パートナー１０が、ネットワークノード１とリンクを構築することを試みる。ネットワークノード１に対して信頼できる機器であることを証明するため、通信パートナー１０は、ワイヤレスインタフェース３を介してメッセージＭを送信する。当該メッセージＭは、ネットワークノード１によって受信される。メッセージＭ内に、送信機測定データマップ８の部分領域を表す照合データ９が含まれている。この場合、当該部分領域は、実際の時間によって規定されている（例えば、測定の最後の２秒）、及び／又は日付によって証明され得る。さらに、メッセージＭは、通常のパケットデータ情報を含んでもよく、例えば通信パートナー１０についての情報を含んでもよい。当該期間は、測定推移中の所定の特徴的な「イベント」に基づいて、例えば２つの測定装置１１の測定データ７の推移に同様に影響を及ぼす負荷変動に基づいて算出されてもよい。

【００３３】

ネットワークノード１は、通信パートナー１０についての情報から、獲得された送信機測定データマップ８とこのネットワークノード１のデータメモリに記憶された受信機測定データマップ８'との間の相関関係を求める。この相関関係は、受信機測定データマップ８'における相当する領域を求めるために（又はその逆）、且つ両方の測定データマップを比較するために、送信機測定データマップ８に適用される。当該両測定データマップが一致する場合、当該一致は、通信パートナー１０が、ネットワークノード１と同じ測定環境１３内に存在することを裏付け、それ故に信頼できると見なされ得る。それ故に、当該肯定的な信頼性の確認後は、さらなるデータ交換に対して、通信パートナー１０とのリンクが構築され得る。同様に、当然に、ネットワークノード１は、通信パートナー１０に対しても信頼できる機器として照合され得る。

【００３４】

攻撃者が、このようなデータ交換を盗聴し、偽りの身元を真正の身元と思わせるために、当該伝送された測定データマップを再び使用することが考えられる（リプレイアタック）。例えば、所定の時間周期の測定データマップが、一回だけ使用され得ることによって、すなわちネットワーク内の複数のネットワークノードからの一回の伝送後は、二度目は拒否されることによって、当該リプレイアタックは阻止され得る。当該データが通信パートナーから供給されなければならない過去の所定の時間周期を、当該ネットワーク内の複数のネットワークノードが、ハンドシェイク法で最初に要求し、この時間周期をそれぞれのデータ交換ごとに新たに（例えば、ランダムに）確立する場合、別の手段があり得る。

【００３５】

場合によって、接続は、通信の盗聴を回避するめに、公知の手順で暗号化されて行われ得る。場合によって、暗号鍵測定データマップ８に基づいて、行われ得る。測定データマップの部分によって既に測定データマップが、相関関係にあることが確認されていて、この部分は、照合データ９内で既に伝達されているので、暗号鍵が、他の（伝達されていない）測定データマップの時間領域に基づいて作成され得、ネットワークノード１が、暗号鍵を、受信機測定データマップ８'に基づいて作成し、且つ通信パートナー１０が、暗号鍵を送信機測定データマップ８に基づいて作成する。この可能性が、両方で同一のコードを生み出し、非常に確実な暗号化メカニズムの実行を可能にするものの、このコードが、両方の通信パートナー間において事前に伝達されている必要は全くない。

【００３６】

確実なリンクを構築する際、この測定データの最初に必要な交換が、事前に攻撃に繋がり得ないこと、例えばここで未だ信用できない（ｕｎ‐ｔｒｕｓｔｅｄ）として扱われることは同様に考慮されなくてはならない。つまり、「マキシマムプロテクション」（ｍａｘｉｍｕｍ　ｐｒｏｔｅｃｔｉｏｎ）設定にあるファイアウォールのように、機能に関して最小限のサブセットのみが駆使可能であることが、考慮されなくてはならない。ローカルに駆使可能なデータの比較は、同様にして、例えば充当に長い時間を経て、充当に可変で

、且つ他に予知可能でない測定信号が使用されることによって、信用できる／信用できない（ｔｒｕｓｔｅｄ／ｕｎｔｒｕｓｔｅｄ）かの判断のための充当な根拠を提供しなければならない。通信パートナーは、既に危殆化していないことを確保することも重要である。これは、例えば、普通に正当な、ローカルに存在するシステムが、既に不正侵入された時、且つ、そうしてこのローカルにのみ駆使可能な情報の認識を有し、且つ既に攻撃者によって操作される時、該当する。これら前提が、確保される時、非常に高い安全規格が達成される。

【００３７】

図１には、別の計測機器１１′が示されている。この計測機器は、測定環境の外側に存在するものの、依然としてデータネットワーク６の無線通信範囲内に存在する。当該別の計測機器１１′は、例えば隣接空間内の他の試験台に配置されている機器であってもよいが、データネットワーク６にサイバー攻撃を試みる隠された機器でもよい。しかしながら、双方の場合、別の計測機器１１′が、リンクを構築しようとしても、ネットワークノード１は、当該別の計測機器１１′を照合しない。何故なら、この別の計測機器の測定データ推移が、他の測定環境に相当し、それ故に測定データマップ８にも一致しないからである。

【００３８】

図２は、本発明の方法が実装されているエンジンテストベンチ１４を示す。エンジンテストベンチ１４に、被検体１６が、配置されていて、例えば内燃機関又は電動発動機が、場合によってパワートレインと接続していて、このパワートレインは、ダイナモメータ１７と接続している。この試験構造において、従来の手法によって、多数の計測機器１１ａ～１１ｄが、配置されていて、これら計測機器の測定は、オートメーションシステム１２によって評価される。オートメーションシステム１２は、被検体１６とダイナモメータ１７のための条件も調整する。

【００３９】

計測機器１１ａ～１１ｄが、これら計測機器の測定トランスデューサ（又はセンサ）のデータを、一定時間（例えば数時間）を経て、周期的に把握し且つ、これらデータを、時間列（同期化された時間情報等と伴に）として、計測機器のデータメモリ５内部に記憶する。メモリの空き容量を節約するために、効果的なデータ削減が行われ得る。例えば一定の変更（測定値における側面、イベント（Ｅｖｅｎｔｓ））が、認識され得、且つイベント（Ｅｖｅｎｔｓ）の概略のみが記憶され得る。

【００４０】

試験台における様々な計測機器１１ａ～１１ｄが、同一の試験構造を観察するので、これら機器が、時間的に相関関係にあるイベント（Ｅｖｅｎｔｓ）を、又は各測定規模に対するこれらイベントの作用を把握しておかねばならない。一般的場合において、システムは、一定の場所的近傍において、相互に一定の物理的作動を、比較可能な時間に、比較可能な手法で把握することが、想定され得る。

【００４１】

一例として、機関の始動に際して、ダイノ測定が、回転数と回転モーメントの変更を認識し、排気ガス測定が、窒素酸化物に関する上昇を認識し、燃料消費測定が、１時間毎の燃料量の変更を認識し、及びシリンダにおける温度測定が、（場合によって遅延された）温度上昇を認識する。これら相関関係は、各測定センサの属性によって、既知であり、又は試験台のために求められ得る。

【００４２】

各計測機器１１ａ～１１ｄは、このような「イベント（Ｅｖｅｎｔｓ）」を、内部のメモリ内に保存する。このようなイベント（Ｅｖｅｎｔｓ）の一定総数の存在にしたがって、一定の確率で、特徴的な詳細（時点、期間、形状…）が合致する際、物理的条件（定義された遅延時間、依存性、物理的規模等）の考慮下における同一のイベント（Ｅｖｅｎｔｓ）のことであって且つ、故に同一の被検体が、予め観察されると想定され得る。つまり、観察時間が、長いほど、関与する機器が、より多くの「共通のヒストリ」を集め、且つ、合致する際に、同じ試験台における計測機器のことであることがより確実である。

【００４３】
識別、他の機器に対する機器「証明」のために、この共通の知識は、帰属性の証拠として上記に解説されたように表され得る。
【００４４】
この知識が、明文よってでなく、暗号法によって暗号化されて外部へ渡される時、この知識が、第三者によって模倣され得ることなく、この知識の機器内における存在のみが、推量され得る。つまり、実際に同時進行の測定を有さない偽造は、不可能である、又は非常に困難である。これによって、つまり、「計測機器が、同じ被検体にある」という情報に加えて、「計測機器が、実際に、リアルな計測機器」であるということも認識され得る。
【００４５】
２つ以上の計測機器１１の測定データ７の組み合わせに基づいて、リアルタイムで第三測定規模を算出することが、一定の状況下において可能である。これは、およそ図２に表示された仮想計測機器１１ｅのような「仮想計測機器」の生成を可能にし、この計測機器の測定データ７は、両方の計測機器１１ａと１１ｂの測定に基づいて作成される。
【００４６】
実際的例として、およそ計測機器１１ａが、被検体１６に送給された燃料量を測定し得、及び計測機器１１ｂが、送給された空気量を測定し得る。これから、排気ガス量のための値が、判明した関係を介して求められる。こうして、この排気ガス量のための値は、アドホックネットワークにおける両計測機器１１ａと１１ｂが、相互に連絡する時、仮想計測機器１１の測定データ７として、オートメーションシステム１２に提供され得る。オートメーションシステム１２が、アドホックネットワークにも組み込まれている場合、仮想計測機器が、オートメーションシステム１２によっても作成され得る。別の計測機器１１ｃと１１ｄは、アドホックネットワークにも組み込まれ得、又は、より旧式の機器、若しくは他の製造者の機器のことであり得、これら機器は、この際ごく普通に使用され得る。
【００４７】
図３は、計測機器１１によって記録された測定データ７と測定データ７に基づいて作成された測定データマップ８間における関係を例示的に表している。表示された場合において、測定データマップ８は、例えば、より低いサンプリングレートを使用することによって、又は他のロスレス（損失のない）データ圧縮方法、又はロッシー（損失のある）データ圧縮方法の応用によって、測定データ７より低いデータ密度を有する。但し、データ密度は、測定データ７の推移に影響する一定のイベント（Ｅｖｅｎｔｓ）を測定データマップ８中にも認識できるように充当に高く選択される。イベントは、例えばプラスのピークによって、及び／又はマイナスのピークによって、及び／又は側面領域の勾配によって認識され得る。測定データマップ８から選出された領域が、（開始時間ｔ１と終了時間ｔ２の間で）照合データ９として使用され得る。そうして、照合データ９は、一定の時間領域における測定データマップ８に相当する。
【００４８】
但し、照合データ９を他の手法で、作成することも可能であり、例えば一定の時間領域における各々に２つのピーク間の距離は、照合データ９を作成するために、データ列として使用される。この場合においても、照合データ９は、測定データマップ８に相当する。しかし、照合データは、勾配の推移、零点等といった測定データマップ８の他の属性にも基づき得、いずれの場合においても、照合データは、各々に少なくとも１つの測定データマップ８のデータの一部を含む。照合データ９が、暗号化されていることも可能である。
【００４９】
場合によって、測定データマップ８から求められたデータ列に基づいて、上記における図１の解説との関係においても、記載された暗号鍵が生み出され得る。
【００５０】
図４において、３つの測定データマップ８、８'及び８"の推移は、センサネットワークの３つの計測機器１１によって、作成され得るように表されている。図４において、３つの計測機器１１は、ノードＳ１、Ｓ２及びＳ３として記載されている。測定データマップ

８、８′、８″は、（図３中に解説されているように）低減されたデータレートを有する各測定データ７に基づいて作成されたデータ推移であり得、又は測定データ７に相当し得る。

【００５１】

表示された例において、ノードＳ１とＳ２は、同じプロセスについて測定し、つまり両ノードＳ１とＳ２の観察結果は、相関関係にある。故にＳ１とＳ２の測定データ７の推移は、合致し、Ｓ２は、Ｓ１に対して、ズレΔｔ分、時間差である。但し、他の認識可能な任意の相関関係は、振動が、エンジンの様々な場所で測定される時に生じる「軽度の」（ｌｅｉｃｈｔｅ）相関関係などでさえ、両測定データ推移の間において支配的であり得る。

【００５２】

ノードＳ３は、他のプロセスについて測定し、Ｓ１とＳ２に対する相関関係は、故に存在しない。

【００５３】

ここで、ノードＳ１が、ノードＳ２に対する通信を（例えば、ノードＳ１が、上に解説されたように、メッセージＭを送ることによって）構築しようとする時、ノードＳ１は、測定データマップ８の部分をメッセージＭに付け加えることで、その正当性を立証する。この部分が、図４中に表示された照合データ９を形成する。

【００５４】

Ｓ１とＳ２の間における相関関係に基づいて、Ｓ２は、測定データマップ８′固有の記録の中に、部分９′を見つけ、この部分が、獲得された照合データ９に相当する。図４の表示の中で、受信機測定データマップ８′は、受信機測定データマップ８に対して、ただ時間的に移動され、データ推移は、他の点で合致する。一層複雑な相関関係も存在し得、これら相関関係からＳ２は、同じプロセスに関して、Ｓ１が、既に測定していて、且つ故にローカルに近いだけでなく、信頼もできることを推量することが可能である。

【００５５】

例えば暗号化されて、信頼できる通信の構築が、その後に続く。プロセスのヒストリの一部の認識が、一致証明として役立つ。こうして、この一部が、信頼済みサイト（ｈｔｔｐｓ）において使用されるような認証といった他のメカニズムを置換する。これは、手間のかかる（多くの場合、ユーザアクセスを要求する）認証管理（Ｚｅｒｔｉｆｉｋａｔｍａｎａｇｅｍｅｎｔ）が、不要であるという利点を提供する。

【００５６】

場合によって、ノードＳ２は、そうしてＳ１にもＳ２が、正当な通信パートナーであることを確証するために、逆に（他の周期からの）データをＳ１に返送し得る。

【符号の説明】

【００５７】

１　ネットワークノード
２　測定トランスデューサ
３　ワイヤレスインタフェース
４　プロセッサユニット
５　データメモリ
６　データネットワーク
７　測定データ
８　送信機測定データマップ
８′　受信機測定データマップ
９　照合データ
１０　通信パートナー
１１　計測機器
１２　オートメーションシステム
１３　測定環境
１４　エンジンテストベンチ

１５　タイミング信号発生装置
１６　被検体
１７　ダイナモメータ
【図面】
【図１】

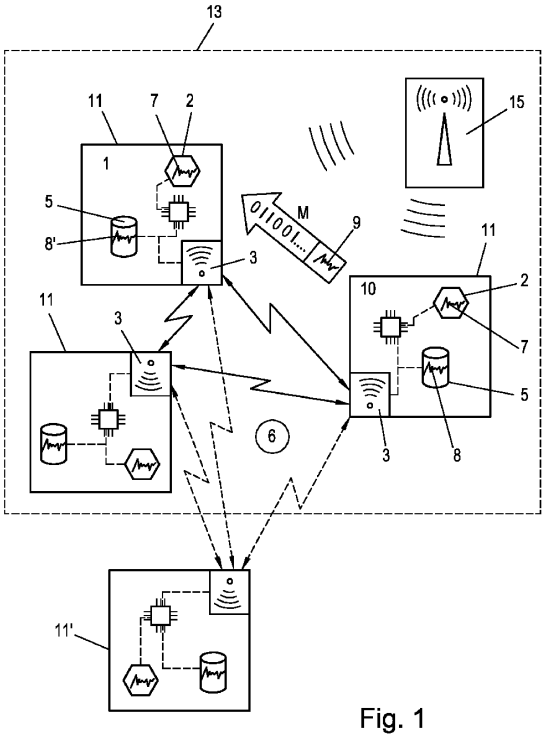

Fig. 1

【図２】

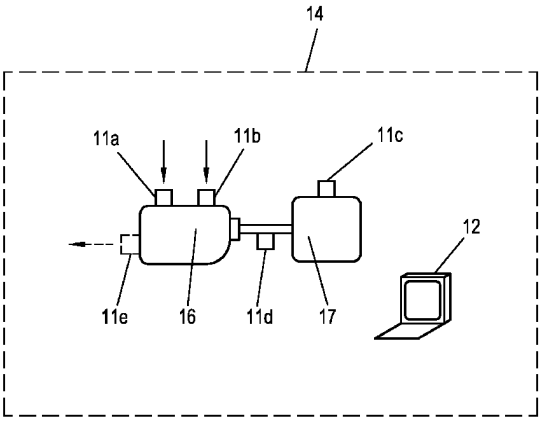

Fig. 2

【図３】

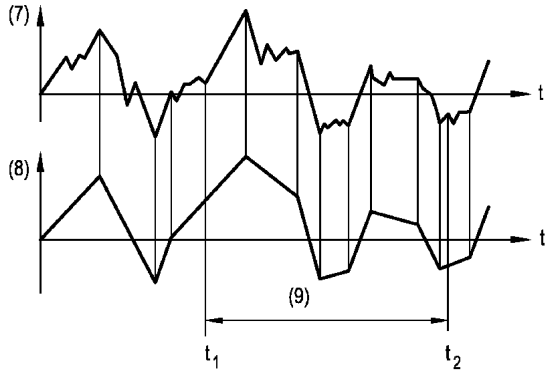

Fig. 3

【図４】

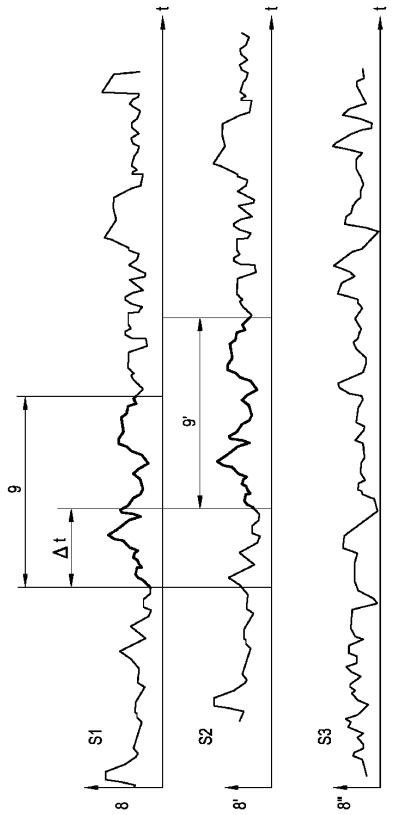

Fig. 4

フロントページの続き

(56)参考文献　　特表２００７－５１９３５５（ＪＰ，Ａ）
特開２０１４－１３８４０４（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　４／００ － ９９／００
Ｈ０４Ｂ　７／２４ －　７／２６