(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6009563号
(P6009563)
(45)発行日　平成28年10月19日(2016.10.19)　(24)登録日　平成28年9月23日(2016.9.23)

(51)Int.Cl.		F I		
H04L 29/06	(2006.01)	H04L	13/00	305B
H04L 12/66	(2006.01)	H04L	12/66	E
H04L 12/22	(2006.01)	H04L	12/22	

請求項の数 15　(全 25 頁)

(21)出願番号	特願2014-522190 (P2014-522190)
(86)(22)出願日	平成24年7月24日 (2012.7.24)
(65)公表番号	特表2014-527741 (P2014-527741A)
(43)公表日	平成26年10月16日 (2014.10.16)
(86)国際出願番号	PCT/IB2012/053759
(87)国際公開番号	WO2013/014609
(87)国際公開日	平成25年1月31日 (2013.1.31)
審査請求日	平成27年7月21日 (2015.7.21)
(31)優先権主張番号	61/511,166
(32)優先日	平成23年7月25日 (2011.7.25)
(33)優先権主張国	米国(US)
(31)優先権主張番号	61/635,490
(32)優先日	平成24年4月19日 (2012.4.19)
(33)優先権主張国	米国(US)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
KONINKLIJKE PHILIPS N.V.
オランダ国　5656　アーエー　アインドーフェン　ハイテック　キャンパス　5
High Tech Campus 5, NL-5656 AE Eindhoven
(74)代理人　110001690
特許業務法人M&Sパートナーズ

最終頁に続く

(54)【発明の名称】安全なエンドツーエンド接続を確立するための方法、デバイス、及びシステム、並びに、データパケットを安全に通信するための方法、デバイス、及びシステム

(57)【特許請求の範囲】
【請求項１】
第１デバイスと第２デバイスとの間でデータパケットを安全に通信するための通信システムであって、
第１伝送プロトコルに基づく第１ネットワークと、
前記第１ネットワークを介して他のデバイスと通信する第１デバイスであって、前記第１伝送プロトコル上に第１伝送セキュリティプロトコルを用いる第１デバイスと、
第２伝送プロトコルに基づく第２ネットワークと、
前記第２ネットワークを介して他のデバイスと通信する第２デバイスであって、前記第２伝送プロトコル上に第２伝送セキュリティプロトコルを用いる第２デバイスと、
前記第１デバイスと前記第１ネットワークを介して通信し、前記第２デバイスと前記第２ネットワークを介して通信し、前記第１伝送セキュリティプロトコルに従って生成された、前記第１ネットワークを介して受信されるデータパケットを、前記第２伝送セキュリティプロトコルに従う前記第２ネットワークを介する通信用のデータパケットに変更し、またその逆の変更を行う、中間デバイスとを含み、
前記第１伝送プロトコル及び前記第２伝送プロトコルの一方はデータグラム・ベース・ネットワーク・プロトコルであり、前記第１伝送プロトコル及び前記第２伝送プロトコルの他方は信頼できる接続指向伝送プロトコルであり、
前記第１デバイスは、前記中間デバイスから受信された第１データパケットのヘッダーであって、前記第２デバイスによって前記中間デバイスに通信され、前記中間デバイスに

よって前記第１データパケットに変更された第１データパケットのヘッダーを、第２データパケットのヘッダーに対応するよう再構成し、
前記第１デバイスは、前記第１データパケットの前記再構成されたヘッダーに基づき受信されたデータパケットのセキュリティ確認フィールドを確認し、前記確認フィールドは、前記第２デバイスによって前記第２伝送セキュリティプロトコルに従って生成される、通信システム。
【請求項２】
前記第１伝送セキュリティプロトコル及び前記第２伝送セキュリティプロトコルは、ハンドシェイクプロトコルを用いて安全な通信セッションを開始し、前記受信されたデータパケットは、前記ハンドシェイクプロトコルのデータパケットである、請求項１に記載の通信システム。
【請求項３】
前記受信されたデータパケットは、前記受信されたデータパケットの信頼性を認証するためのセキュリティ確認フィールドとしてメッセージ認証コードを含む、請求項１に記載の通信システム。
【請求項４】
前記第１デバイスは、まず前記第１伝送セキュリティプロトコルに従って前記セキュリティ確認フィールドを確認し、この確認が失敗の場合、前記第１データパケットのヘッダーが再構成され、前記セキュリティ確認フィールドが、前記第２伝送セキュリティプロトコルに従って、前記第１データパケットの前記再構成されたヘッダーに基づいて確認される、請求項１に記載の通信システム。
【請求項５】
第１デバイスと第２デバイスとの間でデータパケットを安全に通信するための通信システムであって、
第１伝送プロトコルに基づく第１ネットワークと、
前記第１ネットワークを介して他のデバイスと通信する第１デバイスであって、前記第１伝送プロトコル上に第１伝送セキュリティプロトコルを用いる第１デバイスと、
第２伝送プロトコルに基づく第２ネットワークと、
前記第２ネットワークを介して他のデバイスと通信する第２デバイスであって、前記第２伝送プロトコル上に第２伝送セキュリティプロトコルを用いる第２デバイスと、
前記第１ネットワークを介して前記第１デバイスと通信し、前記第２ネットワークを介して前記第２デバイスと通信し、前記第１伝送セキュリティプロトコルに従って生成された、前記第１ネットワークを介して受信されたデータパケットを、前記第２伝送セキュリティプロトコルに従う、前記第２ネットワークを介した通信用のデータパケットに変更し、またその逆の変更を行う、中間デバイスとを含み、
前記第１伝送プロトコル及び前記第２伝送プロトコルの一方は、データグラムベースネットワークプロトコルであり、前記第１伝送プロトコル及び前記第２伝送プロトコルの他方は、信頼できる接続指向伝送プロトコルであり、
前記第１デバイスは、前記中間デバイスから受信された第１データパケットのヘッダーであって、前記第２デバイスによって前記中間デバイスに通信され、前記中間デバイスによって前記第１データパケットに変更された第１データパケットのヘッダーを、第２データパケットのヘッダーに対応するよう再構成し、
前記第１デバイスは、送信される第３データパケットのためのセキュリティ確認フィールドを生成し、前記セキュリティ確認フィールドは前記第１データパケットの前記再構成されたヘッダーに基づき、前記第２伝送セキュリティプロトコルに従って生成される、通信システム。
【請求項６】
前記第１伝送セキュリティプロトコル及び前記第２伝送セキュリティプロトコルは、ハンドシェイクプロトコルを用いて安全な通信セッションを開始し、前記送信される予定の第３データパケットは、前記ハンドシェイクプロトコルのデータパケットである、請求項

５に記載の通信システム。
【請求項７】
前記第１デバイスは、前記第１伝送セキュリティプロトコルに従って生成されたセキュリティ確認フィールドを含む第４データパケットを送信し、また、前記第２伝送セキュリティプロトコルに従って生成された前記セキュリティ確認フィールドを含む前記第３データパケットを送信する、請求項５に記載の通信システム。
【請求項８】
前記第１デバイスは、前記第１デバイスが前記第２伝送セキュリティプロトコルを用いる他のデバイスと通信するか否かを検出し、前記第１デバイスが前記第２伝送セキュリティプロトコルを用いる他のデバイスと通信することを検出した場合、前記第１デバイスは、前記第２伝送セキュリティプロトコルに従って生成された前記セキュリティ確認フィールドを含む前記第３データパケットを送信する、請求項５に記載の通信システム。
【請求項９】
前記第１伝送プロトコルは、インターネット・プロトコル・ベース・ユーザ・データグラム・プロトコルであり、前記第２伝送プロトコルは、インターネット・プロトコル・ベース・トランスポート・コントロール・プロトコルであり、前記第１伝送セキュリティプロトコルは、データグラム・トランスポート・レイヤー・セキュリティ・プロトコルであり、前記第２伝送セキュリティプロトコルは、トランスポート・レイヤー・セキュリティ・プロトコルである、請求項１又は５に記載の通信システム。
【請求項１０】
前記第１デバイスは、ＣｏＡＰを使用し、前記第２デバイスは、ＨＴＴＰを使用する、請求項１又は５に記載の通信システム。
【請求項１１】
請求項１に記載の通信システム内で使用される第１デバイスであって、前記第１デバイスは、
他のデバイスと第１ネットワークを介して通信する第１ネットワークインターフェイスであって、前記第１ネットワークは第１伝送プロトコルに基づき、前記第１伝送プロトコルは、データグラム・ベース・ネットワーク・プロトコル又は信頼できる接続指向伝送プロトコルである、第１ネットワークインターフェイスと、
前記第１伝送プロトコル上に第１伝送セキュリティプロトコルを適用する第１セキュリティプロトコル適用手段と、
第２伝送セキュリティプロトコルがその上に適用される第２伝送プロトコルに基づく第２ネットワークを介して中間デバイスによって受信された第２データパケットのヘッダーに対応するよう、受信された第１データパケットのヘッダーを再構成する再構成ユニットであって、前記第１データパケットは、前記第１ネットワークを介して前記中間デバイスから受信される、再構成ユニットと、
前記第１データパケットの前記再構成されたヘッダーに基づいて、受信されたデータパケットのセキュリティ確認フィールドを確認する確認ユニットであって、前記確認フィールドは、前記第２伝送セキュリティプロトコルに従って生成される、確認ユニットとを有する、第１デバイス。
【請求項１２】
請求項５に記載の通信システム内で使用される第１デバイスであって、前記第１デバイスは、
他のデバイスと第１ネットワークを介して通信する第１ネットワークインターフェイスであって、前記第１ネットワークは、第１伝送プロトコルに基づき、前記第１伝送プロトコルは、データグラム・ベース・ネットワーク・プロトコル又は信頼できる接続指向伝送プロトコルである、第１ネットワークインターフェイスと、
前記第１伝送プロトコル上に第１伝送セキュリティプロトコルを適用する第１セキュリティプロトコル適用手段と、
第２伝送セキュリティプロトコルがその上に適用される第２伝送プロトコルに基づく第

２ネットワークを介して中間デバイスによって受信された第２データパケットのヘッダーに対応するよう、受信された第１データパケットのヘッダーを再構成する再構成ユニットであって、前記第１データパケットは、前記第１ネットワークを介して前記中間デバイスから受信される、再構成ユニットと、

送信される第３データパケットのためのセキュリティ確認フィールドを生成する生成ユニットであって、前記セキュリティ確認フィールドは、前記第１データパケットの前記再構成されたヘッダーに基づき、前記第２伝送セキュリティプロトコルに従って生成される、生成ユニットとを含む、第１デバイス。

【請求項１３】

請求項１乃至５のいずれか一項に記載の通信システム内で使用される中間デバイスであって、前記中間デバイスは、

第１伝送プロトコルに基づく第１ネットワークを介して第１デバイスと通信する第１ネットワークインターフェイスと、

第２伝送プロトコルに基づく第２ネットワークを介して第２デバイスと通信する第２ネットワークインターフェイスと、

前記第１伝送プロトコル上に第１伝送セキュリティプロトコルを適用する第１セキュリティ適用手段と、

前記第２伝送プロトコル上に第２伝送セキュリティプロトコルを適用する第２セキュリティ適用手段であって、前記第１及び第２伝送プロトコルの一方はデータグラム・ベース・ネットワーク・プロトコルであり、前記第１及び第２伝送プロトコルの他方は信頼できる接続指向伝送プロトコルである、第２セキュリティ適用手段と、

前記第１ネットワークを介して受信され、前記第１伝送セキュリティプロトコルに従って生成されたデータパケットを、前記第２伝送セキュリティプロトコルに従う前記第２ネットワークを介した通信用のデータパケットに変更し、またその逆の変更を行う変更ユニットとを含む、中間デバイス。

【請求項１４】

第１デバイスと第２デバイスとの間でデータパケットを安全に通信する方法であって、

第２伝送プロトコルに基づく第２ネットワークを介して、前記第２デバイスより送信された第２データパケットを、中間デバイスが受信するステップであって、前記第２伝送プロトコル上に第２伝送セキュリティプロトコルが用いられる、受信ステップと、

前記中間デバイスが、前記第２データパケットを、第１伝送プロトコルに基づく第１ネットワークを介して送信される第１データパケットに変更するステップであって、前記第１伝送プロトコル上に第１伝送セキュリティプロトコルが用いられ、前記第１伝送プロトコル及び前記第２伝送プロトコルの一方はデータグラムベースネットワークプロトコルであり、前記第１伝送プロトコル及び前記第２伝送プロトコルの他方は信頼できる接続指向伝送プロトコルである、変更ステップと、

前記中間デバイスが、前記第１ネットワークを介して前記第１データパケットを送信するステップと、

前記第１デバイスが、前記第１データパケットを受信するステップと、

前記第１デバイスが、前記第２データパケットのヘッダーに対応するように、前記中間デバイスから受信された前記第１データパケットのヘッダーを再構成するステップと、

前記第１デバイスが、前記第１データパケットの前記再構成されたヘッダーに基づいて、受信されたデータパケットのセキュリティ確認フィールドを確認するステップであって、前記確認フィールドは、前記第２伝送セキュリティプロトコルに従って生成される、方法。

【請求項１５】

第１デバイスと第２デバイスとの間で安全にデータパケットを通信する方法であって、

第２伝送プロトコルに基づく第２ネットワークを介して、前記第２デバイスより送信された第２データパケットを、中間デバイスが受信するステップであって、前記第２伝送プロトコル上に第２伝送セキュリティプロトコルが用いられる、受信ステップと、

前記中間デバイスが、前記第２データパケットを、第１伝送プロトコルに基づく第１ネットワークを介して送信される第１データパケットに変更するステップであって、前記第１伝送プロトコル上に第１伝送セキュリティプロトコルが用いられ、前記第１伝送プロトコル及び前記第２伝送プロトコルの一方はデータグラム・ベース・ネットワーク・プロトコルであり、前記第１伝送プロトコル及び前記第２伝送プロトコルの他方は信頼できる接続指向伝送プロトコルである、変更ステップと、
前記中間デバイスが、前記第１ネットワークを介して前記第１データパケットを送信するステップと、
前記第１デバイスが、前記第１データパケットを受信するステップと、
前記第１デバイスが、前記第２データパケットのヘッダーに対応するよう、前記中間デバイスから受信された前記第１データパケットのヘッダーを再構成するステップと、
前記第１デバイスが、第３データパケットのためのセキュリティ確認フィールドを生成するステップであって、前記セキュリティ確認フィールドは前記第１データパケットの前記再構成されたヘッダーに基づき、前記第２伝送セキュリティプロトコルに従って生成される生成ステップと、
前記第１デバイスが、前記第１ネットワークを介して前記第３データパケットを送信する、方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、複数のセキュリティプロトコル、例えばトランスポート・レイヤー・セキュリティ（ＴＬＳ）プロトコル及びデータグラム・トランスポート・レイヤー・セキュリティ（ＤＴＬＳ）プロトコル等が用いられている状況において、安全なエンドツーエンド接続を確立するための方法、デバイス、及びシステムに関する。

【背景技術】

【０００２】

モノのインターネット（ＩｏＴ）は、例えばヒトからヒト（Ｈ２Ｈ）、ヒトからモノ（Ｈ２Ｔ）、モノからモノ（Ｔ２Ｔ）、又はモノから複数のモノ（Ｔ２Ｔｓ）等、多数の通信パターンに従う高度に多様化されたネットワークエンティティ及びネットワークの相互接続を表す。ＩｏＴという用語は、１９９９年、Ａｕｔｏ－ＩＤセンターによって初めて用いられた。それ以降、ＩｏＴの基礎的な概念の発展は常にそのペースを速めてきた。今日、ＩｏＴは熱心に研究されており、様々なイニシアチブによってＩｏＴにおける（再）設計、アプリケーション、及び標準インターネット技術の使用に関する取り組みがなされている。

【０００３】

ＩｏＴアプリケーションの基本的な構成ブロックとしてのＩＰｖ６の導入は、（１）インターネットホストとの簡単な統合を可能にする均質なプロトコルエコシステム、（２）大きく異なる装置の単純化された展開、（３）アプリケーションレベルプロキシを不要にする、アプリケーション用の統合化されたインターフェイス、を含む、多数の基礎的なメリットの提供を約束する。このような特徴は、ビルオートメーションから製造環境、パーソナルエリアネットワーク（ＰＡＮ）まで、温度センサ、照明、又はＲＦＩＤタグ等大きく異なるモノが、互いに、又はスマートフォンを持っている人若しくはバックエンドサービスと相互作用し得る、想定されるシナリオの展開を大いに簡易化する。

【０００４】

この環境において、多数のＩＥＴＦワーキンググループがスマートなモノの資源制約形ネットワークのための新しいプロトコルを設計している。６ＬｏＷＰＡＮワーキンググループは、ＩＰｖ６パケットのＩＥＥＥ　８０２．１５．４ネットワークにおける効率的な通信及び適合のための方法及びプロトコルの定義に力を注いでいる。ＣｏＲＥワーキンググループは、制約形ＩＰネットワーク（６ＬｏＷＰＡＮ）上で動作するリソース指向アプリケーションのフレームワークを提供する。その主要なタスクの１つは、ＵＤＰ上で動作

し、モノの効率的なアプリケーションレベル通信を可能にするＨＴＴＰプロトコルの軽量版、ＣｏＡＰの定義である。

【０００５】

これらの新しいプロトコルは、ビルオートメーション制御（ＢＡＣ）、健康モニタリング、Ｓｍａｒｔ　Ｅｎｅｒｇｙ等を含む多様なアプリケーションを実行可能にするであろう。この環境において、６ＬｏＷＰＡＮ／ＣｏＡＰネットワークを構成するエンドデバイス（アクチュエータ又はセンサ等）は、リアルタイムモニタリング又は物理的パラメータ及び機器の制御のために用いられる。ＢＡＣの場合、アクチュエータは照明器具及びセンサ（光センサ）でもよく、照明器具は、自身の照明設定を調整する照明センサのリソースにアクセスし得る。他のシナリオにおいては、バックエンドに位置する、すなわち、６ＬｏＷＰＡＮ／ＣｏＡＰネットワークの外側に位置するＣｏＡＰデバイス（例えばクライアント）が、インターネットを６ＬｏＷＰＡＮ／ＣｏＡＰネットワークと相互接続する６ＬｏＷＰＡＮボーダールーター（６ＬＢＲ）を介して６ＬｏＷＰＡＮ／ＣｏＡＰネットワーク内のデバイス（例えばＣｏＡＰサーバ）のリソースにアクセスする。このようなアクセスは、バックエンドから６ＬｏＷＰＡＮ／ＣｏＡＰネットワーク内のＣｏＡＰデバイスが特定のリソースを取得するために、又は、ＣｏＡＰデバイスに特定の構成をプッシュするために要求され得る。

【０００６】

セキュリティは、上記の応用領域及びユースケースにとって鍵となる要素である。セキュリティの具体的な目標は、２つのデバイス間の機密性、認証、又は鮮度等、基礎的なセキュリティサービスを提供することである。対称キー暗号法を用いる場合、このデバイスのペアは、相互認証及び秘密セッションキー導出のための共通のハンドシェイク中に用いられる、共通マスターキーを共有する。このセッションキーは、ｃｉｐｈｅｒ　ｓｕｉｔｅ（暗号スイート）とともに用いられ、両デバイス間の情報の交換において上記セキュリティサービスを提供する。非対称キー暗号法によっても同様なハンドシェイクを実行することができる。

【０００７】

ＩＰプロトコルの場合、ＴＬＳ又はＤＴＬＳを含む異なるセキュリティプロトコルが存在する。ＴＬＳは、トランスミッション・コントロール・プロトコル（ＴＣＰ）上で動作するアプリケーション層のプロトコルを保護するために用いられる。ＤＴＬＳは、ＵＤＰ上で動作するアプリケーションを保護するために用いられる、ＴＬＳの拡張である。ほとんどの搭載ベースサーバはＣｏＡＰではなく、例えば、ＴＣＰ及びＴＬＳと組み合わせて用いられるハイパーテキスト・トランスファー・プロトコル（ＨＴＴＰ）を用いるが、ＣｏＡＰは、ＣｏＡＰ通信の交換を保護するための必須のアプローチとしてＤＴＬＳを特定する。

【０００８】

上記環境において、安全なエンドツーエンド接続の提供は挑戦（チャレンジ）である。その理由の１つは、６ＬｏＷＰＡＮボーダールーター又はプロキシ（６ＬＢＲ）が、２つのデバイス間で交換されるリクエストが６ＬｏＷＰＡＮ／ＣｏＡＰネットワークの内部に位置するか外部に位置するかを検証可能でなければならないことである。これは、例えば公益事業会社のＣｏＡＰクライアントがＣｏＡＰサーバ（例えばスマートメーター）にリクエストを送る際に起こる。６ＬＢＲは、例えばエネルギー枯渇攻撃を防ぐ（又はその影響を抑える）ために、クライアントからのリクエストが有効であることを検証可能でなければならない。他の非常に興味深い状況は、例えば、６ＬｏＷＰＡＮ／ＣｏＡＰネットワーク内のエンドデバイス内の情報にアクセス可能であるべきバックエンド内のレガシーデバイス、例えばＨＴＴＰデバイスが存在する状況である。この状況において、例えばバックエンド内のＨＴＴＰクライアントと６ＬｏＷＰＡＮ／ＣｏＡＰネットワーク内のＣｏＡＰサーバとの間の安全なエンドツーエンド接続を確立することは、現在もなお挑戦である。なぜなら、使用されるキー交換機構が異なる、すなわち、レガシーシステム内ではＴＬＳ（ＴＣＰベース）が用いられる一方、制約形６ＬＯＷＰＡＮネットワークはＤＴＬＳ（

ＵＤＰベース）しかサポートしないからである。これは、６ＬｏＷＰＡＮ／ＣｏＡＰ内のＣｏＡＰデバイスはキー確立リクエストがどこから来ているのか知らないため、さらに複雑である。

【０００９】

いくつかの状況、例えばソフトウェア更新、ネットワークアドミッション、ビリング（支払い）等においては、エンドツーエンド接続は必須である。インターネット上での安全な接続のためには、レガシーシステムはＴＣＰ及びＴＬＳ上ではＨＴＴＰしかサポートしない。したがって、ここで議論される特定の状況は次のように表される。インターネット上のＨＴＴＰデバイスはＣｏＡＰデバイスからのリソースに直接アクセスするためにＨＴＴＰを用いる。プロトコル変換は、両者間に存在するＨＴＴＰ／ＣｏＡＰプロキシによって行われる。この状況における目標は、ＨＴＴＰデバイスがＴＬＳを用いて安全なエンドツーエンド通信を有し得ること、及びＣｏＡＰデバイスがＤＴＬＳを用いて安全なエンドツーエンド通信をセットアップし得ることを保証することである。

【００１０】

ＴＣＰは、信頼性の高い通信を提供する接続指向プロトコルである。しかし、ＵＤＰは接続指向でなく、パケット送信を保証しない。上述したように、ＤＴＬＳはＵＤＰの制限を超えてＵＤＰ上で動作するためのＴＬＳの拡張である。どちらの場合においても、ＴＬＳとＤＴＬＳとの最初のハンドシェイクはクライアントとサーバとの間の４セットのメッセージの交換を含む。以下において、最小のハンドシェイクについて議論する。各ステップは、第１デバイス（例えばクライアント）から第２デバイス（例えばサーバ）への複数のメッセージの送信に言及することに留意されたい。

ステップ１（クライアントからサーバへ）：Ｃｌｉｅｎｔ　Ｈｅｌｌｏ

ステップ２（サーバからクライアントへ）：Ｓｅｒｖｅｒ　Ｈｅｌｌｏ；ＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅ

ステップ３（クライアントからサーバへ）：ＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅ；ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃ；Ｆｉｎｉｓｈｅｄ

ステップ４（サーバからクライアントへ）：ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃ，Ｆｉｎｉｓｈｅｄ

【００１１】

ＤＴＬＳは、ＴＬＳに基づき、上記メッセージは同じままであるが、プロトコルを互いに相互運用不可能にする小さな違いが存在する。違いのうちのいくつかは、以下の通りである。

－　リクエストを発するクライアントの存在を確認するために、ＤＴＬＳ内でクッキー機構を用いることができる。ＴＬＳにおいては、ＴＣＰ３方向ハンドシェイクがクライアントの存在を決定するため、このようなクッキー機構は必要ない。

－　ＤＴＬＳは、ＵＤＰ上でＤＴＬＳを動作させるために必要な信頼性を提供するために追加のフィールドを包含する。ＴＬＳにおいては、基礎をなすＴＣＰ層が必要な信頼性を提供するため、それらのフィールドは必要ない。

－　ＤＴＬＳは、第１デバイスによって送信されたメッセージが第２デバイスによって受信されることを保証するために最初のハンドシェイク中は再送信機構に頼る。ＴＬＳは、信頼性の高い送信がＴＣＰによって保証されるため、このようなアプローチを必要としない。

【発明の概要】

【発明が解決しようとする課題】

【００１２】

したがって、本発明の目的は、制約ネットワークの一部を構成する制約デバイスが、ＣｏＡＰを動作しない他のデバイスと安全なエンドツーエンド接続を確立するために必要な論理を提供することである。非制約デバイスを変更して安全なエンドツーエンド接続を確立することは好ましくなく、また、既存のセキュリティプロトコルを変更することは好ましくない。また、制約デバイス内に大きなオーバーヘッドをつくることは好ましくない。

【課題を解決するための手段】
【００１３】
本発明の第１の側面は、第１デバイスと第２デバイスとの間で安全にデータパケットを通信するための２つの通信システムを提供する。本発明の第２の側面は、本発明の第１の側面の通信システムで用いるための２つのデバイスを提供する。本発明の第３の側面は、本発明の第１の側面の通信システム内で用いるための中間デバイスを提供する。本発明の第４の側面は、第１デバイスと第２デバイスとの間で安全にデータパケットを通信する２つの方法を提供する。好適な実施形態は、従属請求項において定義される。
【００１４】
本発明の第１の側面に係る通信システムは、第１デバイスと第２デバイスとの間で安全にデータパケットを通信するためのものである。通信システムは、第１ネットワーク、第１デバイス、第２ネットワーク、第２デバイス、及び中間デバイスを有する。第１ネットワークは、第１伝送プロトコルに基づく。第１デバイスは第１ネットワークを介して他のデバイスと通信し、第１伝送プロトコル上に第１伝送セキュリティプロトコルを用いる。第２ネットワークは、第２伝送プロトコルに基づく。第１伝送プロトコル及び第２伝送プロトコルの一方は、データグラムベースネットワークプロトコルであり、第１伝送プロトコル及び第２伝送プロトコルの他方は、信頼性の高い接続指向伝送プロトコルである。第２デバイスは、他のデバイスと第２ネットワークを介して通信し、第２伝送プロトコル上に第２伝送セキュリティプロトコルを使用する。中間デバイスは、第１デバイスと第１ネットワークを介して通信し、第２デバイスと第２ネットワークを介して通信する。中間デバイスは、第１ネットワークを介して受信され、第１伝送セキュリティプロトコルに従って生成されたデータパケットを、第２伝送セキュリティプロトコルに従う第２ネットワークを介した通信用のデータパケットに変更し、またその逆の変更も行う。したがって、第２ネットワークを介して受信されたデータパケットも、第１ネットワークを介した通信に適したパケットに変更される。第１デバイスは、第２デバイスによって中間デバイスに通信され、中間デバイスによって第１データパケットに変更された第２データパケットのヘッダーに対応するように、中間デバイスから受信された第１データパケットのヘッダーを再構成する。第１デバイスは、第１データパケットの再構成されたヘッダーに基づき、受信されたデータパケットのセキュリティ確認フィールドを確認する。確認フィールドは、第２デバイスによって第２伝送セキュリティプロトコルに従って生成される。受信されたデータパケット（セキュリティ確認フィールドが確認されたデータパケット）は、ヘッダーが再構成された最初のデータパケットであるか、後に受信された他のデータパケットであり得る。
【００１５】
本発明の解決策は、システム内で用いられる２つの手段に関する。中間デバイスは、第１ネットワーク上で用いられるフォーマットから第２ネットワーク上で用いられるフォーマットにデータバケットを変更する。多くの場合、これはパケットのヘッダーの変更を含み、第１伝送セキュリティプロトコル及び／又は第２伝送セキュリティプロトコルの情報に関する変更を含む。中間デバイスが第１ネットワーク上で用いられるフォーマットから第２ネットワーク上で用いられるフォーマットにデータパケットを変更する一方、ほとんどの場合、データパケットペイロードは変更されないことに留意されたい。続いて、第１デバイスは、第２ネットワークを介して中間デバイスによって受信された元々のヘッダーを再構成することができる（したがって、ヘッダーが第１ネットワーク上での通信に適したフォーマットに変更される前に中間デバイスによって受信されたヘッダー）。続いて、第１デバイスは、再構成されたヘッダーに基づいて、受信されたデータパケットの確認フィールドを確認することができる。受信された確認フィールドは、第２伝送セキュリティプロトコルに基づいて第２デバイスによって生成される。多くの場合、確認フィールドの生成は、入力として１つ以上のデータパケットヘッダー及び／又はデータパケットペイロードを用いる（ハッシュ）関数の使用を含む。したがって、確認フィールドを生成するために用いられたヘッダーは、確認フィールドの確認のための確認デバイスにおいて利用可

能でなければならない。ヘッダーの再構成は、これらのヘッダーの利用可能性を保証する。

【００１６】

いくつかの伝送セキュリティプロトコルにおいては、エンドツーエンド接続は、デバイスのうちの少なくとも１つが確認フィールドを確認できる場合にのみ確立される。したがって、第１伝送セキュリティプロトコルと第２伝送セキュリティプロトコルとの間の違いが解消されるため、本発明は、安全なエンドツーエンド接続の確立を可能にする。いくつかの伝送セキュリティプロトコルにおいては、一度セキュリティ接続が確立されると、確認フィールドは受信されたデータパケットの信頼性を確認するためにそのまま用いられ、本発明はそのための手段を提供する。

【００１７】

本発明の第１の側面によれば、第２デバイスでは変更は要求されない。また、中間デバイスは第１伝送セキュリティプロトコルから第２伝送セキュリティプロトコルにいくらかの変換を行わなければならないが、中間デバイスは、安全なエンドツーエンド接続の確立に能動的に関わらず、情報の確認に能動的に関わらない。これは、エンドデバイスがプライベートな事前共有キーを有する伝送セキュリティプロトコルにおいて、中間デバイスが伝送セキュリティプロトコルの実行に能動的に関わらないため、中間デバイスがこのキーの知識を有さないことを意味する。

【００１８】

セキュリティ確認フィールドの確認は、データパケットの再構成されたヘッダーに基づいて実行されることに留意されたい。「基づいて」とは、データパケットの再構成されたヘッダーに基づく確認に限定されるのではなく、確認は、データパケットのペイロード等他のデータも考慮し得ることを意味する。

【００１９】

オプションで、第１伝送セキュリティプロトコル及び第２伝送セキュリティプロトコルは、ハンドシェイクプロトコルを用いて安全な通信セッションを開始する。確認フィールドを含む受信されたデータパケットは、ハンドシェイクプロトコルのデータパケットである。したがって、ハンドシェイクプロトコルは、確認フィールドを含むデータパケットの交換を規定する。本発明は、確認フィールドの確認を可能にし、したがって、ハンドシェイクプロトコルの実行を可能にする。多くの場合、トランスポート・レイヤー・セキュリティ（ＴＬＳ）又はデータグラム・トランスポート・レイヤー・セキュリティ（ＤＴＬＳ）等においてのように、ハンドシェイクの最後には終了メッセージを送信しなければならず、ハンドシェイクは、ハンドシェイク中に送信されるパケットヘッダー及びペイロードに基づく確認コードを含む。このような場合、本発明によれば、パケットヘッダーは第１デバイスで再構成されることができ、終了メッセージは、第２デバイスによって用いられるプロトコルによって適宜確認できる。

【００２０】

オプションで、受信されたパケットは、受信されたデータパケットの信頼性を認証するためのセキュリティ確認フィールドとして、メッセージ認証コードを有する。いくつかの伝送セキュリティプロトコルにおいて、メッセージの信頼性を確認可能にするためには、確立された安全なエンドツーエンド接続上で通信されるメッセージにはメッセージ認証コードの使用が必須である。メッセージ認証コードは、多くの場合、データパケットの送信時におけるデータパケットのヘッダー及びペイロードに基づく。本発明のシステムのように、データパケットが、中間デバイスによって他の伝送セキュリティプロトコルを有する他のネットワークに沿う送信用に変更される場合、データパケットのヘッダーのコンテンツは変更される可能性があり、したがって、メッセージ認証コードを確認するためには再構成されなければならない。

【００２１】

オプションで、第１デバイスは、まず第１伝送セキュリティプロトコルに従ってセキュリティ確認コードを確認し、この確認が失敗の場合、第１データパケットのヘッダーは再

構成され、セキュリティ確認フィールドは、第２伝送セキュリティプロトコルに従って、第１データパケットの再構成されたヘッダーに基づいて確認される。したがって、第１デバイスは試行錯誤法を適用するよう構成される。第１デバイスは、第１伝送セキュリティプロトコルに基づく確認コードを予期し、したがって、最初はこの予期に従って確認を試みる。成功の場合、確認コードは、明らかに同様に第１伝送セキュリティプロトコルを用いるデバイスから受信された。失敗の場合、ヘッダーが再構成され、ヘッダーの再構成後の第２伝送セキュリティプロトコルに従う確認が成功の場合、データパケットは第２伝送セキュリティプロトコルを用いるデバイスによって元々送信された。したがって、第１デバイスは最初は他方のデバイスに関する知識を有する必要がない。第１デバイスは、どの伝送セキュリティプロトコルが用いられているのかを突き止めることができる。このオプションの実施形態によれば、確認後、第１デバイスは、特定のデバイスから受信されたデータパケットは特定の伝送セキュリティプロトコルに従って送信されるという知識も有する。この知識は、将来の確認コードの確認の試みにおいて、不要な「試行錯誤」ステップを防ぐために用いることができる。

【００２２】

本発明の第１の側面によれば、第１デバイスと第２デバイスとの間でデータパケットを安全に通信するための他の通信システムが提供される。通信システムは第１ネットワーク、第１デバイス、第２ネットワーク、第２デバイス、及び中間デバイスを有する。第１ネットワークは、第１伝送プロトコルに基づく。第１デバイスは、第１ネットワークを介して他のデバイスと通信し、第１伝送プロトコル上に第１伝送セキュリティプロトコルを用いる。第２ネットワークは第２伝送プロトコルに基づく。第１伝送プロトコル及び第２伝送プロトコルの一方はデータグラムベースネットワークプロトコルであり、第１伝送プロトコル及び第２伝送プロトコルの他方は信頼できる接続指向伝送プロトコルである。第２デバイスは、第２ネットワークを介して他のデバイスと通信し、第２伝送プロトコル上に第２伝送セキュリティプロトコルを用いる。中間デバイスは、第１ネットワークを介して第１デバイスと通信し、第２ネットワークを介して第２デバイスと通信する。中間デバイスは、第１ネットワークを介して受信され、第１伝送セキュリティプロトコルに従って生成されたデータパケットを、第２伝送セキュリティプロトコルに従う第２伝送ネットワークを介する通信用のデータパケットに変更し、またその逆の変更を行う。したがって、第２ネットワークを介して受信されたデータパケットは、第１ネットワークを介する通信に適したパケットに変更される。第１デバイスは、第２デバイスによって中間デバイスに通信され、中間デバイスによって第１データパケットに変更された第２データパケットのヘッダーに対応するよう、中間デバイスから受信された第１データパケットのヘッダーを再構成する。第１デバイスは、送信される第３データパケットのためのセキュリティ確認フィールドを生成する。セキュリティ確認フィールドは、第１データパケットの再構成されたヘッダーに基づいて生成され、第２伝送セキュリティプロトコルに従って生成される。

【００２３】

本発明の第１の側面に係るこの他の通信システムは、前述の通信システムに強く関わる。前述の通信システムは、第１デバイスが、本発明の第２の側面に従って生成される確認フィールドを確認できると定め、この他の通信システムは、第１デバイスが、本発明の第２の側面に従って確認フィールドを生成できると定める。したがって、本発明の第１の側面に係るシステムのうちの一方においては、第１デバイスはクライアントで、第２デバイスはサーバであるが、他方のシステムでは役割は逆転される。したがって、言い換えれば、本発明の両方の側面が単一のシステムに組み合わせられれば、第１デバイスがいかなる役割（クライアント／サーバ）を担う場合においても、第１デバイスは第２伝送セキュリティプロトコルを使用する第２デバイスと完全に安全に通信可能である。

【００２４】

オプションで、第１伝送セキュリティプロトコル及び第２伝送セキュリティプロトコルは、ハンドシェイクプロトコルを用いて安全な通信セッションを開始する。送信される第３データパケットは、ハンドシェイクプロトコルである。他のオプションの実施形態に関

連して述べたように、ハンドシェイクプロトコルは、多くの場合、データパケットの１つ以上のヘッダー及びペイロードに基づく確認コードを含む終了（Ｆｉｎｉｓｈｅｄ）メッセージを有する。このオプションの実施形態は、第１デバイスに、第２伝送セキュリティプロトコルに従う確認コードを有するような終了メッセージを生成する能力を与える。したがって、第２デバイスは、このような終了メッセージを第１伝送セキュリティプロトコルに関する知識を有さずとも確認できる。

【００２５】

オプションで、第１デバイスは第１伝送セキュリティプロトコルに従って生成されたセキュリティ確認フィールドを含む第４データパケットを送信し、そして、第２伝送セキュリティプロトコルに従って生成されたセキュリティフィールドを含む第３データパケットを送信する。したがって、第１デバイスは、一方のデータパケットは第１伝送セキュリティプロトコルに基づく確認コードを含み、他方のデータパケットは第２伝送セキュリティプロトコルに基づく確認コードを含む２つの異なるデータパケットを送信することによって、「試行錯誤法」を適用する。オプションの実践的な実施形態においては、第１伝送セキュリティプロトコルに従う確認コードを有する第４パケットがまず送信され、安全な通信のポジティブな継続が検出されない場合、第２伝送セキュリティプロトコルに従う確認コードを有する第３パケットが続いて送信される。安全な通信の非ポジティブな継続は、他方のデバイスがおそらく第１伝送セキュリティプロトコルの確認フィールドを理解できないことを意味し、したがって、おそらく第２伝送セキュリティプロトコルの確認フィールドを理解できることを意味する。

【００２６】

オプションで、第１デバイスは、第２伝送セキュリティプロトコルを使用する他のデバイスと通信するか否かを検出する。第１デバイスは、第２伝送セキュリティプロトコルを使用する他のデバイスと通信すると検出された場合、第２伝送セキュリティプロトコルに従って生成されたセキュリティフィールドを含む第３データパケットを送信するよう構成される。他のデバイスに関する知識は、第１デバイスが他のデバイスによって理解できる伝送セキュリティプロトコルに従う確認コードを含むデータパケットを直ちに送信することを可能にする。これは効率性を向上させる。他のデバイスが第１伝送セキュリティプロトコル又は第２伝送セキュリティプロトコルを用いるかの検出は、２つのオプションの実施形態に関連して前述したように、生成された又は受信された確認フィールドの試行錯誤送信及び／又は確認に基づき得る。

【００２７】

オプションで、第１ネットワーク伝送通信プロトコルはインターネットプロトコル・ベース・ユーザ・データグラム・プロトコルであり、第２ネットワーク伝送通信プロトコルはインターネット・プロトコル・ベース・トランスポート・コントロール・プロトコルであり、第１伝送セキュリティプロトコルはデータグラム・トランスポート・レイヤー・セキュリティ・プロトコルであり、そして第２伝送セキュリティプロトコルはトランスポート・レイヤー・セキュリティ・プロトコルである。特に、第１ネットワークにおけるデータグラム・トランスポート・レイヤー・セキュリティ（ＤＴＬＳ）プロトコル、及び第２ネットワークにおけるトランスポート・レイヤー・セキュリティ（ＴＬＳ）の使用の組み合わせは好適である。なぜなら、ＤＴＬＳに従って送信されるデータパケットのヘッダーは、ＴＬＳに従って送信されるデータパケットと比べて少数の追加フィールドしか有さないからである。したがって、中間デバイスは、パケットが第２ネットワークから受信された場合は追加フィールドを生成することのみが必要があり、パケットが第１ネットワークから受信された場合は追加フィールドを削除することのみが必要である。特に、追加フィールドの生成は、第１デバイスによって容易に逆転できる動作であり、したがって、第１デバイスによるヘッダーの再構成は、第２ネットワーク、第２伝送プロトコル、第２伝送セキュリティプロトコル、又は第２デバイスに関する知識をあまり要さない比較的簡単な動作である。

【００２８】

オプションで、第１デバイスはＣｏＡＰを使用できるように構成されており、第２デバイスはＨＴＴＰを使用できるように構成されている。

【００２９】

本発明の第３の側面によれば、本発明の第１の側面に係る通信システムで使用される第１デバイスが提供される。第１デバイスは、第１ネットワークインターフェイス、第１セキュリティプロトコル適用手段、再構成ユニット、及び確認ユニットを有する。第１ネットワークインターフェイスは、他のデバイスと第１ネットワークを介して通信する。第１ネットワークは、データグラムベースネットワークプロトコル又は信頼できる接続指向伝送プロトコルである第１伝送プロトコルに基づく。第１セキュリティプロトコル適用手段は、第１伝送プロトコル上に第１伝送セキュリティプロトコルを適用する。再構成ユニットは、中間デバイスによって、第２伝送セキュリティプロトコルがその上に適用される第２伝送プロトコルに基づく第２ネットワークを介して受信された第２データパケットのヘッダーに対応するよう、受信された第１データパケットのヘッダーを再構成する。第１データパケットは、第１ネットワークを介して中間デバイスから受信される。確認ユニットは、第１データパケットの再構成されたヘッダーに基づいて、受信されたデータパケットのセキュリティ確認フィールドを確認する。確認フィールドは、第２伝送セキュリティプロトコルに従って生成される。

【００３０】

本発明の第３の側面によれば、本発明の第１の側面に係る通信システムで使用される他の第１デバイスが提供される。第１デバイスは、第１ネットワークインターフェイス、第１セキュリティプロトコル適用手段、再構成ユニット、及び生成ユニットを有する。第１ネットワークインターフェイスは、他のデバイスと第１ネットワークを介して通信する。第１ネットワークは、データグラムベースネットワークプロトコル又は信頼できる接続指向伝送プロトコルである第１伝送プロトコルに基づく。第１セキュリティプロトコル適用手段は、第１伝送プロトコル上に第１伝送セキュリティプロトコルを適用する。再構成ユニットは、中間デバイスによって、その上に第２伝送セキュリティプロトコルが用いられる第２伝送プロトコルに基づく第２ネットワークを介して受信された第２データパケットのヘッダーに対応するよう、受信された第１データパケットのヘッダーを再構成する。第１データパケットは中間デバイスから第１ネットワークを介して受信される。生成ユニットは、送信される第３データパケットのためのセキュリティ確認フィールドを生成するよう構成される。セキュリティ確認フィールドは、第１データパケットの再構成されたヘッダーに基づいて、第２伝送セキュリティプロトコルに従って生成される。

【００３１】

本発明の第２の側面に係る第１デバイスは、本発明の第１の側面に係るシステムと同じ利益を提供し、当該システムの対応する実施形態と同様な効果を有する同様な実施形態を有する。

【００３２】

本発明の第３の側面によれば、本発明の第２の側面に係る通信システムのうちの１つに適用される中間デバイスが提供される。中間デバイスは、第１ネットワークインターフェイス、第２ネットワークインターフェイス、第１セキュリティ適用手段、第２セキュリティ提供手段、及び変更ユニットを有する。第１ネットワークインターフェイスは、第１デバイスと第１ネットワークを介して通信する。第１ネットワークは、第１伝送プロトコルに基づく。第２ネットワークインターフェイスは、第２デバイスと第２ネットワークを介して通信する。第２ネットワークは、第２伝送プロトコルに基づく。第１及び第２ネットワークプロトコルのうちの１つはデータグラムベースネットワークプロトコルであり、第１及び第２ネットワークのうちの他方は信頼できる接続指向伝送プロトコルである。第１セキュリティ適用手段は、第１伝送プロトコル上に第１伝送セキュリティプロトコルを適用する。第２セキュリティ適用手段は、第２伝送セキュリティプロトコルを第２伝送プロトコル上に適用する。変更ユニットは、第１ネットワークを介して受信され、第１伝送セキュリティプロトコルに従って生成されたデータパケットを、第２伝送セキュリティプロ

トコルに従う第２ネットワークを介した通信用のデータパケットに変更し、またその逆の変更も行う。

【００３３】

本発明の第３の側面に係る中間デバイスは、本発明の第１の側面に係るシステムと同じ利益を提供し、当該システムの対応する実施形態と同様な効果を有する同様な実施形態を有する。

【００３４】

本発明の第４の側面によれば、第１デバイスと第２デバイスとの間で安全にデータパケットを通信する方法が提供される。方法は、１）第１伝送プロトコルに基づく第１ネットワークを介して第１データパケットを受信するステップであって、第１伝送セキュリティプロトコルは第１伝送プロトコル上で用いられる受信ステップと、２）第１データパケットを、第２伝送プロトコルに基づく第２ネットワークを介して送信されるべき第２データパケットに変更するステップであって、第２伝送セキュリティプロトコルは第２伝送プロトコル上で用いられ、第１伝送プロトコル及び第２伝送プロトコルのうちの一方はデータグラムベースネットワークプロトコルであり、第１伝送プロトコル及び第２伝送プロトコルのうちの他方は信頼できる接続指向伝送プロトコルである、変更するステップと、３）第２ネットワークを介して第２データパケットを送信するステップと、４）第２データパケットを受信するステップと、５）ヘッダーが第１パケットのヘッダーに対応するように中間デバイスから受信された第２データパケットのヘッダーを再構成するステップと、６）第１データパケットの再構成されたヘッダーに基づいて第２データパケット又は第３データパケットのセキュリティ確認フィールドを確認するステップであって、確認フィールドは第１伝送セキュリティプロトコルに従って生成される確認ステップとを含む。確認フィールドを含む受信されたデータパケットは、受信された第２データパケット又は第２データパケットより後に受信された他のデータパケットであり得る確認フィールドを有し得ることに留意されたい。

【００３５】

本発明の第４の側面によれば、第１デバイスと第２デバイスとの間で安全にデータパケットを通信する他の方法が提供される。方法は、１）第１伝送プロトコルに基づく第１ネットワークを介して第１データパケットを受信するステップであって、第１伝送セキュリティプロトコルが第１伝送プロトコル上に用いられる、受信ステップと、２）第２伝送プロトコル基づく第２ネットワークを介して送信される第１データパケットを第２データパケットに変更するステップであって、第２伝送セキュリティプロトコルが第２伝送プロトコル上で用いられ、第１伝送プロトコル及び第２伝送プロトコルのうちの一方はデータグラムベースネットワークプロトコルであり、第１伝送プロトコル及び第２伝送プロトコルのうちの他方は信頼できる接続指向伝送プロトコルである、変更ステップと、３）第２ネットワークを介して第２データパケットを送信するステップと、４）第２データパケットを受信するステップと、５）第１データパケットのヘッダーに対応するよう、中間デバイスから受信された第２データパケットのヘッダーを再構成するステップと、６）第３データパケットのためのセキュリティ確認フィールドを生成するステップであって、セキュリティ確認フィールドは第１データパケットの再構成されたヘッダーに基づいて、第１伝送セキュリティプロトコルに従って生成される、生成ステップと、７）第２ネットワークを介して第３データパケットを送信するステップとを含む。

【００３６】

本発明の第４の側面に係る方法は、本発明の第１の側面に係るシステムと同じ利益を提供し、当該システムの対応する実施形態と同様な効果を有する同様な実施形態を有する。

【００３７】

本発明のこれら及び他の側面は、下記の実施形態を参照しながら説明されることによって明らかになるであろう。

【００３８】

当業者は、本発明の上記オプション、実施形態、及び／又は側面のうちの２つ以上が、

有用であると見なされる任意の方法で組み合わせられ得ることを理解するであろう。
【００３９】
システムの改変例及び変形例、並びに、説明されたシステムの改変例及び変形例に対応する方法及び／又はコンピュータプログラム製品の改変例及び変形例は、当業者によって本明細書に基づいて実行され得る。
【図面の簡単な説明】
【００４０】
【図１】図１は、本発明の第１の側面に係るシステムを概略的に示す。
【図２ａ】図２ａは、本発明の実施形態を含む、インターネットから６ＬｏｗＰＡＮネットワークにかけての安全なエンドツーエンド通信構造を概略的に示す。
【図２ｂ】図２ｂは、本発明の実施形態を含む、インターネットから６ＬｏｗＰＡＮネットワークにかけての安全なエンドツーエンド通信構造を概略的に示す。
【図３ａ】図３ａは、ＰＳＫを有するＴＬＳハンドシェイクプロトコルのシークエンス図を概略的に示す。
【図３ｂ】図３ｂは、ＰＳＫを有するＤＴＬＳハンドシェイクプロトコルのシークエンス図を概略的に示す。
【図４ａ】図４ａは、ＴＬＳ及びＤＴＬＳをＯＳＩモデルで概略的に示す。
【図４ｂ】図４ｂは、ＤＴＬＳ特有のフィールドがハイライトされたＴＬＳ／ＤＴＬＳパケットの構造を概略的に示す。
【図４ｃ】図４ｃは、ＤＴＬＳ特有のフィールドがハイライトされたＴＬＳ／ＤＴＬＳハンドシェイクメッセージの構造を概略的に示す。
【図５ａ】図５ａは、ＤＴＬＳ特有のフィールドがハイライトされたＴＬＳ／ＤＴＬＳＣｌｉｅｎｔＨｅｌｌメッセージの構造を概略的に示す。
【図５ｂ】図５ｂは、ＤＴＬＳ　ＨｅｌｌｏＶｅｒｉｆｙＲｅｑｕｅｓｔメッセージの構想を概略的に示す。
【図６】図６は、ＴＬＳ／ＤＴＬＳ組み合わせハンドシェイクプロトコルを概略的に示す。
【図７】図７は、ＣｏＡＰサーバが終了メッセージを受信して確認し、その後クライアントへの適切な終了メッセージを生成し送信するためのフローチャートを概略的に示す。
【図８ａ】図８ａは、本発明の第１の方法のフローチャートを概略的に示す。
【図８ｂ】図８ｂは、本発明の第２の方法のフローチャートを概略的に示す。
【００４１】
異なる図面で同じ参照番号で示されたアイテムは、同じ構造的特徴及び同じ機能を有するか、又は同じ信号であることに留意されたい。このようなアイテムの機能及び／又は構造が説明された場合、発明の詳細な説明において説明を繰り返す必要はない。
【００４２】
図は純粋に図式的であり、縮尺通りに描かれているわけではない。特に明瞭さのために、いくつかの寸法は強く誇張されている。
【発明を実施するための形態】
【００４３】
図１は、本発明の第１の側面に係るシステム１００の第１実施形態を概略的に示す。システム１００は、第１伝送プロトコルを用いる第１ネットワーク１２０を含む。第１伝送セキュリティプロトコルは、第１伝送プロトコル上に使用され得る。システム１００は、さらに、第２伝送プロトコルを用いる第２ネットワーク１０８を含む。第２伝送セキュリティプロトコルは、第２伝送プロトコル上に使用され得る。第１ネットワーク１２０には、第１デバイス１２４又は他の第１デバイス１３６が接続されている。第１ネットワーク１２０と第２ネットワーク１０８との間には中間デバイス１１０が接続されている。第２ネットワーク１０８には、第２デバイス１０２が接続されている。
【００４４】
第２デバイス１０２は、第２ネットワーク１０８に直接接続し、第２伝送プロトコルを

用いる第２ネットワークインターフェイス１０６を有する。第２ネットワークインターフェイス１０６は、第２デバイス１０２から第２ネットワーク１０８に伝送されるデータ、及び第２デバイス１０２によって第２ネットワークインターフェイス１０８から受信されるデータに対して第２伝送セキュリティプロトコルを適用する、第２セキュリティプロトコル適用手段１０４に接続されている。

【００４５】

また、中間デバイス１１０は、中間デバイス１１０と第２ネットワーク１０８との間の接続を提供する第２ネットワークインターフェイス１０６を有する。第２セキュリティプロトコル適用手段１０４は、中間デバイス１１０によって、第２ネットワークを介した通信のための第２伝送セキュリティプロトコルを扱うために用いられる。中間デバイス１１０は、さらに、第１ネットワークインターフェイス１２６を有する第１ネットワーク１２０に接続され、また、第１伝送セキュリティプロトコルを第１ネットワーク１２０の第１伝送プロトコル上に適用する第１セキュリティプロトコル適用手段１２８を有する。中間デバイス１１０の重要な機能のうちの１つは、第１ネットワークを介して受信され、第１伝送セキュリティプロトコルに従って生成されたデータパケットを、第２伝送セキュリティプロトコルに従う第２ネットワークを介する通信用のデータパケットへの変更（また、その逆の変更）であり、変更ユニット１２２によって実行される。変更ユニット１２２は、第１伝送プロトコルの第２伝送プロトコルへの変換及びその逆を実行し、また、第１伝送セキュリティプロトコルの第２伝送セキュリティプロトコルへの変換及びその逆を実行する。変更の結果、データパケットのヘッダーは変更され、多くの場合、使用される具体的なプロトコルにもよるが、ペイロードは触れられない。

【００４６】

一実施形態において、変更ユニット１２２は、第１伝送セキュリティプロトコル及び／又は第２伝送セキュリティプロトコルと能動的に関わらない。これは、変更ユニット１２２が各伝送セキュリティプロトコルにおいて用いられる秘密キーに関する知識を有さず、エンドツーエンド接続を確立しないことを意味する。変更ユニット１２２は、データパケットを別々のネットワークによって正常に伝送できるよう、データパケットのヘッダーのみを変更する。さらに、変更ユニット１２２によって、伝送プロトコル及び伝送セキュリティプロトコルの組み合わせに直接関係するパケットヘッダーの比較的簡単な変更を実行してもよい。例えば、データグラム・トランスポート・レイヤー・セキュリティ（ＤＴＬＳ）プロトコルは、元々はトランスポート・レイヤー・セキュリティ・プロトコルによって生成されたデータパケットのパケットヘッダーに限定された数のフィールドを加える。追加のフィールドは、伝送プロトコルとしてユーザ・データグラム・プロトコル（ＵＤＰ）上にトランスポート・レイヤー・セキュリティ（ＴＬＳ）を用いることができるような機能性を提供する。この例において、変更ユニット１２２は、各伝送セキュリティプロトコルのセキュリティ情報に関する知識を有することなく、このようなフィールドを加える。

【００４７】

図１は、第１デバイス１２４及び１３６の２つの異なる実施形態を示す。

【００４８】

第１デバイス１２４の第１実施形態は、第１デバイス１２４を第１ネットワーク１２０に接続する第１ネットワークインターフェイス１２６を有する。また、第１デバイス１２４は、第１伝送セキュリティプロトコルを第１ネットワークを介した通信に適用できる第１伝送セキュリティプロトコル適用手段１２８を有する。また、第１デバイス１２４は、第１ネットワークを介して受信されたデータパケットのヘッダーを、あたかもデータパケットが第２ネットワーク１０８を介して伝送されたかのように、そして、あたかも通信に第２伝送セキュリティプロトコルが用いられたかのように、データパケットのヘッダーに再構成する再構成ユニット１３０を有する。したがって、言い換えれば、再構成ユニット１３０は、中間デバイス１１０の変更ユニット１２２の動作を逆にすることができる。第１デバイス１２４は、さらに、再構成されたヘッダーに基づいて受信されたデータパケッ

ト内の確認フィールドを確認可能な確認ユニット１３２を有する。受信されたデータパケット内の確認フィールドは、第２伝送セキュリティプロトコルに基づくデータパケットを生成する第２デバイス１０２に由来してもよく、したがって、確認フィールドは第２伝送セキュリティプロトコルに基づいて生成される。ほとんどの伝送セキュリティプロトコルは、その特定の伝送セキュリティプロトコルに従って伝送されたデータパケットの１つ以上のヘッダーに基づいて確認フィールドを生成する。したがって、そのような確認フィールドを確認するためには、まず１つ以上のヘッダーを再構成しなければならず、これは再構成ユニット１３０によって行われる。確認フィールドに基づいて、確認ユニット１３２が安全なエンドツーエンド接続を確立するために確認フィールドを確認できるか否か、又は受信データパケットの信頼性を確かめることができる。

【００４９】

第１デバイス１３６の第２実施形態は第１デバイス１２４の第１実施形態に似ているが、第１デバイス１３６の第２実施形態のみが確認ユニット１３２を有さず、代わりに送信されるデータパケットのためのセキュリティ確認フィールドを生成する生成ユニット１３４を有する。セキュリティ確認フィールドは第１データパケットの再構成されたヘッダーに基づいて、第２伝送セキュリティプロトコルに従って生成される。したがって、第１デバイス１３６は、このような確認フィールドを確認可能な第２デバイス１０２にデータパケットを送信できる。したがって、第２デバイス１０２がこのような確認フィールドを明確に確認できる場合、第２デバイスによって安全なエンドツーエンド通信を確立できるか、又は伝送されたデータパケットの信頼性を確認することができる。

【００５０】

第１デバイス１２４の第１実施形態及び第１デバイス１３６の第２実施形態は、確認ユニット１３２及び生成ユニット１３４を含む単一のデバイスに組み合わせられ得ることに留意されたい。

【００５１】

図２ａは、インターネットから制約ＩＰネットワーク（例えば、６ＬＯＷＰＡＮ）にかけての通信を容易化する構造を示す。狙いは、インターネットに接続されたレガシーシステム（トランスポート・レイヤー・セキュリティ（ＴＬＳ）クライアント）が、ＣｏＡＰサーバと安全なエンドツーエンド（Ｄ）ＴＬＳハンドシェイクを確立する一方、プロキシ／ボーダールーターがハンドシェイクの秘密を学ばないことを可能にすることである。

【００５２】

ＴＬＳクライアントとＣｏＡＰサーバとの間の（Ｄ）ＴＬＳハンドシェイクを実行する際、プロキシ／ボーダールーター（中間デバイス）は、ＴＬＳパケットを変換し、ＤＴＬＳパケットに再パッケージングする（又はその逆の）責任を負う。

【００５３】

ハンドシェイクの終わりにおいて、ＣｏＡＰサーバは通信中のクライアントがＴＬＳを実行しているかＤＴＬＳを実行しているかを判断し、対応する「終了（Ｆｉｎｉｓｈｅｄ）メッセージ」を生成してハンドシェイクを完了できる。これは、既存のレガシークライアントが、クライアントの論理を変更する必要なく、ＣｏＡＰサーバとの安全なＥ２Ｅハンドシェイクを確立できることを保証する。

【００５４】

また、ハンドシェイクは、ＤＴＬＳクッキー機構を６ＬＯＷＰＡＮネットワークにローカルに維持しつつ、有効なＴＬＳクライアントの存在をＴＣＰ　Ｓｙｎｃ　Ｒａｎｄｏｍを用いてプロキシ／ボーダールーターによって決定できるよう、ＤＴＬＳとＴＣＰとの間のクロスレイヤー最適化を使用する。

【００５５】

ＣｏＡＰサーバは、自身がＨＴＴＰクライアントと対話しているのか又はＣｏＡＰクライアントと対話しているのかを知らず、また、レガシーシステム（ＨＴＴＰクライアント）を不変に保つことが重要であることを知らないので、ＴＬＳクライアントとの（Ｄ）ＴＬＳハンドシェイクプロトコルの成功を保証するためには、ＣｏＡＰデバイス内の‘ＴＬ

Ｓ　ｅｘｔ’内に追加の論理が必要である。

【００５６】

ハンドシェイク中のＴＬＳとＤＴＬＳとの違い

２つのピアーが（Ｄ）ＴＬＳ及び事前共有キーによって安全な方法でメッセージを交換できる前に、両者はいくつかのセキュリティパラメータ、例えばＣｉｐｈｅｒＳｕｉｔｅ、圧縮方法、又はキーＩＤ等について交渉しなければならない。これは、通信エンティティの認証を含む（Ｄ）ＴＬＳハンドシェイクによって実行される。図３ａ及び図３ｂは、事前共有キー（ＰＳＫ）を有するＴＬＳ及びＤＴＬＳハンドシェイクのシーケンス図を示す。＊が付けられたメッセージはオプションである。

【００５７】

ＴＬＳを使用する場合、ＨＴＴＰクライアントはまず、セッションキーを作成するために用いられるＣｌｉｅｎｔＨｅｌｌｏメッセージを、利用可能なＣｉｐｈｅｒＳｕｉｔｅとともに送信する。ＣｏＡＰサーバは、提供されたＣｉｐｈｅｒＳｕｉｔｅのうちの１つを選び、それをＳｅｒｖｅｒＨｅｌｌｏメッセージ内に入れてクライアントに送り返す。クライアントが適切なキーを選択する助けをする「ＰＳＫＩＤヒント」をＳｅｒｖｅｒＫｅｙＥｘｃｈａｎｇｅに入れて提供するか否かは、サーバ次第である。ヒントが提供できない場合、このメッセージは省略される。Ｈｅｌｌｏメッセージ段階の終わりを示すために、サーバは、ＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅメッセージを送る。次に、ＨＴＴＰクライアントは、サーバからのヒント有り又はヒント無しで、ＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅメッセージを送信することによってどのキーが用いられるかを示す。ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃメッセージを送信後、ハンドシェイクは終了（Ｆｉｎｉｓｈｅｄ）メッセージによって認証される。ＴＬＳ終了メッセージは、マスターシークレットの入力、終了ラベル（「クライアント終了」）、及びその時点までに交換された全てのハンドシェイクのメッセージ（終了メッセージを除く）の連結のハッシュを取る疑似ランダム機能（ＰＲＦ）を用いて計算される。認証及びキー共有が成功すると、情報を安全な接続を介して伝送できる。

【００５８】

ＴＬＳと同様に、ＤＴＬＳにおいてもクライアントはＣｌｉｅｎｔＨｅｌｌｏメッセージから始める。上述のように、クライアントの存在を確認するためにクッキー機構を用いることができる。このフィールドは、最初は空に設定される。クッキーを用いるか否かはサーバの決定次第である。用いない場合、サーバはＳｅｒｖｅｒＨｅｌｌｏメッセージを送り、用いる場合は、クッキーを含むＨｅｌｌｏＶｅｒｉｆｙＲｅｑｕｅｓｔメッセージがクライアントに送られる。後者の場合、クライアントは同じパラメータを有するＣｌｉｅｎｔＨｅｌｌｏメッセージを再び送るが、今回はサーバから与えられたクッキーを含む。その後、メッセージはＴＬＳの場合と同様に、同じ方法及び同じ順番で交換される。

【００５９】

ＴＬＳパケット及びＤＴＬＳパケットの構造

図４ａに示すように、（Ｄ）ＴＬＳはアプリケーション層と伝送層との間の層である。また、（Ｄ）ＴＬＳが層プロトコルであることがわかる。下層上にはレコードプロトコルが配置され、上層上には４つのプロトコル、すなわち、ハンドシェイクプロトコル、アラートプロトコル、ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃプロトコル、及びアプリケーションデータプロトコルが定められる。これらのプロトコルのそれぞれが、所定の時点及び方法で送信される独自のメッセージを提供する。

【００６０】

図４ｂは、レコードメッセージの概略的なデザインを示す。図４ｃに示すように、ハンドシェイクの完了前にはいかなるセキュリティパラメータも確立しないため、これらのメッセージは暗号化されない、又はＭＡＣを含まない。ＴＬＳとＤＴＬＳとの違いがハイライトされる。これは、レコードメッセージにおいては、ＤＴＬＳがヘッダー内に２つのメッセージを追加すること、具体的にはエポック及びシーケンス番号を追加することを意味する。

【００６１】
ハンドシェイクメッセージヘッダーにおいては、メッセージシーケンス番号、フラグメントオフセット、及びフラグメント長が追加される。
【００６２】
図５ａに示すＣｌｉｅｎｔＨｅｌｌｏメッセージは、クッキーのためのフィールドを追加し、ＴＬＳ内にはＨｅｌｌｏＶｅｒｉｆｙＲｅｑｕｅｓｔが存在しない（図５ｂ）。
【００６３】
図６は、組み合わされたＴＬＳ－ＤＴＬＳハンドシェイクを示す。プロキシは、ＤＴＬＳにのみ関連するフィールドを追加又は除くことによってＴＬＳパケットをＤＴＬＳパケットに変換する、又はその逆の責任を負う。サーバがクッキーの使用を望み、ＨｅｌｌｏＶｅｒｉｆｙＲｅｑｕｅｓｔ　メッセージを送信する場合、ＴＬＳではこのメッセージタイプは用いられないため、プロキシはＨＴＴＰクライアントにメッセージを転送してはならない。代わりに、プロキシはＣｏＡＰサーバに対して、サーバから与えられたクッキーを有する第２ＣｌｉｅｎｔＨｅｌｌｏメッセージをもって応答する。終了メッセージが到着すると、プロキシはメッセージをサーバに転送しなければならない。プロキシはクライアント及びサーバが共有するシークレットを有しないため、プロキシはメッセージ内のデータを変更及び確認することはできない。プロキシの他のタスクは、ＤＴＬＳのミッシングメッセージ再送信能力に関する。これはＤＴＬＳクライアントのデューティであるため、プロキシは、信頼性の高い送信を提供する必要がある。
【００６４】
異なるプロトコル用の終了メッセージのコンテンツの交換及び計算
前項で述べたように、ハンドシェイクプロトコルが完了すると、ハンドシェイクを認証するために終了メッセージが送信される。終了メッセージは、基本的に１つのフィールドのみ、すなわち、以下のようにして計算される確認データを含む。
ＰＲＦ（ｍａｓｔｅｒ＿ｓｅｃｒｅｔ，ｆｉｎｉｓｈｅｄ　ｌａｂｅｌ，Ｈａｓｈ（ｈａｎｄｓｈａｋｅ＿ｍｅｓｓａｇｅｓ））［０．．ｖｅｒｉｆｙ＿ｄａｔａ＿ｌｅｎｇｔｈ－１］
ここで、終了ラベル（ｆｉｎｉｓｈｅｄ　ｌａｂｅｌ）はクライアントに対しては「クライアント終了」を意味し、サーバに対しては「サーバ終了」を意味する。パラメータｈａｎｄｓｈａｋｅ＿ｍｅｓｓａｇｅｓは、それまでに交換された全てのメッセージの連結である。
【００６５】
最初の終了メッセージは、ＨＴＴＰクライアントによってＨＴＴＰ／ＣｏＡＰプロキシに送られる。前項で述べたように、プロキシは、レコードヘッダー内にエポック及びシーケンス番号を加えることによってＴＬＳフォーマットの終了メッセージをＤＴＬＳフォーマットに変更する責任を負う。しかし、プロキシは、ハンドシェイクフェーズ中に交渉される、クライアントとサーバとの間で共有される秘密であるマスターシークレットを有しないため、確認データを再計算することができない。終了メッセージは、その後プロキシによってＣｏＡＰサーバに送られる。
【００６６】
ＣｏＡＰサーバは、同じＰＲＦ機能を用いることによってクライアント終了メッセージを確認する。クライアント終了メッセージは、（メッセージ内のレコードヘッダーおよびハンドシェイクヘッダーから知ることができる）ＤＴＬＳハンドシェイクメッセージタイプであるので、ＣｏＡＰサーバはそれまでの全てのＤＴＬＳハンドシェイクメッセージ（終了メッセージ自体は含まない）に基づいて確認データフィールドを計算し、クライアント終了メッセージと照らし合わせる。確認が成功の場合、ＣｏＡＰサーバは、サーバ終了メッセージのＤＴＬＳバージョンをプロキシに送信する。確認が失敗の場合、ＣｏＡＰサーバは、（致命的な）エラーアラートをトリガしたり交換を停止するのではなく、クライアントがＨＴＴＰクライアント（ＴＬＳ）であると見なし、確認データフィールドを再計算しなければならない。ただし、今回は、それまでの全てのハンドシェイクメッセージ内

の追加ＤＴＬＳフィールドが除かれる（すなわち、ＤＴＬＳハンドシェイクヘッダーがＴＬＳハンドシェイクヘッダーに置き換えられ、ＣｌｉｅｎｔＨｅｌｌｏメッセージ内のクッキーフィールドが除かれる）。これによってクライアント終了メッセージが確認される場合、ＣｏＡｐサーバはクライアントがＨＴＴＰクライアント（ＴＬＳ）であると認める。続いて、ＣｏＡＰサーバは、自身がＨＴＴＰクライアント（ＴＬＳ）によって認証されるよう、対応するサーバ終了メッセージを作成し、ハンドシェイクプロトコルを完了してＨＴＴＰクライアントとＣｏＡＰサーバとの間の安全なエンドツーエンドトンネルを確立する。

【００６７】

したがって、まずクライアントから送信された「終了」メッセージをＤＴＬＳメッセージとして確認しようとし、この確認が失敗した場合、「終了」メッセージをＴＬＳメッセージとして確認しようとすることによって、ＣｏＡＰサーバは、ＣｏＡＰ／ＤＴＬＳクライアントとＨＴＴＰ／ＴＬＳクライアントとを識別することができ、いずれの場合においても適切なサーバ「終了」メッセージを生成することができる。これは、図７にも示されている。「終了」メッセージが受信されると（７０２）、ＤＴＬＳプロトコルに基づいて「終了」メッセージが確認される（７０４）。確認の結果が真の場合、したがって、メッセージが認証された場合、ＤＴＬＳプロトコルに従って「ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃ」メッセージが送信され（７０６）、ＤＴＬＳ「終了」メッセージを送信することによってハンドシェイクが終了する（７０８）。確認（７０４）の結果が真でない場合、受信メッセージのヘッダーからＤＴＬＳコンテンツが除かれ（７１０）、必要な場合は過去のメッセージのヘッダーからも除かれる。続いて、ＴＬＳプロトコルに基づいて「終了」メッセージが確認される（７１２）。確認（７１２）が真の場合、つまり、変更されたヘッダーに基づいて終了メッセージの確認フィールドが確認（認証）される場合、「ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃ」メッセージが送信され（７１４）、続いてＴＬＳ「終了」メッセージが送信される。確認（７１２）が真でない場合、エラーが警告され（７１８）、接続が閉じられる（７２０）。

【００６８】

ＴＬＳサーバとＣｏＡＰクライアントとの間の安全なエンドツーエンド通信

図２ｂに示すような他の状況において、いくつかの適用例では、制約デバイスは、ＨＴＴＰ／ＣｏＡＰプロキシを介してインターネット上でバックエンド内のサーバと対話するクライアントとして動作し得る。このセットアップにおいて、クライアントは通常、例えばＧＥＴ関数を用いて、サーバに対してイベント、情報、及びデータのポーリングを行う。この状況において、狙いはプロキシ／ボーダールーターがハンドシェイクの秘密を学ぶことなく、ＣｏＡＰクライアントがレガシーサーバとのエンドツーエンドハンドシェイクを実行できるようにすることである。この環境において、（Ｄ）ＴＬＳハンドシェイクはやはりＣｏＡＰクライアントによって、ＤＴＬＳパケットをＴＬＳパケットに変換する（及びその逆の）責任を負うプロキシ／ボーダールーターを介してＴＬＳサーバにＣｌｉｅｎｔＨｅｌｌｏメッセージを送ることによって開始される。（Ｄ）ＴＬＳハンドシェイクプロトコルは、前述と同様であるが、２つのエンドポイントデバイスの役割が逆転する。プロキシの役割は変わらず、ＤＴＬＳクライアントへの／からのメッセージを転送する際には、ＤＴＬＳ特有フィールドを加える／除く。

【００６９】

ただし、ＣｏＡＰクライアントは自身がＨＴＴＰサーバと対話しているのか、又はＣｏＡＰサーバと対話しているのかを知らず、また、レガシーシステム（ＨＴＴＰサーバ）を不変に保つ重要性を知らないため、ＴＬＳサーバとの（Ｄ）ＴＬＳハンドシェイクプロトコルの成功を保証するために、ＣｏＡＰデバイス内の‘ＴＬＳ　ｅｘｔ’内に追加の論理が必要である。

【００７０】

特に、ＣｏＡＰクライアントは、（Ｄ）ＴＬＳハンドシェイクプロトコルに従い、プロキシを介してＴＬＳサーバに第１終了メッセージを送信しなければならないが、終了メッ

セージがＤＴＬＳプロトコルに従って計算された確認データを含む場合、確認メッセージはＴＬＳサーバによって確認されない。以下に選択可能な解決策を概説する。
１．　ＣｏＡＰクライアントは、２つの「終了」メッセージを生成する。第１メッセージはＴＬＳ「終了」メッセージで、第２メッセージはＤＴＬＳ「終了」メッセージであり、両メッセージはプロキシに送信される。受信後、プロキシはＴＬＳサーバに転送されるべき適切な「終了」メッセージを決定する。
２．　ＣｏＡＰクライアントは、まずＤＴＬＳ「終了」メッセージを生成し、プロキシを介してＴＬＳサーバに送信する。ＴＬＳサーバは、当然ＤＴＬＳ「終了」メッセージを確認することができず、（プロキシを介して）ＣｏＡＰクライアントに解読エラーメッセージを送信する。このメッセージは致命的なエラーを示すため、ハンドシェイクは停止される。ＣｏＡＰクライアントは、自身が通信しているエンティティはレガシーＴＬＳサーバであることを知り、ＴＬＳサーバにとって正しいＴＬＳ「終了」メッセージを生成することを確実にし、ＤＴＬＳ／ＴＬＳハンドシェイクプロトコルを再開する。さらに、ＤＴＬＳクライアントはサーバＤＴＬＳ／ＴＬＳ能力に関する情報を記憶し、その後は第１メッセージとして正しい「終了」メッセージを使用することにより交換を短縮してもよい。
３．　ＣｏＡＰクライアントは、まずＴＬＳ「終了」メッセージを生成し、プロキシを介してＴＬＳサーバに送信する。「終了」メッセージの確認が成功した場合、ＴＬＳサーバとＣｏＡＰクライアントとの間には安全なエンドツーエンドトンネルが確立される。エンドポイントがＨＴＴＰサーバ（ＴＬＳ）ではなくＣｏＡＰサーバ（ＤＴＬＳ）である場合、「終了」メッセージの確認は失敗する。しかし、「終了」メッセージの確認が失敗したとしても、ＤＴＬＳにおいて致命的なエラーは報告されない。したがって、ＣｏＡＰクライアントは、ハンドシェイクを完了するためにＣｏＡＰサーバ（ＤＴＬＳ）にとって正しいＤＴＬＳ「終了」メッセージを続けて生成し得る。これは、ＣｏＡＰクライアントがＤＴＬＳ／ＴＬＳハンドシェイクを再開する必要がないという利点を有する。

【００７１】

図８ａは、本発明の第４の側面に係る方法８００を示す。方法８００は、第１デバイスと第２デバイスとの間でデータパケットを安全に通信するための方法８００である。方法８００は、１）第２伝送プロトコルに基づく第２ネットワークを介して第２データパケットを受信するステップであって、第２伝送セキュリティプロトコルが第２伝送プロトコル上に用いられる受信ステップ（８０２）と、２）第２データパケットを、第１伝送プロトコルに基づく第１ネットワークを介して送信されるべき第１データパケットに変更するステップであって、第１伝送セキュリティプロトコルが第１伝送プロトコル上で用いられ、第１伝送プロトコル及び第２伝送プロトコルのうちの一方はデータグラムベースネットワークプロトコルであり、第１伝送プロトコル及び第２伝送プロトコルのうちの他方は信頼できる接続指向伝送プロトコルである、変更ステップ（８０４）と、３）第１ネットワークを介して第１データパケットを送信するステップ（８０６）と、４）第１データパケットを受信するステップ（８０８）と、５）第２データパケットのヘッダーに対応するように中間デバイスから受信された第１データパケットのヘッダーを再構成するステップ（８１０）と、６）第１データパケットの再構成されたヘッダーに基づいて第１データパケット又は第３データパケットのセキュリティ確認フィールドを確認するステップであって、確認フィールドは第２伝送セキュリティプロトコルに従って生成される確認ステップ（８１２）とを含む。

【００７２】

図８ｂは、本発明の第４の側面に係る他の方法８５０を示す。方法８５０は、第１デバイスと第２デバイスとの間でデータパケットを安全に通信するための方法８５０である。方法８５０は、１）第２伝送プロトコルに基づく第２ネットワークを介して第２データパケットを受信するステップであって、第２伝送セキュリティプロトコルが第２伝送プロトコル上に用いられる、受信ステップ（８５２）と、２）第２データパケットを、第１伝送プロトコル基づく第１ネットワークを介して送信される第１データパケットに変更するステップであって、第１伝送セキュリティプロトコルが第１伝送プロトコル上に用いられ、

第１伝送プロトコル及び第２伝送プロトコルのうちの１つはデータグラムベースネットワークプロトコルであり、第１伝送プロトコル及び第２伝送プロトコルのうちの他方は信頼できる接続指向伝送プロトコルである、変更ステップ（８５４）と、３）第１ネットワークを介して第１データパケットを送信するステップ（８５６）と、４）第１データパケットを受信するステップ（８５８）と、５）ヘッダーが第２データパケットのヘッダーに対応するよう、中間デバイスから受信された第１データパケットのヘッダーを再構成するステップ（８６０）と、６）第３データパケットのためのセキュリティ確認フィールドを生成するステップであって、セキュリティ確認フィールドは第１データパケットの再構成されたヘッダーに基づいて、第２伝送セキュリティプロトコルに従って生成される、生成ステップ（８６２）と、７）第１ネットワークを介して第３データパケットを送信するステップ（８６４）とを含む。

【００７３】

本発明は、以下のように要約することができる。本発明は、安全なエンドツーエンド通信を確立し、安全にデータパケットを通信するための方法、デバイス、及び通信システムを提供する。このような通信システムは、第１デバイス、中間デバイス、及び第２デバイスを含む。第１デバイスは、第１伝送プロトコル及び第１伝送セキュリティプロトコルに基づく第１ネットワークを介して中間デバイスと通信する。第２デバイスは、第２伝送プロトコル及び第２伝送セキュリティプロトコルに基づく第２ネットワークを介して中間デバイスと通信する。中間デバイスは、第１ネットワークを介して受信されたパケットを第２ネットワークに適したパケットに変更し、またその逆の変更も行う。第１デバイスは、受信されたパケットがあたかも第２ネットワーク、並びに第２ネットワーク伝送プロトコル及び第２伝送セキュリティプロトコルによって送信されたかのように、受信されたパケットのヘッダーを再構成できる。さらに、第１デバイスは再構成されたヘッダーに基づき、第２伝送セキュリティプロトコルに基づいて生成された確認フィールドを確認することができる。

【００７４】

上記実施形態はあくまで本発明を説明するものであり、限定するものではなく、また、当業者は特許請求の範囲から逸脱することなく多数の代替的な実施形態を設計し得るであろう。

【００７５】

請求項における括弧内の参照番号は請求の範囲を制限すると解されるべきではない。動詞「含む（又は、有する若しくは備える）」及びその活用形は、請求項に記載の要素又はステップの存在を除外しない。要素は複数を除外しない。本発明は、いくつかの要素を含むハードウェアによって実現することができ、また、適切にプログラミングされたコンピュータによって実現することもできる。いくつかの手段が異なる請求項内に記載されているからといって、これらの手段の組み合わせを好適に用いることができないとは限らない。

【図１】

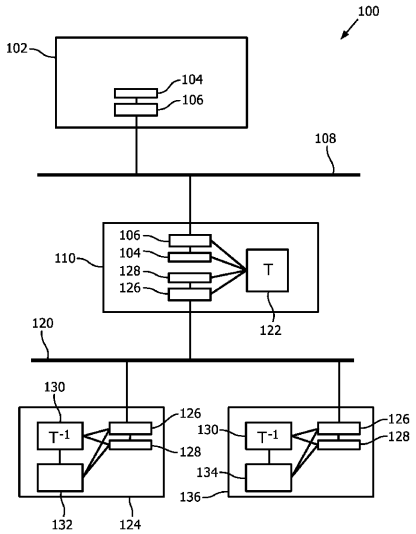


FIG. 1

【図７】

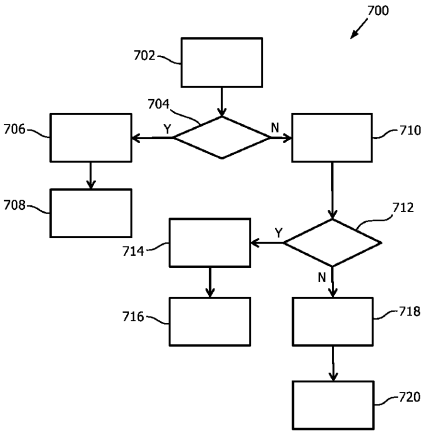


FIG. 7

【図８ａ】

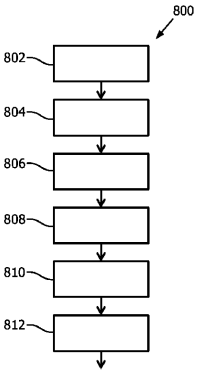


FIG. 8a

【図８ｂ】

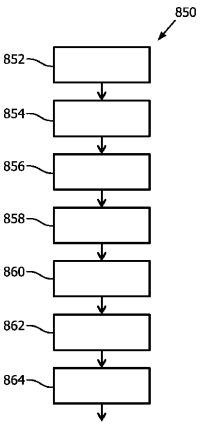
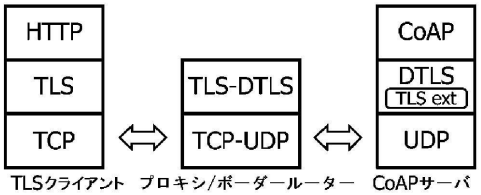
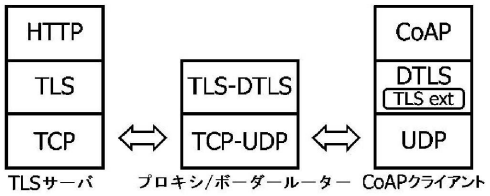


FIG. 8b

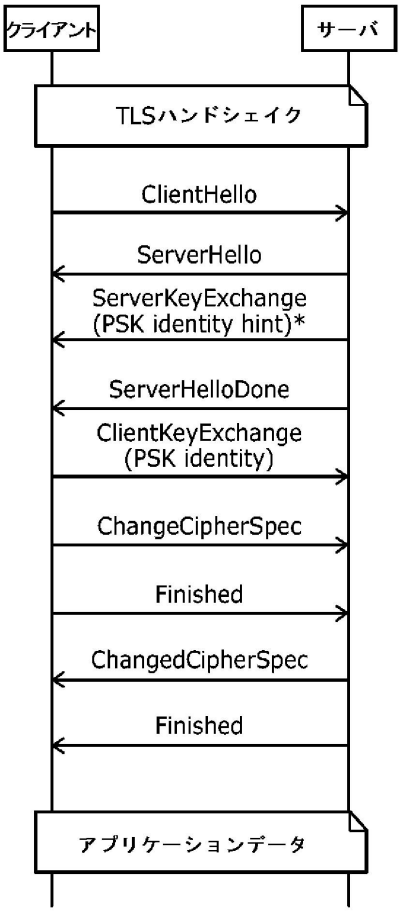
【図２Ａ】



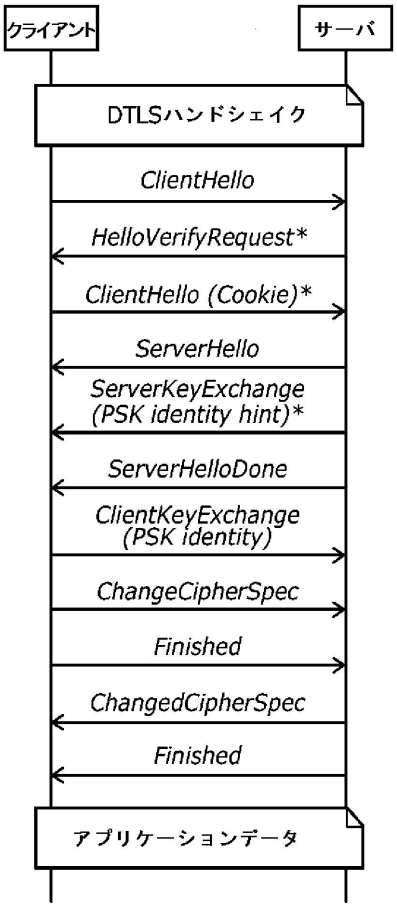
【図２Ｂ】



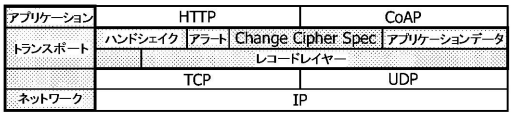
【図３Ａ】



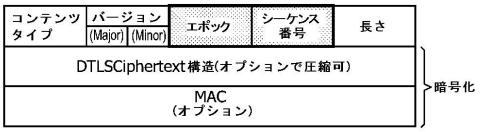
【図３Ｂ】



【図４Ａ】

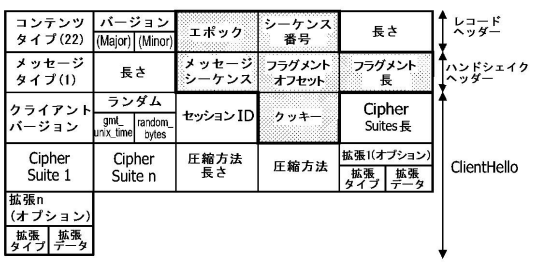


【図４Ｂ】

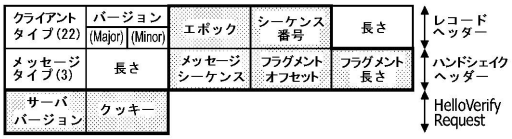


【図４Ｃ】

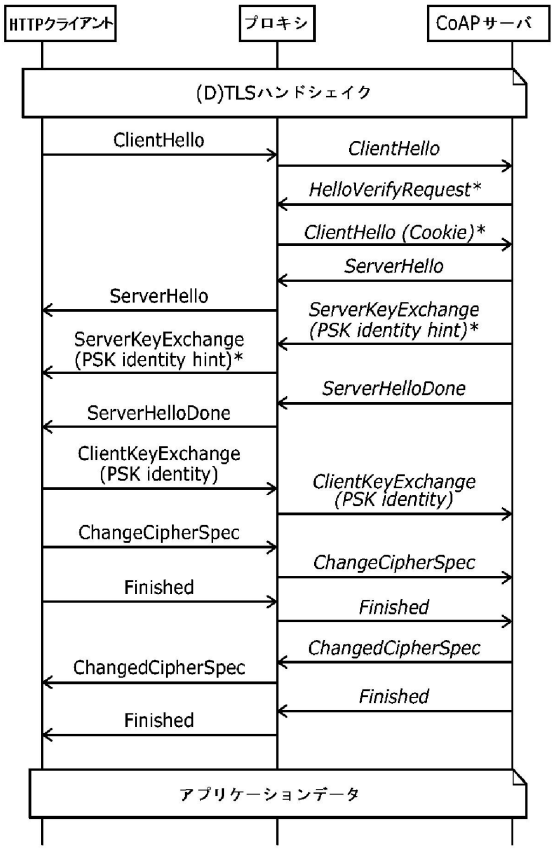
【図５Ａ】



【図５Ｂ】


クライアントタイプ(22)
バージョン
(Major)
(Minor)
エポック
シーケンス番号
長さ
メッセージタイプ(3)
長さ
メッセージシーケンス
フラグメントオフセット
フラグメント長さ
サーババージョン
クッキー
レコードヘッダー
ハンドシェイクヘッダー
HelloVerifyRequest

【図６】


HTTPクライアント
プロキシ
CoAPサーバ
(D)TLSハンドシェイク
ClientHello
ClientHello
HelloVerifyRequest*
ClientHello (Cookie)*
ServerHello
ServerHello
ServerKeyExchange (PSK identity hint)*
ServerKeyExchange (PSK identity hint)*
ServerHelloDone
ServerHelloDone
ClientKeyExchange (PSK identity)
ClientKeyExchange (PSK identity)
ChangeCipherSpec
ChangeCipherSpec
Finished
Finished
ChangedCipherSpec
ChangedCipherSpec
Finished
Finished
アプリケーションデータ

フロントページの続き

(72)発明者 ケオー シェ ルーン
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ビルディング ４４
(72)発明者 ガルシア モーション オスカー
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ビルディング ４４
(72)発明者 クマル サンディープ シャンカラン
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ビルディング ４４
(72)発明者 ブラッチマン マルティナ
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ビルディング ４４
(72)発明者 エルドマン ボゼナ
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ビルディング ４４

審査官 森谷 哲朗

(56)参考文献 米国特許出願公開第２００３／００８１７８３（ＵＳ，Ａ１）
米国特許出願公開第２００４／０１０３２８３（ＵＳ，Ａ１）
特開２００９－０３８５３６（ＪＰ，Ａ）
特開２００４－０８８７６８（ＪＰ，Ａ）
A. Castellani et al., Best practices for HTTP-CoAP mapping implementation, draft-castellani-core-http-mapping-01, ２０１１年 ７月１１日, pp.1-26, ＵＲＬ, https://tools.ietf.org/html/draft-castellani-core-http-mapping-01

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ２９／０６
Ｈ０４Ｌ １２／２２
Ｈ０４Ｌ １２／６６