

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6214088号
(P6214088)

(45) 発行日 平成29年10月18日(2017.10.18)

(24) 登録日 平成29年9月29日(2017.9.29)

(51) Int.Cl.		F I			
HO4L	9/18	(2006.01)	HO4L	9/00	651
HO4L	12/22	(2006.01)	HO4L	12/22	
HO4L	12/717	(2013.01)	HO4L	12/717	

請求項の数 12 (全 27 頁)

(21) 出願番号	特願2013-242470 (P2013-242470)	(73) 特許権者	800000068
(22) 出願日	平成25年11月25日(2013.11.25)		学校法人東京電機大学
(65) 公開番号	特開2015-103933 (P2015-103933A)		東京都足立区千住旭町5番
(43) 公開日	平成27年6月4日(2015.6.4)	(74) 代理人	100119677
審査請求日	平成28年10月3日(2016.10.3)		弁理士 岡田 賢治
(出願人による申告)平成23年度、独立行政法人情報通信研究機構、「高速通信・放送研究開発委託研究/高性能光電子融合型パケットルータ基盤技術の研究開発」、産業技術力強化法第19条の適用を受ける特許出願		(74) 代理人	100115794
			弁理士 今下 勝博
		(72) 発明者	官保 憲治
			東京都足立区千住旭町5番 学校法人東京電機大学内
		(72) 発明者	上野 洋一郎
			東京都足立区千住旭町5番 学校法人東京電機大学内

最終頁に続く

(54) 【発明の名称】 ネットワーク制御システム及び方法

(57) 【特許請求の範囲】

【請求項1】

コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御システムにおいて、

前記スイッチは、ユーザ端末からの通信データを受信すると、当該通信データを複数の断片データに分割して断片データの配列順を変更し、配列順を変更後の各断片データを、出力経路を制御するためのフローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに出力し、

前記コントローラは、変更後の前記断片データの配列順を格納する、
ネットワーク制御システム。

10

【請求項2】

前記スイッチは、ユーザ端末から通信のデータを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて前記スイッチで行った符号化を復号化するために必要なメタデータを前記コントローラに出力し、

前記コントローラは、前記スイッチで符号化された通信データを復号化するために必要なメタデータをさらに格納する

ことを特徴とする請求項1に記載のネットワーク制御システム。

【請求項3】

20

前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化する

請求項 2 に記載のネットワーク制御システム。

【請求項 4】

前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータを当該ユーザ端末へ送信し、

当該ユーザ端末は、前記スイッチから取得するメタデータを用いて前記通信データ又は前記断片データを復号化する

請求項 2 に記載のネットワーク制御システム。

10

【請求項 5】

前記スイッチは、ユーザ端末から通信データの取得要求を受信すると、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信する

ことを特徴とする請求項 1 から 4 のいずれかに記載のネットワーク制御システム。

【請求項 6】

前記スイッチは、

ネットワークに対して要求するセキュリティサービス種別を、ユーザ端末からの前記通信データに含まれるフラグ種別情報から識別し、

前記セキュリティサービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った 1 以上のストレージ端末に向けて、前記断片データを出力するとともに、前記専用通信ネットワークを用いて前記断片データの送信先を前記コントローラに出力し、

20

前記コントローラは、前記断片データの送信先をさらに格納する

請求項 1 から 5 のいずれかに記載のネットワーク制御システム。

【請求項 7】

コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御方法において、

ユーザ端末からの通信データを受信した前記スイッチが、出力経路を制御するためのフローテーブルを参照し、当該通信データを複数の断片データに分割して断片データの配列順を変更し、配列順を変更後の各断片データを前記フローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに格納するデータ送信手順を有するネットワーク制御方法。

30

【請求項 8】

前記データ送信手順において、ユーザ端末からの通信データを受信した前記スイッチが、ユーザ端末からの通信データを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて当該スイッチで符号化された通信データを復号化するために必要なメタデータを前記コントローラに格納する

ことを特徴とする請求項 7 に記載のネットワーク制御方法。

40

【請求項 9】

ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、

前記データ受信手順において、当該スイッチが、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化する

ことを特徴とする請求項 8 に記載のネットワーク制御方法。

【請求項 10】

ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手

50

順の後にさらに有し、

前記データ受信手順において、当該スイッチが、前記コントローラに格納されている前記メタデータを当該ユーザ端末へ送信し、前記スイッチからメタデータを取得した当該ユーザ端末が当該メタデータを用いて前記通信データ又は前記断片データを復号化する

ことを特徴とする請求項 8 に記載のネットワーク制御方法。

【請求項 11】

ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、

前記データ受信手順において、当該スイッチが、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信する

ことを特徴とする請求項 7 から 10 のいずれかに記載のネットワーク制御方法。

【請求項 12】

前記データ送信手順において、

ユーザ端末からの通信データを受信した前記スイッチが、ネットワークに対して要求するセキュリティサービス種別を当該通信データに含まれるフラグ種別情報から識別し、

前記セキュリティサービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った 1 以上のストレージ端末に向けて、前記断片データを出力するとともに、専用通信ネットワークを用いて前記断片データの送信先を前記コントローラに格納する

ことを特徴とする請求項 7 から 11 のいずれかに記載のネットワーク制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、SDNスイッチを用いたネットワーク制御システム及び方法に関する。

【背景技術】

【0002】

ソフトウェア制御が可能なネットワーク (SDN: Software Defined Network) の一つの技術要素として、ネットワークノードの機能をネットワークルーティング機構 (ノードのデータ転送機能) とコントローラ機構 (ノードでの制御ソフトウェア・ルーティング制御機能) とに、分離できるようにインタフェースを公開し、ネットワーク制御をプログラマブルにすることにより、柔軟な経路制御や構成変更、ならびに新しい通信サービス等を実現可能とするネットワーク制御機構が注目されている。SDNではコントローラがネットワーク内の全情報を集め、一元的に定義し、ソフトウェアを活用した集中制御処理に基づいて、ネットワーク全体を制御できる特徴を持つ。コントローラは、スイッチ制御用のソフトウェアを配備することにより、スイッチの動作を制御できる。

【0003】

SDNの実現方法の1つとして、オープンフロー (OpenFlow: 非特許文献 1、2) と呼ばれるネットワークプラットフォームの標準化が進められ、オープンソースによる実装と同時に企業によるシステム/製品群が市場に普及しつつある。SDNを実現するスイッチやコントローラに関しては、オープンソースとして公開したTremaやスタンフォード大学で開発されたBeacon、Nicirria Network社が開発したNOX等がある。SDNを実現する上での課題の一つは、ネットワークで提供されるサービスに対して、セキュリティを高めるための有効な技術を提供することであり、このメカニズムを開示することが本発明の目的である。しかしながら、高いセキュリティを確保した高信頼なデータ配信サービスをSDNの機構を適切に用いて、ネットワーク内で新たなセキュリティ基準のもとに、新しい制御機構技術として組み込んだ例は開示されていない。本発明で開示する技術は、いずれのスイッチやコントローラに対しても、同様に適用することが可能であり、高信頼のネットワークサービスを実現する上での技術基盤を提供で

10

20

30

40

50

きる。

【 0 0 0 4 】

特許文献 1 では、データファイルを分割し、当該分割された断片データを複数のクライアント端末に分散転送するバックアップ技術を用い、データファイルを保有する管理ユーザのサービス要求に見合ったセキュリティレベルでのバックアップを可能にするための技術が開示されている。

特許文献 2 では、各種の P C 端末、モバイル端末等の遊休リソースを積極的に活用し、ファイルの暗号化・分割・複製・分散化技術を組み合わせる事により、信頼性の高いディザスタリカバリを実現可能とする基本技術およびファイル一体化と呼ばれるファイルデータの撹拌技術が開示されている。

10

【 0 0 0 5 】

非特許文献 1 は、オープンフローコントローラが備えるべきデータを分散データベース上に構築し、オープンフローコントローラを介して実装されるネットワークアプリケーションに対して適切な A P I (A p p l i c a t i o n P r o g r a m m i n g I n t e r f a c e) を提供することで、オープンフローコントローラの分散化を実現している。

非特許文献 2 は、データを分散データベース上で管理すると共に、複数のオープンフローコントローラ間で通信を行うことで同期をとる方法が示されている。

【 0 0 0 6 】

ソフトウェア制御を用いてスイッチの出力経路を制御する S D N 内のスイッチと、スイッチ制御用のコントローラにより構成されるネットワーク制御システムを活用して、ファイルバックアップサービスを行う際の暗号化、分散転送、復号化をネットワーク制御装置のみにより、効率的に実施するメカニズムを開示している。具体的には、ユーザ端末（ホスト端末）が送出するパケットデータの中に、ネットワークに対して要求するセキュリティサービス種別をフラグ情報として含め、前記のスイッチに、フラグ情報を識別する機構を持たせることにより、S D N アーキテクチャを活用して、バックアップ用のサービスの中の特定のサービスレベル種別を識別し、ユーザの創出するユーザパケットを、スイッチ内で、当該のサービスレベルの程度に合わせて、適切な、暗号処理化や複製を行う。このことにより、ユーザ端末やゲートウェイでの暗号化等に関わる符号処理を大幅に削減し、ユーザ端末の通信処理用のスループットを大幅に向上することができる。このメカニズムは、ユーザ端末側での暗号処理メカニズムを全く活用せずに、ネットワーク制御装置での当該処理メカニズムを用いることにより、第三者の盗聴が不可能な、秘密データ転送サービスにも活用できる。

20

30

【 0 0 0 7 】

現在、ホストとなるユーザ端末やサーバの処理能力は向上しつつあるものの、セキュリティの高い通信を実現するためには、例えばユーザ端末で、共通鍵暗号の 1 つである A E S 暗号による処理を行う方法がある。この場合、暗号鍵の長さや送信するデータ容量が増加するにしたがって、計算量は一般的に、指数関数的に増加する。近年、通信で扱うデータ容量は増加しつつあり、セキュリティ強度を上げるためには、暗号鍵の長さを長く設定し、暗号処理に必要な計算量が増大する傾向がある。この結果、ユーザ端末での暗号処理に関わるオーバーヘッドが、通信スループット等の低下に対する影響が無視できなくなる状況が生じつつある。

40

【 0 0 0 8 】

通常、ホスト - サーバ間、あるいはホスト - ホスト間における通信で、セキュリティを高めるために I P S e c や S S L / T S L 等のセキュリティプロトコルが導入されている。しかし、いずれのセキュリティプロトコルも、ユーザ端末における通信スループットの低下を来す。例えば、I P s e c は I P パケットのレベルで暗号化を行うことにより、2 台のユーザ端末間の通信を、盗聴や改ざんから保護するためのセキュリティ技術として活用されている。

【 0 0 0 9 】

50

図1に示すようなゲートウェイをユーザ端末に隣接して設ける方法か、または、図2に示すようなPC内蔵ソフトウェアをユーザ端末に組み込む用いる方法が利用されている。例えば、Windows(登録商標)2000以上ではIPsec機能をIPレイヤに標準で組み込んでいる。特に、後者の形態は、暗号化処理に起因するユーザ端末の処理能力を消費するため、高性能の通信スループットが要求される場合には、当該ゲートウェイ装置の導入コストは増加するものの、前者の使用形態が用いられる。IPsecはIP層で暗号化/復号化を行うため、他の暗号処理用のセキュリティプロトコルと比べて、既存のLANやインターネット対応のアプリケーションを変更すること無しに、暗号化が行える点が優れているが、通信確立までの処理オーバーヘッドが大きく、ホスト-サーバ間、またはホスト-ホスト間の通信スループットが劣化するという問題点があった。

10

【0010】

IPsecではAES等の共通鍵暗号を使用し、ネットワーク機器で暗号化処理を実施する手法が利用されているが、いくつかの問題点が存在する。一つは、通信開始時における設定手順が複雑な点である。IPsecの通信開始時におけるシーケンスを図2、図3に示す。IPsecでは、共通鍵暗号を使用してパケットデータを暗号化するため、共通鍵を事前に共有する必要がある。共通鍵情報、通信ノード間の認証を行うために、使用するパラメータを提案、鍵情報の交換をする。

【0011】

図3はIPsecにおけるIKE(Internet Key Exchange)のフェーズ1の通信シーケンスである。フェーズ1では、継続して実施する次の通信シーケンス(フェーズ2)で行うIPsecに必要な共通鍵を安全に交換するためにSA(Session Association)を確立する。図4はIKEのフェーズ2の通信シーケンスである。フェーズ2では実際にIPsecで使用するパラメータや鍵情報を交換する。安全な通信路を確保した後に、鍵を共有する方であるため、フェーズが2段階に別れ、通信開始時までのコストが大きくなり、通信スループットを低下させる原因にもなっている。一方、共通鍵を第三者に予測される危険性が少なくするため、ホスト側では鍵情報を定期的に交換する必要があるが、上記の手法を用いる必要がある。

20

【0012】

これに対して、SDN内のスイッチ(OFS)、コントローラ(OFCC)は、予め決められた端末との接続を対象とし、かつ端末接続時には、認証を行うと共に、規定された仕様を満足していないパケットは異常と見なし、スイッチ(OFS)で廃棄する処理を組み込むことが容易である。このため、第三者による盗聴は困難であると共に、不正侵入等による(スイッチ動作を規定する)ファイルの改竄を起こす危険性は少ない。

30

【先行技術文献】**【特許文献】****【0013】****【特許文献1】**特許第4385111号公報**【特許文献2】**特許第4296304号公報**【非特許文献】****【0014】****【非特許文献1】**K. K o p o n e n e t a l . " O n i x : A D i s t r i b u t e d c o n t r o l P l a t f o r m f o r L a r g e - s c a l e P r o d u c t i o n N e t w o r k s , " I n t h e P r o c . o f t h e 9 t h U S E N I X S y m p o s i u m o n O p e r a t i n g S y s t e m D e s i g n a n d I m p l e m e n t a t i o n (O S D I 1 0) , V a n c o u v e r , C a n a d a , O c t o b e r 2 0 1 0**【非特許文献2】**A . T o o t o c i a n a n d Y . G a n j a l i , " H y p e r F l o w : A D i s t r i b u t e d C o n t r o l P l a n e f o r O p e n F l o w , " I n t h e P r o c . O f N S D I I n t e r n e t N e t w o r k M a n a g e m e n t W o r k s h o p / W o r k s h o p o n R e s e

40

50

arch on Enterprise Networking (INM/WREN),
San Jose, CA, USA, April 2010

【発明の概要】

【発明が解決しようとする課題】

【0015】

本発明は、ホスト間またはホスト - サーバ間での暗号化及び復号化を行う方式から脱却し、SDNの通信ノード内のスイッチで暗号化等の処理を自律的に、かつ第三者には秘密の方法で実施することにより、第三者に対する通信の機密性を確保するとともに、ユーザ端末の負荷を減らすことを目的とする。

【課題を解決するための手段】

【0016】

本発明に係るネットワーク制御システム及びネットワーク制御方法は、SDNの通信ノード内のスイッチで暗号化等の通信の機密性を確保するための処理を行い、スイッチと専用通信ネットワークで接続されたSDNのコントローラにおいてスイッチの行った処理に関するパラメータやメタデータを管理する。

【0017】

具体的には、本発明に係るネットワーク制御システムは、

コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御システムにおいて、

前記スイッチは、ユーザ端末からの通信データを受信すると、当該通信データを複数の断片データに分割して断片データの配列順を変更し、配列順を変更後の各断片データを、出力経路を制御するためのフローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに出力し、

前記コントローラは、変更後の前記断片データの配列順を格納する。

【0018】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ端末から通信のデータを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて前記スイッチで行った符号化を復号化するために必要なメタデータを前記コントローラに出力し、前記コントローラは、前記スイッチで符号化された通信データを復号化するために必要なメタデータをさらに格納してもよい。

【0019】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化してもよい。

【0020】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータを当該ユーザ端末へ送信し、当該ユーザ端末は、前記スイッチから取得するメタデータを用いて前記通信データ又は前記断片データを復号化してもよい。

【0021】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ端末から通信データの取得要求を受信すると、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信してもよい。

【0022】

本発明に係るネットワーク制御システムでは、前記スイッチは、ネットワークに対して要求するセキュリティサービス種別を、ユーザ端末からの前記通信データに含まれるフラグ種別情報から識別し、前記セキュリティサービス種別がバックアップ用のサービスであ

10

20

30

40

50

る場合、前記フローテーブルに従った1以上のストレージ端末に向けて、前記断片データ
を出力するとともに、前記専用通信ネットワークを用いて前記断片データの送信先を前記
コントローラに出力し、前記コントローラは、前記断片データの送信先をさらに格納して
もよい。

【0023】

具体的には、本発明に係るネットワーク制御方法は、コントローラからのソフトウェア
制御を用いてスイッチの出力経路を制御するネットワーク制御方法において、ユーザ端末
からの通信データを受信した前記スイッチが、出力経路を制御するためのフローテーブル
を参照し、当該通信データを複数の断片データに分割して断片データの配列順を変更し、
配列順を変更後の各断片データを前記フローテーブルに従った出力経路に向けて出力する
とともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コント
ローラに格納するデータ送信手順を有する。

10

【0024】

本発明に係るネットワーク制御方法では、前記データ送信手順において、ユーザ端末
からの通信データを受信した前記スイッチが、ユーザ端末からの通信データを符号化して当
該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複
数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワ
ークを用いて当該スイッチで符号化された通信データを復号化するために必要なメタデー
タを前記コントローラに格納してもよい。

【0025】

本発明に係るネットワーク制御方法では、ユーザ認証の完了したユーザ端末から通信デ
ータの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信
するデータ受信手順を、前記データ送信手順の後にさらに有し、前記データ受信手順にお
いて、当該スイッチが、前記コントローラに格納されている前記メタデータに従って前記
通信データ又は前記断片データを復号化してもよい。

20

【0026】

本発明に係るネットワーク制御方法では、ユーザ認証の完了したユーザ端末から通信デ
ータの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信
するデータ受信手順を、前記データ送信手順の後にさらに有し、前記データ受信手順にお
いて、当該スイッチが、前記コントローラに格納されている前記メタデータを当該ユーザ
端末へ送信し、前記スイッチからメタデータを取得した当該ユーザ端末が当該メタデー
タを用いて前記通信データ又は前記断片データを復号化してもよい。

30

【0027】

本発明に係るネットワーク制御方法では、ユーザ認証の完了したユーザ端末から通信デ
ータの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信
するデータ受信手順を、前記データ送信手順の後にさらに有し、前記データ受信手順にお
いて、当該スイッチが、当該通信データを構成する複数の断片データの配列順を前記コント
ローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を
、当該ユーザ端末へ送信してもよい。

【0028】

本発明に係るネットワーク制御方法では、前記データ送信手順において、ユーザ端末
からの通信データを受信した前記スイッチが、ネットワークに対して要求するセキュリティ
サービス種別を当該通信データに含まれるフラグ種別情報から識別し、前記セキュリティ
サービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った1以
上のストレージ端末に向けて、前記断片データを出力するとともに、専用通信ネットワ
ークを用いて前記断片データの送信先を前記コントローラに格納してもよい。

40

【0029】

なお、上記各発明は、可能な限り組み合わせることができる。

【発明の効果】

【0030】

50

本発明によれば、ホスト間またはホスト - サーバ間での暗号化及び復号化を行う方式から脱却し、SDNの通信ノード内のスイッチで暗号化等の処理を自律的に、かつ第三者には秘密の方法で実施することにより、第三者に対する通信の機密性を確保するとともに、ユーザ端末の負荷を減らすことができる。

【図面の簡単な説明】

【0031】

【図1】IPsecの利用形態の第1例を示す。

【図2】IPsecの利用形態の第2例を示す。

【図3】IPsecにおけるIKEフェーズ1の通信シーケンスの一例を示す。

【図4】IPsecにおけるIKEフェーズ2の通信シーケンスの一例を示す。

10

【図5】実施形態1に係るネットワーク制御システムの一例を示す。

【図6】オープンフロースイッチを用いたSDNの基本構成例を示す。

【図7】アクションに指定可能な制御コマンドの一例を示す。

【図8】オープンフローで定義可能なヘッダ情報の一例を示す。

【図9】実施形態1に係る受信手順における第1のシーケンスを示す。

【図10】実施形態1に係る受信手順における第2のシーケンスを示す。

【図11】実施形態1に係るOFCとOFSの制御シーケンスの一例を示す。

【図12】チャレンジレスポンス方式による処理フローの一例を示す。

【図13】認証が成功した場合の通信シーケンスの一例を示す。

【図14】実施形態3に係る通信システムの第1の形態例を示す。

20

【図15】実施形態3に係る通信システムの第2の形態例を示す。

【図16】実施形態4に係る通信システムの第1の形態例を示す。

【図17】フラグ情報の記載方法の一例を示す。

【図18】実施形態4におけるOFS3の処理フローの一例を示す。

【図19】OFSがOFCにメタデータを問い合わせるシーケンスの一例を示す。

【図20】OFSにおけるバッファ処理の一例を示す。

【図21】OFSにおける符号化処理フローの一例を示す。

【図22】OFSにおけるシャッフリング処理フローの一例を示す。

【図23】OFSにおける復号処理の一例を示す。

【図24】実施形態5に係る通信システムの形態例を示す。

30

【図25】実施形態6に係る通信システムの形態例を示す。

【発明を実施するための形態】

【0032】

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

【0033】

本願発明のセキュリティネットワーク制御システムは、ソフトウェア制御を用い、スイッチの出力経路の制御に必要な情報を提供するSDNコントローラ、および当該SDNの指示に基づいて動作するスイッチが共同して、新たにスイッチ内でファイルバックアップ処理をセキュアに実現する上で必要となるメカニズムを、提供できる手段を開示する。

40

【0034】

具体的には、制御用パケットに含まれるフラグ種別情報に基づいて、SDNスイッチが、ユーザから送出される要求パケットデータのセキュリティ上のサービスレベルの種別を判定し、当該レベルに適合した符号化処理（一体化処理等の暗号化、分割、シャッフリング処理および複製等）を行い、また復元時には、上記と逆の動作手順を用いることにより、当該のファイルバックアップサービスが実現できる。

50

【 0 0 3 5 】

本方式で開示する技術を活用することにより、従来 I P s e c 等を用いてセキュリティを確保できる場合の通信サービスと同等以上のセキュリティと安全性を、当該スイッチに上記の符号化および復号化処理を行う機能を内蔵させることにより実現し、ユーザ端末からの通信スループットも向上できる。また、符号化処理に用いるパラメータと、復号処理に必要なデータ（以下、メタデータと呼称する）を、前述の I K E と同様にネットワーク機器間で共有できる。本方式では、S D N の一例として活用されるオープンフロー用のネットワークプラットフォームを用い、コントローラ（O F C）がメタデータを管理し、スイッチ（O F S）と O F C がメタデータを共有することにより、セキュアな通信を実現できる。

10

【 0 0 3 6 】

O F C は O F S あるいは他の O F C のみと接続されているため、O F S および O F C のみにより、メタデータを共有する専用通信ネットワークが必要であり、この条件により共通鍵を共有するための安全なネットワークを確立する I K E のフェーズ 1 の手順を省略することが可能となる。ここで、専用通信ネットワークは、仮想的専用通信ネットワークでもよいし、物理的専用通信ネットワークでもよい。一般に、メタデータのデータサイズは、ファイル送受信の対象となるパケットのデータサイズと比べて、2 ケタ以上に小さいため、上記の専用通信ネットワークの帯域は十分に小さい帯域の通信回線を用いて経済的に構築できる。また、従来から使用されている I P s e c 等の通信形態では、データ通信と共通鍵の共有を同じネットワーク回線を用いるため、頻繁に鍵を交換することにより、ユーザデータの通信のスループットが低下するが、本方式ではメタデータ等の制御データを配信するための通信路とユーザのファイルデータ配信のためのデータ通信路とを分離しているため、メタデータと符号化処理されたパケットを用いた通信データを並列に送受信できる。また、頻繁にメタデータの交換が生じる場合でも、ダイナミックに O F C の負荷を調整できる方式が適用可能であるため、データ通信のスループットに影響を与えることはない。

20

【 0 0 3 7 】

本発明は、クラウド等のコンピュータリソースとの通信やデータのバックアップを実行する際のネットワーク制御装置又はオープンフロー制御機構（パケット処理制御機構）を活用することにより、ネットワーク内のスイッチをインテリジェント化することにより、安全な通信を実現する。また本発明は任意の S D N コントローラに適用できるが、以下の実施形態では S D N コントローラの一例として、O F S および O F C について説明する。

30

【 0 0 3 8 】

（実施形態 1）

図 5 に、本実施形態に係るネットワーク制御システムの一例を示す。本実施形態に係るネットワーク制御システムは、コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御する S D N を用いる。本実施形態では、S D N の基本構成の一例として、一般的なオープンフロースイッチの構成を示す。

【 0 0 3 9 】

オープンフロースイッチでは、従来のルータ等のネットワーク機器が持つ機能を、オープンフローコントローラ（以下、O F C と記す）4 とフローテーブルの内容に基づいてパケットを転送するオープンフロースイッチ（以下、O F S と記す）3 とに分離されている。O F C 4 は、O F S 3 内のスイッチ 3 2 へのパケット入出力処理動作やセキュリティ機能の制御を行う。O F S 3 は、スイッチ 3 2 と、フローテーブル 3 1 を備える。スイッチ 3 2 は、O F C 4 の指示に従い、入力トラヒックのパケットデータのフラグ情報に基づいて、パケットに対するルーティングの処理（アクション）や暗号化等の符号化処理を行う。

40

【 0 0 4 0 】

ネットワーク管理者は、入力トラヒックのパケットに付与されたフラグ情報の種別により、セキュリティ機能を規定し、当該パケットの暗号化、分割化、シャフリング等の秘匿化方法および、経路設定方法等のアクションを、事前に、フローテーブル 3 1 内のフロー

50

エントリーにインストラクションとして登録する。このフローエントリー内のインストラクション等のパケット処理に関わる制御内容は、OFS3の外部にあるOFC4からのソフトウェアにより管理される。OFS3は登録されたフローテーブル31に対して、パケットデータの処理に関わるマッチングルールを適用して、マッチしたフローエントリーに示された転送処理を当該パケットに対して行う。OFS3は、自身のフローテーブル31にて未定義のトラフィックフローが到着した場合、OFC4に未定義フローに対する動作(アクション)を問い合わせる場合がある。OFC4は未定義フローに対する動作を、当該OFS3に指示する。OFS3に入力されるパケット処理用のフラグに対して、予めフローテーブル31(インストラクション等のアクションリスト)に未登録のパケット識別フラグがある場合には、OFS3とOFC4との間で、制御メッセージのやり取りが発生する。

10

【0041】

図6に示すSDNにおけるネットワーク制御を考えた場合、OFC4の位置する制御レイヤ6の下位は、インフラストラクチャーレイヤ5と位置付けるのが一般的である。この場合、レイヤ5の上位に、OFC4を包含する制御レイヤ6があり、OFC4の上位には、ネットワークアプリケーションレイヤ7を配備する方法が一般的である。この場合、ネットワークアプリケーションレイヤ7内の各種アプリケーション71は、OFC4の上位に存在し、新しいネットワーク制御用のアプリケーションソフトウェアを導入する場合や、ネットワーク制御用の経路計算アルゴリズムを変更する場合など、通常のネットワーク管理や監視機能を更改する場合などに活用する。SDNに関する標準化はAPIも含め、

20

まだ十分には進んでおらず、各OFC4の実装に依存してアプリケーション71も実装されているのが現状である。本発明における記述では、既存のOFC4とアプリケーションが1つの物理または仮想マシン上に実装されている場合において、クラウドの等の仮想環境を活用することもできる。将来的にOFC4とアプリケーション71間のAPIが定まった場合は、最も適切なアプリケーションを適用することも実施形態として有効である。

【0042】

図7にスイッチで、アクション用に指定可能な制御コマンドの例を示す。図8にオープンフローで定義可能なヘッダ情報の例を示す。OFS3は、制御コマンドの格納されたアクションテーブルを備え、制御コマンドおよびヘッダ情報の種別を活用して、前記の一連の処理をネットワーク内のスイッチ32に実装することにより、ユーザ端末11がデータ

30

【0043】

バックアップを目的とした暗号化通信を行う場合に必要となる処理負荷を軽減することができる。さらに、セキュアな通信を、OFS3及びOFC4というネットワーク内機器の制御のみで実現することが可能となる。

一方、本実施形態に係るネットワーク制御方法は、データ送信手順と、データ受信手順とを順に有する。データ送信手順において、ユーザ端末11からの通信データを受信したOFS3が、分割処理を行った後にシャッフリング処理を行うとともに、分割処理及びシャッフリング処理の情報を、ユーザ端末11からの通信データのメタデータとしてOFC4に格納する。ここで、分割処理は通信データを複数の断片データに分割する処理をいい、シャッフリング

40

処理は断片データの配列順を変更することをいう。分割処理の情報は、通信データをどのように分割したかの情報であり、例えば、各断片データのデータ量であったり、等分割するために必要となるパディング情報の容量の大きさ等である。シャッフリング処理の情報は、断片データの配列順をどのように変更したかの情報である。データ受信手順においては、OFS3又はユーザ端末11が、OFC4に格納されているメタデータに従って断片データを配列しなおす。これにより、ユーザ端末11から元の通信データに復元する。

【0044】

データ送信手順では、OFS3が、ユーザ端末11からの通信データを符号化して通信データを複数の断片データに分割するか、或いはユーザ端末11からの通信データを複数

50

の断片データに分割して各断片データを符号化することが好ましい。この場合OFS3で行った符号化処理をされたデータを復号化するために必要なデータをメタデータとしてOFC4に格納する。

【0045】

図9に、本実施形態に係る受信手順における第1のシーケンスを示す。

OFS3は、断片データを受信すると、受信データがある旨の受信メッセージを、宛先のユーザ端末11に通知する。

ユーザ端末11が通信データを受信する際には、まず、ユーザ端末11はOFS3からの認証を受ける。例えば、ユーザ端末11がOFS3へ認証要求を行い、OFS3がOFC4に格納されている認証情報に基づいてユーザ端末11の認証を行うことが好ましい。

10

OFS3は、ユーザ端末11の認証の完了後にデータの復元要求メッセージをユーザ端末11から受信すると、OFC4に格納されているメタデータを用いて断片データを元の通信データに復元し、ユーザ端末11へ送信する。このとき、OFS3がユーザ端末11からの通信データを符号化している場合は、断片データの再配列と共に復号化も行う。

これにより、ユーザ端末11は復元した通信データを受信する。また、宛先となるユーザ端末が認証を要求されずに、復元した通信データをOFS3から受信できる通信手順も同様に可能であることは言うまでもない。

【0046】

図10に、本実施形態に係る受信手順における第2のシーケンスを示す。

20

OFS3は断片データを受信すると、断片データを宛先のユーザ端末11に送信する。

ユーザ端末11が元の通信データを受信する際には、まず、ユーザ端末11はOFS3からの認証を受ける。OFS3は、ユーザ端末11の認証の完了後にデータの復元要求メッセージをユーザ端末11から受信すると、OFC4に格納されているメタデータを取得し、ユーザ端末11へ送信する。

ユーザ端末11は、メタデータを用いて断片データを元の通信データに復元する。このとき、OFS3がユーザ端末11からの元の通信データを符号化している場合は、当該メタデータを用いて、断片データの再配列化と共に復号化を行うことも可能である。

【0047】

このように、本実施形態に係る発明は、図11に示すように、ユーザ端末は、暗号化等に関わる処理には関与せず、これらはネットワーク内のOFS3とOFC4を用いることにより、図3、図4に示す通信シーケンスに比べ、大幅にオーバーヘッドを削減して、その分だけユーザ端末の通信スループットを向上できる。したがって、本実施形態に係るシステムは、ホスト側ではセキュリティ機能向上のための暗号処理等を、一切行うことなく、代わりにSDN内のスイッチおよびコントローラが共同して、セキュリティ上の保証を行う安全配信（通信）の実現メカニズムを提供することができる。

30

【0048】

（実施形態2）

本実施形態に係る発明は、ユーザ端末11のファイルバックアップにも適用可能である。具体的には、ユーザ端末11からSDN内のスイッチ（OFS3）へ送られたファイルバックアップのための、ユーザ要求パケットデータに含まれる、フラグ種別情報により、対応するアクションテーブルがアクセスされる。アクションテーブル内の情報に基づいて、スイッチは当該のセキュリティを確保するために、各種の符号化処理（暗号化処理等を含む）を実施し、その後、スイッチ内で分割、シャッフリング及び複製処理を行い、目的の出側方路の先にあるストレージへ格納することにより、第三者によるデータの盗聴時の解読性を困難にすることができる。すなわち、ホスト-ストレージ間やホスト-サーバ間の通信において、SDNのスイッチが自律的に暗号化を行うことが可能になる。

40

【0049】

端末側もしくはサーバ側の通信端末ではなく、通信ノード内のスイッチで暗号化・復号化を行うため、ホストまたはサーバが、暗号化または復号化に使用する鍵を管理する必要

50

はなくなり、利便性の向上と安全性の向上の双方を同時に実現できる。この理由は、スイッチやコントローラが当該の符号化処理アルゴリズムの実行に必要な鍵を管理することにより、悪意のある第三者に対する機密性を高めることができるからである。一般的に、ユーザ端末や、サーバに比べて、OFC4、OFS3等のネットワーク内の制御装置や通信ノードは、外部からのアクセスが困難であり、これらのネットワーク機器に対する制御は、通常はインターネットから分離して運用されることが前提となるからである。一方、ユーザ端末11やサーバはメール送信やインターネットを含めた外部へのサービス公開を行うことが多く、遠隔制御用プログラムの稼働や、不特定多数のユーザ端末との直接的なデータ通信の機会があるため、不正アクセス等により、安全性が損なわれる可能性が高い。

【0050】

具体的には、サービスを利用するユーザ端末11は、バックアップ要求メッセージをOFS3に送信する。OFS3は、認証処理後にバックアップ対象となる元の通信データを符号化処理を行い、その後、メタデータをOFC4に格納する。その後、宛先に対応するストレージに送信する。OFC3は、以後、復元要求があった場合は、OFC4に格納されたメタデータを回収し、これを使用することにより、復号処理を行うことができる。

【0051】

なお、ユーザ端末11が故障等が生じたことにより、バックアップされた断片データの回収ができなくなった場合には、別のユーザ端末11を使用し、適切な認証手順を経て、バックアップ先からの断片データの回収を実現することが可能となる。悪意あるユーザによって、不正にデータを復元されることを防ぐために、元の通信データに復元する際には、認証が必要であることは言うまでもない。認証方式はどのような方式を用いても構わない。以下に、チャレンジレスポンス方式による処理フローの一例を図12に示す。

【0052】

ユーザ端末11は、認証要求メッセージをOFS3に送信する。OFS3は受信した認証要求メッセージをOFC4に転送する。認証要求メッセージを受信したOFC4は、チャレンジと呼ばれるランダムな値を生成し、OFS3に送信する。OFS3はチャレンジをユーザ端末11に転送する。

ユーザ端末11は、受信したチャレンジと、認証に必要な情報で、レスポンスと呼ばれるハッシュ値を生成し、レスポンスをOFS3に送信する。ここで必要な情報は、ユーザIDとパスワードを含むことが好ましい。この場合、ユーザIDとパスワードは、事前にOFC4の認証データベースに保存しておくことが好ましい。OFS3はレスポンスをOFC4に転送する。

レスポンスを受信したOFC4は、ユーザ端末11と同様に送信したチャレンジと、ユーザIDとパスワードから、照合用のレスポンスを生成し、受信したレスポンスと生成したレスポンスとのバイナリコードを比較し、これらが一致すれば、認証が成功した旨を伝えるべく、認証応答を返送する。一致しない場合には、その旨（認証が失敗した旨）を伝える認証応答を返送する。

【0053】

認証が成功した場合、ユーザ端末11は、復元要求メッセージをOFS3に送信する。認証が成功した後の、ユーザ端末11とOFS3、OFC4の間の通信シーケンスをまとめて図13に示す。図13にはOFS3とOFC4の間およびOFS3とストレージ12の間におけるハッシュ値の照合を併せて示す。

OFS3は、認証が成功したユーザ端末11からの復元要求メッセージの場合には、メタデータの問い合わせをOFC4に対して行う。OFS3は、OFC4からハッシュ付きのメタデータを回収し、データのハッシュ値の照合が完了した後に、ストレージ12宛に、断片データの回収を行うための送信要求を送信する。なお、ユーザ端末11からの認証要求における認証が失敗した場合には、OFS3はユーザ端末11からの復元要求メッセージのパケットを破棄する。

ストレージ12は復号フラグを含んだヘッダ情報と保存された断片データのハッシュ値を付加したデータをOFS3に送信する。OFS3は、ストレージ12から受信したハッ

10

20

30

40

50

シュ値の照合を行い、メタデータをもとに復号処理を行い、復号後の元の通信データをユーザ端末11に送信する。

以上述べた手順により、ユーザ端末11が要求した、ストレージ12にバックアップされた断片データは、OFS3によって復号され、ユーザ端末11で回収できる。

【0054】

(実施形態3)

実施形態1の通信システムにおける第1の形態例を図14に示す。第1の実施形態はサービスを利用するユーザ端末11、ストレージ12、オープンフロースイッチ(OFS)3、及びオープンフローコントローラ(OF C)4を備える。ユーザ端末11は、サーバや、パーソナルコンピュータ、携帯端末などの重要データを保持し、記憶デバイスの故障や災害などの危険に遭遇する可能性がある。ストレージ12は、ネットワーク上のユーザ端末11からアクセス可能なデバイスである。例えば、NAS(Network Attached Storage)やファイルサーバ、クラウドストレージなどが該当する。

10

【0055】

OFS3はサービス利用端末11及びストレージ12の間の接続を確立するためのスイッチを含む通信ノードであり、通常OFSにおける目的方路へのルーティングの機能に加え、本発明で開示した、暗号化等を含む符号化処理と復号化処理の機能を実装している。OFS3は、ファイルのバックアップ処理等の通信サービスを実施するため、ユーザ端末11から、バックアップしたい通信データを受け取った場合は、当該の符号化処理を行い、ストレージ12に格納する。ユーザ端末11から復元要求があった場合には、ストレージ12との接続を行い、その後、必要なファイルを読み出し後に、OFS3で復号処理を行い、当該ユーザ端末11に復元結果を転送する。

20

【0056】

OF C4は、OFS3を管理するコントローラであり、ストレージ12と接続を確立する。OF C4はOFS3からバックアップ要求のメッセージを受信後、OFS3での符号化に必要となる、アクションテーブルに格納する情報をOFS3に返送する。この情報は、例えばストレージ12はどのポートと接続されているかや、符号化・復号化の処理に必要な暗号化用パラメータなどを含む。

【0057】

通信ネットワーク21、22、5は通信可能な情報伝達網であり、例えばLAN(Local Area Network)も含まれる。通信ネットワーク5は、OF C4が、OFS3を制御する通信のみに用いる。本実施形態の例では、通信ネットワーク5は、VPN(Virtual Private Network)通信又はSSL(Secure Socket Layer)暗号通信を用いたものであることが好ましい。本実施形態の例では、データセンタ内で適用する例について説明するが、この例に限らず、インターネットを含めた各種ネットワークにも部分的に適用可能である。

30

【0058】

ユーザ端末11は、バックアップしたいデータファイルをUDP/IPを用いて、ストレージ12に格納することが好ましい。例えば伝送回線の品質が高い場合にはUDPを用いる場合が適しているが、この方法に限定されるものではなく、例えば、ホスト間の通信にTCPを用いて実施することも可能である。ユーザ端末11は、バックアップしたいデータを、ストレージ12に送信するために、IPヘッダおよびUDPヘッダ(あるいはTCPヘッダ)を付加するが、同時に、ネットワーク内のスイッチでの、セキュアなバックアップサービスの実現に対応した符号化処理用のフラグ情報をヘッダ内に記載する必要がある。スイッチ内における、バックアップ対象となるデータファイルの処理形態は、ユーザが要求するセキュリティの重要度に基づいて、フラグ情報種別を変更することにより、対処が可能である。例えば、セキュリティの重要度の低いデータファイルは、暗号化せずに平文のまま送信し、セキュリティ上の重要度の高いデータファイルであれば、送信前にAES等で、暗号化してからファイルを送信することも可能である。セキュリティレベルの詳細については、特許文献1に開示されている。

40

50

【 0 0 5 9 】

図 1 5 は本実施形態における第 2 の形態例を示しており、ユーザ端末 1 1 が 1 1 a から 1 1 b の全てを含む場合を想定している。この 1 1 a から 1 1 b の中の一つから、復元要求がある場合に、当該ユーザ端末とストレージ 1 2 との接続を行い、その後、必要なファイルは、1 1 a から 1 1 b のどれからでも読み出しできる場合のシステム構成例を示している。

O F S での復号処理や、当該ユーザ端末に復元結果を転送する方法は、実施形態 1 の場合と同様である。

【 0 0 6 0 】

(実施形態 4)

実施形態 2 の通信システムに係る第 1 の形態例を図 1 6 に示す。本実施形態ではストレージ 1 2 が 1 2 a からストレージ 1 2 d の 4 つのストレージから構成される例を示す。O F C 3 の処理フローは、後述する図 1 8 のステップ S 1 0 9 において、ヘッダ情報を付加して送信する際に、ストレージ 1 2 a ~ 1 2 d の 4 つのストレージに同一パケットを、複製して送信することが、オープンフローを用いて実装可能である。O F C 4 からは、p a c k e t _ o u t メッセージ内にストレージ 1 2 a ~ 1 2 d が接続されているポートに対し、パケットを送出するように指示をすることで実現できる。

【 0 0 6 1 】

また復元処理の際には、O F S 3 が、O F C 4 から受信したメタデータから、ストレージ 1 2 a ~ 1 2 d に対して、データの送信要求を送出し、どれか一つのストレージから断片データが受信できた場合には、復号処理を開始し、復号結果の元の通信データをユーザ端末 1 1 に送信する。ストレージ 1 2 a ~ 1 2 d に対し、同じように符号化された冗長データをバックアップすることにより、信頼性を高めることができる。ストレージ 1 2 a ~ 1 2 d のうちのどれか一つが稼働していれば、復元が可能となるからである。

【 0 0 6 2 】

上記の冗長化の例では、ストレージ端末の耐障害性を高めることができるが、分散方法を工夫することにより、セキュリティ強度を高めることも可能である。例えば、暗号化したデータの半分を、ストレージ 1 2 a、1 2 b に、もう半分をストレージ 1 2 c、1 2 d にバックアップするように p a c k e t _ o u t メッセージを用いて、対応するパラメータ設定を行うことにより、ストレージ 1 2 a か 1 2 b のどちらかが正常であり、かつストレージ 1 2 c か 1 2 d のどちらかが正常である場合に限り復元することができる。この場合、ストレージ 1 2 a と 1 2 b のみでは復元できないため、悪意あるユーザにより、ストレージ 1 2 a か 1 2 b のどちらかがハッキングされ、かつ、ストレージ 1 2 c か 1 2 d のどちらかがハッキングされる条件が揃わない場合以外は、元の通信データの復元は不可能となる。この場合、O F S の中にバッファリングされるパケットデータは、2 分割され、それぞれが別のストレージに格納される。この例の他に、セキュリティのレベルに応じて適切に分割数を大きくとることも同様に可能であることは言うまでもない。

【 0 0 6 3 】

上記の一連の実施形態において、使用されるフラグ情報の記載方法を図 1 7 に示す。図 1 7 には I P ヘッダのオプション領域を使用して、符号化処理を行うフラグ種別、復号処理を行うフラグ種別、符号化、復号処理共に、必要のない、通常のパケット処理を行うフラグの 3 種類のフラグ情報のどれかを記載することにより、セキュリティ機能の異なる通信サービスの要求を実現できる。I P ヘッダ長は 4 の倍数バイト長になるためオプション領域は 4 バイトとなる。スイッチ内において符号化処理を行う必要のあるパケットに関しては、例えばオプション領域のビット列を、0 x 8 0 0 0 0 0 0 0 とする。復号処理が必要なパケットは、0 x 4 0 0 0 0 0 0 0 とする。符号化、復号処理の必要ない通常のパケットは、0 x 0 0 0 0 0 0 0 0 もしくは、オプション領域がないものとする。このように、I P ヘッダのオプション領域を用い、3 種類のパケットを識別するが、この方式に限定されるものではない。例えば、高いセキュリティのレベルのバックアップを実現したい場合には、そのレベル種別数に応じてフラグ種別を設けることで対処が可能である。各種の

10

20

30

40

50

セキュリティレベルの内容の例に関しては、特許文献 1 に開示された技術が対象となる。ユーザ端末 1 1 は、ストレージ 1 2 に送信する際に、上述した IP ヘッダのオプション領域に 0 x 8 0 0 0 0 0 0 0 を設定する。その他のヘッダ情報は、通常の UDP / IP を用いた通信と同様に設定する。この場合の OF S 3 の処理フローを、図 1 8 に示す。

【 0 0 6 4 】

パケットを受信した OF S 3 (ステップ S 1 0 1) は、ヘッダ内容を解析し、符号化処理を行うパケットか、または復号処理を行うパケットか、または通常のパケットか、を上記の IP ヘッダのオプションのフラグで識別する (ステップ S 1 0 2)。通常のパケットの場合は通常処理 S 1 0 3 を行い、パケットを送出する (ステップ S 1 0 3)。符号化処理が必要な場合はステップ S 1 0 4 ~ S 1 1 0 を行い、復号処理が必要な場合はステップ S 1 1 1 ~ S 1 1 7 を行う。

10

【 0 0 6 5 】

ステップ S 1 0 3 では、例えば、ルーティング処理やフォワーディング処理を行う。

ステップ S 1 0 4 ではメタデータを読み込み、ステップ S 1 0 5 ではバッファ処理を行い、ステップ S 1 0 6 では符号化処理を行い、ステップ S 1 0 7 では分割処理を行い、ステップ S 1 0 8 ではシャッフリング処理を行い、ステップ S 1 0 9 ではヘッダを付加してパケットを送信し、ステップ S 1 1 0 では復号化に必要なメタデータを OF C 4 へ送信する。

ステップ S 1 1 1 では当該のメタデータを読み込み、ステップ S 1 1 2 ではバッファ処理を行い、ステップ S 1 1 3 ではシャッフリングされた順番を元に戻し、ステップ S 1 1 4 では復号処理を行い、ステップ S 1 1 5 では分割処理を行い、ステップ S 1 1 6 ではヘッダを付加してパケットを送信し、ステップ S 1 1 7 では復号の完了を OF C 4 に知らせる。

20

【 0 0 6 6 】

符号化処理の場合 (S 1 0 4 ~ S 1 1 0)、符号化処理を行うための各種パラメータ (以後、メタデータと呼称する) を、未設定であることが判断された場合は、OF C 4 に問い合わせる。OF S 3 と OF C 4 の間のメタデータ問い合わせ手順に関する具体的な通信シーケンスを図 1 9 に示す。OF S 3 は未知のパケットが届くと、OF C 4 に packet__in メッセージと呼ばれる未知のパケットのヘッダ情報等を OF C 4 に問い合わせる。packet__in メッセージを受け取った OF C 4 は、受け取った情報をもとに、OF S 3 にメッセージを返送し、未知のパケットの操作を指示し、OF S 3 はフローテーブル 3 1 に指示された操作に従って当該未知のパケットの設定を行う。例えば、パケットを特定のポートから送出的る操作を OF C 4 が指示する場合、OF C 4 は packet__out メッセージを OF S 3 に送る。OF S 3 が持つフローテーブル 3 1 に情報を追加する操作を OF C 4 が指示する場合は、flow__mod メッセージを併せて OF S 3 に送る。

30

【 0 0 6 7 】

本実施形態では、上記の OF S 3、OF C 4 のやりとりに、符号化、復号化に必要なメタデータを送受信するメッセージを定義する必要がある。パケットを受信した OF S 3 は、packet__in メッセージとメタデータの問い合わせを OF C 4 に行う。packet__in メッセージとメタデータの問い合わせを受信した OF C 4 は、ルーティングの決定や、送出先のポートの決定などの、従来のルータ処理に加え、設定すべきメタデータを OF S 3 に送る。OF S 3 は受け取った情報をもとに、バッファ処理、符号化処理、分割処理、シャッフリング処理、パケットの送出手理を行い (ステップ S 1 0 5 ~ S 1 0 9)、復号処理に必要なメタデータを OF C 4 に送信する。OF C 4 は受信したメタデータを復号処理が行われるまで保持する。

40

【 0 0 6 8 】

バッファ処理時 (ステップ S 1 0 5) 及び符号化処理 (ステップ S 1 0 6) のフローの一例を、図 2 0、図 2 1 に示す。メタデータに設定されたパラメータ変数を取り出す (S 2 0 1)。パラメータ変数には、符号化処理用のバッファに格納されたパケット数 N、パ

50

ッファするパケット数 M 、 MSS (Maximum Segment Size)、タイムアウト設定時間 T 等が存在する。 MSS に関しては、通信ネットワーク上で、IPフラグメンテーションを起こさないための最大ペイロード長を指定することが好ましい。

パケットからUDPペイロードを取り出し、符号化処理用のバッファにバッファリングする (S204)。符号化処理のバッファに M 個のパケットをバッファリングした後、バッファリングしたデータサイズが $MSS \times M$ サイズ未満だった場合、 $MSS \times M$ サイズにパディング処理を行い (S209)、図21に示す符号化処理において $MSS \times M$ サイズに合わせた後で当該データを符号化処理する。ここでパディング処理でパディングするビット列は、乱数列であることが好ましい。

また、次のパケットを受信するまでに、タイムアウト設定時間 T が過ぎた場合 (S208においてno)、上記と同様にパディング処理を行い (S209)、図21に示す符号化処理を行う。タイムアウト規定を設ける理由は、パケットがこれ以上のパケットの受信が生じないと推定される場合や、一定の遅延時間を超える状況が発生した場合には、バッファリングしているパケットが、OFS3からまとめて送出されない可能性があるからである。

【0069】

以上の処理を繰り返し、到着パケットに対して、OFS3はステップS105のバッファリングを行う。例えば、最も簡単な一例として、 $M = 3$ 、 $MSS = 1472$ 、 $T = 1\text{ms}$ とした場合、パケットを3個分まで、バッファリングする。符号化処理用のバッファに格納されたパケット数 N が、3になるまでOFS3はバッファリングし (S105)、符号化処理を行う。ただし、2個のパケットを受信した後、3個目のパケットを受信するまでに、 1ms 以上の時間がかかった場合、3個目のパケット分のサイズになるまで、OFS3がパディングして符号化処理を行う。

【0070】

図18に示す符号化処理 (ステップS106) は、上記のバッファ処理で、符号化処理用バッファにバッファリングされた通信データに符号化を行う。例えば、ランダムなビット列とのEXOR演算を行った後に、一体化と呼ばれる可逆演算 (特許文献2で開示) によって攪拌することにより、ビット列をランダムな形態にする。具体的な符号化処理フローの実施形態を図21に示す。

【0071】

まず、受信した通信データに対してランダムなビット列とのEXOR演算処理 (ステップS300) を行い、以降で使用する符号化処理用のデータを初期設定する。

次に、バッファリングされた通信データを、4バイトごとに $x(0)$ 、 $x(1)$ 、...、 $x(n)$ とする (ステップS301)。インデックス $i = 0$ とし、 $x(i+1) = x(i+1) + x(i)$ を、 $i < n$ まで繰り返す (ステップS302 ~ S305)。

最後に $x(0) = x(0) + x(n)$ とする。

【0072】

この符号化処理は予め定めた基準に従って複数回実施し、ビット列を攪拌することが好ましいが、機密性を確保するためには、この回数は適宜、変更することが、より好ましい。また、十分に攪拌処理を行うためには、符号化処理の回数は6回以上であることが好ましい。本実施形態では、加算演算により、元の通信データの攪拌を実施しているが、これは限定されるものではなく、可逆演算であれば、どのような演算種別を用いても良い。例えば、ステップS304、S306の演算を排他的論理和演算に変更して、実施しても良い。

【0073】

符号化処理によって、攪拌されたデータを、1パケットのペイロードサイズ (MSS) に分割を行う (ステップS107) ことが好ましい。バッファ処理において、 $MSS \times M$ サイズにパディング処理を行っているため、攪拌されたデータは、 M 個で MSS サイズのデータとなる。 MSS サイズとするのは、通信ネットワーク上で、フラグメンテーションが発生しないようにするためである。

10

20

30

40

50

【 0 0 7 4 】

シャッフリング処理（ステップ S 1 0 8）は、上記の分割処理（ステップ S 1 0 7）において、分割された M 個の断片データをランダムな順番に、シャッフリングする処理である。具体的なシャッフリング処理フローの例を図 2 2 に示す。シャッフリングは例えば、Fisher-Yates アルゴリズムを用いることが、一様ランダムな配置形態が実現可能であることから、好ましい。Fisher-Yates アルゴリズムでは、先ず、擬似乱数 j を生成し、分割された断片データをステップ S 5 0 2 ~ S 5 0 6 の処理を行うことにより、一様ランダムな順番にシャッフリングを行うことができるためである。擬似乱数 j は、どのような擬似乱数生成を用いてもよいが、真正乱数に近く、推測されにくいアルゴリズムが好ましい。

10

【 0 0 7 5 】

以上述べたバッファ処理、符号化処理、分割処理、シャッフリング処理（ステップ S 1 0 5 ~ S 1 0 8）を行うことで、元の通信データに暗号化処理を行うことができる。M 個のデータを一つのデータとみなして全体の攪拌を行い、攪拌されたデータを M 個に分割し、順番をランダムに並び替えることができる。悪意ある第三者が復号する場合には、M 個の断片データを全て集め、正しい順番に並び替え、復号を行わなければならない（特許文献 1 で開示）。

【 0 0 7 6 】

一般に M を十分大きな数に設定した場合には、全ての断片データを集めたることに加え、更に、元の順番に並び替えるためには、 $M!$ 通りの組み合わせを総当たりで試す必要がある。このため、M の値が 4 0 を超える程度の分割であれば、解読処理量の面からは、計算量的な安全性を十分に確保できると考えられる。なお、スイッチはシャッフリングされた順番に従い、パケットデータに当該ヘッダ情報を付加して送信するが、このパケットデータに付加するヘッダ情報は、受信端末のネットワーク環境を考慮し、ネットワーク装置特有のパラメータに整合させる必要がある。例えば L 2 スイッチとして使う場合は、送信元、送信先 MAC アドレスへの付け替えが必要であり、MAC ヘッダ内の FCS を変更する必要がある。L 3 スイッチとして使用する場合には、上記の変更に加え、IP アドレス情報の書き換えなどが必要である。なお、本発明ではパケットの順番を表すヘッダ情報（例えば IP ヘッダのフラグメントオフセットや TCP ヘッダのシーケンス番号など）は、受信時のヘッダ情報に記された順番ではなく、シャッフリングされた後の順番を記載する必要がある。

20

30

【 0 0 7 7 】

復号化に必要なメタデータは OFS 3 から OFC 4 へ送信する（ステップ S 1 1 0）。復号化に必要なデータ種別には、バッファ処理の際に必要な M S S サイズ、バッファするパケット数 M が含まれる。復号化を実施する場合には、符号化に用いた逆関数、シャッフリング前の順番とシャッフリング後の順番などの情報が必要である。これらの情報を含むメタデータは OFC 4 に送信され、復号化が完了するまで保持される。OFC 4 は他のデバイスと VPN 等の専用網で接続され、インターネットには接続しない構成が好ましい。

【 0 0 7 8 】

本実施形態では、開示内容を明確化するため、メタデータに記載するパラメータを固定した単純な例を示したが、メタデータに記載する情報は、シャッフリング前後の順番に関するデータ以外は記載していないが、例えば、バッファするパケット数 M を動的に変化させることができ、この場合は符号化のたび毎にパラメータの変更値をメタデータとして保持する必要がある。

40

【 0 0 7 9 】

OFS 3 が復号処理する際には、図 1 8 のステップ S 1 1 1 ~ S 1 1 7 に対応する処理の逆を行う。処理内容は、符号化の処理フロー手順（S 1 0 4 ~ S 1 1 0）と逆向きの処理内容に対応する。すなわち、符号化処理によって、攪拌されたデータを、格納されたストレージから回収して、OFS 3 のスイッチ内で復号化するには、攪拌に用いた関数の逆

50

関数を実施する必要がある。図 20、図 21 の符号化処理によって、攪拌されたデータを、復号化する具体的な処理を図 23 に示す。

【0080】

復号処理におけるステップ S 114 は、図 23 に示す逆関数処理を用いた復号処理に該当する。復号処理の完了後、OFS 3 は復号化の完了通知を OFC 4 に送信し、OFC 4 は関連するメタデータを削除する（ステップ S 117）。ステップ S 114 における復号化時には、符号化処理と同様に、データを 4 バイトごとに $x(0)$ 、 $x(1)$ 、 \dots 、 $x(n)$ とし（S 401）、はじめに $x(0) = x(0) + x(n)$ を実行した後（S 402）、 $x(n-1) = x(n-1) + x(n+1)$ を繰り返す（S 403 ~ S 406）。シャッフリングされたデータの順序を元に戻す処理や一体化処理の逆関数を用いることにより、復号処理が実施できる。

10

【0081】

（実施形態 5）

本実施形態に係る通信システムの形態例を図 24 に示す。本実施形態における通信システムは、ユーザ端末 11、ストレージ 62 ~ 67、オープンフロースイッチ（OFS）71、72、73 及びオープンフローコントローラ（OFC）81、82、83 から構成される。通信ネットワーク 91 ~ 93 は、例えば、LAN を使用し、94 は一般の公衆網の場合を想定して以下に説明する。通信ネットワーク 101 ~ 105 は、OFC の制御用の通信網で、VPN 等の専用通信ネットワークであることが好ましい。

【0082】

20

データセンタ 111 は OFS 72、OFC 82、ストレージ 62 ~ 64、データセンタ 112 は OFS 73、OFC 83、ストレージ 65 ~ 67 を持つ。データセンタ 111 と 112 はそれぞれ地理的に離れた場所にある。実施形態 3 では、同じネットワーク内にストレージ 12a ~ 12d が存在したが、実用的には、ストレージ 62 ~ 67 をそれぞれ別のデータセンタ等、地理的に離れた場所に設置することにより、地震などの災害やハッキング等で、ストレージ 62 ~ 67 のすべてが同時に危険にさらされる事がないように構成できる。

【0083】

本実施形態では、実施形態 2 における図 16 において OFS 3 が行った符号化処理と、複製・分散転送する処理を、それぞれ、符号化処理は OFS 71 で行い、複製・分散転送する処理は OFS 72 と 73 で、分担して実施する場合を示している。ここで、例えば、OFS 72、73 は、符号化処理を行わずに複製および分散転送のみを行い、ストレージ 62 ~ 64 および 65 ~ 67 に分散転送する場合の例である。符号化処理や、復号処理、複製・分散転送する機能は、第 3 の実施形態と同様である。

30

【0084】

メタデータは、OFC 81 ~ 83 が、通信ネットワーク 102、103 を用いることで共有できる。従って、バックアップを行った際、ストレージ 62 ~ 64 はデータのハッシュ値を OFC 82 に、ストレージ 65 ~ 67 はデータのハッシュ値を OFC 83 に送り、OFC 82、83 は OFC 81 にハッシュ値を通知する。OFC 81 はメタデータに、OFC 82、83 から受け取ったハッシュ値を記載する。

40

【0085】

ユーザ端末 11 が、復元要求を OFS 71 へ行った場合、OFS 71 が OFC 81 からメタデータを受信し、OFS 72、73 にデータの送信要求を送る。OFS 72、73 は、ストレージ 62 ~ 64、および 65 ~ 67 に送信要求を送る。OFC 71 は、ストレージ 62 ~ 64 および 65 ~ 67 が返送したデータに対する復号処理を行い、復元データをユーザ端末 11 に送信する。このように、OFS 71 で符号化及び復号化を行うことにより、仮に公衆網 94 で第三者による盗聴があった場合でも、元データの復元は、関連する OFC が保持するメタデータと OFS で実施する復号処理メカニズムの詳細が不明である限り、不可能である。一般的には、処理負荷量のバランスを、OFS 同士でとることも可能であることは言うまでもない。

50

【 0 0 8 6 】

(実施形態 6)

本実施形態に係る通信システムの形態例を図 2 5 に示す。本実施形態に係る通信システムは、ユーザ端末 1 6 1、1 6 2、オープンフロースイッチ (OFS) 1 2 1、1 2 2、およびオープンフローコントローラ (OFC) 1 3 1、1 3 2 を備える。ユーザ端末 1 6 1、OFS 1 2 1、OFC 1 3 1 はデータセンタ 1 1 1 内に設置されており、ユーザ端末 1 6 2、OFS 1 2 2、OFC 1 3 2 はデータセンタ 1 1 2 内に設置されている。ユーザ端末 1 6 1、1 6 2 は、相互通信が可能な端末であり、OFS 1 2 1、1 2 2 は、相互に接続を確立している。

【 0 0 8 7 】

OFS 1 2 1、1 2 2 はエッジルータに対応し、データセンタ 1 1 1 とデータセンタ 1 1 2 との間で接続を確立しているノードである。OFC 1 3 1、OFC 1 3 2 は、それぞれ OFS 1 2 1、1 2 2 と接続を確立している制御ノードである。また、OFC 1 3 1、1 3 2 は相互に接続を確立されている。通信ネットワーク 1 4 1、1 4 2 は、データセンタ 1 1 1、1 1 2 内の LAN を想定するが、この形態に限るものではない。通信ネットワーク 1 4 3 は、公衆網である。

【 0 0 8 8 】

通信ネットワーク 1 5 1、1 5 2 は、それぞれ、OFC 1 3 1、1 3 2 が OFS 1 2 1、1 2 2 を制御するための専用の通信ネットワークであり、VPN などの専用通信ネットワークであることが好ましい。通信ネットワーク 1 5 3 は、OFC 1 3 1 と OFC 1 3 2 間で、同期、制御を行うための専用の通信ネットワークであり、通信ネットワーク 1 5 1、1 5 2 と同様に、VPN などの専用通信ネットワークであることが好ましい。通信ネットワーク 1 5 3 は、通信ネットワーク 1 5 1、1 5 2 と異なり、データセンタ 1 1 1 とデータセンタ 1 1 2 を相互接続する通信ネットワークであり、データセンタ内の通信ネットワーク 1 5 1、1 5 2 と同じように、セキュリティに配慮すべき専用ネットワークであることが好ましい。

【 0 0 8 9 】

本実施形態では、前述の実施形態 1 ~ 実施形態 3 とは異なり、ユーザ端末 1 6 1 と 1 6 2 がデータ通信を相互に行う P 2 P 通信を想定している。具体的には、ユーザ端末 1 6 1 が、ユーザ端末 1 6 2 に通信データを送信する際には、OFS 1 2 1 が、図 1 8 に示す符号化処理に対応する処理を行う。この時、メタデータを OFC 1 3 1 から読み込み、バッファ処理、符号化処理、分割処理、シャッフリング処理およびパケットの送信処理を行い、当該のメタデータを OFC 1 3 1 に格納する。OFS 1 2 1 で符号化処理されたパケットは、通信ネットワーク 1 4 3 を経由して、OFS 1 2 2 に届く。

【 0 0 9 0 】

ここで、OFC 1 3 1 はメタデータを OFC 1 3 2 に事前に送信し、OFS 1 2 2 に対して提供する準備を行う。OFS 1 2 2 は、OFS 1 2 1 から受信したパケットに対して、図 1 8 に示す復号処理を、OFC 1 3 2 から受信したメタデータをもとに行い、OFS 1 2 1 からの受信パケットをユーザ端末 1 6 1 が送信した符号化前のパケットに復号し、ユーザ端末 1 6 2 に送信する。その後、OFC 1 3 2 には復号完了の通知を行う。

【 0 0 9 1 】

このように、ネットワーク内の機器である OFS 1 2 1 で符号化し、OFS 1 2 2 で復号することにより、公衆網である通信ネットワーク 1 4 3 で、仮に盗聴されたとしても、元の通信データを復元は非常に困難であり、第三者には解読困難な、秘密通信を実現できる。

【 0 0 9 2 】

ユーザ端末 1 6 2 がユーザ端末 1 6 1 に対して送信を行う場合は、上記とは逆の順番で、OFC 1 3 2、1 3 1 が起動する。具体的には、OFS 1 2 2 が符号化処理を行い、OFS 1 2 1 が復号処理を行い、OFC 1 3 2 がメタデータを OFC 1 3 1 に送信する。OFS 1 2 1 と 1 2 2 が行う符号化、復号化の処理は、前述の実施形態 1 から実施形態 3 と

10

20

30

40

50

同等であるが、バックアップサービスのように、ストレージから、断片データを回収するための手順が省略されている点が異なる。また、一般的には、ユーザ端末 162 は、認証手順を用い、照合が確認された段階で、OFS 122 で復号化された通信データを受信することが好ましい。

【0093】

以上、説明したように、本発明の特徴は、集中制御を前提とした、SDNのアーキテクチャを持つネットワーク制御方式において、

(1) ネットワークを集中制御するコントローラとスイッチの制御機構の活用により、ユーザ端末、あるいはサーバ側の制御とは独立に、高いセキュリティの通信を実現する。

(2) ユーザ端末の処理能力を暗号化処理等のために費やすことが無いため、容易に通信スループットの向上が図れる。

(3) SDN内の専用ネットワークと公衆網の適切な適用により、従来の通信方式に比べて、高いセキュリティを確保できる。

(4) トラフィックの急激な増加やネットワーク機器の故障等の状況に応じて、安全なバックアップサービスが容易に実現できる。

(5) 端末同士の通信を、リアルタイムに、秘密通信として実現できる。

【0094】

すなわち、開示した技術は、SDNのアーキテクチャをもつオープンフロースイッチとコントローラを活用することにより、安全でセキュリティの高い通信を実現すると共に、ユーザ端末であるホスト側の処理負荷の増大を一切起こすことなく、セキュリティ強度の高い暗号通信をネットワーク内のみで実現できるため、通信スループットの大幅な向上が期待できる。

【0095】

本技術は、SDNに代表されるオープンフロータイプのネットワークに適用できるだけでなく、NGNや既存の携帯電話網の制御やオペレーションシステムの制御を行う場合にも適用でき、適用対象範囲は極めて広い。以上説明したように、本技術は、安全で高速なネットワークサービスを実現する上での基盤技術として活用でき、今後の情報通信産業を発展させる上で極めて大きな意義を持つ。

【産業上の利用可能性】

【0096】

本発明は情報通信産業に適用することができる。

【符号の説明】

【0097】

11、161、162 ユーザ端末

12 ストレージ

21、22 データ通信ネットワーク

3、71～73、121、122 オープンフロースイッチ(OFS)

31 フローテーブル

32 スイッチ

4、81～83、131、132 オープンフローコントローラ(OFCC)

5、101～105、151～153 制御用の専用通信ネットワーク

91～94、141～143 データ通信ネットワーク

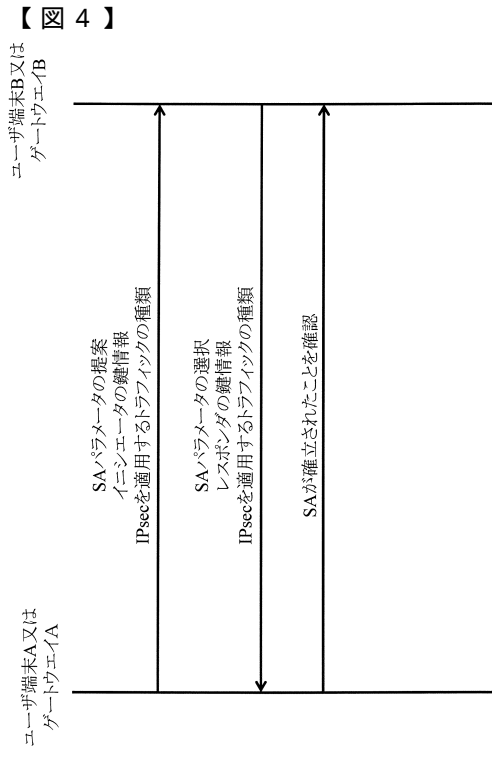
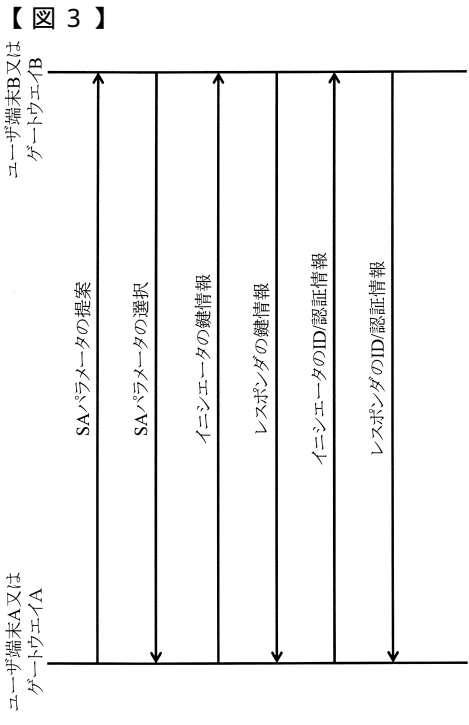
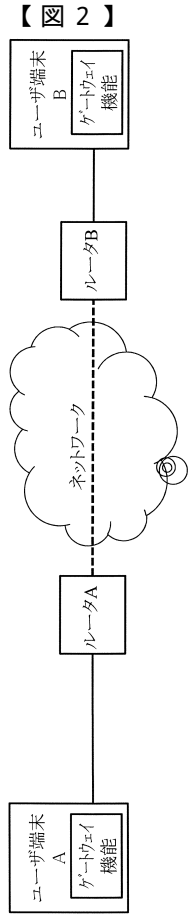
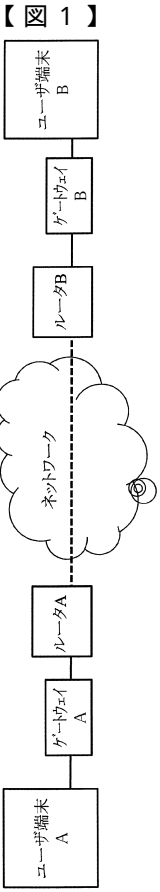
111、112 データセンタ(あるいはサービス利用端末)

10

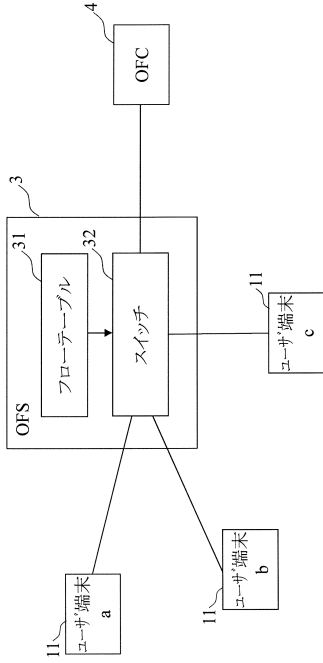
20

30

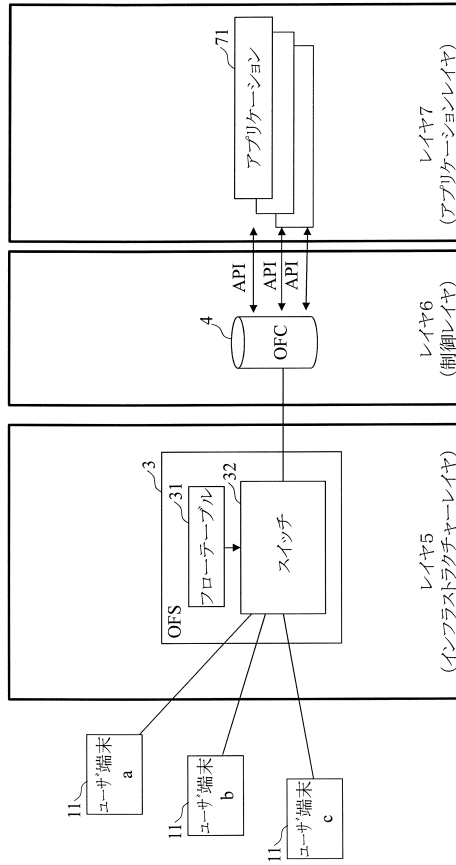
40



【 図 5 】



【 図 6 】



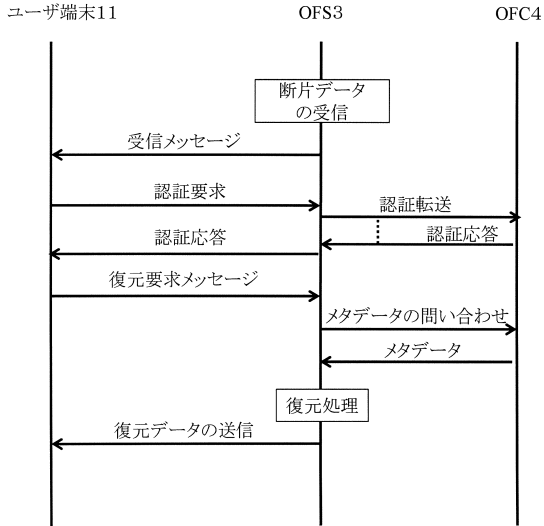
【 図 7 】

値	説明
Forward	パケットを特定の物理ポートに転送する
Drop	パケットを破棄する
Modify-Field	パケットヘッダの値を指定した値に書き換える
store	パケットを一時、格納する
copy	パケットをコピーし、複数ポートにマルチキャストする。
divide	パケットを分割し、複数ポートにマルチキャストする。
Encryption-A	パケットの中身をAESで暗号化する。
Encryption-S	パケットの中身を一体化処理(空間的に攪拌)する。

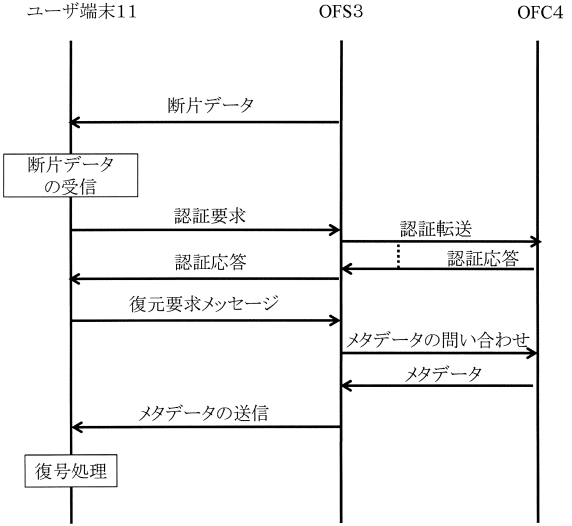
【 図 8 】

No	ヘッダフィールドに指定可能な条件
1	物理ポート番号
2	送信元MACアドレス
3	送信先MACアドレス
4	Etherタイプ
5	VLAN ID
6	VLAN プライオリティ
7	送信元IPアドレス
8	送信先IPアドレス
9	IPプロトコル種別
10	IP TOS情報
11	送信元L4ポート番号
12	送信先L4ポート番号
13	MPLSラベル番号
14	閉域サービスイデンティフィカション番号
15	ファイナルバックアップ用のセキュリティ番号

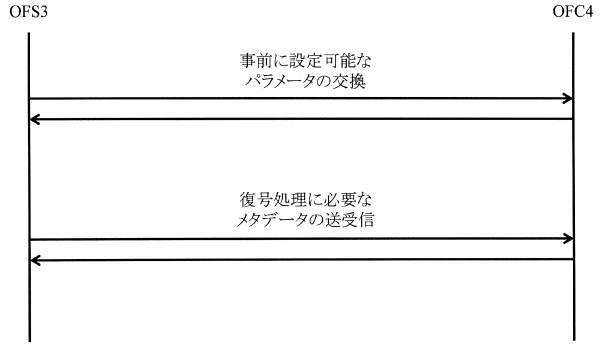
【図9】



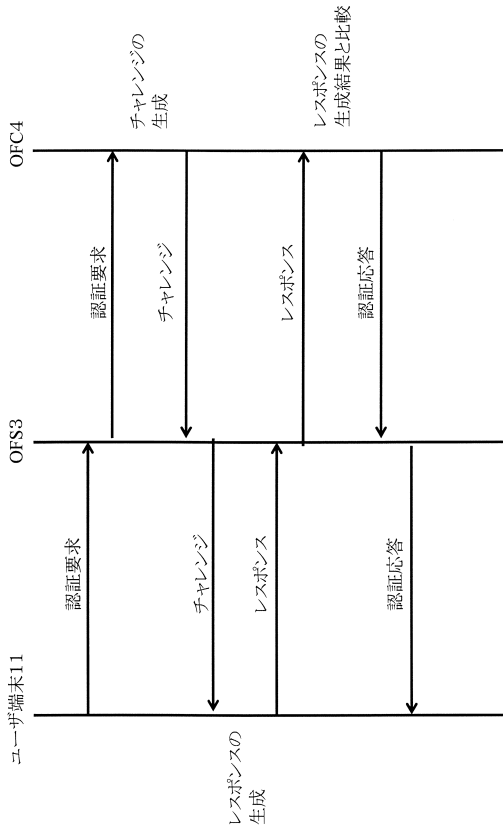
【図10】



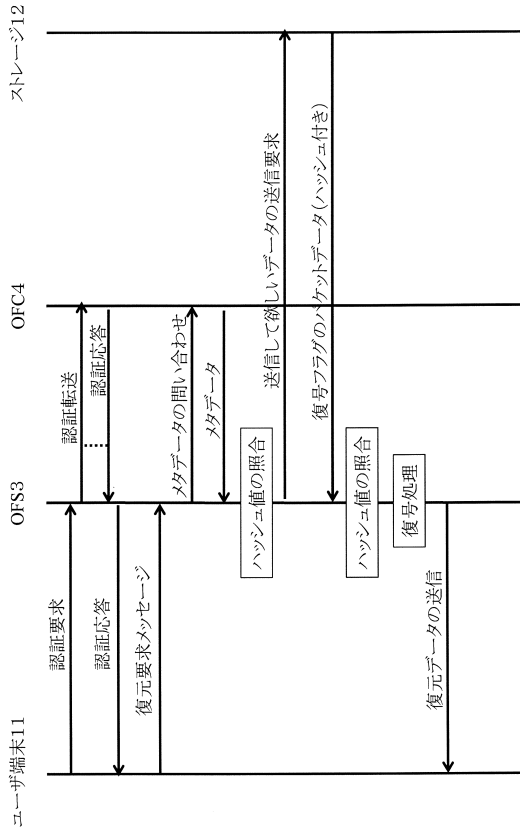
【図11】



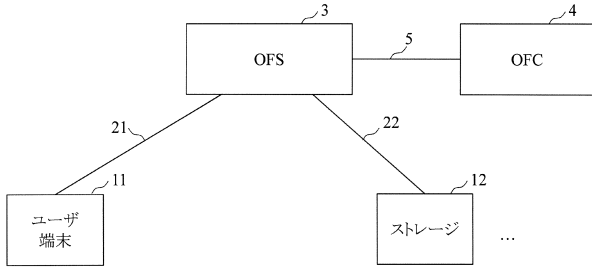
【図12】



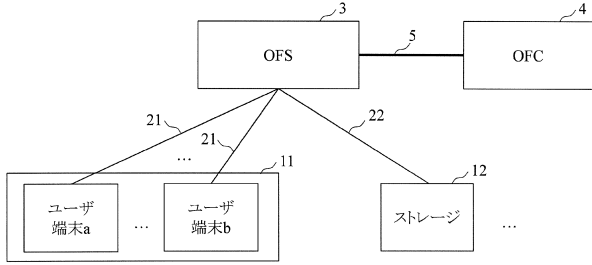
【図13】



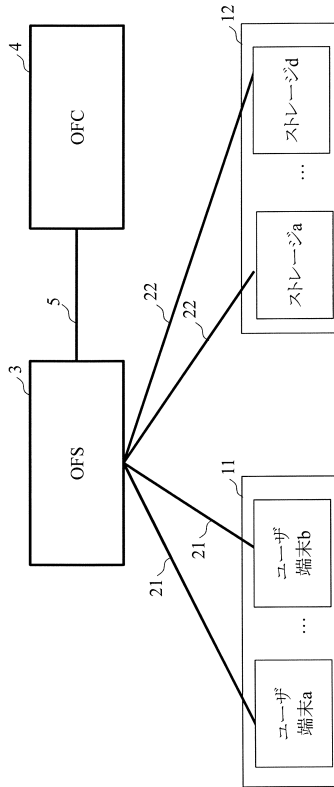
【図14】



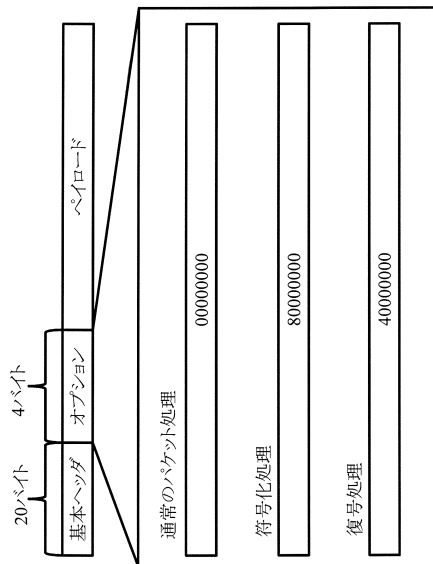
【図15】



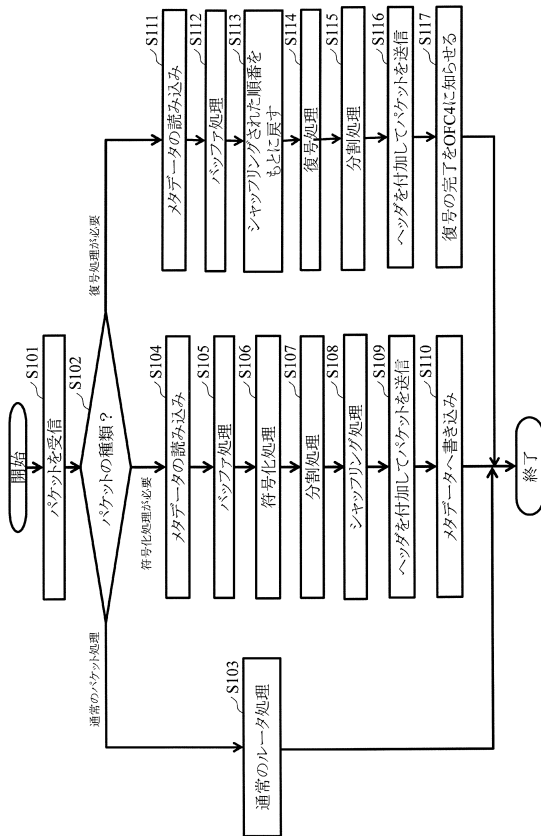
【図16】



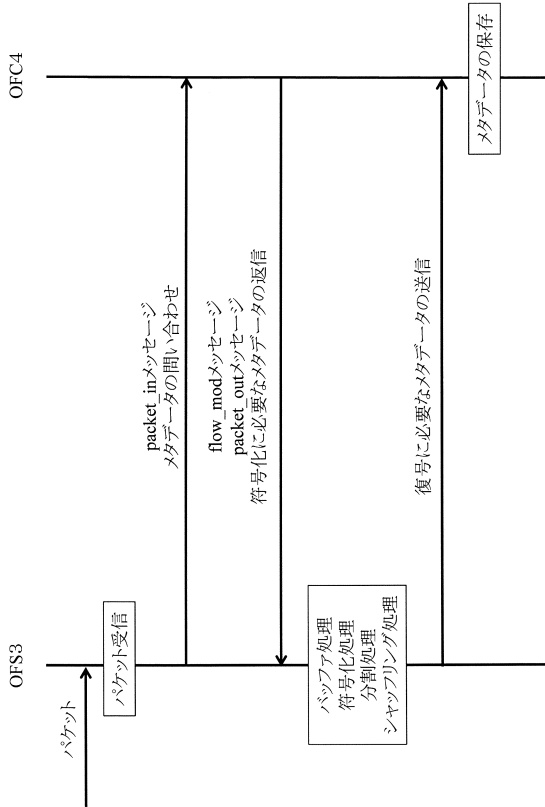
【図17】



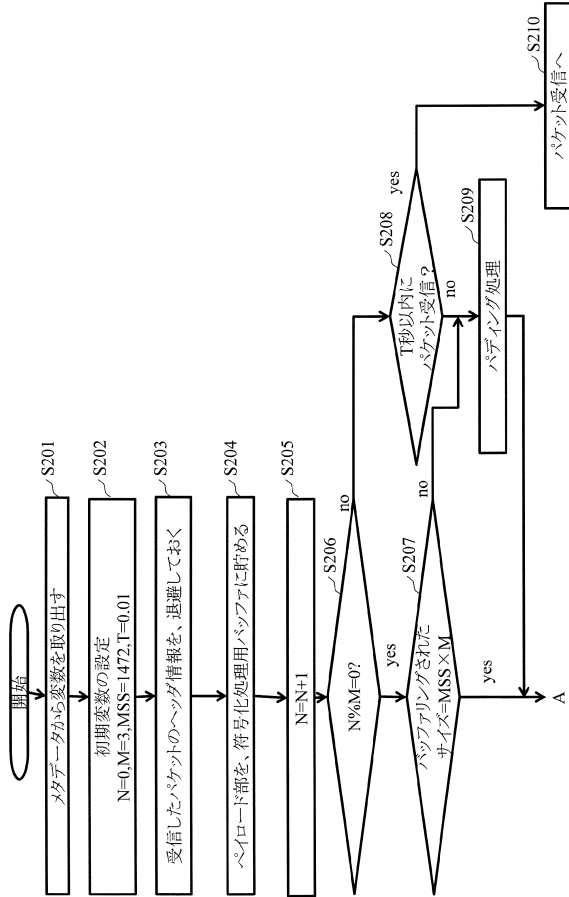
【図18】



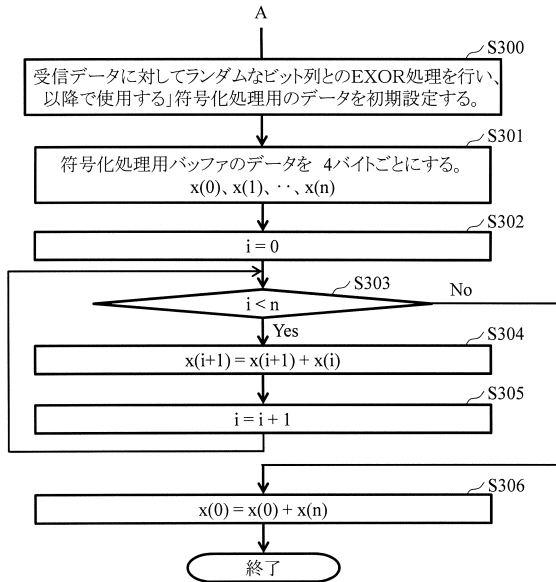
【図 19】



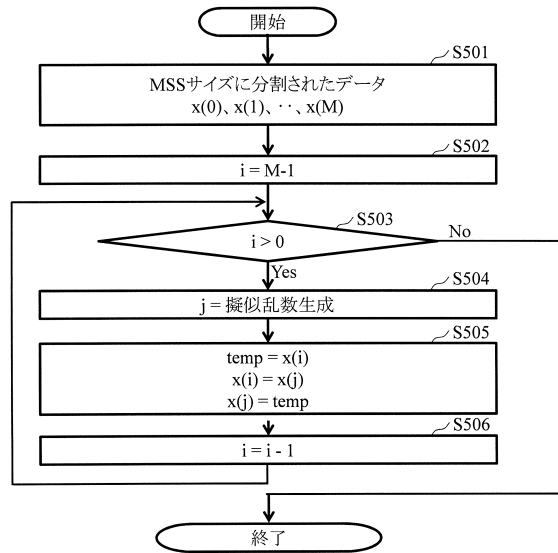
【図 20】



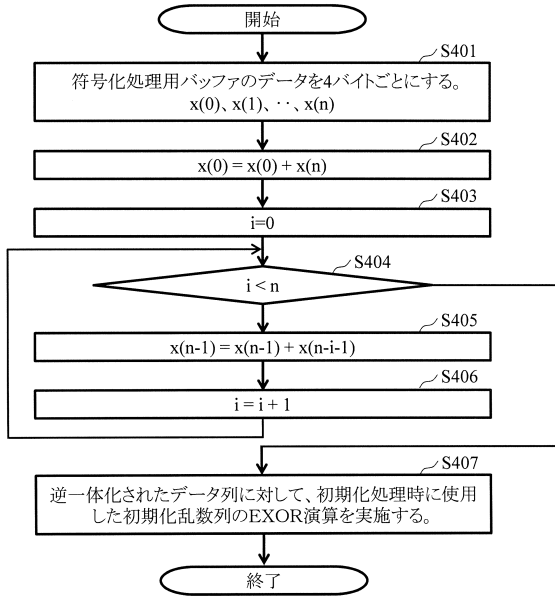
【図 21】



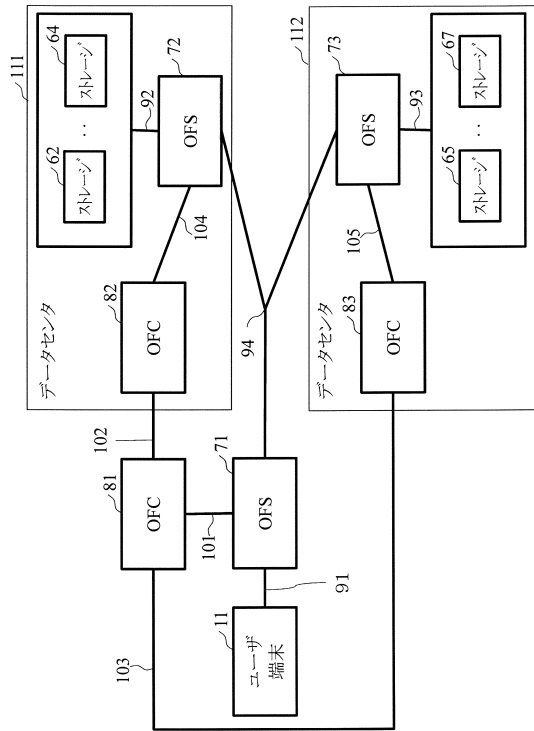
【図 22】



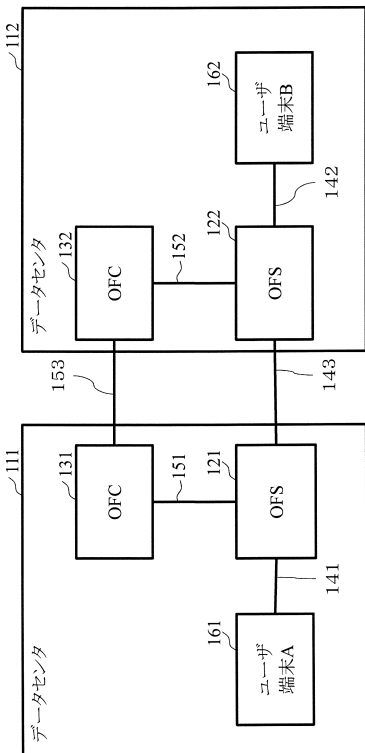
【図23】



【図24】



【図25】



フロントページの続き

- (72)発明者 鈴木 秀一
東京都足立区千住旭町5番 学校法人東京電機大学内
- (72)発明者 古川 雅大
東京都足立区千住旭町5番 学校法人東京電機大学内

審査官 行田 悦資

- (56)参考文献 特表2010-541426(JP,A)
特開平09-321750(JP,A)
特開2005-252846(JP,A)
特開2005-252717(JP,A)
波多 浩昭, SDNスイッチのプラットフォーム要件, 電子情報通信学会技術研究報告, 日本,
一般社団法人電子情報通信学会, 2013年 7月11日, 第113巻, 第140号, p.59-63

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|--------|
| H04L | 9/18 |
| H04L | 12/22 |
| H04L | 12/717 |