(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6251732号
(P6251732)

(45)発行日　平成29年12月20日(2017.12.20)　(24)登録日　平成29年12月1日(2017.12.1)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
H04W 12/04	(2009.01)	H04L	9/00	601E
H04W 4/06	(2009.01)	H04W	12/04	
		H04W	4/06	150

請求項の数 19　(全 12 頁)

(21)出願番号	特願2015-509562(P2015-509562)
(86)(22)出願日	平成25年5月3日(2013.5.3)
(65)公表番号	特表2015-520967(P2015-520967A)
(43)公表日	平成27年7月23日(2015.7.23)
(86)国際出願番号	PCT/IB2013/053548
(87)国際公開番号	WO2013/164803
(87)国際公開日	平成25年11月7日(2013.11.7)
審査請求日	平成28年3月2日(2016.3.2)
(31)優先権主張番号	61/642,169
(32)優先日	平成24年5月3日(2012.5.3)
(33)優先権主張国	米国(US)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エルエム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】ＥＭＢＭＳにおける集中化した鍵管理

(57)【特許請求の範囲】

【請求項１】

ブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）において、マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）トラフィック鍵（ＭＴＫ）を生成する方法であって、

集中化した鍵管理サービスで生成されるＭＢＭＳサービス鍵（ＭＳＫ）に対応するＭＳＫを受信するステップと、

少なくとも受信した前記ＭＳＫの関数として、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化する際に使用される前記ＭＴＫを生成するステップと

を含むことを特徴とする方法。

【請求項２】

受信する前記ステップは、ネットワークインターフェースを介して前記集中化した鍵管理サービスから前記ＭＳＫを受信するステップを含むことを特徴とする請求項１に記載の方法。

【請求項３】

受信する前記ステップは、前記集中化した鍵管理サービスの代わりに前記ＭＳＫを送信するスタンドアロンサーバからの該ＭＳＫをネットワークインターフェースを介して受信するステップを含むことを特徴とする請求項１に記載の方法。

【請求項４】

前記ＭＴＫは、受信した前記ＭＳＫ及びＭＴＫシード値の関数として生成されることを

特徴とする請求項１に記載の方法。
【請求項５】
前記ＭＴＫは、受信した前記ＭＳＫ、ＭＲＫ、及びＣＫ｜｜ＩＫに関連付けられた、サービスＩＤ、鍵ドメインＩＤ、及びＭＳＫ－ＩＤを含むリストから選択された少なくとも１つのパラメータの関数として生成されることを特徴とする請求項４に記載の方法。
【請求項６】
前記少なくとも１つのパラメータは、前記ＭＴＫを生成するのに使用される前に変換されることを特徴とする請求項５に記載の方法。
【請求項７】
前記ＭＴＫシード値は、ＭＴＫ生成鍵、及びＭＴＫ－ＩＤの関数として生成されることを特徴とする請求項４に記載の方法。
【請求項８】
前記ＭＴＫ－ＩＤは、シーケンス番号であることを特徴とする請求項７に記載の方法。
【請求項９】
前記ＭＴＫ生成鍵は、前記ＢＭＳＣには知られているものの、前記ＵＥへは知られていないことを特徴とする請求項７又は８に記載の方法。
【請求項１０】
前記ＭＴＫ生成鍵は、前記集中化した鍵管理サービスによって提供されることを特徴とする請求項７又は８に記載の方法。
【請求項１１】
前記ＭＴＫ生成鍵は、静的な値として、前記集中化した鍵管理サービスによって提供されることを特徴とする請求項１０に記載の方法。
【請求項１２】
前記ＭＴＫ生成鍵は、周期的に、前記集中化した鍵管理サービスによって提供されることを特徴とする請求項１０に記載の方法。
【請求項１３】
コンテンツを確保するための鍵を配信する、集中化された鍵管理サーバで実行される方法であって、
ＭＢＭＳサービス鍵（ＭＳＫ）を生成するステップと、
対応するマルチメディア・ブロードキャスト・マルチキャスト・トラフィック鍵（ＭＴＫ）を送信することなく、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化するＭＴＫを生成する際に使用される前記生成されたＭＳＫをブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）へ送信するステップと、
少なくとも前記送信したＭＳＫの関数として、前記ＢＭＳＣで生成される前記ＭＴＫを用いて、前記ＢＭＳＣによって送信され、かつ暗号化された前記コンテンツを復号化するために、前記ＵＥ用の復号化鍵を該ＵＥへ送信するステップと
を含むことを特徴とする方法。
【請求項１４】
前記復号化鍵は、前記ＢＭＳＣへ送信されない前記ＭＴＫであることを特徴とする請求項１３に記載の方法。
【請求項１５】
前記生成したＭＳＫを送信するステップは、前記ＢＭＳＣへ配信するためにスタンドアロンサーバへ前記生成したＭＳＫを送信するステップを含むことを特徴とする請求項１３に記載の方法。
【請求項１６】
前記ＢＭＳＣへ鍵生成関数を送信するステップをさらに含み、
前記鍵生成関数は、前記ＭＳＫに従ってＭＴＫを生成する際に前記ＢＭＳＣによって使用され、
前記生成されたＭＴＫ及び前記ＭＳＫは、前記コンテンツを暗号化するために使用されることを特徴とする請求項１３に記載の方法。

【請求項１７】
受信した前記ＭＳＫ、ＭＲＫ、及びＣＫ｜｜ＩＫに関連付けられたサービスＩＤ、鍵ドメインＩＤ、及びＭＳＫ－ＩＤの少なくとも１つを前記ＢＭＳＣへ送信するステップをさらに含むことを特徴とする請求項１３に記載の方法。
【請求項１８】
ブロードキャスト・マルチキャスト・サービス・センター・ノードであって、
ユーザ機器ノード及び集中化した鍵管理サーバと通信を行うネットワーク・インターフェースと、
命令を格納するメモリと、
前記格納された命令を実行するプロセッサであって、該格納された命令を実行すると、前記ブロードキャスト・マルチキャスト・サービス・センター・ノードが、
少なくとも前記集中化した鍵管理サーバで生成されるＭＢＭＳサービス鍵（ＭＳＫ）の関数として、前記ユーザ機器ノードへ送信されるコンテンツを暗号化に使用するための、マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）トラフィック鍵（ＭＴＫ）を生成する、
前記プロセッサと
を備えることを特徴とするブロードキャスト・マルチキャスト・サービス・センター・ノード。
【請求項１９】
集中化した鍵管理サーバであって、
ユーザ機器ノードと、ブロードキャスト・マルチキャスト・サービス・センター・ノードと通信するためのネットワークインターフェースと、
命令を格納するメモリと、
前記格納された命令を実行するプロセッサであって、該格納された命令を実行すると、前記集中化した鍵管理サーバが、
マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）サービス鍵（ＭＳＫ）を生成し、
対応するＭＢＭＳトラフィック鍵（ＭＴＫ）を送信することなく、前記ユーザ機器ノードへ送信されるコンテンツを暗号化するＭＴＫを生成する際に使用される前記生成されたＭＳＫを、前記ブロードキャスト・マルチキャスト・サービス・センター・ノードへ送信し、
前記ユーザ機器ノードへ対して、少なくとも前記送信したＭＳＫの関数として、前記ブロードキャスト・マルチキャスト・サービス・センター・ノードで生成される前記ＭＴＫを用いて、前記ブロードキャスト・マルチキャスト・サービス・センター・ノードによって送信され、かつ暗号化された前記コンテンツを復号化するために、前記ユーザ機器ノード用の復号化鍵を送信する、
前記プロセッサと
を備えることを特徴とする集中化した鍵管理サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的には、発展マルチメディア・ブロードキャスト・マルチキャスト・サービス（ｅＭＢＭＳ）における鍵対の管理に関連するものである。
【背景技術】
【０００２】
ライブビデオなどのマルチメディアコンテンツへアクセスするモバイルデータネットワークの使用は、少数のユーザによってのみ使用されるサービスである。しかしながら、それらの使用量は増加しており、少数のユーザであっても、彼らの消費するデータ量は過度に増大している。ロイヤルウェディング、テニスの試合や他の一度きりのイベントなどのライブイベントは、ネットワークへの負荷を増大させうる通信量を発生させてしまう。結

果として、ｅＭＢＭＳは、ロング・ターム・エボリューション（ＬＴＥ）ネットワークでのマルチメディア配信におけるマルチキャスト標準規格として設計されている。

【０００３】

しかしながら、ｅＭＢＭＳを介して配信されたコンテンツがＭＢＭＳサービス鍵（ＭＳＫ）及びＭＢＭＳトラフィック鍵（ＭＴＫ）の使用を通じてコンテンツ配信制御を可能にする方法で管理されなければならないという課題が生じている。同一のｅＭＢＭＳサービスが複数のＢＭＳＣを介して放送されうる分割ｅＭＢＭＳアーキテクチャにおいて集中化したＭＳＫ／ＭＴＫ鍵管理機能の使用をどのように行うかという問題がある。集中化した鍵管理システムがなければ、ユーザは、視聴を害するような体験をモバイル上の問題として経験するであろう。集中化したＭＳＫ／ＭＴＫ鍵管理があれば、全てのブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）が、上記問題を取り除く、ｅＭＢＭＳサービスに対して同一のＭＳＫ／ＭＴＫ鍵を使用する能力を有するであろう。集中化したＭＳＫ／ＭＴＫ鍵管理の必要性は、ＢＭＳＣが同一の又は異なる複数のスタンドアロンサーバ下であっても変わらない。同一のＭＳＫ／ＭＴＫ鍵の使用は、全国的なｅＭＢＭＳサービス上で行われてもよい（例えば、一方向トランスポート（ＦＬＵＴＥ）チャネル上での一ファイル配信）。

【０００４】

そのような解決手法は、ｅＭＢＭＳサービス、ＭＢＳＣモバイル間、スタンドアロンサーバモバイル間への初期登録に有効である必要があり、ユーザ装置（ＵＥ）がセグメントの境界に位置する場合に、セグメント間で行ったり来たりするようなことに関連する問題を好適に避けうるであろう。現状では、そのような統一された解決手法は確立されていない。当業者には、ＭＳＫ／ＭＴＫ鍵の単一の組みを生成し、それらを各ＢＭＣへ送信する集中鍵権限が、各鍵の送信が大量のオーバーヘッドを招くように、オーバヘッドの増大やシステムのセキュリティの劣化を招くことが理解されるであろう。同様に、鍵の傍受や復号化がシステムを危険にさらすであろう。複数の鍵を同時に送信することはオーバヘッドの問題を軽減するものの、セキュリティ周り問題がより不可避なものとなってしまう。それら両方の問題は、スケーリングが考慮される場合には、多くの異なるＢＭＳＣへの鍵送信が集中化した権限での増大した負荷をもたらすように、新たな問題が生まれてしまう。

【０００５】

したがって、上述の問題を回避する又は軽減するシステム及び方法を提供することが望まれる。

【発明の概要】

【０００６】

本発明の目的は、従来技術における少なくとも１つの欠点を回避するか、又は、軽減することにある。

【０００７】

本発明の第１の態様によれば、ＢＭＳＣでＭＴＫを生成する方法を提供する。当該方法は、集中化した鍵管理サービスで生成されるＭＢＭＳサービス鍵（ＭＳＫ）を受信するステップと、受信した前記ＭＳＫに従って、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化する際に使用される前記ＭＴＫを生成するステップとを含む。

【０００８】

本発明の第１の態様によれば、受信する前記ステップは、ネットワークインターフェースを介して前記集中化した鍵管理サービスから前記ＭＳＫを受信するステップを含む。さらに、他の形態によれば、受信する前記ステップは、前記集中化した鍵管理サービスの代わりに、前記ＭＳＫを送信するスタンドアロンサーバからの該ＭＳＫをネットワークインターフェースを介して受信するステップを含む。

【０００９】

他の形態において、前記ＭＴＫは、受信した前記ＭＳＫ及びＭＴＫシード値の関数として生成され、前記関数は、第三世代パートナーシップ・プロジェクトの技術仕様書３３．２２０で定義されている鍵生成関数である標準化鍵生成関数である。他の形態によれば、

ＭＴＫは、受信した前記ＭＳＫ、ＭＲＫ、及びＣＫ｜｜ＩＫに関連付けられた、サービスＩＤ、鍵ドメインＩＤ、及びＭＳＫ－ＩＤを含むリストから選択された少なくとも１つのパラメータの関数として生成され、前記少なくとも１つのパラメータは、前記ＫＤＦへ入力される前に変換される。他の形態において、前記ＭＴＫ－ＩＤは、シーケンス番号であり、前記ＭＴＫシード値は、ＭＴＫ生成鍵、及びＭＴＫ－ＩＤの関数として生成され、前記ＭＴＫ生成鍵は、前記ＢＭＳＣには知らているものの、前記ＵＥへは知られておらず、静的な値として、前記集中化した鍵管理サービスによって提供される。他の形態において、前記ＭＴＫ生成鍵は、周期的に、前記集中化した鍵管理サービスによって提供される。

【００１０】

本発明の第２の形態において、コンテンツを確保するための鍵を配信する、集中化された鍵管理サーバで実行される方法が提供される。当該方法は、ＭＢＭＳサービス鍵（ＭＳＫ）を生成するステップと、マルチメディア・ブロードキャスト・マルチキャスト・トラフィック鍵（ＭＴＫ）を送信することなく、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化する際に使用される前記生成されたＭＳＫをブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）へ送信するステップと、前記ＵＥが前記ＢＭＳＣによって送信される前記コンテンツのストリームを復号化することを可能とするために、前記送信したＭＳＫに従って、前記ＢＭＳＣで生成される復号化鍵を前記ＵＥへ送信するステップとを含む。

【００１１】

本発明の第２の形態における一実施形態において、前記復号化鍵は、前記ＢＭＳＣへ送信されない前記ＭＴＫである。他の形態において、前記生成したＭＳＫを送信するステップは、前記ＢＭＳＣへ配信するためにスタンドアロンサーバへ前記生成したＭＳＫを送信するステップを含む。さらに他の形態において、前記ＢＭＳＣへ鍵生成関数を送信するステップをさらに含み、前記鍵生成関数は、前記ＭＳＫに従ってＭＴＫを生成する際に前記ＢＭＳＣによって使用され、前記生成されたＭＴＫ及び前記ＭＳＫは、前記コンテンツのストリームを暗号化するために使用される。他の形態において、受信した前記ＭＳＫ、ＭＲＫ、及びＣＫ｜｜ＩＫに関連付けられたサービスＩＤ、鍵ドメインＩＤ、及びＭＳＫ－ＩＤの少なくとも１つを前記ＢＭＳＣへ送信するステップをさらに含む。

【００１２】

本発明の第３の形態において、ブロードキャスト・マルチキャスト・サービス・センター・ノードが提供される。当該ノードは、ネットワークインターフェース、メモリ及びプロセッサを備える。ネットワークインターフェースは、ユーザ機器ノード及び集中化した鍵管理サーバと通信を行う。メモリは、命令を格納する。プロセッサは、前記格納された命令を実行するプロセッサであって、該格納された命令を実行すると、ブロードキャスト・マルチキャスト・サービス・センター・ノードが、前記集中化した鍵管理サーバで生成されるＭＢＭＳサービス鍵（ＭＳＫ）に従って、前記ユーザ機器ノードへ送信されるコンテンツを暗号化する際に使用され、マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）トラフィック鍵（ＭＴＫ）を生成する。

【００１３】

本発明の第４の形態において、集中化した鍵管理サーバが提供される。当該サーバは、ネットワークインターフェース、メモリ及びプロセッサを備える。ネットワークインターフェースは、ユーザ機器ノードと、ブロードキャスト・マルチキャスト・サービス・センター・ノードと通信することを可能にする。メモリは、命令を格納する。プロセッサは、前記格納された命令を実行するプロセッサであって、該格納された命令を実行すると、前記集中化した鍵管理サーバが、マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）サービス鍵（ＭＳＫ）を生成し、対応するＭＢＭＳトラフィック鍵（ＭＴＫ）を送信することなく、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化する際に使用される前記生成されたＭＳＫを、ブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）へ送信し、前記ＵＥが前記ＢＭＳＣによって送信された前記コンテンツのストリームを復号化することを可能にするために、前記ＵＥへ対して、前

記送信したＭＳＫに従って前記ＢＭＳＣで生成される復号化鍵を送信する。
【図面の簡単な説明】
【００１４】
【図１】分割アーキテクチャの一例を示す図。
【図２】ＭＳＫから導出されるＭＴＫで鍵の集中化モデルの一例を示す図。
【図３】ＢＭＳＣで実行される方法を示すフローチャート。
【図４】集中化した鍵管理サーバで実行される方法を示すフローチャート。
【図５】図３及び図４のフローチャートの方法を実行するノードを示すブロック図。
【発明を実施するための形態】
【００１５】
本発明の実施形態は、分割アーキテクチャｅＭＢＭＳにおいて集中化した鍵管理を提供するためのシステム及び方法に関連するものである。
【００１６】
添付した図面に従って参照符号を付した特定の要素について以下で説明を行う。以下での説明は実際には一例であり、本発明の範囲を限定するようなものではない。本発明の範囲は、特許請求の範囲に定義しており、以下で詳細に説明する構成によって限定されるべきではなく、当業者には、均等の機能要素で当該要素を置き換えることによって修正されうることが理解されるであろう。
【００１７】
当業者には、全国的なｅＭＢＭＳサービスのコンテンツが、ＢＶＰＳ（ブロードキャスト・ビデオ提供サーバ）などの集中化した場所からＢＭＳＣへ配信されることが理解されるであろう。その後、ＢＭＳＣが、そのローカル放送チャネル上で（典型的には、放送を通じて）コンテンツを配信するであろう。ＢＶＰＳはまた、供給データチャネル（ＳＤＣＨ）上で配信される全国的なＵＳＤ（ユーザ・サービス・ディスクリプション）を定義してもよい。
【００１８】
図１に示すように、分割ＢＭＳＣアーキテクチャにおけるＢＭＳＣは、通常、ＢＶＰＳインターフェースの管理、各配信セッションにおけるスタンドアロンサーバでのセキュリティサービスの作成、ＭＴＬ及びＭＴＫ－ＩＤの生成、ＭＴＫの配信（ＦＬＵＴＥセッションでのＭＩＫＥＹを用いて行われる）、ＭＳＫを用いたＭＴＫの暗号化を行う。図１の分割アーキテクチャ１００では、大きな地理的領域が、複数のＢＭＳＣ（ＢＭＳＣ１　１０２、ＢＭＳＣ２　１０４及びＢＭＳＣ４　１０６）によってサービスの提供を受ける複数の地理的領域にセグメント化され（分割され）、単一のＢＶＰＳ１０８、西部地域にサービスを提供するスタンドアロンサーバ（ｗｅｓｔ．ｓｅｒｖｅｒ．ｃｏｍ１１０）、及び東部地域にサービスを提供するスタンドアロンサーバ（ｅａｓｔ．ｓｅｒｖｅｒ．ｃｏｍ１１２）と通信を行う。各スタンドアロンサーバ１１０、１１２は、通常、ＮＡＦ（Ｋｓ＿ｘｘ＿ＮＡＦからＭＲＫ及びＭＵＫを導出する）を行い、ＭＳＫ、ＭＳＫ－ＩＤ、処理登録、及びＭＵＫで暗号化されたＭＳＫをＵＥへ配信するなどの鍵要求を作成し、登録手続きに基づくユーザＩＭＰＩ及びＩＰへＭＳＫ－ＩＤのマッピングを維持し、加入者権限データベース（サービス＝サービスＩＤ及びＭＳＫ－ＩＤ；加入者＝ＩＭＰＩ／ＴＭＰＩ）を支援する。ＢＭＳＣ１０２、１０４、１０６の１つとスタンドアロンサーバとの間の交換は、ＢＭＳＣに対して配信セッションでのセキュリティサービスを生成することを許容し、スタンドアロンサーバに対してＭＳＫ、ＭＳＫ－ＩＤをＢＭＳＣへ安全に伝送することを可能にする。
【００１９】
図１に示すように、単一のＢＶＰＳ１０８は、複数の異なるＢＭＳＣのそれぞれに接続されうる。複数のＢＭＳＣのそれぞれは、単一のスタンドアロンサーバへ関連付けられ、一方で、単一のスタンドアロンサーバは、複数の異なるＢＭＳＣへサービスを提供することができる。ネットワークワイドチャネルＳＤＨＣ１１４が提供される場合は、ＵＥ１２２は、通常、自身の領域に対してサービスを提供するスタンドアロンサーバへ接続する。

初期接続において、スタンドアロンサーバ１１０への登録処理１２４がＵＥ１２２によって行われる。登録すると、ＵＥ１２２は、ＢＭＳＣ１　１０２によって提供されるローカル放送チャネルへ自身を調整し、当該ローカル放送チャネル１１６でコンテンツ及びメタデータを受信する。ＵＥ１２２が移動すると、ＢＭＳＣ２　１０４によって提供されるローカル放送チャネル１１８へ移行する。この移行はＢＭＳＣ間のモビリティ機能（移動性能）に関与する。ＵＥが移動し続けると、ＢＭＳＣ４によって提供されるローカル放送チャネル１２０へ移行し、スタンドアロンサーバ１１２のサービスの配下となる。この移行は、スタンドアロンサーバ間のモビリティ機能に関与するものであり、単に、前回の移行のＢＭＳＣ間のモビリティ機能に関与するものではない。そのような移動を行っているときに、ＵＥ１２２は、何らかの透過的な方法で同一のコンテンツの受信を継続できるべきである。これを容易にするために、鍵管理の集中化が必要となる。上述したように、ＵＥ１２２が同一のＭＳＫ／ＭＴＫ鍵を用いていない新たなＢＭＳＣへ移動すると、ユーザ経験に否定的な影響を与えるであろうサービスの中断を引き起こす、再登録が必要となろう。

【００２０】

分割アーキテクチャにおけるＭＳＫ及びＭＴＫ機能の集中化は、多くの種々の問題を与えてしまう。そのような問題の１つには、複数のＢＭＳＣが同一のスタンドアロンサーバの配下にあることに関わらず、同一のｅＭＢＭＳサービスを放送する各ＢＭＳＣがＭＳＫ及びＭＴＫ鍵の同一の組みを使用することをどのように保証するかという問題がある。ＭＳＫの集中化に関して、ｅＭＢＭＳシステムでは、ＢＭＳＣのそれぞれが、スタンドアロンサーバから受信する同一のＭＳＫを用いる。スタンドアロンサーバは、セントラル鍵サーバ、例えば、ＢＶＰＳからＭＳＫを受信することができる。スタンドアロンサーバは、ＢＶＰＳからＭＳＫを受信すると、ＭＳＫを複数のＢＭＳＣへ送信する。ＭＳＫの集中化は、ＭＳＫが頻繁に更新される必要が無い場合であれば本質的には実行可能であるように思われる。ＭＳＫが頻繁に変更される必要がない場合は、ＭＳＫの配信が、ネットワーク又はその複数のノード上での過剰な負荷をもたらす結果とはならないであろう。なお、本実施形態におけるＢＭＳＣは上述した複数のノード、即ち、ＢＶＰＳ、セントラル鍵サーバ、スタンドアロンサーバ又は鍵を調整するいくつかの他のノードのいずれかからＭＳＫを受信することができる。

【００２１】

ＭＴＫ管理の集中化によるスケーリング問題を解決するために、ＭＴＫ－ＩＤ及びＭＴＫは、ＢＭＳＣによって局所的に生成されうる。これは、多くの局所的な柔軟性を提供するものの、２つのＢＭＳＣが必ずしも同一のＭＴＫを生成することを保証しないという問題を引き起こす可能性はある。これは、通常、２つのＢＭＳＣが、同一の出力を生成することを保証するような明確な疑似乱数関数（ＰＲＦ）を有していないためである。

【００２２】

第２の形態において、セントラル鍵サーバ１２８はＭＴＫ１３０を複数のＢＭＳＣへ配信することができる。これは、所定のストリーミングサービス、又は、著作権侵害を防止するためのプログラムの実行中にＭＴＫ１３０を頻繁に（例えば、Ｘ秒ごとに）変更するサービス、に対して問題を引き起こす。さらに、これは、複数のＢＭＳＣとセントラル鍵サーバ１２８との間における過度の鍵配信トラフィックをもたらすかもしれない。ＭＴＫ（関連するＭＴＫ－ＩＤを有する）は、事前にまとめて複数のＢＭＳＣへ送信することができるが、まとめてＭＴＫを送信するオーバヘッドは各メッセージの各ＭＴＫを送信する場合よりも少ないものの、送信されるデータの総量は大きいままである。また、ＭＴＫはデータ送信中において保護される必要がある。

【００２３】

第３の形態において、各ＢＭＳＣは、予め定義された鍵導出関数（ＫＤＦ）と、集中化して配信されるランダム値（例えば、ＭＴＫごとに１つのランダム値）とを用いて、自身でＭＴＫを生成することができる。ランダム値（関連するＭＴＫ－ＩＤとともに）が送信される（完全なＭＴＫを送信する代わりに）場合には、これは、セントラル鍵サーバと各

ＢＭＳＣとの間のトラフィック負荷を減少させることができる。しかしながら、ＢＭＳＣの数及び他の要因に基づき、トラフィック負荷は、依然として非常に高い可能性がある。上述した効果を増大させるために、ランダム値（ＭＴＫ－ＩＤとともに）がまとめて複数のＢＭＳＣへ送信されてもよい。ランダム値は、伝送中に保護される必要がある（しかし、全てのＢＭＳＣがＭＴＫの生成の入力として使用される共通のロングターム・シークレット値を知っていれば、第２の形態と同様のケアをする必要はない）。

【００２４】

本発明の提案される解決手法である第４の形態において、各ＢＭＳＣは、入力として、他のパラメータから、ＭＳＫ及びＭＳＫ－ＩＤ（シーケンス番号である）を用いて自身でＭＴＫを生成する。これは、複数のＢＭＳＣが、上述したＭＴＣ鍵配信の形態で説明した問題が発生することなく、同一のオーダーで同一のＭＴＫを生成することを可能にする。そのような実施形態において、ＭＴＫの生成は、ＭＴＫ＝ＫＤＦ(MSK, MTK-seed, “MTK generation”)の形式であってもよい。ＫＤＦ（鍵導出関数）は、３ＧＰＰ　ＴＳ３３．２２０に定義されたＫＤＦなどの標準的な関数である。ＭＳＫは、ＭＢＭＳサービス鍵であってもよく、当該アルゴリズムはセキュリティに関してＫＤＦにあるシークレットを信頼する。他のパラメータは、ＫＤＦへの入力であってもよい（例えば、サービスＩＤ、鍵ドメインＩＤ、ＭＳＫ－ＩＤ、ＭＵＫ、ＭＲＫ、ＣＫ｜｜ＩＫ、又は他の入力）。これらのパラメータは異なるオーダーで用いられてもよい。追加のパラメータの選択及びそれらのオーダーの変化は、セキュア生成関数にもたらされてもよい。これらのパラメータは、ＫＤＦへの入力される前に変換されてもよく、例えば、ＭＳＫは、第１に他の（又は同一の）鍵導出関数へ入力され、そのＫＤＦへの入力結果を通じて変換されてもよく、又は他の文字列が入力として用いられてもよい。

【００２５】

そのような実施形態において、ＭＴＫ－ｓｅｅｄは、ＭＴＫ－ｓｅｅｄ＝ＫＤＦ（ＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹ、ＭＴＫ－ＩＤ）の形式で表され、ここで、ＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹは複数のＵＥによってではなく複数のＢＭＳＣによって知られた鍵であるＭＴＫ－ＩＤは、ＭＴＫの結果として生じるＩＤである。ＭＴＫ＝ＩＤは、通常、ＭＢＭＳのシーケンス番号であるが、他の種別の識別子であってもよく、ＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹは、文字列で定義されている。上述したように、他のパラメータは、様々なオーダーでＫＤＦへ入力されてもよく、それらはさらにＫＤＦへ使用される前に変換されてもよい。そのようなシステムを図２に示す。

【００２６】

図２の例示のアーキテクチャ１２６において、モビリティが、セントラル鍵サーバ１２８の使用を通じて改善される。ＭＳＫの集中化に関し、図２の例示のｅＭＢＭＳサービスについて、スタンドアロンサーバ配下の複数のＢＭＳＣのそれぞれは、通常、スタンドアロンサーバ又は鍵を調整するいくつかの他のノードから受信した、同一のＭＳＫを使用する。したがって、ＢＭＳＣ１　１０２及びＢＭＳＣ２　１０４のそれぞれは、スタンドアロンサーバ１１０からＭＳＫ１３０を受信する。スタンドアロンサーバ１１０は、セントラル鍵サーバ１２８からＭＳＫ１３０を受信している。当該セントラル鍵サーバ機能は、ＢＶＰＳ１０８又はその他のノードに含まれてもよい。ＭＳＫの集中化は、頻繁に更新する必要がない場合には上述したように実行可能であり、ＭＳＫ配信がトラフィック負荷の問題を引き起こすことはない。なお、セントラル鍵サーバ１２８は、ＭＳＫ１３０を、ＢＭＳＣ４　１０６へ提供するスタンドアロンサーバ１１２へ提供することができる。

【００２７】

当業者は、本実施形態が、ＭＳＫが通常、各ＢＭＳＣで既に利用可能であり、効果的なランダム値であるため十分に保護されることが想定されうる、多くの構成上の利点を得ることを理解するであろう。当該鍵は、複数のＢＭＳＣへ提供されうる。ＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹは、いくつかの実施形態において、実際には永続的（又は相対的に永続的）である。ＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹを変更する必要が無い場合、その送信は、システム初期化（又は他のイベント）中に行われ、全体のトラフィック負荷を

低減することができる。或いは、ＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹは、周期的に更新されうる（異なる頻度で更新する異なる実装で）。さらに、ＭＢＭＳ鍵の階層化（３ＧＰＰ　ＴＳ３３．２４６によって定義されているような）では、多くのＭＴＫがＭＳＫで保護される。ＭＳＫ及びＭＴＫが生成される方法は、そのような標準規格で定義されていない。ＭＴＫがＭＳＫから導出される場合、一般的に、システム又はｅＭＢＭＳサービスのセキュリティとしてＭＢＭＳのセキュリティをを変更せず、ＭＳＫのセキュリティを信頼し、ＭＳＫからＭＴＫを導出する強固なＫＤＦを用いることによって、鍵分割が保証され、ＭＴＫからＭＳＫを導出する逆方向への変換はできない。ＫＤＦへのＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹへの導入は、ＭＳＫを取得する悪意あるパーティが、将来的にＭＴＫ鍵を生成することを防止しうる。ＭＳＫ及びＭＴＫ＿ｇｅｎｅｒａｔｉｏｎ＿ＫＥＹの両方が情報漏洩した場合、悪意あるパーティは、複数の値のうちの１つが更新されるまでに固定の時間間隔における鍵を生成することができるのみである。ＫＤＦにおけるＭＴＫ－ＩＤ（即ち、シーケンス番号）の使用は、生成される種々のＭＴＫをもたらし、従って、共通のＭＳＫを有するよりも他の外部の調整なしで、同一のＭＴＫ－ＩＤでＭＴＫの同一のセットを生成することができる種々のＢＭＳＣをもたらす。なお、ＵＥ及びＵＩＣＣのいずれもが上述した実施形態による影響を受けないことに注意されたい。

【００２８】

上述したように、ＭＳＫ及びＭＴＫの集中化は、ＵＥが境界で第１のＢＭＳＣから第２のＢＭＳＣ（及び可能な元の位置）を行ったり来たりするように動く場合のピンポン問題と同じく、ＢＭＳＣ間のモビリティ、スタンドアロンサーバ間のモビリティの両方を緩和することができる。集中化した鍵管理で使用する場合、各ＢＭＳＣが同一のＭＳＫ／ＭＴＫ鍵を効果的に使用するため、ＵＥは、任意のスタンドアロンサーバへの初期登録を実行し、正しいＭＳＫ／ＭＴＫを受信することができる。

【００２９】

図３は、ＢＭＳＣで実行される方法の一例を示す。ステップ２００において、ＢＭＳＣは、ＭＴＫ生成関数を受信する。ＭＴＫ生成関数は、上述したように、セントラル鍵管理サービスによって設定され、静的（ＢＭＳＣの初期設定中プログラムされる場合）であるか、或いは、動的であって周期的に送信される。ステップ２０２で、ＢＭＳＣは、生成されたＭＳＫを受信する。このＭＳＫはＭＴＫの生成にステップ２０４で使用される。当業者には、当該鍵生成関数及びＭＳＫがセントラル鍵管理サービスで創出されるものの、それらはスタンドアロンサーバなどの中間ノードによって受信されることが理解されるであろう。鍵生成関数は、ＭＴＫの生成において、ＭＳＫ及びＭＴＫシード値を使用し、選択的に、サービスＩＤ、鍵ドメインＩＤ、受信されるＭＳＫに関連付けられるＭＳＫ－ＩＤ、ＭＲＫ及びＣＫ｜｜ＩＫの何れか１つを使用してもよい。当業者はまた、ＭＴＫシード値が、集中化した鍵管理サービスから受信される値に基いてＢＭＳＣ自身で生成されることを理解するであろう。

【００３０】

図４は、集中化した鍵管理サーバで実行される方法の一例を示す。ステップ２０６で、ＭＳＫが生成される。ＭＳＫはステップ２０８でＢＭＳＣへ送信されるが、対応するＭＴＫは送信されない。ステップ２１０で、復号化鍵がＵＥへ送信され、ＵＥがＢＭＳＣによって（図３で説明したプロセスを用いて）生成されたＭＴＫを用いて暗号化されたコンテンツを復号することを可能にする。当業者は、対称の暗号化システムにおいて、復号化鍵がＭＴＫであることを理解するであろう。集中化した鍵管理サーバは、意図した受け手へ中継する（鍵を要求した受け手が待機している可能性があれば）中間ノードへＭＳＣを送信することによって、ＭＳＫをそれらの宛先（例えば、ＢＭＳＣ）へ送信してもよい。さらに、サーバは、鍵生成関数をＢＭＳＣへ送信し、ＢＭＳＣが受信したＭＳＫに基づいてＭＴＫを生成することを可能にする。

【００３１】

図５は、プロセッサ３０２、ネットワークインターフェース３０４、及びメモリ３０６を備えるノード３００の一例を示す。メモリ３０６は、プロセッサ３０２によって実行さ

れた場合に、ノード３００が図３及び図４の何れかの方法を実行する（格納された命令に従って）ことを可能とする命令を格納するために使用されうる。ノード３００は、当業者が理解しうる方法でネットワークインターフェース３０４を通じて他のノードと通信を行う。さらに、ノード３００が上述したセントラル鍵サーバ１２８又はＢＭＳＣノードとして使用され、メモリ３０６が上述した種々の実施形態を実行するために必要な命令を格納することが理解されるであろう。

【００３２】

本発明の実施形態は、機械で読取可能な媒体（それらの具現化されたコンピュータで読取可能なプログラムコードを有する、コンピュータで読取可能な媒体、プロセッサで読取可能な媒体又はコンピュータで使用可能な媒体とも称する。）に格納されたプログラムとして実現されてもよい。機械で読取可能な媒体とは、ディスケット、コンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク読み取り専用メモリ（ＤＶＤ－ＲＯＭ）、メモリデバイス（揮発性又は不揮発性）又は類似の記憶機構などの、磁性的な、光学的な又は電気的な記憶媒体を含む任意の適切な有形の媒体であってもよい。機械で読取可能な媒体は、命令、コードシーケンス、設定情報、又は他のデータを含んでもよく、実行されると、プロセッサに本発明の実施形態に係る方法の各ステップを実行させるように機能する。当業者は、本発明を実現するために必要な他の命令やオペレーションが機械で読取可能な媒体に格納されうることを理解するであろう。機械で読取可能な媒体から実行されるソフトウェアは、上述したタスクを実行する回路とインターフェースで接続されうる。

【００３３】

本発明の上述した実施形態は、例示として意図されている。代替、修正及び変化が、本発明の範囲から逸脱することなく、添付の特許請求の範囲によって定義された範囲内で当業者によって特定の実施形態へもたらされうる。

【図１】

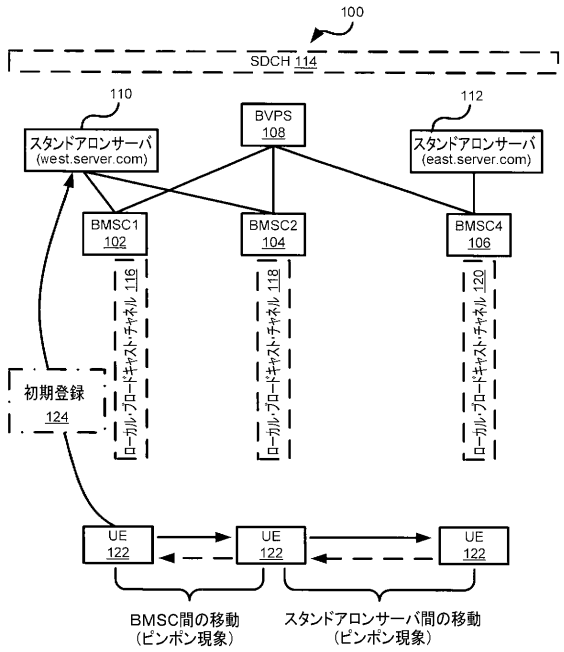

Figure 1

【図２】

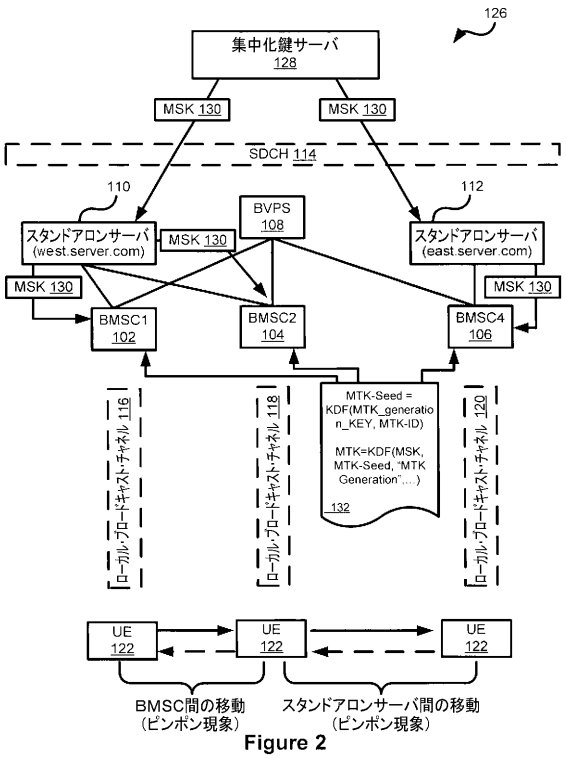

Figure 2

【図３】

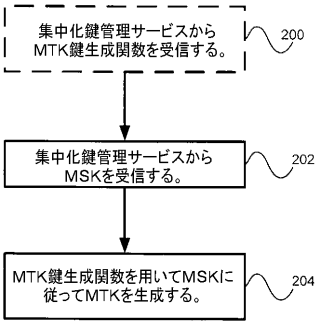

Figure 3

【図４】

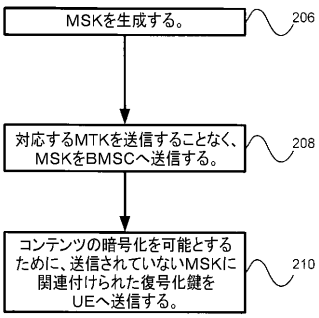

Figure 4

【図５】

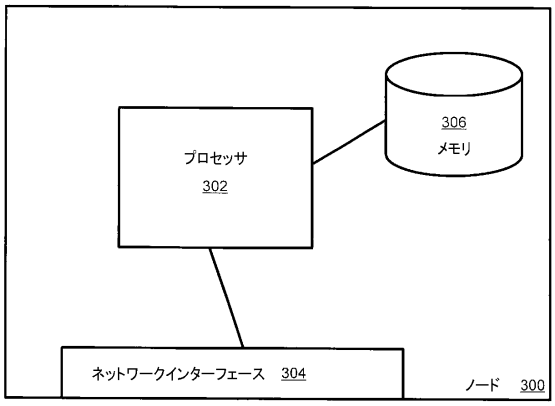

Figure 5

フロントページの続き

(72)発明者 レヘトヴィルタ, ベサ
フィンランド国 エスポー エフアイー０２６２０, ヴェインインマキ １０ビー
(72)発明者 ノルマン, カール
スウェーデン国 ストックホルム エスー１１６ ２８, スティグベルグスガタン ３２エー
(72)発明者 スルシンガル, ミカエル ジョン
スウェーデン国 スケールホルメン エスー１２７ ４６, エークホルムスヴェーゲン ２５３
(72)発明者 ターコット, ジョセフ エリック
カナダ国 ケベック州 エイチ４ピー １エヌ６, モントリオール, ブライユ ４２２２

審査官 青木 重徳

(56)参考文献 米国特許出願公開第２００８／０００９２７４（ＵＳ，Ａ１）
特表２０１０－５２７２１１（ＪＰ，Ａ）
特開２００９－０７１８５４（ＪＰ，Ａ）
特表２０１１－５２３２８３（ＪＰ，Ａ）
特表２００８－５２７８９９（ＪＰ，Ａ）
国際公開第２０１０／１１４４７５（WO，Ａ１）
David Lecompte, et al., Evolved Multimedia Broadcast/Multicast Service (eMBMS) in LTE-Advanced: Overview and Rel-11 Enhancements, IEEE Communication Magazine, 米国, IEEE, ２０１２年１１月, pp.68-74

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｗ ４／０６
Ｈ０４Ｗ １２／０４