【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和1年12月26日(2019.12.26)

【公表番号】特表2019-506779(P2019-506779A)
【公表日】平成31年3月7日(2019.3.7)
【年通号数】公開・登録公報2019-009
【出願番号】特願2018-532084(P2018-532084)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｗ　4/70　(2018.01)
Ｈ０４Ｗ　12/02　(2009.01)
Ｈ０４Ｗ　12/08　(2009.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｗ　12/04
Ｈ０４Ｗ　4/70
Ｈ０４Ｗ　12/02
Ｈ０４Ｗ　12/08
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】令和1年11月18日(2019.11.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ゲートウェイにおける通信の方法であって、
第1の鍵を取得するステップと、
前記第1の鍵、および無線アクセスネットワーク(RAN)ノードに固有のパラメータに基づいている、第2の鍵を取得するステップと、
前記第2の鍵を前記RANノードに供給するステップと、
前記第2の鍵、およびセルラーデバイスに固有のパラメータに基づいて、第3の鍵を取得するステップと、
前記第3の鍵を前記セルラーデバイスに供給するステップであって、前記第1の鍵は、前記RANノードおよび前記セルラーデバイスに知られておらず、前記ゲートウェイに知られている、ステップと
を備える方法。
【請求項２】
前記第2の鍵は、非アクセス層(NAS)メッセージの中で前記RANノードに供給される、請求項1に記載の方法。
【請求項３】
前記第3の鍵は、セキュアな非アクセス層(NAS)メッセージの中で前記セルラーデバイスに供給される、請求項1に記載の方法。
【請求項４】
前記第3の鍵は、暗号化された情報要素(IE)として前記セルラーデバイスに供給され、

前記IEは、前記IEを暗号化するために使用されたアルゴリズムを識別するアルゴリズム識別子を含む、請求項1に記載の方法。
【請求項５】
ゲートウェイであって、
通信ネットワークのノードと通信するための通信インターフェースと、
前記通信インターフェースに結合された処理回路とを備え、前記処理回路は、
第1の鍵を取得し、
前記第1の鍵、および無線アクセスネットワーク(RAN)ノードに固有のパラメータに基づいている、第2の鍵を取得し、
前記第2の鍵を前記RANノードに供給し、
前記第2の鍵、およびセルラーデバイスに固有のパラメータに基づいて、第3の鍵を取得し、
前記第3の鍵を前記セルラーデバイスに供給し、前記第1の鍵は、前記RANノードおよび前記セルラーデバイスに知られておらず、前記ゲートウェイに知られているよう適合される、
ゲートウェイ。
【請求項６】
前記処理回路は、
いかなる他の鍵からも前記第1の鍵を取得することなく、前記第1の鍵を取得するよう、および/または
前記ゲートウェイにおいて前記第1の鍵をランダムに生成することによって、前記第1の鍵を取得するよう、さらに適合される、
請求項5に記載のゲートウェイ。
【請求項７】
無線アクセスネットワーク(RAN)ノードであって、
通信ネットワークのノードと通信するための通信インターフェースと、
前記通信インターフェースに結合された処理回路とを備え、
前記処理回路は、
第1の鍵に基づいている第2の鍵をゲートウェイから取得し、前記RANノードに固有のパラメータを取得し、
デバイス識別情報および第1の完全性保護値を含むスモールデータメッセージをセルラーデバイスから取得し、
前記第2の鍵および前記デバイス識別情報に基づいている第3の鍵を取得し、
前記第3の鍵に基づいている第2の完全性保護値を取得し、
前記第1の完全性保護値を前記第2の完全性保護値と比較し、
前記第1の完全性保護値が前記第2の完全性保護値に等しくないことを比較結果が示す場合、前記スモールデータメッセージを廃棄し、
前記第1の完全性保護値が前記第2の完全性保護値に等しいことを前記比較結果が示す場合、前記スモールデータメッセージを前記ゲートウェイへ送信し、前記第1の鍵は、前記RANノードおよび前記セルラーデバイスに知られておらず、前記ゲートウェイに知られているよう適合される、
無線アクセスネットワーク(RAN)ノード。
【請求項８】
前記第1の完全性保護値および前記第2の完全性保護値は、少なくとも1つのナンスおよび/またはタイムスタンプを使用して取得され、
前記処理回路は、
第1のナンスおよび/もしくは前記タイムスタンプを、前記デバイス識別情報によって識別されるデバイスに供給するよう、ならびに/または
前記デバイスから第2のナンスを取得するよう、
さらに適合される、

請求項7に記載の無線アクセスネットワーク(RAN)ノード。
【請求項９】
前記処理回路は、
ランダムアクセスプロシージャの間に、前記第1のナンスおよび/または前記タイムスタンプを供給し、前記第2のナンスを取得するよう、さらに適合される、
請求項8に記載の無線アクセスネットワーク(RAN)ノード。
【請求項１０】
前記スモールデータメッセージは、前記第3の鍵を用いて暗号化されており、
前記処理回路は、
前記第3の鍵を使用して前記スモールデータメッセージを解読するよう、さらに適合される、
請求項7に記載の無線アクセスネットワーク(RAN)ノード。
【請求項１１】
前記処理回路は、
トラフィック負荷値を監視し、
前記トラフィック負荷値が所定のしきい値を上回ることを検出し、
前記トラフィック負荷値が前記所定のしきい値を上回るという検出に応答して、前記デバイス識別情報によって識別されるデバイスへ、前記RANノードへ送信される次の1つまたは複数のメッセージの中に前記第1の完全性保護値を含めるよう前記デバイスに要求するメッセージを送信するよう、
さらに適合される、
請求項7に記載の無線アクセスネットワーク(RAN)ノード。
【請求項１２】
ネットワークは前記所定のしきい値を構成する、請求項11に記載の無線アクセスネットワーク(RAN)ノード。
【請求項１３】
前記処理回路は、
少なくとも1つのナンスおよび/またはタイムスタンプを使用して、前記第1の完全性保護値および前記第2の完全性保護値を取得するよう、さらに適合される、
請求項7に記載の無線アクセスネットワーク(RAN)ノード。
【請求項１４】
前記処理回路は、
デバイスとの初期接続プロシージャの間にアクセス層セキュリティ構成を折衝するようさらに適合され、前記アクセス層セキュリティ構成は、スモールデータメッセージが前記デバイスから、セキュリティを用いずに送信されるのか、完全性保護を用いて送信されるのか、暗号化を用いて送信されるのか、完全性保護および暗号化を用いて送信されるのか、および/またはオンデマンド完全性保護を用いて送信されるのかを指定し、完全性保護および暗号化は、前記第3の鍵を使用して実行される、
請求項7に記載の無線アクセスネットワーク(RAN)ノード。
【請求項１５】
セルラーデバイスであって、
通信ネットワークのノードと通信するための通信インターフェースと、
前記通信インターフェースに結合された処理回路とを備え、
前記処理回路は、
第2の鍵に基づいている第3の鍵をゲートウェイから取得し、前記セルラーデバイスに固有のパラメータを取得し、前記第2の鍵は、第1の鍵、およびRANノードに固有のパラメータに基づいており、前記第1の鍵は、前記ゲートウェイに知られており、前記セルラーデバイスおよび前記RANノードに知られておらず、
前記RANノードとアクセス層セキュリティ構成を折衝し、
前記第3の鍵を使用して前記アクセス層セキュリティ構成に基づいてスモールデータ

メッセージを保護し、

前記第3の鍵を使用して保護された前記スモールデータメッセージを前記RANノードへ送信するよう、適合される、

セルラーデバイス。