201921886

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201921886 A

(43)公開日： 中華民國 108 (2019) 年 06 月 01 日

(21)申請案號：107124928 (22)申請日： 中華民國 107 (2018) 年 07 月 19 日

(51)Int. Cl.： *H04L9/14 (2006.01)*

(30)優先權：2017/08/23 印度 201741029838

2017/12/08 美國 15/835,943

(71)申請人：美商高通公司 (美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：巴明蒂 雷維奇瑞 BAMIDI, RAVI KIRAN (IN)；奇哈瓦 奇雷格瑪農傑庫瑪 KHARVAR, CHIRAG MANOJKUMAR (IN)

(74)代理人：李世章

申請實體審查：無 申請專利範圍項數：30 項 圖式數：7 共 51 頁

(54)名稱

用於經最佳化的網路層訊息處理的系統和方法

SYSTEMS AND METHODS FOR OPTIMIZED NETWORK LAYER MESSAGE PROCESSING

(57)摘要

描述了一種由網狀設備進行的方法。該方法包括以下步驟：利用與接收的封包的網路辨識符（NID）相匹配的隱私金鑰來對該封包的第一資訊進行去混淆。該方法亦包括以下步驟：基於經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密。

A method by a mesh device is described. The method includes de-obfuscating first information of a received packet with a privacy key that matches a network identifier (NID) of the packet. The method also includes determining whether to decrypt second information of the packet based on the de-obfuscated first information.

指定代表圖：

TW 201921886 A

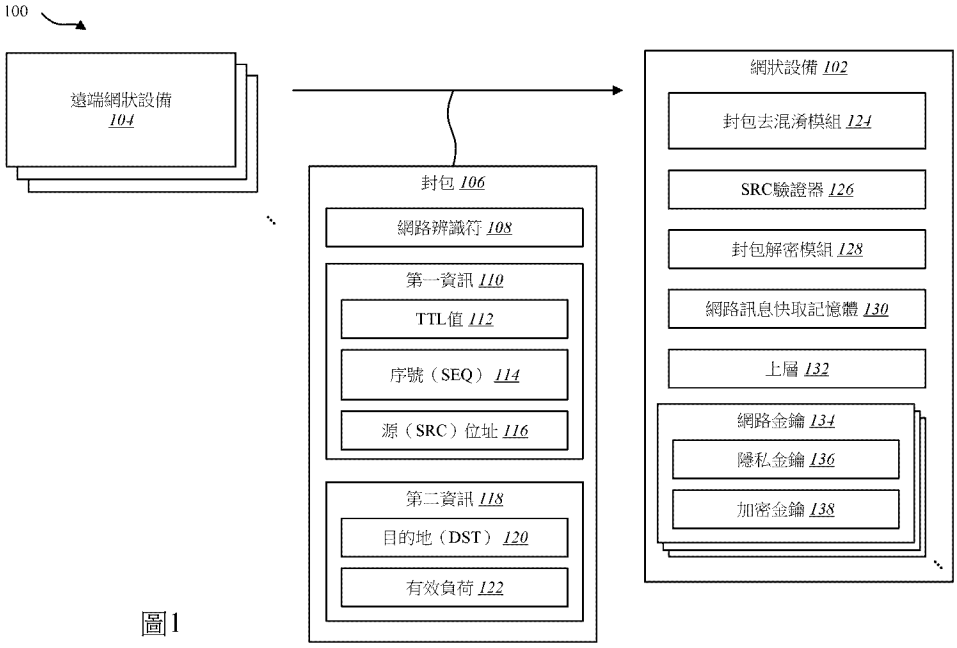

圖1

符號簡單說明：

100・・・網狀網路

102・・・網狀設備

104・・・遠端網狀設備

106・・・封包

108・・・匹配的 NID

110・・・第一資訊

112・・・存活時間(TTL)值

114・・・SEQ

116・・・SRC

118・・・第二資訊

120・・・DST

122・・・有效負荷

124・・・封包去混淆模組

126・・・SRC 驗證器

128・・・封包解密模組

130・・・網路訊息快取記憶體

132・・・上層

134・・・網路金鑰

136・・・隱私金鑰

138・・・加密金鑰

【發明說明書】

【中文發明名稱】用於經最佳化的網路層訊息處理的系統和方法

【英文發明名稱】SYSTEMS AND METHODS FOR OPTIMIZED NETWORK LAYER MESSAGE PROCESSING

【技術領域】

【0001】 本案與以下申請案相關並且主張來自以下申請案的優先權：於2017年8月23日提出申請的、針對「SYSTEMS AND METHODS FOR OPTIMIZED NETWORK LAYER MESSAGE PROCESSING」的印度臨時專利申請案第201741029838。

【0002】 大體而言，本案內容係關於無線通訊。更具體地，本案內容係關於用於經最佳化的網路層訊息處理的系統和方法。

【先前技術】

【0003】 在最近數十年來，對無線通訊設備的使用已經變得常見。具體而言，電子技術的發展已經減少了日益複雜並且有用的無線通訊設備的成本。成本減少以及消費者需求已經使得對無線通訊設備的使用激增，從而使得無線通訊設備在現代社會中幾乎無處不在。隨著對無線通訊設備的使用已經擴張，對無線通訊設備的新的並且改良的特徵的需求亦隨之擴張。更具體而言，執行新功能及/或更快、更高效或更可靠地執行功能的無線通訊設備常常是所追求的。

【0004】 技術的進步已經導致更小且更強大的無線通訊設備。例如，目前存在各種無線通訊設備，諸如均是小型、羽量級並且能夠容易被使用者攜帶的可攜式無線電話（例如，智慧型電話）、個人數位助理（PDA）、膝上型電腦、平板電腦和傳呼設備。

【0005】 無線通訊設備可以利用一或多個無線通訊技術。例如，無線通訊設備可以使用藍芽技術或其他無線技術進行通訊。在一些情況下，無線通訊設備可以是網狀網路中的節點。目前，網狀網路中的網狀設備所接收的封包在對照網路金鑰被認證之前必須被去混淆並且解密。然而，可以經由基於來自封包的經去混淆的資訊來決定是否要執行解密認證，從而最佳化網路層訊息處理。

【發明內容】

【0006】 描述了一種由網狀設備進行的方法。該方法包括以下步驟：利用與接收的封包的網路辨識符（NID）相匹配的隱私金鑰來對該封包的第一資訊進行去混淆。該方法亦包括以下步驟：基於經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密。

【0007】 該封包可以是藍芽低能網狀封包。該第一資訊可以包括序號（SEQ）及/或源（SRC）位址中的至少一項。該第二資訊可以包括目的地（DST）資訊和有效負荷。

【0008】 決定是否要對該第二資訊進行解密可以包括：決定該封包的該SRC位址是有效的。決定該封包的

該SRC位址是有效的可以包括：決定該SRC位址不是未被指派的群組位址或虛擬位址。決定該封包的該SRC位址是有效的可以包括：決定該SRC位址不屬於該網狀設備。若該SRC位址是無效的，則該方法亦可以包括以下步驟：使用具有與該封包的該NID相匹配的NID的所有已知網路來決定該封包的該SRC位址是否是有效的。若該SRC位址是無效的，則該封包可以在不對該第二資訊進行解密的情況下被丟棄。

【0009】 若該SRC位址是有效的，則決定是否要對該第二資訊進行解密亦可以包括：決定在網路訊息快取記憶體中是否已經存在該封包的SEQ和該SRC位址。若在該網路訊息快取記憶體中已經存在該封包的該SEQ和該SRC位址，則該封包可以在不對該第二資訊進行解密的情況下被丟棄。若在該網路訊息快取記憶體中不存在該封包的該SEQ和該SRC位址，則該第二資訊可以被解密。

【0010】 亦描述一種網狀設備。該網狀設備包括：處理器；記憶體，其與該處理器相通訊；及被儲存在該記憶體中的指令。該等指令可由該處理器執行以進行以下操作：利用與接收的封包的NID相匹配的隱私金鑰來對該封包的第一資訊進行去混淆。該等指令亦可執行以進行以下操作：基於經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密。

【0011】 亦描述了一種儲存電腦可執行代碼的非暫時性有形電腦可讀取媒體。該電腦可讀取媒體包括：用於使

得網狀設備利用與接收的封包的NID相匹配的隱私金鑰來對該封包的第一資訊進行去混淆的代碼。該電腦可讀取媒體亦包括：用於使得該網狀設備基於經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密的代碼。

【0012】 亦描述一種裝置。該裝置包括：用於利用與接收的封包的NID相匹配的隱私金鑰來對該封包的第一資訊進行去混淆的構件。該裝置亦包括：用於基於經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密的構件。

【圖式簡單說明】

【0013】 圖1是圖示其中可以實現經最佳化的網路層訊息處理的無線通訊系統的一種配置的方塊圖；

【0014】 圖2是圖示用於經最佳化的網路層訊息處理的方法的流程圖；

【0015】 圖3是圖示用於經最佳化的網路層訊息處理的另一種方法的流程圖；

【0016】 圖4圖示網狀網路通訊協定資料單元（PDU）的實例；

【0017】 圖5是圖示用於根據藍芽網狀規範的網路層訊息處理的方法的流程圖；

【0018】 圖6是圖示用於經最佳化的網路層訊息處理的方法的流程圖；及

【0019】 圖7圖示可以被包括在網狀設備內的某些元件。

【實施方式】

【0020】 現在參照附圖描述各種配置，其中相同的元件符號可以指示功能上相似的元素。可以在多種多樣的不同配置中佈置和設計如本文附圖中整體描述並且圖示的系統和方法。因此，下文對如在附圖中表示的若干配置的更詳細的描述並不意欲限制系統和方法的範疇（如所主張保護的），而僅是代表該等系統和方法。

【0021】 圖1是圖示其中可以實現經最佳化的網路層訊息處理的無線通訊系統的一種配置的方塊圖。無線通訊系統可以包括網狀設備102和一或多個遠端網狀設備104。無線通訊系統被廣泛地部署以提供諸如語音、資料等的各種類型的通訊內容。

【0022】 一些無線通訊設備可以使用多種通訊技術。例如，一種通訊技術可以用於行動無線系統（MWS）（例如，蜂巢）通訊，而另一種通訊技術可以用於無線連接（WCN）通訊。MWS可以代表較大的無線網路（例如，無線廣域網路（WWAN）、蜂巢式電話網路、長期進化（LTE）網路、行動通訊全球系統（GSM）網路、分碼多工存取(CDMA)網路、CDMA 2000網路、寬頻CDMA（W-CDMA）網路、通用行動電信系統（UMTS）網路、全球互通微波存取性（WiMAX）網路等）。WCN可以代表相對較小的無線網路（例如，無線區域網路（WLAN）、無線個人區域網路（WPAN）、電氣與電

子工程師協會（IEEE）802.11（Wi-Fi）網路、藍芽（BT）網路、無線通用序列匯流排（USB）網路等）。

【0023】 無線通訊系統（例如，多工存取系統）中的通訊可以經由無線鏈路上的傳輸來實現。此種無線鏈路可以是經由單輸入單輸出（SISO）、多輸入單輸出（MISO）或多輸入多輸出（MIMO）系統來建立的。MIMO系統包括傳輸器和接收器，其分別被配備有用於資料傳輸的多個（N_T個）傳輸天線和多個（N_R個）接收天線。SISO和MISO系統是MIMO系統的特定實例。若利用由多個傳輸和接收天線建立的額外維度，則MIMO系統可以提供改良的效能（例如，更高的輸送量、更大的容量或改良的可靠性）。

【0024】 網狀設備102是可以被配置為使用藍芽網狀協定或其他網狀協定來進行通訊的電子設備。網狀設備102亦可以被稱為無線通訊設備、無線設備、行動設備、行動站、用戶站、客戶端、客戶端站、使用者設備（UE）、遠端站、存取終端、行動終端、終端、使用者終端、用戶單元等。網狀設備102的實例係包括膝上型電腦或者桌上型電腦、蜂巢式電話、智慧型電話、無線數據機、電子閱讀器、平板設備、遊戲系統、鍵盤、小鍵盤、電腦滑鼠、遠端控制器、耳機、頭戴式耳機、無線揚聲器、感測器、路由器、計量儀、物聯網路（IoT）設備、醫療設備等。

【0025】 在一種實現中，網狀設備102可以使用藍芽協定進行通訊。藍芽設備可以被配置為與具有藍芽收發機的

一或多個目標設備建立鏈路。藍芽是具有主-從結構的基於封包的協定。藍芽在工業、科學和醫療(ISM)2.4 GHz短距離射頻頻帶（例如，2400－2483.5 MHz）中進行操作。藍芽使用被稱為躍頻擴展頻譜的無線電技術，其中傳輸的資料被劃分為封包106，並且每個封包106是在指定的藍芽頻率（例如，通道）上傳輸的。

【0026】 可以基於主設備輪詢系統來實現藍芽網路中的通訊。主設備輪詢系統可以利用分時雙工（TDD），其中藍芽設備可以向目標設備發送封包106。例如，遠端藍芽設備可以在配對期間或在連接請求期間向藍芽設備發送封包106。在一種實現中，藍芽設備可以是主設備，而目標藍芽設備可以是從設備。在主設備輪詢系統中，發送封包106的藍芽設備給予從無線設備用於傳輸返回的能力。

【0027】 藍芽無線通訊標準通常用於在短距離內在固定或行動的啟用藍芽的設備之間交換通訊。在一些配置中，本文揭示的系統和方法可以應用於藍芽低能（BLE）設備。LE代表藍芽標準的「低能」擴展。BLE擴展集中於能量受限的應用，例如，電池供電的設備、感測器應用等。BLE擴展亦可以被稱為藍芽智慧。

【0028】 以下描述使用與藍芽和藍芽LE標準相關聯的術語。然而，該等概念可以適用於涉及調制和傳輸數位資料的其他技術和標準。因此，儘管依據藍芽標準提供了一

些描述，但是可以更通常在可能不符合藍芽標準的無線通訊設備中實現本文揭示的系統和方法。

【0029】 應當注意的是，藍芽網狀協定可以用在非藍芽設備（例如，WiFi-藍芽閘道）上。該等非藍芽設備可以實現網狀，以在傳輸控制協定（TCP）及/或使用者資料包通訊協定（UDP）上遠端地接收封包106（例如，網路通訊協定資料單元（PDU）），並且隨後可以在BLE上發送封包106。

【0030】 網狀網路100可以包括多個節點。在一種實現中，節點可以被稱為物聯網路（IoT）設備、IOT節點或者網狀節點，此舉取決於在其之下的技術。網狀網路100亦可以被稱為IoT網路。在一種方法中，網狀網路100可以將藍芽低能用作底層無線電技術來在設備之間進行通訊。

【0031】 在藍芽網狀簡介網路中，傳輸藍芽設備可以向接收藍芽設備發送封包106（亦被稱為網路PDU）。藍芽網狀聯網規範定義了對於實現針對BLE無線技術的交互操作網狀聯網的要求。結合圖4描述了根據藍芽網狀簡介的網路PDU的實例。

【0032】 在BLE網狀術語中，傳輸或接收網狀設備102可以被稱為網狀承載。承載是在其上傳輸或接收網狀網路PDU的協定。例如，可以經由網狀承載來傳輸或接收BLE通告、BLE通用屬性（GATT）連接、TCP/UDP等。

【0033】 在網路層訊息接收的情況下，藍芽網狀簡介規範聲明需要對所接收的封包106進行去混淆、解密並且對照網路金鑰134進行認證。結合圖5描述了藍芽網狀簡介規範中的用於網路層訊息接收的指定方法。

【0034】 可以以不同的方式來分發網路金鑰134。在第一種方法中，網狀設備102可以被設置有一或多個網路金鑰134。對基本資訊（例如，單播位址和網路金鑰134）進行認證並且向網狀設備102提供該基本資訊的過程被稱為設置或進行設置。網狀設備102必須被設置有網路金鑰134，以變成網狀網路100中的節點。一旦被設置，節點就可以在網狀網路100中傳輸或接收訊息。網路金鑰134可以用於在網路層處保護和認證訊息。

【0035】 用於向網狀設備102提供網路金鑰134的第二種方法是經由配置模型（一旦網狀設備102被設置有網路金鑰134）。例如，網狀設備102可以被配置有使用第一網路金鑰134的一或多個另外的網路金鑰134。

【0036】 封包106包括網路辨識符（NID）欄位108。NID欄位108可以包含7位元網路辨識符，其允許對用於對封包106進行認證和加密的隱私金鑰136和加密金鑰138的檢視。在一些實現中，可以以明文傳輸NID 108。

【0037】 網狀設備102可以知曉多個網路金鑰134。可以根據網路金鑰134來推導出NID 108，以使得每個網路金鑰134產生一個網路ID 108。然而，應當注意的是，多個網路可以具有相同的NID 108。可以結合隱私金鑰

136和加密金鑰138，根據網路金鑰134來推導出NID值108。可以根據網路金鑰134來推導出加密金鑰138。即使隱私金鑰136被損害，亦可以根據網路金鑰134，使用金鑰推導函數來推導出隱私金鑰136，以保護網路金鑰134。

【0038】 隱私金鑰136用於對封包106中的資訊（亦即，第一資訊110）進行混淆和去混淆。混淆是應用於資訊以有意地使得在不知道所應用的演算法的情況下難以對資訊進行反向的過程。去混淆是將經混淆的資訊變換回其原始的未被混淆的形式的過程。去混淆可以使用用於對資訊進行混淆的隱私金鑰136來執行。

【0039】 在一些實現中，混淆可以用作隱私機制，其利用高級加密標準（AES），以使用隱私金鑰136來對源（SRC）位址116、序號（SEQ）114和其他標頭資訊（例如，網路控制訊息指示（CTL）、存活時間（TTL）值112）進行編碼。混淆的意圖是使得追蹤節點更加困難。然而，應當注意的是，混淆並不需要秘密（例如，加密金鑰138）來理解資料。

【0040】 另一態樣，加密金鑰138可以用於對封包106中的資訊（亦即，第二資訊118）進行加密和解密。經加密的資訊與經混淆的資訊相比更為安全。可以僅使用秘密加密金鑰138來對經加密的資訊進行解密。然而，相比對資訊進行去混淆而言，對資訊進行解密的過程可能需要更多的計算資源。

【0041】 根據藍芽網狀簡介規範，在決定是接受還是丟棄接收的封包106之前，既對封包106中的資訊進行去混淆，亦對其進行解密。例如，參照圖5，在步驟508中(「網路金鑰驗證訊息完整性檢查（MIC）」)，網狀設備102必須使用AES電編碼簿（ECB）以及隱私金鑰136來對CTL、TTL 112、SEQ 114及/或SRC 116進行去混淆。該步驟亦包括網狀設備102使用以下項：使用具有加密金鑰138的AES-CCM對目的地（DST）120及/或有效負荷122的解密認證。

【0042】 因為多個網路可能具有相同的NID 108，所以需要辨識正確的網路金鑰134。換言之，當網狀設備102接收到封包106時，NID 108可能對於多個已知網路而言是相同的。在此種情況下，網狀設備102可能不知道何者網路金鑰134（以及因此隱私金鑰136和加密金鑰138）應當用於處理(例如，去混淆及/或解密)封包106。

【0043】 根據規範，SRC位址116應當是單播位址，其中最高有效位元是「0」。當網狀設備102利用錯誤的隱私金鑰136（亦即，由於使用錯誤的網路金鑰134）對封包106進行去混淆時，存在關於SRC位址116的最高有效位元（MSB）可能是「1」（其指示群組位址或虛擬位址）或「0」（其指示單播位址）的百分之50的機會。當SRC位址116具有設置為「1」的MSB時，此情形指示封包106是無效封包，並且無法用於進一步的處理。然而，根據網狀簡介規範，即使網狀設備102在去混淆之後知曉

此種情況，網狀設備102亦在丟棄封包106之前進一步進行解密和認證。

【0044】 在具有作為單播位址的SRC位址116的有效封包106的情況下，在對照已知網路的成功認證之後，網狀設備102可以經由將封包106與網路訊息快取記憶體130的內容進行比較，來檢查其是否已經被較早地處理。根據規範，序號（SEQ）114對於元素（SRC 116）而言是唯一的。每個新網路層封包106將具有新的SEQ 114。因為在對封包106的去混淆之後SEQ 114和SRC 116是可用的，所以若SEQ 114及/或SRC 116已經存在於網路訊息快取記憶體130中，則對整個封包106進行解密是不必要的。

【0045】 在以上場景中，對封包106的冗餘解密導致不必要的處理。此種處理浪費功率以及延遲新封包處理。經由決定基於經去混淆的資訊來決定是否對封包106的資訊進行解密，可以實現益處。

【0046】 網狀設備102可以包括封包去混淆模組124。封包去混淆模組124可以使用與接收的封包106的網路辨識符（NID）108相匹配的第一隱私金鑰136來對封包106的第一資訊110進行去混淆。經混淆的第一資訊110可以包括封包106的TTL值112、SEQ 114和SRC 116。

【0047】 網狀設備102可以被設置有或配置有多個網路金鑰134，其與封包106的NID 108相匹配。網狀設

備102可以從複數個設置/配置的網路金鑰134中選擇網路金鑰134。網狀設備102可以使用所選擇的網路金鑰134來獲得第一隱私金鑰136。封包去混淆模組124可以使用第一隱私金鑰136對封包106的第一資訊110（例如，TTL值112、SEQ 114和SRC 116）進行去混淆。

【0048】 網狀設備102亦可以包括SRC驗證器126。SRC驗證器126可以檢查SRC位址116是否是有效的。在一種方法中，SRC驗證器126可以決定SRC位址116是否不是未被指派的群組位址或虛擬位址。在未被指派的位址的情況下，SRC位址116可以具有空值（例如，SRC 116欄位的所有位元皆是0）。在群組位址或虛擬位址的情況下，SRC驗證器126可以決定SRC位址116的MSB是否是1（其指示群組位址或虛擬位址）。因此，若SRC位址116是全零或者若SRC 116的MSB是1，則SRC 116是無效的。

【0049】 SRC驗證器126亦可以決定封包106是否源自於網狀設備102。例如，封包106可以是由網狀網路100中的節點發送的，但是同一節點隨後可能從遠端網狀設備104接收作為被中繼的訊息的封包106。在此種情況下，封包106的SRC位址116將屬於網狀設備102。因此，若SRC位址116不是網狀設備102自身的元素位址之一，則SRC驗證器126可以決定SRC位址116是有效的。

【0050】 若SRC位址116是無效的，則網狀設備102可以嘗試利用具有匹配的NID 108的下一個網路金鑰

134對第一資訊110進行去混淆。例如，網狀設備102可以從已知網路金鑰134中選擇與NID 108相匹配的第二網路金鑰134。網狀設備102隨後可以使用與第二網路金鑰134相關聯的第二隱私金鑰136對第一資訊110進行去混淆。網狀設備102隨後可以嘗試對SRC位址116進行驗證，如上所描述的。

【0051】 網狀設備102可以重複關於選擇相匹配的網路金鑰134的該程序，直到SRC位址116被驗證或所有相匹配的網路金鑰134皆已經被使用為止。若使用已知網路金鑰134沒有獲得有效的SRC位址116，則網狀設備102可以丟棄封包106，而不對第二資訊118進行解密，此舉節省了處理時間和能量。

【0052】 若SRC位址116是有效的，則網狀設備102可以檢查在網路訊息快取記憶體130中是否已經存在SEQ 114及/或SRC位址116。例如，若網狀設備102已經接收到封包106，則網狀設備102可以將封包106保存在網路訊息快取記憶體130中。網狀設備102可以檢查SRC位址116是否已經在網路訊息快取記憶體130中。若是的話，網狀設備102可以進行檢查以決定SEQ 114是否指示封包106是新的。換言之，若所接收的封包106的SEQ 114與經快取的封包106的SEQ 114相同或小於經快取的封包106的SEQ 114，則在網路訊息快取記憶體130中已經存在經快取的封包106。在此種情況下，網狀

設備102可以丟棄所接收的封包106，而不對第二資訊118進行解密。

【0053】 若在網路訊息快取記憶體130中不存在所接收的封包106，則網狀設備102可以繼續對封包106進行解密和認證。網狀設備102可以包括封包解密模組128，其對封包106的第二資訊118（例如，DST 120及/或有效負荷122）進行解密。

【0054】 在對第二資訊118進行解密之後，網狀設備102可以決定目的地（DST）120是否是有效的。DST 120欄位可以是16位元的值，其辨識封包106所指向的一或多個元素。DST 120位址可以是單播位址、群組位址或虛擬位址。DST 120欄位可以是由源節點設置的，並且未被作為中繼節點操作的節點中的網路層改變。網狀設備102可以決定DST 120是否是有效的單播位址、群組位址或虛擬位址。若DST 120是無效的，則網狀設備102可以丟棄所接收的封包106。

【0055】 若DST 120是有效的，則網狀設備102可以將所接收的封包106添加到網路訊息快取記憶體130中。網狀設備102可以將所接收的封包106轉發給上層132以用於另外的處理。

【0056】 本文描述的系統和方法提供了與用於網路層訊息處理的現有方法相比的優勢。當利用具有相匹配的NID 108的錯誤網路（例如，網路金鑰134）進行處理時，對於50%的封包106，可以經由在去混淆之後立即驗

證SRC位址116來避免解密認證。對於所有重複或中繼的封包106，可以經由在去混淆之後立即將封包106的SEQ 114及/或SRC位址116與網路訊息快取記憶體130的內容進行比較，來避免解密認證。此舉帶來功率節省和改良的處理速度。

【0057】 圖2是圖示用於經最佳化的網路層訊息處理的方法200的流程圖。該方法200可以由連接到網狀網路100中的一或多個遠端網狀設備104的網狀設備102來實現。

【0058】 網狀設備102可以從遠端網狀設備104接收202封包106。封包106可以是藍芽低能網狀封包。

【0059】 網狀設備102可以利用與所接收的封包106的網路辨識符（NID）108相匹配的隱私金鑰136來對封包106的第一資訊110進行去混淆204。例如，網狀設備102可以選擇與封包106的NID 108相匹配的已知網路金鑰134。在一些實現中，網狀設備102可以使用AES-ECB以及與所選擇的網路金鑰134相關聯的隱私金鑰136來對第一資訊110進行去混淆204。封包106的第一資訊110可以包括序號（SEQ）114及/或源（SRC）位址116中的至少一項。

【0060】 網狀設備102可以基於經去混淆的第一資訊110來決定206是否要對封包106的第二資訊118進行解密。第二資訊118可以包括封包106的目的地（DST）120資訊和有效負荷122。

【0061】 決定是否要對第二資訊118進行解密可以包括決定封包106的SRC位址116是否是有效的。網狀設備102可以經由決定SRC位址116不是未被指派的群組位址或虛擬位址，來決定SRC位址116是有效的。網狀設備102亦可以經由決定SRC位址116不屬於網狀設備102（例如，封包106沒有被中繼回網狀設備102），來決定SRC位址116是有效的。

【0062】 若網狀設備102決定SRC位址116是無效的，則網狀設備102可以選擇與封包106的NID 108相匹配的第二隱私金鑰136。網狀設備102隨後可以利用第二隱私金鑰136來對所接收的封包106的第一資訊110進行去混淆，以決定SRC位址116是否是有效的。在使用與封包106的NID 108相匹配的所有已知網路金鑰134之後，若SRC位址116是無效的，則丟棄封包106，而不對第二資訊118進行解密。

【0063】 若SRC位址116是有效的，則網狀設備102可以決定在網路訊息快取記憶體130中是否已經存在封包106的SEQ 114和SRC位址116。若在網路訊息快取記憶體130中已經存在封包106的SEQ 114和SRC位址116，則可以丟棄封包106，而不對第二資訊118進行解密。若在網路訊息快取記憶體130中不存在封包106的SEQ 114和SRC位址116，則對第二資訊118進行解密。

【0064】 圖3是圖示用於經最佳化的網路層訊息處理的另一種方法300的流程圖。該方法300可以由連接到網

狀網路100中的一或多個遠端網狀設備104的網狀設備102來實現。

【0065】 網狀設備102可以接收302封包106。封包106可以是從遠端網狀設備104接收的。封包106可以是藍芽低能網狀封包。例如，封包106可以是網路PDU。

【0066】 網狀設備102可以決定304與封包106的NID相匹配的網路金鑰134。網狀設備102可以知曉多個網路金鑰134。例如，網狀設備102可以被設置有或配置有多個網路金鑰134。網路金鑰134可以與給定的NID 108相關聯。網狀設備102可以決定來自封包106的NID 108。使用封包NID 108，網狀設備102可以選擇與NID 108相匹配的網路金鑰134。

【0067】 網狀設備102可以利用相匹配的網路金鑰134的第一隱私金鑰136來對所接收的封包106的第一資訊110進行去混淆306。例如，網狀設備102可以使用相匹配的網路金鑰134來推導出隱私金鑰136。在一種實現中，網狀設備102可以使用AES-ECB以及與所選擇的網路金鑰134相關聯的隱私金鑰136來對第一資訊110進行去混淆306。封包106的第一資訊110可以包括序號（SEQ）114及/或源（SRC）位址116中的至少一項。

【0068】 網狀設備102可以決定308 SRC位址116是否是有效的。例如，網狀設備102可以經由決定SRC位址116不是未被指派的群組位址或虛擬位址，來決定SRC位址116是有效的。網狀設備102亦可以經由決定SRC位

址116不屬於網狀設備102（例如，封包106沒有被中繼回網狀設備102），來決定SRC位址116是有效的。

【0069】 若SRC位址116不是有效的，則網狀設備102可以決定310是否存在與封包106的NID 108相匹配的另一網路金鑰134。若網狀設備102選擇用於封包106的不正確的網路金鑰134，則去混淆過程可能導致無效的SRC位址116。在此種情況下，網狀設備102可以選擇與封包106的NID 108相匹配的另一網路金鑰134，並且重複利用新的相匹配的網路金鑰134的隱私金鑰136來對所接收的封包106的第一資訊110進行去混淆306。

【0070】 網狀設備102可以嘗試使用針對與NID 108相匹配的每個已知網路金鑰134的隱私金鑰136來對所接收的封包106的第一資訊110進行去混淆306。若沒有獲得有效的SRC位址116，並且網狀設備102決定310不存在與封包106的NID 108相匹配的另外的網路金鑰134，則網狀設備102可以丟棄312封包106，而不對第二資訊118進行解密。

【0071】 若網狀設備102決定308 SRC位址116是有效的，則網狀設備102可以決定314在網路訊息快取記憶體130中是否已經存在封包106的SEQ 114和SRC位址116。若在網路訊息快取記憶體130中已經存在封包106的SEQ 114和SRC位址116，則可以丟棄312封包106，而不對第二資訊118進行解密。

【0072】 若網狀設備102決定314在網路訊息快取記憶體130中不存在封包106的SEQ 114和SRC位址116，則網狀設備102可以使用相匹配的網路金鑰134的加密金鑰138來對第二資訊118（例如，DST 120及/或有效負荷122）進行解密316。例如，網狀設備102可以使用相匹配的網路金鑰134來推導出加密金鑰138。隨後可以使用加密金鑰138來對第二資訊118進行解密。

【0073】 圖4圖示網狀網路通訊協定資料單元（PDU）406的實例。網路PDU 406可以是結合圖1描述的封包106的實現。具體地，網路PDU 406可以根據藍芽網狀簡介規範來實現。

【0074】 網路PDU 406可以包括多個欄位。NID欄位408可以包含7位元的網路辨識符，其允許對用於對該網路PDU 406進行認證和加密的加密金鑰138和隱私金鑰136的更容易的檢視。可以結合加密金鑰138和隱私金鑰136，根據網路金鑰134來推導出NID值。

【0075】 網路PDU 406亦可以包括CTL 442。CTL 442可以是網路控制訊息指示。CTL欄位可以是1位元的值，其用於決定網路PDU 406是控制訊息還是存取訊息的一部分。

【0076】 網路PDU 406亦可以包括存活時間（TTL）欄位412。使用為零的TTL值允許節點傳輸其已知將不被中繼的網路PDU 406，並且因此接收節點可以決定發送

節點相距單個無線電鏈路。使用為一或更大值的TTL值無法用於此種決定。

【0077】 網路PDU 406亦可以包括SEQ 414。SEQ欄位可以是24位元的整數。SEQ 414可以是對於由給定節點發起的每個新的網路PDU 406而言唯一的值。

【0078】 網路PDU 406亦可以包括SRC 416（亦被稱為SRC位址）。SRC欄位可以是16位元的值，其辨識發起該網路PDU 406的元素（例如，網狀設備）。SRC 416位址可以是單播位址。SRC欄位可以是由源元素設置的，並且未被作為中繼節點操作的節點改變。

【0079】 網路PDU 406亦可以包括DST 420。DST欄位可以是16位元的值，其辨識該網路PDU 406所指向的一或多個元素。該位址可以是單播位址、群組位址或虛擬位址。DST欄位可以是由源節點設置的，並且未被作為中繼節點操作的節點中的網路層改變。

【0080】 網路PDU 406亦可以包括傳輸PDU 422。從網路層的角度而言，傳輸PDU欄位是一系列八位元組的資料。傳輸PDU 422可以是結合圖1描述的有效負荷122的實現。

【0081】 網路PDU 406亦可以包括網路訊息完整性檢查（MIC）（例如，NetMIC）444。NetMIC欄位可以是32位元或64位元的欄位（取決於CTL位元的值），其認證DST 420和傳輸PDU 422沒有被改變。

【0082】 使用根據（如NID欄位408所辨識的）單個網路金鑰134所推導出的金鑰來保護網路PDU 406。然而，相同的NID值可以代表多個網路。CTL 442、TTL 412、SEQ 414和SRC 416可以是經混淆的資訊410。網路層可以利用隱私金鑰136來對經混淆的資訊410進行混淆和去混淆。DST 420和傳輸PDU 422可以是經加密的資訊418。網路層可以利用加密金鑰138來對經加密的資訊418進行加密和解密。

【0083】 網狀設備的網路層可以使用用於網路PDU 406的序號來對該網路PDU的DST 420和傳輸PDU 422進行加密。網路層隨後可以對CTL 442、TTL 412、SEQ 414和SRC 416進行混淆，以使得僅有NID 408是以明文可見的。混淆可以用於隱藏來自網路PDU 406中的可能的辨識資訊。

【0084】 為了對網路標頭（例如，CTL 442、TTL 412、SEQ 414和SRC 416）進行混淆，該等值可以與單個加密函數的結果進行組合，該加密函數被設計為阻止被動竊聽者經由偵聽網路PDU 406來決定節點的身份。混淆可以是使用來自網路PDU 406內的可用的資訊來計算的。此種混淆被設計為輔助阻止簡單的被動竊聽者追蹤節點。決定攻擊者仍然可能探索此種混淆內的模式，此舉可能導致暴露節點的SRC 416或SEQ 414。混淆並不強制對加密函數的輸入是唯一的。

【0085】 混淆並不保護隱私金鑰136免遭損害。然而，即使隱私金鑰136被損害，亦可以根據網路金鑰134，使用金鑰推導函數來推導出隱私金鑰136，以保護網路金鑰134。

【0086】 圖5是圖示用於根據藍芽網狀規範的網路層訊息處理的方法500的流程圖。網狀設備102可以接收502封包106。接收網狀設備102可以被稱為網狀承載。

【0087】 網狀設備102決定504 NID 108是否是已知的。在接收到封包106之後，網狀設備102檢查NID欄位108值的值是否與一或多個已知（例如，被配置或設置）的NID 108相匹配。若NID 108欄位108值與已知NID 108不匹配，則丟棄506封包106。

【0088】 若NID 108是已知的，則網狀設備102可以使用網路金鑰134（NetKey）來對封包106進行認證508，以驗證訊息完整性檢查（MIC）。在該步驟中，網狀設備102必須使用隱私金鑰136來對SEQ 114和SRC位址116進行去混淆，並且使用加密金鑰138來對DST 120和有效負荷122進行解密。一旦對封包106去混淆和解密，網狀設備102就可以使用網路金鑰134來對封包106進行認證508。若網路金鑰134沒有認證508封包106，則丟棄510封包106。應當注意的是，該步驟需要網狀設備102在對封包106進行認證508之前對封包106進行解密。

【0089】 若網路金鑰134認證了508封包106，則網狀設備102可以決定512 SRC位址116和DST 120是否是有效的。若SRC位址116或DST 120是無效的，則丟棄514封包106。

【0090】 若SRC位址116和DST 120是有效的，則網狀設備102可以決定516封包106是否已經在網路訊息快取記憶體130中。若封包106已經在網路訊息快取記憶體130中，則丟棄518封包106。

【0091】 若封包106沒有在網路訊息快取記憶體130中，則網狀設備102可以將封包106添加520到網路訊息快取記憶體130中。網狀設備102可以將封包106轉發522給上層132以用於進一步處理。

【0092】 網狀設備102可以決定524是否要對封包106進行中繼。例如，若DST 120指示網狀設備102是封包106的預期接收者，則網狀設備102不對封包106進行中繼。若DST 120指示網狀設備102不是封包106的預期接收者，則網狀設備102可以對封包106進行中繼526。

【0093】 圖6是圖示用於經最佳化的網路層訊息處理的方法600的流程圖。網狀設備102可以接收602封包106。接收網狀設備102可以被稱為網狀承載。

【0094】 網狀設備102可以決定604 NID 108是否是已知的。此舉可以如結合圖6所描述地來完成。若NID欄位值與已知NID 108不匹配，則丟棄606封包106。

【0095】 若NID 108是已知的，則網狀設備102可以利用相匹配的NID 108的隱私金鑰136進行去混淆608。例如，網狀設備102可以選擇與封包106的NID 108相匹配的已知網路金鑰134。在一種實現中，網狀設備102可以使用AES-ECB以及與所選擇的網路金鑰134相關聯的隱私金鑰136來對第一資訊110進行去混淆。封包106的第一資訊110可以包括序號（SEQ）114及/或源（SRC）位址116中的至少一項。

【0096】 網狀設備102可以決定610封包106的SRC位址116是否是有效的。例如，網狀設備102可以經由決定SRC位址116不是未被指派的群組位址或虛擬位址，來決定610 SRC位址116是有效的。網狀設備102亦可以經由決定SRC位址116不屬於網狀設備102（例如，封包106沒有被中繼回網狀設備102），來決定SRC位址116是有效的。在使用了與封包106的NID 108相匹配的所有已知網路金鑰134之後，若SRC位址116是無效的，則丟棄612封包106，而不對封包106進行解密。

【0097】 若SRC位址116是有效的，則網狀設備102可以決定614封包106是否已經在網路訊息快取記憶體130中。例如，若在網路訊息快取記憶體130中已經存在封包106的SEQ 114和SRC位址116，則可以丟棄616封包106，而不對第二資訊118進行解密。

【0098】 若在網路訊息快取記憶體130中不存在SEQ 114和SRC位址116，則網狀設備102可以利用MIC來對

封包106進行驗證618（亦即，認證）。在該步驟中，網狀設備102可以對封包106進行解密。例如，網狀設備102可以使用與所選擇的網路金鑰134相關聯的加密金鑰138來對封包106的DST 120及/或有效負荷122進行解密。網狀設備102隨後可以對封包106進行驗證618。若利用MIC沒有驗證封包106，則丟棄620封包106。

【0099】 若利用MIC驗證了618封包106，則網狀設備102可以決定622 DST 120是否是有效的。若DST 120是無效的（例如，未被指派的位址），則丟棄624封包106。

【0100】 若DST 120是有效的，則網狀設備102可以將封包106添加626到網路訊息快取記憶體130中。網狀設備102可以將封包106轉發628給上層132以用於進一步處理。

【0101】 網狀設備102可以決定630是否要對封包106進行中繼。例如，若DST 120指示網狀設備102是封包106的預期接收者，則網狀設備102不對封包106進行中繼。若DST 120指示網狀設備102不是封包106的預期接收者，則網狀設備102可以對封包106進行中繼632。

【0102】 圖7圖示可以被包括在網狀設備702內的某些元件。網狀設備702可以是無線設備、存取終端、行動站、使用者設備（UE）、膝上型電腦、桌上型電腦、平板電

腦、無線耳機等。例如，網狀設備702可以是圖1的網狀設備102或遠端網狀設備104。

【0103】 網狀設備702包括處理器703。處理器703可以是通用單晶片或者多晶片微處理器（例如，高級RISC（精簡指令集電腦）機器（ARM））、專用微處理器（例如，數位信號處理器（DSP））、微控制器、可程式設計閘陣列等。處理器703可以被稱為中央處理單元（CPU）。儘管在圖7的網狀設備702中僅圖示單個處理器703，但是在替代的配置中，可以使用處理器的組合（例如，ARM和DSP）。

【0104】 網狀設備702亦包括與處理器進行電子通訊的記憶體705（亦即，處理器可以從記憶體讀取資訊及/或將資訊寫入記憶體中）。記憶體705可以是能夠儲存電子資訊的任何電子元件。記憶體705可以被配置為隨機存取記憶體（RAM）、唯讀記憶體（ROM）、磁碟儲存媒體、光學儲存媒體、RAM中的快閃記憶體設備、與處理器包括在一起的機載記憶體、可抹除可程式設計唯讀記憶體（EPROM）、電子可抹除可程式設計唯讀記憶體（EEPROM）、暫存器以及包括其組合的類似記憶體。

【0105】 可以將資料707a和指令709a儲存在記憶體705中。指令可以包括一或多個程式、常式、子常式、函數、程序、代碼等。指令可以包括單個電腦可讀取語句或者許多電腦可讀取語句。指令709a可以可由處理器703執行以實現本文揭示的方法。執行指令709a可以涉及對

儲存在記憶體705中的資料707a的使用。當處理器703執行指令709時，可以將指令709b的各個部分載入到處理器703上，以及可以將資料707b的各個片段載入到處理器703上。

【0106】 網狀設備702亦可以包括傳輸器711和接收器713，以允許經由一或多個天線717向網狀設備702傳輸信號以及從網狀設備702接收信號。傳輸器711和接收器713可以被統稱為收發機715。網狀設備702亦可以包括（未圖示）多個傳輸器、多個天線、多個接收器及/或多個收發機。

【0107】 網狀設備702可以包括數位信號處理器（DSP）721。網狀設備702亦可以包括通訊介面723。通訊介面723可以允許使用者與網狀設備702進行互動。

【0108】 網狀設備702的各個元件可以經由一或多個匯流排耦合在一起，其可以包括功率匯流排、控制信號匯流排、狀態信號匯流排、資料匯流排等。為了清楚起見，在圖7中將各個匯流排示為匯流排系統719。

【0109】 在上文描述中，有時已經結合各個術語使用了元件符號。在結合元件符號使用術語的情況下，此舉可能意味著代表在該等圖中的一或多個圖中圖示的特定元素。在沒有元件符號的情況下使用術語時，此舉可能意味著整體上代表該術語，而不限於任何特定圖。

【0110】 術語「決定」涵蓋各種各樣的動作，並且因此，「決定」可以包括計算、運算、處理、推導、調查、檢視

（例如，在表格、資料庫或者另一資料結構中檢視）、查明等。此外，「決定」可以包括接收（例如，接收資訊）、存取（例如，存取記憶體中的資料）等。此外，「決定」可以包括解析、選擇、選定、建立等。

【0111】 除非另外明確地指定，否則短語「基於」並不意味著「僅基於」。換言之，短語「基於」描述「僅基於」以及「至少基於」二者。

【0112】 術語「處理器」應當被廣義地解釋為包含通用處理器、中央處理單元（CPU）、微處理器、數位信號處理器（DSP）、控制器、微控制器、狀態機等。在一些情況下，「處理器」可以代表特殊應用積體電路（ASIC）、可程式設計邏輯設備（PLD）、現場可程式設計閘陣列（FPGA）等。術語「處理器」可以代表處理設備的組合，例如，數位信號處理器（DSP）和微處理器的組合、複數個微處理器、一或多個微處理器結合數位信號處理器（DSP）核，或者任何其他此種配置。

【0113】 術語「記憶體」應當被廣義地解釋為包含能夠儲存電子資訊的任何電子元件。術語記憶體可以代表各種類型的處理器可讀取媒體，例如，隨機存取記憶體（RAM）、唯讀記憶體（ROM）、非揮發性隨機存取記憶體（NVRAM）、可程式設計唯讀記憶體（PROM）、可抹除可程式設計唯讀記憶體（EPROM）、電子可抹除PROM（EEPROM）、快閃記憶體、磁性或者光資料儲存單元、暫存器等。記憶體被認為是與處理器進行電子通

訊，若處理器能夠從記憶體讀取資訊及/或將資訊寫入到記憶體中的話。作為處理器的組成部分的記憶體與處理器進行電子通訊。

【0114】 術語「指令」和「代碼」應當被廣義地解釋為包括任何類型的電腦可讀取語句。例如，術語「指令」和「代碼」可以代表一或多個程式、常式、子常式、函數、程序等。「指令」和「代碼」可以包括單個電腦可讀取語句或者許多電腦可讀取語句。

【0115】 如本文中所使用的，術語「及/或」應當被解釋為意指一或多個項目。例如，短語「A、B及/或C」應當被解釋為意指以下各項中的任何項：僅A、僅B、僅C、A和B（但是沒有C）、B和C（但是沒有A）、A和C（但是沒有B），或所有的A、B和C。

【0116】 如本文中所使用的，短語「……中的至少一個」應當被解釋為意指一或多個項目。例如，短語「A、B和C中的至少一個」或短語「A、B或C中的至少一個」應當被解釋為意指以下各項中的任何項：僅A、僅B、僅C、A和B（但是沒有C）、B和C（但是沒有A）、A和C（但是沒有B），或所有的A、B和C。如本文中所使用的，短語「……中的一或多個」應當被解釋為意指一或多個項目。例如，短語「A、B和C中的一或多個」或短語「A、B或C中的一或多個」應當被解釋為意指以下各項中的任何項：僅A、僅B、僅C、A和B（但是沒有C）、B和C

（但是沒有A）、A和C（但是沒有B），或所有的A、B和C。

【0117】 本文描述的功能可以用由硬體執行的軟體或者韌體來實現。該等功能可以作為一或多個指令儲存在電腦可讀取媒體上。術語「電腦可讀取媒體」或「電腦程式產品」代表能夠由電腦或者處理器存取的任何有形儲存媒體。經由舉例而非限制的方式，電腦可讀取媒體可以包括RAM、ROM、EEPROM、CD-ROM或其他光碟儲存、磁碟儲存或者其他磁性儲存設備，或者能夠用於攜帶或儲存具有指令或資料結構形式的期望程式碼並且能夠被電腦存取的任何其他媒體。如本文中所使用的，磁碟（disk）和光碟（disc）包括壓縮光碟（CD）、鐳射光碟、光碟、數位多功能光碟（DVD）、軟碟和藍光®光碟，其中磁碟通常磁性地複製資料，而光碟則用鐳射來光學地複製資料。應當注意的是，電腦可讀取媒體可以是有形和非暫時性的。術語「電腦程式產品」代表與可以由計算設備或者處理器執行、處理或運算的代碼或者指令（例如，「程式」）相結合的計算設備或者處理器。如本文中所使用的，術語「代碼」可以代表可由計算設備或者處理器執行的軟體、指令、代碼或資料。

【0118】 軟體或者指令亦可以在傳輸媒體上傳輸。例如，若利用同軸電纜、光纖光纜、雙絞線、數位用戶線路（DSL）或無線技術（例如，紅外線、無線電和微波）從網站、伺服器或其他遠端源傳輸軟體，則同軸電纜、光

纖光纜、雙絞線、DSL或者無線技術（例如，紅外線、無線電和微波）被包括在傳輸媒體的定義中。

【0119】 本文揭示的方法包括用於實現所描述的方法的一或多個步驟或動作。該等方法步驟及/或動作可以在不脫離請求項的範疇的情況下彼此互換。換言之，除非對於所描述的方法的正確操作而言要求步驟或動作的特定次序，否則可以在不脫離請求項的範疇的情況下，修改特定步驟及/或動作的次序及/或使用。

【0120】 此外，應當明白的是，用於執行本文描述的方法和技術的模組及/或其他合適的構件可以由設備下載及/或以其他方式獲得。例如，設備可以耦合到伺服器以促進用於執行本文描述的方法的構件的傳輸。或者，可以經由儲存構件（例如，隨機存取記憶體（RAM）、唯讀記憶體（ROM）、諸如壓縮光碟（CD）或軟碟之類的實體儲存媒體等）提供本文描述的各種方法，從而使得在將儲存構件耦合到設備或向設備提供儲存構件之後，該設備可以獲得各種方法。此外，可以利用用於向設備提供本文描述的方法和技術的任何其他適當的技術。

【0121】 應當理解的是，請求項不限於上文說明的精確配置和元件。可以在不脫離請求項的範疇的情況下，在本文描述的系統、方法和裝置的佈置、操作和細節態樣進行各種修改、改變和變化。

【符號說明】

【0122】

100 網狀網路

102 網狀設備

104 遠端網狀設備

106 封包

108 匹配的NID

110 第一資訊

112 存活時間（TTL）值

114 SEQ

116 SRC

118 第二資訊

120 DST

122 有效負荷

124 封包去混淆模組

126 SRC驗證器

128 封包解密模組

130 網路訊息快取記憶體

132 上層

134 網路金鑰

136 隱私金鑰

138 加密金鑰

200 方法

202 接收

204 去混淆

206 決定

300 方法

302 接收

304 決定

306 去混淆

308 決定

310 決定

312 丟棄

314 決定

316 解密

406 網路PDU

408 NID欄位

410 經混淆的資訊

412 TTL

414 SEQ

416 SRC

418 經加密的資訊

420 DST

422 傳輸PDU

442 CTL

444 網路訊息完整性檢查（MIC）

500 方法

502 接收

504 決定

506 丟棄

508 認證

510 丟棄

512 決定

514 丟棄

516 決定

518 丟棄

520 添加

522 轉發

524 決定

526 中繼

600 方法

602 接收

604 決定

606 丟棄

608 去混淆

610 決定

612 丟棄

614 決定

616 丟棄

618 驗證

620 丟棄

622 決定

624 丟棄

626 添加

628 轉發

630 決定

632 中繼

702 網狀設備

703 處理器

705 記憶體

707a 資料

707b 資料

709a 指令

709b 指令

711 傳輸器

713 接收器

715 收發機

717 天線

719 匯流排系統

721 數位信號處理器（DSP）

723 通訊介面

【生物材料寄存】

【0123】 國內寄存資訊 (請依寄存機構、日期、號碼順序註記)

無

【0124】 國外寄存資訊 (請依寄存國家、機構、日期、號碼順序註記)

無

201921886
專利案號：107124928

201921886

【發明摘要】

【中文發明名稱】用於經最佳化的網路層訊息處理的系統和方法

【英文發明名稱】SYSTEMS AND METHODS FOR OPTIMIZED NETWORK LAYER MESSAGE PROCESSING

【中文】

描述了一種由網狀設備進行的方法。該方法包括以下步驟：利用與接收的封包的網路辨識符（NID）相匹配的隱私金鑰來對該封包的第一資訊進行去混淆。該方法亦包括以下步驟：基於經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密。

【英文】

A method by a mesh device is described. The method includes de-obfuscating first information of a received packet with a privacy key that matches a network identifier (NID) of the packet. The method also includes determining whether to decrypt second information of the packet based on the de-obfuscated first information.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

100 網狀網路

102 網狀設備

104 遠端網狀設備

106 封包

108 匹配的NID

110 第一資訊

112 存活時間（TTL）值

114 SEQ

116 SRC

118 第二資訊

120 DST

122 有效負荷

124 封包去混淆模組

126 SRC驗證器

128 封包解密模組

130 網路訊息快取記憶體

132 上層

134 網路金鑰

136 隱私金鑰

138 加密金鑰

【特徵化學式】

無

【發明申請專利範圍】

【第1項】：一種由一網狀設備進行的方法，包括以下步驟：

利用與一接收的封包的一網路辨識符（NID）相匹配的一隱私金鑰來對該封包的第一資訊進行去混淆；及

基於該經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密。

【第2項】根據請求項1之方法，其中該封包是一藍芽低能網狀封包。

【第3項】根據請求項1之方法，其中該第一資訊包括一序號（SEQ）及/或一源（SRC）位址中的至少一項，並且其中該第二資訊包括目的地（DST）資訊和一有效負荷。

【第4項】根據請求項1之方法，其中決定是否要對該第二資訊進行解密之步驟包括以下步驟：

決定該封包的一SRC位址是有效的。

【第5項】根據請求項4之方法，其中決定該封包的該SRC位址是有效的之步驟包括以下步驟：

決定該SRC位址不是一未被指派的群組位址或虛擬位址。

【第6項】根據請求項4之方法，其中決定該封包的該

SRC位址是有效的之步驟包括以下步驟：

決定該SRC位址不屬於該網狀設備。

【第7項】 根據請求項4之方法，其中若該SRC位址是無效的，則該方法亦包括以下步驟：

使用具有與該封包的該NID相匹配的一NID的所有已知網路來決定該封包的該SRC位址是否是有效的。

【第8項】 根據請求項4之方法，其中若該SRC位址是無效的，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第9項】 根據請求項4之方法，其中若該SRC位址是有效的，則決定是否要對該第二資訊進行解密之步驟亦包括以下步驟：

決定在一網路訊息快取記憶體中是否已經存在該封包的一SEQ和該SRC位址。

【第10項】 根據請求項9之方法，其中若在該網路訊息快取記憶體中已經存在該封包的該SEQ和該SRC位址，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第11項】 根據請求項9之方法，其中若在該網路訊息快取記憶體中不存在該封包的該SEQ和該SRC位址，則該第二資訊被解密。

【第12項】 一種網狀設備，包括：

一處理器；

一記憶體，其與該處理器相通訊；及

被儲存在該記憶體中的指令，該等指令可由該處理器執行以進行以下操作：

利用與一接收的封包的一網路辨識符（NID）相匹配的一隱私金鑰來對該封包的第一資訊進行去混淆；及

基於該經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密。

【第13項】 根據請求項12之網狀設備，其中可執行以決定是否要對該第二資訊進行解密的該等指令包括可執行以進行以下操作的指令：

決定該封包的一SRC位址是有效的。

【第14項】 根據請求項13之網狀設備，其中若該SRC位址是無效的，則該等指令亦可執行以進行以下操作：

使用具有與該封包的該NID相匹配的一NID的所有已知網路來決定該封包的該SRC位址是否是有效的。

【第15項】 根據請求項13之網狀設備，其中若該SRC位址是無效的，則該封包在不對該第二資訊進行

解密的情況下被丟棄。

【第16項】 根據請求項13之網狀設備，其中若該SRC位址是有效的，則可執行以決定是否要對該第二資訊進行解密的該等指令亦包括可執行以進行以下操作的指令：

決定在一網路訊息快取記憶體中是否已經存在該封包的一序號（SEQ）和該SRC位址。

【第17項】 根據請求項16之網狀設備，其中若在該網路訊息快取記憶體中已經存在該封包的該SEQ和該SRC位址，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第18項】 根據請求項16之網狀設備，其中若在該網路訊息快取記憶體中不存在該封包的該SEQ和該SRC位址，則該第二資訊被解密。

【第19項】 一種儲存電腦可執行代碼的非暫時性有形電腦可讀取媒體，包括：

用於使得一網狀設備利用與一接收的封包的一網路辨識符（NID）相匹配的一隱私金鑰來對該封包的第一資訊進行去混淆的代碼；及

用於使得該網狀設備基於該經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密的代碼。

【第20項】 根據請求項19之電腦可讀取媒體，其中該

用於使得該網狀設備決定是否要對該第二資訊進行解密的代碼包括：

用於使得該網狀設備決定該封包的一 SRC 位址是否是有效的代碼。

【第21項】 根據請求項20之電腦可讀取媒體，其中若該 SRC 位址是無效的，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第22項】 根據請求項20之電腦可讀取媒體，其中若該 SRC 位址是有效的，則該用於使得該網狀設備決定是否要對該第二資訊進行解密的代碼亦包括：

用於使得該網狀設備決定在一網路訊息快取記憶體中是否已經存在該封包的一序號（SEQ）和該 SRC 位址的代碼。

【第23項】 根據請求項22之電腦可讀取媒體，其中若在該網路訊息快取記憶體中已經存在該封包的該 SEQ 和該 SRC 位址，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第24項】 根據請求項22之電腦可讀取媒體，其中若在該網路訊息快取記憶體中不存在該封包的該 SEQ 和該 SRC 位址，則該第二資訊被解密。

【第25項】 一種裝置，包括：

用於利用與一接收的封包的一網路辨識符（NID）

相匹配的一隱私金鑰來對該封包的第一資訊進行去混淆的構件；及

用於基於該經去混淆的第一資訊來決定是否要對該封包的第二資訊進行解密的構件。

【第26項】 根據請求項25之裝置，其中該用於決定是否要對該第二資訊進行解密的構件包括：

用於決定該封包的一SRC位址是有效的構件。

【第27項】 根據請求項26之裝置，其中若該SRC位址是無效的，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第28項】 根據請求項26之裝置，其中若該SRC位址是有效的，則該用於決定是否要對該第二資訊進行解密的構件亦包括：

用於決定在一網路訊息快取記憶體中是否已經存在該封包的一SEQ和該SRC位址的構件。

【第29項】 根據請求項28之裝置，其中若在該網路訊息快取記憶體中已經存在該封包的該SEQ和該SRC位址，則該封包在不對該第二資訊進行解密的情況下被丟棄。

【第30項】 根據請求項28之裝置，其中若在該網路訊息快取記憶體中不存在該封包的該SEQ和該SRC位址，則該第二資訊被解密。