



(12) 发明专利

(10) 授权公告号 CN 101785343 B

(45) 授权公告日 2014. 04. 30

(21) 申请号 200880024497. 3

H04W 28/24 (2009. 01)

(22) 申请日 2008. 06. 30

(56) 对比文件

(30) 优先权数据

11/777, 673 2007. 07. 13 US

WO 2006032046 A1, 2006. 03. 23,

WO 2006031974 A1, 2006. 03. 23,

CN 1883225 A, 2006. 12. 20,

(85) PCT国际申请进入国家阶段日

2010. 01. 13

审查员 程小亮

(86) PCT国际申请的申请数据

PCT/US2008/068840 2008. 06. 30

(87) PCT国际申请的公布数据

W02009/012052 EN 2009. 01. 22

(73) 专利权人 英特尔公司

地址 美国加利福尼亚

(72) 发明人 K·索德

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 宋献涛 王英

(51) Int. Cl.

H04W 12/06 (2009. 01)

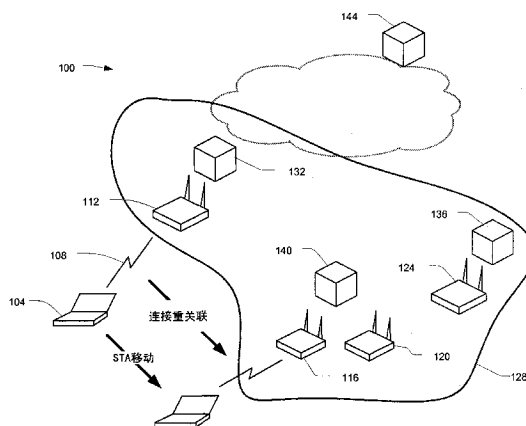
权利要求书2页 说明书8页 附图5页

(54) 发明名称

用于快速转换资源协商的方法、系统和装置

(57) 摘要

本发明概括地描述了在无线网络中用于快速转换资源协商的方法、装置、机器可读介质和系统,包括:与网络节点建立无线连接;向另一网络节点发送包含标识所需资源类型的资源标识符的快速转换 (FT) 认证请求;从该另一网络节点接收指示该另一网络节点是否支持所需资源类型的 FT 认证响应;并至少部分地根据 FT 认证响应来选择该另一网络节点作为用于重关联无线连接的重关联目标。



1. 一种用于快速转换资源协商的方法,包括以下步骤:
 - 与网络节点建立无线连接;
 - 向另一个网络节点发送快速转换(FT)认证请求,所述 FT 认证请求包含标识所需资源类型的资源标识符;
 - 从所述另一个网络节点接收 FT 认证响应,所述 FT 认证响应指示所述另一个网络节点是否支持所述所需资源类型;
 - 至少部分地根据所述 FT 认证响应来选择所述另一个网络节点作为用于重关联所述无线连接的重关联目标;以及
 - 在发送所述 FT 认证请求之后,向所述另一个网络节点发送包含所述资源标识符的重关联请求。
2. 如权利要求 1 所述的方法,还包括以下步骤:
 - 通过所述网络节点在数据帧中向所述另一个网络节点发送所述 FT 认证请求。
3. 如权利要求 1 所述的方法,其中,在与所述网络节点的所述无线连接中使用安全密码,所述发送所述重关联请求的步骤包括以下步骤:发送所述安全密码的标识。
4. 如权利要求 1 所述的方法,其中,所述重关联请求是完整性受保护的消息。
5. 如权利要求 1 所述的方法,还包括以下步骤:
 - 向所述另一个网络节点发送包含所述资源标识符的资源信息容器数据信息单元(RDIE)。
6. 如权利要求 1 所述的方法,其中,所述所需类型包括:无线多媒体扩展资源类型。
7. 一种用于快速转换资源协商的系统,包括:
 - 用于提供无线网络接入的全向天线;
 - 包含转换管理器的主机,所述转换管理器用于:
 - 通过所述全向天线向网络节点发送快速转换(FT)认证请求,所述 FT 认证请求包含标识所需资源类型的资源标识符;
 - 通过所述全向天线从所述网络节点接收 FT 认证响应,所述 FT 认证响应指示所述网络节点是否支持所述所需资源类型;
 - 至少部分地根据所述 FT 认证响应来选择所述网络节点作为用于重关联无线连接的重关联目标;以及
 - 在发送所述 FT 认证请求之后,向所述网络节点发送包含所述资源标识符的重关联请求。
8. 如权利要求 7 所述的系统,其中,所述无线连接初始时与另一个网络节点关联,所述转换管理器用于:通过所述另一个网络节点在数据帧中向所述网络节点发送所述 FT 认证请求。
9. 如权利要求 7 所述的系统,其中,所述转换管理器还用于:将所述重关联请求作为完整性受保护的消息进行发送。
10. 一种用于快速转换资源协商的装置,包括:
 - 与主机耦接的无线网络接口卡,所述无线网络接口卡用于为所述主机提供无线网络接入;
 - 包含关联管理器的所述主机,所述关联管理器用于:

通过所述无线网络接口从网络节点接收快速转换(FT)认证请求,所述 FT 认证请求包含具有标识所述网络节点所需资源类型的资源标识符和一个或多个所请求服务质量(QoS)资源的第一资源协商请求;

生成指示所述装置支持所述所需资源类型的 FT 认证响应;

通过所述无线网络接口向所述网络节点发送所述 FT 认证响应;

通过所述无线网络接口从所述网络节点接收包含第二资源协商请求的重关联请求;以及

至少部分地根据所述第一资源协商请求是否匹配所述第二资源协商请求,来分配从所述一个或多个所请求 QoS 资源中选定的至少一个资源。

11. 如权利要求 10 所述的装置,其中,所述关联管理器还用于:使一个或多个资源处理状态机针对来自所述网络节点的后续请求做好准备,以分配所述资源类型的资源。

12. 如权利要求 10 所述的装置,其中,所述关联管理器还用于:

通过所述无线网络接口从所述网络节点接收所述重关联请求,其中所述重关联请求包含安全密码的标识并用于请求将与另一个网络节点的到所述装置的现有无线连接进行重关联;

还至少部分地根据所述安全密码的标识是否对应于在所述网络节点和另一个网络节点之间的所述现有无线连接中使用的安全密码,来分配从所述一个或多个所请求 QoS 资源中选定的至少一个资源。

13. 一种用于快速转换资源协商的系统,包括:

用于从网络节点无线接收快速转换(FT)认证请求的模块,所述 FT 认证请求包含标识所述网络节点所需资源类型的资源标识符和一个或多个所请求服务质量(QoS)资源;

用于检验资源请求的模块;

用于确定所述系统是否支持所述所需资源类型的模块;

用于如果确定所述系统不支持所述所需资源类型,则生成指示不支持所述所需资源类型的 FT 认证响应的模块;

用于如果确定所述系统支持所述所需资源类型,则生成指示所述系统支持所述所需资源类型的 FT 认证响应的模块;

用于如果确定所述系统支持所述所需资源类型,则建立内部资源处理状态机的模块;以及

用于向所述网络节点无线发送所述 FT 认证响应的模块。

用于快速转换资源协商的方法、系统和装置

技术领域

[0001] 概括地说,本发明的各实施例涉及无线网络领域,具体地说,本发明涉及无线网络中的快速转换资源协商。

背景技术

[0002] 无线网络中的通信会话一般涉及本地站点与远程站点通过通信链路进行通信。此通信链路可包含本地站点与接入点之间的无线连接。由于种种原因,接入点与本地站点之间的无线连接质量可能会变差。这可能是由于接入点过载、站点移动、干扰等等造成的。为了保持已建立的通信链路,本地站点可以将无线连接重新关联至另一接入点。当通信会话涉及不容延迟的传输(例如:音频或视频)时,对于无线连接的成功而高效的重关联来说,存在很多服务质量(QoS)方面的挑战。

[0003] 设想的用于提供快速转换(FT)的技术涉及一个站点与一个或多个接入点之间的认证过程。此认证过程允许站点决定将区域中的哪些接入点作为进行重关联的候选接入点。这包括生成站点与重关联候选接入点之间的共享密钥。一旦建立好认证,站点就可以选择接入点,以重新关联无线连接并开始资源协商。

[0004] 资源协商通过接入点和站点之间所交换的一些进行完整性检查的消息(通过使用共享密钥)得以实现。资源协商可以在重关联过程之前发生或与重关联过程同时发生。站点会通过资源协商请求为自己分配足够的资源以保证无线连接的QoS等级。如果接入点有可分配的资源,则其会进行分配并开始重关联过程。如果资源协商失败,站点则可能无法与此接入点重关联,而需要与另一接入点重新开始此过程。这一延迟会影响站点提供高QoS等级无线连接的能力。

附图说明

[0005] 本发明的各实施例以示例而非限定的方式在附图中的各图表中示出,其中相同的标注表示相同的元素,其中:

[0006] 图1,依据本发明的多个实施例,示出了提供快速转换的网络;

[0007] 图2,依据本发明的多个实施例,示出了快速转换操作的消息序列;

[0008] 图3,依据本发明的多个实施例,示出了资源协商请求的数据结构;

[0009] 图4,依据本发明的多个实施例,示出了资源信息容器数据信息单元的数据结构;

[0010] 图5,依据本发明的多个实施例,示出了资源定义;

[0011] 图6,依据本发明的多个实施例,示出了描述快速转换操作的流程图;

[0012] 图7,依据本发明的多个实施例,示出了资源协商响应的数据结构;

[0013] 图8,依据本发明的多个实施例,示出了站点的各组件;

[0014] 图9,依据本发明的多个实施例,示出了接入点的各组件;

[0015] 图10,依据本发明的多个实施例,示出了计算设备。

具体实施方式

[0016] 本发明的各实施例可提供用于在无线网络中进行快速转换资源协商的方法、制品、装置和系统。

[0017] 本申请所示实施例的各个方面都会使用本领域技术人员惯用的词语进行描述以使他们所做工作的内容可以传递给本领域的其他技术人员。但是,对于本领域技术人员而言显而易见的是,其它的实施例仅通过本申请描述的某些方面就可以实现。出于解释说明的目的,本申请中描述具体的设备和配置以便提供对所示实施例的透彻理解。但是,对于本领域技术人员而言显而易见的是,其它的实施例不需要这些具体细节也可以实现。在其他例子中,将各公知特征忽略或简化,以避免混淆本申请所示实施例。

[0018] 另外,本申请会顺序地、以最有助于理解本发明的方式,将各种操作描述为多个分立的操作;尽管描述是有顺序的,但是不应就此认为这些操作必须是顺序固定的。尤其是,这些操作不需要按照本申请所示的顺序执行。

[0019] 本申请会重复用到短语“在一个实施例中”。此短语一般情况下并不是指同一个实施例,但也有这个可能。除非上下文中指明了不同的意义,否则词语“包括”“含有”和“包含”是同义词。

[0020] 给与各个实施例有关的用语提供一些明确的语境:短语“A/B”指(A)或(B);短语“A和/或B”指(A)、(B)或(A和B);短语“A、B和/或C”指(A)、(B)、(C)、(A和B)、(A和C)、(B和C)或(A、B和C)。

[0021] 本申请用到的“组件”的说法可以是指用于获取所需结果的硬件、软件和/或固件组件。尽管本申请仅示出和/或描述了一定数目的分立组件,但是这些组件可以由更多的或更少的组件来实现,而并不会脱离本发明所示实施例的主旨和范围。

[0022] 根据本发明的一个实施例,图1示出了网络100,其使用快速转换(FT)资源协商来支持移动无线设备的FT。具体地说,多个实施例中的FT资源协商可以包括:在多个网络实体之间进行的认证交换中确定所支持的资源类型。在执行此资源类型确定的同时进行认证可以使实体根据之前FT操作的多种可能性来识别进行重关联的目标。本申请还会根据多个实施例对一些安全机制进行描述,其中这些安全机制用于解决在认证过程的结果之前可能会阻碍所执行的确定操作的问题。

[0023] 简单地说,网络100可能是无线局域网(WLAN)、无线城域网(WMAN)等等,其可包括无线网络节点,如:站点104,其具有与其他无线网络节点(如:接入点(AP)112)的无线连接108。网络100还可以包括其他无线网络节点,如:AP116、120和124。这些AP可以由基础设施提供商运营的移动域(MD)128的一部分。提供商可以将MD128定义为管理功能体。

[0024] 最开始,无线连接108可以在通信会话开始时与AP112关联。通过分布在MD128中的多个密钥持有者可以保证通信会话的安全。每个AP可以与一个密钥持有者(KH)关联。例如,AP112可以与KH132关联;AP116和120都可以与KH140关联;AP124可以与KH136关联。可以看到,一个KH既可以与一个AP唯一关联(有时在同一设备上实现),也可以与一个以上的AP关联。

[0025] 在无线连接108的初始关联之后,站点104和认证服务器144可以使用诸如可扩展认证协议(EAP)来进行互相认证。在互相认证之后,认证服务器144可以向AP112和站点104传送主密钥(MSK)。

[0026] 与 AP112 关联的 KH (如 :KH132) 可以用 MSK 来计算第一级成对主密钥(PMK)-R0。在此情况下, KH132 也可以称为 R0KH132。

[0027] 此时, 站点 104 和认证服务器 144 也可以对安全密码达成一致, 这些安全密码例如 : 加密密码、认证密码和 / 或密钥包密码, 而它们可以用于在通信会话中提供加密和认证功能。当站点 104 在利用 FT 的各 AP 之间移动时, 这些安全密码用于保证站点 104 与 MD128 中的 AP 之间的通信安全。

[0028] R0KH132 可以使用 PMK-R0 和 R1KH 的标识(可以是用于初始关联的 R0KH132) 来生成第二级成对主密钥, 例如 : PMK-R1 密钥。PMK-R1 则可以用于生成成对暂时密钥(PTK) 会话密钥。

[0029] 站点 104 可以使用 MSK 以类似于 R0KH132 的方式来生成 PMK-R0、PMK-R1 和 PTK 密钥。由站点 104 生成的密钥可以匹配由 R0KH132 生成的密钥, 这是因为二者使用相同的密钥生成函数的相同成分。利用正确生成的密钥, 站点 104 可以通过无线连接 108 的连接与 AP112 进行安全关联。

[0030] 在确定通信会话的性质的情况下, 如果站点 104 观察到无线连接 108 的质量恶化, 站点 104 可以启动 FT 操作以将无线连接 108 与能够提供适当服务质量(QoS) 等级的另一 AP 进行重关联。在多个实施例中, 通信会话可以包括对延迟和 / 或抖动敏感的网络业务, 例如但不限于 : 流式多媒体、互联网协议(IP)电话(如 : IP 语音(VoIP))、视频会议等等。因此, 需要以某种方式来进行 FT 操作, 以避免对已建立通信的可检测破坏。

[0031] 本申请所使用的“快速转换”也可以称为“快速漫游”, 其与电气与电子工程师协会(IEEE) 无线标准中描述的快速转换操作兼容, 这些标准包括例如 : 802. 11-2007 标准及其任何修订版、修改版或更新版, 而这些版本中包括但不限于 : 关于快速基本服务集转换的 802. 11r 修改版。

[0032] 尽管以上实施例讨论了站点和接入点之间的无线连接初始关联以及与另一接入点的无线连接重关联, 但其他实施例可能包括其他无线网络节点组合之间的关联。例如 : 无线连接关联可以在 AP 和 AP 之间、站点和站点之间等等。本申请所使用的“关联”既可包括初始关联, 也可包括重关联。

[0033] 无线网络节点可以是任何类型的能够执行本文所述涉及 FT 操作的关联的设备。在一些实施例中, 网络节点可以是移动网络客户端设备, 例如但不限于 : 个人计算设备、膝上型计算设备、电话等等, 或网络基础设施设备, 例如 : 服务器、接入点等等。

[0034] 根据本发明的多个实施例, 图 2 示出了包含 FT 操作的消息序列 200。FT 操作可以遵循站点 104 和 AP112 之间的安全关联 204, 其可以按上文所述建立。

[0035] 在启动 FT 操作之前, 站点 104 发现其他相邻 AP 的初始 FT 信息以确定 FT 操作是否可行, 在某些实施例中, 此初始 FT 信息可以包括资源标识符。在某些实施例中, MD128 中的 AP 会发送管理帧来将此初始 FT 信息提供给站点。这些管理帧可在信标消息 208 中发送, AP (如 : AP116) 可以周期性地广播信标消息 208 (例如, 每 100 毫秒广播一次)。在另一实施例中, 站点 104 会向 AP116 发送探测请求 212, AP116 则会在探测响应 216 中使用初始 FT 信息作出响应。在另一实施例中, 此信息可使用 AP 邻居(AP-neighbor)报告来发送。例如, AP112 可以从其相邻 AP 处收集此信息, 并在管理帧中向站点 104 发送此信息, 其中管理帧可以以管理操作帧的形式发送。

[0036] 在某些实施例中, AP 可以选择不在信标中通告资源标识符以减小信标的体积。

[0037] 如果 FT 操作对一个或多个 AP 而言可行,那么站点 104 会将这些 AP 标识为重关联候选 AP,并在需要时启动与一个或多个重关联候选 AP 的重关联过程。

[0038] 站点 104 可以通过构造资源协商请求并在 FT 认证请求 220 中将其发送至 AP116 的方式来启动 FT 操作。

[0039] 根据本发明的实施例,图 3 示出了可在 FT 认证请求 220 中发送的资源协商请求 300 的数据结构。资源协商请求 300(下文称“资源请求 300”)也可称为资源信息容器(RIC),其可以包括:第一数据流资源请求(如:流 304)和第二数据流资源请求(如:流 308)。不同的流可以指示不同类型的网络业务。例如,流 304 可以用于视频,而流 308 可以用于音频。

[0040] 流 304 可以包括对流 304 进行标识的 RIC 数据信息单元(RDIE)312,如资源 ID-a,其后跟有多个 QoS 资源,如资源描述符-1316、资源描述符-2320。QoS 资源可以是按优选顺序列出的备选资源。也就是说,资源描述符-1316 是基站 104 的第一选择,资源描述符-2320 是第二选择,诸如此类。

[0041] QoS 资源可以包括:业务规格信息单元(TSPEC IE),其描述正在请求服务的业务模式(如:数据速率、数据包尺寸、延迟和服务间隔);业务分类(TCLAS)IE,其规定某些参数以标识数据包所属的通信会话;以及 TCLAS 处理 IE,其提供关于数据包处理的信息。这些信息单元可能与 IEEE802.11(e)(出版于 2005 年 11 月 11 日)及其更新版、修订版和 / 或修改版等中所描述的同名单元类似。

[0042] 流 308 可能具有仅跟有一个资源描述符-1328 的 RDIE324。因此,没有另外的 QoS 资源被列出用于流 308。

[0043] 根据本发明的多个实施例,图 4 示出了可包含在资源协商请求 300 中的 RDIE400 的数据结构。RDIE312 和 / 或 324 可以与 RDIE400 具有相似的结构。

[0044] RDIE400 可以包括用于将 RDIE400 标识为特定类型信息单元的单元 ID404 和用于指示剩余 RDIE400 尺寸的长度 408。

[0045] RDIE400 还可以具有独特标识符 RDIE-ID412,其后跟有资源标识符 416。与初始 FT 信息中所发送的资源标识符相似的资源标识符 416 可以唯一地标识出在与 RDIE400 相关联的流中可能请求的资源类型。资源标识符 416 可以是标识字段,当网络实体(如:AP116)接收到 RDIE400 时,则该实体将该标识字段与资源定义相互参照。这可以防止 AP116 处理所请求的 QoS 资源(包括任何必要的容错方案和 / 或纠错过程)以及尝试将它们与其可能支持的资源进行匹配以确定是否支持此资源类型,而上述操作会为 FT 操作增加不必要的延时。

[0046] 在资源请求 300 中传输资源标识符可以允许在站点没有收到初始 FT 信息中的信息的情况下(如:由于 AP 为了减小信标体积而没有广播此信息),确定 AP 是否具有特定的资源类型,其中该特定的资源类型是在该 AP 被标识为 FT 候选 AP 的情况下有用的资源类型。

[0047] 根据本发明的多个实施例,图 5 示出了用于定义特定 AP 可能支持的资源类型的资源定义 500。资源定义 500 可以包括资源标识符 504,其后跟有资源类型 508 和资源描述 512。资源标识符 504 可以是用于独特标识资源类型 508 的标识符。在一个实施例中,它可以包括组织内唯一标识符(OUI)516 和数值 520。OUI516 可以由诸如 IEEE 之类的注册机构分配的数字,其用于对供货商、制造商或其他组织进行独特标识。诸如 802.11e、WiFi 联盟等之类的组织会定义它们自己的可在资源请求中携带的特定资源类型。数值 520 是另一

个数字,结合 OUI516,其可以允许特定组织定义多于一个资源类型。

[0048] 在多个实施例中,资源类型 508 可以涉及多种资源类型,例如基于以下内容的资源:音频/视频/控制 QoS、介质访问控制(MAC) 区块确认、对后端服务的网络接入、基于位置的服务、新型视频 MAC 增强等等。在多个实施例中,资源类型 508 可以是基于 802.11e 的资源(如:混合协调功能受控信道接入(HCCA)或增强型分布式信道接入(EDCA))、WiFi 联盟的基于 WiFi 多媒体(WMM)的资源或其他现有或将来制定的资源类型。

[0049] 资源描述 512 可以是对特定资源类型的文本描述,例如:此资源类型描述了 802.11e 视频业务流参数。

[0050] 网络 100 的实体可以访问资源定义 500 中包含的信息(例如通过可实施的标准)并且可以相应地调整它们的行为过程。

[0051] 再次参看图 4,RDIE400 还可以含有资源描述符计数 420 和状态码 424,其中,资源描述符计数 420 用于指示跟在 RDIE400 之后的备选资源描述符的数目,状态码 424 可用在响应消息中以指示请求的结果。当 RDIE400 包含在请求中时,可以将状态码 424 设为零并在收到后忽略。

[0052] 根据本发明的多个实施例,图 6 示出了 AP116 在接收到 FT 认证请求 220 之后的操作。AP116 在方框 604 中接收 FT 认证请求 220 并在方框 608 中检验此资源请求。如果在方框 612 中确定 AP116 不支持与资源标识符关联的资源类型,那么在方框 616 中 AP116 会生成 FT 认证响应以指示不支持此资源类型。在某些实施例中,如果站点 104 可以使用另一资源类型,那么 AP116 可以在 FT 认证响应中包含一个或多个所支持的资源类型。在方框 620 中 AP116 会向站点 104 发送 FT 认证响应。

[0053] 如果在方框 612 中确定支持与资源标识符关联的资源类型,那么在方框 624 中 AP116 会生成 FT 认证响应以指示支持此资源。然后,在方框 628 中 AP116 会设置内部资源处理状态机以预测后续资源请求。此时 AP116 还会与 QoS 服务器进行后端资源验证。此时这些资源不会被分配,以防止站点向网络 100 中的多个 AP 发出多个未经认证的资源请求而发生服务拒绝(DoS)攻击。但是,当收到后续认证资源请求时,状态机准备就绪从而足可以减少资源分配的延时。在方框 620 中 AP116 会向站点 104 发送 FT 认证响应。

[0054] 再次参看图 2, AP116 会在处理 FT 认证请求 220 之后发送 FT 认证响应 224,对 FT 认证请求 220 的处理可以以与上文参照图 6 所述的类似方式来进行。

[0055] 根据本发明的多个实施例,图 7 示出了可在 FT 认证响应 224 中发送的资源协商响应 700 的数据结构。资源协商响应 700 (下文称“资源响应 700”)可以包括针对资源请求中的每个流的数据流资源响应,例如:流 704 对应于流 304,流 708 对应于流 308。

[0056] 在此实施例中, AP116 可以含有在流 304 中请求的第一 QoS 资源。相应地,流 704 可以包括 RDIE712,其后跟有资源描述符-1716。流 704 还可以包括任何相关资源详情 720。

[0057] 在此实施例中, AP116 可以不含有在流 308 中请求的 QoS 资源。相应地, RDIE724 的状态码可以指示不支持此资源类型。在某些实施例中,流 708 可以包括站点 104 建议备选的可用和/或支持资源类型的当前列表。

[0058] FT 认证请求 220 和 FT 认证响应 224 可以通过分配系统(ODS)发生,例如通过 AP112 或通过空中(OTA)。如果这些认证消息是通过 OTA 发送的,那么它们会在管理帧中发送。如果这些认证消息是通过 ODS 发送的,那么它们会在管理帧或数据帧中发送。在数据帧中发

送认证消息可以实现更大的后端灵活性,尤其是后端 AP 供货商互操作性。

[0059] 也可以在 FT 认证请求 220 和 FT 认证响应 224 中发送安全信息,以允许站点 104 和 AP116 通过生成适当的会话密钥进行互相认证。

[0060] 安全信息还可以包括多个密钥持有者标识(如 :ROKH-ID 和 R1KH-ID),以有助于生成和分配 PMK-R1 密钥。这些 KH-ID 会通过认证消息中的快速转换信息单元(FTIE)进行传输。

[0061] 生成会话密钥的操作可以包括与 AP116 关联的 KH (如 :KH140)和生成新 PTK 的站点 104。为此,KH140 可能需要 ROKH132 的标识,其中该标识负责生成并向 MD128 中的各 KH 发出 PMK-R1 密钥,以便请求 PMK-R1 密钥。在从 ROKH132 接收 PMK-R1 密钥后,KH140 (本例中也称 R1KH140)会生成 PTK。

[0062] 站点 104 可以接收 R1KH140 的标识并生成应与由 R1KH140 生成的 PTK 会话密钥相匹配的 PTK 会话密钥。

[0063] 在多个实施例中,无线网络节点的标识可以是网络地址,该地址例如但不限于:介质访问控制(MAC)地址。

[0064] 一旦会话密钥已生成,站点 104 则会在完整性受保护的关联消息(如:重关联请求 228)中发送资源请求。然后,在接收到重关联请求后,AP116 会校验重关联请求的多个方面。

[0065] AP116 可以校验重关联请求 228 的资源请求是否匹配于 FT 认证请求 220 的资源请求。在多个实施例中,其可以包括完全或部分匹配。例如,AP116 可以校验资源请求的某些部分是否互相匹配,例如:资源 ID 和 QoS 资源。这种校验过程可以帮助防止改变资源请求后认证处理的站点 104 发生降级攻击(downgrade attack)。

[0066] AP116 还可以通过分析重关联请求 228 中的消息完整性码-密钥确认密钥(MIC-KCK)字段来校验重关联请求 228 是否通过了完整性检验。

[0067] AP116 还可以确保没有为了要利用网络 100 中的潜在漏洞而改变安全密码。考虑例如站点 104 使用第一密码(如:有线等效保密(WEP))与 AP116 初始关联的情况。如果站点 104 移动到共享 KH140 的 AP120,则其使用相同的 PMK-R1 密钥,并可以将第一密码改变为诸如临时密钥完整性协议(TKIP)之类的第二密码。为了避免站点对检测到的密码漏洞进行处理而损害使用相同根密钥的其它 AP 上的通信会话,AP116 会校验重关联请求 228 中包含的安全密码与初始安全关联 204 中使用的密码是否相同。安全密码的标识可以包含在稳固安全网络 IE (RSNIE)中。

[0068] 在其它实施例中,可将其它机制用于确保站点在特定 MD 中的不同 AP 之间移动时保持相同的安全密码。例如,在网络 100 内的站点的初始关联中使用的安全密码的标识可以与 PMK-R1 密钥的生成相结合。改变安全密码会妨碍生成适合的会话密钥。

[0069] 一旦 AP116 校验了重关联请求 228 的多个方面,它就会继续分配可用的 QoS 资源。所分配的资源可通过完整性受保护的关联响应 232 发送给站点 104。在某些情况下,可能此时 AP116 无法分配任何所请求的资源。这时,可以在重关联响应 232 中将未对资源进行分配和/或建议备选资源发送给站点 104。

[0070] 根据本发明的多个实施例,图 8 示出了站点 104 的一些组件。站点 104 可以包括无线网络接口卡(WNIC)804 以帮助其与网络 100 中其他设备的无线通信。WNIC804 可以帮

助处理去往 / 来自主机 808 的组件的消息。WNIC804 可以与天线构件 812 协同工作以提供到网络 100 中其他设备的接入。

[0071] 在多个实施例中,天线构件 812 可包含 :一个或多个主要在一个方向上(如 :在 120 度内)发射或接收的定向天线,它们互相协同耦接以提供基本上全向的覆盖 ;或者一个或多个全向天线,这些天线在各个方向上均可以发射和接收。

[0072] 在多个实施例中,主机 808 可包括诸如无线局域网(WLAN)驱动器 816 之类的驱动器,其为主机 808 的诸如转换管理器 820 之类的其它组件来驱动 WNIC804。转换管理器 820 可以控制站点 104 的 FT 操作,这些操作例如本发明实施例所讨论的那些操作。

[0073] 在一个实施例中,驱动器 816 可以包括请求程序 824,其作为安全软件组件来工作,以用于例如执行 MIC 计算。

[0074] 根据本发明的多个实施例,图 9 示出了 AP116 的一些组件。AP116 可以包括 WNIC904 和天线构件 908 以帮助与网络 100 中各无线设备进行的无线通信,并且这两个组件类似于站点 104 中的同名组件。AP116 可以包含具有驱动器 916 的主机 912,驱动器 916 为主机 912 的诸如关联管理器 920 之类的其它组件来驱动 WNIC904。关联管理器 920 可以控制 AP116 的 FT 操作,这些操作例如本发明实施例所讨论的那些操作。

[0075] 在一个实施例中,驱动器 916 可以包括请求程序 924,其作为安全软件组件来工作,以用于例如执行 MIC 计算。

[0076] 根据本发明的多个实施例,图 10 示出了能够实现无线网络设备的计算设备 1000。如图所示,对于此类实施例,计算设备 1000 包括处理器 1004、内存 1008 和总线 1012,并且它们如图所示互相耦接。另外,计算设备 1000 包括互相耦接的存储器 1016 和通信接口 1020 (如 :WNIC),以及所示的在上文中描述的元件。

[0077] 具体而言,内存 1008 和存储器 1016 可以分别包括 FT 逻辑 1024 的临时性和永久性副本。根据本发明的多个实施例,FT 逻辑 1024 可以包括一些指令,其中当处理器 1004 访问这些指令时,使计算设备 1000 执行结合各种无线网络设备所描述的 FT 操作。

[0078] 在多个实施例中,内存 1008 可以包括 :RAM、动态 RAM (DRAM)、静态 RAM (SRAM)、同步 DRAM (SDRAM)、双倍数据速率 RAM (DDRDRAM) 等等。

[0079] 在多个实施例中,处理器 1004 可以包括一个或多个单核处理器、多核处理器、控制器、专用集成电路(ASIC) 等等。

[0080] 在多个实施例中,存储器 1016 可以包括集成和 / 或外围存储设备,例如但不限于 :磁盘及相关驱动(如 :磁的或光学的)、通用串行总线(USB)存储设备及相关端口、闪存、只读存储器(ROM)、非易失性半导体设备等等。

[0081] 在多个实施例中,存储器 1016 可以是计算设备 1000 的部分物理存储资源,或者其可以由计算设备 1000 访问但并不必须是它的一部分。例如,存储器 1016 可以由计算设备 1000 通过网络来访问。

[0082] 在多个实施例中,计算设备 1000 可以具有更多或更少的组件和 / 或不同构件。在多个实施例中,计算设备 1000 可以是站点、接入点或某些其它的无线网络节点。

[0083] 尽管本发明在上文所示的实施例中得到了描述,但是本领域普通技术人员应该理解的是,在不脱离本发明保护范围的前提下,预期达到同样目的的众多备选和 / 或等效实现方式可以在所示和所述具体实施例中进行替换。本领域技术人员还将理解的是,本发明

可以实现在各种各样的实施例中。本申请中的描述应理解为对本发明实施例的说明而不是限定。

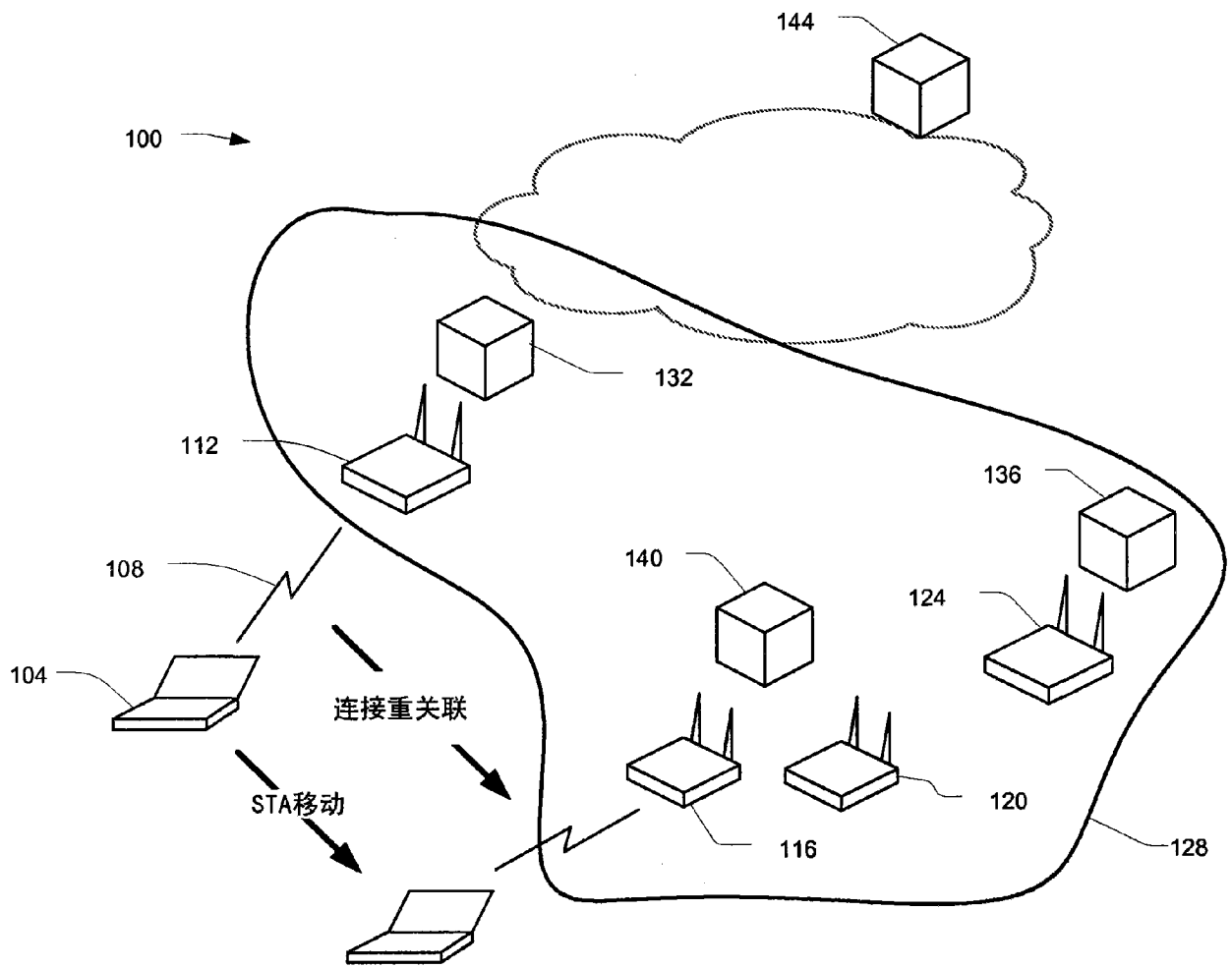


图 1

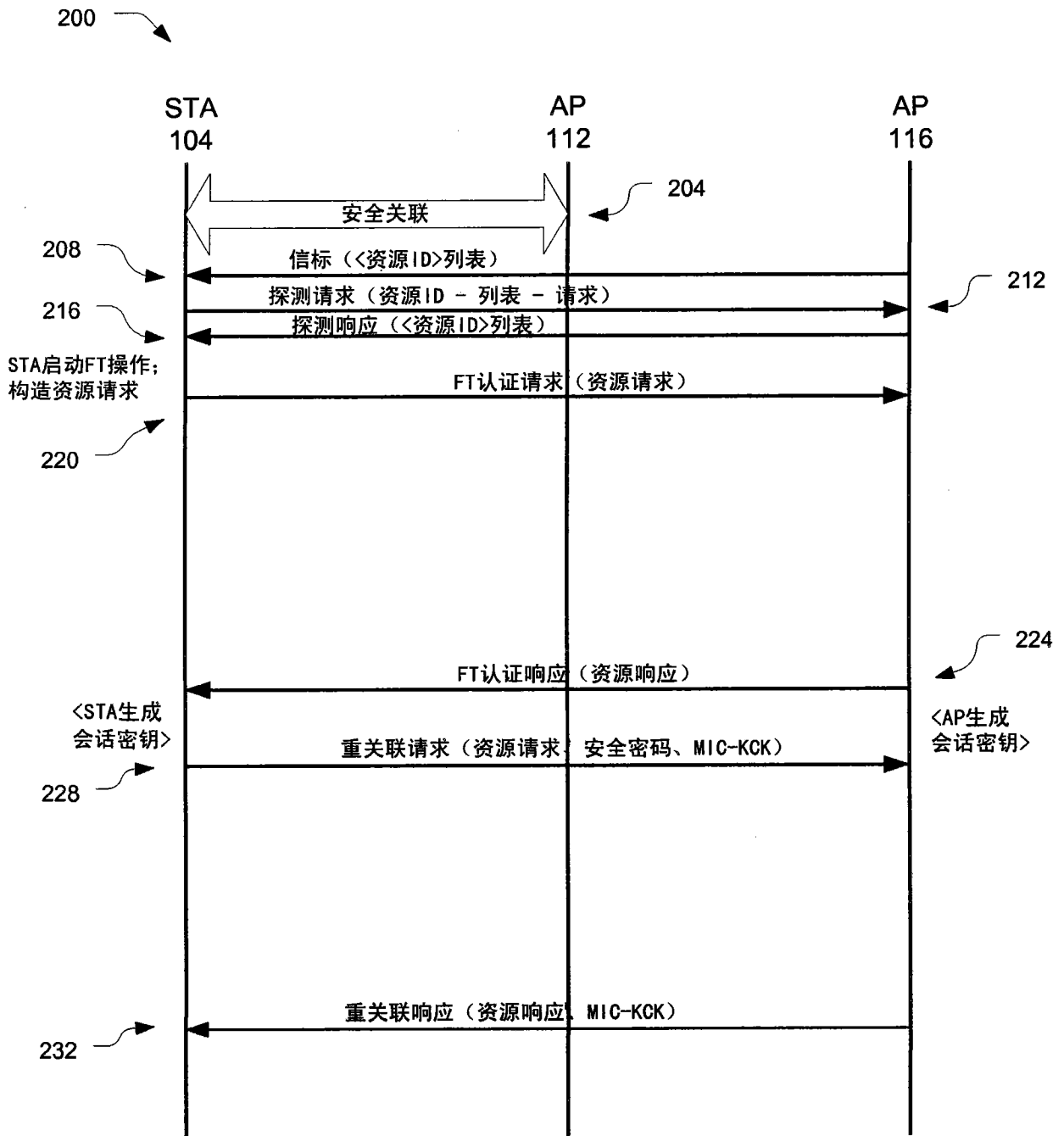


图 2

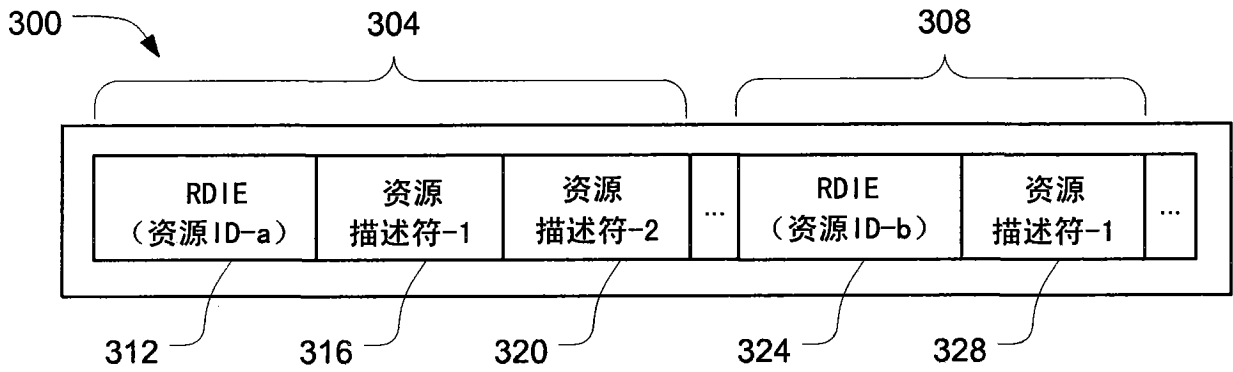


图 3

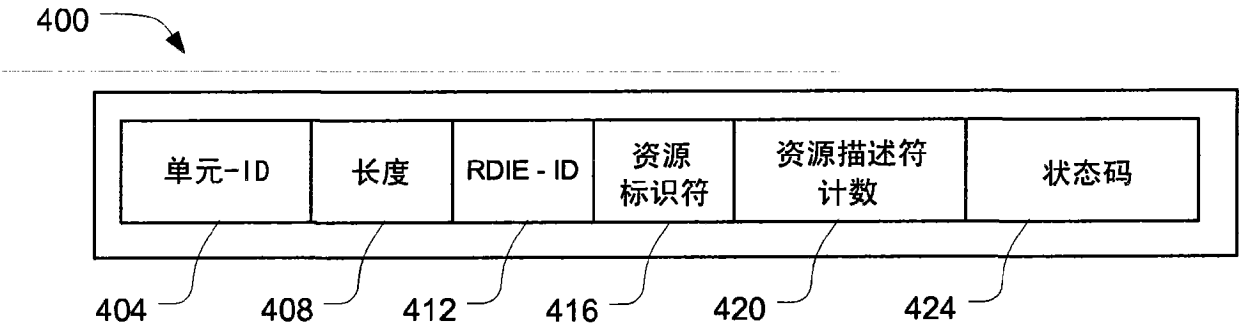


图 4

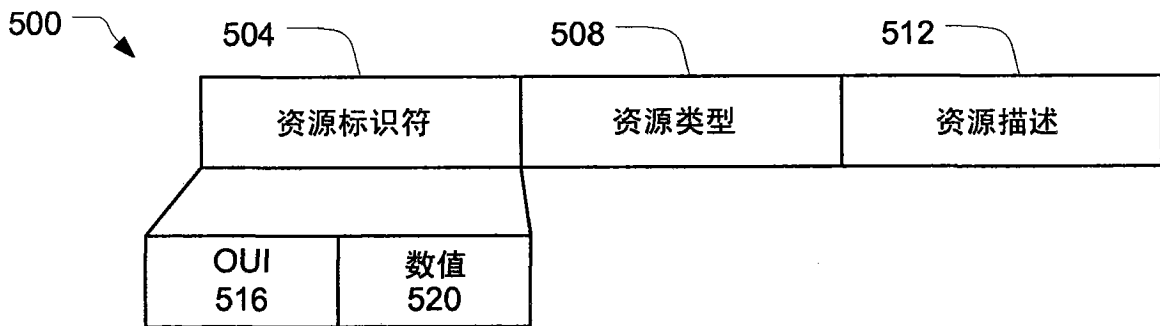


图 5

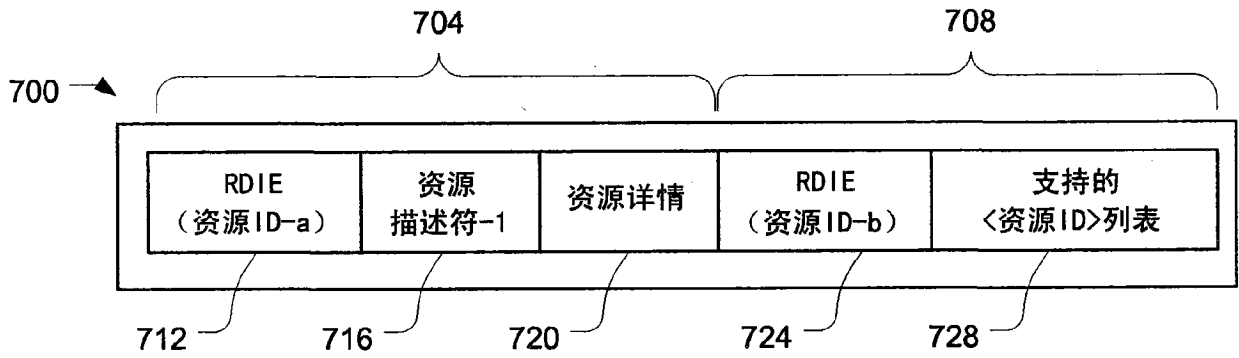


图 7

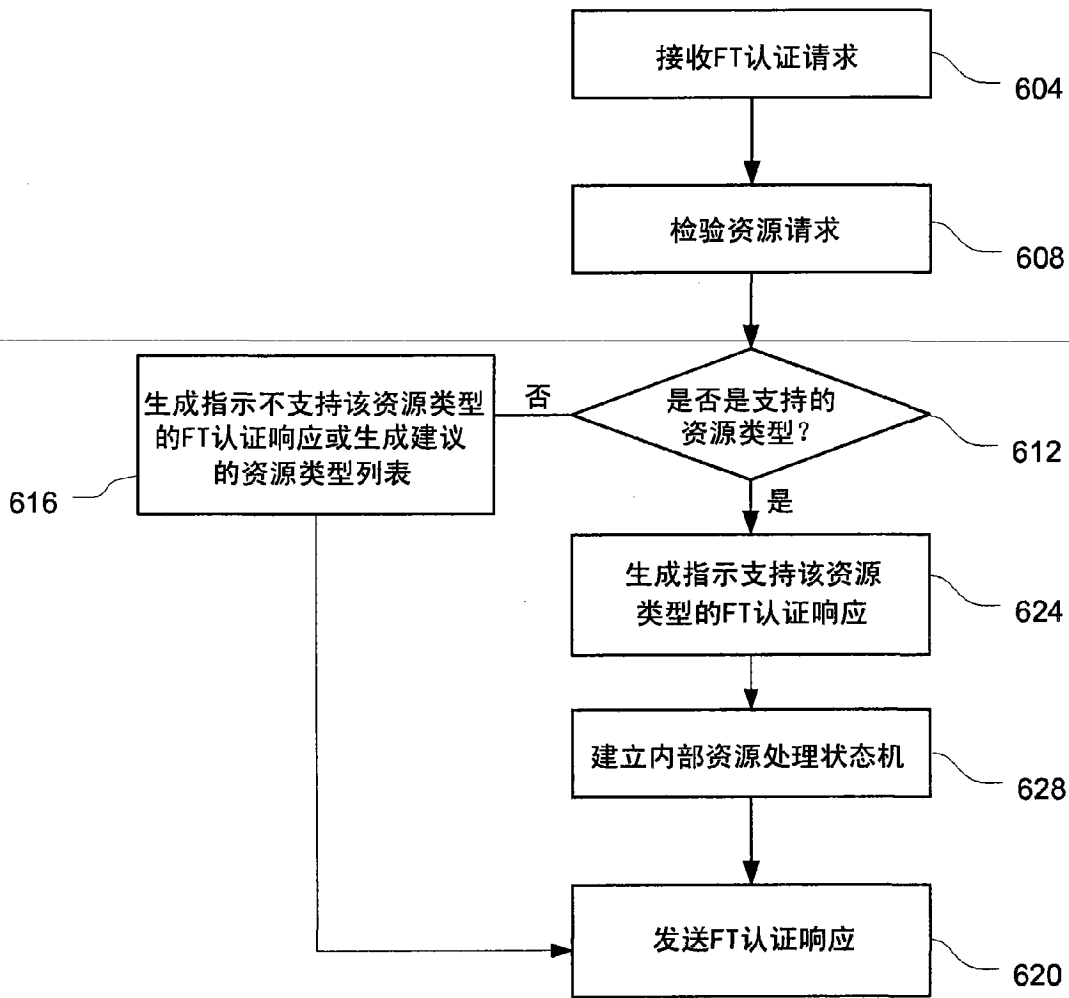


图 6

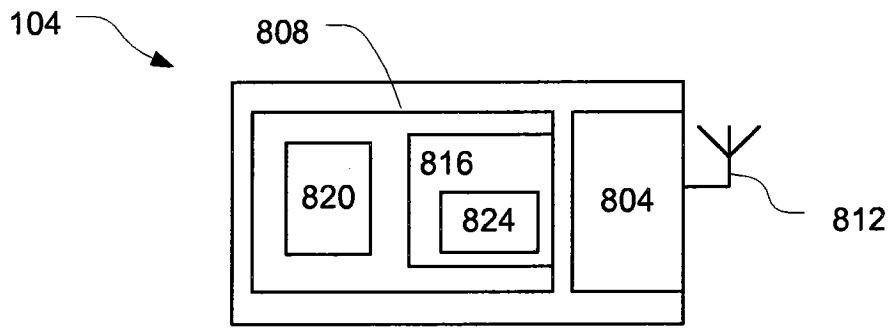


图 8

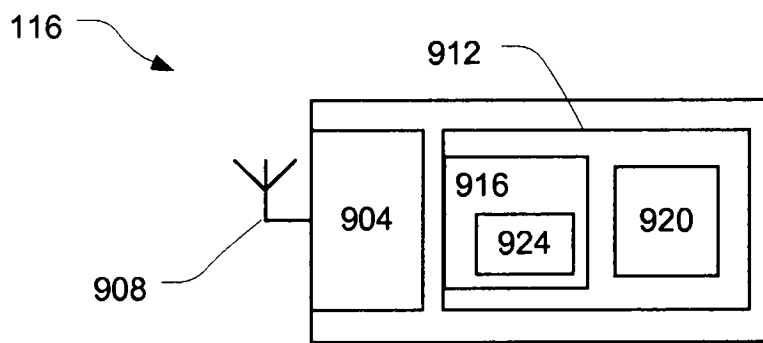


图 9

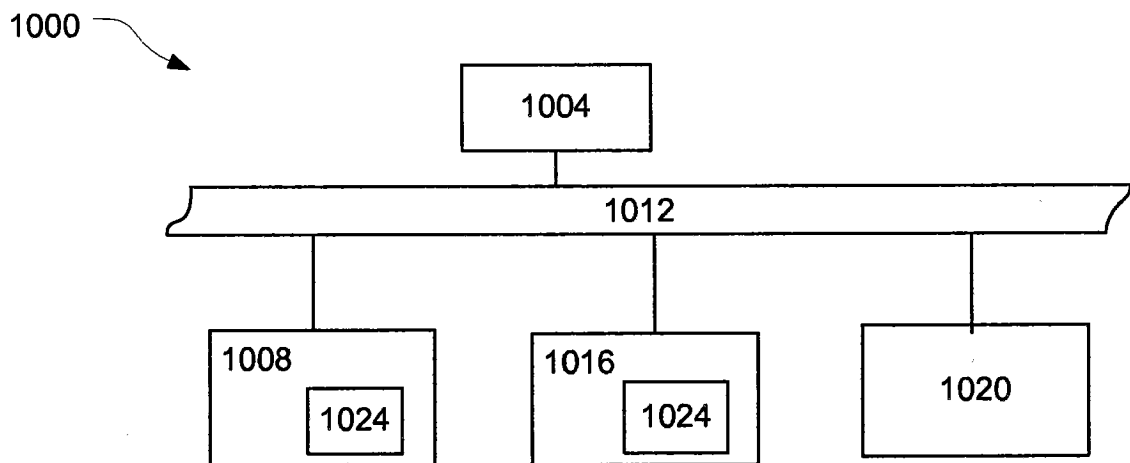


图 10