

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2009 年 7 月 30 日 (30.07.2009)



(10) 国际公布号
WO 2009/092318 A1



- (51) 国际专利分类号:
H04L 9/08 (2006.01) *H04N 7/16* (2006.01)
H04W 12/00 (2009.01)
- (21) 国际申请号: PCT/CN2009/070142
- (22) 国际申请日: 2009 年 1 月 14 日 (14.01.2009)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
200810017315.1
2008 年 1 月 17 日 (17.01.2008) CN
- (71) 申请人 (对除美国外的所有指定国): 西安西电捷通
无线网络通信有限公司 (CHINA IWNCOMM CO.,
LTD.) [CN/CN]; 中国陕西省西安市高新区科技二路
68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): 铁满霞 (TIE, Manxia)

[CN/CN]; 中国陕西省西安市高新区科技二路 68 号
西安软件园秦风阁 A201, Shaanxi 710075 (CN)。曹
军 (CAO, Jun) [CN/CN]; 中国陕西省西安市高新
区科技二路 68 号西安软件园秦风阁 A201, Shaanxi
710075 (CN)。庞辽军 (PANG, Liaojun) [CN/CN];
中国陕西省西安市高新区科技二路 68 号西安软件
园秦风阁 A201, Shaanxi 710075 (CN)。赖晓龙 (LAI,
Xiaolong) [CN/CN]; 中国陕西省西安市高新区科技
二路 68 号西安软件园秦风阁 A201, Shaanxi 710075
(CN)。黄振海 (HUANG, Zhenhai) [CN/CN]; 中国
陕西省西安市高新区科技二路 68 号西安软件园秦
风阁 A201, Shaanxi 710075 (CN)。

- (74) 代理人: 北京集佳知识产权代理有限公司 (UNI-
TALEN ATTORNEYS AT LAW); 中国北京市朝阳区
建国门外大街 22 号赛特广场 7 层, Beijing 100004
(CN)。

[见续页]

(54) Title: A SECURE TRANSMISSION METHOD FOR BROADBAND WIRELESS MULTIMEDIA NETWORK BROADCASTING COMMUNICATION

(54) 发明名称: 一种宽带无线多媒体网络广播通信的安全传输方法

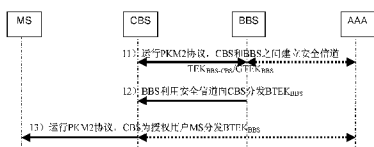


图 1 / FIG. 1

11) RUNNING PKM2 PROTOCOL, AND ESTABLISHING A SECURE CHANNEL BETWEEN CBS AND BBS
12) BBS DISTRIBUTES BTEK_{BBS} TO CBS THROUGH THE SECURE CHANNEL
13) RUNNING PKM2 PROTOCOL, AND CBS DISTRIBUTES BTEK_{BBS} FOR THE AUTHORIZED USER MS

(57) Abstract: A secure transmission method for broadband wireless multimedia network broadcasting communication includes the following steps: a secure channel between big base station and small base station is established by utilizing security protocols; the big base station distributes a Broadcast Traffic Encryption Key to each small base station through the secure channel; the small base station transmits the Broadcast Traffic Encryption Key to the user passing the authentication and authorization. The above solution solves the problem of broadcast secure communication of the big base station working in the mixed covering mode of large and small cells, realizes the identification of not only the user but also the base station, and ensures that only the authorized user can receive broadcast service.

(57) 摘要:

一种宽带无线多媒体网络广播通信的安全传输方法, 该方法包括以下步骤: 大基站与小基站之间利用安全协议建立安全信道; 大基站通过所述安全信道, 将广播通信加密密钥分发给各小基站; 小基站将所述广播通信加密密钥发送至通过认证授权的用户。上述技术方案解决了工作在大小小区制混合覆盖模式下的大基站的广播安全通信问题, 不仅实现了用户的身份认证, 而且实现了基站的身份认证, 并且确保只有授权用户才能收到广播业务。

WO 2009/092318 A1



(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告。

一种宽带无线多媒体网络广播通信的安全传输方法

本申请要求于 2008 年 1 月 17 日提交中国专利局、申请号为 200810017315.1、发明名称为“一种宽带无线多媒体网络广播通信的安全传输方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本发明涉及一种宽带无线多媒体网络广播通信的安全传输方法。

背景技术

10 宽带无线多媒体网络BWM (Broadband Wireless Multimedia networks) 旨在寻求一种运行高效、成本低廉的技术途径，从空中接口、无线接入网络、核心网络、业务平台和终端等不同侧面全方位地达成“三网融合”的总体目标。

15 BWM网络是一种融合移动电视网络和宽带无线接入网络技术特征的新型宽带无线移动网络，同时它又区别于宽带无线接入网络和移动电视网络。BWM网络可以配置强大的IP核心网络和综合业务管理平台，并为不同的终端业务配置了相同的运行维护支撑平台。在无线接入网络架构方面，BWM网络充分考虑了移动电视网络和宽带无线接入网络的组网特征，既支持传统广播电视网络的大基站覆盖的大区模式，又支持以蜂窝组网为特征的全小基站覆盖的小区模式，同时，在覆盖热点和室内场景时，允许针对点到点或者点到多点的通信模式进行优化组网。

BWM网络有三种典型的网络规划模式：

20 1) 以大基站构成的大区制覆盖模式，即单一广播基站应用模式。

单一广播基站BBS (Broadcast Base Station)，也称为大基站，其应用模式主要考虑从现有广播系统到BWM网络的平滑过渡。该应用模式下，单个广播基站BBS可覆盖50公里左右的范围，因此，几个广播基站就可覆盖一座城市。现有广播系统为单向广播系统，因此，在BWM的单一广播基站应用模式中，
25 接入网部分只有BBS和移动站点MS (Mobile Station)，移动站点MS接收来自广播基站BBS的单向视频/音频广播节目。

在运营商仅仅选择运营广播电视/音频业务时，传统的大区覆盖模式是最适当的网络规划方案。

-2-

2) 以大基站和小基站构成的大小区制混合覆盖模式, 即广播基站加蜂窝基站应用模式。

在这种工作模式下, 广播基站与单一广播基站应用模式中的功能相同, 若干广播基站发送同步的单向广播节目(全网广播)。蜂窝基站CBS(Cellular Base Station), 也称为小基站, 不仅实现双向数据发送, 而且为单向全网广播提供回传路径, 以支持点播业务、增强对用户的授权和认证等安全机制。

采用大基站发射广播电视/音频业务, 小基站发射宽带无线数据业务, 这样可以沿用既设的广播电视/音频系统和蜂窝系统的基站台, 降低建设基站的工程成本, 提升现有装置的使用寿命和效率。同时, 混合式的无线网络在开展运营服务时具有非常强的灵活性, 适应广播电视/音频业务和宽带无线接入业务分离和合成运营模式, 便于首先开展广播电视/音频业务, 随后开展宽带无线接入业务的演进式运营实施模式。广播电视业务的服务质量也可以优先得到保证, 尤其适合传统广电运营商为主开展商业服务。

3) 以全小基站构成的小区制覆盖模式, 即单一蜂窝基站应用模式。

单一蜂窝基站CBS应用模式下, 整个BWM只通过CBS以蜂窝结构进行覆盖, CBS之间可以采用时分复用TDM(Time-Division Multiplexing)、频分复用FDM(Frequency-Division Multiplexing) 或混合的复用方式。在该应用模式下, 原先由BBS实现的全网广播也由CBS实现, 因此, CBS支持的业务包括以全网广播方式的移动电视/音频, 以及以蜂窝方式通信的宽带无线接入业务。

BWM网络融合了数据通信和广播通信, 属于一种新型的无线网络体系结构, 同样需要解决安全接入与保密通信问题。由于全大基站模式不符合三网融合的目的, 该模式不属于BWM网络的主流模式, 因此该模式下的BWM网络的安全方案不予讨论, 仅讨论主要工作于全小基站模式或大小基站混合应用模式下的BWM网络的安全。在单一蜂窝基站应用模式下, 可利用IEEE802.16e提供的密钥管理协议PKM2(Privacy Key Management version 2) 或者基于三元对等鉴别的访问控制方法TePA-AC(Access Control method based on Tri-element Peer Authentication) 的安全协议, 实现用户与基站之间的身份认证及业务密钥的协商与分发, 实现用户的安全接入与业务的保密传输。而在大小基站混合应用模式下, 大基站的广播通信业务(视频、音频) 有时也需要进行保密传输或授权

-3-

传输,但由于大基站通常不具备上行信道,因此大基站无法接收用户的信息,从而无法实现大基站与用户之间的授权与安全通信。

发明内容

本发明实施例提供一种宽带无线多媒体网络广播通信的安全传输方法,以
5 实现在大小基站混合应用模式下,大基站与用户之间的授权与安全通信,技术方案如下:

一种宽带无线多媒体网络广播通信的安全传输方法,包括:

大基站与小基站之间利用安全协议建立安全信道;

大基站通过所述安全信道,将广播通信加密密钥分发给各小基站;

10 小基站将所述广播通信加密密钥发送至通过认证授权的用户。

其中,所述安全协议,可以是 IEEE802.16e 的密钥管理协议 PKM2 协议或基于三元对等鉴别的访问控制方法 TePA-AC 的安全协议。

以上技术方案利用 IEEE802.16e 提出的 PKM2 安全协议或者基于三元对等鉴别的访问控制方法 TePA-AC 的安全协议,大基站与小基站之间建立信任关系,形成安全通道,使得大基站的广播通信加密密钥可通过安全信道分发给小
15 基站,再由小基站秘密分发给各授权用户,确保只有授权用户才能接收到大基站的广播业务,解决了工作在大小区制混合覆盖模式下的不具有上行信道的大基站的广播安全通信问题。

本发明技术方案具有如下优点:

20 1) 不仅实现了用户的身份认证,而且实现了基站的身份认证;

2) 确保只有授权用户才能收到广播业务;

3) 可为不同的广播业务分发不同的通信加密密钥;

4) 实现广播通信加密密钥的动态更新。

附图说明

25 图 1 为本发明实施例一的方法示意图;

图 2 为本发明实施例二的方法示意图。

具体实施方式

为使上述发明目的和优点能够更加明显易懂,下面结合附图和具体实施方式对本发明技术方案作进一步详细的说明。

-4-

参见图 1 所示, 本发明实施例一的具体步骤如下:

11) 利用 IEEE802.16e 的 PKM2 协议, 大小基站之间建立信任关系, 形成安全信道;

11.1) 在建网时, 大小基站之间首先运行基于 RSA 的授权协议或 EAP 认证协议, 完成大小基站之间的身份认证及授权密钥 $AK_{BBS-CBS}$ (Authorization Key) 协商, 其中应用 EAP 认证协议时, 还需验证、授权和计费 AAA (Authentication、Authorization 和 Accounting) 服务器的参与;

11.2) 基于该授权密钥 $AK_{BBS-CBS}$, 大小基站通过密钥交换协议协商与分发大小基站之间的业务加密密钥 $TEK_{BBS-CBS}$ (Traffic Encryption Key) 与大基站的组播业务加密密钥 $GTEK_{BBS}$ (Group Traffic Encryption Key), 这里, 大小基站之间的业务包括大基站向小基站通告其广播通信加密密钥 $BTEK_{BBS}$ (Broadcast Traffic Encryption Key) 的消息及其他管理消息;

12) 通过安全信道, 大基站将广播通信加密密钥 $BTEK_{BBS}$ 秘密分发给各小基站,

15 大基站利用大小基站之间已协商的业务加密密钥 $TEK_{BBS-CBS}$ 将广播通信加密密钥 $BTEK_{BBS}$ 安全地分发给各小基站, 或者利用大基站已分发给各小基站的组播业务加密密钥 $GTEK_{BBS}$ 将广播通信加密密钥 $BTEK_{BBS}$ 安全地通告给各小基站;

13) 当用户登录至小基站时, 通过 IEEE802.16e 的 PKM2 协议认证授权后, 得到大基站的广播通信加密密钥 $BTEK_{BBS}$;

13.1) 当用户登录至小基站时, 运行基于 RSA 的授权协议或 EAP 认证协议, 完成用户与小基站之间的身份认证及授权密钥 AK_{CBS-MS} 协商, 其中应用 EAP 认证协议时, 还需 AAA 服务器的参与;

13.2) 基于该授权密钥 AK_{CBS-MS} , 用户与小基站通过密钥交换协议完成基站组播密钥加密密钥 $GKEK_{BS}$ (Group Key Encryption Key) 和组播业务加密密钥 $GTEK_{BS}$ 的分发; 其中组播业务加密密钥 $GTEK_{BS}$ 不仅包括小基站的组播业务加密密钥 $GTEK_{CBS}$, 同时还包括大基站的广播通信加密密钥 $BTEK_{BBS}$; 该过程实现了只有合法的授权用户才能得到大基站的广播通信加密密钥 $BTEK_{BBS}$, 从而使得授权用户能够秘密接收大基站的广播通信。

参见图 2 所示, 本发明实施例二的具体步骤如下:

21) 通过基于三元对等鉴别的访问控制方法 TePA-AC 的安全协议, 大小基站之间建立信任关系, 形成安全信道;

5 21.1) 在建网时, 大小基站之间运行接入认证与授权协议, 通过认证服务器 AS (Authentication Server) 完成大小基站之间的身份认证及授权密钥 $AK_{BBS-CBS}$ 协商;

10 21.2) 基于该授权密钥 $AK_{BBS-CBS}$, 大小基站通过连接业务密钥管理协议协商与分发大小基站之间的单播业务加密密钥 $UTEK_{BBS-CBS}$ (Unicast Traffic Encryption Key) 与大基站的组播业务加密密钥 $GTEK_{BBS}$; 这里, 大小基站之间的业务包括大基站向小基站通告其广播通信加密密钥 $BTEK_{BBS}$ 的消息及其他管理消息;

22) 通过安全信道, 大基站将广播通信加密密钥 $BTEK_{BBS}$ 秘密分发给各小基站;

15 大基站利用大小基站之间已协商的单播业务加密密钥 $UTEK_{BBS-CBS}$ 将广播通信加密密钥 $BTEK_{BBS}$ 安全地分发给各小基站, 或者利用大基站已分发给各小基站的组播业务加密密钥 $GTEK_{BBS}$ 将广播通信加密密钥 $BTEK_{BBS}$ 安全地通告给各小基站;

20 23) 当用户登录至小基站时, 通过基于三元对等鉴别的访问控制方法 TePA-AC 的安全协议认证授权后, 得到大基站的广播通信加密密钥 $BTEK_{BBS}$;

23.1) 当用户登录至小基站时, 运行接入认证与授权协议, 通过认证服务器 AS 完成用户与小基站之间的身份认证及授权密钥 AK_{CBS-MS} 协商;

25 23.1) 基于该授权密钥 AK_{CBS-MS} 通过组播连接业务密钥管理协议完成基站组播密钥加密密钥 $GKEK_{BS}$ 和组播业务加密密钥 $GTEK_{BS}$ 的分发; 其中组播业务加密密钥 $GTEK_{BS}$ 不仅包括小基站的组播业务加密密钥 $GTEK_{CBS}$, 同时还包括大基站的广播通信加密密钥 $BTEK_{BBS}$; 该过程实现了只有合法的授权用户才能得到大基站的广播通信加密密钥 $BTEK_{BBS}$, 从而使得授权用户能够秘密接收大基站的广播通信。

在实际应用中, 大基站可以根据广播业务的不同, 采用不同的广播通信加

—6—

密密钥进行保护传输，因此两个实施例的步骤 12) 或步骤 22) 中分发给各小基站的广播通信加密密钥可以是多个。为了进一步提高安全性，大基站的广播通信加密密钥还可进行动态更新，当密钥更新时，大基站可通过大基站的组播业务加密密钥 $GTEK_{BBS}$ 秘密通告给各小基站，再由各小基站通过小基站的组播密钥加密密钥 $GKEK_{BS}$ 秘密通告给各授权用户。

5

权 利 要 求

1、一种宽带无线多媒体网络广播通信的安全传输方法，其特征在于，包括：

大基站与小基站之间利用安全协议建立安全信道；

5 大基站通过所述安全信道，将广播通信加密密钥分发给各小基站；

小基站将所述广播通信加密密钥发送至通过认证授权的用户。

2、根据权利要求 1 所述的方法，其特征在于，所述安全协议为 IEEE802.16e 的密钥管理协议 PKM2。

10 3、根据权利要求 2 所述的方法，其特征在于，所述大基站与小基站之间利用安全协议建立安全信道，包括：

大基站与小基站之间首先运行基于 RSA 的授权协议或 EAP 认证协议，完成大基站与小基站之间的身份认证及授权密钥 $AK_{BBS-CBS}$ 协商；

15 基于该授权密钥 $AK_{BBS-CBS}$ ，大基站与小基站通过密钥交换协议协商大基站与小基站之间的业务加密密钥 $TEK_{BBS-CBS}$ 以及大基站的组播业务加密密钥 $GTEK_{BBS}$ 。

4、根据权利要求 2 所述的方法，其特征在于，所述大基站通过安全信道，将广播通信加密密钥分发给各小基站，包括：

20 大基站利用已协商的业务加密密钥 $TEK_{BBS-CBS}$ 将广播通信加密密钥 $BTEK_{BBS}$ 分发给各小基站，或者利用大基站已分发给各小基站的组播业务加密密钥 $GTEK_{BBS}$ 将广播通信加密密钥 $BTEK_{BBS}$ 通告给各小基站。

5、根据权利要求 2 所述的方法，其特征在于，所述小基站将广播通信加密密钥发送至通过认证授权的用户，包括：

当用户登录至小基站时，运行基于 RSA 的授权协议或 EAP 认证协议，完成用户与小基站之间的身份认证及授权密钥 AK_{CBS-MS} 协商；

25 小基站通过基于该授权密钥 AK_{CBS-MS} 的密钥交换协议，向用户分发组播密钥加密密钥 $GKEK_{BS}$ 和组播业务加密密钥 $GTEK_{BS}$ 。

6. 根据权利要求 3 至 5 任一项所述的方法，其特征在于，当大基站的广播通信加密密钥 $BTEK_{BBS}$ 更新时，大基站通过大基站的组播业务加密密钥 $GTEK_{BBS}$ 通告给各小基站，再由各小基站通过小基站的组播密钥加密密钥

GKEK_{BS} 通告给各授权用户。

7、根据权利要求 1 所述的方法，其特征在于，所述安全协议为基于三元对等鉴别的访问控制方法 TePA-AC 的安全协议。

8、根据权利要求 7 所述的方法，其特征在于，所述大基站与小基站之间
5 利用安全协议建立安全信道，包括：

大基站与小基站之间运行接入认证与授权协议，通过认证服务器 AS 完成大基站与小基站之间的身份认证及授权密钥 AK_{BBS-CBS} 协商；

基于该授权密钥 AK_{BBS-CBS}，大基站与小基站通过连接业务密钥管理协议协商大基站与小基站之间的单播业务加密密钥 UTEK_{BBS-CBS} 以及大基站的组播
10 业务加密密钥 GTEK_{BBS}。

9、根据权利要求 7 所述的方法，其特征在于，所述大基站通过安全信道，将广播通信加密密钥分发给各小基站，包括：

大基站利用已协商的单播业务加密密钥 UTEK_{BBS-CBS} 将广播通信加密密钥 BTEK_{BBS} 分发给各小基站，或者利用大基站已分发给各小基站的组播业务加密
15 密钥 GTEK_{BBS} 将广播通信加密密钥 BTEK_{BBS} 安全地通告给各小基站。

10、根据权利要求 7 所述的方法，其特征在于，所述小基站将广播通信加密密钥发送至通过认证授权的用户，包括：

当用户登录至小基站时，运行接入认证与授权协议，通过认证服务器 AS 完成用户与小基站之间的身份认证及授权密钥 AK_{CBS-MS} 协商；

20 小基站通过基于该授权密钥 AK_{CBS-MS} 的组播连接业务密钥管理协议，向用户分发组播密钥加密密钥 GKEK_{BS} 和组播业务加密密钥 GTEK_{BS}。

11、根据权利要求 8 至 10 任一项所述的方法，其特征在于，当大基站的广播通信加密密钥 BTEK_{BBS} 更新时，大基站通过大基站的组播业务加密密钥 GTEK_{BBS} 通告给各小基站，再由各小基站通过小基站的组播密钥加密密钥
25 GKEK_{BS} 通告给各授权用户。

12、根据权利要求 5 或 10 所述的方法，其特征在于，所述组播业务加密密钥 GTEK_{BS}，包括小基站的组播业务加密密钥 GTEK_{CBS} 和大基站的广播通信加密密钥 BTEK_{BBS}。

- 1/1 -

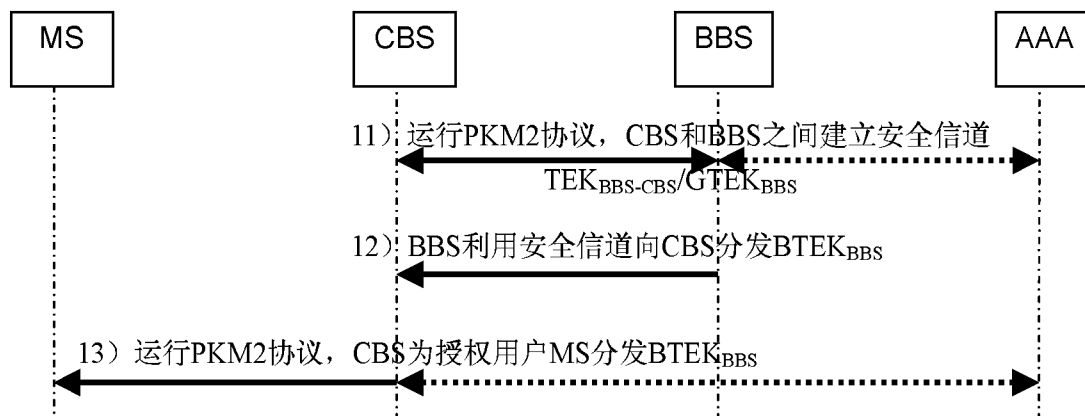


图 1

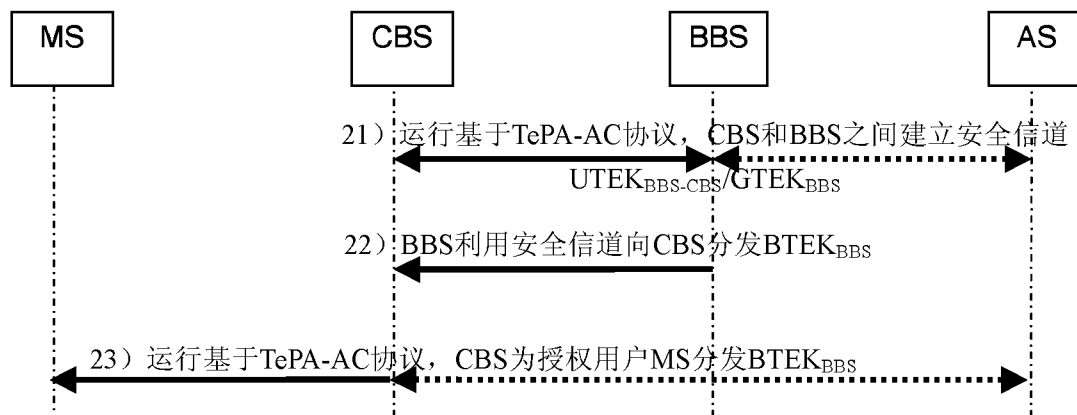


图 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/070142

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L,H04N,H04Q,H04B,H04J,H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT,CNKI,WPI,EPODOC,PAJ,IEEE: broadband wireless multimedia, BWM, broadband wireless access, broadcast+, multicast+, television, mobile television, big base station, small base station, broadcast+ base station, cellular base station, cell, mix, merge, secur+, safe, key, distribut+, WiMax, WiFi,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN101217811A (XIAN XIDIAN JIETONG WIRELESS NETWORK COM) 09 Jul.2008 (09.07.2008) the whole document	1-12
A	CN1852418A (CHINESE MOBILE COMMUNICATIONS GROUP CORP) 25 Oct. 2006 (25.10.2006) the whole document	1-12
A	CN1909546A (UNIV QINGHUA) 7 Feb. 2007 (07.02.2007) the whole document	1-12

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
13 Mar. 2009(13.03.2009)Date of mailing of the international search report
26 Mar. 2009 (26.03.2009)Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451Authorized officer
GAO, Xia
Telephone No. (86-10)62413541

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/070142

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP1028559A2 (SONY CORPORATION) 16 Aug. 2000 (16.08.2000) the whole document	1-12
A	ZHANG, Xiaodong et al., Research and Development of New Broadband Wireless Access System, ZTE COMMUNICATIONS, Apr. 2007, Vol.13 No.2, pages 20-24	1-12
A	WALKER, K. et al. The FLO™ Physical Layer, an Optimized Multicast Solution for Terrestrial Mobile Multimedia. 2005 IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, 14 Sep. 2005, Vol. 2, Pages 1238-1244	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2009/070142

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101217811A	09.07.2008	NONE	
CN1852418A	25.10.2006	NONE	
CN1909546A	07.02.2007	NONE	
EP1028559A2	16.08.2000	JP2000232423A	22.08.2000
		US7003115B1	21.02.2006

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/070142

CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i

H04W 12/00 (2009.01) i

H04N 7/16 (2006.01) i

A. 主题的分类		
参见附加页		
按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L,H04N,H04Q,H04B,H04J,H04W		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CNPAT,CNKI,WPI,EPODOC,PAJ,IEEE: 宽带无线多媒体, BWM, 宽带无线接入, 广播, 多播, 电视, 移动电视, 大基站, 小基站, 广播基站, 蜂窝基站, 大区, 小区, 混合, 融合, 安全, 密钥, 密钥协商, 密钥分发, WiMax, WiFi, broadband wireless multimedia, broadband wireless access, broadcast+, multicast+, television, mobile television, big base station, small base station, broadcast+ base station, cellular base station, cell, mix, merge, secur+, safe, key, distribut+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN101217811A (西安西电捷通无线网络通信有限公司) 09.7 月 2008 (09.07.2008) 全文	1-12
A	CN1852418A (中国移动通信集团公司) 25.10 月 2006 (25.10.2006) 全文	1-12
A	CN1909546A (清华大学) 07.2 月 2007 (07.02.2007) 全文	1-12
☒ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 13.3 月 2009(13.03.2009)		国际检索报告邮寄日期 26.3 月 2009 (26.03.2009)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		受权官员 高霞 电话号码: (86-10) 62413541

C(续). 相关文件

类 型	引用文件, 必要时, 指明相关段落	相关的权利要求
A	EP1028559A2 (SONY CORPORATION) 16.8 月 2000 (16.08.2000) 全文	1-12
A	张小东等, 新型宽带无线接入系统研发进展, 中兴通讯技术, 2007 年 4 月, 第 13 卷第 2 期, 第 20-24 页	1-12
A	WALKER, K. et al. The FLO TM Physical Layer, an Optimized Multicast Solution for Terrestrial Mobile Multimedia. 2005 IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, 2005 年 9 月 14 日, 第 2 卷, 第 1238-1244 页	1-12

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2009/070142

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101217811A	09.07.2008	无	
CN1852418A	25.10.2006	无	
CN1909546A	07.02.2007	无	
EP1028559A2	16.08.2000	JP2000232423A	22.08.2000
		US7003115B1	21.02.2006

主题的分类

H04L 9/08 (2006.01) i

H04W 12/00 (2009.01) i

H04N 7/16 (2006.01) i