(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
2010 年 1 月 7 日 (07.01.2010)

PCT

(10) 国际公布号
WO 2010/000171 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2009/072156

(22) 国际申请日: 2009 年 6 月 5 日 (05.06.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810129174.2 2008 年 6 月 30 日 (30.06.2008) CN

(71) 申请人 (对除美国外的所有指定国): **成都市华为赛门铁克科技有限公司 (HUAWEI SYMANTEC TECHNOLOGIES CO., LTD)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **刘利锋 (LIU, Lifeng)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。 **张东 (ZHANG, Dong)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。

(74) 代理人: **北京三高永信知识产权代理有限责任公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.)**; 中国北京市海淀区学院路蓟门里和景园 A-1-102, Beijing 100088 (CN)。

(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, CL, 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)。

[见续页]

(54) **Title**: COMMUNICATION ESTABLISHING METHOD, SYSTEM AND DEVICE

(54) **发明名称**: 一种通信的建立方法、系统和装置

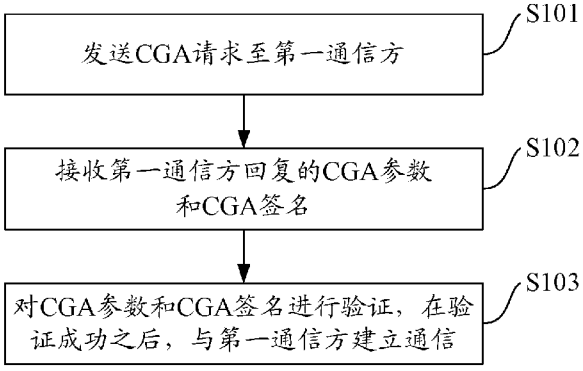

图 1 / FIG. 1

S101 sending a CGA request to the first communication party
S102 receiving a CGA parameter and a CGA signature that are returned by the first communication party
S103 verifying the CGA parameter and the CGA signature and after a successful verification, establishing communication with the first communication party

(57) **Abstract**: The embodiments of the present invention disclose a method, a system and a device for establishing communication. The communication establishing method is used for establishing communication between at least two communication parties which include the first communication party and the second communication party. The method involves sending a cryptographically generated address CGA request to said first communication party; receiving a CGA parameter and a CGA signature that are returned by the first communication party; verifying the CGA parameter and the CGA signature and after a successful verification, establishing communication with the first communication party. Based on the embodiments of the present invention, during the communication establishing procedure, the communication party confirms the reality of the CGA by verifying the CGA parameter and the CGA signature included in the CGA extension head, effectively prevents IP address cheating and prevents or lightens network security problems caused by IP address cheating.

[见续页]

WO 2010/000171 A1

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明实施例公开了一种通信的建立方法、系统和装置，所述通信的建立方法用于建立至少两个通信方之间的通信，包括第一通信方和第二通信方，包括：发送加密生成地址 CGA 请求至所述第一通信方；接收所述第一通信方回复的 CGA 参数和 CGA 签名；对所述 CGA 参数和 CGA 签名进行验证，在验证成功之后，与所述第一通信方建立通信。通过本发明实施例，在建立通信的过程中，通信方通过验证 CGA 扩展头所包括的 CGA 参数和 CGA 签名，确定 CGA 的真实性，有效防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

说 明 书

一种通信的建立方法、系统和装置

本申请要求于2008年06月30日提交中国专利局、申请号为200810129174.2、发明名称为“一种通信的建立方法、系统和装置”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。

技术领域

本发明实施例涉及通信技术领域，特别涉及一种通信的建立方法、系统和装置。

背景技术

在IP（Internet Protocol，因特网协议）地址、子网段和自动系统中，部分容许IP地址欺骗。因此，大部分的互联网都很容易遇到IP地址欺骗的问题，而且持续频发的这种IP地址欺骗可能成为一个非常严重的问题。例如:

a）伪装源地址的能力会衍生出某种类型的网络攻击，比如回应攻击，中间人攻击;

b）伪装以后的源地址可以实现某些其他形式的攻击，比如DDOS（Distribute Denial of Service，分布式拒绝服务攻击）攻击，而且非常难以被发觉;

c）允许伪装的源地址进入网络将无法通过查看源地址来得知IP数据包的来源。

现有技术中的URPF（Unicast Reverse Path Forwarding，单播反向路径转发）方法可以很好地解决IP地址欺骗的问题。URPF设定了以下数据包转发机制，当路由器接收到一个数据包时，该路由器检查路由表，确定返回数据包的源IP地址的路由是否从接收到该数据包的接口出去，如果是，则正常转发该数据包，否则，就会丢弃该数据包。

在实现本发明的过程中，发明人发现现有技术至少存在以下问题:

采用URPF在网络边界阻断伪造源地址IP的攻击，对于当前的DDoS攻击，并不能奏效，其根本原因就在于URPF的基本原理是路由器判断出口流量的源地址，如果该出口流量的源地址不属于内部子网的地址，则阻断出口流量。但是攻击者完全可以伪造其所在子网的IP地址进行DDoS攻击，这样就完全可以绕过URPF的防护策略。因此，现有技术仍然会使带有虚假源地址的数据包通过。

发明内容

本发明实施例提供一种通信的建立方法、系统和装置，以实现通过 CGA 参数和 CGA 签名，验证地址的真实性，防止 IP 地址欺骗。

本发明实施例一方面提供一种通信的建立方法，用于建立至少两个通信方之间的通信，包括第第一通信方和第二通信方，包括:

发送加密生成地址 CGA 请求至所述第一通信方;

接收所述第一通信方回复的 CGA 参数和 CGA 签名;

对所述 CGA 参数和 CGA 签名进行验证，在验证成功之后，与所述第一通信方建立通信。

另一方面，本发明实施例还提供一种通信的建立系统，包括:

第一通信方,用于接收加密生成地址 CGA 请求,并回复 CGA 参数和 CGA 签名;

第二通信方，用于发送所述 CGA 请求至所述第一通信方，接收所述第一通信方回复的 CGA 参数和 CGA 签名，并对所述 CGA 参数和 CGA 签名进行验证，在验证成功之后，与所述第一通信方建立通信。

再一方面，本发明实施例还提供一种通信设备，包括:

发送模块，用于发送加密生成地址 CGA 请求至另一通信设备;

接收模块，用于接收所述另一通信设备回复的 CGA 参数和 CGA 签名;

验证模块,用于对所述接收模块接收的 CGA 参数和 CGA 签名进行验证;

通信建立模块，用于在所述验证模块验证成功之后，与所述第一通信方建立通信。

再一方面，本发明实施例还提供一种传输帧格式，所述传输帧格式包括加密生成地址 CGA 请求数据，用于在两个通信方采用通信的建立方法建立通信的过程中，在两个通信方之间传输 CGA 请求，所述传输帧格式包括类型字段和预留域字段。

与现有技术相比，本发明实施例具有以下优点：通过本发明实施例，在建立通信的过程中，通信方通过验证 CGA 扩展头所包括的 CGA 参数和 CGA 签名，确定 CGA 的真实性，有效防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例通信的建立方法的流程图；

图 2 为本发明通信的建立方法实施例一的流程图；

图 3 为本发明通信的建立方法实施例二的流程图；

图 4 为本发明通信的建立方法实施例三的流程图；

图 5 为本发明实施例提供的一种传输帧格式的示意图；

图 6 为本发明实施例提供的另一种传输帧格式的示意图；

图 7 为本发明实施例提供的再一种传输帧格式的示意图；

图 8 为本发明实施例通信的建立系统的一种结构图；

图 9 为本发明实施例通信的建立系统的另一种结构图；

图 10 为本发明实施例通信设备的一种结构图；

图 11 为本发明实施例通信设备的另一种结构图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明的一部分实施例，

而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例提供一种通信的建立方法，解决了IP地址伪造、仿冒等IP地址欺骗问题，解决或者减轻了由于IP地址欺骗引起的一系列网络安全问题。

本发明实施例在 IPv6（Internet Protocol version 6，因特网协议版本 6）扩展头中增加 CGA（Cryptographically Generated Addresses，加密生成地址）扩展头，该 CGA 扩展头包括 CGA Request（CGA 请求）、CGA Params（CGA 参数）、CGA Sig（CGA 签名）。

如图 1 所示，为本发明实施例通信的建立方法的流程图，具体包括:

S101，发送 CGA 请求至第一通信方。具体可以为:

第二通信方接收第一通信方发送的会话请求，并对该会话请求进行检查，当该会话请求中的 IPv6 扩展头不包括 CGA 扩展头，或者该会话请求包括内容为空的 CGA 扩展头时，第二通信方发送 CGA 请求至第一通信方。

S102，接收第一通信方回复的 CGA 参数和 CGA 签名。

在接收到第二通信方发送的 CGA 请求之后，第一通信方向第二通信方回复 CGA 参数和 CGA 签名。本发明实施例在 IPv6 扩展头中增加 CGA 扩展头，第一通信方回复的 CGA 参数和 CGA 签名携带在 IPv6 扩展头的 CGA 扩展头中。

S103，对 CGA 参数和 CGA 签名进行验证，在验证成功之后，与第一通信方建立通信。

另外，在第二通信方接收第一通信方回复的 CGA 参数和 CGA 签名的同时，该第二通信方还可以接收第一通信方发送的 CGA 请求，在验证第一通信方回复的 CGA 参数和 CGA 签名成功之后，第二通信方向第一通信方回复该第二通信方的 CGA 参数和 CGA 签名。在第一通信方验证该第二通信方的 CGA 参数和 CGA 签名成功之后，第二通信方与第一通信方建立通信。这时，第一通信方和第二通信方相互验证了对方 CGA 的真实性。

上述通信的建立方法，在建立通信的过程中，通信方通过验证 CGA 扩展头所包括的 CGA 参数和 CGA 签名，确定 CGA 的真实性，有效防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

如图 2 所示，为本发明通信的建立方法实施例一的流程图，在实施例一

中，第一通信方为应答方，第二通信方为发起方。具体包括:

S201，发起方向应答方发送 CGA 请求。

S202，应答方收到 CGA 请求后，向发起方回复 CGA 参数、CGA 签名。

S203，发起方验证 CGA 参数及 CGA 签名，在验证成功之后，开始后续通信。如果验证失败，则停止通信过程。

上述通信的建立方法，发起方向应答方发送 CGA 请求，在接收到应答方回复的 CGA 参数及 CGA 签名之后，发起方验证 CGA 参数及 CGA 的签名，确定应答方 CGA 的真实性，从而防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

如图 3 所示，为本发明通信的建立方法实施例二的流程图，实施例二中，第一通信方为发起方，第二通信方为应答方。具体包括:

S301，发起方发起会话请求。

S302，应答方收到会话请求后，检查 IP 扩展头中是否有 CGA 扩展头，如果有，则进一步判断该 CGA 扩展头的内容是否为空，当该 CGA 扩展头的内容不为空时，执行 S304；如果 IP 扩展头中没有 CGA 扩展头，或者会话请求中的 CGA 扩展头的内容为空时，应答方发送 CGA 请求至发起方。

S303，发起方接收 CGA 请求，如果发起方支持 CGA 扩展，则回复 CGA 参数、CGA 签名；如果发起方不支持 CGA 扩展，则该发起方丢弃该 CGA 请求。

S304，应答方收到发送方回复的 CGA 参数、CGA 签名后，验证该 CGA 参数及 CGA 签名，在验证成功之后，开始后续通信。如果验证失败，则应答方丢弃发送方回复的 CGA 参数和 CGA 签名。

上述通信的建立方法，在应答方收到发起方的会话请求之后，应答方向发起方发送 CGA 请求，并验证发起方回复的 CGA 参数及 CGA 签名，确定发起方 CGA 的真实性，从而防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

如图 4 所示，为本发明通信的建立方法实施例三的流程图，实施例三中，第一通信方为发起方，第二通信方为应答方。具体包括:

S401，发起方发起会话请求，该会话请求包括内容为空的 CGA 扩展头。

S402，应答方收到会话请求后，发送 CGA 请求至发起方。

S403，发起方收到 CGA 请求后，向应答方回复 CGA 参数、CGA 签名，并向应答方发送 CGA 请求。

S404，应答方收到发起方发送的 CGA 请求后，应答方先验证发起方回复的 CGA 参数及 CGA 签名，在验证成功之后，应答方向发起方回复该应答方的 CGA 参数及 CGA 签名；如果验证失败，则应答方丢弃发起方发送的 CGA 参数、CGA 签名和 CGA 请求。

S405，发起方收到应答方回复的 CGA 参数，CGA 签名后，验证 CGA 参数及 CGA 签名，在验证成功之后，开始后续通信。如果验证失败，则发起方丢弃该 CGA 参数，CGA 签名。

上述通信的建立方法，在应答方收到发起方的会话请求之后，应答方向发起方发送 CGA 请求，并验证发起方回复的 CGA 参数及 CGA 签名，同时发起方也向应答方发送 CGA 请求，验证应答方回复的 CGA 参数及 CGA 签名，发起方和应答方相互确定对方 CGA 的真实性，从而防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

本发明实施例通过增加 CGA 扩展头，在建立通信的过程中，要求通信方在消息中添加包括 CGA 参数和 CGA 签名的扩展头，用于验证 CGA 的真实性，防止 IP 地址欺骗，防止或减轻由于 IP 地址欺骗引起的一些网络安全问题。

以 TCP（Transmission Control Protocol，传输控制协议）-SYN（Synchronization，同步）洪水攻击为例，攻击者通过僵尸网络发起大量虚假地址的 SYN 请求。

应用本发明实施例，服务器收到 SYN 请求后，不会立即回应 SYN-ACK（Acknowledgement，确认）并建立半连接状态，而是先检查 SYN 请求里面有没有 CGA 扩展头。1）如果 SYN 请求没有 CGA 扩展头，服务器发送 CGA 请求且不需要为该 SYN 请求建立状态信息，由于 SYN 请求中的源地址为虚假地址，所以服务器不会再收到回应；2）如果 SYN 请求中带有 CGA 扩展头，服务器会先验证 CGA 的有效性，如果 SYN 请求中的源地址为虚假地址，服

务器只需做简单的哈希运算，即可判断该 SYN 请求是非法的，丢弃该 SYN 请求即可。应用本发明实施例，虽然服务器仍需要为虚假地址的 SYN 请求耗费一些资源，但相对于回应 SYN-ACK 并建立半连接状态，资源消耗很小，并且不需要为虚假地址的请求保持半连接状态，很大程度上解决了 TCP-SYN 洪水攻击问题。

以中间人攻击为例:

“中间人”（主机 C，攻击者）处于通信发起方（主机 A）与应答方（主机 B）之间，同时冒充发起方和应答方的地址，分别与主机 A、主机 B 通信。若主机 A 知道主机 B 的地址，那么在应用本发明实施例时，攻击者无法篡改主机 B 发给主机 A 的消息，因为通过应用 CGA 签名，将主机 B 的身份和 CGA 进行绑定，攻击者不知道主机 B 的私钥，无法得出篡改后消息的正确签名。

上述实施例是在 IPv6 扩展头中增加 CGA 扩展头，该 CGA 扩展头包括 CGA 请求、CGA 参数、CGA 签名。此外，在另一个实施例中，还可以在现有 IPv6 的目的选项头（Destination Options header）携带 CGA 相关信息，该 CGA 相关信息包括 CGA 请求、CGA 参数、CGA 签名。

本发明实施例还提供了一种传输帧格式，该传输帧格式包括 CGA 请求数据，用于在两个通信方采用本发明实施例提供的通信的建立方法建立通信的过程中，在两个通信方之间传输 CGA 请求。在通信过程中，通信任意一方均可以通过发送包括了 CGA 请求选项的 IP 数据包来向对方请求 CGA 参数和 CGA 签名。接收到该 IP 数据包的通信方需要在回复的数据包中包括 CGA 参数、CGA 签名。

本发明实施例提出的 CGA 请求选项的格式如图 5 所示，该 CGA 请求选项包括:

类型（Type）字段，为 8 比特无符号整数，在本实施例中，当该类型字段的数值为 193 时，表明该数据包为 CGA 请求。在其它实施例中，也可用其它数值表明该数据包为 CGA 请求。

预留域（Reserved）字段，长度为 24 比特，以备将来扩展使用。该预留域字段必须设为 0。

序列号（Sequence Number）字段，为 32 比特随机数，包括防止重放攻击

的信息。

本发明实施例还提供了一种传输帧格式，该传输帧格式包括 CGA 参数数据，用于在两个通信方采用本发明实施例提供的通信的建立方法建立通信的过程中，在两个通信方之间传输 CGA 参数，接收到 CGA 参数的通信方根据该 CGA 参数对 CGA 进行验证。

本发明实施例提出的 CGA 参数选项的格式如图 6 所示，该 CGA 参数选项包括:

类型（Type）字段，为 8 比特无符号整数。在本实施例中，当该类型字段的数值为 194 时，表明该数据包为 CGA 参数。在其它实施例中，也可用其它值表明该数据包为 CGA 参数。

长度（Length）字段，为 8 比特无符号整数，以字节为单位，表明整个 CGA 参数的长度，为类型字段、长度字段、填充长度字段、预留域字段、序列号字段、CGA 参数字段以及填充字段等各字段长度的总和，在另一个实施例中，长度字段可以是 8 字节。

填充长度（Pad Length）字段，为 8 比特无符号整数，表示填充字段的长度，单位为字节。

预留域（Reserved）字段，长度为 8 比特字段，以备将来扩展使用。该预留域字段必须设为 0。

序列号（Sequence Number）字段，为 32 比特整数，包括防止重放攻击的信息。如果该 CGA 参数用于响应 CGA 请求，该序列号字段的值为 CGA 请求中的序列号的值加 1；否则，将该序列号字段置为 0。

参数（Parameters）字段，长度可变，包括 CGA 参数信息。

填充（Padding）字段，可变长度域，用于使数据包长度为 8 字节的整数倍。该填充字段的内容必须为 0。

本发明实施例还提供一种传输帧格式，该传输帧格式包括 CGA 签名数据，用于在两个通信方采用本发明实施例提供的通信的建立方法建立通信的过程中，在两个通信方之间传输 CGA 签名，CGA 签名用于发送使用 CGA 参数中的公钥所对应的私钥对数据包的签名。

本发明实施例提出的 CGA 签名选项的格式如图 7 所示，该 CGA 签名选项包括:

类型（Type）字段，为 8 比特无符号整数。在本实施例中，若类型字段的数值为 195 时，表明该数据包为 CGA 签名。在其它实施例中，也可用其它数值表明该数据包为 CGA 签名。

长度（Length）字段，为 8 比特无符号整数，以字节为单位表明整个 CGA 签名的长度，为类型字段、长度字段、填充长度字段、预留域字段、CGA 签名字段和填充字段等各字段长度的总和。

填充长度（Pad Length）字段，为 8 比特无符号整数，表示填充字段的长度，单位为字节。

预留域（Reserved）字段，长度为 8 比特，以备将来扩展使用。该预留域字段必须设为 0。

签名（Signature）字段，为可变长度字段，包括用发送者私钥对数据包内容的签名。

填充（Padding）字段，为可变长度字段，用于使数据包长度为 8 字节的整数倍。该填充字段的内容必须为 0。

如图 8 所示，为本发明实施例通信的建立系统的结构图，包括:

第一通信方 81，用于接收 CGA 请求，并回复 CGA 参数和 CGA 签名;

第二通信方 82，用于发送 CGA 请求至第一通信方 81，接收第一通信方 81 回复的 CGA 参数和 CGA 签名，并对该 CGA 参数和 CGA 签名进行验证，在验证成功之后，与第一通信方 81 建立通信。

在本发明的另一实施例中，如图 9 所示，第二通信方 82 可以包括:

发送模块 821，用于发送 CGA 请求至第一通信方 81;

接收模块 822，用于接收第一通信方 81 回复的 CGA 参数和 CGA 签名;

验证模块 823，用于对接收模块 822 接收的 CGA 参数和 CGA 签名进行验证;

通信建立模块 824，用于在验证模块 823 验证成功之后，与第一通信方 81 建立通信。

该发送模块 821 可以包括:

会话请求接收子模块 8211，用于接收第一通信方 81 发送的会话请求;

CGA 请求发送子模块 8212，用于当会话请求接收子模块 8211 接收的会话请求的 IPv6 扩展头中不包括 CGA 扩展头，或者该会话请求包括内容为空的 CGA 扩展头，或该会话请求的 IPv6 扩展头中不包括目的选项头，或该会话请求的 IPv6 的目的选项头不包括 CGA 相关信息时，发送 CGA 请求至第一通信方 81。

该第二通信方 82 还可以包括:

CGA 请求接收模块 825，用于在接收模块 822 接收第一通信方 81 回复的 CGA 参数和 CGA 签名的同时，接收第一通信方 81 发送的 CGA 请求;

CGA 回复模块 826，用于在 CGA 请求接收模块 825 接收到第一通信方 81 发送的 CGA 请求，且验证模块 823 验证 CGA 参数和 CGA 签名成功之后，向第一通信方 81 回复第二通信方 82 的 CGA 参数和 CGA 签名。

上述通信的建立系统，在建立通信的过程中，第二通信方 82 通过验证第一通信方 81 回复的 CGA 参数和 CGA 签名，确定第一通信方 81CGA 的真实性，有效防止了 IP 地址欺骗，防止或减轻了由于 IP 地址欺骗引起的一些网络安全问题。

如图 10 所示，为本发明实施例通信设备 10 的结构图，包括:

发送模块 101，用于发送 CGA 请求至另一通信设备;

接收模块 102，用于接收另一通信设备回复的 CGA 参数和 CGA 签名;

验证模块 103，用于对接收模块 102 接收的 CGA 参数和 CGA 签名进行验证;

通信建立模块 104，用于在验证模块 103 验证成功之后，与另一通信设备建立通信。

在本发明的另一实施例中，如图 11 所示，发送模块 101 可以包括:

会话请求接收子模块 1011，用于接收另一通信设备发送的会话请求;

CGA 请求发送子模块 1012，用于当会话请求接收子模块 1011 接收的会话请求的 Ipv6 扩展头中不包括 CGA 扩展头，或者该会话请求包括内容为空

的 CGA 扩展头，或该会话请求的 IPv6 扩展头中不包括目的选项头，或该会话请求的 IPv6 扩展头中目的选项头不包括 CGA 相关信息时，发送该 CGA 请求至另一通信设备。

该通信设备 10 还可以包括:

CGA 请求接收模块 105，用于在接收模块 102 接收另一通信设备回复的 CGA 参数和 CGA 签名的同时，接收所述另一通信设备发送的 CGA 请求;

CGA 回复模块 106，用于在 CGA 请求接收模块 105 接收到另一通信设备发送的 CGA 请求，且在验证模块 103 验证 CGA 参数和 CGA 签名成功之后，向另一通信设备回复该通信设备的 CGA 参数和 CGA 签名。

上述通信设备，在与另一通信设备建立通信的过程中，发送模块 101 发送 CGA 请求至另一通信设备，接收模块 102 接收另一通信设备回复的 CGA 参数和 CGA 签名，验证模块 103 对接收模块 102 接收的 CGA 参数和 CGA 签名进行验证，确定第一通信方 51CGA 的真实性，在验证模块 103 验证成功之后，通信建立模块 104 与另一通信设备建立通信。使用本发明实施例提供的上述通信设备，可以有效防止 IP 地址欺骗，防止或减轻由于 IP 地址欺骗引起的一些网络安全问题。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

权 利 要 求 书

1、一种通信的建立方法，用于建立至少两个通信方之间的通信，包括第一通信方和第二通信方，其特征在于，包括:

发送加密生成地址 CGA 请求至所述第一通信方;

接收所述第一通信方回复的 CGA 参数和 CGA 签名;

对所述 CGA 参数和 CGA 签名进行验证，在验证成功之后，与所述第一通信方建立通信。

2、如权利要求 1 所述通信的建立方法，其特征在于，在所述发送 CGA 请求至第一通信方之前，还包括: 接收所述第一通信方发送的会话请求，当所述会话请求的因特网协议版本 6 IPv6 扩展头不包括 CGA 扩展头，或所述会话请求的 IPv6 扩展头中不包括目的选项头时，发送 CGA 请求至所述第一通信方。

3、如权利要求 1 所述通信的建立方法，其特征在于，在所述发送 CGA 请求至第一通信方之前，还包括: 接收所述第一通信方发送的会话请求，当所述会话请求包括内容为空的 CGA 扩展头，或所述会话请求的 IPv6 扩展头的目的选项头不包括 CGA 相关信息时，发送 CGA 请求至所述第一通信方。

4、如权利要求 1 所述通信的建立方法，其特征在于，在所述接收第一通信方回复的 CGA 参数和 CGA 签名的同时，还接收所述第一通信方发送的 CGA 请求;

在验证所述 CGA 参数和 CGA 签名成功之后，向所述第一通信方回复所述第二通信方的 CGA 参数和 CGA 签名;

在所述第一通信方验证所述第二通信方的 CGA 参数和 CGA 签名成功之后，建立与所述第一通信方通信。

5、如权利要求 1 至 4 任意一项所述通信的建立方法，其特征在于，所述 CGA 参数和 CGA 签名携带在 IPv6 扩展头的 CGA 扩展头中或携带在 IPv6 的目的选项头中。

6、一种通信设备，其特征在于，包括:

发送模块，用于发送加密生成地址 CGA 请求至另一通信设备;

接收模块，用于接收所述另一通信设备回复的 CGA 参数和 CGA 签名;

验证模块，用于对所述接收模块接收的 CGA 参数和 CGA 签名进行验证;

通信建立模块，用于在所述验证模块验证成功之后，与所述另一通信设备建立通信。

7、如权利要求 6 所述通信设备，其特征在于，所述发送模块包括:

会话请求接收子模块，用于接收所述另一通信设备发送的会话请求;

CGA 请求发送子模块，用于当所述会话请求接收子模块接收的会话请求的 IPv6 扩展头中不包括 CGA 扩展头，或者所述会话请求包括内容为空的 CGA 扩展头，或所述会话请求的 IPv6 扩展头中不包括目的选项头，或所述会话请求的 IPv6 扩展头中目的选项头不包括 CGA 相关信息时，发送所述 CGA 请求至所述另一通信设备。

8、如权利要求 6 所述通信设备，其特征在于，还包括:

CGA 请求接收模块，用于在所述接收模块接收所述另一通信设备回复的 CGA 参数和 CGA 签名的同时，接收所述另一通信设备发送的 CGA 请求;

CGA 回复模块，用于在所述 CGA 请求接收模块接收到所述另一通信设备发送的 CGA 请求，且所述验证模块验证所述 CGA 参数和 CGA 签名成功之后，向所述另一通信设备回复所述通信设备的 CGA 参数和 CGA 签名。

9、一种通信的建立系统，其特征在于，包括:

第一通信方，用于接收加密生成地址 CGA 请求，并回复 CGA 参数和 CGA 签名;

第二通信方，用于发送所述 CGA 请求至所述第一通信方，接收所述第一通信方回复的 CGA 参数和 CGA 签名，并对所述 CGA 参数和 CGA 签名进行验证，在验证成功之后，与所述第一通信方建立通信。

10、如权利要求 9 所述通信的建立系统，其特征在于，所述第二通信方的特征如权利要求 6－8 任一项所述。

11、一种传输帧格式，其特征在于，所述传输帧格式包括加密生成地址 CGA 请求数据，用于在两个通信方采用权利要求 1 所述的通信的建立方法建立通信的过程中，在两个通信方之间传输 CGA 请求，所述传输帧格式包括类型字段和预留域字段。

12、如权利要求 11 所述传输帧格式，其特征在于，所述传输帧格式还包

序列号字段，所述序列号字段，包括防止重放攻击的信息。

13、如权利要求 11 所述传输帧格式，其特征在于，所述类型字段标识所述传输帧为 CGA 请求帧。

14、如权利要求 11 所述传输帧格式，其特征在于，所述传输帧格式还包括:

长度字段、填充长度字段、参数字段和填充字段，其中，所述参数字段，包括 CGA 参数信息。

15、如权利要求 14 所述传输帧格式，其特征在于，所述类型字段，标识所述传输帧为 CGA 参数帧;

所述长度字段，以字节为单位表示整个传输帧的长度。

16、如权利要求 11 所述传输帧格式，其特征在于，所述传输帧格式还包括:

长度字段、填充长度字段、签名字段和填充字段，其中，所述签名字段，包括用发送者私钥对数据包内容的签名。

17、如权利要求 16 所述传输帧格式，其特征在于，所述类型字段，标识所述传输帧为 CGA 签名帧;

所述长度字段，以字节为单位表示整个传输帧的长度。

说 明 书 附 图

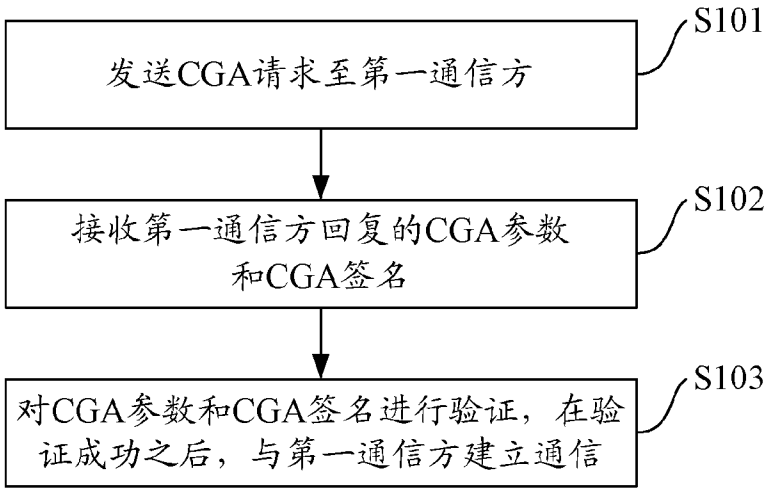
S101
发送CGA请求至第一通信方
S102
接收第一通信方回复的CGA参数和CGA签名
S103
对CGA参数和CGA签名进行验证，在验证成功之后，与第一通信方建立通信

图 1

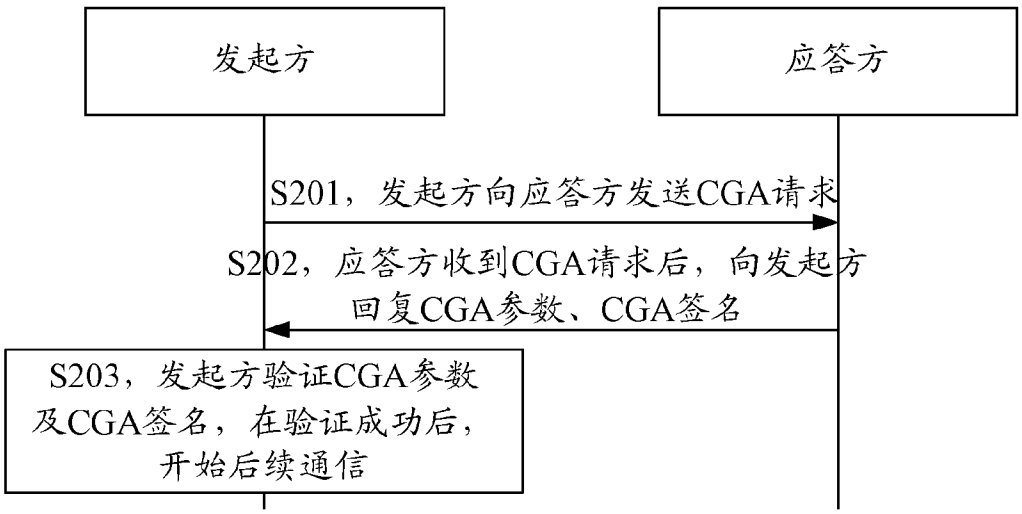
发起方
应答方
S201，发起方向应答方发送CGA请求
S202，应答方收到CGA请求后，向发起方回复CGA参数、CGA签名
S203，发起方验证CGA参数及CGA签名，在验证成功后，开始后续通信

图 2

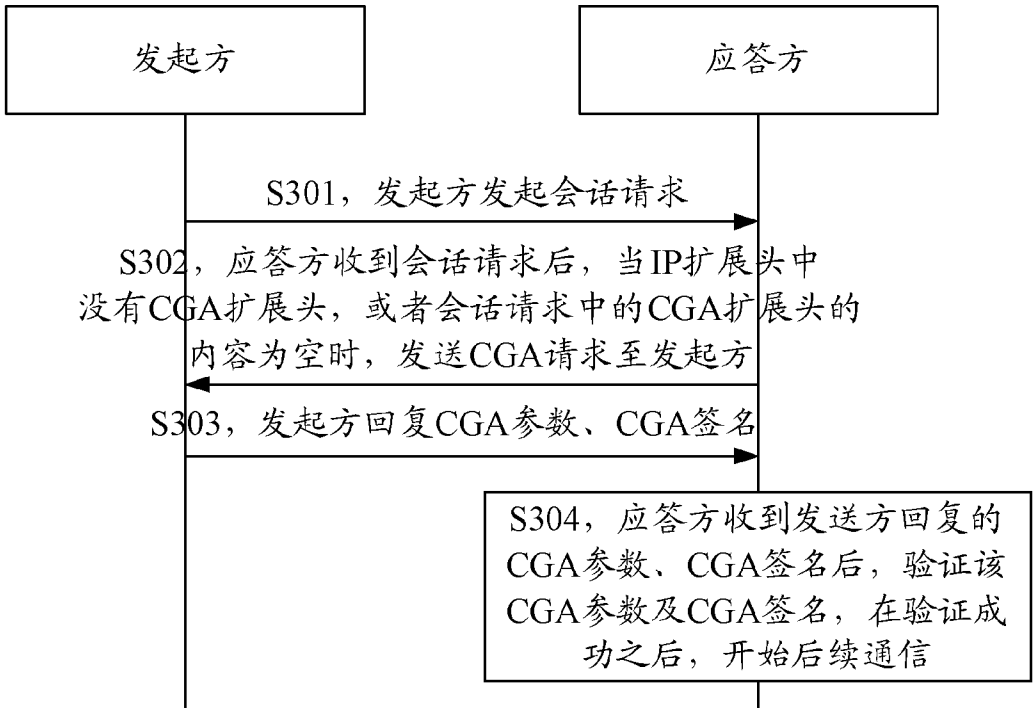
发起方
应答方
S301，发起方发起会话请求
S302，应答方收到会话请求后，当IP扩展头中没有CGA扩展头，或者会话请求中的CGA扩展头的内容为空时，发送CGA请求至发起方
S303，发起方回复CGA参数、CGA签名
S304，应答方收到发送方回复的CGA参数、CGA签名后，验证该CGA参数及CGA签名，在验证成功之后，开始后续通信

图 3

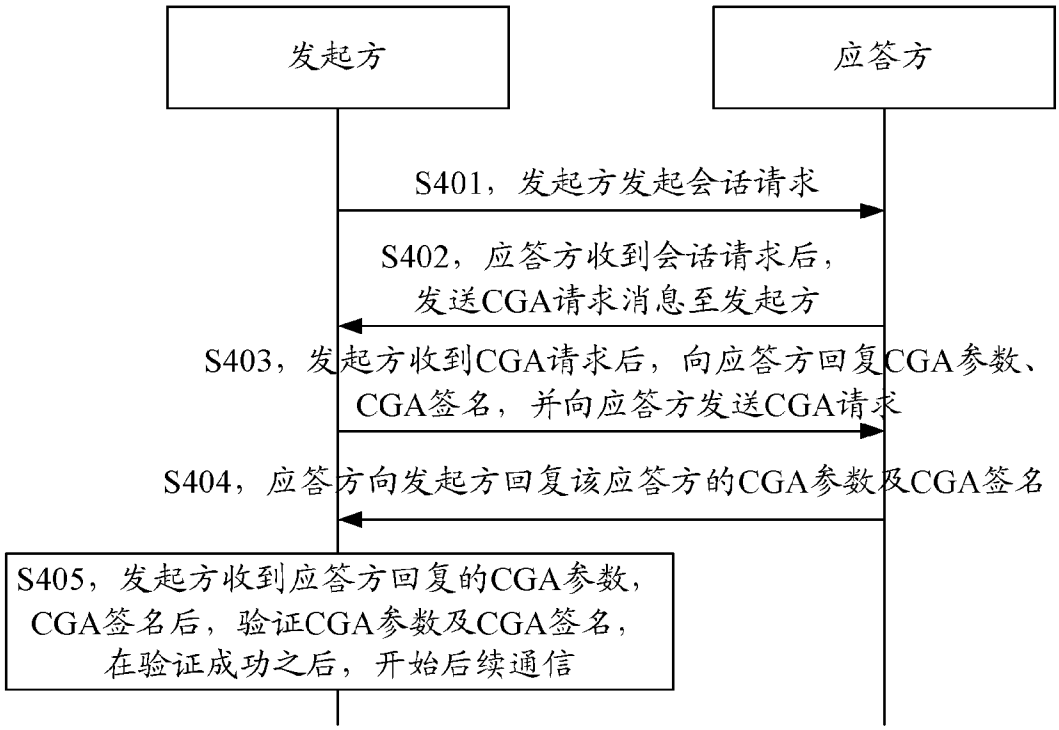
发起方
应答方
S401，发起方发起会话请求
S402，应答方收到会话请求后，发送CGA请求消息至发起方
S403，发起方收到CGA请求后，向应答方回复CGA参数、CGA签名，并向应答方发送CGA请求
S404，应答方向发起方回复该应答方的CGA参数及CGA签名
S405，发起方收到应答方回复的CGA参数，CGA签名后，验证CGA参数及CGA签名，在验证成功之后，开始后续通信

图 4

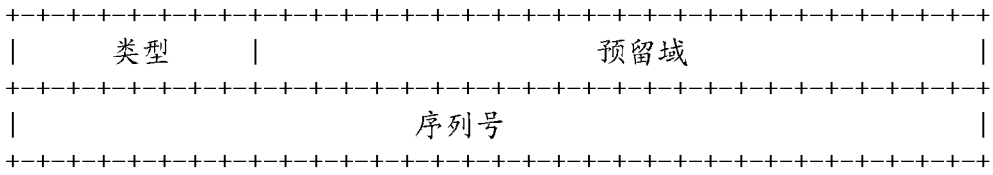

图 5

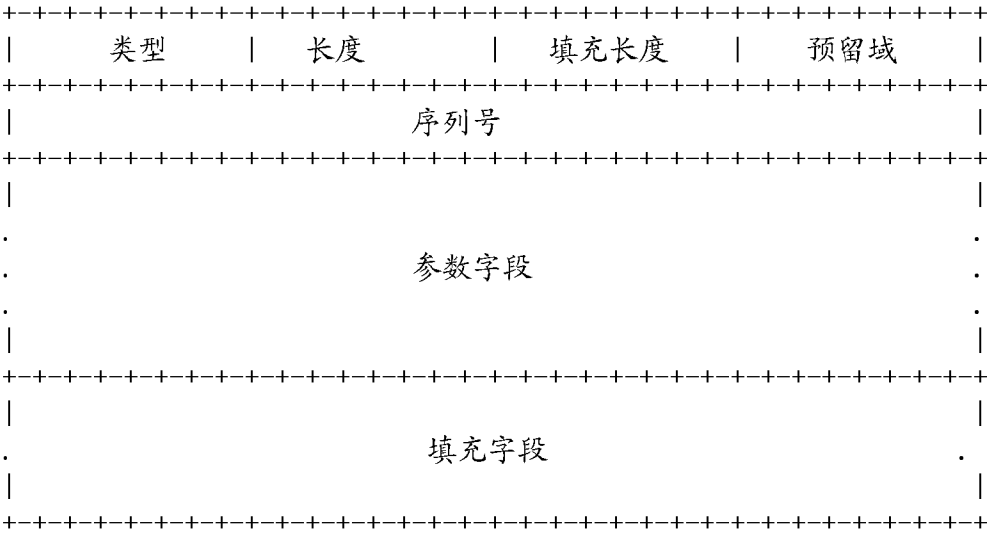

图 6

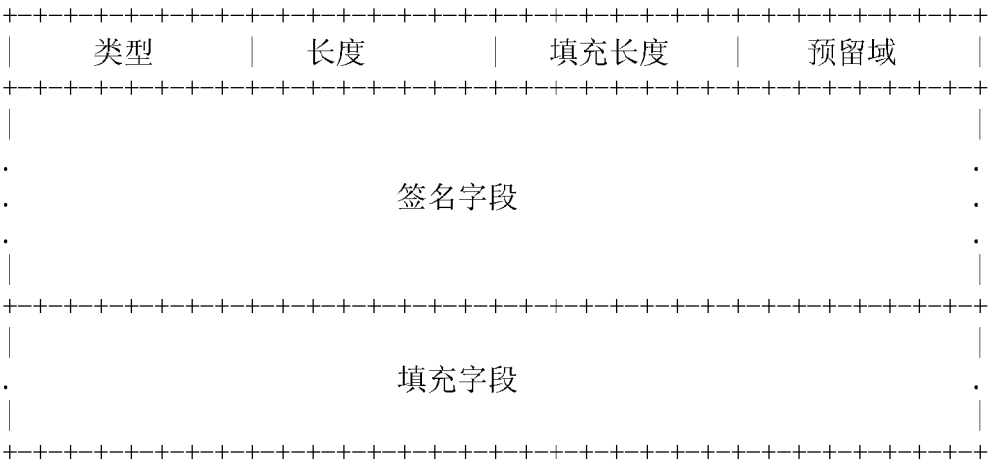

图 7

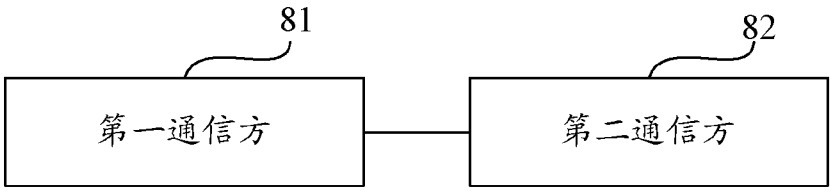
81
82
第一通信方
第二通信方

图 8

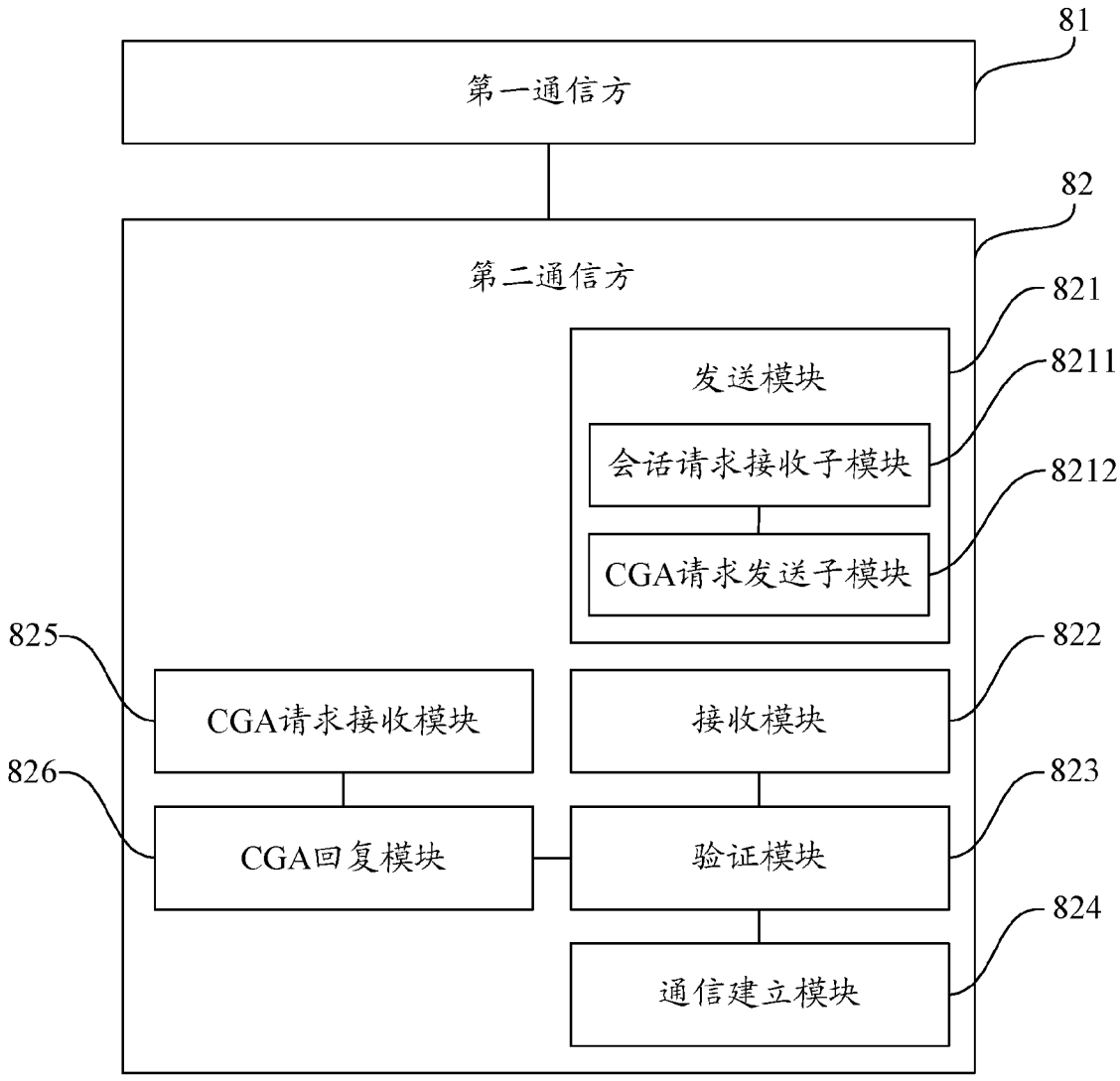
81
第一通信方
82
第二通信方
821
发送模块
8211
会话请求接收子模块
8212
CGA请求发送子模块
825
CGA请求接收模块
822
接收模块
826
CGA回复模块
823
验证模块
824
通信建立模块

图 9

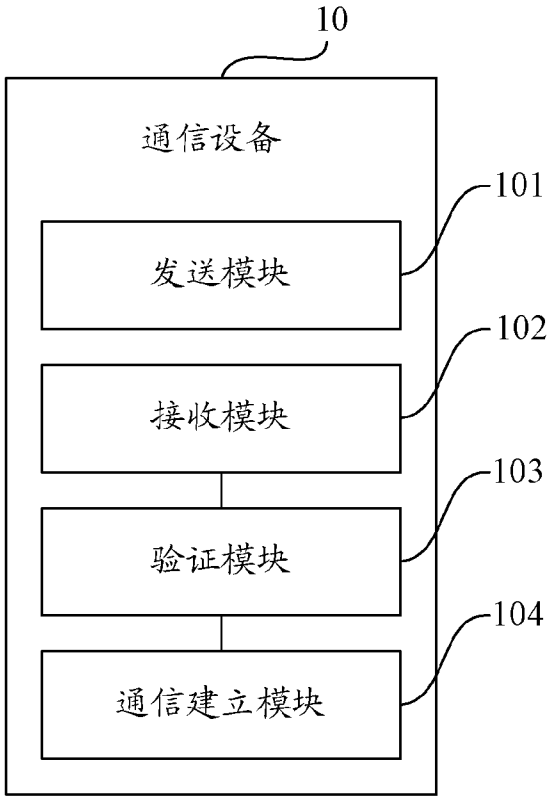

图 10

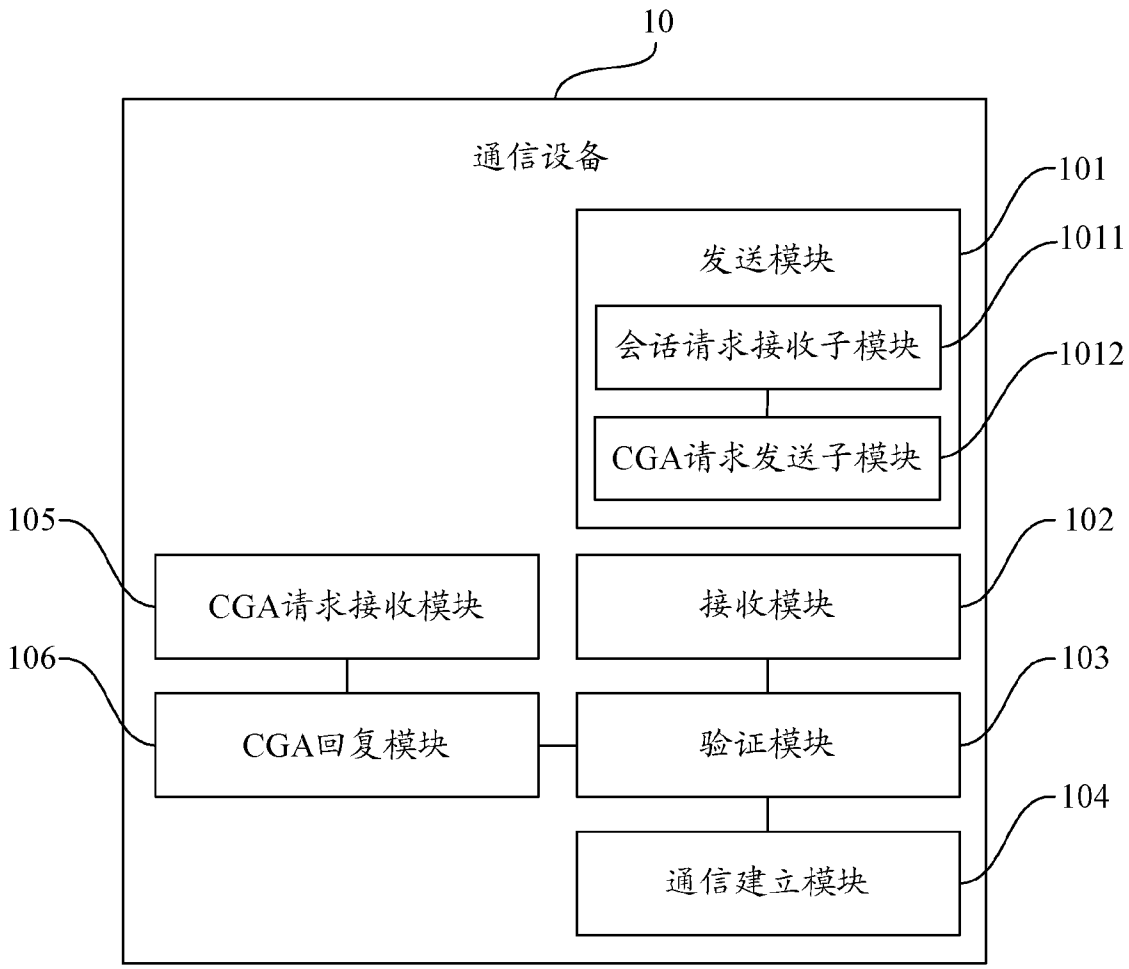
10
通信设备
101
发送模块
1011
会话请求接收子模块
1012
CGA请求发送子模块
105
CGA请求接收模块
102
接收模块
106
CGA回复模块
103
验证模块
104
通信建立模块

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/072156

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32 (2006.01)i

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: H04L9/-, H04L12/-, H04L29/-

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, INSPEC, PATENT SEARCH SYSTEM: CGA, SYN, ACK, DDOS, CRYPT+ W GENERAT+ W ADDRESS, ATTACK+, DENIAL 2W SERVICE, ADDRESS 2D (CHEAT+ OR SPOOF+), FLOOD+, REQUEST+, ACKNOWLEDGE, CERTIFIC+, AUTHOR+, AUTHENTIC+, VERIF+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN1505308A (INT BUSINESS MACHINES CORP.) 16 Jun. 2004 (16.06.2004) See description page 12 line 8-page 14 line 15, figure 4	1-10
Y	CN101106568A (HUAWEI TECHNOLOGY CO., LTD.) 16 Jan. 2008 (16.01.2008) See description page 11 line 28-page 14 line 3, figure 6	1-10
PX	CN101299668A (HUAWEI TECHNOLOGY CO., LTD.) 05 Nov. 2008 (05.11.2008) See claims 1-12	1-10

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 Aug. 2009(17.08.2009)	**10 Sep. 2009 (10.09.2009)**
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. 86-10-62019451	Authorized officer YAO, Hongying Telephone No. (86-10)62413502

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/072156

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PY	CN101404579A (HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 08 Apr. 2009 (08.04.2009)	1-10
A	CN1921488A (UNIV. TSINGHUA) 28 Feb. 2007 (28.02.2007) See the whole document	1-10
A	US2007/0113075A1 (JO, Manhee et al.) 17 May 2007 (17.05.2007) See the whole document	1-10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/072156

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 11-17
because they relate to subject matter not required to be searched by this Authority, namely:
The subject-matter of claims 11-17 is a transmission frame format, and therefore is mere presentations of information.

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/072156

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1505308A	16.06.2004	US2004111635A1	10.06.2004
CN101106568A	16.01.2008	WO2009012676A1	29.01.2009
CN101299668A	05.11.2008	None	
CN101404579A	08.04.2009	None	
CN1921488A	28.02.2007	None	
US2007/0113075A1	17.05.2007	WO2007059419A2	24.05.2007
		JP2009516435T	16.04.2009

国际检索报告

国际申请号
PCT/CN2009/072156

A. 主题的分类

H04L9/32 (2006.01)i

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: H04L9/-, H04L12/-, H04L29/-

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, INSPEC, 专利检索系统：加密地址生成，攻击，冒充，伪造，欺骗，洪水，泛洪，拒绝服务，半连接，同步，应答，回应，验证，CGA，SYN，ACK，DDOS，CRYPT+ W GENERAT+ W ADDRESS, ATTACK+, DENIAL 2W SERVICE, ADDRESS 2D (CHEAT+ OR SPOOF+), FLOOD+, REQUEST+, ACKNOWLEDGE, CERTIFIC+, AUTHOR+, AUTHENTIC+, VERIF+

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
Y	CN1505308A (国际商业机器公司) 16.6 月 2004 (16.06.2004) 参见说明书第 12 页第 8 行-第 14 页第 15 行，附图 4	1-10
Y	CN101106568A (华为技术有限公司) 16.1 月 2008 (16.01.2008) 参见说明书第 11 页第 28 行-第 14 页第 3 行，附图 6	1-10
PX	CN101299668A (华为技术有限公司) 05.11 月 2008 (05.11.2008) 参见权利要求 1-12	1-10
PY	CN101404579A (成都华为赛门铁克科技有限公司) 08.4 月 2009 (08.04.2009) 参见说明书第 9 页第 4-26 行，附图 5	1-10
A	CN1921488A (清华大学) 28.2 月 2007 (28.02.2007) 参见全文	1-10
A	US2007/0113075A1 (JO, Manhee 等) 17.5 月 2007 (17.05.2007) 参见全文	1-10

☐ 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	国际检索报告邮寄日期
17.8 月 2009(17.08.2009)	**10.9 月 2009 (10.09.2009)**
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 姚宏颖 电话号码：(86-10) **62413502**

国际检索报告

国际申请号
PCT/CN2009/072156

第II栏　关于某些权利要求不能作为检索主题的意见(接第 1 页第 2 项)

按条约 17(2)(a)对某些权利要求未作国际检索报告的理由如下：

1. ☒ 权利要求：11-17

因为它们涉及到不要求本国际检索单位进行检索的主题，即：
权利要求 11-17 的主题是传输帧格式，属于单纯的信息表达。

2. ☐ 权利要求：

因为它们涉及到国际申请中不符合规定的要求的部分，以致不能进行任何有意义的国际检索，
具体地说：

3. ☐ 权利要求：

因为它们是从属权利要求，并且没有按照细则 6.4(a)第 2 句和第 3 句的要求撰写。

第III栏　关于缺乏发明单一性时的意见(接第 1 页第 3 项)

本国际检索单位在该国际申请中发现多项发明，即：

1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告针对全部可作检索的权利要求。

2. ☐ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本国际检索单位未通知缴纳任何附加费。

3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求。
具体地说，是权利要求：

4. ☐ 申请人未按时缴纳被要求的附加检索费。因此，本国际检索报告仅涉及权利要求中首次提及的发明；
包含该发明的权利要求是：

关于异议的说明： ☐ 申请人缴纳了附加检索费，同时提交了异议书，缴纳了异议费。

☐ 申请人缴纳了附加检索费，同时提交了异议书，但未缴纳异议费。

☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2009/072156

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1505308A	16.06.2004	US2004111635A1	10.06.2004
CN101106568A	16.01.2008	WO2009012676A1	29.01.2009
CN101299668A	05.11.2008	无	
CN101404579A	08.04.2009	无	
CN1921488A	28.02.2007	无	
US2007/0113075A1	17.05.2007	WO2007059419A2	24.05.2007
		JP2009516435T	16.04.2009