

(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
2017 年 5 月 18 日 (18.05.2017)



(10) 国际公布号
WO 2017/080488 A1

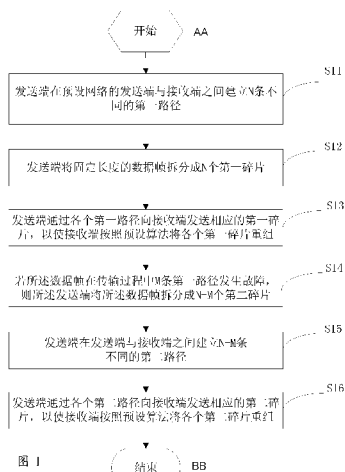
- (51) 国际专利分类号:
H04L 9/08 (2006.01) H04L 12/24 (2006.01)
- (21) 国际申请号: PCT/CN2016/105322
- (22) 国际申请日: 2016 年 11 月 10 日 (10.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510770033.9 2015 年 11 月 12 日 (12.11.2015) CN
- (71) 申请人: 苏州大学张家港工业技术研究院
(ZHANGJIAGANG INSTITUTE OF INDUSTRIAL
TECHNOLOGIES, SOOCHOW UNIVERSITY)
[CN/CN]; 中国江苏省苏州市张家港市市长泾路 10 号,
Jiangsu 215600 (CN)。
- (72) 发明人: 沈纲祥 (SHEN, Gangxiang); 中国江苏省苏
州市张家港市市长泾路 10 号, Jiangsu 215600 (CN)。
李龙飞 (LI, Longfei); 中国江苏省苏州市张家港市
市长泾路 10 号, Jiangsu 215600 (CN)。 江昊岷 (JI-
ANG, Haoming); 中国江苏省苏州市张家港市市长泾
路 10 号, Jiangsu 215600 (CN)。

- (74) 代理人: 北京集佳知识产权代理有限公司
(UNITALEN 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)。
- (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,
CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR,
IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR,
LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH,
PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,
SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA,
RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,
BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, 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,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: DATA TRANSMISSION METHOD AND DEVICE

(54) 发明名称: 一种数据传输方法及装置



S11 A SENDING END ESTABLISHES N DIFFERENT FIRST PATHS BETWEEN THE SENDING END AND A RECEIVING END OF A PRESET NETWORK
S12 THE SENDING END DIVIDES A FIXED-LENGTH DATA FRAME INTO N FIRST FRAGMENTS
S13 THE SENDING END SENDS CORRESPONDING FIRST FRAGMENTS TO THE RECEIVING END THROUGH EACH FIRST PATH, THEREBY ENABLING THE RECEIVING END TO REGROUP ALL THE FIRST FRAGMENTS ACCORDING TO A PRESET ALGORITHM
S14 IF M FIRST PATHS ARE IN FAILURE DURING A TRANSMISSION PROCESS OF THE DATA FRAME, THE SENDING END DIVIDES THE DATA FRAME INTO N-M SECOND FRAGMENTS
S15 THE SENDING END ESTABLISHES N-M DIFFERENT SECOND PATHS BETWEEN THE SENDING END AND THE RECEIVING END
S16 THE SENDING END SENDS CORRESPONDING SECOND FRAGMENTS TO THE RECEIVING END THROUGH EACH SECOND PATH, THEREBY ENABLING THE RECEIVING END TO REGROUP ALL THE SECOND FRAGMENTS ACCORDING TO THE PRESET ALGORITHM
AA START
BB END

(57) Abstract: The present application provides a data transmission method and device. The data transmission method comprises: a sending end establishes N different first paths between the sending end and a receiving end of a preset network; the sending end divides a fixed-length data frame into N first fragments; the sending end sends corresponding first fragments to the receiving end through each first path; if M first paths are in failure during a transmission process of the data frame, the sending end divides the data frame into N-M second fragments; the sending end establishes N-M different second paths between the sending end and the receiving end; and the sending end sends corresponding second fragments to the receiving end through each second path. The present application is capable of enabling a military communication network to have the abilities of secret communication and network self-healing at the same time, and is beneficial for constructing an ultra-strong military communication network.

(57) 摘要: 本申请提供了一种数据传输方法及装置, 数据传输方法包括: 发送端在预设网络的发送端与接收端之间建立 N 条不同的第一路径; 所述发送端将固定长度的数据帧拆分成 N 个第一碎片; 所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片; 若所述数据帧在传输过程中 M 条第一路径发生故障, 则所述发送端将所述数据帧拆分成 N-M 个第二碎片; 所述发送端在所述发送端与所述接收端之间建立 N-M 条不同的第二路径; 所述发送

端通过各个所述第二路径向所述接收端发送相应的第二碎片。本申请能够使军事通信网络同时兼顾保密通信和网络自愈能力, 有利于构建超强军事通信网络。



WO 2017/080488 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种数据传输方法及装置

本申请要求于 2015 年 11 月 12 日提交中国专利局、申请号为 201510770033.9、发明名称为“一种数据传输方法及装置”的中国专利申请的优先权，其全部内容引用在本申请中。

5

技术领域

本申请涉及网络领域，特别涉及一种数据传输方法及装置。

背景技术

10 随着信息时代的急速到来，军事通信网络也逐步成为了军事活动中不可或缺的内容，其中，保密通信和网络自愈能力是构建超强军事通信网络的两大要素。

目前，军事通信网络采用的保密通信方法为应用层保密通信技术，因为应用层保密通信技术相对较为成熟，在没有掌握加密、解密钥匙及采用算法的情况下难以破解。

15 另一方面，网络自愈能力指的是，在网络遇到故障或袭击而导致一条或多条网络链路同时断裂的情况下，点与点之间的通信能很快地恢复自愈，几乎不受影响。针对军事应用，网络自愈能力要求更高，具体体现为需要自愈的网络故障数更多，范围更广，如同时三故障、区域性故障等。

20 然而，在已有的关于保密通信和网络自愈的研究中，两者往往是被割裂，独立研究，导致军事通信网络不能兼顾保密通信和网络自愈能力，不利于构建超强军事通信网络。

发明内容

25 为解决上述技术问题，本申请实施例提供一种数据传输方法及装置，以达到使军事通信网络同时兼顾保密通信和网络自愈能力，有利于构建超强军事通信网络的目的，技术方案如下：

一种数据传输方法，包括：

发送端在预设网络的发送端与接收端之间建立 N 条不同的第一路径, 所述 N 为大于 1 的整数;

所述发送端将固定长度的数据帧拆分成 N 个第一碎片, 每个第一碎片各自对应一条所述第一路径, 各个第一碎片对应的第一路径各不相同, 第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$, 所述 L 为所述数据帧的长度, 所述 $P(i)$ 为预设密钥按照预设算法生成的随机数, 所述 $P(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^N P(i) = 1$;

所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片, 以使所述接收端按照所述预设算法将各个第一碎片重组;

若所述数据帧在传输过程中 M 条第一路径发生故障, 则所述发送端将所述数据帧拆分成 $N-M$ 个第二碎片, 所述 M 为不小于 1 且不大于 $N-1$ 的整数, 第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$, 所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P'(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M} P'(i) = 1$;

所述发送端在所述发送端与所述接收端之间建立 $N-M$ 条不同的第二路径, 每个第二碎片各自对应一条所述第二路径, 各个第二碎片对应的第二路径各不相同;

所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片, 以使所述接收端按照所述预设算法将各个第二碎片重组。

优选的, 所述 $P(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数;

和/或, 所述 $P'(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数。

优选的, 在所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片之后, 还包括:

若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险, 则所述发送端将所述数据帧拆分成 $N-J$ 个第三碎片, 所述 J 为不小于 1 且不大于 $N-1$ 的整数, 第 i 个第三碎片的长度为 $L * P''(i) / \sum_{i=1}^{N-J} P''(i)$, 所述 $P''(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P''(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-J} P''(i) = 1$;

所述发送端通过未发生故障危险的 $N-J$ 条第一路径向所述接收端发送相应的第三碎片。

优选的, 在所述发送端通过各个所述第二路径向所述接收端发送相应的第

二碎片之后,还包括:

若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险,则所述发送端将所述数据帧拆分成 $N-M-H$ 个第四碎片,所述 H 为不小于 1 且不大于 $N-M$ 的整数,第 i 个第四碎片的长度为 $L * P_1''(i) / \sum_{i=1}^{N-M-H} P_1''(i)$,所述 $P_1''(i)$ 为所述

5 预设密钥按照所述预设算法生成的随机数,所述 $P_1''(i)$ 大于 0 且小于 1,所述

$$\sum_{i=1}^{N-M-H} P_1''(i) = 1;$$

所述发送端通过未发生故障危险的 $N-M-H$ 条第二路径向所述接收端发送相应的第四碎片。

一种数据传输装置,包括:

10 第一建立单元,用于在预设网络的发送端与接收端之间建立 N 条不同的第一路径,所述 N 为大于 1 的整数;

第一拆分单元,用于将固定长度的数据帧拆分成 N 个第一碎片,每个第一碎片各自对应一条所述第一路径,各个第一碎片对应的第一路径各不相同,第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$,所述 L 为所述数据帧的长度,所述 $P(i)$

15 为预设密钥按照预设算法生成的随机数,所述 $P(i)$ 大于 0 且小于 1,所述

$$\sum_{i=1}^N P(i) = 1;$$

第一发送单元,用于通过各个所述第一路径向所述接收端发送相应的第一碎片,以使所述接收端按照所述预设算法将各个第一碎片重组;

第二拆分单元,用于若所述数据帧在传输过程中 M 条第一路径发生故障,

20 则所述发送端将所述数据帧拆分成 $N-M$ 个第二碎片,所述 M 为不小于 1 且不大于 $N-1$ 的整数,第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$,所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数,所述 $P'(i)$ 大于 0 且小于 1,所述

$$\sum_{i=1}^{N-M} P'(i) = 1;$$

第二建立单元,用于在所述发送端与所述接收端之间建立 $N-M$ 条不同的

25 第二路径,每个第二碎片各自对应一条所述第二路径,各个第二碎片对应的第二路径各不相同;

第二发送单元,用于通过各个所述第二路径向所述接收端发送相应的第二碎片,以使所述接收端按照所述预设算法将各个第二碎片重组。

优选的,还包括:

30 第三拆分单元,用于在所述第一发送单元通过各个所述第一路径向所述接

收端发送相应的第一碎片之后,若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险,则所述发送端将所述数据帧拆分成 N-J 个第三碎片,所述 J 为不小于 1 且不大于 N-1 的整数,第 i 个第三碎片的长度为 $L * P''(i) / \sum_{i=1}^{N-J} P''(i)$, 所述 $P''(i)$ 为所述预设密钥按照所述预设算法生成的随机数,所述 $P''(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-J} P''(i) = 1$;

第三发送单元,用于通过未发生故障危险的 N-J 条第一路径向所述接收端发送相应的第三碎片。

优选的,还包括:

第四拆分单元,用于在所述第二发送单元通过各个所述第二路径向所述接收端发送相应的第二碎片之后,若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险,则所述发送端将所述数据帧拆分成 N-M-H 个第四碎片,所述 H 为不小于 1 且不大于 N-M 的整数,第 i 个第四碎片的长度为 $L * P_1''(i) / \sum_{i=1}^{N-M-H} P_1''(i)$, 所述 $P_1''(i)$ 为所述预设密钥按照所述预设算法生成的随机数,所述 $P_1''(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M-H} P_1''(i) = 1$;

第四发送单元,用于通过未发生故障危险的 N-M-H 条第二路径向所述接收端发送相应的第四碎片。

与现有技术相比,本申请的有益效果为:

在本申请中,发送端将固定长度的数据帧拆分成 N 个第一碎片进行传输,其中第 i 个碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$, $P(i)$ 为预设密钥按照预设算法生成的随机数,接收端按照与发送端相同的预设算法将各个碎片重组,实现了数据的保密传输。

若数据帧在保密传输过程中 M 条第一路径发生故障,则发送端重新将所述数据帧拆分成 N-M 个第二碎片,通过建立的 N-M 条第二路径向接收端发送各个第二碎片,其中第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$, 所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数,恢复数据的保密传输,实现了网络的自愈。

可见,本申请能够使军事通信网络同时兼顾保密通信和网络自愈能力,有利于构建超强军事通信网络。

附图说明

为了更清楚地说明本申请实施例中的技术方案，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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

- 5 图 1 是本申请提供的数据传输方法的一种流程图；
图 2 是本申请提供的数据传输方法的另一种流程图；
图 3 是本申请提供的数据传输方法的再一种流程图；
图 4 是本申请提供的数据传输装置的一种逻辑结构示意图。

具体实施方式

- 10 下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

15 实施例一

请参见图 1，其示出了本申请提供的数据传输方法的一种流程图，可以包括以下步骤：

步骤 S11：发送端在预设网络的发送端与接收端之间建立 N 条不同的第一路径。

- 20 其中，所述 N 为大于 1 的整数。

步骤 S12：所述发送端将固定长度的数据帧拆分成 N 个第一碎片，每个第一碎片各自对应一条所述第一路径，各个第一碎片对应的第一路径各不相同。

- 25 在本实施例中，第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$ ，所述 L 为所述数据帧的长度，所述 $P(i)$ 为预设密钥按照预设算法生成的随机数，所述 $P(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^N P(i) = 1$ 。

在本实施例中，并不对预设密钥和预设算法进行限定，只要适用应用层加密均可。

步骤 S13: 所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片, 以使所述接收端按照所述预设算法将各个第一碎片重组。

步骤 S11 至步骤 S13 通过建立 N 条不同的第一路径, 将数据帧拆分成 N 个第一碎片, 并通过各个第一路径向接收端发送相应的第一碎片, 实现了数据
5 帧的多路径保密传输。

步骤 S14: 若所述数据帧在传输过程中 M 条第一路径发生故障, 则所述发送端将所述数据帧拆分成 N-M 个第二碎片。

在本实施例中, 所述 M 为不小于 1 且不大于 N-1 的整数, 第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$, 所述 $P'(i)$ 为所述预设密钥按照所述预设算法生
10 成的随机数, 所述 $P'(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M} P'(i) = 1$

步骤 S15: 所述发送端在所述发送端与所述接收端之间建立 N-M 条不同的第二路径。

其中, 每个第二碎片各自对应一条所述第二路径, 各个第二碎片对应的第二路径各不相同。

15 步骤 S16: 所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片, 以使所述接收端按照所述预设算法将各个第二碎片重组。

在本实施例中, 在 M 不大于 N-2 时, 同样能够实现数据帧的多路径保密传输。

在本实施例中, 由于 M 最大取值为 N-1, 因此在 N-1 条第一路径发生故障时, 发送端仍能通过剩余的一条路径继续向接收端发送数据, 具有很强的网络自愈能力, 即使网络大面积受损, 只要两点相同, 就可以保证正常保密通信。
20 但是在 M 取值为 N-1 时, 数据帧将通过唯一的一条路径进行保密传输, 失去了多路径保密通信方式, 相比于多路径保密通信传输, 数据将会很容易被全部窃取。

25 在本实施例中, 若在数据帧传输过程中, 预设密钥受击失效时, 预设密钥虽然不能再按照预设算法产生随机数, 但是由于发送端和接收端均采用相同的预设算法, 因此发送端和接收端仍能按照原有预设算法继续工作, 具有很强的鲁棒性和保密性。

在本申请中，发送端将固定长度的数据帧拆分成N个第一碎片进行传输，其中第i个碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$ ， $P(i)$ 为预设密钥按照预设算法生成的随机数，接收端按照与发送端相同的预设算法将各个碎片重组，实现了数据的保密传输。

5 若数据帧在保密传输过程中M条第一路径发生故障，则发送端重新将所述数据帧拆分成N-M个第二碎片，通过建立的N-M条第二路径向接收端发送各个第二碎片，其中第i个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$ ，所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数，恢复数据的保密传输，实现了网络的自愈。

10 可见，本申请能够使军事通信网络同时兼顾保密通信和网络自愈能力，有利于构建超强军事通信网络。

进一步的，由于将数据帧拆分成多个碎片，在多个路径上传输，因此窃听破解信息需要在不同地理位置同时获取所有数据，多点切入，导致窃听破解困难，增强了军事通信网络的保密性。

15 在本实施例中，需要说明的是，步骤S12中的 $P(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数；

和/或，步骤S14中的 $P'(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数。

20 其中， $P(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数指的是，预设密钥可以在不同时间点采用不同的预设算法生成随机数，时间点的不同由预设密钥确定。

其中， $P'(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数指的是，预设密钥可以在不同时间点采用不同的预设算法生成随机数，时间点的不同由预设密钥确定。

25 在 $P(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数时，在数据传输过程中，不再一直采用同一种预设算法，而是随着时间的改变采用不同的预设算法，进一步增强了网络的保密性。

和在 $P'(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随

机数时,在数据传输过程中,不再一直采用同一种预设算法,而是随着时间的改变采用不同的预设算法,进一步增强了网络的保密性。

实施例二

5 在本实施例中,在图 1 示出的数据传输方法的基础上扩展出另外一种数据传输方法,请参见图 2,可以包括以下步骤:

步骤 S21:发送端在预设网络的发送端与接收端之间建立 N 条不同的第一路径。

其中,所述 N 为大于 1 的整数。

10 步骤 S22:所述发送端将固定长度的数据帧拆分成 N 个第一碎片,每个第一碎片各自对应一条所述第一路径,各个第一碎片对应的第一路径各不相同。

在本实施例中,第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$,所述 L 为所述数据帧的长度,所述 $P(i)$ 为预设密钥按照预设算法生成的随机数,所述 $P(i)$ 大于 0 且小于 1,所述 $\sum_{i=1}^N P(i) = 1$ 。

15 步骤 S23:所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片,以使所述接收端按照所述预设算法将各个第一碎片重组。

步骤 S24:若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险,则所述发送端将所述数据帧拆分成 N-J 个第三碎片。

20 所述 J 为不小于 1 且不大于 N-1 的整数,第 i 个第三碎片的长度为 $L * P''(i) / \sum_{i=1}^{N-J} P''(i)$,所述 $P''(i)$ 为所述预设密钥按照所述预设算法生成的随机数,所述 $P''(i)$ 大于 0 且小于 1,所述 $\sum_{i=1}^{N-J} P''(i) = 1$ 。

在本实施例中,在所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片之后,若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险,则所述发送端将所述数据帧拆分成 N-J 个第三碎片。

25 在 J 条第一路径存在发生故障的危险时,选择剩余的第一路径重新传输数据,避免高危区域,增强了网络的保密性。

步骤 S25:所述发送端通过未发生故障危险的 N-J 条第一路径向所述接收端发送相应的第三碎片。

步骤 S26: 若所述数据帧在传输过程中 M 条第一路径发生故障, 则所述发送端将所述数据帧拆分成 N-M 个第二碎片。

在本实施例中, 所述 M 为不小于 1 且不大于 N-1 的整数, 第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$, 所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P'(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M} P'(i) = 1$

步骤 S27: 所述发送端在所述发送端与所述接收端之间建立 N-M 条不同的第二路径。

其中, 每个第二碎片各自对应一条所述第二路径, 各个第二碎片对应的第二路径各不相同。

步骤 S28: 所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片, 以使所述接收端按照所述预设算法将各个第二碎片重组。

实施例二

在本实施例中, 在图 1 示出的数据传输方法的基础上扩展出另外一种数据传输方法, 请参见图 3, 可以包括以下步骤:

步骤 S31: 发送端在预设网络的发送端与接收端之间建立 N 条不同的第一路径。

其中, 所述 N 为大于 1 的整数。

步骤 S32: 所述发送端将固定长度的数据帧拆分成 N 个第一碎片, 每个第一碎片各自对应一条所述第一路径, 各个第一碎片对应的第一路径各不相同。

在本实施例中, 第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$, 所述 L 为所述数据帧的长度, 所述 $P(i)$ 为预设密钥按照预设算法生成的随机数, 所述 $P(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^N P(i) = 1$ 。

步骤 S33: 所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片, 以使所述接收端按照所述预设算法将各个第一碎片重组。

步骤 S34: 若所述数据帧在传输过程中 M 条第一路径发生故障, 则所述发送端将所述数据帧拆分成 N-M 个第二碎片。

在本实施例中, 所述 M 为不小于 1 且不大于 $N-1$ 的整数, 第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$, 所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P'(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M} P'(i) = 1$

5 步骤 S35: 所述发送端在所述发送端与所述接收端之间建立 $N-M$ 条不同的第二路径。

其中, 每个第二碎片各自对应一条所述第二路径, 各个第二碎片对应的第二路径各不相同。

步骤 S36: 所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片, 以使所述接收端按照所述预设算法将各个第二碎片重组。

10 步骤 S37: 若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险, 则所述发送端将所述数据帧拆分成 $N-M-H$ 个第四碎片。

所述 H 为不小于 1 且不大于 $N-M$ 的整数, 第 i 个第四碎片的长度为 $L * P_1''(i) / \sum_{i=1}^{N-M-H} P_1''(i)$, 所述 $P_1''(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P_1''(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M-H} P_1''(i) = 1$

15 在本实施例中, 在所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片之后, 若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险, 则所述发送端将所述数据帧拆分成 $N-M-H$ 个第四碎片。

在 H 条第二路径存在发生故障的危险时, 选择剩余的第二路径重新传输数据, 避免高危区域, 增强了网络的保密性。

20 步骤 S38: 所述发送端通过未发生故障危险的 $N-M-H$ 条第二路径向所述接收端发送相应的第四碎片。

实施例四

25 与图 1 示出的数据传输方法相对应, 本实施例提供了数据传输装置的一种逻辑结构示意图, 请参见图 4, 数据传输装置包括: 第一建立单元 41、第一拆分单元 42、第一发送单元 43、第二拆分单元 44、第二建立单元 45 和第二发送单元 46。

第一建立单元 41, 用于在预设网络的发送端与接收端之间建立 N 条不同

的第一路径。

所述 N 为大于 1 的整数。

第一拆分单元 42, 用于将固定长度的数据帧拆分成 N 个第一碎片, 每个第一碎片各自对应一条所述第一路径, 各个第一碎片对应的第一路径各不相同, 第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$, 所述 L 为所述数据帧的长度, 所述 $P(i)$ 为预设密钥按照预设算法生成的随机数, 所述 $P(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^N P(i) = 1$ 。

第一发送单元 43, 用于通过各个所述第一路径向所述接收端发送相应的第一碎片, 以使所述接收端按照所述预设算法将各个第一碎片重组。

10 第二拆分单元 44, 用于若所述数据帧在传输过程中 M 条第一路径发生故障, 则所述发送端将所述数据帧拆分成 N-M 个第二碎片, 所述 M 为不小于 1 且不大于 N-1 的整数, 第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$, 所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P'(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-M} P'(i) = 1$ 。

15 第二建立单元 45, 用于在所述发送端与所述接收端之间建立 N-M 条不同的第二路径, 每个第二碎片各自对应一条所述第二路径, 各个第二碎片对应的第二路径各不相同。

第二发送单元 46, 用于通过各个所述第二路径向所述接收端发送相应的第二碎片, 以使所述接收端按照所述预设算法将各个第二碎片重组。

20 在本实施例中, 图 4 示出的数据传输装置还可以包括: 第三拆分单元和第三发送单元。

第三拆分单元, 用于在所述第一发送单元通过各个所述第一路径向所述接收端发送相应的第一碎片之后, 若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险, 则所述发送端将所述数据帧拆分成 N-J 个第三碎片, 所述 J 为不小于 1 且不大于 N-1 的整数, 第 i 个第三碎片的长度为 $L * P''(i) / \sum_{i=1}^{N-J} P''(i)$, 所述 $P''(i)$ 为所述预设密钥按照所述预设算法生成的随机数, 所述 $P''(i)$ 大于 0 且小于 1, 所述 $\sum_{i=1}^{N-J} P''(i) = 1$ 。

第三发送单元, 用于通过未发生故障危险的 N-J 条第一路径向所述接收端发送相应的第三碎片。

在本实施例中，图 4 示出的数据传输装置还可以包括：第四拆分单元和第四发送单元。

5 第四拆分单元，用于在所述第二发送单元通过各个所述第二路径向所述接收端发送相应的第二碎片之后，若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险，则所述发送端将所述数据帧拆分成 N-M-H 个第四碎片，所述 H 为不小于 1 且不大于 N-M 的整数，第 i 个第四碎片的长度为 $L * P_1''(i) / \sum_{i=1}^{N-M-H} P_1''(i)$ ，所述 $P_1''(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P_1''(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-M-H} P_1''(i) = 1$ 。

10 第四发送单元，用于通过未发生故障危险的 N-M-H 条第二路径向所述接收端发送相应的第四碎片。

15 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

20 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

25 以上对本申请所提供的一种数据传输方法及装置进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求

1、一种数据传输方法，其特征在于，包括：

发送端在预设网络的发送端与接收端之间建立 N 条不同的第一路径，所述 N 为大于 1 的整数；

5 所述发送端将固定长度的数据帧拆分成 N 个第一碎片，每个第一碎片各自对应一条所述第一路径，各个第一碎片对应的第一路径各不相同，第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$ ，所述 L 为所述数据帧的长度，所述 $P(i)$ 为预设密钥按照预设算法生成的随机数，所述 $P(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^N P(i) = 1$ ；

10 所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片，以使所述接收端按照所述预设算法将各个第一碎片重组；

若所述数据帧在传输过程中 M 条第一路径发生故障，则所述发送端将所述数据帧拆分成 $N-M$ 个第二碎片，所述 M 为不小于 1 且不大于 $N-1$ 的整数，第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$ ，所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P'(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-M} P'(i) = 1$ ；

15 所述发送端在所述发送端与所述接收端之间建立 $N-M$ 条不同的第二路径，每个第二碎片各自对应一条所述第二路径，各个第二碎片对应的第二路径各不相同；

所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片，以使所述接收端按照所述预设算法将各个第二碎片重组。

20 2、根据权利要求 1 所述的方法，其特征在于，所述 $P(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数；

和/或，所述 $P'(i)$ 具体为所述预设密钥在不同时间点按照不同预设算法生成的随机数。

25 3、根据权利要求 1 所述的方法，其特征在于，在所述发送端通过各个所述第一路径向所述接收端发送相应的第一碎片之后，还包括：

若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险，则所述发送端将所述数据帧拆分成 $N-J$ 个第三碎片，所述 J 为不小于 1 且不大于 $N-1$ 的整数，第 i 个第三碎片的长度为 $L * P''(i) / \sum_{i=1}^{N-J} P''(i)$ ，所述 $P''(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P''(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-J} P''(i) = 1$ ；

30 所述发送端通过未发生故障危险的 $N-J$ 条第一路径向所述接收端发送相

应的第三碎片。

4、根据权利要求 1 所述的方法，其特征在于，在所述发送端通过各个所述第二路径向所述接收端发送相应的第二碎片之后，还包括：

5 若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险，则所述发送端将所述数据帧拆分成 N-M-H 个第四碎片，所述 H 为不小于 1 且不大于 N-M 的整数，第 i 个第四碎片的长度为 $L * P_1''(i) / \sum_{i=1}^{N-M-H} P_1''(i)$ ，所述 $P_1''(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P_1''(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-M-H} P_1''(i) = 1$ ；

10 所述发送端通过未发生故障危险的 N-M-H 条第二路径向所述接收端发送相应的第四碎片。

5、一种数据传输装置，其特征在于，包括：

第一建立单元，用于在预设网络的发送端与接收端之间建立 N 条不同的第一路径，所述 N 为大于 1 的整数；

15 第一拆分单元，用于将固定长度的数据帧拆分成 N 个第一碎片，每个第一碎片各自对应一条所述第一路径，各个第一碎片对应的第一路径各不相同，第 i 个第一碎片的长度为 $L * P(i) / \sum_{i=1}^N P(i)$ ，所述 L 为所述数据帧的长度，所述 $P(i)$ 为预设密钥按照预设算法生成的随机数，所述 $P(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^N P(i) = 1$ ；

20 第一发送单元，用于通过各个所述第一路径向所述接收端发送相应的第一碎片，以使所述接收端按照所述预设算法将各个第一碎片重组；

25 第二拆分单元，用于若所述数据帧在传输过程中 M 条第一路径发生故障，则所述发送端将所述数据帧拆分成 N-M 个第二碎片，所述 M 为不小于 1 且不大于 N-1 的整数，第 i 个第二碎片的长度为 $L * P'(i) / \sum_{i=1}^{N-M} P'(i)$ ，所述 $P'(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P'(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-M} P'(i) = 1$ ；

第二建立单元，用于在所述发送端与所述接收端之间建立 N-M 条不同的第二路径，每个第二碎片各自对应一条所述第二路径，各个第二碎片对应的第二路径各不相同；

30 第二发送单元，用于通过各个所述第二路径向所述接收端发送相应的第二碎片，以使所述接收端按照所述预设算法将各个第二碎片重组。

6、根据权利要求 5 所述的装置，其特征在于，还包括：

第三拆分单元，用于在所述第一发送单元通过各个所述第一路径向所述接收端发送相应的第一碎片之后，若所述数据帧在传输过程中 J 条第一路径存在发生故障的危险，则所述发送端将所述数据帧拆分成 N-J 个第三碎片，所述 J 为不小于 1 且不大于 N-1 的整数，第 i 个第三碎片的长度为 $L * P''(i) / \sum_{i=1}^{N-J} P''(i)$ ，所述 $P''(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P''(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-J} P''(i) = 1$ ；

第三发送单元，用于通过未发生故障危险的 N-J 条第一路径向所述接收端发送相应的第三碎片。

10 7、根据权利要求 5 所述的装置，其特征在于，还包括：

第四拆分单元，用于在所述第二发送单元通过各个所述第二路径向所述接收端发送相应的第二碎片之后，若所述数据帧在传输过程中 H 条第二路径存在发生故障的危险，则所述发送端将所述数据帧拆分成 N-M-H 个第四碎片，所述 H 为不小于 1 且不大于 N-M 的整数，第 i 个第四碎片的长度为 $L * P_1''(i) / \sum_{i=1}^{N-M-H} P_1''(i)$ ，所述 $P_1''(i)$ 为所述预设密钥按照所述预设算法生成的随机数，所述 $P_1''(i)$ 大于 0 且小于 1，所述 $\sum_{i=1}^{N-M-H} P_1''(i) = 1$ ；

第四发送单元，用于通过未发生故障危险的 N-M-H 条第二路径向所述接收端发送相应的第四碎片。

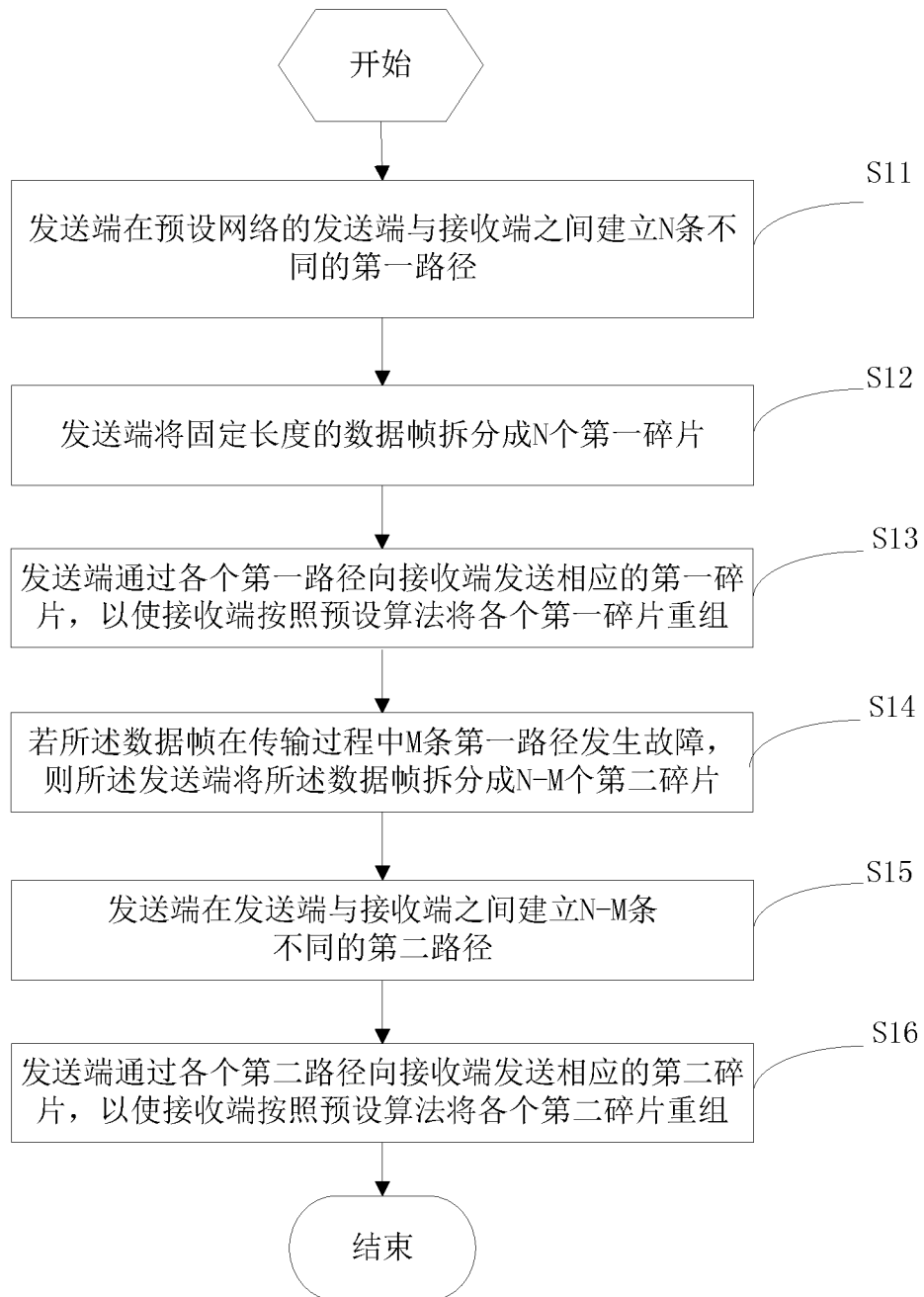


图 1

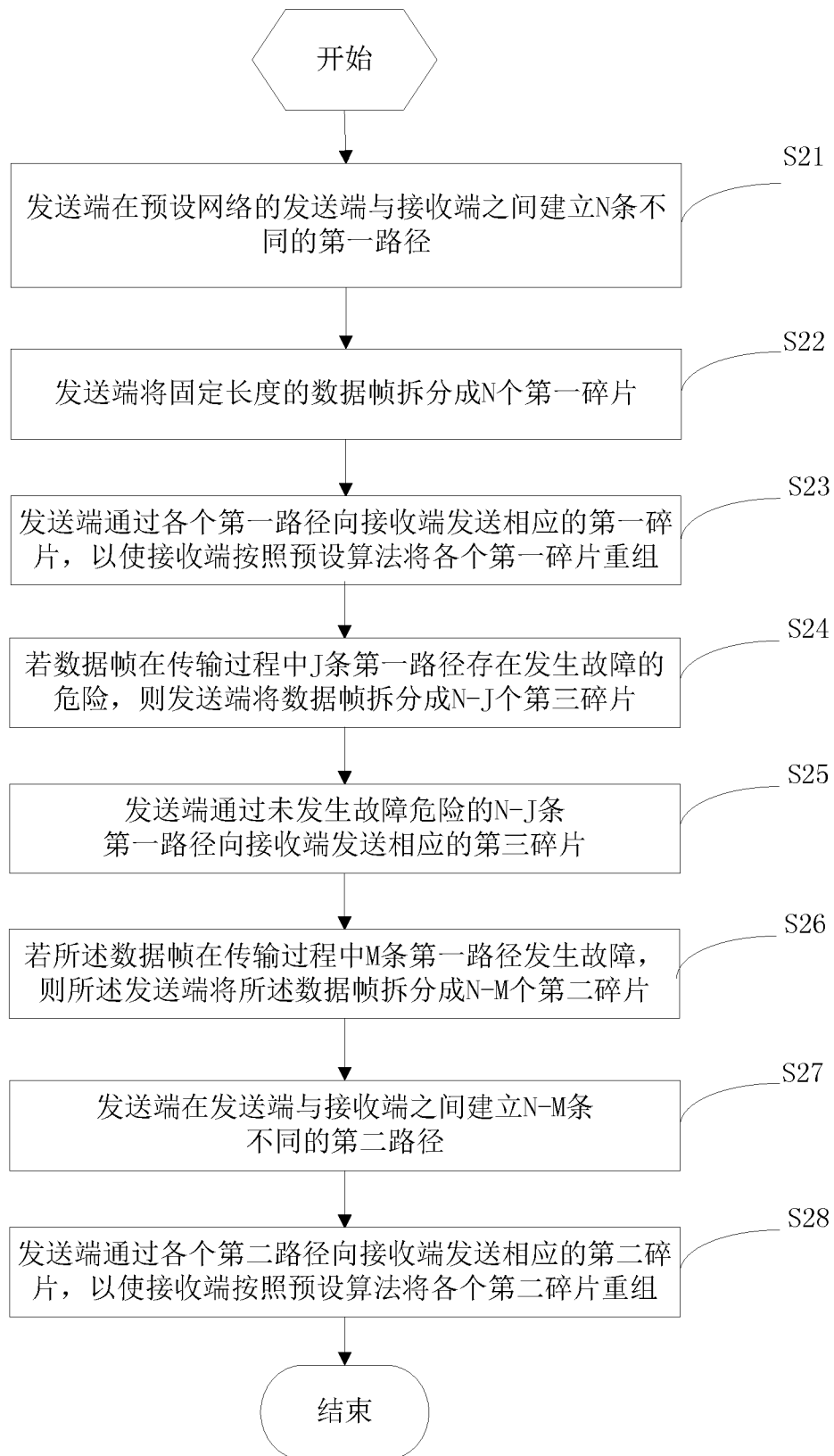


图 2

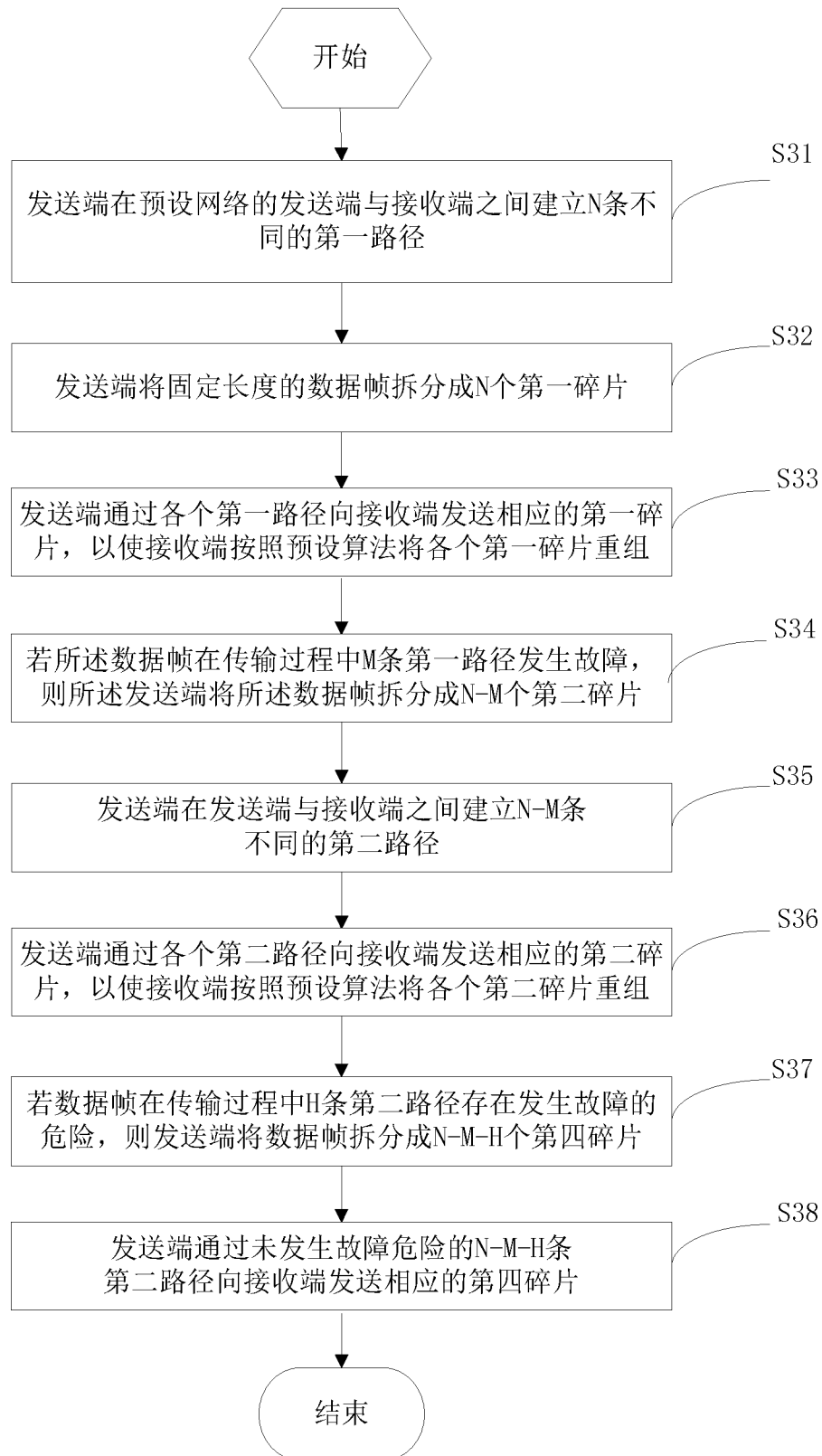


图 3

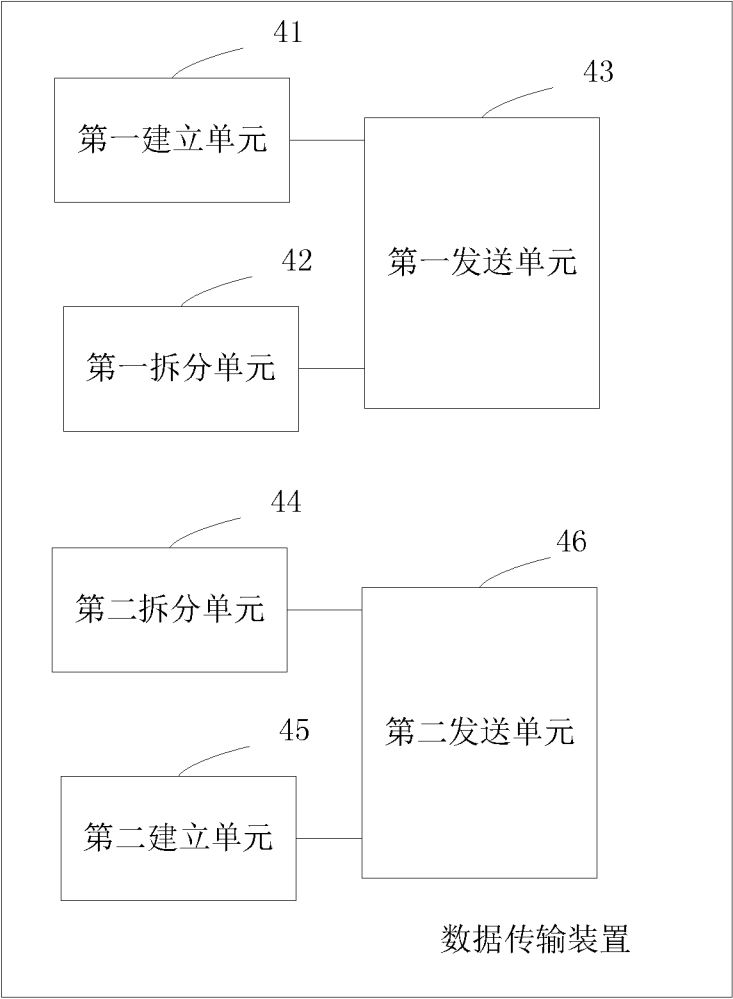


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/105322

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i; H04L 12/24 (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)

H04L

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)

CNKI, CNPAT, WPI, EPODOC: split, slice, recombine, combine, data, message, package, connect, multitape, different, every, succeed, encryption key, random number, size, segment, piece, divide, block, path, link, channel, fault, failure, encrypt, key, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105450390 A (ZHANGJIAGANG INSTITUTE OF INDUSTRIAL TECHNOLOGIES SOOCHOW UNIVERSITY), 30 March 2016 (30.03.2016), claims 1-7, and description, paragraphs [0044]-[0120]	1-7
A	CN 1551509 A (SONY CORPORATION), 01 December 2004 (01.12.2004), description, page 1, last paragraph to page 8, paragraph 1	1-7
A	CN 102882960 A (NEUSOFT CORPORATION), 16 January 2013 (16.01.2013), the whole document	1-7
A	CN 102938730 A (QINGDAO HISENSE TRANSTECH CO., LTD.), 20 February 2013 (20.02.2013), the whole document	1-7
A	CN 101138262 A (FUJITSU LIMITED), 05 March 2008 (05.03.2008), the whole document	1-7
A	WO 2010148866 A1 (ZTE CORP.), 29 December 2010 (29.12.2010), the whole document	1-7

☐ 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 January 2017 (13.01.2017)	Date of mailing of the international search report 26 January 2017 (26.01.2017)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Xiaoli Telephone No.: (86-10) 62414494

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/105322

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105450390 A	30 March 2016	None	
CN 1551509 A	01 December 2004	JP 2004350259 A	09 December 2004
		US 2005002421 A1	06 January 2005
		KR 20040094320 A	09 November 2004
CN 102882960 A	16 January 2013	None	
CN 102938730 A	20 February 2013	None	
CN 101138262 A	05 March 2008	US 2008051123 A1	28 February 2008
		WO 2006095423 A1	14 September 2006
		EP 2528261 A1	28 November 2012
		EP 1860894 A1	28 November 2007
		JP 4733689 B2	27 July 2011
		KR 20070116025 A	06 December 2007
WO 2010148866 A1	29 December 2010	CN 101715209 A	26 May 2010

A. 主题的分类 H04L 9/08(2006.01)i; H04L 12/24(2006.01)i 按照国际专利分类(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) H04L 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)) CNKI, CNPAT, WPI, EPDOC:拆分, 分片, 分割, 划分, 片, 块, 段, 重组, 组合, 数据, 报文, 包, 连接, 路径, 链接, 通道, 链路, 多条, 不同, 每一个, 成功, 失败, 故障, 密钥, 随机数, 大小, 尺寸, segment, piece, divide, block, path, link, channel, fault, failure, encrypt, key, random		
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	CN 105450390 A (苏州大学张家港工业技术研究院) 2016年 3月 30日 (2016 - 03 - 30) 权利要求1-7, 说明书第[0044]-[0120]段	1-7
A	CN 1551509 A (索尼株式会社) 2004年 12月 1日 (2004 - 12 - 01) 说明书第1页最后1段-第8页第1段	1-7
A	CN 102882960 A (东软集团股份有限公司) 2013年 1月 16日 (2013 - 01 - 16) 全文	1-7
A	CN 102938730 A (青岛海信网络科技股份有限公司) 2013年 2月 20日 (2013 - 02 - 20) 全文	1-7
A	CN 101138262 A (富士通株式会社) 2008年 3月 5日 (2008 - 03 - 05) 全文	1-7
A	WO 2010148866 A1 (中兴通讯股份有限公司) 2010年 12月 29日 (2010 - 12 - 29) 全文	1-7
☐ 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(如具体说明的) “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 2017年 1月 13日		国际检索报告邮寄日期 2017年 1月 26日
ISA/CN的名称和邮寄地址 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 李晓利 电话号码 (86-10)62414494

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/105322

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105450390	A	2016年 3月 30日	无			
CN	1551509	A	2004年 12月 1日	JP	2004350259	A	2004年 12月 9日
				US	2005002421	A1	2005年 1月 6日
				KR	20040094320	A	2004年 11月 9日
CN	102882960	A	2013年 1月 16日	无			
CN	102938730	A	2013年 2月 20日	无			
CN	101138262	A	2008年 3月 5日	US	2008051123	A1	2008年 2月 28日
				WO	2006095423	A1	2006年 9月 14日
				EP	2528261	A1	2012年 11月 28日
				EP	1860894	A1	2007年 11月 28日
				JP	4733689	B2	2011年 7月 27日
				KR	20070116025	A	2007年 12月 6日
WO	2010148866	A1	2010年 12月 29日	CN	101715209	A	2010年 5月 26日