文章编号:1671-4598(2018)02-0259-05 DOI:10.16526/j.cnki.11—4762/tp.2018.02.064 中图分类号:TP391 文献标识码:A

无线 Mesh 网络中基于奖励机制的均衡传输方案

何 健
(罗定职业技术学院 电子信息系,广东 罗定 527200)

摘要:无线 Mesh 网络由于自私节点的存在而造成双向流量传输不均衡,为解决这一问题,提出了一种基于奖励机制的均衡传输方案;首先,研究了自私 TAPs 和自私网关在无线 Mesh 网络中如何影响双向流量的均衡传输问题;然后,建立了一套公平参考模型和虚拟信用币,为提出的机制提供理想基准,并推导出了每个传输访问点(TAP)的双向目标吞吐量;最后,提出一种奖励机制,通过信用币和代币支付策略来鼓励闲置 TAP 转发数据,同时使网关尽可能均衡地向 TAP 传输下行数据;该模型是通过转发数据来获得信用币,通过发送局部数据来消耗信用币;在一个具有 3 个 TAP 的无线 Mesh 网络上仿真结果表明,该方法能够在存在自私节点情况下确保双向流量的均衡;实验结果也证明了提出的基于奖励机制的均衡传输方案正确且有效。

关键词:无线 Mesh 网络;双向流量;奖励机制;均衡传输

Application of Balanced Transmission Mechanism Based on Reward in Wireless Mesh Network

He Jian
(Department of Electronic Information, Luoding Polytechnic, Luoding 527200, China)

Abstract: In order to solve this problem, wireless mesh network (WMN) is unbalanced due to the existence of selfish nodes. A balanced transmission scheme based on reward mechanism is proposed. First, we study how the selfish TAPs and selfish gateways affect the balanced transmission of bidirectional traffic in wireless Mesh networks. Then, a set of fair reference models and virtual credits were created, providing an ideal benchmark for the proposed mechanism and deriving the bidirectional target throughput for each Transport Access Point (TAP). Finally, an incentive mechanism is proposed to encourage idle TAPs to forward data through credit and token payment strategies, while enabling gateways to transmit downlink data to TAPs as evenly as possible. The model obtains the credit currency by forwarding the data and consumes the credit currency by sending the partial data. The simulation results on a wireless Mesh network with 3 TAPs show that this method can ensure the bidirectional traffic to be balanced in the presence of selfish nodes. The experimental results also prove that the proposed balanced transmission scheme based on incentive mechanism is correct and effective.

Keywords: wireless mesh network; bidirectional traffic; Incentive mechanism; balanced transmission

0 引言

无线 Mesh 网络即“无线网格网络”,它是多跳(multi—hop)网络,是解决“最后一公里”问题的关键技术之一[1]。在多跳无线 Mesh 网络中,从移动用户到有限网络的流量是经由网关通过多无线传输访问点(Transit Access Points,TAPs)进行处理。然而,在现有 MAC 操作中,对于一些距离网关几跳距离的用户,其可能会遭受较低的吞吐量[2]。甚至会由于多跳中继、流聚合和底层 MAC 层机制而导致吞吐量饥饿情况。为此,需要可以确保无线 Mesh 网络中公平资源共享的解决方案[3]。无线 Mesh 网络系统模型见图 1。

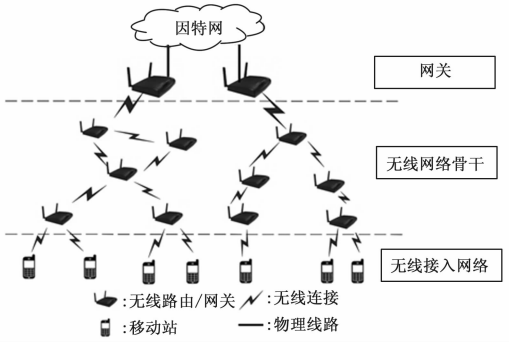

图 1 无线 Mesh 网络系统模型

由于无线 Mesh 网络中的下行流量不能通过逐跳传输进行聚合,因此当前的研究[4-6]集中于上行流量。事实上,下行流量通过扩散方式从网关传输到各个目标 TAP,因此,由流量聚合和 TAP 之间的竞争而导致下行流量出现问题的概率较小。然而,下行流量的量常常要大于上行流量,这是因为移动用户常常从有线网络中下载数据。如果无线 Mesh 网络中的节点(TAPs 和网关)为独立实体,那么去往不同 TAPs 的下行网络将会严重受到传输不均衡问题的影响[7-9]。迄今为止,极少有学者尝试解决这一点上的均衡问题。文献[10]提出了一种针对包含了自私 TAPs 的多跳无线 Mesh 网络的基于激励的传输机制,但是仅考虑了上行流量。由于上行流量和下行流量的均衡机制的关键设计问题不同,所以现有机制不能适用于解决具有自私节点的无线网格网络下行和双向流量的均衡传输问

收稿日期:2017-10-23; **修回日期**:2017-11-13。
基金项目:广东省教育厅 2015 年度高职教育质量工程建设项目(粤教高函[2016]135 号);广东职业教育信息化研究会 2016 年度科研规划项目(YZGY161710)。
作者简介:何 健(1978-),男,江西九江人,硕士,讲师,工程师,主要从事网络技术、信息安全等方向的研究。

题。基于此，提出了一种基于奖励的传输机制，该方法主要创新点如下：

1）研究了自私 TAPs 和自私网关在无线 Mesh 网络中如何影响双向流量的均衡传输问题。

2）推导出了每个传输访问点（TAP）的双向目标吞吐量，并提出了一种基于奖励的均衡传输机制，通过信用币和代币支付策略来鼓励闲置 TAP 转发数据，同时使网关尽可能均衡地向 TAP 传输下行数据。

1 公平参考模型和虚拟信用币

1.1 公平参考模型

很多研究已经提出各种解决方案来解决无线 Mesh 网络中双向传输的均衡问题。然而，这些方案并没有考虑公平访问问题。要验证提出的基于奖励的均衡传输机制能否解决双向传输的公平问题，首先应该建立一套公平参考模型，为提出的机制提供理想基准，推导出理想状态下 TAPs 的客观吞吐量。要建立这样一个理想基准，则要做到以下几点。第一，公平的间隔尺寸为一个 TAP－聚合流量，这是因为提出的机制是从服务提供者而非移动用户的角度而设计的。第二，使用广播时间取代吞吐量作为网络中的资源从而避免 IEEE 802.11 无线网络中的性能异常。一个 TAP 的目标吞吐量与其链路容量成比例，为 TAPs 支付更多的操作者理应拥有更高的链接容量，这对现实世界的商业模式也合理。第三，在不考虑 TAPs 到网关距离的情况下，所有 TAPs 都应当分配到相同的时间。这在多跳无线 Mesh 网络中是必要性能，因为不同位置上的 TAPs 不应该由于其到网关的距离受到处罚，必须最大化空间复用从而保证链接得到充分利用。

1.2 虚拟币假设

本文定义了两种虚拟货币：信用币和代币。信用币在多跳无线 Mesh 网络中没有实际的货币价值。当 TAP 向前一跳 TAPs 转发数据时可获得信用币，当其与局部移动用户进行数据包传输时使用信用币。该策略有助于鼓励 TAP 参加数据转发，以此增加其信用币的存量。对于 TAP 发送一个单位局部数据包所能获得的确切信用币数量，其是根据网络中每个 TAP－聚合流量的目标吞吐量来确定的。与信用币不同，代币拥有实际货币价值。移动用户向处理其数据的相关 TAP 支付代币，TAP 向网关支付代币来促使其尽可能多地传输数据。另外，TAP 和网关在负责交易代币的中央银行兑现各自的代币。节点（即，用户、网关和 TAP）可通过可用链路与中央银行进行交流，中央银行利用代币不同的卖出和买入价格来从中获利。其中，中央银行通常属于网络运营者或设备提供者。

总之，该策略鼓励 TAP 通过为其他 TAP 转发数据来增加信用币存量，并通过发送数据到其局部移动用户来赚取代币。本文假设每个 TAP 具备一个基于信任计算的防篡改模块，该模型是通过转发数据来获得信用币，通过发送局部数据来消耗信用币。因此，在提出的机制中，每个 TAP 信用币的生成和消耗均可以防篡改。

2 基于奖励的双向均衡传输机制

2.1 奖励机制

无线 Mesh 网络中因自私节点导致的均衡传输问题已得到广泛认知，并且已经提出一些支持节点间合作的机制[11-13]。这些机制大体可分为两类：1）基于信誉的机制，其监控每个节点的行为并惩罚非合作节点；2）基于支付的机制，其引进了一些虚拟货币来支持向其他节点发送数据包。然而在无线 Mesh 网络中，收益主要来自于移动用户，而不是现有研究假设的 TAPs 或有线网络的终点。因此，上述基于信誉和基于支付的机制不能扩展用于解决包含自私节点的无线 Mesh 网络中的均衡传输问题。为此，本文提出的基于奖励的均衡传输机制兼顾了这些问题。

2.2 下行流量的均衡传输机制

先前的研究主要集中于无线 Mesh 网络中上行流量的均衡传输问题，上行流量在中间 TAPs 丢弃数据包，然而几乎所有的下行流量都在网关进行丢弃。因此，当网络节点为自私时，用于上行和下行流量的均衡传输机制的也存在不同。对于上行流量，关键角色为中间 TAPs，设计的传输机制必须鼓励 TAPs 转发所有传输数据并向其移动用户提供真实的数据速率。然而对于下行流量，网关才是机制设计中最重要的一环，这是因为所有数据流量都必须从网关向无线 Mesh 网络发送。如果网关为自私的，就会造成中间 TAPs 的转发问题，显然，这种自私行为会造成下行流量的传输不均衡问题，因为网关控制了下行流量的整体性能[14]。因此，提出的新方法需要处理中间 TAPs 的转发问题，并且促进网关均衡地向不同 TAPs 传输数据。使每个 TAP 对其他 TAPs 的最优策略为转发所有传输数据，而对网关的最优策略，则是根据不同 TAPs 到最近 TAPs 的吞吐量，来确定下行数据传输到哪些 TAPs。在提出的均衡传输机制中，每个 TAP 通过向邻近 TAP 转发一个单位传输数据获得一个信用币。为了赚取真实收益，TAPs 必须收集足够的信用币来向其移动用户发送数据。向移动用户发送一个单位数据所需的信用币数量并不固定为一个。此外，根据 TAPs 接收的吞吐量，其向网关支付代币来确保网关会尽全力向无线 Mesh 网络传输下行数据。TAPs 向网关支付的接收一个单位数据所需的代币数量也不固定，其是根据所有 TAPs 吞吐量的均衡指数来确定的。

TAPs 也向通向网关的路由通道中的闲置 TAPs 支付代币，当 TAPs 和网关与银行有较好的链路链接时，其可以在中央银行兑现代币。因此，在提出的均衡传输机制下，这种消耗信用币和代币的支付设计，是鼓励自私 TAPs 转发所有的传输数据，而网关必须尽力向网络均衡地传输下行数据。

设计的策略具体如下：

1）通过控制每个时期自动产生的信用币数量和 TAPs 向网关支付的代币数量，并根据 TAPs 的目标吞吐量，使网关尽可能均衡地向 TAPs 传输下行数据。

2）调整每个 TAP 发送一个单位数据到其移动用户所需的信用币数量。用来确保每个 TAP 将会向其他 TAPs 转发所有的传输数据。

3）向路由通道中闲置的 TAPs 支付代币来鼓励其参与到数据转发中。

2.3 双向流量的目标吞吐量

首先，使每个 TAP 的下行和上行流量共享的时间一致，从而推导出多速率多权值 Mesh 网络中双向流量状况下的 TAPs 共享的目标时间。然后证明了当 TAPs 可以控制下行和上行流量之间的比率时，下行和上行流量的目标吞吐量的可行性（即，所有 TAPs 传输所有局部和传输数据所需时间为 1，并且所有 TAPs 都有充足时间来传输所有传输数据）。

提出的基于奖励的均衡传输机制考虑了具有 N 个 TAPs（即，$TAP_1, TAP_2, \ldots, TAP_N$）和 F 个聚合流量的网络，包括所有上行和下行流量。定义 R_f 表示去往/来自网关的流量 f 所在的路由路径上的链接集合。C_l 为链接 l 的链路容量，并且所有流量均为饱和。然后本文将 t_l^f 表示为链接 l 上流量 f 共享的时间，并且 l_1^f 为流量 f 的第一个链接。为了避免每个流量穿过不同数量 TAPs 产生可能的空间偏差，设定：

$$\frac{t_{l_1^f}^f}{W_{TAP_m}} = \frac{t_{l_1^g}^g}{W_{TAP_n}}, \text{flow} f(g) \text{ is belong to } TAP_m(TAP_n) \quad (1)$$

其中：W_{TAP_i} 为网络中 TAP_i 的权重。还需保证每个 TAP 有足够时间来转发来自前面 TAPs 的所有传输数据因此有：

$$t_i^f C_i = t_i^f C_j, \forall i,j \in R_f \quad (2)$$

然后，必须满足下列方程式来获得最大聚合吞吐量。

$$\sum_{f=1}^{F} \sum_{l \in R_f} t_l^f = 1 \quad (3)$$

这里为了描述简单，先假设无线 Mesh 网络中所有链接都有着相同的干扰范围（即，只有一个链接可以在网络中传输）。对于可以空间复用的网络，必须找到干扰范围内具有最多流量的瓶颈链接。h_l 为链接 l 上运行的流量数，CL_l 表示链接 l 的干扰范围内链接的集合。然后瓶颈链接定义为具有最大 $\sum_{l \in CL_l} h_l$ 值的链接。由于希望所有上行和下行流量都可以充分利用网络资源，所以用等式 $\sum_f {}^F \sum_{l \in CL_k} t_l{}^f = 1$ 表示瓶颈链接的时间份额。

根据公式（1）～（3），可以将每个流量 x 的第一个链接的时间份额计算如下：

$$t_{l_1^x}^x = W_{TAP_k} * \left(\sum_f^F \frac{C_{l_1^f}^f * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \text{flow} x(f) \text{is belong to } TAP_k(TAP_m) \quad (4)$$

其中：$\bar{\rho}^f = \left(\sum_{l \in R_f} \frac{1}{C_l} \right)^{-1}$。

由于每个链接可能具有不同链路容量，所以确定每个链接上的每个流量的目标时间份额如下：

$$t_l^x = \frac{C_{l^x}}{C_l} * W_{TAP_k} * \left(\sum_f^F \frac{C_{l_1^f}^f * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \text{flow } x(f) \text{ is belong to } TAP_k(TAP_m) \quad (5)$$

因此，具有双向流量的无线 Mesh 网络中每个 TAP 的目标时间份额为下行和上行流量时间份额的总和：

$$t_{TAP_i} = 2 * W_{TAP_i} * \left(\sum_f^F \frac{C_{l_1^f}^f * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \text{flow } x(f) \text{ is belong to } TAP_m \quad (6)$$

其中：t_{TAP_i} 表示 TAP_i 的总时间份额。

然而，在真实无线 Mesh 网络中，TAPs 应该有权控制上行和下行流量的比率。定义 TAP_i 的上行和下行流量的时间份额如下：

$$t_{l_1^{uTAP_i}}^{uTAP_i} / t_{l_1^{dTAP_i}}^{dTAP_i} = A^{uTAP_i} / A^{dTAP_i} \quad (7)$$

其中：A^{uTAP_i}（A^{dTAP_i}）表示 TAP_i 的上行（下行）比率，而 $l_1^{uTAP_i}$（$l_1^{dTAP_i}$）表示无线 Mesh 网络中 TAP_i 的上行（下行）流量的第一个链接。然后可以推导出每个 TAP 的上行和下行流量的时间份额：

$$t_{l_1^{uTAP_i}}^{uTAP_i} = A^{uTAP_i} * 2 * W_{TAP_i} * \left(\sum_f^F \frac{C_{l_1^f}^f * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \quad (8)$$

$$t_{l_1^{dTAP_i}}^{dTAP_i} = A^{dTAP_i} * 2 * W_{TAP_i} * \left(\sum_f^F \frac{C_{l_1^f}^f * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \quad (9)$$

根据公式（2）可以得出中间 TAPs 在考虑链路容量之后从 TAP_i 转发传输数据所需传输时间，如公式（10）和（11）所示：

$$t_l^{uTAP_i} = \frac{C_{l_1^{uTAP_i}}^{uTAP_i}}{C_l} A^{uTAP_i} * 2 * W_{TAP_i} * \left(\sum_f^F \frac{C_{l_1^f}^f * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \quad (10)$$

$$t_l{}^{uTAP_i} = \frac{C_{l_1{}^{uTAP_i}}{}^{uTAP_i}}{C_l} A^{uTAP_i} * 2 * W_{TAP_i} * \left(\sum_f^F \frac{C_{l_1{}^{f\,f}} * W_{TAP_m}}{\bar{\rho}^f} \right)^{-1} \quad (11)$$

然后，TAP_i 的上行和下行流量的目标吞吐量为：

$$\rho_i^u = t_{l_1^{uTAP_i}}^{uTAP_i} * C_i \quad (12)$$

$$\rho_i^d = t_{l_1^{dTAP_i}}^{dTAP_i} * C_i \quad (13)$$

2.4　提出的均衡双向传输机制

本小节为无线 Mesh 网络中的双向流量提出了一种基于奖励的均衡传输机制。在每个测量周期的开始，网络中各 TAP 会宣布其上行和下行流量的比率以及来自和去往移动用户的流量负载。然后根据公式（12）和（13），TAPs 和网关可以计算每个 TAP 的上行和下行流量的目标吞吐量。ρ_i^u 和 ρ_i^d 分别表示 TAP_i 上行和下行流量的目标吞吐量。与下行流量的奖励机制相似，每个中间 TAP 通过转发一个单位传输流量获得一个信用币。最初边界 TAP_b 和网关分别自动产生 $\rho_i^u + \rho_i^d$ 和 $\sum \rho_i^d$ 信用币，这是因为它们没有数据转发。然后，鼓励 TAPs 和网关转发所有传输数据，从而可以从移动用户和 TAPs 处挣得最多代币，发送一个单位的局部数据需要的信用币数量是根据上行和下行流量的目标吞吐量来计算的，表示如下：

$$\begin{cases} \varepsilon_{bound} = 1 \quad \text{for bound TAPs and Gateway} \\ \varepsilon_i = \dfrac{\sum_{j \in ST_i} (\rho_j{}^u + \rho_j{}^d)}{\rho_i{}^u + \rho_i{}^d} \quad \text{for other TAPs} \end{cases} \quad (14)$$

其中：ST_i 为流量穿过 TAP_i 的 TAPs 的集合。

此外，r_i^u（r_i^d）表示 TAP_i 的上行（下行）流量端到端吞吐量。基于根据公式（16）得到的 TAP 上行和下行流量真实吞吐量之间的比率，确定移动用户需要向其相关 TAPs 支付的代币数。目标是防止 TAPs 宣布虚假比率或没有根据其宣布比率向移动用户发送上行和下行数据。如果上行和下行吞吐量的比率等于宣布的比率（即，$\frac{r_i^u}{r_i^d} = \frac{A^{uTAP_i}}{A^{dTAP_i}} * (1 \pm \delta)$，其中 δ 为允许误差范围），那么移动用户需要支付更多代币（即，$\omega_T > \omega_L$）来接收一个单位数据。

$$if \ \frac{r_i^u}{r_i^d} = \frac{A^{uTAP_i}}{A^{dTAP_i}} * (1 \pm \delta), \text{then} \quad \omega = \omega, \text{otherwise} \quad \omega = \omega_L, \text{where} \quad \omega_L > \omega_L \quad (15)$$

为了从有限网络向无线 Mesh 网络传输下行数据，网关从网络中所有 TAPs 处挣得代币。对于双向流量，公式如下：

$$AT\_FI = (\sum r_i^d / (A^{dTAP_i} * C_{TAP_i} * W_{TAP_i} / (A^{dTAP_i} + A^{uTAP_l})))^2 / (fiownum * \sum (r_i^d / (A^{uTAP_i} * C_{TAP_i} * W_{TAP_i} / (A^{dTAP_i} + A^{uTAP_l})))^2) \quad (16)$$

根据公式（16），当网关根据 $TAPs$ 目标吞吐量传输下行

流量时，AT_FI 的值为 1。结果，网关转发一个单位数据就从 TAPs 接收 $\zeta * AT\_FI$ 个代币。与前文描述的基于奖励的下行流量机制类似，TAP_i 向路由通路中闲置 $TAPs$ 支付 λ 代币来传输一个单位下行或上行数据。值得注意的是参数 ω、λ 和 ζ 之间的关系为 $\omega > \lambda + \zeta$。

3 仿真评估

3.1 实验环境

本章利用 NS－2 网络仿真器评估了提出的双向流量的均衡传输机制。重点关注双向流量的机制是因为空间限制以及双向流量包括下行流量。图 2 仿真模型是一个具有 3 个双向流量的 $TAPs$ 的无线 Mesh 网络，在该网络结构中，处于两个跳跃之外的 $TAPs$ 位于载波检测范围内。无线链接速率均设置为 11 Mbps。这些仿真中使用的 MAC 协议是不具有 RTS/CTS 的 IEEE 802.11 DCF。在接下来的仿真中假设 $TAPs$ 可以通过交换信息学习移动用户的聚合流量负载。根据前面提到的设计原则，ω、ζ 和 λ 的值分别为 10、2 和 0.1/字节数据。提出的机制设定 δ 的值为 5%。测量周期为 1 s。仿真中的所有 $TAPs$ 都运行双向流量并且数据流量是数据大小为 1000 字节的 UDP CBR 流量。首先，所有 $TAPs$ 饱和（即，总是有流量传输到移动用户或从移动用户传出），并且 $TAPs$ 的上行和下行流量的比率为：A^{uTAP_1}：$A^{dTAP_1} = 2$：3，A^{uTAP_2}：$A^{dTAP_2} = 3$：7，A^{uTAP_3}：$A^{dTAP_3} = 1$：4。

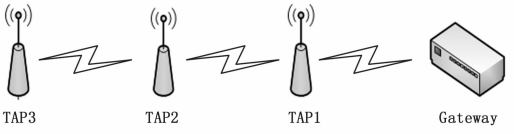

图 2 具有 3 个双向流量 $TAPs$ 的无线 Mesh 网络

3.2 仿真结果

仿真结果如表 1 显示，初始条件下每个 $TAPs$ 的上行流量和下行流量的平均吞吐量分别为：583 和 460、433 和 390、85 和 405，均衡机制条件下分别为：302 和 446、225 和 520、154 和 592。基于原始 802.11 MAC 协议，双向流量的平均吞吐量明显不公平。相反，均衡传输机制下的仿真结果与系统设置则十分接近。值得注意的是这里使用广播时间替代吞吐量作为网络中的资源从而避免 IEEE 802.11 无线网络的性能异常。表 2 显示了每个流量的平均吞吐量，每个 TAP 的目标吞吐量大约为 742 字节，这与仿真结果十分接近。上行和下行流量间的比率也确认了提出方法的配置。此外，仿真结果的平均吞吐量与公平参考模型下的目标吞吐量也十分接近。

表 1 $TAPs$ 上行和下行流量的平均吞吐量

	初始条件下			均衡传输机制下		
流量/kbps	上行	下行	总计	上行	下行	总计
TAP1	583	460	1043	302	466	768
TAP2	433	390	823	225	520	745
TAP3	85	405	490	154	592	746

表 2 每个流量的平均吞吐量

	$uTAP_1$	$dTAP_1$	$uTAP_2$	$dTAP_2$	$uTAP_3$	$dTAP_3$
总吞吐量/kbps	746		742		742	
平均吞吐量/kbps	302	444	220	522	147	595
上行和下行流量比率	0.68 (≈2:3)	0.42 (≈3:7)	0.24 (≈1:4)			

接下来本文讨论了自私 TAPs 的不正当行为，即其宣布处于忙碌状态的错误信息。表 3 分别显示了 TAP_2 在真实闲置和谎称非闲置时，在真实非闲置和谎称闲置时，其获得的代币。可以看出，当 TAP_2 为闲置时，在宣布闲置时 TAP_3 将会支付其 114.24 个代币来转发其上行和下行流量。然而，如果其行为不当或错误宣布其忙碌，则 TAP_3 和 TAP_2 的移动用户将不会向 TAP_2 支付代币，这是因为 TAP_2 忙碌，没有数据从移动用户传出或传向移动用户。同样，当 TAP_2 真实忙碌（即，其有来自于移动用户的局部数据要发送），它将无法谎称空闲。这是因为当其谎称空闲时，其他 TAPs 的支付要远少于移动用户（即，$\omega > \lambda$）的支付。

表 3 TAP_2 在闲置和非闲置情况下获得的代币

宣布状态	真实闲置	谎称非闲置
获得的代币	114.24	0
宣布状态	真实非闲置	谎称闲置
获得的代币	7429.33	74.27

4 总结

对于无线 Mesh 网络中存在的自私节点问题，提出基于奖励的均衡传输机制来解决。再构建公平参考模型，并推导出理想状态下，每个 TAP 的客观吞吐量并证明了每个 TAP 上行和下行流量目标吞吐量的可行性。然后建立基于奖励的传输机制，最后，将均衡机制下的仿真结果与推导出的每个 TAP 的客观吞吐量进行比较，验证了基于奖励的均衡传输机制的可行性。此外，该网络中没有自私行为出现。

未来将会考虑复杂的网络环境，例如多网关、多信道分配、负载平衡以及资源分配问题。

参考文献：

[1] 冯琳函，钱志鸿，金冬成. 增强型的无线 mesh 网络信道分配方法 [J]. 通信学报，2012，33 (10)：44－50.

[2] 陈星晨，张丽萍. 基于无线传输的车载温湿度测量系统设计 [J]. 计算机测量与控制，2017，25 (5)：42－44.

[3] Narlikar G，Wilfong G，Zhang L. Designing multihop wireless backhaul networks with delay guarantees. [J]. Wireless Netw，2010，16 (1)：23－54.

[4] Avokh A，Mirjalily G. Load－balanced Multicast Tree Routing in Multi Channel Multi Radio Wireless Mesh Networks Using a New Cost Function [J]. Wireless Personal Communications，2013，69 (1)：75－106.

[5] 樊秀梅，李晓辉，何 骞. 无线 Mesh 网络中的组播机会路由研究 [J]. 电子学报，2010：38 (1)：32－36.

[6] Jun J，Sichitiu M L. Fairness and QoS in multihop wireless networks. [J]. IEEE VTC，2003，5 (5)：2936－2940.

[7] Liu T，Liao W. Location－dependent throughput and delay in wireless mesh networks [J]. IEEE Trans Veh Technol 2008，57 (2)：88－98.

[8] 符 琦，陈志刚，蒋云霞. 集中式无线 Mesh 网络信道分配策略研究 [J]. 计算机应用研究，2012，29 (8)：2821－2825.

[9] 夏汉铸，刘辉元. 无线 Mesh 网络中基于信道状态的动态信道分配算法研究 [J]. 重庆邮电大学学报：自然科学版，2014，26 (3)：362 - 366.
[10] Lee J，Liao W，Chen M. An incentive－based fairness mechanism for multi－hop wireless backhaul networks with selfish nodes [J]. IEEE Trans Wirel Commun. ，2008，7 (2)：697 - 704.
[11] 许世文. 基于 SDN 的信息中心网络的技术研究 [D]. 北京：北京邮电大学，2013. 22 - 24.
[12] 王　坚，李玉柏，蒋勇男. 片上网络通信性能分析建模与缓存分配优化算法 [J]. 电子与信息学报，2009，31 (5)：1059 - 1062.
[13] Ernst J B，Denko MK. The design and evaluation of fair scheduling in wireless mesh networks. [J]. Academic Press，Inc，2011 ，77 (4) ：652 - 664.
[14] Kabbani A，Salonidis T，Knightly E. A distributed low－complexity maximum－throughput scheduling for wireless backhaul networks. [J]. IEEE INFOCOM，2007，20 (3)：63 - 71.

(上接第 254 页)

环，共消耗 (512) 个时钟周期。当下一个 FPGA _ CLK 时钟信号的上升沿到来后，state 进入 produce 状态，生成密钥流，如图 8 所示。进入该状态时，分别对寄存器 *i*，*j* 分别进行清零操作。state 信号进入同步有限状态机 (FSM) state2，首先进入 remainder _ i 状态，对寄存器 i 进行取余操作；当 FPGA _ CLK 时钟上升沿到来时，进入 remainder _ j 状态，对寄存器 j 进行取余操作；在 swap _ 2 状态下，“任意”交换一维数组 S；在 remainder _ t 状态下，对寄存器 t 进行取余操作；在 myflow 状态下，生成密钥流 k。至此，一帧明文数据对应的密钥流 k 生成完成，当 FPGA _ CLK 时钟下一个上升沿到来时，state 进入下一次循环中。在 produce 状态下，循环次数与一帧明文数据中有效数据信息的字节数相关，在本设计中，有效数据信息假定为 3 字节，因此在 produce 状态下，共循环 3 次，消耗 15 个时钟周期。在本设计中，生成对应的密钥流 k 共消耗 783 个 FPGA _ CLK 时钟周期。

4　实验方法步骤、验证及结果分析

根据上述 RC4 算法的设计方案，本系统采用 Xilinx 公司的 ISE 14.7 软件对其进行编译综合，并在 Modelsim SE 10.1a 软件中进行时序仿真。RC4 算法时序仿真图如图 9 所示，仿真时假定输入明文有效数据信息 sv _ data _ i 为 24'h33aa55，当异步复位信号 sl _ rst _ i 有效 (高电平) 时，输出密文数据 sv _ data _ o 为 24'h000000，当 done _ sig 信号为高电平时，产生 RC4 算法加密模块结束提示信号，当下一个 FPGA _ CLK 时钟上升沿到来时，生成的密钥流 k 为 24'h2fb7f6，进行异或操作后输出密文数据 24'h1c1da3，并存储在寄存器 sv _ data _ o 中。

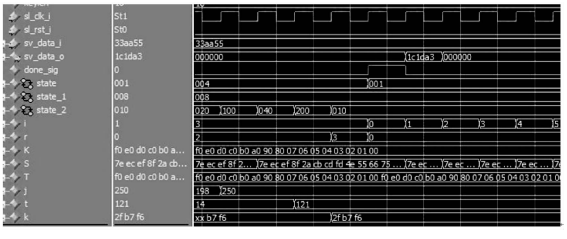

图 9　RC4 算法加密时序仿真图

通过 Xilinx 公司的 chipscope 软件，上板测试程序的可执行性，相关的信号波形如图 10 所示。

从上述测试结果可以看出，RC4 算法加密模块可以满足本系统的需求，且其工作状态正常，相比软件加密方式，时钟消耗更低；相比普通 RC4 加密算法消耗时钟降低。根据相关文献[1]中 RC4 算法消耗的时钟约在 (明文数据字节数) 时钟数，本系统中 RC4 消耗 (明文数据字节数) 个时钟数，相比

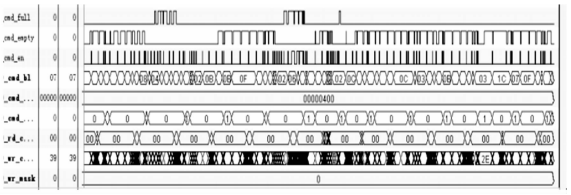

图 10　测试波形图

之前的算法设计减少 256 个时钟，且消耗硬件资源占比更低。在 ISE 14.7 中完成该模块的综合并下载到 FPGA 开发板上进行验证。结果表明，本设计满足系统设计需求。

5　结语

本文用 Verilog HDL 语言以有限状态机 (FSM) 的形式设计了一种基于 FPGA 的 RC4 加密传输数据帧的系统，比通常设计中时钟的需求更少，并在仿真软件 Modelsim SE 10.1a 中进行了仿真测试，得到的仿真波形满足设计需求。并且通过 ISE 14.7 中进行综合并下载到 FPGA 开发板中实现了功能验证，证实了系统运行的可靠性。本系统可应用于通信数据传输中，具有一定的实际应用价值。

参考文献：

[1] 杨　梅，张耀文，等. RC4 流密码原理与硬件实现 [J]. 信息通信，2009 (6)：40 - 43.
[2] 候整风，孟毛广，等. RC4 流密码算法的分析与改进 [J]. 计算机工程与应用，2015 (24)：50 - 53.
[3] 黄道林，杨　军，等. RC4 加密算法的 FPGA 设计与实现 [J]. 云南大学学报，2009 (51)：80 - 83.
[4] 张　开，陆洪毅，等. RC4 加解密算法的硬件实现 [M]. 中国会议，2010 (10).
[5] 宫大力，黄玉划，等. RC4 算法研究与改进 [M]. 中国会议，2011.
[6] 连至助. 序列密码的设计与分析研究 [D]. 西安：西安电子科技大学，2012，10.
[7] 刘志巍. 密码算法的随机性测试研究 [D]. 西安：西安电子科技大学，2011. 08.
[8] 胡　亮，迟　令，等. RC4 算法的密码分析与改进 [J]. 吉林大学学报，2012，50 (3)：511 - 516.
[9] 王　诚，吴继华，等. Altera FPGA/CPLD 设计 (基础篇) [M]. 北京：人民邮电出版社，2005.
[10] 高为民，朱凌志，等. 混沌加密算法在 J2ME 平台中的应用研究 [J]. 计算机仿真，2013 (03).
[11] 张洪福，杨小梅，等. 基于 AD9516 的宽带高动态数字中频系统采样时钟设计与应用 [J]. 电子器件，2009，32 (6).
[12] 吕　波，张　涌，等. 基于 FPGA 的四口 RAM 设计与实现 [J]. 仪表技术与传感器，2017 (1)：34 - 37.