引用本文：聂敏，谢珲，杨光，等. 基于 MDP 模型决策安全策略的软件定义量子保密网络[J]. 光通信技术，2020，44(9)：1–6.

# 基于 MDP 模型决策安全策略的软件定义量子保密网络

聂 敏[1]，谢 珲[1*]，杨 光[1,2]，张美玲[1]

（1.西安邮电大学 通信与信息工程学院，西安 710121；2.西北工业大学 电子信息工程学院，西安 710072）

**摘要**：为了提升量子保密网络对数据流量的适应匹配能力以及提升网络服务质量(QoS)和用户体验，提出基于马尔科夫决策过程(MDP)安全策略的软件定义量子保密网络(SDQSN)。SDQSN 可根据网络流量变化自适应地选择不同的量子密钥管理策略，通过对量子链路的实时监测，基于 MDP 计算网络收益，决策系统的安全策略，让系统在量子加密和经典加密的安全策略间进行灵活切换，在维护网络安全的同时保证网络的 QoS 收益。仿真结果表明：SDQSN 比传统量子保密网络更具灵活性和动态可调性，能够有效保证网络的全局收益，提升用户体验。

**关键词**：软件定义量子保密网络；马尔科夫决策过程；量子密钥管理；服务质量

**中图分类号**：TN918.9　**文献标志码**：A　**文章编号**：1002-5561(2020)09-0001-06

DOI：10.13921/j.cnki.issn1002–5561.2020.09.001　**开放科学(资源服务)标识码(OSID)**：

# Software–defined quantum secure network based on MDP model decision security policy

NIE Min[1], XIE Hui[1*], YANG Guang[1,2], ZHANG Meiling[1]

(1. School of Communication and Information Engineering, Xi'an University of Posts and Telecommunication, Xi'an 710121, China;
2. School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China)

**Abstract**: In order to improve the adaptive matching ability of quantum security network to data flow and improve network quality of service(QoS) and user experience, a software-defined quantum security network(SDQSN) based on Markov decision process (MDP) security policy is proposed. SDQSN can adaptively select different quantum key management strategies with the change of network traffic, and rely on the real-time monitoring of quantum link, calculate network revenue based on MDP, and determine the security policy of the system, so that the system can flexibly switch between the security policies of quantum encryption and classic encryption, and maintain network security and ensuring network QoS benefits. The simulation results show that the SDQSN is more flexible and dynamic adjustable than the traditional quantum security network, which can effectively ensure the overall benefits of the network and enhance the user experience.

**Key words**: software-defined quantum security network; Markov decision process; quantum key management; quality of service

## 0 引言

量子保密网络是未来信息安全领域的研究热点之一，国内外的科研团队在该领域已取得了很多成就[1–7]。然而，随着万物互联时代的到来，大规模移动智能业务不断涌现更迭，未来网络流量将呈爆发式增长，用户对网络服务质量(QoS)的要求将越来越高。目前，最先进的量子密钥分发(QKD)系统[7]只能达到 2~3 Mb/s 的安全密钥速率，不能满足加密网络中所有的数据流量。聂敏等人[8–11]的研究还表明量子信息在自由空间传输时不可避免地会受各种环境影响，QKD 无法全天候进行。当量子链路状态较差时，若网络继续采用量子加密策略会造成网络资源的浪费以及用户传输时延的增加，最终导致用户体验差。因此，要实现量子保密网络走向应用化和规模化，就必须解决上述密钥管理和提升网络 QoS 的问题。

**收稿日期**：2020–01–01。

**基金项目**：国家自然科学基金(61971348)资助；陕西省国际科技合作与交流计划项目(2015KW–013)资助。

**作者简介**：聂敏(1964—)，男，博士后，教授，主要从事量子通信领域的研究工作。主持和参与的省部级、国家级项目 6 项；作为第一发明人，获得国家专利局 3 项发明专利授权；出版专著和译著 4 本；在国内外学术期刊和国际会议发表论文 30 余篇。

*** 通信作者**：谢珲(E–mail: 553401298@qq.com)。

软件定义网络(SDN)[12]基于解耦化思想,将数据转发层与控制层相分离,使网络具备充分的开放性和可编程性,已在网络虚拟化、无线局域网、数据中心网络和云计算等领域得到应用[13-15]。本文为了增强量子保密网络对数据流量的适应匹配能力以及提升网络 QoS 和用户体验,结合 SDN 的思想,提出软件定义量子保密网络(SDQSN)模型,并基于该模型提出一种基于马尔科夫决策过程(MDP)的安全策略切换算法,为量子保密网络的健康发展奠定理论根基。

## 1 SDQSN 分层模型和加密机制

### 1.1 SDQSN 分层模型

为了增强量子保密网络对数据流量的适应匹配能力,在 SDQSN 中,量子密钥的管理策略分为 2 种:当网络中流量相对较低或量子链路状态良好时,使用 QKD 策略进行安全通信;当数据量增加或量子链路状态相对较差时,仅使用量子密钥对经典的对称密钥进行更新,以维持网络必要的安全级别。SDQSN 系统可以根据量子链路的实时状态,通过可编程控制器自适应地管理量子密钥和部署安全策略,能够使网络更加灵活。SDQSN 分层模型如图 1 所示。

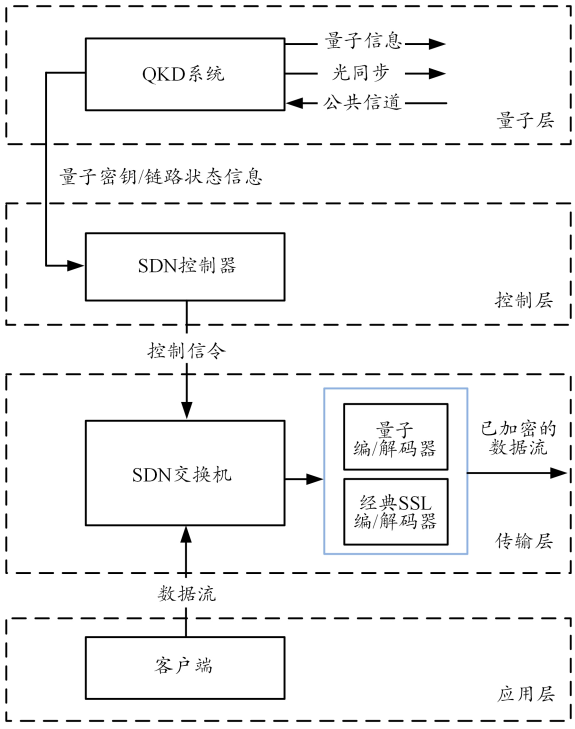


图 1 SDQSN 分层模型

从图 1 可知,SDQSN 包括以下 4 层:

◆量子层。核心部分由 QKD 系统和用于密钥管理的软件程序组成。它只负责量子信息交换、光同步以及向控制层提供量子密钥。公共信道用于交换 QKD 协议中产生的数据交换(如测量信息等)。有关量子密钥的任何处理(筛选、纠错等)都在 QKD 系统中实现。

◆控制层。主要负责管控传输层和量子层的相关设备。SDN 控制器会监控 QKD 系统的状态,合理管理密钥,并基于 MDP 决策安全策略,命令交换机使用不同的编/解码器将数据路由至下一个安全通道。

◆传输层。由 SDN 交换机及量子/经典编/解码器组成,负责执行网络路由和数据交换。交换机根据控制器指令将应用层生成的数据路由到相应的编/解码器,执行不同的加密方式,再通过光信道将加密数据发送到目标节点。

◆应用层。主要由各类网络通信终端(客户端)及软件应用组成。

在 SDQSN 中,当应用层生成的用户数据被发送至交换机时,如果预先设置的量子链路被损耗,数据包将由交换机转发至控制器,控制器根据不同量子密钥管理策略下的量子保真度和可用量子安全密钥生成率产生的网络 QoS 收益进行多属性决策,判断是否将安全策略切换至完全经典的加密方式。如果控制器决策模块接收切换请求,则控制器将下发相应指令,让 SDN 交换机将数据包路由至经典安全套接层(SSL)编/解码器,再通过经典通道发送至目标节点。

### 1.2 SDQSN 的逐跳加密机制

由于 SDN 中存在各节点间的信息交换,当 SDQSN 使用 QKD 策略进行安全通信时,可采用逐跳加密策略,该策略采用一次一密的加密算法,在理论上能够充分保证信息的安全传输。逐跳加密示意图如图 2 所示,其加密过程如下:相邻节点间共享量子密钥,节点 $R_1$ 将明文 $M$ 直接与密钥 $K_1$ 进行异或运算并发送至节点 $R_2$,节点 $R_2$ 运用与节点 $R_1$ 共享的密钥 $K_1$ 和与节点 $R_3$ 共享的密钥 $K_2$ 对密文 $M$ 进行异或运算操作得到 $M\oplus K_2$ 发送给节点 $R_3$,节点 $R_3$ 进行同理操作得到 $M\oplus K_3$ 发送至节点 $R_4$,节点 $R_4$ 运用密钥 $K_3$ 与节点 $R_3$ 发过来的密文进行异或运算解密,最终得到节点 $R_1$ 发送的明文 $M$。同理可推 $N$ 节点间的加密过程。

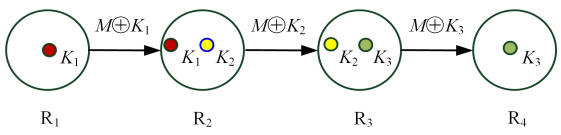


图 2 逐跳加密示意图

## 2 基于 MDP 的安全策略切换方法

决策系统是否进行安全策略的切换是实现 SDQSN 的关键所在。MDP 对系统当前的决策时刻收益以及下一个决策时刻的可能收益进行迭代计算,能够保证每一步的决策最终所得到的全局收益是最大的。因此,本文进一步提出一种基于 MDP 的安全策略切换方法以保证 SDQSN 收益。

### 2.1 状态空间

MDP 模型的状态是用来得到收益的,状态要反映出实时信息,不同状态的变换导致的实时收益也不同。由于数据当前所处的量子链路状态是实时的,且系统中量子密钥的应用策略也是实时变化的。因此,将这两大要素定义为决策模型的状态空间。

$$s=\{\eta,k_Q,k_C\}\in S \tag{1}$$

其中,$S$ 表示马尔科夫决策过程数学模型中的状态空间集合,$s$ 表示模型不同时刻的状态空间,$\eta$ 表示量子链路下一时刻的损耗程度,$\eta\in\{1,2,\cdots,\zeta\}$。$\zeta$ 为满足 QKD 条件的链路损耗极值对应的链路损耗程度,当链路损耗程度超过这个值后,默认系统执行强制安全策略切换。$k_Q$ 表示量子密钥用于数据加密,该密钥管理策略对链路的实时损耗状态要求很高,$k_Q\in\{0,1\}$。当 $k_Q$=1 时,表示系统正在执行该策略;当 $k_Q$=0 时,表示系统没有在执行该策略。$k_C$ 表示量子密钥用于经典对称密钥的更新,此时系统的安全策略使用经典对称密钥,该密钥管理策略对量子链路损耗的要求具有非实时性,$k_C\in\{0,1\}$。同理,当 $k_C$=1 时,表示系统正在执行该策略;当 $k_C$=0 时,表示系统没有在执行该策略。依据文献[16],满足 QKD 的基础条件应使量子信道中的信噪比约为 5.89:1,在其它参数取典型值的情况下可计算出满足量子通信条件的信道衰减极值为:

$$\zeta_{link}\geqslant 10\times\lg(10^{-6})\ \text{dB}=-60\ \text{dB} \tag{2}$$

从式(2)可知,标准的量子保密网络中的总链路损耗不应超过 60 dB。在满足量子通信条件的信道衰减极值内,将链路衰减程度划分为 6 个等级,对应的链路损耗如表 1 所示。故 $\zeta$=6,$\eta\in\{1,2,3,4,5,6\}$。

表 1 链路损耗程度划分

| $\eta$ | 链路损耗程度/dB |
|---|---|
| 1 | [0,10] |
| 2 | [10,20] |
| 3 | [20,30] |
| 4 | [30,40] |
| 5 | [40,50] |
| 6 | [50,60] |

### 2.2 动作行为

动作行为是系统在当前状态下根据链路状态变化及网络收益作出的决策,系统通过动作行为 $w$ 改变当前系统安全策略的状态。

$$w=\begin{cases}0,\text{保留}\\1,\text{切换}\end{cases} \tag{3}$$

动作行为 $w$=0 表示系统保持基于量子密钥的数据加密方式,$w$=1 表示系统切换至完全经典的加密方式。

### 2.3 状态转移概率

为了使 SDQSN 具有更高的安全级别,本算法模型定义量子密钥安全策略用于安全通信的优先级大于量子密钥仅用于更新经典对称密钥的优先级,将 2 种密钥管理策略的执行情况用图 3 所示的状态转移图表示。

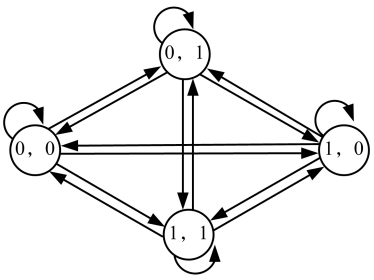


图 3 量子密钥管理策略状态转移图

假设系统中 2 种量子密钥管理策略的执行和离去都服从 Poisson 分布,且每条链路每次只能执行一种密钥管理策略,即同一时刻相同两节点间通过量子纠缠产生的量子密钥只能用于该链路上数据的安全通信或是对经典对称密钥的更新。

策略 $k_Q$ 的执行率和离去率分别为 $\lambda_1$ 和 $\mu_1$,策略 $k_C$ 的执行率和离去率分别为 $\lambda_2$ 和 $\mu_2$,则某链路执行一次 $k_Q$ 的概率和其离去的概率分别为 $\lambda_1 e^{-\lambda_1}$ 和 $\mu_1 e^{-\mu_1}$,分别记为 $A_1$ 和 $B_1$。该链路保持执行 $k_Q$ 的概率为 $1-\lambda_1 e^{-\lambda_1}-\mu_1 e^{-\mu_1}$,记为 $C_1$。同理,某链路执行一次 $k_C$ 的概率和其离去的概率分别为 $\lambda_2 e^{-\lambda_2}$ 和 $\mu_2 e^{-\mu_2}$,分别记为 $A_2$ 和 $B_2$。该链路保持执行策略 $k_C$ 的概率为 $1-\lambda_2 e^{-\lambda_2}-\mu_2 e^{-\mu_2}$,记为 $C_2$。那么,策略 $k_Q$ 和 $k_C$ 执行状态的转移概率矩阵为:

$$P=\begin{bmatrix}C_1\cdot C_2 & C_1\cdot C_1 & C_1\cdot C_2 & C_1\cdot C_2\\ C_1\cdot B_2 & C_1\cdot C_2 & A_1\cdot B_2 & A_1\cdot C_2\\ B_1\cdot C_2 & B_1\cdot A_2 & C_1\cdot C_2 & C_1\cdot A_2\\ B_1\cdot B_2 & B_2\cdot C_2 & C_1\cdot B_2 & C_1\cdot C_2\end{bmatrix} \tag{4}$$

忽略工程中链路状态发生变化的不定因素,为了便于模型的建立,假设本网络中的量子链路的损耗程度不会发生越级变化,即链路的损耗状态仅能在相邻的损耗等级中来回变化,其状态转移图如图 4 所示。默认链路初始状态良好,即此时 $\eta$=1。当控制器将网络的安全策略切换至完全的经典加密策略后,状态空间中的 $\eta$ 必定以概率 1 返回链路的初始状态。

假设量子链路发生状态转移的概率为 $\delta$,则链路

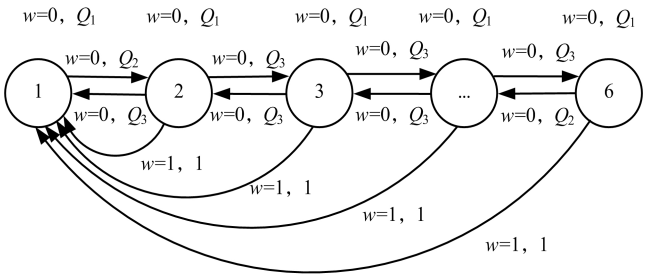


图 4 量子链路状态转移图

状态继续保持原状态的概率为 $Q_1=1-\delta$,链路由初始状态或损坏状态到达相邻状态的概率 $Q_2=\delta$。链路由非初始状态转移至相邻状态的概率为 $Q_3$,由于非初始状态及损坏状态下的链路状态有可能向任意相邻的任意一个状态转移,因此 $Q_3=\delta/2$。

由 $Q_1$、$Q_2$ 和 $Q_3$ 可以计算链路状态变化的概率,结合图 4 可以得到链路损耗程度 $\eta$ 的转移概率矩阵 $\boldsymbol{Q}$。$Q_{i,j}$ 表示链路损耗程度 $i$ 转移至链路损耗程度 $j$ 的概率,其中 $i=1,2,3\cdots,6$,$j=1,2,3\cdots,6$。图 3 未提及的概率,如跨损耗等级的转移概率 $Q_{1,3}$ 等均默认为 0。结合式(4)与矩阵 $\boldsymbol{Q}$ 可得到状态空间 $s=\{\eta,k_Q,k_C\}\in S$ 的状态转移概率矩阵 $\boldsymbol{\Phi}$ 如式(5)所示。

$$\boldsymbol{\Phi}=\begin{bmatrix} P\times Q_{1,1} & P\times Q_{1,2} & \cdots & P\times Q_{1,6} \\ P\times Q_{2,1} & P\times Q_{2,2} & \cdots & P\times Q_{2,6} \\ \cdots & \cdots & \cdots & \cdots \\ P\times Q_{6,1} & P\times Q_{6,2} & \cdots & P\times Q_{6,6} \end{bmatrix} \tag{5}$$

矩阵 $\boldsymbol{\Phi}$ 大小为(4×6)×(4×6),(4×6)为状态空间的总数量。$\boldsymbol{\Phi}$ 中的元素表示 SDQSN 由某个状态空间 $s$ 经过动作行为 $w$ 转移至状态空间 $s'$的概率 $\boldsymbol{\Phi}(s'|s,w)$。

### 2.4 收益函数

收益函数依赖于当前所处的状态,收益函数需要根据状态空间 $s$ 计算。

#### 2.4.1 量子保真度收益函数

由文献[17]可知,量子保真度随量子态作为信道的时间演化而降低。本文将量子保真度与量子态在信道持续时间的关系简化为线性,并定义当链路持续通信时间为 $\Delta t$ 时,即量子态作为信道的时间 $t=\Delta t$ 时,通信链路具有最高的量子保真度,此时链路损耗程度 $\eta=1$。综合考虑 2 种量子密钥管理策略对量子保真度的要求,将量子保真度收益函数定义为:

$$F=(s,w)=[k_Q,k_C]\cdot\{\alpha_1[F_0+K_F(\eta-1)],\ \alpha_2[F_0+K_F(\eta-1)]\} \tag{6}$$

其中,$\alpha_1$、$\alpha_2$ 分别表示量子保真度对策略 $k_Q$ 和 $k_C$ 的收益影响,策略 $k_Q$ 将 QKD 策略用于安全通信,具有实时性,因此对量子保真度要求较高。策略 $k_C$ 将量子密钥仅用于更新对称密钥,具有非实时性,对量子保真度要求较低。因此,$\alpha_1$ 取值应大于 $\alpha_2$ 取值。$F_0$ 为链路状态良好的情况下(即 $\eta=1$ 时)系统的初始量子保真度。$K_F$ 为量子保真度随链路状态变化的衰减常系数。随着动作行为 $w$ 发生变化,安全策略的切换会导致 $\eta$ 的更新。

#### 2.4.2 可用量子安全密钥生成率的收益函数

若采用有限长诱骗态 QKD 系统,依据文献[18],在使用弱相干光源进行 QKD 时,诱骗态协议系统的安全密钥生成率 $R_{key}$ 为:

$$R_{key}\geqslant 1/2\{Q_\mu f(E_\mu)H_2(E_\mu)+Q_1[1-H_2(e_1)]\} \tag{7}$$

其中,$\mu$ 为平均光子数,$Q_\mu$、$E_\mu$ 分别为光源量子态的接收率及误码率,$f(E_\mu)$为双边误码纠错效率,$Q_1$ 和 $e_1$ 为单光子到达接收端的概率及误码率,$H_2(x)=-x\log(x)-(1-x)\log(1-x)$。

策略 $k_Q$ 和 $k_C$ 对系统的安全密钥生成率有着不同的需求,若系统所提供的安全密钥生成率与策略需求速率相等时,即可获得最大的收益;若系统提供的安全密钥生成率高于需求速率会造成量子资源浪费,而提供的安全密钥生成率低于需求速率则会导致用户体验不足。针对 2 种策略的不同需求,文献[19]中的相关函数将系统可获得的量子安全密钥生成率的收益函数定义为:

$$R(s,w)=[k_Q,k_C]\cdot\left\{\beta_1\exp\left[-\frac{\left(R_{key}-R_Q^2\right)}{2R_Q^2}\right],\ \beta_2\exp\left[-\frac{\left(R_{key}-R_C^2\right)}{2R_C^2}\right]\right\} \tag{8}$$

其中,$\beta_1$、$\beta_2$ 分别表示可获得速率对 2 种量子密钥应用策略的收益影响;$\exp\left[-\frac{\left(R_{key}-R_Q^2\right)}{2R_Q^2}\right]$ 和 $\exp\left[-\frac{\left(R_{key}-R_C^2\right)}{2R_C^2}\right]$ 分别表示系统提供的安全密钥生成率与策略 $k_Q$ 和 $k_C$ 需求速率之间的关系;$R_Q$ 表示 QKD 策略用于安全通信的需求速率,$R_C$ 表示量子密钥用于更新经典对称密钥的需求速率。

#### 2.4.3 成本消耗

网络成本消耗函数 $C(s,w)$ 可表示为:

$$C(s,w)=[k_Q,k_C]\cdot w\times\overline{\omega} \tag{9}$$

其中,$\overline{\omega}=[K_\omega C_Q,K_\omega C_C]$ 为成本向量,$C_Q$、$C_C$ 分别表示量子密钥用于数据直接加密和用于更新对称密钥所消耗的系统资源,$K_\omega$ 为成本消耗相对于整个网络收益的权重系数。

### 2.5 最优化目标函数

收益函数 $B(s,w)$ 为:

$$B(s,w)=F(s,w)+R(s,w)-C(s,w) \tag{10}$$

根据收益函数,对瞬时收益函数求期望即可得到全局收益目标函数,如式(11)所示:

$$g^{\pi}(s^0)=E_{\pi}\left\{\sum_{t=0}^{\infty}\xi^t B(s^t,w^t)\right\} \tag{11}$$

其中,$\pi$ 为当前系统的加密策略,$s^0$ 为SDQSN 中量子链路及密钥管理策略的初始状态,折扣因子$\xi\in[0,1]$表示后一状态的收益相对于当前状态收益的影响程度,$\xi=0$表示系统只考虑当前状态的系统收益,$\xi=1$ 表示系统认为之后状态的收益和当前状态的收益一样重要。在式(11)中寻找全局收益最大的函数,并对该式进行 2 次 Bellman 等式变换,以含有状态转移概率 $\Phi(s'|s,w)$的形式展开,记 $E_{\pi}\{\xi^t B(s^{t+1},w^{t+1})\}$为 $g^{\pi}(s')$,可得到最终的最大全局收益目标函数为:

$$g^{\pi^*}(s^0)=\max_{w^0\in w}\left\{\sum_{s'\in S}\Phi[s'|s^0,w^0]B(s^0,w^0)+\sum_{s'\in S}\xi\Phi[s'|s^0,w^0]g(s')\right\} \tag{12}$$

每个状态的全局收益函数值由于系统采取不同的安全策略而发生变化,因此,SDQSN 采用数值迭代的方法求解最大全局收益目标函数,模型求解流程如图 5 所示。

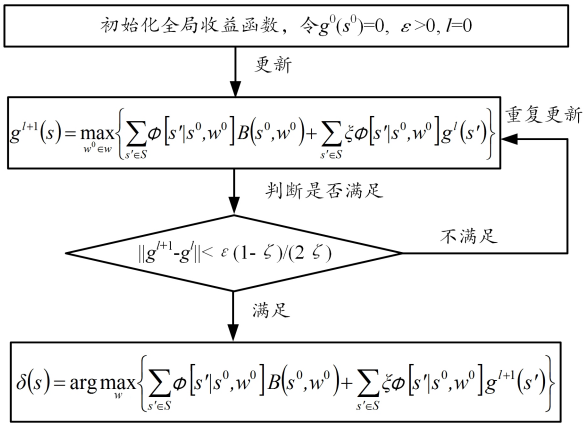


图 5 模型求解流程

$\delta(s)$即为能在最大程度上兼顾用户体验、保护网络安全和使网络收益最大的安全策略。

## 3 仿真分析

传统的量子保密网络采用单一的量子密钥管理策略 $k_Q$,且不考虑量子链路损耗对网络 QoS 的影响,因此无法时刻保证用户体验。对于本文所提出的 SDQSN 而言,量子链路的实时衰减程度以及量子密钥的应用策略的状态$[k_Q,k_C]$是变化的,SDN 控制器会根据系统收益决策安全策略。在此情况下,将基于 MDP 安全策略的 SDQSN 与传统的量子保密网络进行对比。

基于量子加密的安全策略所带来的全局收益随链路状态变化的情况如图 6 所示。横坐标为决策时刻(随链路状态 $\eta$ 变化,系统判断是否进行加密策略切换的时刻),纵坐标为网络的全局收益。TQSN 和 SDQSN 分别表示传统量子保密网络和基于 MDP 安全策略的量子保密网络的全局收益变化情况。从仿真结果可以看出,本文提出的 SDQSN 获得的全局收益相对于 TQSN 有明显提高,从而证实了 SDQSN 能够较好地提升量子保密网络中的用户体验以及网络的 QoS。

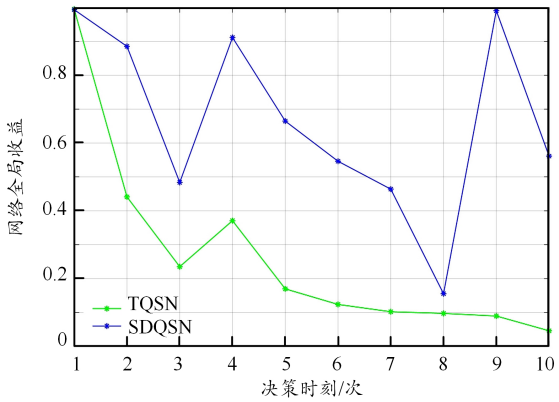


图 6 全局收益对比

基于量子密钥的安全策略所产生的量子保真度收益随链路状态变化的情况如图 7 所示。SDQSN 基于 MDP 系统的安全策略,通过对网络当前的决策时刻收益以及下一个决策时刻的可能收益进行迭代计算,保证每一步的决策最终所得到的全局收益是最大的。因此,SDQSN 的量子保真度收益受链路损耗影响明显较小。即使在链路损耗程度较大时,TQSN 仍然使用 QKD

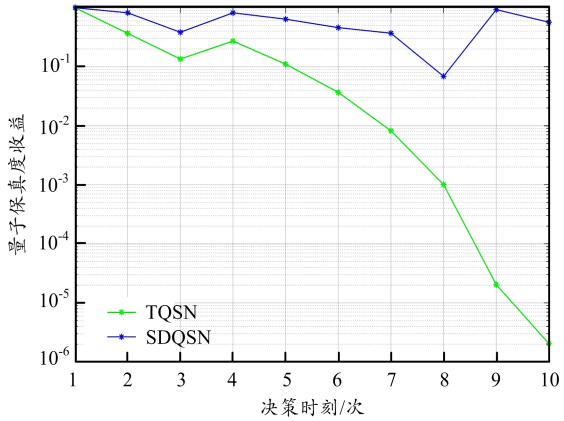


图 7 量子保真度收益对比

策略进行安全通信，所以其保真度收益受链路损耗的波动相对较大。

量子安全密钥生成率收益随着链路状态变化的情况如图 8 所示。可以看出，大部分决策时刻下，SDQSN 能够保证系统可获得的安全密钥生成率收益高于 TQSN；由于系统所提供的速率是不同的，因此在某些决策时刻下，也出现了 TQSN 收益较好的情况。

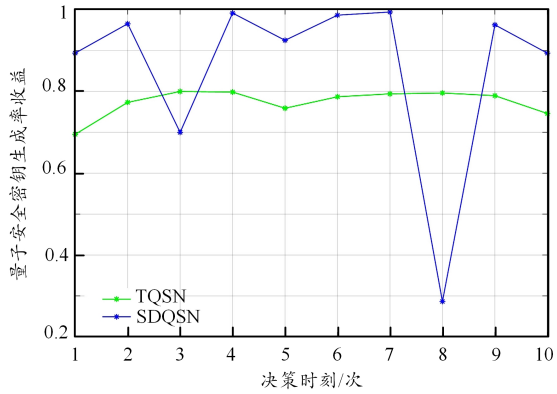


图 8 可用量子安全密钥生成率收益对比

综上所述，基于 MDP 加密策略的 SDQSN 在可获得的安全密钥生成率收益方面能获得更好的网络 QoS。

## 4 结束语

SDQSN 在网络流量相对较低时使用 QKD 策略进行安全通信；当数据量增加或量子链路状态相对较差时，仅使用量子密钥更新经典的对称密钥维持网络必要的安全级别，能够有效增强量子保密网络对数据流量的适应匹配能力。基于 MDP 的安全策略切换算法能够使 SDQSN 根据量子链路的实时变化在量子加密和经典加密方式间灵活切换，保证网络的 QoS 收益及用户体验，从而有效提高量子保密网络的适应性、可应用性。

**参考文献：**

[1] LIU Y, CHEN T Y, WANG L J, et al. Experimental measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2013, 111(13): 130502-1–130502-5.

[2] VALIVARTHI R, LUCIO-MARTINEZ I, CHAN P, et al. Measurement-device-independent quantum key distribution: from idea towards application[J]. Journal of Modern Optics, 2015, 62(14): 1141–1150.

[3] TANG Z, WEI K, BEDROYA O, et al. Experimental measurement-device-independent quantum key distribution with imperfect sources [J]. Physical Review A, 2016, 93(4): 042308-1–042308-4.

[4] 彭承志，潘建伟. 量子科学实验卫星—“墨子号”[J]. 中国科学院院刊，2016，31(9)：1096–1104.

[5] LIAO S K, CAI W Q, LIU W Y, et al.Satellite-to-ground quantum key distribution[J]. Nature, 2017, 549(7670): 43–47.

[6] 王晋岚. 世界首条量子保密通信干线开通[J]. 科学，2017(6)：52–53.

[7] PATEL K A, DYNES J F, LUCAMARINI M, et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks [J]. Applied Physics Letters, 2014, 104(5): 051123-1–051123-4.

[8] 聂敏，尚鹏钢，杨光，等. 中尺度沙尘暴对量子卫星通信信道的影响及性能仿真[J]. 物理学报，2014，63(24)：240303-1–240303-6.

[9] 聂敏，任杰，杨光，等. PM2.5 大气污染对自由空间量子通信性能的影响[J]. 物理学报，2015，64(15)：150301-1–150301-7.

[10] 聂敏，任家明，杨光，等. 非球形气溶胶粒子及大气相对湿度对自由空间量子通信性能的影响 [J]. 物理学报，2016，65 (19)：190301-1–190301-5.

[11] 聂敏，唐守荣，杨光，等. 中纬度地区电离层偶发 E 层对量子卫星通信性能的影响[J]. 物理学报，2017，66(7)：070302-1–070302-6.

[12] 张朝昆，崔勇，唐嵩嵩，等. 软件定义网络(SDN)研究进展[J]. 软件学报，2015，26(1)：62–81.

[13] MIJUMB I, RASHI D, SERRA T, et al. Network Function Virtualization: State-of-the-art and Research Challenges[J]. IEEE Communications Surveys & Tutorials, 2015, 18(1): 236–262.

[14] SURESH L, SCHULZZANDER J, MERZE R, et al. Demo: programming enterprise WLANs with odin [J]. Computer Communication Review, 2012, 42(4): 279–280.

[15] KANNAN K, BANERJEE S. Scissors: Dealing with header redundancies in data centers through SDN [C]//Proceedings of the 8th International Conference on Network and Service Management, October 22–26, 2012, Las Vegas, USA. Piscataway: IEEE, 2012: 295–301.

[16] 尹浩，马怀新. 军事量子通信概论[M]. 北京：军事科学出版社，2006.

[17] 卫容宇，聂敏，杨光，等. 基于软件定义量子通信的自由空间量子通信信道参数自适应调整策略 [J]. 物理学报，2019，68 (14)：140302-1–140302-7.

[18] 吴承峰，杜亚男，王金东，等. 弱相干光源测量设备无关 QKD 系统的性能优化分析[J]. 物理学报，2016，65(10)：15–23.

[19] MATIAS J, GARAY J, TOLEDO N, et al. Toward an SDN-enabled NFV architecture[J]. IEEE Communications Magazine, 2015, 53(4): 187–193.