无线网络中基于量子隐形传态的鲁棒安全通信协议

马鸿洋*①②　　王淑梅①　　范兴奎①
①(青岛理工大学理学院　青岛　266033)
②(中国海洋大学信息科学与工程学院　青岛　266100)

摘　要：该文在深入研究无线网络 802.11i 鲁棒安全通信的基础上，提出基于量子隐形传态的无线网络鲁棒安全通信协议，利用量子纠缠对的非定域关联性保证数据链路层的安全。首先，对量子隐形传态理论进行描述，并着重分析临时密钥完整性协议和计数器模式及密码块链消息认证协议的成对密钥、组密钥的层次结构；其次，给出了嵌入量子隐形传态的成对密钥、组密钥的层次结构方案；最后，在理论上给出安全证明。该协议不需要变动用户、接入点、认证服务器等基础网络设备，只需增加产生和处理纠缠对的设备，即可进行量子化的密钥认证工作，网络整体框架变动较小。

关键词：量子通信；无线网络；量子隐形传态；鲁棒安全网络
中图分类号：TN918.91　　**文献标识码**：A　　**文章编号**：1009-5896(2014)11-2744-06
DOI: 10.3724/SP.J.1146.2013.01838

A Robust Security Communication Protocol for Wireless Network Based on Quantum Teleportation

Ma Hong-yang①②　　Wang Shu-mei①　　Fan Xing-kui①
①(*School of Sciences*, *Qingdao Technological University*, *Qingdao* 266033, *China*)
②(*College of Information Science and Engineering*, *Ocean University of China*, *Qingdao* 266100, *China*)

Abstract: A robust security communication protocol for wireless network based on quantum teleportation is proposed in this paper by further study about wireless security protocol 802.11i, and quantum entanglement of nonlocality is used to enhance the security of data link layer of wireless network. This paper focuses on the description of theory of quantum teleportation and the analysis of pairwise key hierarchy and group key hierarchy of temporal key integrity protocol and counter-mode/CBC-MAC protocol, puts forward the design and corresponding algorithm of embedding quantum teleportation in the hierarchy of pairwise key and group key, theoretically brings forth network security. There is no need to change the user, access points and authentication server, which belong to the network infrastructure. It is only required to add relevant equipment for quantum key authentication work, which can ensure the overall framework of network to make less change.

Key words: Quantum communication; Wireless network; Teleportation; Robust security network

1　引言

无线网络[1,2]是电磁波与通信技术相互融合，实现数据传输的无线通信系统。因为其数据传输的方便快捷，目前已在政府、企业、国防等方面广泛应用；其数据链路层采用 3 种经典加密协议：有线等效保密(Wired Equivalent Privacy, WEP)、临时密钥完整性协议(Temporal Key Integrity Protocol, TKIP)、计数器模式及密码块链消息认证协议(Counter mode with CBC-MAC Protocol, CCMP)。WEP 最初制定原则是无线网安全性能达到有线网络，其密钥结构长度为 40 位(或者 104 位)密钥和 24 位初始向量，这种结构造成初始向量空间较小；TKIP 是替代 WEP 的折中协议，将初始向量长度从 24 位增加到 48 位，有效避免了空间小的缺陷，但其核心算法依旧是 WEP; CCMP 是替代 WEP 的新协议，把初始向量长度扩展到 128 位，不宜被经典计算机破解。但随着量子计算机的产生，CCMP 被破解也很容易。所以，这 3 种加密协议均易遭到破解，增强无线网络的安全性成为众多领域急需解决的技术问题。

量子通信的相关理论[3−5]和实验逐渐成熟。

2013-11-21 收到，2014-04-29 改回
山东省高等学校科技计划项目(J11LG07)，青岛市科技计划基础研究项目(12-1-4-4-(6)-JCH)和国家自然科学基金(61173056, 11304174)资助课题
*通信作者：马鸿洋　hongyang_ma@aliyun.com

1983 年 Bennett 等人[6]提出以偏振光为载体的量子密钥通信协议。1991 年 Ekert[7]提出以量子纠缠态为载体的 EPR 通信协议。2006 年 Ma 等人[8]提出以 GHZ 态为跨簇中转点的多量子节点通信协议等。诸多理论和实验为量子通信与无线网络的相互融合提供了契机，吸引许多科学家进行了深入研究。2010 年，周南润等人[9]利用量子隐形传态设计了数据链路层的选择重传 ARQ 同步通信协议，该协议考虑了如何通过不可靠信道建立有效的量子信道，完成相应数据帧和量子确认帧传输。2013 年，Gong 等人[10]提出了基于直接通信的无源光网络的量子虚拟专用网通信协议，该协议考虑了网络用户之间的量子身份认证。以上协议没有涉及无线网络的密钥层次结构。

本文是在无线网络和量子隐形传态的基础上，提出基于量子隐形传态的无线网络鲁棒安全通信协议，利用量子纠缠对的非定域关联性保证数据链路层的安全，实现不需要变动用户、接入点、认证服务器等基础网络设备，只需增加产生和处理纠缠对的设备即可进行量子化的密钥认证。

2　相关基础理论

2.1 量子隐形传态基本理论

假设甲地的 Alice 与乙地的 Bob 分开一段距离，Alice 有粒子 a，b，Bob 有粒子 c。粒子 a 处的量子态表达式为：$|\Psi\rangle_a = \alpha\,|0\rangle_a + \beta\,|1\rangle_a$，其中 $|\alpha|^2 + |\beta|^2 = 1$。需要将粒子 a 的量子态传送给 Bob，因此，Alice 与 Bob 必须通过量子信道和经典信道进行通信，其过程如下：

(1)Alice 与 Bob 构建量子信道，即粒子 b，c 组成量子纠缠对，其表达式为

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_b|1\rangle_c - |1\rangle_b|0\rangle_c\right) \tag{1}$$

(2)Alice 与 Bob 手中的 3 个粒子 a，b，c 组成的量子态为

$$\left(\alpha\,|0\rangle_a + \beta\,|1\rangle_a\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_b|1\rangle_c - |1\rangle_b|0\rangle_c\right) \tag{2}$$

(3)Alice 对粒子 a，b 进行 Bell 基测量，则 3 个粒子组成的量子态变为

$$\begin{aligned}&\frac{1}{2}\left[\left|\Psi^-\right\rangle_{ab}\left(-\alpha|0\rangle_c - \beta|1\rangle_c\right) + \left|\Psi^+\right\rangle_{ab}\left(-\alpha|0\rangle_c + \beta|1\rangle_c\right)\right]\\&+\frac{1}{2}\left[\left|\Phi^-\right\rangle_{ab}\left(\beta|0\rangle_c + \alpha|1\rangle_c\right) + \left|\Phi^+\right\rangle_{ab}\left(-\beta|0\rangle_c + \alpha|1\rangle_c\right)\right]\end{aligned} \tag{3}$$

其中 $\left|\Phi^\pm\right\rangle = (1/\sqrt{2})\left(|00\rangle \pm |11\rangle\right)$，$\left|\Psi^\pm\right\rangle = (1/\sqrt{2})\left(|01\rangle \pm |10\rangle\right)$，称为 Bell 基。

(4)利用经典信道，Alice 将其测量结果点对点地发送给 Bob。

(5)Bob 接收到测量结果并选择合适的量子门，对粒子 c 应用幺正变换，完成量子隐形传态。当 Alice 测量结果为 $\left|\Psi^-\right\rangle_{ab}$ 时，Bob 对 $-\alpha\,|0\rangle_a - \beta\,|1\rangle_a$ 应用幺正变换 $-\boldsymbol{I}$，获得量子态 $\alpha\,|0\rangle_a + \beta\,|1\rangle_a$；同理，为 $\left|\Psi^+\right\rangle_{ab}$ 时，应用幺正变换 $-\boldsymbol{Z}$；为 $\left|\Phi^-\right\rangle_{ab}$ 时，应用幺正变换 $\boldsymbol{X}$；为 $\left|\Phi^+\right\rangle_{ab}$ 时，应用幺正变换 $-i\boldsymbol{Y}$。其中，$\boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$，$\boldsymbol{Z}=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$，$\boldsymbol{X}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$，$\boldsymbol{Y}=i\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$。

2.2 无线网络 802.11i 鲁棒安全分层结构

802.11i 由两种数据链路层的加密协议 TKIP 和 CCMP 组成，其鲁棒安全分层结构分为成对密钥、组密钥。

成对密钥的作用是确保工作站与接入点之间数据的安全，由 256 位成对主密钥生成成对临时密钥；TKIP, CCMP 包含的成对临时密钥不同。TKIP 的成对临时密钥总长度为 512 位，包括 128 位 EAPOL 密钥确认密钥(KCK), 128 位 EAPOL 密钥加密密钥(KEK), 128 位临时密钥(TK), 128 位完整性校验密钥(MIC Key); CCMP 的成对临时密钥总长度为 384 位，包括 128 位 EAPOL 密钥确认密钥(KCK), 128 位 EAPOL 密钥加密密钥(KEK), 128 位临时密钥(TK)。

组密钥的作用是确保广播与组播数据的安全，由 128 位组主密钥(Group Master Key, GMK)生成组临时密钥(Group Transient Key, GTK); TKIP, CCMP 包含的 GTK 不同。TKIP 的 GTK 包括 128 位临时密钥(group temporal key), 128 位完整性校验密钥(MIC key); CCMP 的 GTK 包括 128 位临时密钥(group temporal key)。

2.3 量子纠错码基本理论

在实际传输过程量子态不可避免地出现误码，需要纠错。码 C 的最小距离 $d = d(C)$ 定义为 C 中 2 个码字之间 Hamming 距离最小值，即 $d = d(C) = \min\{d_H(u,v) \mid u,v\in C, u\neq v\}$。CSS(Calderbank-Shor-Steane)码是 1 类典型的量子纠错码，其中有 2 个 n 元经典纠错码集合：$[n,k_1]$ 线性编码集合 C_1 与 $[n,k_2]$ 线性编码集合 C_2，则 C_1 和 C_2 的对偶代码集合同时都能纠正等于与小于 $t = (d-1)/2$ 位的比特翻转和相位翻转错误。假设 $x\in C_1$，量子态 $\left|x + C_2\right\rangle$ 的表达式为

$$\left|x + C_2\right\rangle = \frac{1}{2^{k_2/2}}\sum_{y\in C_2}|x + y\rangle \tag{4}$$

其中右边之和满足按比特模 2 加的关系。

3 嵌入量子隐形传态的分层安全结构

本节设计嵌入量子隐形传态的成对密钥、组密钥层次结构，利用量子隐形传态解决数据链路层的安全；其中，嵌入量子隐形传态的成对密钥层次结构简称量子化成对密钥层次结构，见图 1；嵌入量子隐形传态的组密钥层次结构简称量子化组密钥层次结构，见图 2。

3.1 量子化成对密钥层次结构

量子化成对密钥包括量子化 TKIP 成对密钥，量子化 CCMP 成对密钥。量子化 TKIP 成对密钥编码规则是一方面包含原有的 KCK, TK, MIC key，另一方面将 128 位 KEK 编码为量子比特流，利用量子隐形传态将其发送；量子化 CCMP 成对密钥编码规则是一方面包含原有的 KCK, TK，另一方面将 128 位 KEK 编码为量子比特流，利用量子隐形传态将其发送。这样编码优点是不破坏 TKIP 和 CCMP 原先的层次结构。

3.2 量子化组密钥层次结构

量子化组密钥包括量子化 TKIP 组密钥，量子化 CCMP 组密钥。量子化 TKIP 组密钥编码规则是一方面包含原有的完整性校验密钥，另一方面将 128 位临时密钥编码为量子比特流，利用量子隐形传态将其发送；量子化 CCMP 组密钥是将 128 位临时密钥编码为量子比特流，利用量子隐形传态将其发送。

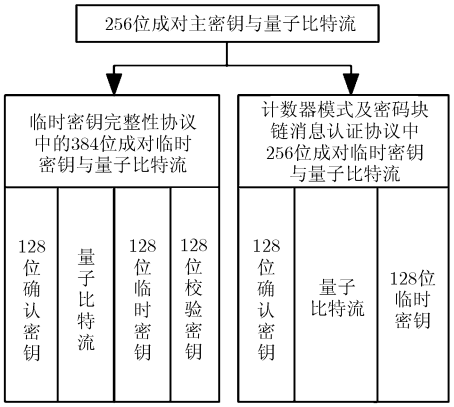

图 1 量子化成对密钥层次结构

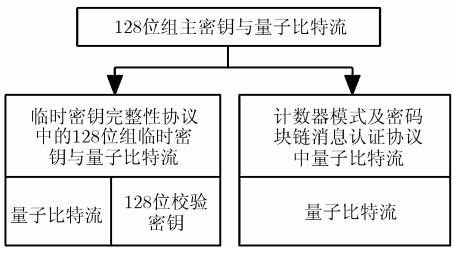

图 2 量子化组密钥层次结构

4 基于量子隐形传态的无线网络鲁棒安全通信协议

本通信协议分为初始化阶段、量子化成对密钥启动阶段、量子化成对密钥纠错阶段、量子化组密钥启动阶段、数据通信阶段、注销阶段等 6 部分；其中，申请接入的无线客户端(STAtion, STA)，接入点(Access Point, AP)，认证服务器(Authentication Server, AS)在原有功能的基础上能处理量子信息。

4.1 初始化阶段

(1)STA 关联到 AP，需要关联请求(Association Request)，关联响应(Association Response)两个数据帧，如果关联成功则继续，否则取消关联。

(2)STA 向 AP 发出启动帧。

(3)AP 收到启动帧后，回复身份请求数据帧，即向 STA 提出认证要求。

(4)STA回复身份响应数据帧，AP收到后转换成RADIUS访问请求数据帧发送给AS。

(5)AS 将 EAP 请求封装于 RADIUS 访问质询数据帧中并经过 AP 发送给 STA。

(6)STA 回复 EAP 响应数据帧，AP 收到后转换成 RADIUS 访问数据帧发送给 AS。

(7)AS 将 RADIUS 认证接受数据帧经过 AP 转换成 EAP 授权数据帧发给 STA, STA 获得使用连接端口的授权。至此，启动结束。

4.2 量子化成对密钥启动阶段

(8)AP 收到授权数据帧，启动 4 步握手协议，进行量子化成对密钥、组密钥分配工作。

(9)AP 向 STA 发出包含自身 MAC 地址(APA)、重放计数器字段值 m_1 等数据的服务器通知数据帧(Authenticator Nonce, ANonce)。

(10)STA 收到服务器通知数据帧，并从中得到重放计数器字段值 m_1。与之前关联时收到字段值 m_2 比较，$m_1 \le m_2$，STA 丢弃该数据帧，$m_1 > m_2$，STA 生成包含自身 MAC 地址(SA)等数据的客户端通知数据帧(Supplicant Nonce, SNonce)。STA 向 AP 发送 SNonce，利用 ANonce, SNonce, APA, SA 生成量子化的成对密钥，见图 3。KCK 是保证 4 步握手阶段认证与完整性保护密钥；TK 是 STA 与 AP 之间的普通加密密钥；STA 将 128 位 KEK 密钥编码成量子比特流，其表达式：$|\Psi\rangle_a^1 = \alpha_1|0\rangle_a + \beta_1|1\rangle_a$，$|\Psi\rangle_a^2 = \alpha_2|0\rangle_a + \beta_2|1\rangle_a, \cdots, |\Psi\rangle_a^j = \alpha_j|0\rangle_a + \beta_j|1\rangle_a, \cdots, |\Psi\rangle_a^N = \alpha_N|0\rangle_a + \beta_N|1\rangle_a$。其中 $|\alpha_j|^2 + |\beta_j|^2 = 1$，$N = 128$，其中 STA 手中的粒子为 a。STA 制备 128 个量子纠缠对将 KEK 编码的量子比特流传递给 AP，其中第 j 个纠缠对的表达式为：$\frac{1}{\sqrt{2}}(|0\rangle_b|1\rangle_c$

$-|1\rangle_b|0\rangle_c\big)$，并与之对应粒子 b，c 分别在 STA, AP 手中。a ,b ,c 组成的量子态为式(2)，其变形式为

$$\begin{aligned}\left|\Omega_j\right\rangle_{abc}=&\frac{1}{2}\Big[\left|\Psi^-\right\rangle_{ab}\left(-\alpha_j|0\rangle_c-\beta_j|1\rangle_c\right)\\&+\left|\Psi^+\right\rangle_{ab}\left(-\alpha_j|0\rangle_c+\beta_j|1\rangle_c\right)\Big]\\&+\frac{1}{2}\Big[\left|\Phi^-\right\rangle_{ab}\left(\beta_j|0\rangle_c+\alpha_j|1\rangle_c\right)\\&+\left|\Phi^+\right\rangle_{ab}\left(-\beta_j|0\rangle_c+\alpha_j|1\rangle_c\right)\Big]\end{aligned}\tag{5}$$

根据 2.1 小节描述的可知，STA 测量结果为 $\left|\Psi^-\right\rangle_{ab}$ 时，利用幺正变换 $-\boldsymbol{I}$，AP 获得发送量子态 $\alpha_j|0\rangle_c+\beta_j|1\rangle_c$；同理，为 $\left|\Psi^+\right\rangle_{ab}$ 时，利用幺正变换 $-\boldsymbol{Z}$，获得发送 $\alpha_j|0\rangle_c+\beta_j|1\rangle_c$；为 $\left|\Phi^-\right\rangle_{ab}$ 时，利用幺正变换 $\boldsymbol{X}$，获得 $\alpha_j|0\rangle_c+\beta_j|1\rangle_c$；为 $\left|\Phi^+\right\rangle_{ab}$ 时，利用幺正变换 $-i\boldsymbol{Y}$，获得 $\alpha_j|0\rangle_c+\beta_j|1\rangle_c$。量子态接受之后，依次利用量子纠缠对将 128 位密钥传送完毕。

4.3 量子化的成对密钥纠错阶段

(11)因为信道噪声的问题，量子态中必定出现误码，其中包括比特翻转 e_b 与相位翻转 e_p。该阶段使用 CSS 码进行纠错。当然，这种纠错码的局限是只能纠正等于与小于 t 位的误码。假设接受 128 位的量子比特串 w，其编码表达式为

$$\left|w+C_2\right\rangle=\frac{1}{2^{k_2/2}}\sum_{v\in C_2}|w+v\rangle\tag{6}$$

误码的出现有 3 种情况：第 1 种情况，比特串 w 中仅仅有比特翻转 e_b，则编码表示式为：$\frac{1}{2^{k_2/2}}\sum_{v\in C_2}\left|w+v+e_b\right\rangle$，由 $\left(w+v+e_b\right)\boldsymbol{H}_1=e_b\ \boldsymbol{H}_1$ 可知其错误的位置并纠正。第 2 种情况，仅仅有相位翻转 e_p，编码表示式变换为

$$\frac{1}{2^{k_2/2}}\sum_{v\in C_2}(-1)^{(w+v)\cdot e_p}|w+v\rangle$$

将 128 位量子比特分别进行 $\boldsymbol{H}$ 门，$\boldsymbol{H}_2^{\mathrm{T}}$ 门操作，完成相位翻转比特的检测和纠正。其 $\boldsymbol{H}_1$，$\boldsymbol{H}_2^{\mathrm{T}}=(\boldsymbol{h}_1^{\mathrm{T}},\cdots,\boldsymbol{h}_m^{\mathrm{T}})$，$m=n-\dim C_2$ 是可存在的好码，见文献[11]。第3种情况，比特串 w 中比特翻转 e_b 与相位翻转 e_p 均存在，则编码表示式为

$$\frac{1}{2^{k_2/2}}\sum_{v\in C_2}(-1)^{(w+v)\cdot e_p}\left|w+v+e_b\right\rangle$$

先进行比特误码纠错，再进行相位误码纠错。

(12)AP 将纠错完成后的码解码为经典信息，返回量子化成对临时密钥确认数据帧。至此，量子化的成对密钥结束启动。

4.4 量子化组密钥启动阶段

(13)量子化组密钥启动与量子化成对密钥是相同算法。

STA 收到确认数据帧后，AP 将 128 位组临时密钥编码成量子比特流，其表达式：$|\Phi\rangle_{a'}^1=\alpha_1|0\rangle_{a'}+\beta_1|1\rangle_{a'}$；$|\Phi\rangle_{a'}^2=\alpha_2|0\rangle_{a'}+\beta_2|1\rangle_{a'},\cdots,\ |\Phi\rangle_{a'}^k=\alpha_k|0\rangle_{a'}+\beta_k|1\rangle_{a'},\cdots,|\Phi\rangle_{a'}^M=\alpha_M|0\rangle_j+\beta_M|1\rangle_j$。其中 $|\alpha_k|^2+|\beta_k|^2=1$，$M=128$；AP 拥有的粒子为 a'，粒子 b'，

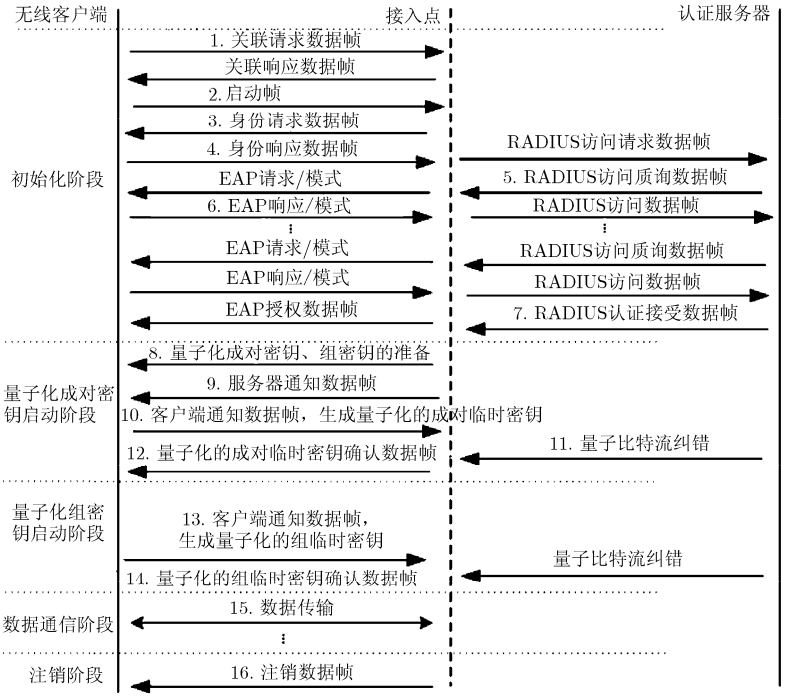

图 3 协议流程图

c' 分别在 AP, STA 手中。粒子 a'，b'，c' 组成的量子态为 $\left(\alpha_k|0\rangle+\beta_k|1\rangle\right)_{a'} \otimes\frac{1}{\sqrt{2}}\left(|0\rangle_{b'}|1\rangle_{c'}-|1\rangle_{b'}|0\rangle_{c'}\right)$，依然进行幺正变换，获得传递过来的 128 位量子比特流。对于这一部分也要进行量子信息的纠错，具体执行参照 4.3 节。纠错完成后，STA 将量子比特流解码为组临时密钥，这样利用量子隐形传态保证广播密钥的安全。

(14)STA 与 AP 之间的认证结束，生成量子化的组临时密钥确认信息，成对临时密钥和组临时密钥均装载成功。

4.5 数据通信阶段

(15)STA, AP 的成对临时密钥和组临时密钥都是崭新的，随之进行数据传输。

4.6 注销阶段

(16)STA 数据传输结束后，向 AP 发送注销数据帧，AP 的授权端口恢复成未授权状态。

本协议与经典的无线网络通信协议不同，用量子隐形传态传输成对临时密钥和组临时密钥，用经典信息传递 KCK, TK, MIC key, group MIC key，通过两部分分别进行传输，减少网络通信时延，降低经典信道负担。

上面研究的均是理想情况，在现实情况中 Bell 测量有一定的效率，比如现有的测量技术只能区分 3 个 Bell 态，效率为 3/4，而光子在信道中传输时链路有损耗，探测器也有损耗。假设所有的损耗加在一起，传输效率为 η，那么实际上我们协议中使用的“128 个纠缠对”是不够的，应该是 $128/\eta$ 个纠缠对才行。总之在实际系统中实现时，要考虑损耗和探测效率因素，使用的纠缠对要足够多，一般远大于 128 个。

5 安全性分析

下面从 4 个方面证明协议的安全性。

5.1 物理攻击 —— 伪装 AP 攻击模式

防范窃听者的前提是 AP 作为可信接入点，但是，AP 被伪装的可能性是存在的。因为无线网络中 IEEE802.11b 协议 STA 向 AP 认证是单方向的，STA 无法处理 AP 的真伪。假设窃听者将可信的 AP 的安全功能全部关闭，构建非法的 AP, STA 可以在非法的 AP 的帮助下，解密式(5)中的信息；从这一点单独来看，伪装 AP 的物理攻击是可以成功的。但是，从式(3)中分析可知，要得到式(5)中的信息，必须在 STA 的 Bell 态的测量操作帮助下才行，如果攻击者不但控制了 AP，而且又控制了 STA，是没有讨论意义的。所以，窃听者在没有 STA 的协助下，是无法得到相关合法信息。此外，量子隐形传态本身就是安全的。因为 STA 是与 AP 间共享了纠缠态，那么 STA 的量子态一定传给了 AP，伪装 AP 没有与 STA 共享量子态，所以一定收不到 STA 传来的量子态。

5.2 针对 4 次握手协议的 DoS 攻击模式

DoS 攻击是无线网络中严重的攻击方式，目的是使无线网络的服务丧失其可用性，攻击原理如下：AP 与 STA 在发送关联请求，关联响应两个数据帧时，均包含 RSN Information Element 字段，这个字段中有加密、认证、密钥管理模式等信息，攻击者可以从中伪造关联请求，作为合法的报文传输。因为本协议中在成对密钥、组密钥中增加量子隐形传态认证部分，不管攻击者伪造的关联请求再理想，如果没有量子隐形传态授权，是无法开启受控端口的。

5.3 窃听者作为中间人的攻击模式

假设窃听者在 STA 与 AP 的量子化成对密钥通信过程中，截取光子信息，对 STA 与 AP 两者分别进行欺骗，即 STA 自我认为是与合法的 AP 进行通信，而 AP 自我认为与合法的 STA 进行通信。由于窃听者无法获得正确的 ANonce 信息，并从中无法得到正确的重放计数器字段值 m_1, STA 会一直丢弃该数据帧，窃听者作为中间人是无法获取通信信息的；同理，STA 向 AP 发送的量子化的成对密钥，窃听者作为中间人截取光子信息，将自己的非法信息发送给 AP，但是没有正确的 SNonce 信息，AP 是无法解密该信息的。所以，采用中间人的攻击模式，窃听者是无法得到相关合法信息。

5.4 流量注入的攻击模式

存在于有线网络通信中的帧欺骗在无线网络中也是同样存在，而且由于 802.11 协议使用电磁波介质，将更有利于窃听者利用合适的设备伪造 802.11 协议接口的 MAC 地址，在无线网站通信的数据流中混入非法的指令代码，实现流量注入攻击。而本协议在数据流中提供了量子密钥加密部分，窃听者常规的“0”，“1”代码在量子密钥加密部分是无法执行的，在加密层面上防范了流量注入攻击模式。

6 结束语

本文提出了基于量子隐形传态无线网络鲁棒安全通信协议，在密钥层次结构中嵌入量子隐形传态，不需要变动用户、接入点、认证服务器这些基础网络设备，只需增加相关的生成纠缠对的设备即可进行密钥认证工作，在理论方面进行了较完备的证明。当然，本文仅仅从理论层面进行研究，下一步将继续深入在实验层面的研究，其中包括器件与技术方面的研究。

参 考 文 献

[1] Yang Guo-min, Huang Qiong, Wong D S, *et al.*. Universal authentication protocols for anonymous wireless communications[J]. *IEEE Transactions on Wireless Communications*, 2010, 9(1): 168–174.

[2] Perrig A, Szewczyk R, Tygar J D, *et al.*. SPINS: security protocols for sensor networks[J]. *ACM Wireless Network*, 2002, 8(5): 521−534.

[3] Zhou Nan-run, Cheng Hu-lai, and Liao Qing-hong. Three-party stop-wait quantum communication protocol for data link layer based on GHZ state[J]. *International Journal of Theoretical Physics*, 2013, 52(3): 811–819.

[4] Lü Xin, Ma Zhi, and Feng Deng-guo. Quantum secure direct communication using quantum calderbank-shor-steane error correcting codes[J]. *Journal of Software*, 2006, 17(3): 509–515.

[5] Nielson M and Chuang I. Quantum Computation and Quantum Information[M]. Cambridge: Cambridge University Press, 2000: 593–602.

[6] Bennett C H, Brassard G, Crépeau C, *et al.*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. *Physical Review Letters*, 1993, 70(13): 1895–1899.

[7] Ekert A K. Quantum cryptography based on bell's theorem[J]. *Physical Review Letters*, 1991, 67(6): 661–663.

[8] Ma Hong-yang, Chen Bing-quan, Guo Zhong-wen, *et al.*. Development of quantum network based on multiparty quantum secret sharing[J]. *Canadian Journal of Physics*, 2008, 86(9): 1097–1101.

[9] 周南润, 曾宾阳, 王立军, 等. 基于纠缠的选择自动重传量子同步通信协议[J]. 物理学报, 2010, 59(4): 2193–2199.
Zhou Nan-run, Zeng Bin-yang, Wang Li-jun, *et al.*. Selective automatic repeat quantum synchronous communication protocol based on quantum entanglement[J]. *Acta Physica Sinica*, 2010, 59(4): 2193–2199.

[10] Gong Li-hua, Liu Ye, and Zhou Nan-run. Novel quantum virtual private network scheme for PON via quantum secure direct communication[J]. *International Journal of Theoretical Physics*, 2013, 52(9): 3260–3268.

[11] Calderbank A R and Shor P W. Good quantum error-correcting codes exist[J]. *Physical Review A*, 1996, 54(2): 1098–1106.

马鸿洋：男，1976 年生，博士，副教授，研究方向为无线网络安全、量子网络.

王淑梅：女，1975 年生，研究生，高级工程师，研究方向为网络通信安全、量子信息技术.

范兴奎：男，1970 年生，博士，副教授，研究方向为网络编码理论.