无线通信安全量子加密新协议

文献标识码： A

1 简介

随着信息技术的发展无线网络已普遍进入家庭、 办公室和企业当中，无线网络已经能够在移动载体上进行高速高质的信息交换。但与之相关的安全问题也成为重要的关注话题。 在本文中采用一种新方法，即在 802.11 网络上利用量子加密法进行密钥分配。

由于无线通信使用无线电波， 因此比有线通信更易受到截获和攻击。 随着无线通信服务越来越普遍， 目前无线协议和加密方法存在着很大的安全风险。 基于物理学原理， 量子加密允许两个远程双方绝对安全地进行密钥交换。 海森堡原则认为， 成对的物理实体是通过以下方式联系在一起的： 测量一个实体的同时阻碍了观察者测量另一个实体。 所以当偷听者截取一个光子时一定会改变那个光子上的编码信息，这样就可以检测到任何安全漏洞。

我们采用光子的状态来传输密钥源，用量子加密产生和分配密钥，这种方法叫做 QKD。现在已经有一些 QKD协议了，如 BB84, B92和六态。其中 BB84在实际网络中应用最为广泛。在我们的研究中，采用了 BB84的变种协议 SARG04。同时，因为距离比较小，噪声等环境条件对光子传输的影响变得非常低。 所以量子加密更适用于 IEEE802.11 无线局域网。 802.11 网络一般用在咖啡

厅，机场和会议大厅等地方。 802.11 网络提供了用户和网络设备之间视距路径， 而视距路径是量子加密的关键要求之一； 另一方面，使用 802.11 网络需要与服务提供方之间有安全的通信路径。量子加密可以为 802.11 无线网络提供高度安全的数据通信。因此研究在 802.11 无线局域网中采用量子加密是很有意义的。

2 IEEE 802.11i 标准

2004 年 IEEE802.11 标准修正为 IEEE802.11i 。IEEE802.11i 有两类安全算法：鲁棒安全网络关联（ RSNA）和过渡安全网络（TSN） 。 IEEE802.11i 中采用两种新的机密算法处理两种密码，分别为暂时密钥完整性协议（ TKIP）和计数器模式 /CBC-MAC 协议（CCMP），并且将认证和密钥管理分开，采用 IEEE802.1x 和共享前密钥进行认证。 IEEE802.1x 提供了有效的框架，用于认证、管理密钥和控制用户流量以保护大网络。 IEEE802.11i 采用可扩展的认证协议（ EAP），从而可接纳多样化的认证机制。

图 1 RSN 关联， IEEE802.1X 认证和密钥建立过程

802.1x 的认证过程发生在三个要素之间。认证者或者访问点只允许由认证服务器授权的申请方访问网络。图 1 展示了 RSN 连接、IEEE802.1x 认证和密钥建立过程。 图 1 的步骤 1 到步骤 6 展示了 IEEE802.11 连接和认证过程。 一旦 IEEE802.11 连接完成，IEEE802.x 认证过程开始了，如图 1 的步骤 7 到 13 所示。

3 无线网络的 QKD 技术

现在私有 / 公共密钥加密中最主要的问题是密钥的安全分

配。量子力学正好能提供这样一个解决方案。　　量子加密使密钥分配“绝对安全”。　对比传统的公共密钥加密法，　　量子加密的安全性建立在量子力学的基础上。　量子加密采用了量子物理学的基本原理，即无人能在不引入干扰的情况下，　　测量一个携带信息并任意偏振的光子的状态。传统的密钥分配总是处于被动监视状态，合法的用户无法意识到入侵行为的发生。　　然而在量子力学中，　任何入侵行为将产生干扰进而可以被检测出。　　因此，无线密钥分配中使用 QKD技术在数据安全性方面就占据极大的优势。

无线网络中一个主要的安全问题是验证数据通信中参与方信息的真实性。这可以通过交互认证完成，　即双方进行相互认证。在 802.11i 网络中有两处需要交互认证。　第一，选择一个正确的EAP类型例如 EAP-TLS/EAP-TTLS，能在 IEEE802.1x 认证过程提供交互认证。第二，　IEEE802.11i 的四向握手协议，交互认证发生在第二和第三消息上。　在四向握手协议的第二个消息中，　认证方接收来自申请方的回应和　MIC。认证方通过检测接收到的　MIC和计算好的 MIC验证申请方。在第三个消息中，　认证方发送计算好的 MIC到申请方，申请方检测 MIC验证认证方，　交互认证过程就此完成。

4 提出的协议

在研究中我们特别关注　802.11i 网络中交互认证这个阶段。因此，利用 EAP类型，将 QKD引入 80211i 网络中。为了使 QKD更好地匹配无线通信，我们的目标是在　　802.1x 认证完成后立刻

引入量子密钥传输。协议如图 2 所示。

在 IEEE802.1x 认证末端，申请方和认证方都持有 PMK。如图 1 的步骤 13 所示，802.1x 协议的最后一个信息是 EAPOL信息，该信息将 EAP密钥从认证方传送给申请方。由于双方在这个阶段交互认证，因此这个信息一定是真实的。我们将这个信息作为量子传输的起始点。通过这个方式可以安全地开始交换量子密钥。只要申请方一接收到 EAP密钥消息，通信就转换到量子通道上。

图 2 提出的协议

申请方通过向认证方发送一系列光子，开始进行 SARG04密钥分配。一旦光子传输完成，通信就回到传统的无线信道，随后就完成了 SARG04量子密钥交换过程，如图 2 的步骤 3 到 6 所示。

在 SARG04协议最后密钥的恢复过程中，将会遗漏一些传输比特。我们最终想让 QKD密钥的长度等于 PTK的长度。对于 CCMP, PTK 是 256 比特，而 TKIP 占 PMK的 384 比特。必须确保导出的 Q-密钥的比特数大于或等于 PTK的比特数。所以在这一阶段，去除 Q-密钥额外的比特，使之与 PTK长度相等，将简化后的 Q-密钥作为 PTK。一旦得到了 PTK，就可以利用 PRF得到包含其他所有密钥的密钥层。从 PTK中，可以剥离得到 KEK，KCK和 TK，而从 KCK可以计算出 MIC。利用 MIC，就可以完成后续协议信息的交互认证。为了简化无线网络在这一阶段的操作，申请方利用 MIC及 PMK中相同长度的第一组比特进行 XOR操作，称此时的 MIC为量子 MIC（Q-MIC），并能得到如下协议：

Q-MIC=（MIC）XOR（PMK中与 MIC长度相同的第一组比特） 。

申请方然后向认证方发送 Q-MIC，如图 2 中的步骤 7。一旦收到 Q-MIC，认证方就验证 Q-MIC。如果两者匹配，申请方就通过了认证。认证方将认证成功的消息和 Q-MIC一起发送给申请方，如图 2 的步骤 8。申请方通过 Q-MIC来验证认证方，这样完成交互认证的过程。从此时起，双方开始用 TK进行数据加密和安全通信，如果需要也使用 GTK进行多点传送。

有研究显示 BB84和之后的 SARG04都易受到中间人攻击。 即使申请方和认证方在 EAP认证过程中进行了交互认证， 如果窃听者得到 EAP密钥消息，窃听者就能向认证方伪造一个光子传输。假如得到 EAP密钥消息， 窃听者立刻向认证方发送伪造的光子传输（图 2 的步骤 2）。一旦通过 SARG04过程得到了 Q-密钥，申请方就向认证方发送 Q-MIC（如步骤 7）。认证方能够检测这个 Q-MIC值，因为该 Q-MIC值能产生自己的 Q-MIC。这样任何伪造的 SARG04过程在此阶段都能够被识别出来。

5 结论

对比传统的密钥交换方式， 量子加密的优点是在很大程度上信息交换是安全的，不用考虑很难的数学问题。在研究中，利用 QKD提供的“ 绝对安全性 ”，将 QKD技术融合到 802.11i 无线网络中。对于小的无线网络，例如 IEEE802.11，量子加密可以提供更安全的数据通信。 考虑到 QKD和无线网络视距问题， 我们讨论了 3 种模型，即：较不分散的视线短距离室内传播环境，对数

正态分布通道，准　LOS链路。这　3 种模型都可以由　Nakagami 分布通道和高斯分布通道利用高分散户外　　NLOS传播环境而形成模型。