无线通信研究
2019 年 8 月第 1 卷第 1 期

Security of key distribution protocol

Guo Min

Zhengzhou University, Zhengzhou

Abstract: Secure wireless network data transmission requires not only encryption and decryption algorithms, but also the support of secure key distribution protocol. A key distribution protocol (KDP) distributes the key to the message bearer in a secure and efficient manner. There is no secure key distribution protocol, even if the use of a powerful encryption/decryption algorithm, the whole system will exist insecure factors. The commonly used encryption/decryption algorithms are either based on public key or private key. And the private key password system is fast, but the security performance is poor. This paper discusses the security key distribution protocol in wireless network, which can improve the security of the system.

Key words: Wireless networks; Safety; Key distribution protocol

Received: 2019-07-19; Accepted: 2019-08-02; Published: 2019-08-07

文章引用：郭鸣. 密钥分配协议的安全性探讨 [J]. 无线通信研究，2019，1 (1)：16–22.
https://doi.org/10.35534/rwc.

密钥分配协议的安全性探讨

郭　鸣

郑州大学，郑州

邮箱：m_guo293@qq.com

摘　要：安全的无线网络数据传输，不仅需要加密、解密算法，还需要有安全的密钥分配协议的支持。一个密钥分配协议（简称 KDP）是将密钥以一种安全、有效的方式分发给消息传递者。没有安全的密钥分配协议，即使使用了强有力的加 / 解密算法，整个系统也会存在着不安全的因素。常用的加 / 解密算法或是基于公钥，或是基于私钥（公钥密码系统有较好的安全性，但速度慢； 而私钥密码系统速度快，但安全性能差）。本文探讨无线网络中安全密钥分配协议，可提高系统的安全性。

关键词：无线网络；安全；密钥分配协议

收稿日期：2019–07–19；录用日期：2019–08–02；发表日期：2019–08–07

https://doi.org/10.35534/rwc.

与传统网络相比，无线网络具有节点分布稠密，存储空间和计算能力有限，带宽有限，周边环境恶劣，易遭受物理破坏等特性，这使得在无线网络中得到较高的安全性变得非常困难。同时无线网络还面临来自各方面的攻击，归纳起来主要有如下两大类：从直接面临的攻击进行分类和从网络分层的观点进行分类。鉴于无线网络面临的诸多威胁，必须要为无线网络设计合适的安全防护机制，以实现无线网络的安全通信，密钥协商策略在此过程中起了一个基础的、举足轻重的作用。

1　密钥分配概述

密钥分配是密钥管理中最大的问题。密钥必须通过最安全的通路进行分配。例如，可以派非常可靠的信使携带密钥分配给互相通信的各用户。这种方法称为网外分配方式。但随着用户的增多和通信量的增大，密钥更换频繁（密钥必须定期更换才能做到可靠），派信使的办法将不再适用。这时应采用网内分配方式，即对密钥自动分配。

密钥的网内分配方式有两种。一种分配方式是在用户之间直接实现分配。例如 A 用密钥 K 对报文加密后发给 B，只有在 B 也具有密钥 K 的情况下才能对此密文进行解密。但 A 怎样才能使 B 得到密钥 K 呢？直接在网上发送密钥 K 是很不安全的。因此必须用另一个密钥 “K” 对密钥 K 加密后才能在网上发送。但密钥 “K” 又怎样传送给网络上的 B 呢？这就是传统密钥分配中最困难的问题。另一种分配方法是设立一个密钥分配中心 KDC，通过 KDC 来分配密钥。后一种方法已成为使用得较多的密钥分配方法。

在公开密钥体制中，如果每个用户都具有其他用户的公开密钥，就可以实现安全通信。看来好像可以如电话簿那样公布用户的公开密钥。其实不然。由于用户经常更换，由于需要更换已暴露的密钥，由于需要周期性地更换密钥以减少密钥暴露的机会，密钥更换，增加和删除的频度是很高的。另一方面，虽然公开密钥不需对任何人保密，但公开密钥的完整性却是必须保证的。如果公开密钥被篡改或替换，则安全性就得不到保证。分配大量的 “电话簿” 而又能保证其完整性，是一项十分复杂的工作。随着开放系统的不断扩大，这种密钥 “电

话簿“将变得无法管理。此外，公开密钥相当长，人工密钥输入相当麻烦且易出错。所以，我们仍然要对它进行网内密钥分配。

2　无线网络中的密钥分配协议

在无线节点部署之前，由离线的服务器将密钥或者能产生密钥的信息预先配置在节点中，这种密钥管理的方法叫做预分配密钥管理。当前主要的密钥分配协议都可以认为属于预分配密钥管理协议，各个节点之间利用预先保存在其节点的秘密信息，自组织、分布式建立密钥。由于节点存储和能量的限制，预分配密钥管理协议必须考虑节省存储空间和减少通信开销。最简单的密钥分配协议就是所有节点共享一个密钥，但是如果一个节点被捕获并取出密码，安全将不复存在。最安全的密钥分配协议是预先给每两个节点生成一个对偶密钥，把这些密钥保存在节点中，但是由于网络规模巨大，节点存储器非常受限，每个节点需保存 n ~ 1 个密钥，可扩展性非常差，只能用于小规模网络。

Eschenauer、Gligor 引入随机图理论，提出了基本的随机密钥预分配协议（简称 EG 协议），在布置之前每个节点从一个大的密钥池中选取少数的密钥保存在存储器中，节点布置好后只要两个邻居节点至少共享一个密钥，就采用这个密钥作为对偶密钥，但这个密钥很容易被破获，在实际应用中仍存在着很大程度的漏洞。Chan、Perrig、Song 在 EG 协议基础上，提出了 q 复合模式、多路增强模式，以一定代价，有效地改进了 EG 协议的安全性能。当敌人捕获很少的节点时，q 复合模式会体现出更好的安全性能；但是随着被捕获节点的增多，q 越大，性能反而变差，q 复合模式是以额外的计算负载为代价，提高安全性能，并且只适合只有少数节点被捕获的场合。多路增强模式以额外的通讯负载为大家比较好地提高了安全性能，但多路径增强密钥模型以增加通讯开销为代价，提高了安全性能，是不是划算需要看具体的应用。Blom 密钥预分配协议给出了另一种密钥对的分布模型，分析表明，在相同存储空间的支持下，模型效果可以达到让网络拓扑实现安全连通，且该模型比随机密钥对模型表现更好，但是对节点的资源开销占用极大，计算开销较大。在 EG 协议基础上，Du、Deng 等结合 Blom 协议，Liu、Ning 结合 Blundo 的多项式密钥分配，分别提出两种非常类似的多重

https://doi.org/10.35534/rwc.

空间密钥预分配协议。但是这两种协议都需要大素数的模余运算，对节点要求高，但计算负载较大。

基于二元 t 次多项式的密钥对模型是以 C. Blundo 等在 1993 年发表的“Perfectly — secure key distribution for dynamic conferences”中提出了用多项式方法解决密钥预分布问题为基础的密钥对分配模型。原始文献中提供的算法是解决组密钥预分布模型的算法，其计算开销太大不适合无线网络，但是其密钥对分配模型部分却可以被无线网络所利用。基于多项式的密钥分配模型非常类似于 Blom 协议，同样具有 λ 门限特性。

C. Blundo 提出的密钥对生成模型是根据定义在有限域 F（q）上的一个二元 t 次多项式 $f(x, y)$，$f(x, y)$ 需要满足对称特性，即 $f(x, y) = f(y, x)$ 每个节点根据自己惟一的 ID 值计算与其他节点 ID′ 之间的共享密钥对 f（ID，ID′ ）。根据对称特性，两个节点根据同一多项式计算出来的通信密钥永远是相同的。该模型需要每个节点保存一个以各自节点为参数的二元 t 次多项式 f（ID，x），ID 为本节点编号，f（ID，x）的值表示与邻近节点通过计算获得的共享通信密钥对值。该模型显示各节点在与邻居节点交换建立通信密钥过程中，除了广播自己的节点 ID 以及进行相应计算以外，不增加任何通信开销，保证每两个通信节点间有独立的安全链路，提高破解难度。从理论上计算，该模型在被俘节点个数不超过 t 的前提下其安全链路不会被完全破解，不会泄露无线网络的任何信息。

二元 t 次多项式一般如下定义：

$f(x, y) = a_{t0}x^t + a_{(t-1)1}x^{(t-1)}y + \cdots + a_{1(t-1)}xy^{(t-1)} + a_{0t}y^t$ 要求保证每个 a_{ij} 完全不同且对每个节点完全保密。每个节点中存储一个二元 t 次多项式，所有的多项式系数 $_{0t}$，$a1_{(t-1)}$，…，$a_{(t-1)1}$，a_{t0} 均保密，只保存由本节点 ID 计算后的一元 t 次多项式 f（ID，x），通过广播得到的邻居节点的 ID′ ，将由多项式计算获得的 f（ID，ID′ ）作为两个节点之间通信密钥。当敌方捕获网络中的一个节点时，则可以通过这个节点计算出该节点与其他节点之间全部的通信密钥，但不能计算出其他节点之间的通信密钥； 只有当敌方俘获到 t 至 t 个以上节点时，可以通过解方程组计算出所有

不可知的 a_{0t}，$a_{1(t-1)}$，…，$a_{(t-1)1}$，a_{t0} 参数，最终得到完整的二元 t 次多项式 $f(x, y)$，获取所有节点之间的通信密钥，安全链路被完全破解。该方式仍然存在一定漏洞，当一个节点被破获后，该节点与其他节点的通信密钥被全部破获，因此课题从密钥环出发，重新对多项式密钥分配协议进行设计。每个节点均从密钥池中分配一定数量的密钥构成密钥环，同时分配给每个密钥相应的多项式，不同的密钥其对应的多项式是完全不同的。只有当与邻居节点具有相同的密钥值时，才使用相应的多项式进行计算获得与邻居节点的通信密钥，因此当敌方在破获一个节点以后，如果不知道与邻居节点相同的密钥值，则无法计算出两节点之间的通信密钥，更大程度地提高了无线网络通信的一条安全链路的破解难度。

在无线网络中使用多项式密钥分配协议，当攻击者捕获 Nc 个节点时，其中存在有 i 个相同密钥的概率如下式：

$$P_i = \frac{N_c!}{(N_c-!)!i!}\left(\frac{s'}{s}\right)\left(1-\frac{s'}{s}\right)^{(Nc-i)} \quad (1)$$

由上式得，节点密钥环中一个密钥被捕获的概率为

$$P_{cd} = 1-\sum_{i=0}^{t} P_i \quad (2)$$

因此，在 Nc 个节点被捕获的情况下，无线网络安全链路被破解的概率如下式所示：

$$P_{becracked} = P_{cd}^{s'^{*}\ N_c}\left[\left(1-\frac{s'}{s}\right)\right] \quad (3)$$

3 结语

由于无线网络独有的特性使得其要达到较高的安全性能变得十分困难，需要面临来自各方面的攻击。为了实现节点间的安全通信通常在节点部署之前，预先进行密钥分配过程。二元 t 次多项式密钥分配协议便是在已有密钥分配协议上发展起来，针对无线网络存储空间、资源和计算能力有限的特性，减少了节点间的通信消耗。

https://doi.org/10.35534/rwc.

参考文献

[1] Eschenauer L, Gligor V D. A key management scheme for distributed sensor networks. in Proceedings of the 9th ACM conference on Computer and Communications Security [C]. Washington DC, 2002.

[2] Blundo C, Santis A D, Herzberg A, et al. Perfectly Secure Key Distribution for Dynamic Conferences[C]. Academic Press, Inc. 1998: 1-23.

[3] Du W, Deng J, Han Y S. A key management scheme for wireless sensor networks using deployment knowledge [C]. Twenty — third Annual Joint Conference of the IEEE Computer and Communications Societies, 2004.

[4] 郎为民, 程文青, 杨宗凯. An efficient authentication scheme based on one-way key chain for sensor network [J]. Journal of Harbin Institute of Technology, 2007, 14 (6): 756-760.

[5] Deng, Jing. A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks [C] // IJITEE, 2003.

[6] Wadaa A, Olariu S, Wilson L. Scalable cryptographic key management in wireless sensor networks [C] / 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings. IEEE, 2004.

[7] Du W, Deng J, Han Y S, et al. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge [C] // Joint Conference of the IEEE Computer & Communications Societies. IEEE, 2004.

[8] 贾小华. 无线传感器网络中的查询路由和数据采集最优化 [C] // 科技、工程与经济社会协调发展——中国科协第五届青年学术年会论文集, 2004.

[9] 梁韦华, 于海斌. 无线传感器网络物理层协议的研究现状 [C] // 中国仪器仪表学会第六届青年学术会议论文集, 2004.