无线 Mesh 网络中多服务器的门限认证系统构建*

刘东升[1]，杨亚涛[2,3]
（1. 浙江工商大学计算机与信息工程学院，浙江 杭州 310018；
2. 北京邮电大学网络与交换国家重点实验室信息安全中心，北京 100876；
3. 北京电子科技学院，北京 100070）

摘 要： 在无线 Mesh 网络中，传统的集中式 AAA 认证模式很容易由于遭受 DOS 攻击或者被恶意者的破坏而导致服务瘫痪，为了解决该问题，基于 Asmuth－Bloom 门限机制，提出了多服务器的无线 Mesh 网络门限认证系统模型，设计了具体的无线接入和认证流程。在该系统中，只有认证服务器组中的成员才可以执行有效的认证过程，同时，只有当认证服务器组中的 n 个服务器中有不少于 t 个服务器才能恢复共享密钥 K，这样可以避免假冒攻击和防止单个服务器被攻陷。分析结果表明，通过所计设的门限认证系统，保证了接入认证过程的有效性，提高了系统的安全性能，为无线 Mesh 网络的接入认证提供了一条有效解决思路，具有较高的实际应用和参考价值。

关键词： 网络安全；认证；门限技术；无线 Mesh 网络；认证服务器组
中图分类号： TP393.08 **文献标识码：** A **文章编号：** 0529-6579（2008）06-0100-04

无线 Mesh 网（Wireless Mesh Network，WMN）是一种多跳、具有自组织和自愈特点的宽带无线网络，是一种高容量、高速率的接入网络，可以认为，WMN 是一种由无线链路连接路由器和终端设备而构成的无线网络，是 Internet 的无线版本[1]。作为一种新型网络结构形态，Mesh 结构已被纳入到 802.16－2004，802.16e 和即将制定的 802.11s 标准中。

目前，对 Mesh 网络安全问题的研究还很不成熟，基本的安全机制并没有很好的定义或规范[2]。针对无线 Mesh 网络的认证模式，目前大多倾向于采用集中式的单个 AAA 认证服务器的机制，但在这种传统的集中式的 AAA 认证模式下，服务器容易遭受攻击而瘫痪，进而引起网络服务的功能中断；也可能会造成未经授权的移动用户接入网络，引起网络资源的滥用。因此，多个 AAA 服务器的认证模式便成为一种可能的解决思路和途径。

国内外学者对于无线 Mesh 网络中的认证机制提出了不少可行的解决办法。Anand R. Prasad 在文献［3］中分析了家庭环境下基于网状无线局域网的安全问题，利用复活雏鸭安全策略模型，解决了无线家庭局域网络（WHAN）所关心的授权、认证、可管理性等相关问题，但该方案只适用于小型家庭用户，在规模较大的社区，网络性能降低很快。文献［4］为无线 Mesh 网络设计了一个灵活的混合型结构，采用了 AAA 结构作为接入认证模式，在此多跳结构中，终端用户可以通过 WiMax 技术从 802.16 基站接入高速的无线网络。这些认证方案都是基于单认证服务器的模式，在实际应用中，一旦这个唯一的认证服务器不能工作，整个网络就面临瘫痪的危险。为了提高大规模复杂无线 Mesh 网络的系统安全性，防范恶意入侵者对单个认证服务器的破坏，可以尝试构建多服务器的认证系统。

1 传统的 Mesh 认证模式

无线 Mesh 网络（WMN）主要采用混合型网络结构，WMN 中主要存在着以下网络实体：移动节点（Station，STA）、Mesh 接入点（Mesh Access Point，MAP），Mesh 端点（Mesh Portal，MPP）。与传统点对多点网络不同，WMN 中的每个节点都具备二层（MAC 层）路由选择的功能，而且每个节点只与其临近节点进行通信，一般情况下，移动的 STA 可以通过 MAP 接入由 MPP 组成的骨干 Mesh 网，通过 MPP 的中转处理再接入 Internet 或其他网络。

文献［5］分析了无线 Mesh 接入网络中的中心结构、分级结构和分布式结构，指出分级认证结

* 收稿日期：2008－09－10
基金项目：浙江省科技计划资助项目（2007C24004）；北京电子科技学院信息安全与保密重点实验室资助项目
作者简介：刘东升（1974年生），男，博士研究生；通讯联系人：杨亚涛；E-mail：lds1118@zjgsu.edu.cn

构在移动接入中具有较高效率；在目前实际应用中，也多采用集中式的单个认证服务器的混合结构，该结构可扩充性好，网络规模不受限制。然而，单认证服务器很容易由于 DOS 攻击或者是恶意者的破坏变得不可用，这是实际中潜在的安全隐患。

2　多服务器的门限认证系统构建

Desmedt 和 Frankel 在文献［6］中介绍了门限签名理论，在一个（t，n）门限签名机制中，一个合法的签名只能由 n 个参与者中 t 或者大于 t 个产生，当 $t-1$ 或者更少的参与者无法重构合法签名，t 称为方案的门限值。根据这个理念，我们可以采用门限机制来设计多 AAA 服务器的门限认证系统，也就是说，在此认证系统中，n 个认证服务器中有 t 或者大于 t 个服务器联合，才能恢复出共享密钥 K，才能同意用户的网络接入请求。目前被广泛使用的门限机制是基于多项式的 Shamir 门限体制[7]，可是在无线 Mesh 网络中，多项式的计算繁琐，对网络资源消耗较大；而另外一种实用的基于中国剩余定理（Chinese Remainder Theory，CRT）的 Asmuth－Bloom 门限体制[8]比 Shamir 门限体制计算量小，在实际网络中对网络资源消耗较少，可以提高网络的工作效率[9-10]，所以本文采用基于 Asmuth－Bloom 门限机制来构建无线 Mesh 网络的多认证服务器的门限认证系统。

基于 Asmuth－Bloom 门限机制构建的多服务器的无线 Mesh 网络门限认证系统如图 1 所示。为了简化问题，在图 1 中，我们将 MPP 组合成的节点群，作为一级结构，类似于骨干网，采用高频率通信；将簇头节点 MPP 和簇内成员 MAP 组成的结构为二级结构，采用较低频率通信。AS－1、AS－2、AS－3…AS－N 组成了认证服务器组，MPP 具有网络路由器和网关两种功能，在下面的具体流程描述中，用户 STA 从 AP 接入网络，最后由认证服务器组（ASG）发出接受或者拒绝认证的消息。

3　认证流程设计

STA 接入由 n 个认证服务器组成的认证服务器组（ASG）的无线 Mesh 网络时，首先在 CA 处进行初始化注册，进而可以获得以下信息：一个对称密钥 K，n 个子秘钥份额 K_i，以及 n 个认证服务器的数字证书。

门限认证系统设计的基本思路是：用户首先把子秘钥 K_i 分发给认证服务器组（ASG）中的 n 个认证服务器，n 个认证服务器中的 t 个或者大于 t 个可以恢复出共享秘钥 K；随后用户把子消息 N_j 分别发送给参与合成共享秘钥的 t 个认证服务器，他们把子消息 N_j 按照一定的算法 $f(R)$ 合成消息 N，进而保存到 ASG 中特定的代理 AS－P；然后，用户把子消息按照同样的合成算法 $f(R)$ 把子消息 N_j 合成完整消息 N'，用共享密钥加密后也发给 AS－P，AS－P 用共享密钥 K 解密后即可获得 N'，如果 $N = N'$ 那么对 STA 的认证通过。基本的认证框架主要包含 2 个大的步骤：与 AP 建立连接和接入认证，下面分别进行描述。

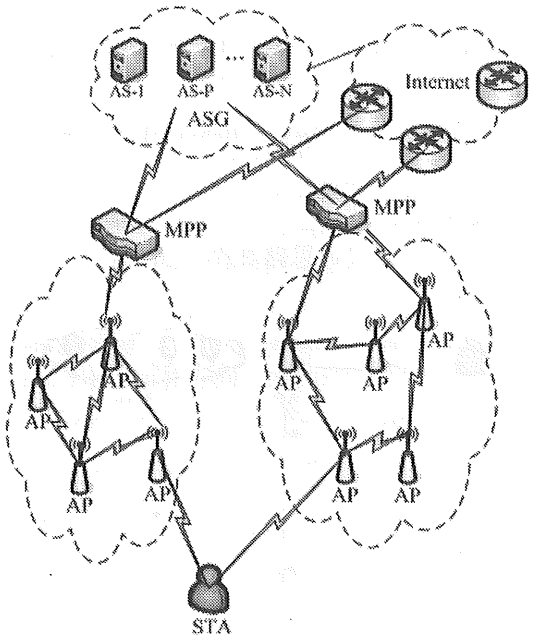

图 1　采用门限机制的 Mesh 网络结构

Fig. 1　The structure of WMN with threshold method

3.1　与 AP 建立连接

STA 与 AP 建立连接的设计思路如图 2 所示。

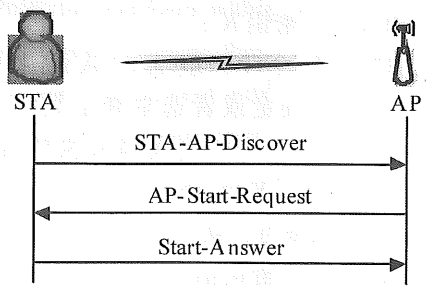

图 2　STA 与 AP 建立连接示意图

Fig. 2　Connection established between STA and AP

（1）用户 STA 接入 Mesh 网络时，首先发送链路多播消息 STA－AP－Discover 来发现并选择能够提供认证授权服务的 AP。

（2）AP 收到 STA－AP－Discover 消息后，向

STA 发送消息 AP－Start－Request，表明自己可以提供认证授权服务，并给 STA 配置本地局部使用的 IP 地址。

（3）STA 发送 Start－Answer 消息来响应 AP 的 Start－Request 消息。

3.2 接入认证

接入认证的设计思路如图 3 所示。

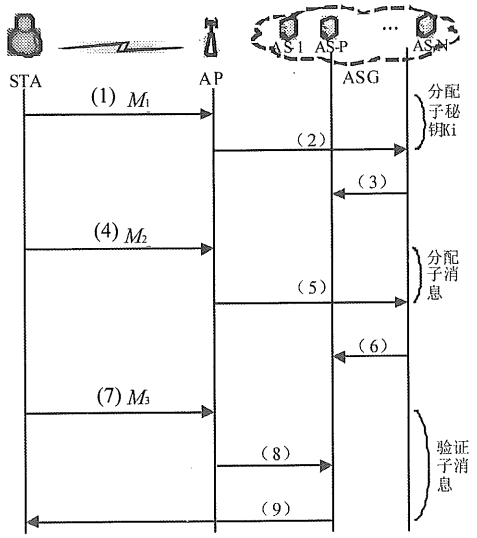

图 3 门限机制下的接入认证流程

Fig. 3 Access authentication flow under threshold scheme

详细说明如下：

（1）经过注册阶段之后，STA 可以将子密钥 K_i（$i=1, 2\cdots n$）以及 STA 的自身相关信息，比如 ID 号、MAC 地址等分别用 AS－i（$i=1, 2\cdots n$）的公钥进行加密，形成如下的信息 M_1 发给 AP：

$$M_1 = [\text{STA} - \text{MAC} \| \text{STA} - \text{ID} \| K_i]PK_{\text{AS}-i}$$

（2）AP 将信息 M_1 转发给 AS－i（$i=1, 2\cdots n$），AS－i 收到 M_1 后，分别用自己公钥进行解密，即可获得相应的子密钥 K_i；

（3）对于 N 个 AS 组成的认证服务器组（ASG）可以事先确定或者选举确定其中一个 AS（例如 AS－P）作为 ASG 的代理来执行信息的处理。根据门限机制，N 个 AS－i 中有 t 个或者大于 t 个认证服务器的参与，就可以合成对称密钥 K，t 个 AS 可以把各自的密钥信息发给 AS－P，AS－P 也可以代为合成共享密钥 K；

（4）STA 把 t 个消息 N_j（$1<j<t$）分别用 t 个子密钥 K_j（$1<j<t$）进行加密，然后再用 AS－i 的公钥加密，形成信息 M_2 后送到 AP；换句话说，消息 N_1 用 K_1 加密，消息 N_2 用 K_2 加密，依次类推，消息 N_t 用 K_t 加密；

$$M_2 = [[N_j]K_j]PK_{\text{AS}-i}$$

（5）AP 把信息 M_2 转发到 AS－i（$i=1, 2\cdots t$）之后，AS－i 分别用自己的私钥解密 M_2，然后再用已经收到的子秘钥 K_i 继续解密数据包，可以分别得到子消息 N_j（$j=1, 2\cdots t$）；在此过程中，消息 N_1 给了 AS－1，消息 N_2 给了 AS－2，依次类推，消息 N_t 给了 AS－t；

（6）AS－1，AS－2…AS－t 通过消息合成算法 $f(R)$，把 N_j 合成一个完整的消息 N，保存到 AS－P。此处的合成算法与步骤（7）中 STA 合成 t 个子消息 N_j 为完整消息 N' 的合成算法要保持一致；本方案中设计的消息合成算法为：$f(R) = (N_1 \oplus N_2 \oplus N_3 \cdots \oplus N_j)$；

（7）STA 把 t 个消息 N_j 的合成消息 $N' = (N_1 \oplus N_2 \oplus N_3 \cdots \oplus N_j)$ 用共享秘钥 K 加密，再用 AS－P 的公钥加密，形成消息 M_3 后发给 AP；

$$M_3 = [[N']K]PK_{\text{AS-P}}$$

（8）AP 将消息转发给 AS－P，AS－P 用自己的私钥解密，再用合成得到的共享密钥 K 对信息 M_3 解密，此时可以得到消息 N'；AS－P 把消息 N' 与收到的合成消息 N 比较，如果一致，通过验证；如果不一致，拒绝服务；

（9）AS－P 把最终的认证结果通过 AP 送给 STA。

这样以来，STA 通过认证之后，就可以建立会话密钥，当然，还要涉及到密钥更新问题，比如每 5 000 次数据传输，进行一次密钥更新，这个就涉及到密钥管理问题，这里不做详细描述。

4 小 结

本文基于 Asmuth－Bloom 门限机制构建了多服务器的无线 Mesh 网络门限认证系统。在该系统中，共有 N 个认证服务器（AS）组成了一个认证服务组，只有认证服务器组中的成员才可以执行有效的认证过程，而非群体成员无法参与认证过程，可以避免假冒攻击；同时只有当认证服务器的个数不少于门限值时，才能恢复共享密钥 K，从而可以有效防止单个服务器被攻陷，此认证方式替代了单个认证服务器认证移动用户的缺陷，提升了系统的安全性能。与 Shamir 门限体制相比，本系统采用的 Asmuth－Bloom 门限方法计算相对简单，对网络资源消耗相对较少，系统延时也较小。无线 Mesh 网络中，当用户通过认证之后，如何高效安全地使用、更新用于安全通信的共享密钥 K，可以作为下一步的研究重点。

参考文献：

[1] FACCIN S M, WIJTING C, KNECKT J, et al. Mesh

WLAN networks: concept and system design [J]. IEEE Wireless Communications, 2006, 13(2): 10 - 16.

[2] SIDDIQUI M S, HONG C S. Security issues in wireless Mesh networks[C]//The Proceedings of 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), IEEE Computer Society, 2007: 717 - 722.

[3] PRASAD A R. Securing Mesh networks-A novel solution for home scenario[C]//The Proceedings of 2nd International Conference on Communication Systems Software and Middleware (COMSWARE 2007), IEEE Computer Society, 2007: 1 - 5.

[4] SAMHAT A E, ABDI M. Security and AAA architecture for WiFi - WiMAX Mesh network[C]//The Proceedings of 4th International Symposium on Wireless Communication Systems (ISWCS 2007), Society, 2007: 587 - 591.

[5] ROOS A, WIELAND S, SCHWARZBACHER A Th, et al. Time behaviour and network encumbrance due to authentication in wireless mesh access networks[C]//The Proceedings of IEEE 65th Vehicular Technology Conference (VTC2007), IEEE Press, 2007: 1219 - 1223.

[6] DESMEDT Y, FRANKEL Y. Threshold cryptosystem [C]//The Proceeding of CRYPTO89, LNCS 435, Berlin: Springer - Verlag, 1990: 307 - 315.

[7] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 24(11): 612 - 613.

[8] ASMUTH C A, BLOOM J. A modular approach to key safeguarding [J]. IEEE Transactions on Information Theory, 1983, 29(2): 208 - 210.

[9] KAYA K, SELCUK A A. Threshold cryptography based on Asmuth - Bloom secret sharing[J]. Information Sciences, 2007, 177(19): 4148 - 4158.

[10] ZHAO J J, ZHANG J Z, ZHAO R. A practical verifiable multi-secret sharing scheme[J]. Computer Standards & Interfaces, 2007, 29(1): 138 - 141.

Design of Threshold Authentication System with Multi-Servers in Wireless Mesh Network

LIU Dong-sheng[1], *YANG Ya-tao*[2,3]

(1. College of Computer and Information Engineering, Zhejiang University of Industry and Business, Hangzhou 310018, China;
2. Information Security Center, Beijing University of Posts and Telecommunications, State Key Laboratory of Networking and Switching, Beijing 100876, China;
3. Beijing Electronic Science & Technology Institute, Beijing 100070, China)

Abstract: Traditional centralized AAA authentication model is prone to suffer from service paralysis due to the DoS (Denial of Service) attack or malicious destroy in wireless Mesh network. To salve this isswe, the scheme of threshold authentication with multi-servers is proposed based on the Asmuth-Bloom threshold technology, then wireless access and authentication flow are designed and analyzed. Only the members within Authentication Server Group (ASG) can carry out the valid authentication process, moreover, only t or more than t authentication servers can resume the shared key K, which can avoid the fraudulent attack and can prevent single authentication server from being captured. Analysis result shows that, the validity of authemtication mechanism can be guaranteed and the security of system also can be enhanced by the designed threshold authentication systme, our novel idea provides an effective solution to access authentication in wireless Mesh network and has better applied and referenced value.

Key words: network security; authentication; threshold technology; wireless Mesh network; authentication servers group