doi:10.3969/j.issn.1000-436x.2014.08.001

# 基于改进的 Diameter/EAP-MD5 的 SWIM 认证方法

吴志军，赵婷，雷缙
（中国民航大学 天津市智能信号处理重点实验室，天津 300300）

**摘 要**：广域信息管理(SWIM, system wide information management)采用面向服务的体系结构(SOA, service oriented architecture)提供民航信息交互与数据共享功能。在分析 SWIM 体系结构和基于 Diameter 协议的 EAP-MD5 应用子协议基础上，给出标准 Diameter/EAP-MD5 认证过程中存在的安全隐患，改进了 EAP-MD5 认证协议，提出基于改进的 Diameter/EAP-MD5 协议的 SWIM 用户身份认证方法，研究基于 Diameter 的 SWIM 认证服务，并在模拟的 SWIM 环境中对改进方法进行仿真实验和安全性分析。实验结果表明，改进的 Diameter/EAP-MD5 认证方法可在计算性能相当的前提下提高 SWIM 认证系统的安全性，为 SWIM 安全服务框架的构建提供保障。
**关键词**：广域信息管理系统；Diameter 协议；扩展认证协议；信息—摘要算法；身份认证
**中图分类号**：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)08-0001-07

# Authentication method in SWIM based on improved Diameter/EAP-MD5

WU Zhi-jun, ZHAO Ting, LEI Jin
(Tianjin Key laboratory for Advanced Signal Processing, Civil Aviation University of China, Tianjin 300300, China)

**Abstract:** System wide information management (SWIM) provides the civil aviation information exchange and data sharing function by using service-oriented architecture (SOA). Based on the analysis of SWIM architecture and the sub-protocol EAP-MD5 of Diameter, the security vulnerable of authenticating process in standard Diameter/EAP-MD5 is explored, the EAP-MD5 authentication protocol is improved, and the SWIM authentication service based on Diameter is studied, then the SWIM authentication method based on improved Diameter/EAP-MD5 protocol is proposed. Experiments on the security of SWIM authentication service based on Diameter are performed in SWIM simulation environment, results show that the improved Diameter/EAP-MD5 authentication method can enhance the security of SWIM authentication and guarantee SWIM security service.
**Key words:** system wide information management (SWIM); Diameter protocol; extensible authentication protocol (EAP); message-digest (MD) algorithm; identity authentication

## 1 引言

随着我国民航业务的全面扩展和信息化建设的迅速发展，整个民航领域的企业、单位和部门越来越依赖通信网开展业务交易、进行内部资源共享、实现协调决策。基于面向服务架构(SOA, service oriented architecture)的民航广域信息管理系统(SWIM, system wide information management)服务架构应运而生，为相互独立的空中交通管理(ATM, air traffic management)系统之间提供资源整合、数据共享和统一服务，构建系统级的航空信息管理体系[1,2]。

SWIM 具有数据高速交互和信息共享的优势，

**收稿日期**：2013-05-29；**修回日期**：2013-07-14
**基金项目**：国家自然科学基金资助项目（61170328）；天津市应用基础与前沿技术研究计划基金资助项目（12JCZDJC20900）；中央高校基本科研业务费专项基金资助项目（31122013P007, ZXH2012P004）；中国民航大学研究生课程建设基金资助项目（2013）
**Foundation Items:** The National Natural Science Foundation of China(61170328); The Natural Science Foundation of Tianjin(12JCZDJC20900); The Fundamental Research Funds for the Central Universities (31122013P007, ZXH2012P004); Postgraduate Course Construction Projects of Civil Aviation University of China (2013)

包括很多航空业务关键数据和保密信息在内，越来越多的业务数据在SWIM网络中传输和交换，面临的安全威胁也越来越突出，数据安全和隐私保护成为SWIM发展必然要面临的课题[3,4]，只有对SWIM用户身份做出可靠的确认才能有效地保证合法用户接入SWIM网络并对其使用的相应资源进行保护[5]，同时阻止非法航空用户对SWIM网络进行恶意访问和破坏[6]。

本文根据SWIM的体系结构，结合我国民航SWIM具体布局，采用新一代AAA(authentication、authorization、accounting)协议——Diameter协议，实现SWIM系统的安全认证，保障SWIM共享数据的安全和隐私保护。

## 2 SWIM安全认证框架

SWIM是一个虚拟信息池，存储实时的航空飞行数据、监视数据和气象信息等，ATM要求必须保证SWIM数据的保密性、完整性和可用性[6]。Diameter协议包括基础协议[7,8]和各种应用协议，完全支持IPsec安全协议，并提供可选的安全传输层(TLS, transport layer security)协议对数据进行保护，可以实现网络层、传输层及应用层的加密认证功能，以保证国际民航组织(ICAO, international civil aviation organization)对SWIM的要求[6]。

### 2.1 SWIM服务架构的安全技术

欧洲SWIM-SUIT计划定义了SWIM信息和服务模型[1]，将SWIM用户的身份认证和访问控制作为安全服务的一个子项；联邦航空局(FAA, federal aviation administration)的下一代交通运输系统NextGen (next generation air transportation system)构建XML网关基础设施为SWIM提供安全服务[5]；欧洲的SWIM-SUIT计划进入了工程实施阶段，并且已经与美国的SWIM网络开展了互联工作，通过两者的互联，欧美在SWIM网络融合和系统交互的过程中建议采用PKI网络安全认证技术。国际民航组织于2010年10月出台了SWIM相关的网络服务安全标准[6]，该标准将SWIM的网络安全技术分为3层：网络层采用基于IPsec协议的逐跳安全机制；传输层采用基于SSL/TLS协议的端到端安全机制；应用层则负责实现XML安全、消息安全、访问控制、身份管理、安全管理等。

### 2.2 新一代AAA协议—Diameter协议

可提供AAA服务的现行Radius协议因其本身固有的缺陷，例如，C/S模式、基于UDP面向非连接的传输、没有失败恢复机制、认证与授权必须成对出现等，限制了它的进一步发展。而新一代AAA协议——Diameter协议克服了Radius协议的诸多缺陷，如采用Peer-to-Peer模式、基于TCP/SCTP面向连接的传输协议、提供可靠的失败恢复机制、认证与授权分离等，拥有优良的兼容性、标准的规范化、极强的可扩展性和更高的安全性，更容易进行新应用的扩展以满足新的需求[7]。目前，IETF、3GPP、3GPP2、ETSI TISPAN、Packet Cable、MSF、ITU等标准组织已经普遍接受Diameter协议，在GSM/UMTS、CDMA、LTE、有线电视等网络中采用Diameter协议来做它的AAA接口。

### 2.3 基于Diameter/EAP协议的SWIM认证架构

根据我国空中交通管理体系的民航空管局、地区空管局、空管分局站三层管理架构，SWIM面向的是空中交通管理各级组织及其下属的各级用户，采用Diameter协议为SWIM提供用户身份认证可以更好地解决全国民航空中交通管理业务分布式应用和跨域认证的问题。Diameter在中国SWIM中部署结构如图1所示。

基于Diameter/EAP协议的认证系统与SWIM架构的星型拓扑结构相互契合，其结构实际上是一个以用户、接入服务器（包括重定向服务器和代理服务器）、认证服务器为主，注册服务器为辅，注册信息和认证信息数据库为支撑的节点结构，如图2所示[3]。

在认证过程中，SWIM用户采用NAI（network access identify），即“user@realm”的结构进行注册，其中，user是用户名，realm是管理域名，恰好可与用户所在区域相对应，由NAI的realm可以得知用户的注册网络。每次登录时提交认证请求，接入服务器主要进行协议转换和消息转发，并识别用户的realm信息，将其认证请求转发至相应的Diameter认证服务器，Diameter服务器依托注册信息数据库对用户进行最终认证，同时依据用户的realm信息为其提供漫游管理，最后将用户的认证状态记录于认证信息数据库。

## 3 Diameter/EAP-MD5协议分析及改进

标准的Diameter/EAP-MD5认证在为SWIM提供基本的用户认证服务中存在一定的安全隐患。本文在针对标准的Diamter/EAP-MAD5认证流程进行

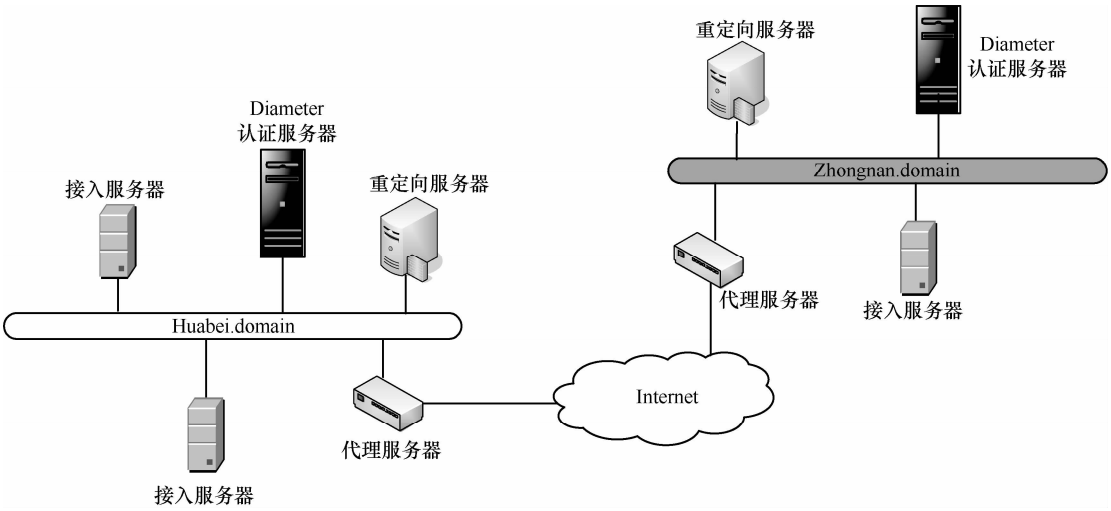



图 1　SWIM 中的 Diameter 部署

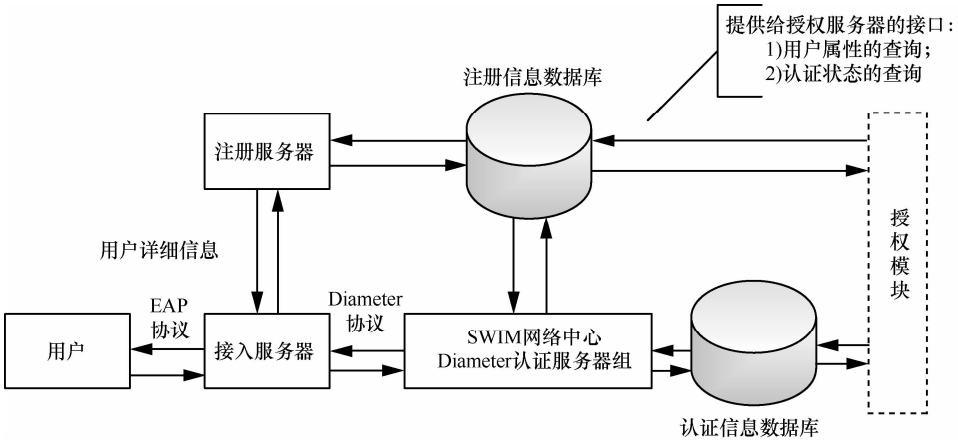



图 2　SWIM 架构下基于 Diameter/EAP 协议的认证模块结构

安全隐患分析的基础上，提出改进的 Diameter/EAP-MD5 认证协议，并将其应用到 SWIM 中。

### 3.1　标准的 Diameter/EAP-MD5 认证流程

EAP-MD5 是一个 IETF 的开放标准，其认证无需证书，部署简单。标准的 Diameter/EAP-MD5 认证流程如图 3 所示[9,10]。

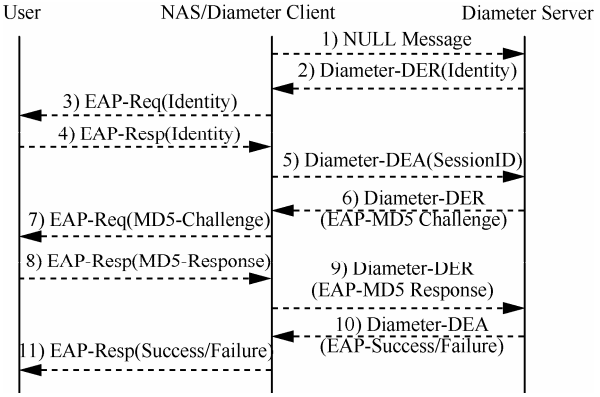



图 3　Diameter/EAP-MD5 标准认证

1) NAS 向 Diameter 认证服务器发送 NULL Message，标志认证过程的开始。

2) Diameter 认证服务器向 NAS 发送 DER 消息，要求用户提供身份信息。

3) NAS 将 DER 消息解封后重新封装成 EAP-Request 消息后转发给用户。

4) 用户将身份信息以明文形式包含在 EAP-Response 消息中返回 NAS。

5) NAS 提取用户身份信息后将其封装在 DEA 消息中转发给 Diameter 认证服务器。

6) Diameter 认证服务器将接收到的用户 ID 与数据库中存储的信息对比，若不匹配则发布认证失败消息，若匹配则向 NAS 发送 DER 消息，其中包含服务器端产生的随机数。

7) NAS 提取其中的随机数并向用户转发 EAP-Request 消息。

8) 用户使用接收到的随机数与密码做散列运

算，并将结果同用户 ID 一同发往 NAS。

9) NAS 将该 EAP-Response 消息重新封装在 DER 消息中发往 Diameter 认证服务器。

10) Diameter 服务器本地计算原随机数与用户名对应密码的散列值，并与接收到的散列值作比较，若相同则返回认证成功消息，若不同则返回认证失败消息。

11) NAS 向用户转发相应的 EAP-Success/Failure 消息。

### 3.2 标准的 Diameter/EAP-MD5 认证安全性分析

标准的 Diameter/EAP-MD5 认证在 SWIM 安全服务架构的具体实现中存在一定的安全隐患，若直接应用到 SWIM 网络中，不仅会造成航空用户信息的泄露，更有可能威胁到整个 SWIM 网络。标准的 Diameter/EAP-MD5 认证可能存在的缺陷和漏洞主要表现在以下 3 个方面[11,12]。

1) 认证过程中用户 ID 始终明文传输，机密性的缺失往往是致命的。一旦这些用户的身份信息被攻击者截获，若用来对服务器或数据库进行各种注入式攻击，则会导致更多敏感甚至机密数据的泄露。SWIM 用户涉及机场、航空公司、空管局及其下属单位等，以管制员为例，若攻击者截获该管制员 ID，借此破译其认证密码，则极有可能凭借管制员权限查看到相应保密级别的信息，严重的有可能威胁到航空飞行安全，甚至危及到国家领空的安全。

2) NAS /Diameter Client 只起到转发作用，其身份未被确认，一旦被攻击者仿冒，则很容易进行中间人攻击，造成用户信息和服务器信息的双重泄露，即使用户和服务器之间传输的消息是经过加密的，若此消息被截获，也可利用猜测攻击获得相关明文甚至是密钥。SWIM 信息池包含海量的飞行数据、监视数据、气象信息等，NAS 的仿冒者极有可能在服务器返回用户请求的过程中截获这些信息从事非法活动。

EAP 的安全性说明要求 EAP 使用的认证方法应实现双向认证，而 EAP-MD5 仅实现了服务器对用户的认证，并没有实现用户对服务器的认证。若用户盲目地向攻击者仿冒的服务器提供个人信息，则会造成不必要的损失。

### 3.3 改进的 Diameter/EAP-MD5 认证流程

在分析标准 Diameter/EAP-MD5 认证过程存在缺陷和漏洞的基础上，本文针对这些安全缺陷和漏洞做出相应的改进[11~15]，保证其在 SWIM 的实际应用中提供更强的安全性。以下均以用户 client@huabei.net 为例，进行说明改进的 Diameter/EAP-MD5 协议在 SWIM 中的认证过程，如图 4 所示。

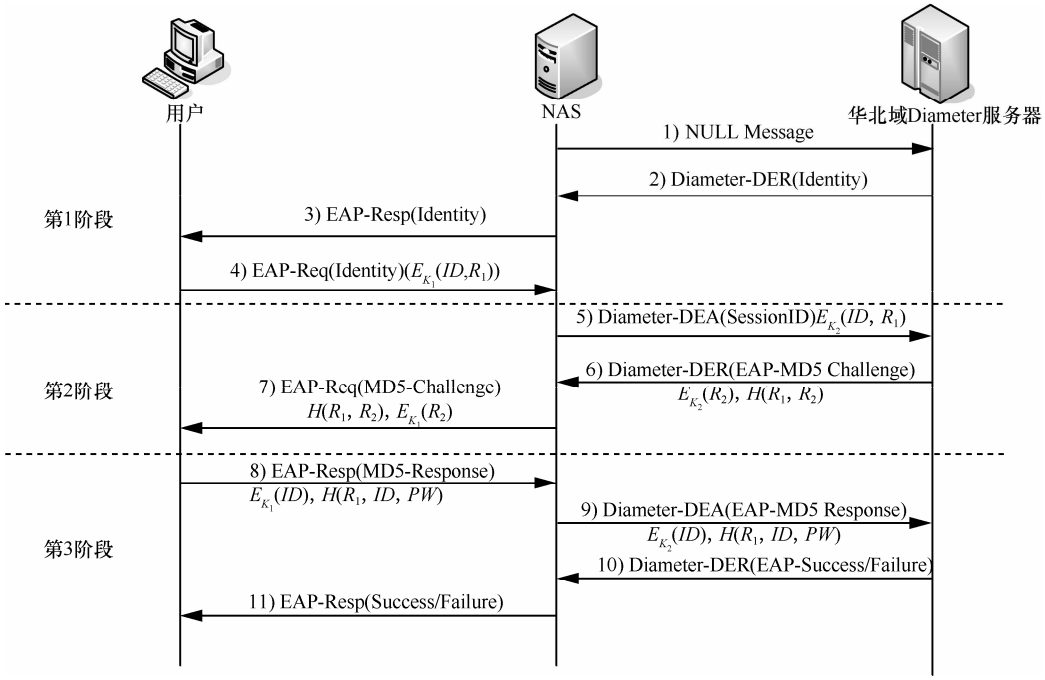



图 4　Diameter/EAP-MD5 改进认证

改进的 Diameter/EAP 认证可分为 3 个阶段[11]。

第 1 阶段：SWIM 用户与 NAS 之间的相互认证。

1) NAS 向 Diameter 认证服务器发送 NULL Message，标志认证过程的开始。

2) Diameter 认证服务器向 NAS 发送 DER 消息，要求用户提供身份信息。

3) NAS 将 DER 消息解封后重新封装成 EAP-Request 消息后转发给用户。

4) 用户产生一随机数 $R_1$，使用与 NAS 共享的 AES 算法对称密钥 $K_1$ 将用户 *ID* 和 $R_1$ 同时加密后封装在 EAP-Response 消息中发往 NAS，若 NAS 持有相应的 $K_1$，则可实现与用户的相互认证并提取用户 *ID*，否则认证失败。

第 2 阶段：用户对服务器的认证。

5) NAS 使用 $K_1$ 解密消息后得到用户 *ID* 和随机数 $R_1$，判断用户的 reaml 信息以确定转发至哪个 Diameter 认证服务器，然后使用与 Diameter 认证服务器约定的 AES 算法对称密钥 $K_2$ 对其进行加密后封装在 DER 消息中转发给 Diameter 认证服务器。

6) Diameter 服务器使用 $K_2$ 解密消息得到用户 *ID* 并加以判断，若未存用户 *ID*，则对用户域名加以判断，如仍不匹配则发布认证失败消息，若已存在用户 *ID*，则生成随机数 $R_2$，连同与 $R_1$ 一起做散列运算 $H(R_1, R_2)$返回给 NAS。

7) NAS 使用 $K_2$ 得到 $R_2$ 后再用 $K_1$ 进行加密，将 $H(R_1, R_2)$一同包含在向用户发送的 EAP-Request 消息中。

8) 用户通过 $K_1$ 得到 $R_2$ 之后自行计算 $R_1$、$R_2$ 的散列值并与接收到的 $H(R_1, R_2)$对比，若不相同则对 Diameter 服务器重新发起认证，若相同则向 NAS 发送包含用户 *ID* 和 $H(ID, PW, R_2)$的 EAP-Response 消息。

第 3 阶段：服务器对用户的认证。

9) NAS 使用 $K_1$ 得到用户 *ID* 后用 $K_2$ 加密，连同 $H(ID, PW, R_2)$一起向 Diameter 服务器发送 Diameter-EAP-Request 消息。

10) Diameter 服务器对比接收到的 $H(ID, PW, R_2)$与本地的计算结果，若一致则认证成功，若不一致则认证失败，回复相应的 Success/Failure 消息。

11) NAS 向用户转发 EAP-Success/EAP-Failure 消息。

以上过程针对标准 Diameter/EAP-MD5 认证方法中存在的用户身份信息明文传输，未对 NAS 进行身份确认，为实现用户与服务器的双向认证等主要缺陷实现了改进。

## 4　仿真实验和结果分析

本节基于改进的 Diameter/EAP-MD5 认证协议在仿真的 SWIM 环境下进行实验，并对实验数据和结果进行分析。

### 4.1　实验环境

按照 SWIM 架构下基于 Diameter/EAP 协议的认证模块结构（如图 2 所示），根据 SOA 模型搭建模拟的 SWIM 环境。其中，用户、NAS（双网卡）、Diameter 认证服务器均安装 Red Hat Linux 5.5 系统和由 OpenDiameter 组织开发的 opendiameter-1.0.7-i 软件包，部署 Diameter 协议运行环境；进行用户身份 XML 文档（以 user@huabei.net 为例）、各 PC 的 IP 地址及端口号、服务器后方注册数据库和认证状态信息数据库的配置分别在用户 PC、NAS 和 Diameter 认证服务器端启动认证客户端程序、NAS 程序以及服务器认证程序，先后实现 Diameter/EAP-MD5 标准和改进认证方法，调整参数并统计实验数据。

### 4.2　Diameter/EAP-MD5 改进认证的时间复杂度分析

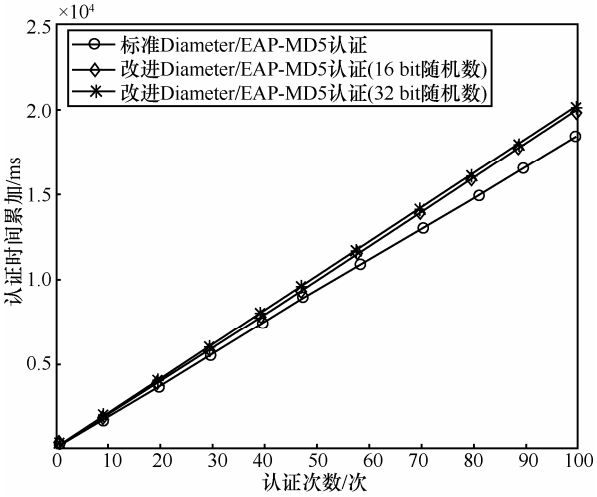
SWIM 网络具有庞大的航空用户群和海量的数据。由于航空安全飞行要求数据实时通信，SWIM 安全访问要求具有很强的实时性，对认证系统的时间复杂度性能提出较高的要求。身份认证作为航空用户访问 SWIM 网络的门户，同样需要达到合理的时间复杂度要求。

Diameter/EAP-MD5 认证改进前后三方收发消息的条数未改变，已知随机数位数与认证安全性之间存在正比例关系，仿真实验中对认证改进前后随机数位数分别为 16 bit、32 bit，密钥长度分别为 128 bit、256 bit，AES 加密算法时的认证时间做 100 次抽样，记录数据如表 1 所示。

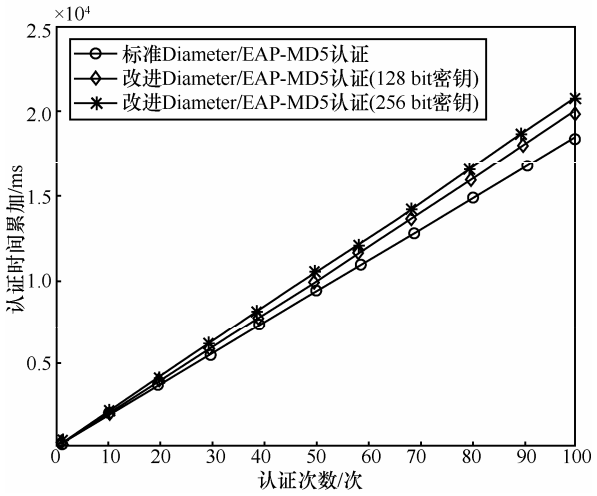
对表 1 所列抽样数据进行统计，结果表明改进前后的单次平均认证时间仅相差约 16 ms；随机数 16 bit 与 32 bit 的单次平均认证时间相差不足 3 ms；密钥长度 128 bit 与 256 bit 的单次平均认证时间相差约 8 ms。为使参数变化情况下认证时间差更加直观，对其进行 100 次时间累加，得到的时间复杂度实验结果如图 5 所示。

**表 1**　　**100 次抽样结果（单位：ms）**

| 抽样次数 | 标准认证 | 改进 16 bit(AES128) | 改进 32 bit(AES128) | 改进 16 bit(AES256) |
|---|---|---|---|---|
| 1 | 180.437 | 199.375 | 204.118 | 213.845 |
| 2 | 178.890 | 194.373 | 189.565 | 201.769 |
| 3 | 194.919 | 206.586 | 205.274 | 198.468 |
| 4 | 179.316 | 201.468 | 196.479 | 207.820 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 97 | 187.062 | 197.349 | 197.017 | 221.385 |
| 98 | 179.331 | 215.821 | 189.288 | 197.154 |
| 99 | 174.047 | 195.467 | 212.526 | 214.528 |
| 100 | 186.250 | 198.694 | 201.365 | 202.273 |
| 平均值 | 184.35 | 200.63 | 203.13 | 208.69 |




(a) 16 bit 和 32 bit 随机数




(b) 128 bit 和 256 bit 密钥

图 5　时间复杂度实验统计结果

从图 5 中可以看出，认证改进前后以及随机数位数分别为 16 bit（AES128）、32 bit（AES128）和 16 bit (AES256)的 100 次累加认证时间分别为 18 435.647 ms、20 062.956 ms、20 312.956 ms 和 20 869.308 ms，即改进的 Diameter/EAP-MD5 认证比标准认证平均每次多花费 16.273 ms；随机数位长对改进认证的时间复杂度影响是 32 bit 比 16 bit 平均每次多花费 2.5 ms；密钥长度 256 bit 比 128 bit 的单次平均每次多花费 7.964 ms。而一般登录的页面响应时间在 2 s 内为宜，网络延时在 30 ms 内为宜，可见改进的 Diameter/ EAP-MD5 认证在时间复杂度上的牺牲几乎可以忽略不计。

### 4.3　Diameter/EAP-MD5 改进认证的安全性分析

改进后的 Diameter/EAP-MD5 协议认证方法的安全性从以下几个方面分析。

1) 机密性：不同于标准认证的用户 *ID* 明文传输，改进的认证方法中用户与 NAS 之间、NAS 和认证服务器之间分别采用约定的对称密钥 $K_1$、$K_2$ 对消息进行加密。

2) 双向认证：标准的 Diameter/EAP-MD5 认证仅实现服务器对用户的认证相比，改进的 Diameter/EAP-MD5 认证流程中，用户和 NAS 之间依靠对称密钥 $K_1$ 实现了双向认证，同时用户利用本地产生的随机数 $R_1$ 和认证服务器产生的随机数 $R_2$ 实现了对服务器的认证。

3) 抵御重放攻击：每一次新的认证，用户生成新的随机数 $R_1$，Diameter 认证服务器生成新的随机数 $R_2$，且 $R_1$ 位长可选，2 个随机数的配合使重放攻击的可能性大大降低。

4) 猜测攻击：攻击者若想分析得到用户 *ID* 和密码，首先需要截获用户、NAS 和 Diameter 服务器之间的通信数据，此时 $K_1$、$K_2$ 提供第一道保障，

其次，用户 *ID* 与 $R_1$ 相互连接，而每次认证所产生的 $R_1$ 不同，若无法确定 $R_1$ 的长度，则依然无法分离出用户 *ID*。

5) 角色仿冒：在实现了用户、NAS、Diameter 服务器之间的两两认证之后仍要做一次 $R_1$、$R_2$ 的散列运算以供 Diameter 服务器验证，其目的是为了再次确认完成用户与 NAS 之间的相互认证和用户对服务器的认证之后各主体并未发生变化，有效防范攻击者仿冒合法用户或者 NAS。

基于上述分析可以看出，改进后的 Diameter/EAP-MD5 认证协议在 SWIM 的数据安全和隐私保护方面具有较高的安全性，可以避免 SWIM 敏感信息的外泄和阻止非法航空用户的访问。

## 5　结束语

本文综合考虑我国民航发展现状、安全基础设施部署难度以及安全强度要求等情况，设计采用 Diameter 协议为民航 SWIM 架构提供安全认证服务。Diameter/EAP 认证模块结构与 SWIM 的星型拓扑结构相互契合，为其软硬件的部署提供了十分有利的条件。改进后的 Diameter/EAP-MD5 认证未增加流程消息数，并在几乎没有增加时间复杂度的基础上对双向认证、抵御重放攻击、机密性、防猜测攻击和防角色仿冒等方面都做了部分改善，从而提高了网络 AAA 服务基础设施的安全性和准入严格性，强化了 SWIM 系统安全服务，同时采用 NAI 格式的用户 ID，从而更加适宜 SWIM 系统结构。

然而，改进方法中增加了用户、NAS 和 Diameter 认证服务器之间的对称密钥，这又从另一方面加大了密钥分配的难度，今后的工作重点应放在开发一种可动态分配密钥的 Diameter/EAP-MD5 认证方法上，权衡考虑高安全性和低密钥分配难度的折衷。

## 参考文献：


[1] DARIO D C, ANTONIO S, GEORG T. SWIM- a next generation ATM information bus-the SWIM-SUIT prototype[A]. 2010 14th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW)[C]. 2010.41- 46.

[2] 吕小平, 齐鸣. 浅谈 SWIM[J]. 民航管理, 2009,(5): 68-69.
LV X P, QI M. A brief discussion of SWIM[J]. Civil Aviation Management, 2009, (5): 68-69.

[3] BOB S. Security architecture for system wide information management[A]. The 24th 2005 Digital Avionics Systems Conference (DASC 2005)[C]. 2005.

[4] BOB S. System-wide information management (SWIM) demonstration security architecture[A]. 2006 IEEE/AIAA 25th Digital Avionics Systems Conference[C]. 2006. 1-12.

[5] Federal Aviation Administration. System Wide Information Management (SWIM) eXtensible Markup Language (XML) Gateway Requirements[S]. 2009.

[6] International Civil Aviation Organization. Web service security standards[A]. Aeronautical Telecommunication Network Implementation Coordination Group-Eighth Working Group Meeting[C]. Christchurch New Zealand, 2010.

[7] 邱锡鹏, 刘海鹏. Diameter 协议研究[J]. 计算机科学, 2013, 30(2): 75-78.
QIU X P, LIU H P. Research on diameter protocols[J]. Computer Science, 2013, 30(2):75-78.

[8] IETF RFC3588. Diameter Base Protocol[S]. 2003.

[9] IETF RFC3748. Extensible Authentication Protocol(EAP)[S]. 2004.

[10] IETF RFC 4072, Diameter Extensible Authentication Protocol(EAP) Application[S]. 2005.

[11] 陈凤其，姚国祥. 一种基于 Hash 函数的 EAP 认证协议[J]. 计算机系统应用, 2010, 19(6): 74-77.
CHEN F Q, YAO G X. A hash-based EAP authentication protocl[J]. Computer Systems & Applications, 2010, 19(6):74-77.

[12] 陈世伟, 金晨辉. MD5 碰撞攻击中的充要条件集[J]. 软件学报, 2009,20(6):1617-1624.
CHEN S W, JIN C H. Set of necessary and sufficient conditions in collision attacks on MD5[J]. Journal of Software, 2009, 20(6):1617-1624.

[13] 赵志新, 祝跃飞, 梁立明. 无线局域网隧道认证协议 PEAP 的分析与改进[J]. 信息工程大学学报, 2005, 6(3):52-55.
ZHAO Z X, ZHU Y F, LIANG L M. The analysis and mend of PEAP protocol in WLAN[J]. Journal of Information Engineering University, 2005,6(3):52-55.

[14] 吉晓东. 支持身份隐藏的 EAP-PSK 协议改进[J]. 南通大学学报(自然科学版), 2007, 6(2):74-77.
JI X D. Improvement of EAP-PSK protocol enabling identity privacy[J]. Journal of Nantong University (Natural Science), 2007,6(2): 74-77.

[15] 王志中. MD5 算法在口令认证中的安全性改进[J]. 电脑知识与技术, 2012, 8(2):296-297.
WANG Z Z. Security improvement of MD5 algorithm in password authentication[J]. Computer Knowledge and Technology, 2012, 8(2): 296-297.


## 作者简介：


**吴志军**（1965-），男，河南固始人，中国民航大学教授、博士生导师，主要研究方向为网络与信息安全。

**赵婷**（1989-），女，山西临汾人，中国民航大学硕士生，主要研究方向为网络与信息安全。

**雷缙**（1982-），女，四川泸州人，中国民航大学博士生、讲师，主要研究方向为网络与信息安全。