一种混合机制的TETRA双向鉴权协议

李 晖 马春光 杨义先
(北京邮电大学信息安全中心 北京 100876)
(北京邮电大学国家重点实验室 北京 100876)

摘 要 该文详细分析了TETRA系统移动台和网络之间的鉴权协议，分析表明采用共享秘密的挑战应答协议存在若干缺陷：(1)当无法保证访问位置寄存器和归属位置寄存器之间的通信安全时会产生对已知明文攻击的开放性；(2)网络规模较大时，在网络端难于保存和维护大量的鉴权密钥。在理论分析的基础上该文给出了一种基于身份公钥的网络端对移动台和基于哈希链的移动台对网络端的鉴权协议，所提出的协议可以有效弥补上述缺陷。

关键词 保密通信，鉴权，TETRA，挑战-应答协议，基于身份的公钥
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)01-0147-04

A Mixed Mechanism Mutual Authentication Protocol for TETRA

Li Hui Ma Chun-guang Yang Yi-xian
(*Information Security Center, Beijing Univ. of Posts and Telecomm., Beijing* 100876, *China*)
(*National Key Lab, Beijing Univ. of Posts and Telecomm., Beijing* 100876, *China*)

Abstract The mutual authentication between the Mobile Station(MS) and Switching and Management Infrastructure(SwMI) for TETRA is analyzed in this paper and theoretical analysis shows that some drawbacks exist when using the shared secrets in the challenge-response protocol: (1) Open attack for known text might occur once the communication security between visiting location register and home location register can not be guaranteed; (2) It is difficult to store and maintain large amount of authentication keys when the network is large. An authentication protocol for TETRA using identity-based public keys for the SwMI authenticate the MSs and an authentication protocol based on hash chain for the MSs authenticate the SwMI are presented based on the theoretical analysis, which can effectively compensate the above-mentioned drawbacks.

Key words Secure communication, Authentication, TETRA, Challenge-response protocol, Identity-based public key

1 前言

TETRA系统是ETSI(欧洲通信标准协会)联合使用部门、制造商、检测部门乃至政府部门，为了满足欧洲各国的专业部门对移动通信的需要设计、制订的统一标准的开放性系统[1-4]。TETRA系统具有鉴权、空中接口加密和端到端加密3种安全保密功能，其中鉴权功能实现移动台(MS)与交换和管理基础设施(SwMI)间双向身份识别功能，用于防止非授权用户接入系统和授权用户接入假冒系统。TETRA系统的鉴权采用挑战-应答协议，由系统鉴权中心或移动台产生一个随机数，系统和终端用各自的鉴权密钥和鉴权算法对该随机数进行运算，并比较各自的结果是否一致。

本文对TETRA系统中鉴权协议进行了深入的分析，结果表明目前的TETRA系统鉴权协议存在如下缺陷：(1)当无法保证访问位置寄存器(VLR)和归属位置寄存器(HLR)之间的通信安全时，该协议具有对已知明文攻击的开放性的缺点；(2)网络规模较大时，网络端需要保存和维护大量的鉴权主密钥，同时需要有完善的密钥分配方案[5]。这意味着不仅要增大系统建设初期的投资，而且对系统的安全运行管理提出了更高的要求。为弥补这些缺陷，本文给出了一种基于身份公钥的网络端对移动台和基于哈希链的移动台对网络端的鉴权协议，并对给出的协议进行了详细分析，分析结果表明所提出的算法可以有效弥补上述缺陷，并适用于网络端和移动台的资源和安全需求具有不对称性的TETRA网络中。

2004-07-09 收到, 2005-03-18 改回
国家自然科学基金(60372094，90204017)资助课题

2 TETRA 系统的鉴权协议及其分析

描述方便首先列出下文中所用术语的缩略形式：

移动台(Mobile Station, MS), 交换和管理基础设施(Switching and Management Infrastructure, SwMI), 鉴权中心(Authentication Center, AuC), 用户身份识别码(Individual TETRA Subscriber Identity, ITSI), 访问位置寄存器(Visiting Location Register, VLR), 归属位置寄存器(Home Location Register, HLR), 鉴权实体(Authentication Entity, AE), 随机数种子(Random Seed, RS), 密钥管理(Key Management Infrastructure, KMI), 密钥认证中心(Key Authentication Center, KAC)。

在 TETRA 系统中的鉴权参与方为 SwMI 的 HLR/AuC 和 MS。对 MS 进行鉴权的目的是为了识别由 TETRA 系统中唯一的 ITSI 标识的用户，从而防止非授权移动台接入网络；对 SwMI 进行鉴权的目的是为了识别合法的 SwMI，从而防止移动台接入假冒的 TETRA 网络。

2.1 TETRA 系统的鉴权协议

根据 TETRA 系统的设置，可以实现 TETRA 网络对移动台、移动台对 TETRA 网络的单向鉴权，或 TETRA 网络与移动台之间的双向鉴权，图 1 是以由 SwMI 作为鉴权发起方为例给出的 MS 与 SwMI 之间进行的双向鉴权结构。其中 AuC 和 AE 共同组成 SwMI，密钥 K 一般通过带外机制(out-of-band)保存在 MS 的固件中和 SwMI 的 AuC 的数据库中。

具体的鉴权协议如下：

(1) AuC→AE RS，KS=TA11(RS，K)，KS’=TA21(RS,K)

(2) AE→MS RS，RAND1

(3) MS→AE RES1=TA12(KS，RAND1)，RAND2

(4) AE→MS R1=CMP(RES1，XRES1)，RES2= TA22 (KS’，RAND2)

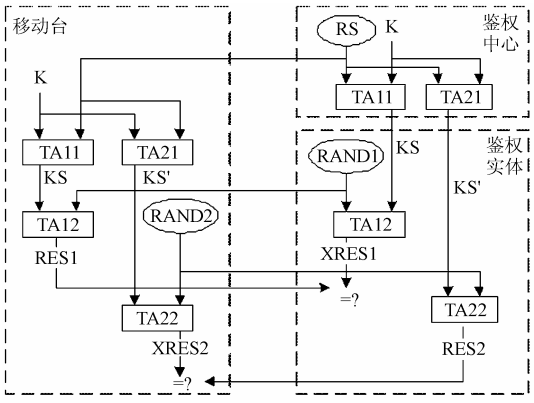

图1 TETRA系统的双向鉴权协议

(5) MS→AE R2=CMP(RES2，XRES2)

其中，TA*ij*(*x*,*y*)表示对x和y进行TA*ij*(*i*,*j*=1,2)运算；CMP(*x*,*y*)表示比较*x*和*y*是否相等。

2.2 TETRA 系统的鉴权协议的分析

TETRA系统的鉴权部分的安全性很大程度上依赖于算法TA11，TA12，TA21，TA22[2]。需要注意的是，如果原TETRA鉴权协议的执行实体是VLR，则需要假设VLR与HLR/AuC之间具有安全通道，一旦无法保证VLR与HLR之间的连接是安全的，则会产生对已知明文攻击的开放性[6]。原因是MS与VLR之间交换的RS，可在随后的消息流中找到与之对应的密文信息 (即KS)。在每次执行协议时，被动攻击者可以通过搭线窃听的方法，收集到一组RS(相当于明文)和KS(相当于密文)信息。通过长期不断的窃听，攻击者至少可建立起一个加密表，甚至可以根据所采用的加密算法强度，进一步攻破此方案并发现主密钥K。这违背了设计认证协议的一般要求，即要求所交换的加密消息的相应明文不会被攻击者得到或推出。

目前TETRA系统中的双向鉴权采用挑战-应答协议，MS端和SwMI端要保存一个共享的秘密，即鉴权的主密钥K，如果在网络规模较大时，SwMI端需要保存和维护大量的MS的鉴权主密钥K的信息，同时需要有完善的密钥分配方案[5]。这意味着不仅要增大系统建设初期的投资，而且对系统的安全运行管理提出了更高的要求。另外，随着移动电子政务的发展，移动文件审批、移动信息发布等功能的应用需要系统能够提供不可否认性服务，目前TETRA系统的安全机制还没有提供有效的签名能力，从而无法实现不可否认性服务。

针对 TETRA 系统鉴权协议的上述不足，本文将在下一节描述一种采用混合机制的 TETRA 双向鉴权协议。

3 一种混合机制的 TETRA 双向鉴权协议

实际上，包括数字集群在内的移动通信网络都具有资源不对称的特点，网络端不仅具有较大的存储空间，而且具有较强的计算能力，而移动台具有较小的存储空间和较弱的处理能力；虚假移动台对网络进行欺骗的可能性远远大于虚假基站对移动台的欺骗，因此，网络端和移动台的对鉴权的安全需求也具有不对称性，一般来说，更重要的是要防止虚假移动台对网络进行欺骗。基于移动通信网的这种不对称性，本文提出了采用不同的机制实现 TETRA 双向鉴权功能，即采用基于身份的公钥密码体制实现网络基础设施对移动台的鉴权，采用基于哈希链的机制实现移动台对网络基础设施

的鉴权。

3.1　基于身份公钥的网络端对移动台的鉴权

为解决采用共享秘密的鉴权协议中的密钥分发和存储，一些基于公钥算法的认证技术已经被引入到移动通信中的用户身份识别系统中[7]，但这些系统同样存在网络基础设施需要保存大量的用户公钥的问题。因此本文提出采用基于身份的公钥密码体制[8]在移动通信系统中实现网络基础设施对移动台的鉴权。

基于身份的公钥的 TETRA 鉴权协议的特点是不再需要额外储存移动台秘密信息或公钥证书的鉴权中心，移动台的公钥可由任何人根据其身份信息(即移动台的 ITSI)计算出来，因此不需验证公钥的有效性。而移动台的私钥由密钥管理机构产生。在此系统中，每个移动台首先访问密钥认证中心(KAC)并确定自己的身份，一旦移动台被系统接受，则 KAC 为用户提供一个秘密参数(私钥)。具体的结构如图 2 所示。

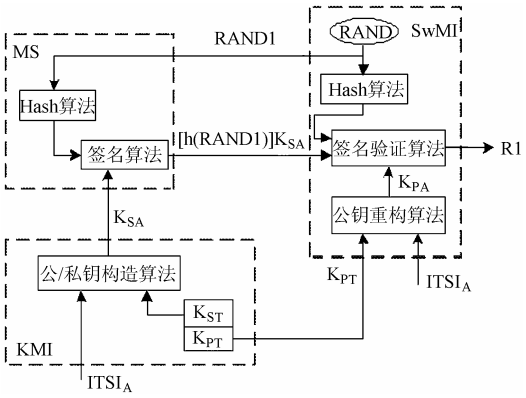

图 2　基于身份公钥的 TETRA 鉴权协议结构

基于身份公钥的TETRA鉴权协议通过下面3个阶段来实现：系统初始阶段、移动台注册阶段、鉴权阶段。具体如下：

(1)系统初始阶段　设定系统参数，主要是指密钥管理机构需要生成它的私钥K_{ST}和公钥K_{PT}，并将密钥管理机构的公钥K_{PT}传给网络端用于移动台的公钥重构；

(2)移动台注册阶段　移动台首先将自己的身份信息$ITSI_A$传送给密钥认证中心，密钥认证中心为移动台产生公/私钥对，例如移动台A的私钥K_{SA}和公钥K_{PA}并通过安全信道存储到相应的移动台中；

(3)鉴权阶段　(a)首先移动台A向网络端提出鉴权申请，在鉴权申请中包含移动台A的身份信息，这里为系统中唯一的个人身份识别码(ITSI)；(b)由TETRA网络端的鉴权实体产生一个随机数RAND1，然后将它发送给需要鉴权的移动台A，计算RAND1的哈希值备用，同时，根据接收到的移动台A的身份信息ID_A，利用公钥重构算法计算出移动台A的公钥K_{PA}；(c) 移动台A采用自己的私钥K_{SA}和签名算法对接收到的RAND1的哈希值进行签名，并将签名结果发给网络；(d) 网络端的鉴权实体收到用移动台A的私钥签名的h(RAND1)后，用在(b)步中计算出来的移动台A的公钥K_{PA}使用签名验证算法来检验签名的有效性。如果验证通过则为合法的移动台，反之，为不合法的移动台。

3.2　移动台对网络端的鉴权

由于移动台的处理能力和存储空间有限，所以建议采用速度较快的椭圆密码算法(ECC)实现上述鉴权协议的签名和验证算法。对ECC本身而言，签名比验证快 2 – 5 倍[9]，如果在计算能力受限的设备上执行，则签名时间和验证时间的绝对值之差更大，因此本文采用效率较高的秘密共享的挑战应答协议实现移动台对网络基础设施的鉴权，其中采用哈希链机制的目的是为了保护初始密钥K_0。具体如下：

(1)系统初始阶段　设定系统参数，主要是指可信的密钥管理机构随机生成初始密钥K_0，利用单向哈希函数对K_0重复计算n次，获得一个长度为n+1的哈希链：

K_0，$K_1=h^1(K_0)$，$K_2=h^2(K_0)$，…，$K_i=h^i(K_0)$，…，$K_{n-1}=h^{n-1}(K_0)$，$K_n=h^n(K_0)$

其中n的取值由系统安全策略决定。同时可信的密钥管理机构通过安全信道将初始密钥K_0送到网络端；

(2)移动台注册阶段　密钥管理机构为移动台随机分配一对数据$(i,K_i)(1<i<=n)$，通过安全信道传送到相应的移动台中，(i,K_i)用于将来对网络端的验证；

(3)鉴权阶段　如果移动台通过了网络端的鉴权，则转入下面的移动台对网络的鉴权过程。

(a) 移动台A产生一个随机数RAND2，将$(i$,RAND2)发给网络端；

(b) 由TETRA网络端根据收到的i，对K_0运行i 次哈希运算，得到K_i，根据RAND2和Ki运行与原TETRA系统中TA12类似的算法，计算的结果为RES2，并把RES2返回给移动台A；

(c) 移动台A采用自己的Ki和RAND2运行和网络端相同的算法等到XRES2，比较XRES2和收到的RES2，如果相同则网络端合法，反之，为不合法的网络。

注意尽管这里采用哈希链机制来保护初始密钥K_0，但是K_0泄漏的可能性仍然存在，为了减少K_0泄漏要为所有的移动台来重新分配密钥的代价，在系统实施过程中，可以采用按照用户组织来分配K_0，系统为每个不同的用户组织保存一个K_0，这样当某个组织的K_0泄漏时，只需要更新该组织内部的

移动端的密钥即可。

3.3 新协议的分析

通过对上面提出的鉴权协议进行分析可得出如下结论:

(1) 本方案的安全性依赖于方案中的加密算法、签名算法的安全性和密钥管理机构对用户身份识别的严格性及私钥的保密性;

(2) 在基于身份公钥的网络端对移动台的鉴权协议中,由于是 MS 对挑战 RAND1 经过了一次哈希变换后再用自己的私钥进行签名,因此即使在不安全信道上进行传输,也不能够造成对已知明文攻击的开放性,同时这种采用随机数作为挑战的方式可以有效防止重放攻击;

(3) 网络端对移动台的鉴权协议是基于身份公钥的挑战应答协议,所以既不需要像原TETRA系统那样需要网络端保存和维护大量的鉴权主密钥的信息,也不需要像传统的公钥密码体制那样保存大量的公钥信息,网络端只需要秘密保存好用于实现移动台对网络端的鉴权的初始密钥K_0;

(4) 从网络收到鉴权发起端的鉴权请求开始计算,在进行双向鉴权时新协议的信息交互次数也为 5 次,与原协议的信息交换次数相同,而且,新协议与原协议的信息交互量也基本相同;

(5) 由于在每个移动台端存有自己的私钥,因此易于提供有效的签名功能,实现不可否认性服务。

4 结束语

本文通过分析 TETRA 系统移动台和网络之间共享秘密的挑战应答式的鉴权协议,结合 TETRA 网络的网络端和移动台资源和安全需求不对称性的特点,给出了一种采用混合的机制实现 TETRA 双向鉴权功能,即采用基于身份的公钥密码体制实现网络基础设施对移动台的鉴权,而移动台对网络基础设施的鉴权采用基于哈希链的机制,所提出的协议可以有效弥补已有系统的缺陷。

参 考 文 献

[1] ETSI ETS 300 392-1. Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design.

[2] ETSI ETS 300 392-7 (2003). Terrestrial Trunked Radio (TETRA); Voice Plus Data (V+D); Part 7: Security.

[3] ETSI EN 300 392-2. Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI).

[4] TETRA MoU. Security and Fraud Prevention Group: End to End Voice Encryption and Key Management. Recommendation 02.

[5] TETRA MoU. Security and Fraud Prevention Group: TETRA Key Distributed. Recommendation 01.

[6] 王育民, 刘建伟. 通信网的安全—理论与技术. 西安: 西安电子科技大学出版社, 2002: 368 – 370.

[7] Chang-Seop Park. On certificate-based security protocols for wireless mobile communication systems. *IEEE Network*, 1997, 11(5): 50 – 55.

[8] Shamir A. Identity-base cryptosystems and signature schemes. Proc. of Crypto'84, Lecture Notes in Computer Science, Springer-Verlag, 1984,Vol. 196: 47 – 53.

[9] The Elliptic Curve Cryptosystem for Smart Cards. Certicom ECC Whitepaper. May 1998. http://www.cer ticom.com

李 晖: 女, 1970 年生, 博士生, 研究方向为信息和网络安全、移动通信安全.

马春光: 男, 1974 年生, 讲师, 博士生, 研究方向为密码学、信息安全、网络安全、电子支付等.

杨义先: 男, 1961 年生, 教授, 博士生导师, 长江学者, 研究方向为密码学、信息网络安全等.