Advances in Applied Mathematics 应用数学进展, 2020, 9(5), 759-764
Published Online May 2020 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2020.95090

Hans汉斯

Improved Lightweight Anonymous Authentication Protocol

Shiqi Zhao, Shengnan Liu, Yiqiao Jia, Xuehan Zhai, Jingshu Jiao, Ping Zhang

School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang Henan
Email: 1309736471@qq.com, 1927160556@qq.com, 869318098@qq.com, 1852351487@qq.com, 1027413286@qq.com, zhangping76@126.com

Received: May 1st, 2020; accepted: May 19th, 2020; published: May 26th, 2020

Abstract

Based on the lightweight anonymous authentication protocol based on Li protocol, an improved lightweight anonymous authentication protocol is proposed in this paper. By assigning serial numbers to user information stored in the serve, in the authentication stage, the user only needs to send the location serial number encrypted by the corresponding public and private keys and the encrypted user's real information to the server for authentication. The authentication server works out the location serial number of the user and calculates the user's information corresponding to this serial number and verifies it to complete the authentication process. Further performance analysis shows that the proposed scheme not only has the high security of lightweight anonymous authentication protocol, but also has more efficient authentication.

Keywords

Smartphone, Anonymous Authentication, Shared Key, Lightweight

改进的轻量级匿名认证协议方案

赵士琦，刘胜男，贾亦巧，翟薛涵，焦靓姝，张　平

河南科技大学数学与统计学院，河南　洛阳
Email: 1309736471@qq.com, 1927160556@qq.com, 869318098@qq.com, 1852351487@qq.com, 1027413286@qq.com, zhangping76@126.com

收稿日期：2020年5月1日；录用日期：2020年5月19日；发布日期：2020年5月26日

摘　要

本文基于Li协议的轻量级匿名认证协议，提出了一种改进的轻量级匿名认证协议方案。通过对服务器中

文章引用: 赵士琦, 刘胜男, 贾亦巧, 翟薛涵, 焦靓姝, 张平. 改进的轻量级匿名认证协议方案[J]. 应用数学进展, 2020, 9(5): 759-764. DOI: 10.12677/aam.2020.95090

存储的用户信息进行序号分配，认证阶段用户仅需发送经相应公私钥对共同加密后的位置序号以及加密后的用户真实信息到服务器进行认证，认证服务器反解出用户序号，计算该序列号所对应的用户信息并验证，完成认证过程。进一步的性能分析表明，所提方案不仅具有轻量级匿名认证协议的高安全性，也使得认证过程更加高效。

关键词

智能手机，匿名认证，共享密钥，轻量级

1. 引言

随着无线通讯技术的不断发展，如今选择使用智能设备访问网络来获取信息的人数日趋增多。而用户在使用无线移动互联网络(Wireless Mobile Internet, WMI)时往往很容易受到攻击等各种各样的安全问题，如无线网络的开放性较高，传输信号不稳定，鲁棒性较差，且无线网络的拓扑结构是动态的等。导致用户在使用无线网络时易受到主动干扰、被动窃听信息数据、在无线网络环境下攻击者通过使用假基站诱使用户与其进行认证而获取用户的身份信息等。这使得构建一个安全高效的匿名认证方案成为了热门话题。

现有的无线网络匿名认证方案主要分为基于共享密钥和基于非共享密钥两种。现有方案大多是基于非共享密钥的，此类匿名认证方案主要是通过签名算法[1] [2]、公钥算法[3]、零知识证明[4]等算法来实现匿名。但此类方案计算量较大、对储存空间要求较大、不适用于无线网络环境。目前匿名认证方案主要通过假名机制[6]、*HASH*机制[7]等途径来实现匿名认证，而少部分是基于共享密钥的匿名认证方案[5]。

文献[6]中 *Li* 基于非共享密钥提出了一种使用 *k*-假名集合来实现匿名性的轻量级无线匿名认证协议。文献[8]通过研究发现在 *Li* 所提的匿名认证协议中，认证服务器对用户认证请求的处理时延会导致用户身份的泄露，之后提出了一个有分组机制的改进 *Li* 协议的匿名认证方案。本文对改进了的 *Li* 协议的匿名认证进行分析，发现此方案中并没有找到一个合理的分组机制，且方案中存在服务器需对用户所在组 *GID* 进行遍历才能验证用户身份的情况，导致此认证方案较为低效，故本文将在此基础上提出一个更为高效与安全的匿名认证方案。

现对本文中所用到的一些匿名认证算法中的符号含义进行简单的介绍，具体的内容如表 1 所示。

Table 1. The comparison table for protocol symbols
表 1. 协议对照表

符号	含义
SNonce	认证服务器生成的随机数
CNonce	用户生成的随机数
C	用户真实身份标识
GID	用户所在组的组标识
HMAC	哈希函数

Continued

Key	用户和认证服务器的共享密钥
SK	用户和认证服务器的会话密钥
e_1	认证服务器的公钥
d_1	认证服务器的私钥
e_2	用户的公钥
d_2	用户的私钥
N	用户序号

2. 改进的轻量级匿名认证协议方案

本协议需要认证服务器预先给用户进行序号分配，并将序号通过安全信道分发给用户，代替了原协议中将用户进行分组并将用户所在组的组标识发送给用户这一过程。在本协议中，服务器和每个用户都拥有自己的公钥以及私钥，用户在请求认证时，将由用户私钥及认证服务器的公钥加密后的随机数、排序序号等认证信息发送给用户，认证服务器经认证服务器私钥和用户公钥反解出该序号，计算认证信息并验证用户信息，从而完成服务器对该用户的认证，用户与认证服务器的具体流程如图 1 所示。

step1 用户→认证服务器

首先由用户请求开始匿名认证，消息内容是 32 比特长的字符串信息。

step2 认证服务器→用户

认证服务器收到用户发送的请求消息。产生随机数 $SNonce$ 发送给用户，长度为 64 比特。

step3 用户→认证服务器

该步骤与原协议的计算方法有所不同，随机数 $SNonce$ 到达用户端后，用户生成随机数 $CNonce$，然后计算 N_C，M_C。规定 N_C，M_C 的计算公式分别如下

$$N_C = e_1 d_2 (N)$$

$$M_C = HMAC(SNonce \| CNonce \| ID)$$

$$L = e_1 (e_2)$$

其中 e_1，d_2 分别为认证服务器的公钥和用户的私钥，公式中“||”是字符串联接符，N 为用户序号，ID 为用户真实身份标识。

用户发送 M_C，$CNonce$，N_C，L 到服务器进行认证。

step4 认证服务器→用户

匿名认证服务器接收用户发送的 M_C，$CNonce$，N_C，L。首先依据 $d_1(L)$反解出用户的公钥 e_2，然后再根据 $d_1 e_2(N_C)$反解出 N，然后计算服务器中第 N 位用户的 M_C' 并验证是否与 M_C 相等，其中

$$M_C' = HMAC(SNonce \| CNonce \| ID)$$

若相等，则认证成功；若不相等，则认证失败。

若认证成功，则服务器计算

$$M_S = HMAC(CNonce \| e_1)$$

并将 M_S 发送给用户，用户收到消息后，以相同方式计算 M_S’然后进行比对，若相同，则客户端认证服务器成功，否则即是失败。

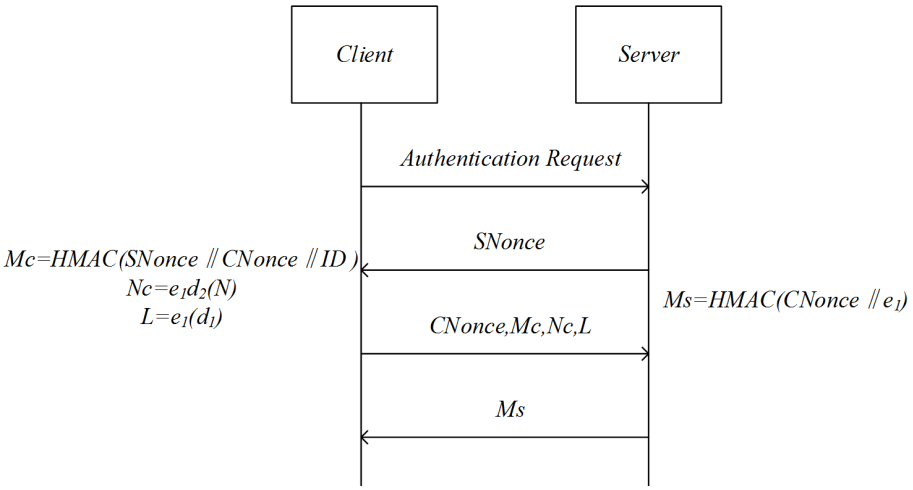

Figure 1. The improved lightweight anonymous authentication protocol
图 1. 改进的轻量级匿名认证协议

3. 安全性分析

3.1. 抵抗时间关联攻击

Li 所设计方案中在认证过程中虽然使用了 *k*-假名集合，但是在认证过程中直接以明文的方式发送了包含用户的真实 *ID* 的假名集合给认证服务器，且容易被攻击者截获，通过文献[8]可知，攻击者可通过认证时间来判断用户真实 *ID* 在假名集合中的位置，从而便可进一步确定用户真实身份，造成用户隐私信息泄露。

本文方案使用公私钥以及 *Hash* 机制对用户的身份信息进行加密，由于 *Hash* 机制为单向函数，故攻击者不可依据所截取的认证消息反解出用户的身份等信息，进一步保证了用户的不可追踪性，因此可以保证用户的隐私安全。

3.2. 抵抗重放攻击

本文所设计匿名身份认证协议的交互过程引入了挑战-应答机制。保证了认证过程中传输消息的新鲜性。认证服务器收到用户发来的认证请求后发送一个随机数 *SNonce* 给用户。用户使用共享密钥和 *SNonce* 生成一条认证消息 M_C，并将 M_C 和自己生成的随机数 *CNonce* 发往认证服务器。认证服务器用共享密钥计算 M_C 与 M_C 比较即可知道该消息是不是具有新鲜性。因为只用相同的随机数计算的消息才会相同，而认证服务器使用的是最新产生的随机数。同理用户也可以通过自己产生的随机数 *CNonce* 验证服务器发来的消息是否具有新鲜性，因此可以抵抗重放攻击。

3.3. 抵抗伪装攻击

本文所设计匿名身份认证协议通过公私钥加密来抵抗伪装攻击。用户在认证之前需要先到认证服务器注册。然后获得自己所在服务器中的用户序号，交互过程中用户发送认证消息 M_C 到认证服务器。认证服务器使用服务器的私钥反解出用户的公钥，再运用用户的公钥服务器的私钥反解出用户序号，进而依据 M_C' 公式生成消息 M_C' 与 M_C 进行比较。因为用户的私钥和服务器的私钥只有用户和认证服务器拥有，而攻击者没有，因此若 M_C' 与 M_C 相等则可证明该消息是来自用户的，且引入的挑战－应答机制避免了消息的重放攻击，因此能抵抗攻击者伪装合法用户。同理用户亦可通过消息 M_S 来识别认证服务器是否被伪装。基于上述分析可知所设计匿名认证协议能够抵抗攻击者的伪装和对认证服务器的攻击。

4. 性能分析

4.1. 认证时间

认证时间是评估一个身份认证协议性能的重要标准。基于 *Li* 协议的轻量级匿名认证协议通过在服务器端对用户分组来进行认证，而在认证过程中会出现服务器需要遍历 *GID* 的情况，故此协议用户分组的大小是影响认证时间的重要因素。

本文所提出的改进的轻量级匿名认证协议方案选择利用公私钥对进行加密从而避开了用户分组机制中对用户分组方式不明确以及在服务器认证用户阶段时遍历 *GID* 导致的认证效率低下的问题，从而减少了认证时间，提高了认证效率。

4.2. 计算量

计算量指的是认证过程中计算认证消息所需计算量，分别为用户端计算量和认证服务器端计算量。用户在认证过程中需要进行的计算主要包括以下内容：

1) 用户端计算量包括 2 次异或运算、2 次 *Hash* 运算和 2 次随机数运算；

2) 认证服务器端计算量包括 2 次异或运算、2 次 *Hash* 运算和 1 次随机数运算。

根据上述计算量统计，并与现有的基于共享密钥的研究进行对比，对比结果如表 2 所示。可以看出本文所设计出方案在保证上述优点的同时并不增加计算量，并且通过合理的设置认证服务器端用户分组大小，可以保证用户端和认证服务器端的性能。

Table 2. Comparison of calculation
表 2. 计算量对比

运算方式	文献[5]	文献[6]	文献[8]	本文
Hash 运算	n + 10	r + 3	r + 3	4
异或运算	13	4	4	4
随机数运算	2	4	4	4

其中 r 表示用户真实身份标识在假名集合中的具体位置，n 表示用户分组大小。上述性能测试与评估结果表明所设计匿名认证协议具有认证时间短、计算量小、所需存储空间小的特点，因此该方案具有轻量级的特点，能更好的适用于无线网络环境。

5. 结论

本文简单介绍了基于 *Li* 协议的轻量级匿名认证协议的缺陷，即在认证过程中认证服务器存在需遍历用户所在分组 *GID* 才可完成认证的情况，且并未对如何确定有效合适的 *GID* 分组方法进行具体研究。通过引入用户与认证服务器的公私钥，提出了一种改进的轻量级匿名认证方案。本文所设计的认证方案能够抵抗时间关联等攻击，同时也规避了无法有效合理地将用户分组的问题，并通过安全性及性能分析，证实了本文所提的改进的轻量级匿名认证方案具有较强的安全性，同时具备轻量级且高效的特点。

基金项目

河南省高等学校重点科研项目(项目编号：20A520012)；河南科技大学大学生研究训练计划(SRTP)项目(项目编号：2019201)。

参考文献

[1] Shao, J., Lin, X., Lu, R., *et al*. (2016) A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Transactions on Vehicular Technology*, **65**, 1711-1720. https://doi.org/10.1109/TVT.2015.2405853

[2] Chim, T.W., Yiu, S.M., Hui, L.C.K., *et al*. (2009) SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs. *Ad Hoc Networks*, **9**,189-203. https://doi.org/10.1016/j.adhoc.2010.05.005

[3] Wan, Z., Ren, K. and Preneel, B. (2008) A Secure Privacy-Preserving Roaming Protocol Based on Hierarchical Identity-Based Encryption for Mobile networks. *ACM Conference on Wireless Network Security*, *WISEC* 2008, Alexandria, 31 March-April, DBLP, 62-67. https://doi.org/10.1145/1352533.1352544

[4] Goldwasser, S., Micali, S. and Rackoff, C. (1989) The Knowledge Complexity of Interactive Proof-Systems. DBLP, 291-304.

[5] Gódor, G. and Imre, S. (2012) Hash-Based Mutual Authentication Protocol for Low-Cost RFID Systems. *Proceedings of the Information and Communication Technologies*, Budapest, 76-87. https://doi.org/10.1007/978-3-642-32808-4_8

[6] Li, X., Liu, H., Wei, F., *et al*. (2015) A Lightweight Anonymous Authentication Protocol Using k-Pseudonym Set in Wireless Networks. *IEEE Global Communications Conference*, IEEE, 1-6. https://doi.org/10.1109/GLOCOM.2015.7417584

[7] Syamsuddin, I., Dillon, T., Chang, E., *et al*. (2008) A Survey of RFID Authentication Protocols Based on Hash-Chain Method. *International Conference on Convergence and Hybrid Information Technology*, IEEE, 559-564. https://doi.org/10.1109/ICCIT.2008.314

[8] 钟成, 李兴华, 宋园园, 马建峰. 无线网络中基于共享密钥的轻量级匿名认证协议[J]. 计算机学报, 2018, 41(5): 4-6.