

应用于网间互联控制协议的轻量级认证方法

卢波^{1,2}, 刘赞³, 张洁⁴, 陆月明^{1,2}

- (1. 北京邮电大学网络空间安全学院, 北京 100876;
2. 可信分布式计算与服务教育部重点实验室, 北京 100876;
3. 海军参谋部航行保证局, 北京 100847;
4. 军事科学院系统工程院, 北京 100091)

摘要: 针对天地一体化网络对网间互联安全控制的需求以及有限资源不能采用高计算复杂度认证方法的问题, 提出了一种应用于网间互联控制协议的轻量级认证方法, 在公钥加解密算法和签名算法中, 采用了随机填充的思想, 通过有限资源的计算, 在网间互联控制协议中实现实体认证, 采用形式化分析工具 Scyther 对协议进行安全性分析, 并通过仿真实验和其他安全通信协议做性能比较, 结果表明该方法可以满足网络有限资源计算的要求, 且保证了安全性。

关键词: 轻量级认证; 有限资源计算; Rabin 算法; 安全通信协议

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018090

Lightweight authentication method for network interconnection control protocols

LU Bo^{1,2}, LIU Yun³, ZHANG Jie⁴, LU Yueming^{1,2}

1. School of Cyber Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing 100876, China
3. Naval Staff Navigation Assurance Agency, Beijing 100847, China
4. Institute of Systems Engineering, Academies of Military Science, Beijing 100091, China

Abstract: As network interconnection controls are required for the space-earth integrated network and the limited resources are not suitable for high computing complexity degree authentication methods, a lightweight authentication method for network interconnection control protocols is proposed. Through the calculation of limited resources, using the idea of random fill, It design and implement public key encryption and signature algorithm which is components of the networks interconnection control authentication protocol. Formal analysis tool Scyther is used to analyze the security of the protocol. Comparing with other secure communication protocols, the method can meet the requirements of resource-constrained networks and ensure the safety.

Key words: lightweight authentication, limited resource computing, Rabin algorithm, security communication protocol

1 引言

天地一体化网络军民共用, 不同网络安全域

差异化大, 网间互联安全控制难度大, 通过网间互联控制协议实现细粒度控制是一种有效的安全通信手段。网间互联控制协议中, 实体之间为了

收稿日期: 2018-07-01; 修回日期: 2018-10-03

通信作者: 陆月明, ymlu@bupt.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0800302)

Foundation Item: The National Key R&D Program of China (No.2016YFB0800302)

保证可信和安全需要认证, 结合承载于卫星的网络安全控制设备计算资源是受限的实际情形, 传统的一些通信协议, 如安全超文本传输协议 (HTTPS, hyper text transfer protocol over secure socket layer)、安全传输层 (TLS, transport layer security) 协议、互联网安全关联和密钥管理协议 (ISAKMP, Internet security association key management protocol)、安全外壳 (SSH, secure shell) 协议等并不满足资源受限环境下的认证和加密需求。在卫星加密通信方面, 吕涛等^[1]介绍了卫星通信加密机 DLE-7000 (data link escape-7000), 它是一款可团体定制密码模块, 对卫星通信进行加密。向红权等^[2]设计实现了基于 FPGA (field programmable gate array) 的对称序列密码算法和密码同步电路, 对卫星通信系统的链路进行加密。邹宇聪等^[3]提出了一种以混沌加密为基础的微小卫星通信数据加密技术。郑建宏等^[4]提出了椭圆曲线算法和对称加密算法结合的混合加密算法并应用于卫星通信系统。王宝成等^[5-6]在 DVB-RCS (digital video broadcasting; interaction channel for satellite distribution systems) 设计上实现了加密系统和密钥管理系统, 采用 AES (advanced encryption standard) 对称分组密码算法、椭圆曲线密码 (ECC, elliptic curve cryptography) 算法、SHA1 (secure hash algorithm) 密码杂凑算法, 并从硬件物理噪声获取随机数。以上都提供了相应的轻量级加密算法来实现卫星之间的加密通信。陈铁明等^[7]提出了一种基于 WSN (wireless sensor networks) 混沌密码的轻量级无线传感器网络链路加密协议 (TinyTCSec, tiny protocol for securing sensor networks with tree parity machine and chaos technology)。马韶璞等^[8-9]提出了在甚小口径卫星终端 (VSAT, very small aperture terminal) 网络下采用 RSA (ron rivest, adi shamir, leonard adleman) 公钥算法实现轻量级认证协议。高利军^[10]和汪洋^[11]采用 RFID (radio frequency identification) 技术实现轻量级物联网无线通信协议。该协议基于 Rabin 加密体制和 AES 对称加密混合实现。吴伟民等^[12]提出了一种基于混沌密码的轻量级 RFID 所有权转移协议, 通过 BAN 逻辑进行安全性分析并且和一些传统协议做了比较。

综合上面的情形, 所采用的加密方案可以做如下归类: DES 加密、序列加密、混沌加密等对称加密算法; 椭圆曲线加密、RSA 加密通信、Rabin 加密等非对称加密或签名算法; SHAx 等摘要算法。文献[1-2]侧重对设备的硬件实现做介绍, 对密码算法组合实现的协议较少做设计和安全分析; 文献[1-3,7,12]通过混沌、AES 或者 DES 对称加密实现协议; 文献[4-6]采用了 ECC 公钥算法, 而 ECC 算法硬件实现相比 Rabin 算法较为复杂; 文献[8-9]通过 RSA 实现通信协议, 没有 Rabin 加密速度快; 文献[10-11]通过 Rabin 算法和对称加密算法的组合实现轻量级通信协议。在安全性分析方面, 文献[5-6,10]对协议的安全性分析仅限于有限的几种已知攻击类型, 并未做形式化安全分析; 文献[11]通过 BAN 逻辑对协议做了形式化安全分析, 但 BAN 逻辑对敌手的假设太弱, 很多协议的漏洞 (如 Needham-Schroeder 协议) 在基于 BAN 逻辑的形式化分析中没有被发现。本文基于 Rabin 算法设计公钥加密算法和签名, 通过加密算法组合实现通信协议, 并基于 Dolev-Yao 攻击模型对协议做形式化安全分析, 增加了协议安全可信度。

在应用层面, 资源受限为网络空间安全带来了新的挑战, 已有的安全通信手段不能够直接适用于资源受限的设备, 原因有很多方面, 包括通信数据分组过于庞大、协议通信握手次数较多、能源和带宽消耗过多。

针对计算资源受限问题, 本文提出一种轻量级的认证方法 (简称“轻量级认证方法”) 应用于天地一体化网络的网间互联安全控制协议。轻量级认证方法设计的“网间互联安全控制协议”是一种相对封闭和通信量小, 运行在计算资源受限的载体上, 可处理加密、认证和签名等功能的协议。

2 轻量级认证方法

轻量级认证方法包括加解密算法、签名算法、协议设计以及对两类算法进行随机化填充的方法。在加解密算法和签名算法中都采用了 Rabin 算法。Rabin 算法是基于整数分解的困难性问题, 整数分解 (IF, integer factorization) 问题表述为: 通过输入一个整数 N , 把其分解为 2 个素因子, 要求算法能够计算出 N 的一个素因子 p , 满足 $p|N$,

这个问题是困难的。

这个问题意味着一种情形：用户随机地筛选出2个大素数 p 、 q ，计算其合数 $N=pq$ 作为算法输入，而对手获取 N 后，他的目标是找到 N 的一个因子 p 或者 q ，使 p 整除 N 或者 q 整除 N 。在这个过程中，用户随机筛选 p 、 q 的过程和计算合数 $N=pq$ 的过程是易于计算的，普通的计算机就能够胜任。但敌手仅仅通过 N 分解出它的因子 p 或者 q ，在通常情况下是代价高昂的，如运用大量的网络并行计算资源在多项式时间内都无法计算出来。利用整数分解的计算困难性构造密码系统，整数分解问题并不总是困难的，需要进一步量化这个情形，使密码系统涉及整数 N 的因子分解都是困难性问题，下面具体地量化这种情形。

整数分解假设（IF 假设）：一个整数分解器是一个概率多项式时间复杂度的 PPT（probabilistic

polynomial time）算法 A ，满足概率 $\varepsilon > 0$ 且 $\varepsilon = \Pr[A(N) \text{ 整除 } N, 1 < A(N) < N]$ 。令 IG（integer generator）是整数生成器，输入 1^k ，在 k 的多项式时间输出 $2k$ bit 的模 $N=pq$ 。其中， p 和 q 是 k bit 的随机奇素数。IG 满足整数分解假设，对于所有足够大的 k ，若对于 k 不可忽略的概率 $\varepsilon > 0$ ，不存在由 IG(1^k)所产生的整数分解算法。

上面的假设意味着，对于合理的安全参数设置，该问题是困难的。当前因子分解的主要算法类型为数域筛选法，相对于当前并行计算机的计算能力，模 N 的长度在 1 024 bit 是一个比较安全的世界。

本文用到的所有符号说明如表 1 所示。

Rabin 算法的映射记为 $f: Z_n \rightarrow Z_n$ ，映射具体的表达式是在模 N 运算下的一元二次表达式 $f(m, b, N) = m^2 + bm \pmod{N}$ 。通过输入不同的明文 m ，能够计算出对应的密文 c ；同样地，在已知密文 c

表 1 符号释义

符号	解释
Z_n	模 n 剩余类记为 $\{[0], [1], [2], \dots, [n-1]\}$
f, f^{-1}	函数 f 和对应的逆函数 $f^{-1}: Z_n \rightarrow Z_n$ ，分别对应 Rabin 加密过程和解密过程
N	合数，在本文加解密算法和签名算法中 $N=pq$ 。
p, q	素数（只有 1 和它本身是因子的数）
PPT 算法	多项式时间内可以计算出结果的随机概率算法
1^k	表达的是问题的规模，只有问题规模足够大时，IF 问题才有可能困难的
$(\text{mod } N)$	模 N 运算是对于整数模 N 取其余数作为计算结果
M	明文，待加密的文字
c	密文，加密后的符号序列
$\equiv$	$a \equiv b$ (a 和 b 同余)，即 a 和 b 模 N 取余数相等
$1_p, 1_q$	1_p 是指和 1 在模 p 下同余的数， 1_q 同理
p_x, q_x	p_x 是指和密文 c 在模 p 下同余的数， q_x 同理
b	区间 $[0, N-1]$
k_{pub}	用公钥加密的密文，只能用对应的私钥解密
k_{pri}	用私钥加密的密文，只能用对应的公钥解密
$K_{\text{pubA}}, K_{\text{pubB}}, K_{\text{pubC}}$	分别指用户 A、B、C 持有的私钥相对应的公钥
$K_{\text{priA}}, K_{\text{priB}}, K_{\text{priC}}$	分别指用户 A、B、C 持有的私钥
R_A, R_B, R_C	分别指用户 A、B、C 产生的一次性随机数
$User_A, User_B, User_C$	分别指用户 A、B、C 的格式化身份信息
$\parallel$	比特串连接运算，将 2 个串连接在一起

的情形下，逆向求解过程就是解一元二次方程的根，在复数域下有 2 个根，但是在离散状态下求解，就变成了求解二次剩余问题，它的求解方法和 N 的因子 p 、 q 有关，特别地，在 Blum 整数（即满足 $p \equiv q \equiv 3 \pmod{4}$ ）条件下可以很快地求解 Δ 的二次剩余，从而解得方程的根，其中有一个解是 m 。

f 是一个单向限门函数，限门为 (p, q) ，即只有在知道具体 p 、 q 的取值下，求解 $f(m, b, N) - c = 0$ 的解才会容易，否则只知道 N 是困难的。通过这种特性，可以实现加解密和签名。

更进一步地，在只知道 N 的条件下，求解 $f(m, b, N) - c = 0$ 的困难性和 $p-1$ 、 $q-1$ 的因子结构有很大关系，确保都有大因子是保证困难性的必要条件，本文通过采用强非平滑素数的方法，保证了这一点。设 $N=pq$ ， p 和 q 为 Blum 整数，即满足 $p \equiv q \equiv 3 \pmod{4}$ ，并且 p 和 q 都是强非平滑素数，即 $\frac{p-1}{2}$ 、 $\frac{q-1}{2}$ 仍然是素数，这种设定保证了大因子的困难性条件。综上所述，Rabin 变换记为 $f(m, b, N) = m^2 + bm \equiv c \pmod{N}$ ，其中，公钥 $k_{\text{pub}} = (b, N)$ ，私钥 $k_{\text{pri}} = (b, N, p, q)$ 。

2.1 Rabin 加解密

Rabin 加解密包括加密和解密两部分，其中加密过程为

$$c \equiv f(m, b, N) \pmod{N}$$

解密过程为

$$f^{-1}(c, b, N, p, q) = m = \frac{-b \pm \Delta}{2}$$

$$\Delta = \sqrt{b^2 - 4c}$$

根据中国剩余定理求解同余方程组，解得由 $\text{mod } p$ 下的同余 1_p 、 $\text{mod } q$ 下的同余 1_q 、 $p_x \equiv c \pmod{p}$ 、 $q_x \equiv c \pmod{q}$ 这 4 个参数共同构成的 4 个解： $x_1 = 1_p p_x + 1_q q_x$ 、 $x_2 = 1_p(p - p_x) + 1_q q_x$ 、 $x_3 = 1_p p_x + 1_q(q - q_x)$ 、 $x_4 = 1_p(p - p_x) + 1_q(q - q_x)$ ，通过有效识别机制找到对应明文解 x_i 作为明文 m 。

2.2 Rabin 签名

Rabin 签名包括签名和验证两部分，其中，签名过程为

$$\text{sign}(c) = f^{-1}(c, b, N, p, q) \pmod{N}$$

验证过程为

$$\text{verify}(c) = f(m, b, N) \pmod{N}$$

3 轻量级认证流程

协议中 $\{M\}_K$ 表示对消息 M 使用密钥 K 加密。只有拥有与 K 相匹配的解密密钥 K^{-1} 的主体可以解密出 M 。 $[M]_K$ 表示密钥 K 对消息 M 的单向变换，表明对 M 提供的安全性服务具有消息源识别的数据完整性。 R_A 代表用户 A 产生的随机数， Cert_C 代表用户 C 的公钥证书。

通过构造协议 1——网间互联控制子协议（Sub-NICAP, sub-network interconnection control protocols）实现用户和管理员之间的基本认证功能，再将其作为协议 2——（网间互联控制协议（NICAP, network interconnection control protocols）的一部分共同完成用户 A 和用户 C 在管理员用户 B 参与下的身份认证。

3.1 协议 1

网间互联控制子协议的通信过程如下。

1) 用户 A 给用户 B 发送的内容是

$$[\{R_A\}_{K_{\text{pubB}}}, \text{User}_A, \text{User}_C]_{K_{\text{priA}}}$$

该部分密文内部结构为一元组，密文和其他 2 个身份格式化信息共同构成三元组结构的消息，消息和消息摘要共同构成两元组结构的最终消息，通过底层协议编码发送。

2) 用户 B 给用户 A 发送的内容是

$$[\{R_A, R_B\}_{K_{\text{pubA}}}, \text{Cert}_C]_{K_{\text{priB}}}$$

该部分密文内部结构为二元组，密文和身份格式化信息共同构成二元组结构的消息，消息和消息摘要共同构成两元组结构的最终消息，通过底层协议编码发送。

3) 用户 A 给用户 B 发送的内容是

$$[\{R_B\}_{K_{\text{pubA}}}]_{K_{\text{priA}}}$$

该部分密文内部结构为一元组，密文和对应的消息摘要共同构成两元组结构的最终消息，通过底层协议编码发送。

协议 1 的功能理解为用户 A 和用户 B 的双向认证，并从用户 B 下载用户 C 的证书。整个过程记为 $p(\text{User}_A, \text{User}_B, \text{User}_C)$ 。

3.2 协议 2

网间互联控制协议的通信过程如下。

1) $p(\text{User}_A, \text{User}_B, \text{User}_C)$, 即用户 A 向用户 B 请求下载用户 C 的证书。

2) 用户 A 给用户 C 发送的内容是

$$[\{R_A\}_{K_{\text{pubC}}}, \text{User}_A]_{K_{\text{priA}}}$$

该部分密文内部结构为一元组, 密文和身份格式化信息共同构成二元组结构的消息, 消息和消息摘要共同构成两元组结构的最终消息, 通过底层协议编码发送。

3) $p(\text{User}_C, \text{User}_B, \text{User}_A)$, 即用户 C 向用户 B 请求下载用户 A 的证书。

4) 用户 C 给用户 A 发送的内容是

$$[\{R_A, R_C\}_{K_{\text{pubA}}}]_{K_{\text{priC}}}$$

该部分密文内部结构为二元组, 密文和对应消息摘要共同构成两元组结构的最终消息, 通过底层协议编码发送。

用户 A 给用户 C 发送的内容是

$$[\{R_C\}_{K_{\text{pubC}}}]_{K_{\text{priA}}}$$

该部分密文内部结构为一元组, 密文和对应的消息摘要共同构成两元组结构的最终消息, 通过底层协议编码发送。

协议 2 的功能理解为用户 A 和用户 B 双向认证, 用户 C 和用户 B 双向认证, 用户 A 从用户 B 获取用户 C 的公钥证书, 用户 C 从用户 B 获取用户 A 的公钥证书, 然后用户 A 和用户 C 完成双向认证。这里的用户 B 是一个具有管理功能的中心节点, 能够为其他节点提供证书查询服务, 帮助其他节点之间完成双向认证。

在轻量级认证方法中, 会对协议中用到的加密和签名做具体的阐释, 将加密和签名原语中的明文、密文、公私钥、签名做对应的实现。

4 轻量级认证方法实现

结合实际应用所面临的安全情形, 进一步增强加密和签名的语义安全性。采用“随机填充”的方式进一步细化对应的算法内部结构, 以达到挫败敌手攻击意图的目的。

4.1 算法 1: Rabin 最优非对称加密填充

设 $(N, G, H, b, p, q, k_0, k_1) \rightarrow \text{Gen}(1^k)$ 满足: $(N, b,$

$p, q)$ 是 Rabin 密钥信息, 公钥为 (N, b) , 私钥为 (N, b, p, q) , 其中, $N=pq$; $|N|=k=n+k_0+k_1$, n 为明文的分组长度; G, H 是 2 个杂凑函数, 且满足

$$G: \{0,1\}^{k_0} \mapsto \{0,1\}^{k-k_0}, H: \{0,1\}^{k-k_0} \mapsto \{0,1\}^{k_0}$$

在加密过程中, 把格式化的明文通过杂凑函数和随机数均匀地扩散到整个消息空间中。发送分组消息为 $m \in \{0,1\}^n$, 发送方执行如图 1 所示加密过程运算。

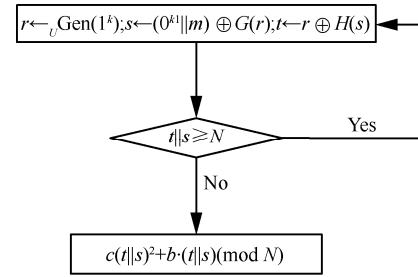


图1 加密过程

在解密过程, 通过偏移量解析出对应的解密片段, 再通过 $\oplus$ 运算还原明文。

收到密文 c 后, 执行如图 2 所示解密过程运算。

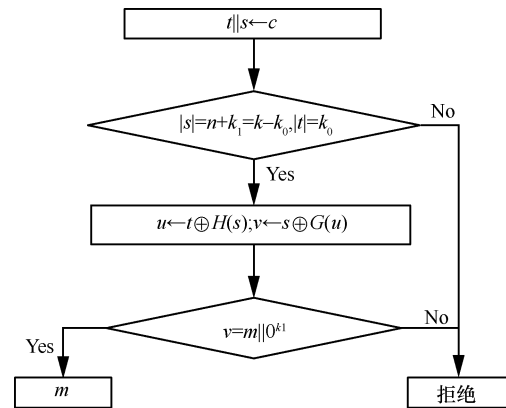


图2 解密过程

下面 Rabin 加解密/签名实例中, 模 N 的长度为 1 024 bit, 强素数 p, q 长度为 512 bit。在借鉴 Bouncy Castle Java Cryptography API 库^[13-14]的基础上, 按照该库的接口规范实现 Rabin 加解密和签名的扩展, 包括引擎部分、块处理操作、公私钥接口实现等。在可变长散列函数的实现方面, 采用 512 bit 的 SHA-512 算法构造短摘要类, 从而构造出加解密和签名所需要的 G, H 散列函数。加密和签名都用 text 对应的字符串作为明文 m 进行验证, 对于可以间接推导出的参数, 限于篇幅省略不写。

$t||s$ 作为解密结果有 4 个解, 还原以后可以根据明文尾部是否有 k_1 ($k_1=8$) 个 0 作为选取依据。具体情形如表 2 加解密实例所示。

表 2 加解密实例

text	name:Alice;tel:123456789;e-mail:123@yahoo.com;
p	f71678552cfc9f7a68867c9c4ab00ecd9...
q	fb15efc6f0001ee59a3d17ed12ea85a8f...
b	2a1a9238e303556c7eb21bc3d54784958...
r	2cc1ba5087540445e1283950ca34be05d...
$G(r)$	34DF289FA40DB3A94F2CB37B52E2424C6...
$H(s)$	871DA2AFB096BC71D3C91F75055A65A7F...
c	1C675FBA47083290DA3B8A925BFBA5086...
$t s[2]$	00ABDC18FF37C2B83432E12625CF6EDBA...

从表 2 可以看出, 解密后得到 4 个解 $t||s[0]$ 、 $t||s[1]$ 、 $t||s[2]$ 、 $t||s[3]$ 中对应的明文是 $t||s[2]$, 对其进行还原并检验对应明文的 k_1 个 0 特征, 把符合条件的这个明文作为最终的解密明文 m 。2 个散列函数 G 、 H 起到单向的作用, 并且通过异或的方式确保了密文的可还原性。

4.2 算法 2: Rabin 概率签名

设 $(N, G, H, b, p, q, k_0, k_1) \rightarrow {}_u\text{Gen}(1^k)$ 满足: (N, b, p, q) 是 Rabin 密钥信息, 公钥为 (N, b) , 私钥为 (N, b, p, q) , 其中, $N=pq$; $|N|=k=k_0+k_1$; G 、 H 是 2 个杂凑函数, 将 G 输出的结果分成 2 个子串, 前面 k_g bit G_1 , 其余 $k-k_1-k_g-1$ bit G_2 , 且满足

$$G: \{0,1\}^{k_1} \mapsto \{0,1\}^{k-k_1-1}, H: \{0,1\}^* \mapsto \{0,1\}^{k_1}$$

签名生成过程同样采用了杂凑函数和随机数组合的方法实现消息的扩散, 由于只选取一个解作为签名, 在验证过程中不需要明文的格式化机制识别解, 具体签名过程如图 3 所示。

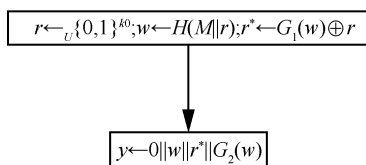


图 3 签名过程

签名验证过程在解密后按照偏移量来解析对

应的解密片段, 再通过 $\oplus$ 运算实现验证过程, 具体验证签名过程如图 4 所示。

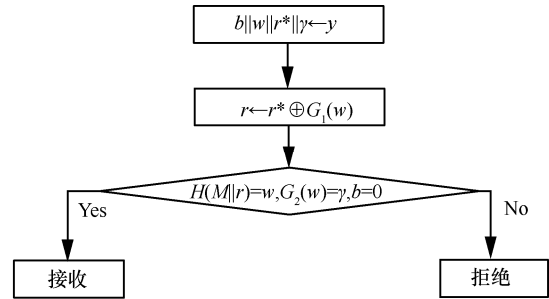


图 4 验证签名过程

在该 Rabin 签名实例中 $k_0=k_1=512$ bit, 通过对 text 作为签名对象 m , 最终生成签名结果 signPSS, 具体情形如表 3 签名实例所示。

表 3 签名实例

text	name:Alice;tel:123456789;e-mail:123@yahoo.com
r	1097a956f6149717e8f4838369987d6392...
$W=H(M r)$	421CF65E6A537D2114C664FFF838598FC8...
$G(w)$	DE6573294E9FB449973A28434D4273699F...
signPSS	EB0CF452BE09DE1BD69CAA79C798D966FD...

4.3 认证协议实现

根据前面设计的算法, 用户 A 的公钥 K_A 进一步表示为 (N_A, b_a) , 持有的私钥 $K_{\text{priA}}=(N_A, b_a, p_a, q_a)$, 用户 B、用户 C 同上。在用户 B 为管理者, 用户 A、用户 C 为普通用户的情形下, 用户 B 和用户 C 实现在线认证的时序图如图 5 协议 1 具体设计结构所示。

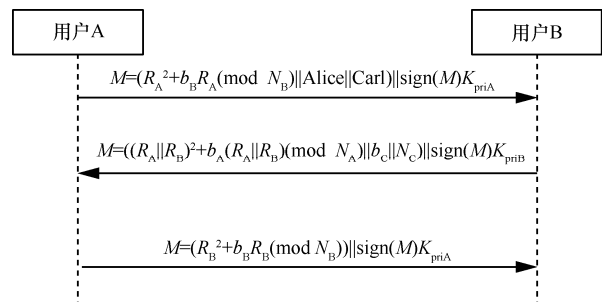


图 5 协议 1 具体通信流程

将协议 1 简记为 $p(\text{User}_A, \text{User}_B, \text{User}_C)$, 该过程实现的是用户 A 和用户 B 之间的双向认证, 且用户 A 从用户 B 查询了用户 C 的公钥证书。

下面通过 3 个用户说明协议的工作流程，他们分别是 Alice、Bob 和 Carl。完整的认证过程如图 6 协议 2 具体设计结构所示。

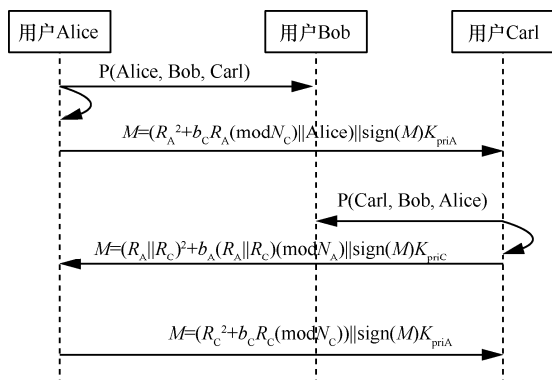


图 6 协议 2 具体通信流程

5 安全性分析

Rabin 算法的安全性已经由 Dan^[15]等做了分析和证明，将 Rabin 算法抽象成一般的加密原语，作为协议的加密元素进行统一建模分析。采用基于项的运算进行形式化安全分析。其中包括角色、消息通信、敌手攻击、协议安全认证性质几个部分，对整个安全通信过程进行形式化分析，通过对迹空间的搜索，证明违背协议安全认证性质的敌手攻击（记为迹）不存在，从而验证了协议的安全。在本协议安全性分析过程中，使用 Dolev-Yao 攻击模型，该模型是安全分析中常用的攻击模型，具体包括如下几个特点：① 可以控制公共网络，包括窃听、篡改消息、改变消息流；② 可以伪装或者控制合法用户为他所用，因而可以以合法用户和其他用户进行会话；③ 不能从大的空间中猜测随机数；④ 没有密钥，无法从密文中恢复明文；⑤ 不能通过明密文对求解出私钥等私有部分。

Scyther 工具是 Cremers 团队^[16]开发的一款自动化协议分析器，采用了 Athena 算法的思想将安全协议的分析^[17-19]模型化为对协议中对应的串空间中迹的分析和搜索，并将协议的安全属性分为机密性和认证性 2 个部分，认证性具体细分为活性性、非单射/单射同步性、非单射/单射一致性几个方面^[20]。本文将协议通过 Scyther 工具所规定语法对其建立协议分析模型，并使用 Scyther

工具进行分析，分析结果表明协议各个角色都具备机密性和认证性（具体包括活性性、同步性和一致性）。具体分析结果如图 7 协议 1 安全属性分析、图 8 协议 2 安全属性分析所示。

Property	Role	Status
clatn SELF.A Weakagree_t5	-	Ok [does not occur]
clatn SELF.A Alive_t6	-	Ok [does not occur]
clatn SELF.A Secret_t7	Ra	Ok [proof of correctness]
clatn SELF.A Secret_t8	Rb	Ok [proof of correctness]
clatn SELF.B Weakagree_s6	-	Ok [does not occur]
clatn SELF.B Alive_s7	-	Ok [does not occur]
clatn SELF.B Secret_s8	Ra	Ok [proof of correctness]
clatn SELF.B Secret_s9	Rb	Ok [proof of correctness]

图 7 协议 1 安全属性分析

Property	Role	Status
clatn SHARE.A Weakagree_t11	-	Ok [does not occur]
clatn SHARE.A Alive_t12	-	Ok [does not occur]
clatn SHARE.A Secret_t13	Ra	Ok [proof of correctness]
clatn SHARE.A Secret_t14	Rb	Ok [proof of correctness]
clatn SHARE.A Secret_t15	Ra2	Ok [proof of correctness]
clatn SHARE.A Secret_t16	Rc2	Ok [proof of correctness]
clatn SHARE.C Weakagree_r10	-	Ok [does not occur]
clatn SHARE.C Alive_r11	-	Ok [does not occur]
clatn SHARE.C Secret_r12	Rc	Ok [proof of correctness]
clatn SHARE.C Secret_r13	Rb2	Ok [proof of correctness]
clatn SHARE.C Secret_r14	Ra2	Ok [proof of correctness]
clatn SHARE.C Secret_r15	Rc2	Ok [proof of correctness]
clatn SHARE.B Weakagree_s11	-	Ok [does not occur]
clatn SHARE.B Alive_s12	-	Ok [does not occur]
clatn SHARE.B Secret_s13	Ra	Ok [proof of correctness]
clatn SHARE.B Secret_s14	Rb	Ok [proof of correctness]
clatn SHARE.B Secret_s15	Rc	Ok [proof of correctness]
clatn SHARE.B Secret_s16	Rb2	Ok [proof of correctness]

图 8 协议 2 安全属性分析

6 性能比较

通过该协议获取对方证书的认证过程，需要进行 3 次双向握手，在加密过程中需要进行 2 次乘法运算复杂度为 $O((\log N)^2)$ ，解密过程中通过模指数运算来求解子群 Z_p^* , Z_q^* 下的二次剩余运算复杂度为 $O((\log_2 N)^3)$ ，签名/验证签名过程与加解密过程相反。将该协议和网络上常用的 HTTPS、SSH、L2TP/IPSec 协议（Layer Two Tunneling Protocol/Internet Protocol Security）^[21-22] 进行比较。

在该实验中，通过抓包工具 Wireshark1.12.1 对协议通信双方的数据分组捕获并分析，解析查看数据分组的格式和大小。对于 HTTPSTLSv1.2 协议，通过在服务器端搭建 Tomcat 服务器，并配置 HTTPS 所需要的公钥证书（采用 RSA 2048 bit 公钥证书）启动服务，且在客户端访问该网址，将截获的相关数据分组大小记录。对于 SSH 协议，在服务器端安装 SSH 服务（OpenSSH_6.6.1p1），并通过客户端命令行使用 ssh 命令远程

登录服务器端，且记录数据分组大小。对于 I2TP/IPSec 协议，在服务器端安装 openwan2.0，做相关配置以后启动 ipsec、xl2tpd 服务，并通过手机连接该虚拟专用网络（VPN, virtual private network），且将截获数据分组大小做记录。对于协议 2，采用 Java 语言编程实现基于 UDP 的套接字，通过捕获客户端和服务器的通信数据记录数据分组大小。

通过表 4 的对比分析可以看出，该协议运行的数据流量较小，摒弃了较大的传输控制协议（TCP, transmission control protocol）数据通信方式，采用用户数据报协议（UDP, user datagram protocol）的方式通信，同时协议运行所依赖的算法在计算复杂度上较 RSA、ECDSA（elliptic curve digital signature algorithm）有一定优势，能够适用于资源有限的设备在网络中进行认证^[22-23]。该仿真过程在 Ubuntu14.0 操作系统上，采用 JDK1.8 编译源程序，在 EclipseMARS.2 集成开发环境上运行程序。仿真测试结果如表 5 所示。

表 4 通信数据分组对比

协议	数据分组	TCP 头	ISAKMP	数据
HTTPSTLSv1.2	258	28	×	205
SSH	342	28	×	288
I2TP/IPSec	542	×	500	×
协议 2（NICAP）	226	×	×	192

表 5 仿真测试结果

	运行时间/ms	内存消耗/kbit
加密	1	1 270
解密	10	1 269
签名	8	1 270
验证签名	0.2	137
协议 1（Sub-NICAP）	61	3 771
协议 2（NICAP）	189	11 302

从表 5 中可以看出，轻量级协议对系统资源要求少，运行速度快，满足了资源受限设备的轻量级通信需求。

7 结束语

利用整数分解问题的困难性结合 Rabin 算

法^[24]，本文设计了轻量级认证方法，以及应用于资源受限设备的网间互联安全控制协议。实验表明，该协议能够低能耗完成认证过程。轻量级认证方法通过系统中各用户设备在管理者参与的网络中实现彼此之间的相互认证，从而为后续的天地一体化网络安全控制通信提供了一个建立会话密钥信道的基础。

参考文献：

- [1] 吕涛. 卫星通信加密机及其接口[J]. 通信保密, 1989 (2): 7-11.
LV T. Satellite communication encryption machine and its interface[J]. Communications Security, 1989 (2): 7-11.
- [2] 向红权. 一种卫星通信链路的加密技术实现研究[D]. 成都: 电子科技大学, 2008.
XIANG H Q. Research on encryption technology implementation of a satellite communication link[D]. Chengdu: University of Electronic Science and Technology, 2008.
- [3] 邹宇聪. 一种应用于微小卫星的通信数据加密技术[J]. 信息通信, 2016, (10): 223-24.
ZOU Y C. A communication data encryption technology applied to micro-satellite[J]. Information Communication, 2016, (10): 223-24.
- [4] 郑建宏, 周亮. 椭圆曲线加密算法在卫星通信中的应用[J]. 信息通信, 2016 (2): 209-210.
ZHENG J H, ZHOU L. Application of elliptic curve encryption algorithm in satellite communication[J]. Information Communication, 2016 (2): 209-210.
- [5] 王宝成. 基于 DVB-RCS 卫星通信系统的通信加密技术研究[D]. 北京: 北京邮电大学, 2012.
WANG B C. Research on communication encryption technology based on dvb-rs satellite communication system[D]. Beijing: Beijing University of Posts and Telecommunications, 2012.
- [6] WANG B C, TANG C M, YANG Y X. The construction of GLV-friendly elliptic curves with fast point multiplication[J]. International Journal of Advancements in Computing Technology, 2012, 4(4): 268-75.
- [7] 陈铁明, 葛亮, 蔡家楣, 等. TinyTCSec: 一种新的轻量级无线传感器网络链路加密协议[J]. 传感技术学报, 2011, 24 (2): 275-82.
CHEN T M, GE L, JIA M, MA S L. TinyTCSec: a new lightweight wireless sensor network link encryption protocol[J]. Journal of Sensor Technology, 2011, 24 (2): 275-82.
- [8] 马韶璞. VSAT 网络认证与数据加密的研究[D]. 天津: 中国民航大学, 2015.
MA S P. Research on VSAT network authentication and data encryption[M]. Tianjin: Civil Aviation University of China, 2015.
- [9] MA L. WNN-based prediction of security situation awareness for the civil aviation network[J]. Journal of Intelligent Systems, 2015, 24(1): 55-67.
- [10] 高利军. 无线射频识别系统安全认证协议研究[D]. 天津: 天津大学, 2015.
GAO L J. Research on security authentication protocol of radio frequency identification system[D]. Tianjin: Tianjin University, 2015.
- [11] 汪洋. 物联网轻量级认证和加密技术研究[D]. 南京: 南京邮电

- 大学, 2017.
- WANG Y. Research on lightweight authentication and encryption technology of Internet of things[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2017.
- [12] 吴伟民, 张晶晶, 彭家进, 等. 基于混沌加密的轻量级 RFID 所有权转移协议[J]. 计算机工程与应用, 2018, 54(9): 62-66+206.
- WU W M, ZHANG J J, PENG J C, et al. Lightweight RFID ownership transfer protocol based on chaos encryption[J]. Computer Engineering and Application, 2018, 54(9): 62-66.
- [13] PANDA M, NAG A. Plain text encryption using AES, DES and SALSA20 by java based bouncy castle API on Windows and linux[C]//Second International Conference on Advances in Computing and Communication Engineering. 2015: 541-548.
- [14] SIVASANKARI M N, SUJATHA S. Performance metric analysis for mobile encryption algorithm using bouncy castle toolkit[C]//International Conference on Emerging Trends in Electrical and Computer Technology. 2011: 1097-1101.
- [15] DAN B. Simplified OAEP for the RSA and rabin functions[C]//Advances in Cryptology – CRYPTO. 2001: 275-91.
- [16] CREMERS C, MAUW S. Operational semantics and verification of security protocols[M]//Information Security and Cryptography. Berlin: Springer, 2012.
- [17] StatVerif. Verification of stateful processes[C]//IEEE 24th Computer Security Foundations Symposium. 2011: 33-47.
- [18] ZHANG F, ZHAO Y W, MA D F, et al. Formal verification of behavioral AADL models by stateful timed CSP[J]. IEEE Access, 2017, 2: 27421-27438.
- [19] ZHAO Y, ZHANG P F, WANG Y K, et al. Troubleshooting data plane with rule verification in software-defined networks[J]. IEEE Transactions on Network and Service Management. 2017: 1.
- [20] YANG Y F, HUANG X L, CHENG S, CHEN S Y, et al. A method of network verification with stateful header space analysis[C]//IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS). 2016: 232-238.
- [21] NARAYAN S, ISHRAR S, KUMAR A, et al. Performance analysis of 4 to 6 and 6 to 4 transition mechanisms over point to point and IP-Sec VPN protocols[C]//Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN). 2016: 1-7.
- [22] PETERSIDE G B, ZAVARSKY P, BUTAKO S. Automated security configuration checklist for a Cisco IPsec VPN router using SCAP 1.2[C]//10th International Conference for Internet Technology and Secured Transactions (ICITST). 2015: 355-360.
- [23] HOSSAIN M, HASAN R. Boot-IoT: a privacy-aware authentication scheme for secure bootstrapping of IoT Nodes[C]//IEEE International Congress on Internet of Things (ICIOT). 2017.
- [24] 康镇麒, 吕克伟. RSA/Rabin-Paillier 陷门函数的比特安全性[J]. 密码学报, 2014, 1(3): 244-254.
- KANG Z Q, LV K W. On bit security of RSA/Rabin-paillier trapdoor functions[J]. Journal of Cryptologic Research, 2014, 2: 244-254.

[作者简介]



卢波 (1988-), 男, 山西晋中人, 北京邮电大学博士生, 主要研究方向为应用安全。



刘赞 (1986-), 男, 北京人, 硕士, 海军参谋部航行保证局工程师, 主要研究方向为无线电导航和惯性导航。

张洁 (1981-), 女, 军事科学研究院系统工程教授, 主要研究方向为信息安全。

陆月明 (1969-), 男, 江苏吴县人, 北京邮电大学教授、博士生导师, 主要研究方向为云计算、搜索引擎、智能光网络、大数据存储与计算、智能家居体系与标准、互联网安全。