文章编号：2095-4980(2013)02-0299-05

一种基于椭圆曲线的社交网络协议

张斯芸，陈　杰，刘建伟

(北京航空航天大学 电子信息工程学院，北京 100191)

摘　要：为了解决社交网络(SNS)易遭受中间友人攻击的缺点，提出了一个新协议，通过结合异或(XOR)编码，并引入杂凑函数、消息认证等密码学机制，使得提出的协议简单易行且为轻量级。通过安全性分析和计算量分析，证明该协议能够有效地抵抗中间友人攻击和重放攻击，同时较大程度降低计算量，节省存储空间。

关键词：社交网络；中间友人攻击；椭圆曲线；XOR 编码；轻量级

中图分类号：TN915.04；TP393.0　　**文献标识码：**A

An elliptic curve-based protocol for Social Networks

ZHANG Si-yun, CHEN Jie, LIU Jian-wei

(Beihang University, School of Electronics & Information Engineering, Beijing 100191, China)

Abstract: In order to resist friend-in-middle attack in Social Networks(SNS), a new protocol is proposed to solve above issues. Combined with Exclusive OR(XOR) coding, cryptology schemes of hash function and message authentication, the protocol is easy to be carried out and light-weighted. Through security and computing overhead analysis, the protocol has been proved to be efficient in resisting friend-in-middle attack and replay attack, as well as largely reducing computation overhead, cutting down the storage space. As other protocols at present can not efficiently solve above issues, the new one is evidently advanced and applicable.

Key words: Social Networks; friend-in-middle-attack; elliptic curve; Exclusive OR coding; light-weighted

针对社交网络的攻击方式，有典型的网络攻击方式[1]，也有针对社交网络特点的攻击方式。文献[2–3]中提出了社交网络抵抗女巫攻击的方案。文献[4]中针对社交网络基于“友谊”的特点，提出了中间友人攻击。中间友人攻击与中间人攻击类似。文献[5]中针对在线社交网络提出了抗匿名攻击。文献[6–7]针对社交网络中用户及用户关系构成的拓扑结构特点，提出了邻居攻击。其中，文献[6]在文献[7]的基础上进行改进，从而能够处理文献[7]中机制不能抵抗的直接邻居攻击。

针对社交网络攻击中比较常见的中间友人攻击，提出一种基于椭圆曲线，并结合 XOR 编码，以及杂凑函数、消息认证等密码学机制的协议，分析它的安全性及计算开销。

1　中间友人攻击

文献[4]中首次提出了中间友人攻击的概念。通过攻击网络层，拦截超文本传送协议(Hypertext Transport Protocol，HTTP)对话来实现这一攻击，再通过对拦截的数据进行挖掘，利用滥发上下文感知信息以及社交网络钓鱼的方式来展开大规模攻击。由于大多数社交网络网站都缺乏对网络层的保护，因此这种攻击并不难实现。

为了解决这个问题，很多网站的做法是保证用户和社交网络服务器间的通信是在安全超文本传输协议(Hypertext Transfer Protocol over secure socket layer, HTTPS)上进行。但是，现在许多社交网络并不支持 HTTPS[4]，仍然存在很大限制。

收稿日期：2012-04-18；**修回日期：**2012-06-17

基金项目：国家重点基础研究发展计划资助项目(973 计划)(2012CB315905)；高等学校博士学科点专项科研基金资助项目(20091102110004)

2 基于椭圆曲线的中间友人攻击抵抗协议

本文中提出了一种基于椭圆曲线的中间友人攻击抵抗协议。通过借用文献[8]中关于椭圆曲线的机制，同时与异或网络编码，以及杂凑函数、消息认证等密码学机制相结合，提出一种简单易行的轻量级协议，用于新兴的社交网络领域，从而有效地抵抗中间友人攻击。

2.1 协议模型

假设 1 社交网络服务器在初始化阶段生成一个随机数 n_S 作为自己的私钥 K_S^S，并且该私钥是绝对安全的，只对该社交网络供应商公开，对所有用户均保密，不存在被窃取或泄漏等情况。因为一旦该私钥泄漏，整个网络将变得不安全。

假设 2 每个用户在注册时设定的密码 C_i 将作为该用户的私钥 K_S^i，只对该用户公开，并且认定每个用户都能牢记自己设定的密码，并保证密码不泄漏。

假设 3 利用椭圆曲线来生成社交网络服务器和每个用户的公钥，具体算法是 $K_P=K_S\times G$。并且，椭圆曲线 E 和其上一点 G 的选取是随机的，每个用户与社交网络服务器间共用一个点，以达到生成共享密钥的目的。同时，每个用户与社交网络服务器间共用的点 G 均是不一样的。由绝对安全的可信第三方为每对用户和社交网络服务器随机选取并提供共享点 G。具体的协议模型见图 1 所示。

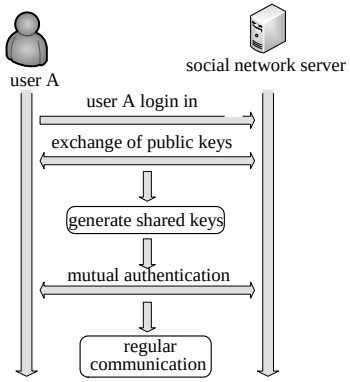

Fig.1 A model of the elliptic curve-based protocol to defend man-in-the-middle attack
图 1 基于椭圆曲线的中间友人攻击抵抗协议模型

2.2 协议建立过程

2.2.1 用户注册

1) 按照现有的社交网络界面，一个用户想要加入某个社交网络，必须先进行注册，得到认证后才能加入。对于大多数社交网络来说，用户 A 注册时需要先输入注册名 ID_A， 向社交网络服务器发出信息 $\{req_{r_A}\|ID_A\}$。

2) 在收到 $\{req_{r_A}\|ID_A\}$ 后，社交网络服务器会验证用户名是否有效。如果有效，可信第三方就会立即从有限域 F 中选取一个点 G_A，生成对应公钥：

$$K_P^{SA}=K_S^S\times G_A \tag{1}$$

并且将 K_P^{SA} 发送给用户 A。

3) 同时，用户 A 会生成一个对应密码 C_A，C_A 即是 A 的私钥 K_S^A，进一步生成用户 A 的公钥为：

$$K_P^A=K_S^A\times G_A \tag{2}$$

然后，用户 A 将 K_P^A 发送给社交网络服务器。

4) 社交网络服务器在收到 K_P^A 后，利用私钥 K_S^S 计算出与用户 A 的共享密钥：

$$K_{SA}=K_S^S\times K_P^A=K_S^S\times K_S^A\times G_A \tag{3}$$

同样，用户 A 在收到 K_P^{SA} 后，利用私钥 K_S^A 计算出共享密钥：

$$K_{SA}^{'}=K_S^A\times K_P^{SA}=K_S^A\times K_S^S\times G_A=K_S^S\times K_S^A\times G_A=K_S^S\times K_P^A=K_{SA} \tag{4}$$

5) 在共享密钥产生后，用户 A 与社交网络服务器间需要进行互相认证。因为 $K_{SA}^{'}$ 是有限域上一个点，设 $K_{SA}^{'}=(x_{SA}^{'},y_{SA}^{'})$，其中 $x_{SA}^{'}$ 与 $y_{SA}^{'}$ 都是一个数字串。

2.2.2 社交网络服务器认证用户 A

首先，用户 A $\rightarrow$ 社交网络服务器：

$$\{ID_A\|m_A\|MAC^{'}=h(m_A\|x_{SA}^{'}\|y_{SA}^{'})\|r_A\|x_{SA}^{'}\oplus r_A\oplus y_{SA}^{'}\} \tag{5}$$

用户 A 向社交网络服务器发送自己的身份 ID_A，一段明文 m_A，消息认证码 $h(m_A\|x_{SA}^{'}\|y_{SA}^{'})$，一个挑战 r_A 以及根据 r_A 得到的异或运算值 $x_{SA}^{'}\oplus r_A\oplus y_{SA}^{'}$。社交网络服务器根据 ID_A，选取对应的共享密钥 K_{SA}，再根据明文 m_A 进行杂凑运算，得到：

$$MAC=h(m_A\|x_{SA}\|y_{SA}) \tag{6}$$

比较 MAC(Message Authentication Code)与 MAC$'$，如果 $MAC=MAC'$，则用户 A 得到社交网络服务器认证。

2.2.3 用户 A 认证社交网络服务器

社交网络服务器→用户 A：

$$\{x'_{SA} \oplus r_A \oplus y'_{SA} \| h(r_A \| x_{SA} \| y_{SA})\} \tag{7}$$

在式(7)中，社交网络服务器收到 A 发来的消息，通过异或运算：

$$x_{SA} \oplus x'_{SA} \oplus r_A \oplus y'_{SA} \oplus y_{SA} \tag{8}$$

由于 $x_{SA}=x'_{SA}$，$y_{SA}=y'_{SA}$，可以由式(8)得到 r_A。

然后社交网络服务器通过 1 次杂凑运算得到：

$$h(r_A \| x_{SA} \| y_{SA}) \tag{9}$$

将式(9)连同 $x'_{SA} \oplus r_A \oplus y'_{SA}$ 一道发给用户 A。A 收到消息后，计算：

$$h(r_A \| x'_{SA} \| y'_{SA}) \tag{10}$$

将式(10)与式(9)进行比较，如果两者相等，则 A 认证了社交网络服务器，完成注册。此处，将 $x'_{SA} \oplus r_A \oplus y'_{SA}$ 一道发给用户 A 是为了向 A 证明，挑战 r_A 没有被更改过。

2.2.4 用户 A 与社交网络服务器间进行实时通信

1) 用户 A 向社交网络服务器发送消息：

$$\{ID_A \| M_A \| MAC' = h(M_A \| x'_{SA} \| y'_{SA}) \| x'_{SA} \oplus t_{A_i} \oplus y'_{SA} \| t_{A_i}\} \tag{11}$$

式(11)的认证过程与 2.2.3 节相似。由于引入了消息发送时间 $ST=t_{A_i}$，可以防止重放攻击。

2) 社交网络服务器向用户 A 发送消息：

$$\{M_S \| MAC = h(M_S \| x_{SA} \| y_{SA}) \| x_{SA} \oplus t_{S_i} \oplus y_{SA} \| t_{S_i}\} \tag{12}$$

具体的认证过程与 2.2.3 节相似。

3　性能分析

3.1 安全性分析

本文提出的协议可以有效地防止中间友人攻击，下面对协议各步骤分别进行安全性分析。

3.1.1 用户注册过程安全性分析

在 2.2.1 的第 4)步中，即使公钥 K_P^A 或 K_P^{SA} 在路由过程中被截获，攻击者也无法与社交网络服务器或者用户 A 建立联系。因为式(1)和式(2)中点 G_A 是随机选取的，且每个用户得到的点都不同，所以攻击者无法生成正确的公钥发送给社交网络服务器或者用户 A。这就有效地杜绝了大规模社交网络中用户对其他封闭群体的攻击。如果用户 A 或者社交网络服务器经计算验证后发现 $K_{SA} \neq K'_{SA}$，就会发现中间友人攻击，从而立即停止通信，使得攻击失败。

3.1.2 服务器认证用户过程安全性分析

在 2.2.2 中，用户 A 发送给社交网络服务器的信息式(5)不用再次加密就是安全的。如果式(5)被中间人拦截，设中间人为恶意用户 J，那么他能做的更改有以下几种：

1) 将 ID_A 替换为自己的身份 ID_J，假冒为 A。但是这样会使得社交网络服务器无法找到正确的共享密钥，导致认证失败。因此，这样的攻击没有意义。

2) 替换明文 m_A。但是这样的简单更改，社交网络服务器在验证时很容易发现。J 还可能会同时替换明文 m_A 为 m_J，替换 ID_A 为 ID_J，得到：

$$h(m_A \| x_{SA} \| x_{SA}) = h(m_J \| x_{SJ} \| y_{SJ}) \tag{13}$$

但是，这种巧合的可能性极低。比如，明文的长度只有非常短的 8 bit，共享密钥的横坐标和纵坐标数值也都只取很小的 8 bit，可以认为 $0 \leqslant x \leqslant 127$，$0 \leqslant y \leqslant 127$。现在国际通用的杂凑函数算法均可满足，当 $x \neq y$ 时，必有 $h(x) \neq h(y)$。所以，J 想要得到式(13)的结果，只能是：

$$m_A \| x_{SA} \| y_{SA} = m_J \| x_{SJ} \| y_{SJ} \tag{14}$$

其概率为 $p=1/2^{24} \approx 5.96\times10^{-8}$。这个概率非常小。而事实上，一般明文段的长度都会远大于 8 bit。因为在一个大规模的有限域中取点，该有限域的范围也必然远大于 127×127。因此，得到概率 $p << 5.96\times10^{-8}$。由于如此小的概

率完全可以忽略，所以可以认为不可能得到式(14)的结果，即等式(13)不可实现。

3) 替换或更改 $MAC' = h(m_A \| x'_{SA} \| y'_{SA})$。但是太容易被发现，没有实际意义。

4) 同时替换以上 3 个要素。如果 J 也为新注册用户，那么 J 本身也需要验证，同时替换 3 个元素就相当于 J 自己与社交网络服务器间进行认证，与用户 A 没有联系。如果 J 为老用户，那么他的攻击行为立刻就会被发现。以上 2 种情况都导致这种攻击没有实际意义。

5) 替换或更改 $x'_{SA} \oplus r_A \oplus y'_{SA}$ 和/或 r_A。没有实际意义，将在 3.1.3 节中具体说明。

3.1.3 用户认证服务器过程安全性分析

当恶意用户 J 发起 3.1.2 节 5)中提到的攻击时，根据 2.2.3 用户 A 认证社交网络服务器过程，可知：

1) 如果 J 更改 r_A 或 $x'_{SA} \oplus r_A \oplus y'_{SA}$，那么社交网络服务器在经过 2 次异或运算后将得出 2 个不同的挑战值，就可以知道遭受到了中间友人攻击。

2) 如果 J 同时更改 r_A 和 $x'_{SA} \oplus r_A \oplus y'_{SA}$，因为 J 不知道共享密钥，也就不知道 $x_{SA}, y_{SA}, x'_{SA}, y'_{SA}$。社交网络服务器得出 2 个不同挑战值时将发现这种更改。

3.1.4 正常通信过程安全性分析

在 2.2.4 中，由于认证过程与 2.2.3 中类似，可以验证该步骤依然可以有效抵抗中间友人攻击。

消息式(11)中加入了消息发送时间 $ST = t_{A_i}$，从而可以防止重放攻击。社交网络服务器接收到消息时，记接收时间为 RT，比较 RT-ST 与消息生存时间 TTL，可以知道是否发生重放攻击。

3.2 计算量分析

本协议主要依靠消息认证来完成用户和社交网络服务器间的互相认证并保证正常通信，从而大大降低计算开销量和对存储空间的需求。本协议中使用的 XOR 运算，计算量极小，可以忽略。计算开销主要来源于椭圆曲线加密和杂凑函数运算，在保证安全强度的前提下与其他协议相比，计算开销相对较小，存储空间需求相对较少。

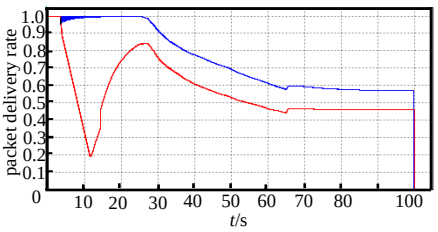

Fig.2 Comparison of packet delivery rate
图 2 包交付率比较

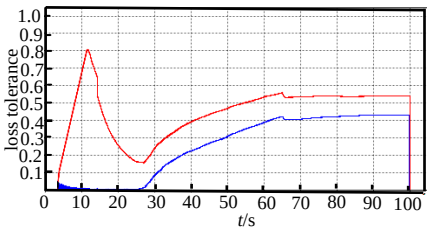

Fig.3 Comparison of loss tolerance
图 3 丢包率比较

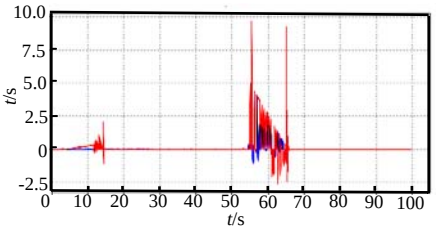

Fig.4 Comparison of jitter
图 4 抖动率比较

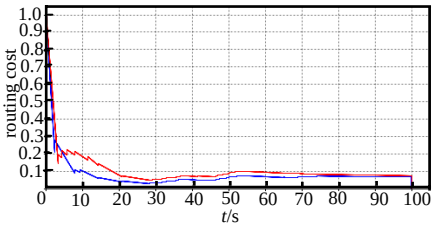

Fig.5 Comparison of routing cost
图 5 路由开销比较

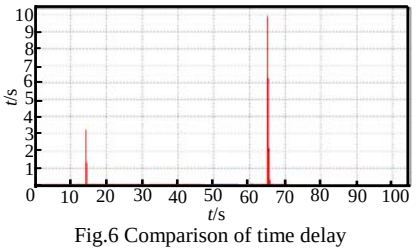

Fig.6 Comparison of time delay
图 6 时延比较

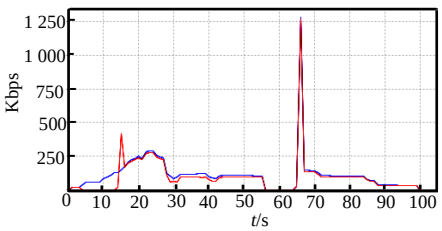

Fig.7 Comparison of throughput
图 7 吞吐量比较

4 仿真分析

在 NS2 环境下调用 OpenSSL 库比较 ECC(Elliptic Curve Cryptography)加密与 RSA(Rivest Shamir Adleman)算法加密下的协议开销，仿真比较图见图 2~图 7，蓝线为椭圆曲线密码编码 ECC 加密，红线为同等安全强度密码系统 RSA 加密。通过对比可知，同等安全强度下，ECC 加密的包交付率、吞吐量均优于 RSA 加密，丢包率、抖动率、路由开销和时延明显比 RSA 加密小。相比其他协议，新协议的优势显而易见。

5 结论

本文提出了一种基于椭圆曲线的中间友人攻击抵抗协议。通过与异或网络编码，以及杂凑函数、消息认证

等密码学机制相结合，提出的协议简单易行且为轻量级。通过安全性分析、计算量分析和仿真分析，该协议能够有效抵抗中间友人攻击和重放攻击，同时较大限度降低计算量，节省存储空间，更加稳定可靠。

参考文献

[1] 陈虹志,周安民,邓赟. 基于网络环境安全的可信访问控制策略[J]. 信息与电子工程, 2010,8(4):463-466. (CHEN Hongzhi,ZHOU Anmin,DENG Yun. One trusted computing access control strategy based on network environment security[J]. Information and Electronic Engineering, 2010,8(4):463-466.)

[2] XU L,Chainan S,Takizawa H. Resisting Sybil Attack By Social Network and Network Clustering[C]// 2010 10th Annual International Symposium on Applications and the Internet. Seoul:[s.n.], 2011:15-21.

[3] Fong L. Preventing Sybil Attacks by Privilege Attenuation:A Design Principle for Social Network Systems[C]// 2011 IEEE Symposium on Security and Privacy. Oakland,California:[s.n.], 2011:263-278.

[4] Huber M,Mulazzani M,Kitzler G. Friend-in-the-middle attacks, Exploiting Social Networking Sites foe Spam[J]. IEEE Computer Society, 2011,15(3):28-34.

[5] Ding X,Zhang L,Wan Z. A Brief Survey on De-anonymization Attacks in Online Social Networks[C]// 2010 International Conference on Computational Aspects of Social Networks. Taiyuan:[s.n.], 2010:611-615.

[6] Tripathy B K,Panda G K. A New Approach to Manage Security Against Neighborhood Attacks in Social Networks[C]// 2010 International Conference on Advances in Social Networks Analysis and Mining. athens,Greek:[s.n.], 2010:264-269.

[7] Zhou B,Pei J. Preserving privacy in social networks against neighborhood attacks[C]// Simon Fraser University,ICDE. 2008:506-515.

[8] Du X,Guizani M,Xiao Y. A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks[J]. IEEE Transactions on wireless communications, 2009,8(3):1223-1229.

作者简介:

张斯芸(1988-)，女，成都市人，硕士，主要研究方向为信息与网络安全.email:zhangsycindy@163.com.

陈　杰(1985-)，男，陕西省铜川市人，博士，主要研究方向为信息与网络安全.

刘建伟(1964-)，男，山东省莱州市人，教授，博士生导师，主要从事移动通信网络、Ad hoc 网络、无线传感器网络、无线 mesh 网络、社交网络、车辆自组织网络、云计算等的保密和认证技术研究。发表论文 40 余篇，出版专著和教材 5 部，获教育部优秀教材一等奖，山东省科学技术进步三等奖，山东省计算机应用新成果二等奖.