计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(1):267−272 [doi: 10.15888/j.cnki.csa.008285]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

轻量级的一对多认证和密钥协商方案①

杨鹏飞, 李雅斌, 严翌瑄

(长安大学 信息工程学院, 西安 710064)
通信作者: 杨鹏飞, E-mail: 1714104678@qq.com

摘　要: 在物联网数据传输过程中, 需要认证通信双方的身份和加密传输数据. 目前, 已有大量的认证和密钥协商方案已经被设计, 但是, 现有方案容易遭受多种攻击, 例如智能卡被盗攻击, 拒绝服务攻击等; 针对现有方案存在问题, 本文提出了一种轻量级的一对多认证和密钥协商方案, 在用户端和传感器端分别使用椭圆曲线密码学和异或操作来实现相互认证, 利用预共享密钥的方法将传感器端扩展为多个. 最后, 通过功能比较, 计算代价, 通信代价对比, 显示所提方案优于其他方案, 更适合于多传感器场景.

关键词: 认证; 密钥协商; 椭圆曲线密码学; 匿名性; 物联网

引用格式: 杨鹏飞,李雅斌,严翌瑄.轻量级的一对多认证和密钥协商方案.计算机系统应用,2022,31(1):267–272. http://www.c-s-a.org.cn/1003-3254/8285.html

Lightweight One-to-many Authentication and Key Agreement Scheme

YANG Peng-Fei, LI Ya-Bin, YAN Yi-Xuan

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: In the data transmission process of the Internet of Things, it is necessary to authenticate the identities of the communicating parties and encrypt the transmitted data. At present, a large number of authentication and key agreement schemes have been designed, but they are vulnerable to various attacks, such as smart card stolen attack and denial of service attack. In view of the problems of existing schemes, this study proposes a lightweight one-to-many authentication and key agreement scheme, using elliptic curve cryptography and XOR operation on the user and the sensor sides respectively to achieve mutual authentication and the method of a pre-shared key to expand the sensor side to multiple ones. Finally, through the comparison of functions, computation cost, and communication cost, it is shown that the proposed scheme is better than other schemes and is more suitable for multi-sensor scenarios.

Key words: authentication; key agreement; elliptic curve cryptography; anonymity; Internet of Things (IoT)

物联网[1]技术的发展, 极大地便利了人们的生活, 人们足不出户就可以获取千里之外的传感器收集的实时数据, 然而, 由于数据在公开信道中传输的自然特性, 使得信息被截获, 篡改等事件时常发生, 为了保证在公开信道中传输数据的安全性, 研究人员将认证和密钥协商技术应用于物联网环境中.

1976 年, Diffie-Hellman第一次提出密钥协商的概念[2], 随后, 研究人员在其思想影响下, 提出了大量的密钥协商方案[3–9]; 然而, 现有的大多数方案存在以下两个问题: (1) 很多方案在传感器端采用昂贵的双线性对或椭圆曲线密码学技术, 这不太适合于资源受限的传感器; (2) 大多数方案为一个用户和一个传感器密钥协商方案, 当用户想要访问 n 个传感器数据时, 需要将协议运行 n 次, 这样极大地增加了用户端的负担, 浪费了计算和通信资源.

基于以上存在问题, 本文提出了一个一对多认证

① 收稿时间: 2021-04-05; 修改时间: 2021-04-29; 采用时间: 2021-05-11; csa 在线出版时间: 2021-12-17

和密钥协商方案, 其中传感器端使用了异或, 哈希等计算代价较小的操作, 并且实现了一个用户和 n 个传感器同时进行密钥协商.

1 背景知识

1.1 椭圆曲线[10]

令q是一个大素数, F_q表示阶数为q的有限域, F_q上的椭圆曲线 E 定义为满足等式$y^2 = x^3 + ax + b \bmod p$的点$(x,y)$的集合, 其中, a,b满足$4a^3 + 27b^2 \neq 0 \bmod q$, 无穷远点$O$和 E 上点形成循环加法群$\mathbb{G}$, 阶数是q, 生成元是 P.

1.2 椭圆曲线上困难问题假设[11]

椭圆曲线计算性Diffie-Hellman 问题 (ECCDHP) 假设: 给定任意$P, aP, bP \in \mathbb{G}$, $(a,b \in Z_q^*)$, 在多项式时间算法内很难算出$abP \in \mathbb{G}$.

1.3 哈希函数

哈希(Hash)函数是一个确定的函数, 它可以将任意长度的消息映射为固定长度.

哈希函数特点:

(1) 输入可变: 输入可以是任意位数的数据.

(2) 输出定长: 输出的长度是固定位数.

(3) 单向性: 对于任意消息 M, 在多项式时间内计算$H(M)$是可行的; 相反, 已有任意$h = H(M)$, 在多项式时间内计算 M 是不可行的.

1.4 网络模型

所提方案的网络模型如图 1 所示, 模型中包含 3 个实体, 分别是网关GWN, 用户U_i, 传感器$S_j (j = 1,2,\cdots,n)$.

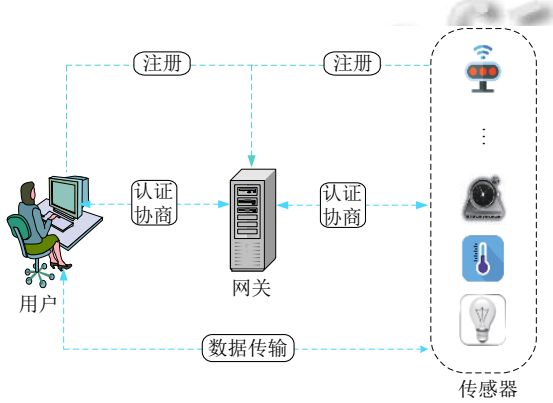

图 1 网络模型图

(1)GWN: 表示一个可信实体, 主要负责用户U_i和传感器$S_j (j = 1,2,\cdots,n)$的注册, 同时协助用户U_i和传感器S_j完成相互认证.

(2)U_i: 表示第i个用户, 在GWN处注册获得认证信息, 通过认证信息证明自己的合法身份, 经过GWN认证后, 可以访问传感器数据.

(3)S_j: 表示第j个传感器, 向GWN注册获得认证信息, 利用认证信息证明身份的合法性, 经过GWN认证后, 可以向用户提供相应数据.

1.5 安全性需求

匿名性: 方案应该保证攻击者不能通过在公开信道中传输的消息揭露用户或传感器的真实身份.

不可追踪性: 方案应该满足不可追踪性, 即攻击者无法将同一实体在公开信道中传输的消息关联在一起.

用户仿冒攻击: 攻击者不能伪造用户的登录信息, 成功通过网关验证, 并与传感器建立会话密钥.

网关仿冒攻击: 攻击者不能伪造网关信息, 完成与用户或传感器的双向认证.

传感器仿冒攻击: 攻击者不能伪造传感器秘密信息, 成功通过网关验证, 并与用户建立会话密钥.

重放攻击: 攻击者不能将之前在公开信道中传输的消息重新传输, 从而误导其他实体认为该消息为合法实体所发.

中间人攻击: 攻击者不能在用户和网关, 网关和传感器之间发送消息, 让通信双方误以为在与合法实体通信.

拒绝服务攻击: 攻击者不能向网关发送大量的无用消息来造成网关瘫痪.

智能卡被盗攻击: 敌手即使获得合法用户的智能卡, 也无法仿冒用户发起认证和密钥协商请求.

2 本文方案

2.1 系统建立

网关GWN选择一个阶数为q的群$\mathbb{G}$, 生成元是P, 选择$s \in Z_q^*$作为自己的私钥, 计算相对应公钥$S = s \cdot P$.

GWN选择哈希函数$h(\cdot): \{0,1\}^* \to Z_q^*$, 公开系统参数: $(P, \mathbb{G}, q, S, h(\cdot))$.

2.2 用户注册

用户U_i要想成为合法授权用户, 必须要和网关GWN注册. 具体过程如图 2 所示.

(1)U_i选择自己的身份UID_i, 密码PW_i和随机数$t \in Z_q^*$, 计算$BPW_i = h(PW_i \| t)$, 将(UID_i, BPW_i)通过安全信道发送给GWN.

(2)GWN收到后, 计算$a = h(UID_i \| s)$, $EPW_i =$

$BPW_i \oplus a$, 在智能卡中存储$(EPW_i, P, h(\cdot))$, 最后, 将智能卡安全地发送给U_i.

(3) U_i收到后, 输入身份UID_i和密码PW_i, 计算$A = h(UID_i||PW_i) \oplus t$, $B = h(UID_i||BPW_i||t)$, 存储(A, B), 此时, 智能卡中包含$(A, B, EPW_i, P, h(\cdot))$信息.

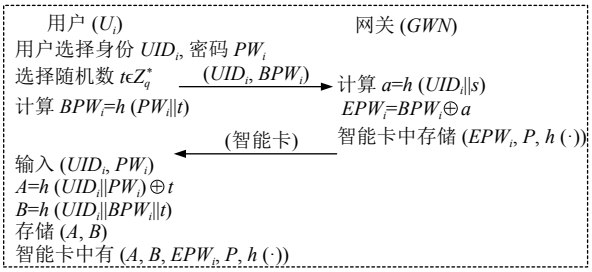

图 2 用户注册

2.3 传感器注册

所有传感器需要和网关GWN注册. 具体过程如图 3 所示.

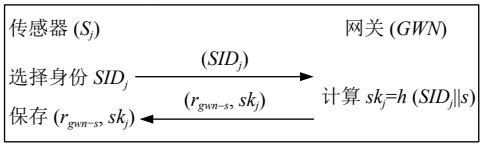

图 3 传感器注册

(1) 传感器$S_j(j = 1,2,\cdots,n)$选择自己的身份SID_j, 通过安全信道发送给网关GWN.

(2)GWN收到后, 选择一个随机数$r_{gwn-s} \in Z_q^*$作为所有传感器的共同密钥, 同时计算传感器私钥$sk_j = h(SID_j||s)$, 将(r_{gwn-s}, sk_j)安全地发送给S_j.

(3)S_j收到后, 将(r_{gwn-s}, sk_j)存储在自己的内存中.

2.4 相互认证和密钥协商

当用户U_i想要访问传感器$S_j(j = 1,2,\cdots,n)$的数据时, 必须与所有传感器协商出会话密钥. 具体过程如图 4 所示.

(1) U_i输入身份UID_i, 密码PW_i, 计算$t = A \oplus h(UID_i||PW_i)$, $BPW_i = h(PW_i||t)$, $B' = h(UID_i||BPW_i||t)$, 验证等式$B' = B$是否成立, 若不成立, 说明输入的身份或密码有错误; 提示用户输入正确的身份和密码; 否则, U_i选择随机数$b \in Z_q^*$, 时间戳TS_1, 计算$a = EPW_i \oplus BPW_i$, $M_1 = b \cdot P$, $pk = h(b \cdot S)$, $c = h(a||TS_1)$, $M_2 = UID_i \oplus h(M_1||pk||TS_1)$, $M_3 = h(UID_i||GID||a||TS_1)$, 通过公开信道发送消息$(M_1, M_2, M_3, TS_1)$到网关$GWN$.

(2)GWN收到消息后, 检查是否$|TS_1 - TS_1'| \le \Delta TS$, 成立则继续计算$pk = h(sM_1)$, $UID_i' = M_2 \oplus h(M_1||pk||TS_1)$, $a' = h(UID_i'||s)$, $M_3' = h(UID_i'||GID||a'||TS_1)$, 验证等式$M_3' = M_3$是否成立, 若成立则选择时间戳$TS_2$, 计算$c = h(a'||TS_1)$, $M_4 = r_{gwn-s} \oplus c$, $M_5 = UID_i' \oplus h(r_{gwn-s})$, $M_6 = h(UID_i'||c||TS_2)$, 最后, GWN将消息(M_4, M_5, M_6, TS_2)广播给所有传感器.

(3) 传感器S_j收到消息后, 检查是否$|TS_2 - TS_2'| \le \Delta TS$, 计算$c' = M_4 \oplus r_{gwn-s}$, $UID_i' = M_5 \oplus h(r_{gwn-s})$, $M_6' = h(UID_i'||c'||TS_2)$, 验证等式$M_6' = M_6$是否成立, 若成立则选择时间戳$TS_3$, 计算$M_7 = r_{gwn-s} \oplus SID_j$, $M_8 = h(r_{gwn-s}||SID_j||sk_j||TS_3)$, 传感器将消息$(M_7, M_8, TS_3)$发送给$GWN$.

(4) GWN收到消息后, 检查是否$|TS_3 - TS_3'| \le \Delta TS$, 计算$SID_j' = M_7 \oplus r_{gwn-s}$, 接着验证传感器的合法性, 计算$sk_j = h(SID_j||s)(j = 1,2\cdots n)$, $M_8' = h(r_{gwn-s}||SID_j||sk_j||TS_3)$, 验证是否$M_8' = M_8$; 若成立, 则说明传感器是合法的. GWN选择时间戳TS_4, TS_5, 计算$K = \sum_{j=1}^{n} sk_j$, $M_9 = h(K||r_{gwn-s}||TS_4)$, $M_{10} = M_9 \oplus r_{gwn-s}$, $SK = h(UID_i'||c||GID||M_9)$, $M_{11} = h(SK||M_9||r_{gwn-s}||TS_4)$, $M_{12} = M_9 \oplus h(pk||TS_5)$, $M_{13} = h(SK||M_9||TS_5)$, 广播消息$(M_{10}, M_{11}, TS_4)$给所有传感器, 发送消息$(M_{12}, M_{13}, TS_5)$给$U_i$.

(5) S_j收到消息后, 检查是否$|TS_4 - TS_4'| \le \Delta TS$, 成立则计算$M_9' = M_{10} \oplus r_{gwn-s}$, 会话密钥$SK = h(UID_i'||c'||GID||M_9')$, 验证等式$M_{11}' = h(SK||M_9'||r_{gwn-s}||TS_4)$是否成立.

(6) U_i收到消息后, 检查是否$|TS_5 - TS_5'| \le \Delta TS$, 成立则继续计算$M_9' = M_{12} \oplus h(pk||TS_5)$, $SK = h(UID_i||c||GID||M_9')$, 验证$M_{13}' = h(SK||M_9'||TS_5)$.

通过上述过程, 用户U_i和所有传感器之间协商出共同的会话密钥SK. 此时, 用户U_i就可以访问所有传感器数据了.

3 协议分析

3.1 安全性分析

本小节将分析第 1.5 节中所给的安全性需求.

用户匿名性: 方案中, 用户身份被$pk = bsP$和$h(r_{gwn-s})$保护, 只有知道主私钥s, 随机数b或r_{gwn-s}才能计算出用户身份UID_i, 因此, 攻击者不可能知道用户身份, 所以, 该方案提供了用户匿名性.

用户不可追踪性: 方案中, 用户身份被$pk = bsP$和时间戳TS_1保护, 随机数b和TS_1在每次认证和密钥协商过程中都是变化的, 因此不能将消息关联起来, 所以, 方案提供了用户不可追踪性.

传感器匿名性: 传感器S_j的身份被共同密钥r_{gwn-s}保护, 只有网关GWN和合法传感器才拥有r_{gwn-s}, 因此, 方案提供了传感器匿名性.

用户仿冒攻击: 方案中, 只有正确输入用户的身份和密码才能通过智能卡认证, 因此, 除授权用户外, 其他实体不能通过认证.

网关仿冒攻击: 只有拥有主私钥 s 才能仿冒网关, 然而 s 只有网关知道, 所以, 其他实体无法仿冒网关.

传感器仿冒攻击: (1) 传感器外部仿冒攻击: 未授权传感器想要仿冒授权传感器, 必须知道共同密钥r_{gwn-s}和想要仿冒传感器的私钥sk_j; (2) 传感器内部仿冒攻击: 当授权传感器想要仿冒网络模型中的其他传感器, 必须知道想要仿冒传感器的私钥sk_j; 显然, 其他实体是无法得到这些秘密值, 因此方案可以抵抗传感器仿冒攻击.

重放攻击: 方案中传输的消息中都包含了时间戳TS_i, 因此所提方案可以抵抗重放攻击.

中间人攻击: 要发起中间人攻击需要知道实体的秘密信息, 但攻击者无法获得这些信息, 因此, 方案可以抵抗中间人攻击.

拒绝服务攻击: 当攻击者发来大量消息时, 实体首先会检查其中包含的时间戳TS_i, 当时间戳无效时, 就会丢弃消息, 因此可以抵抗拒绝服务攻击.

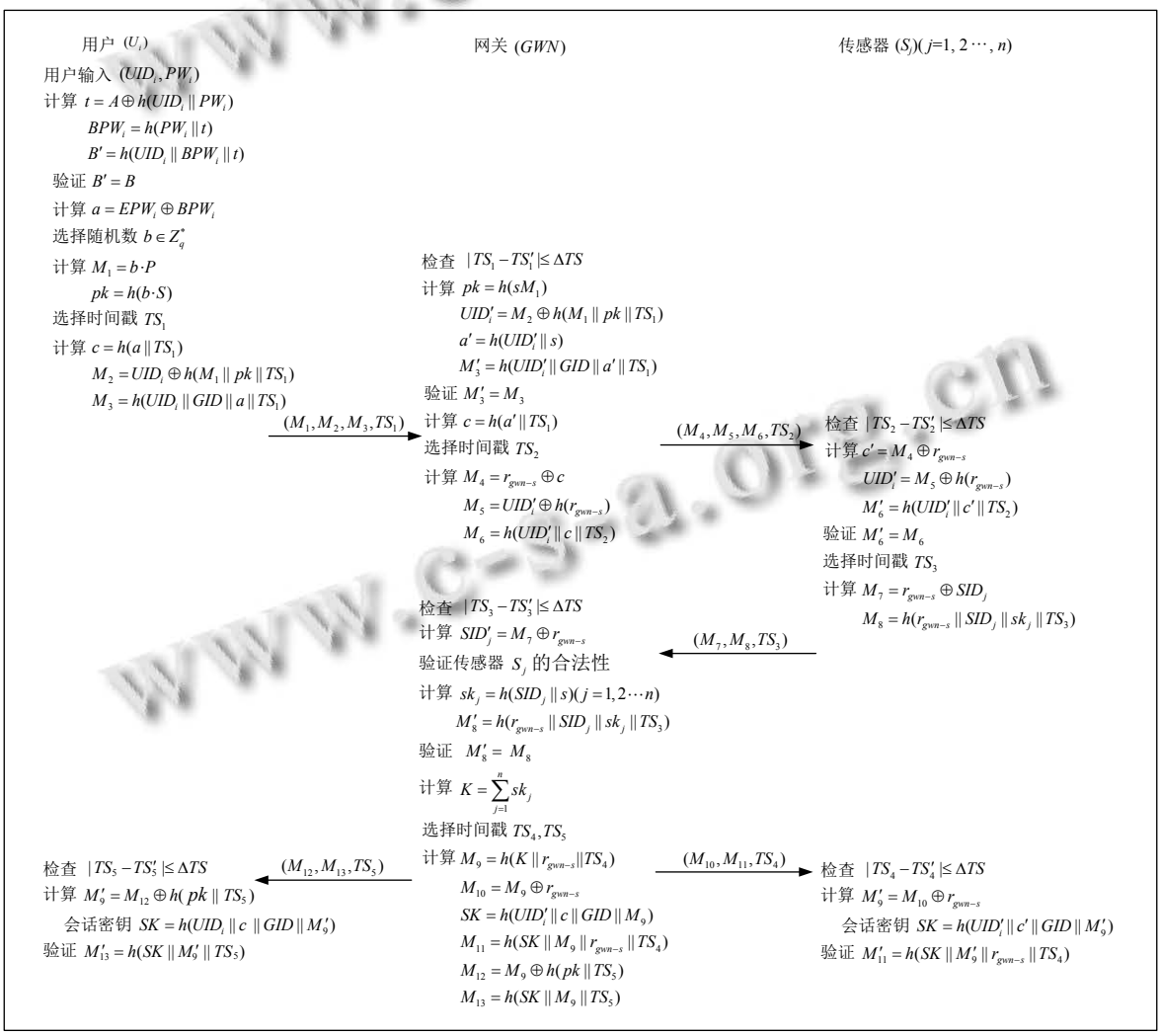

图 4 相互认证和密钥协商

智能卡被盗攻击: 方案中, 智能卡中含有信息$(A,B,EPW_i,P,h(\cdot))$, 攻击者需要得到a来发起协商请求, 然而a被UID_i,PW_i保护, 攻击者无法获得UID_i和PW_i, 所以方案可以抵抗智能卡被盗攻击.

3.2 功能比较

本小节将所提方案与文献 [12–15] 进行功能比较. 如表 1, 其中, R1: 相互认证; R2: 用户匿名性; R3: 用户不可追踪性; R4: 传感器匿名性; R5: 用户仿冒攻击; R6: 网关仿冒攻击; R7: 传感器外部仿冒攻击; R8: 传感器内部仿冒攻击; R9: 重放攻击; R10: 中间人攻击; R11: 拒绝服务攻击; R12: 一对多方案. 从表 1 中可以看出, 文献 [12–14] 均为一个用户和一个传感器密钥协商方案, 且文献 [12] 不满足用户匿名性, 文献 [14] 不能抵抗拒绝服务攻击, 文献 [15] 虽然为一个用户和多个传感器密钥协商方案, 但不能抵抗传感器内部仿冒攻击.

表 1 功能比较

功能	文献[12]	文献[13]	文献[14]	文献[15]	所提方案
R1	√	√	√	√	√
R2	×	√	√	√	√
R3	√	√	√	√	√
R4	√	√	√	√	√
R5	√	√	√	√	√
R6	√	√	√	√	√
R7	√	√	√	√	√
R8	√	√	√	×	√
R9	√	√	√	√	√
R10	√	√	√	√	√
R11	√	√	×	√	√
R12	×	×	×	√	√

注: “√”表示满足, “×”表示不满足.

3.3 计算代价比较

表 2 列出了所提方案与文献 [12–15] 所使用的密码学操作运行的平均时间, 本文使用 MIRACL Crypto SDK[16] 得到上述数据, 运行环境为2.53 GHz, i7CPU和4 GB内存的64位Windows 10操作系统. 表 3 给出了所提方案和文献 [12–15] 计算代价比较, 图 5 给出了计算代价与传感器数量关系图, 从图中可以看出: 文献 [13,14] 访问一个传感器时, 计算代价已经超过了所提方案, 虽然文献 [12,15] 在访问少量传感器时, 计算代价小于所提方案, 但当传感器数量分别超过 30 和 91 时, 计算代价将会超过所提方案, 因此, 所提方案更适合于多传感器场景.

3.4 通信代价比较

为了更好地比较通信代价, 本文做了如下假定: 假定ECC中$|\mathbb{G}|$的长度为 160 bits; 身份, 哈希函数的输出, 随机数的长度均为 160 bits; 对称加密的密文长度为 128 bits; 时间戳的长度为 32 bits; 表 4 给出了所提方案与文献 [12–15] 通信代价比较, 图 6 给出了通信代价与传感器数量关系图; 从图中可以看出: 随着传感器数量的增加, 所提方案的通信代价低于文献 [12–14], 虽然所提方案的通信代价高于文献 [15], 但在功能和计算代价优于文献 [15].

表 2 密码运算运行时间

概念	描述	执行时间 (ms)
T_h	通常哈希运算	0.001 3
T_{m-ecc}	ECC下的标量乘法运算	0.385 1
T_m	Z_q^*下的标量乘法运算	0.004 4
T_s	对称加密$(AES-128)$	0.002 6

注: 加法和异或运算的执行时间已经被忽略.

表 3 具体方案计算代价对比 (ms)

方案	访问单传感器计算开销	访问多传感器计算开销
文献[12]	$22T_h+8T_s=0.0494$	$(22T_h+8T_s)n$
文献[13]	$31T_h+6T_{m-ecc}=2.3509$	$(31T_h+6T_{m-ecc})n$
文献[14]	$22T_h+5T_{m-ecc}=1.9541$	$(22T_h+5T_{m-ecc})n$
文献[15]	$19T_h+6T_s+4T_m=0.0579$	$15T_h+3T_s+2T_m+(4T_h+3T_s+2T_m)n$
所提方案	$29T_h+3T_{m-ecc}=1.193$	$22T_h+3T_{m-ecc}+7nT_h$

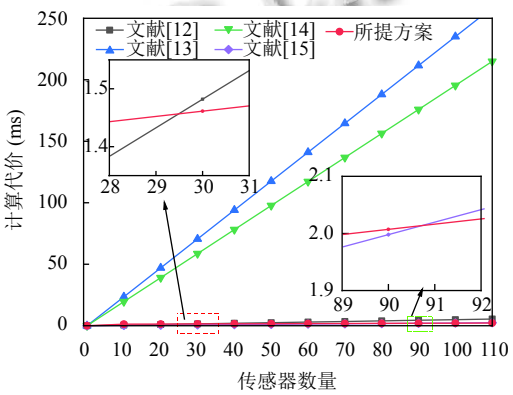

图 5 计算代价比较

表 4 具体方案通信代价对比 (bits)

方案	访问单传感器通信开销	访问多传感器通信开销
文献[12]	1 952	$1952n$
文献[13]	1 248	$1248n$
文献[14]	1 952	$1952n$
文献[15]	2 112	$992+1120n$
所提方案	2 080	$864+1216n$

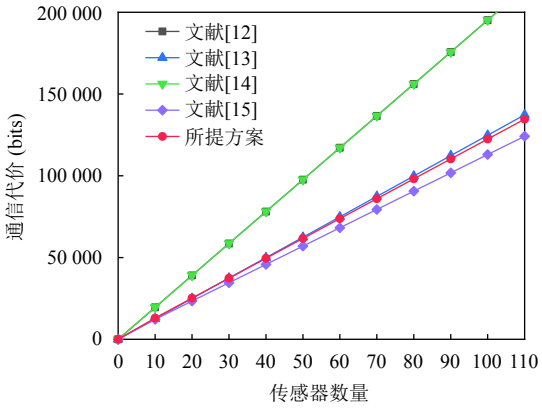

图 6 通信代价比较

4 结论与展望

本文利用椭圆曲线密码学技术, 异或等操作提出了一个轻量级的一对多认证和密钥协商方案, 在网关的帮助下, 用户和多个传感器之间实现了相互认证并且协商出对称加密会话密钥, 减少了用户端的计算代价和通信代价; 预共享共同密钥方法的使用使得所提方案具有扩展性, 更符合现代物联网场景, 性能比较表明, 所提方案在计算和通信代价方面更为高效. 接下来的研究工作是如何实现用户端是多个用户的认证和密钥协商方案, 这样可以进一步减少传感器端的计算和通信代价.

参考文献

1 任补补. 物联网中无线传感器网络安全认证方法研究 [硕士学位论文]. 兰州: 兰州理工大学, 2020.

2 Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644–654. [doi: 10.1109/TIT.1976.1055638]

3 Al-Turjman F, Ever YK, Ever E. Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks. IEEE Access, 2017, 5: 24617–24631. [doi: 10.1109/ACCESS.2017.2766090]

4 Mo JQ, Li KM. A secure and efficient anonymous user authentication and key agreement scheme for global mobility networks based on bilinear pairing. 2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT). Shenzhen: IEEE, 2020. 579–584.

5 Khatoon S, Rahman M, Alrubaian M, *et al*. Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment. IEEE Access, 2019, 7: 47962–47971. [doi: 10.1109/ACCESS.2019.2909556]

6 Hamid HAA, Rahman M, Hossain MS, *et al*. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access, 2017, 5: 22313–22328. [doi: 10.1109/ACCESS.2017.2757844]

7 孟磊. 基于双线性对的高效身份认证密钥协商协议研究 [硕士学位论文]. 重庆: 重庆邮电大学, 2020.

8 Ma MM, He DB, Wang HQ, *et al*. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular Ad-Hoc networks. IEEE Internet of Things Journal, 2019, 6(5): 8065–8075. [doi: 10.1109/JIOT.2019.2902840]

9 Jia XY, He DB, Kumar N, *et al*. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks, 2019, 25(8): 4737–4750. [doi: 10.1007/s11276-018-1759-3]

10 Koblitz N. Elliptic curve cryptosystem. Mathematics of Computation, 1987, 48(177): 203–209. [doi: 10.1090/S0025-5718-1987-0866109-5]

11 光笑黎, 张露露, 刘继增. 一种轻量级基于证书的认证密钥协商方案. 计算机系统应用, 2021, 30(1): 264–269. [doi: 10.15888/j.cnki.csa.007806]

12 Wazid M, Das AK, Odelu V, *et al*. Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things Journal, 2018, 5(1): 269–282. [doi: 10.1109/JIOT.2017.2780232]

13 Soni P, Pal AK, Islam SKH. An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Computer Methods and Programs in Biomedicine, 2019, 182: 105054. [doi: 10.1016/j.cmpb.2019.105054]

14 Kumar D, Singh HK, Ahlawat C. A secure three-factor authentication scheme for wireless sensor networks using ECC. Journal of Discrete Mathematical Sciences and Cryptography, 2020, 23(4): 879–900. [doi: 10.1080/09720529.2019.1627072]

15 Vinoth R, Deborah LJ, Vijayakumar P, *et al*. Secure multifactor authenticated key agreement scheme for industrial IoT. IEEE Internet of Things Journal, 2021, 8(5): 3801–3811. [doi: 10.1109/JIOT.2020.3024703]

16 Shamus S. Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL). http://www.certivox.com/miracl/