(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107493165 B
(45)授权公告日 2021.02.09

(21)申请号 201710931255.3

(22)申请日 2017.10.09

(65)同一申请的已公布的文献号
申请公布号 CN 107493165 A

(43)申请公布日 2017.12.19

(73)专利权人 重庆邮电大学
地址 400065 重庆市南岸区南山街道崇文路2号

(72)发明人 周由胜 龙兴旺 刘思伶 蒋溢 刘宴兵

(74)专利代理机构 重庆市恒信知识产权代理有限公司 50102
代理人 刘小红

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)

审查员 董玉慧

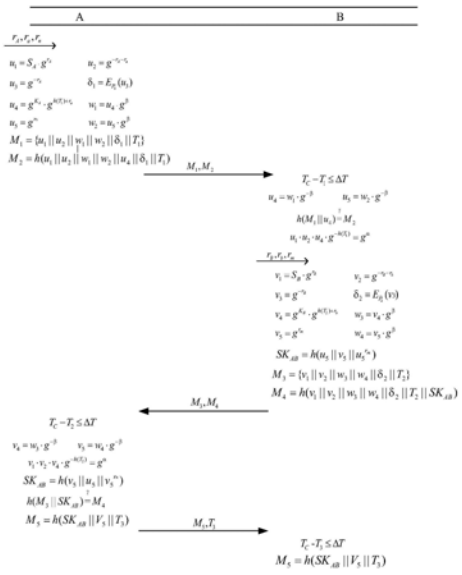
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种具有强匿名性的车联网认证及密钥协商方法

(57)摘要

本发明请求保护一面向车联网的两方认证及密钥协商方法，涉及车联网领域。密钥协商被广泛的应用于车联网认证方案中，但是现有的认证方案中存在大量的三方协议，即完成密钥协商过程需要三方共同合作。在某些特定环境下，这些方案无法达到预期效果。例如，车辆在没有完善的路侧基础设施的情况下，很难完成与其它车辆的认证与安全通信，本发明提供了一种安全的车联网认证及密钥协商方法来解决这种问题。本发明具有身份匿名、消息不可连接、恶意车辆可追踪等安全优势，因此具有良好的隐私保护性和可靠的安全性。由于本方法使用的无双线性对的密码运算，因此本方法执行效率更加高效。本发明具有适用范围的确定性，将范围确定于车联网应用。



CN 107493165 B

1.一种具有强匿名性的车联网认证及密钥协商方法,其特征在于,该方法包括三个步骤:

1)、系统初始化步骤,用于完成车辆及服务器初始化的相关工作;

2)、车辆注册步骤,对合法用户进行注册登记;

3)、认证及密钥协商步骤,采用包括散列函数、模乘法群在内的密码学基本知识,在基于计算性Diffie-Hellman难题的基础上实现两方认证及密钥协商,使得对等的通信双方能够在无第三方的帮助下,实现相互认证并完成密钥协商,完成对其他车辆的认证,并与其安全通信;

所述步骤1)的系统初始化步骤主要包括:车辆用户i获取车辆V_i的唯一身份信息ID_i以及设定一个只有自己知道的口令PW_i;服务器S生成自己的公私钥对:公钥P_k、私钥P_s,并选取随机数X作为自己的主密钥,再选取随机数α,β作为秘密值,然后选取hash函数h(•)及非对称加密算法E_k(•),最后公布公共信息h(•),E_k(•)和P_k;

所述车辆注册过程包括:需注册的车辆V_i通过安全的渠道将自己的身份信息ID_i和用户口令PW_i提交给服务器S;服务器S得到这些数据后,会计算相关的参数K_i、S_i、φ_i、θ_i;其中K_i表示将主密钥和车辆身份进行hash后的参数,S_i表示带有系统秘密值α的参数,φ_i表示带有用户口令的参数,θ_i表示带有用户口令以及系统秘密值β的参数,计算方式为:$K_i=h(ID_i||X)$;$S_i = g^{-K_i+\alpha}$;$\varphi_i = g^{K_i}\cdot g^{-h(PW_i)}$;$\theta_i = g^{\beta}\cdot g^{-h(PW_i)}$,g表示循环加法群G的生成元,然后服务器S会将参数S_i、φ_i、θ_i返回给车辆V_i,车辆V_i将接受到的参数存放于防篡改装置TPD中;S_A、S_B分别表示系统返回给车辆A、车辆B的带有系统秘密值α的参数,K_A、K_B分别表示将主密钥和车辆A、车辆B的车辆身份进行hash计算后参数,$E_{P_k}(.)$表示采用非对称加密算法中的公钥P_k执行加密操作;

所述认证及密钥协商过程会完成以下工作;假设车辆V_A需要与车辆V_B进行通信,过程如下:

对于车辆V_A来说,为了发起一个认证及密钥协商过程,它首先选取3个随机数r_A、r_a、r_n,然后计算通信时所需的参数u_1,u_2,w_1,w_2,δ_1,u_1表示带有随机值r_A的参数,u_2表示带有随机值r_a、r_A的参数,w_1表示使用秘密值β将参数u_4隐藏后的参数,w_2表示使用秘密值β将参数u_5隐藏后的参数,δ_1表示使用非对称加密算法将参数u_3加密后的参数,然后将消息$M_1=\{u_1||u_2||w_1||w_2||\delta_1||T_1\}$用$u_4$进行hash运算得到$M_2=h(u_1||u_2||w_1||w_2||u_4||\delta_1||T_1)$,最后将消息组$(M_1,M_2)$发送给车辆$V_B$;

对于车辆V_B来说,当接收到来自车辆V_A的消息后,首先检查时间戳的有效性以防止重放攻击,$T_C-T_1\leq\Delta T$,其中T_C表示当前时间戳,T_1表示第一时间戳,ΔT表示网络中的最大传输时延,如果不等式成立,则计算$u_4=w_1\cdot g^{-\beta}$,然后用u_4验证hash值M_2是否正确,$h(M_1||u_4)\overset{?}{=}M_2$,其中符号?表示验证是否正确,如果等式成立,车辆$V_B$会通过等式$u_1\cdot u_2\cdot u_4\cdot g^{-h(T_1)}=g^{\alpha}$验证车辆$V_A$的合法性,等式成立则通过验证,反之则放弃此次协商;如果车辆V_A通过了认证,车辆V_B将返回验证结果给车辆V_A;

车辆V_A接收到车辆V_B返回的消息后，首先检查时间戳的有效性$T_C-T_2 \leqslant \Delta T$，如果不等式成立，则计算$v_4=w_3 \cdot g^{-\beta}$和$v_5=w_4 \cdot g^{-\beta}$，并通过等式$v_1 \cdot v_2 \cdot v_4 \cdot g^{-h(T_2)} = g^{\alpha}$验证车辆$V_B$的合法性，如果等式成立，则通过验证；反之则放弃此次协商；如果车辆V_B通过了认证，那么车辆V_A计算共享密钥$SK_{AB} = h(v_5 || u_5 || v_5^{r_n})$，并通过$h(M_3 || SK_{AB}) \stackrel{?}{=} M_4$验证hash值，成立的话，完成密钥协商；最后计算$M_5=h(SK_{AB}||V_5||T_3)$，并将消息$(M_5,T_3)$发送给车辆$V_B$，其中$T_3$为第三时间戳；

对于车辆V_B来说，接收到V_A的返回消息后，首先检查时间戳，$T_C-T_3 \leqslant \Delta T$，如果等式成立，验证$M_5=h(SK_{AB}||V_5||T_3)$，等式成立的话，完成密钥协商；

所述车辆V_A对u_1,u_2,w_1,w_2,δ_1的计算方式为：$u_1 = S_A \cdot g^{r_A}$；

$u_2 = g^{-r_A-r_a}$；$u_3 = g^{-r_A}$；$\delta_1 = E_{P_k}(u_3)$；$u_4 = g^{K_A} \cdot g^{h(T_1)+r_a}$；$w_1=u_4 \cdot g^{\beta}$；

$u_5 = g^{r_n}$；$w_2=u_5 \cdot g^{\beta}$；

如果车辆V_A通过了认证，车辆V_B将返回验证结果给车辆V_A，具体包括；

车辆V_B选取3个随机数r_B、r_b、r_m，并计算需要返回的相关参数v_1,v_2,w_3,w_4,δ_2，计算方式为：$v_1 = S_B \cdot g^{r_B}$；$v_2 = g^{-r_B-r_b}$；$v_3 = g^{-r_B}$；

$\delta_2 = E_{P_k}(v_3)$；$v_4 = g^{K_B} \cdot g^{h(T_2)+r_b}$；$w_3=v_4 \cdot g^{\beta}$；$v_5 = g^{r_m}$；$w_4=v_5 \cdot g^{\beta}$；其中$T_2$为第二时间戳，然后$V_B$计算共享密钥$SK_{AB} = h(u_5 || v_5 || u_5^{r_m})$，并将消息$M_3=\{v_1||v_2||w_3||w_4||\delta_2||T_2\}$用$SK_{AB}$进行hash运算得到$M_4=h(v_1||v_2||w_3||w_4||\delta_2||T_2||SK_{AB})$，最后将消息$(M_3,M_4)$发送给车辆$V_A$。

一种具有强匿名性的车联网认证及密钥协商方法

技术领域

[0001] 本发明属于车联网领域，具体涉及一种面向车联网的两方认证及密钥协商方法。

背景技术

[0002] 车联网能够为智能交通系统的发展与部署提供极大的帮助，因此受到了社会各层的广泛关注。由于典型的车联网结构由三部分组成，分别是可信第三方、车载单元、路侧单元，由于大量的密钥协商方案都是需要路侧单元支持的三方认证方案，而这在现实生活中又是有一定局限性的。例如，车辆在一些人烟稀少的偏远地区行驶，同样需要获得该区域的一些路况信息，而这些地区可能由于地处偏僻，并没有部署路侧单元，那么此时就只能通过车辆与车辆之间的两方认证来完成通信及信息交换。现有的一些两方认证及密钥协商方法也能达到此目的，但是在效率上存在缺陷。比如一些方法中使用的是双线性对技术，这提高了方法的安全性却大幅降低了方法的高效性。总而言之，如何权衡安全性、高效性、隐私保护这三方面，设计出一种合理的认证及密钥协商方法是本研究的难点所在。因此，本文在保证安全性和隐私保护的前提下，提出一种无双线性对运算的两方认证及密钥协商方法。

发明内容

[0003] 本发明旨在解决以上现有技术的问题。提出了一种计算开销相对较小、在确保安全的前提下提高了方法的性能的具有强匿名性的车联网认证及密钥协商方法，本发明的技术方案如下：

[0004] 一种具有强匿名性的车联网认证及密钥协商方法，该方法包括三个步骤：

[0005] 1)、系统初始化步骤，用于完成车辆及服务器初始化的相关工作；

[0006] 2)、车辆注册步骤，对合法用户进行注册登记；

[0007] 3)、认证及密钥协商步骤，用于在特定环境下，采用包括散列函数、模乘法群在内的密码学基本知识，在基于计算性Diffie-Hellman难题的基础上实现两方认证及密钥协商，使得对等的通信双方能够在无第三方的帮助下，实现相互认证并完成密钥协商，完成对其他车辆的认证，并与其安全通信；

[0008] 所述步骤1)的系统初始化步骤主要包括：车辆用户i获取车辆V_i的唯一身份信息ID_i以及设定一个只有自己知道的口令PW_i；服务器S生成自己的公私钥对：公钥P_k、私钥P_s，并选取随机数X作为自己的主密钥，再选取随机数α，β作为秘密值，然后选取hash函数h(•)及非对称加密算法E_k(•)，最后公布公共信息h(•)，E_k(•)和P_k；

[0009] 所述车辆注册过程包括：需注册的车辆V_i通过安全的渠道将自己的身份信息ID_i和用户口令PW_i提交给服务器S；服务器S得到这些数据后，会计算相关的参数K_i、S_i、φ_i、θ_i；其中K_i表示将主密钥和车辆身份进行hash后的参数，S_i表示带有系统秘密值α的参数，φ_i表示带有用户口令的参数，θ_i表示带有用户口令以及系统秘密值β的参数，计算方式为：$K_i=h(ID_i||X)$；$S_i = g^{-K_i+\alpha}$；$\varphi_i = g^{K_i}\cdot g^{-h(PW_i)}$；$\theta_i = g^{\beta}\cdot g^{-h(PW_i)}$，g表示循环加

法群G 的生成元，然后服务器S会将参数S_i、φ_i、θ_i返回给车辆V_i，车辆V_i将接受到的参数存放于防篡改装置TPD中；

[0010] 所述认证及密钥协商过程会完成以下工作；假设在特定环境下，车辆V_A需要与车辆V_B进行通信，过程如下：

[0011] 对于车辆V_A来说，为了发起一个认证及密钥协商过程，它首先选取3个随机数r_A、r_a、r_n，然后计算通信时所需的参数u_1,u_2,w_1,w_2,δ_1，u_1表示带有随机值r_A的参数，u_2表示带有随机值r_a、r_A的参数，w_1表示使用秘密值β将参数u_4隐藏后的参数，w_2表示使用秘密值β将参数u_5隐藏后的参数，δ_1表示使用非对称加密算法将参数u_3加密后的参数，然后将消息 $M_1=\{u_1||u_2||w_1||w_2||\delta_1||T_1\}$用$u_4$进行hash运算得到 $M_2=h(u_1||u_2||w_1||w_2||u_4||\delta_1||T_1)$，最后将消息组$(M_1,M_2)$发送给车辆$V_B$；

[0012] 对于车辆V_B来说，当接收到来自车辆V_A的消息后，首先检查时间戳的有效性以防止重放攻击，$T_C-T_1\leqslant\Delta T$，其中T_C表示当前时间戳，T_1表示第一时间戳，ΔT表示网络中的最大传输时延，如果不等式成立，则计算$u_4=w_1\cdot g^{-\beta}$，然后用u_4验证hash值M_2是否正确，$h(M_1||u_4)\stackrel{?}{=}M_2$，其中符号?表示验证是否正确，如果等式成立，车辆$V_B$会通过等式$u_1\cdot u_2\cdot u_4\cdot g^{-h(T_1)}=g^{\alpha}$验证车辆$V_A$的合法性，等式成立则通过验证，反之则放弃此次协商；如果车辆V_A通过了认证，车辆V_B将返回验证结果给车辆V_A；

[0013] 车辆V_A接收到车辆V_B返回的消息后，首先检查时间戳的有效性 $T_C-T_2\leqslant\Delta T$，如果不等式成立，则计算$v_4=w_3\cdot g^{-\beta}$和$v_5=w_4\cdot g^{-\beta}$，并通过等式$v_1\cdot v_2\cdot v_4\cdot g^{-h(T_2)}=g^{\alpha}$验证车辆$V_B$的合法性，如果等式成立，则通过验证；反之则放弃此次协商；如果车辆V_B通过了认证，那么车辆V_A计算共享密钥$SK_{AB}=h(v_5||u_5||v_5^{r_n})$，并通过$h(M_3||SK_{AB})\stackrel{?}{=}M_4$验证hash值，成立的话，完成密钥协商；最后计算$M_5=h(SK_{AB}||V_5||T_3)$，并将消息$(M_5,T_3)$ 发送给车辆V_B，其中T_3为第三时间戳；

[0014] 对于车辆V_B来说，接收到V_A的返回消息后，首先检查时间戳， $T_C-T_3\leqslant\Delta T$，如果等式成立，验证$M_5=h(SK_{AB}||V_5||T_3)$，等式成立的话，完成密钥协商；

[0015] 所述车辆V_A对u_1,u_2,w_1,w_2,δ_1的计算方式为：$u_1=S_A\cdot g^{r_A}$；

$u_2=g^{-r_A-r_a}$；$u_3=g^{-r_A}$；$\delta_1=E_{P_k}(u_3)$；$u_4=g^{K_A}\cdot g^{h(T_1)+r_a}$；$w_1=u_4\cdot g^{\beta}$；

$u_5=g^{r_n}$；$w_2=u_5\cdot g^{\beta}$；

[0016] 如果车辆V_A通过了认证，车辆V_B将返回验证结果给车辆V_A，具体包括；

[0017] 车辆V_B选取3个随机数r_B、r_b、r_m，并计算需要返回的相关参数 v_1,v_2,w_3,w_4,δ_2，计算方式为：$v_1=S_B\cdot g^{r_B}$； $v_2=g^{-r_B-r_b}$； $v_3=g^{-r_B}$；

$\delta_2=E_{P_k}(v_3)$；$v_4=g^{K_B}\cdot g^{h(T_2)+r_b}$；$w_3=v_4\cdot g^{\beta}$；$v_5=g^{r_m}$；$w_4=v_5\cdot g^{\beta}$；其中$T_2$为第二时间戳，然后$V_B$计算共享密钥$SK_{AB}=h(u_5||v_5||u_5^{r_m})$，并将消息$M_3=\{v_1||v_2||$

$w_3||w_4||\delta_2||T_2\}$用$SK_{AB}$进行hash运算得到 $M_4=h(v_1||v_2||w_3||w_4||\delta_2||T_2||SK_{AB})$，最后将消息$(M_3,M_4)$发送给车辆$V_A$。

[0018] 本发明的优点及有益效果如下：

[0019] 本发明创新性的在基于计算性Diffie-Hellman难题的基础上使用模幂运算、hash运算等方法来构造一个安全的认证及密钥协商方法，一般而言，基于Diffie-Hellman难题的两方认证方案，能够保证一定的安全性，但是在对用户的匿名性和争议可追踪性上存在着矛盾。想要保证匿名性就必须隐藏个性化特征，但这样就达不到可追踪性的要求；保证可追踪性就必须提供个性化特征，但这样就达不到匿名性的要求。因此，在方案中通过模幂运算、hash运算、随机化等方法将车辆个性化特征带入传递参数，例如$u_4 = g^{K_A} \cdot g^{h(T_1)+r_a}$、$v_4 = g^{K_B} \cdot g^{h(T_2)+r_b}$等。这使得方案在获得可追踪性的同时也保证了匿名性，另外由于对δ_1,δ_2的加密处理：$\delta_1 = E_{P_k}(u_3)$、$\delta_2 = E_{P_k}(v_3)$，使得方案具有数据间不可关联性，具有更可靠的安全性。由于采用的方法计算量都较小，所以在确保安全的前提下，也能较好的提高方法的性能。本发明存在现实应用场景，当车辆在偏远地区，附近没有路侧单元或基站时，可以通过本发明的方法进行安全的通信过程，不用在各个地方部署路侧设备，这可以节省大量的人力和物力资源。

附图说明

[0020] 图1是本发明提供优选实施例的场景图；

[0021] 图2为两方认证的注册过程图；

[0022] 图3为两方认证的认证及密钥协商过程图。

具体实施方式

[0023] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、详细地描述。所描述的实施例仅仅是本发明的一部分实施例。

[0024] 本发明解决上述技术问题的技术方案是：

[0025] 参照图1-图3所述，本发明的技术方案是：

[0026] 1)在如图1的场景中，我们假设车辆V_A和车辆V_B都是已经注册过得合法用户，即车辆V_A和车辆V_B都已经获得了通信时所需的所有相关参数。

[0027] 2)对于车辆V_A来说，为了发起一个认证及密钥协商过程，它首先选取3个随机数r_A、r_a、r_n，然后计算通信时所需的参数u_1,u_2,w_1,w_2,δ_1。计算方式为：

$u_1 = S_A \cdot g^{r_A}$ ； $u_2 = g^{-r_A-r_a}$ ； $u_3 = g^{-r_A}$ ； $\delta_1 = E_{P_k}(u_3)$ ；

$u_4 = g^{K_A} \cdot g^{h(T_1)+r_a}$ ；$w_1=u_4 \cdot g^{\beta}$；$u_5 = g^{r_n}$ ；$w_2=u_5 \cdot g^{\beta}$。其中T_1为时间戳，然后将消息$M_1=\{u_1||u_2||w_1||w_2||\delta_1||T_1\}$用$u_4$进行hash运算得到 $M_2=h(u_1||u_2||w_1||w_2||u_4||\delta_1||T_1)$，最后将消息组$(M_1,M_2)$发送给车辆$V_B$。如图1中的①所示。

[0028] 3)对于车辆V_B来说，当接收到来自车辆V_A的消息后，首先检查时间戳的有效性以防止重放攻击，$T_C-T_1 \leq \Delta T$，其中T_C表示当前时间戳，ΔT表示网络中的最大传输时延。如果不

等式成立，则计算$u_4=w_1 \cdot g^{-\beta}$，然后用u_4验证hash 值M_2是否正确，$h(M_1||u_4)\overset{?}{=}M_2$，这样做的目的是为了防止消息被篡改。如果等式成立，车辆V_B会通过等式$u_1 \cdot u_2 \cdot u_4 \cdot g^{-h(T_1)}=g^{\alpha}$验证车辆$V_A$的合法性，等式成立则通过验证，反之则放弃此次协商。如果车辆V_A通过了认证，接下来车辆V_B将选取3个随机数r_B、r_b、r_m，并计算需要返回的相关参数 v_1,v_2,w_3,w_4,δ_2。计算方式为：$v_1=S_B \cdot g^{r_B}$； $v_2=g^{-r_B-r_b}$； $v_3=g^{-r_B}$；

$\delta_2=E_{P_k}(v_3)$； $v_4=g^{K_B} \cdot g^{h(T_2)+r_b}$；$w_3=v_4 \cdot g^{\beta}$；$v_5=g^{r_m}$；$w_4=v_5 \cdot g^{\beta}$。其中$T_2$为时间戳，然后$V_B$计算共享密钥$SK_{AB}=h(v_5||u_5||v_5^{r_n})$，并将消息 $M_3=\{v_1||v_2||w_3||w_4||\delta_2||T_2\}$用$SK_{AB}$进行hash运算得到 $M_4=h(v_1||v_2||w_3||w_4||\delta_2||T_2||SK_{AB})$，最后将消息$(M_3,M_4)$发送给车辆$V_A$。如图1中②所示。

[0029] 4)对于车辆V_A来说，接收到车辆V_B返回的消息后，首先检查时间戳的有效性以防止重放攻击，$T_C-T_2 \leqslant \Delta T$，如果不等式成立，则计算$v_4=w_3 \cdot g^{-\beta}$和 $v_5=w_4 \cdot g^{-\beta}$，并通过等式$v_1 \cdot v_2 \cdot v_4 \cdot g^{-h(T_2)}=g^{\alpha}$验证车辆$V_B$的合法性，如果等式成立，则通过验证；反之则放弃此次协商。如果车辆V_B通过了认证，那么车辆V_A计算共享密钥$SK_{AB}=h(v_5||u_5||v_5^{r_n})$，并通过$h(M_3||SK_{AB})\overset{?}{=}M_4$验证hash值，成立的话，完成密钥协商。最后计算 $M_5=h(SK_{AB}||V_5||T_3)$，并将消息(M_5,T_3)发送给车辆V_B，其中T_3为时间戳。如图1中③所示。

[0030] 5)对于车辆V_B来说，接收到V_A的返回消息后，首先检查时间戳，$T_C-T_3 \leqslant \Delta T$，如果等式成立，验证$M_5=h(SK_{AB}||V_5||T_3)$，等式成立的话，完成密钥协商。

[0031] 以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

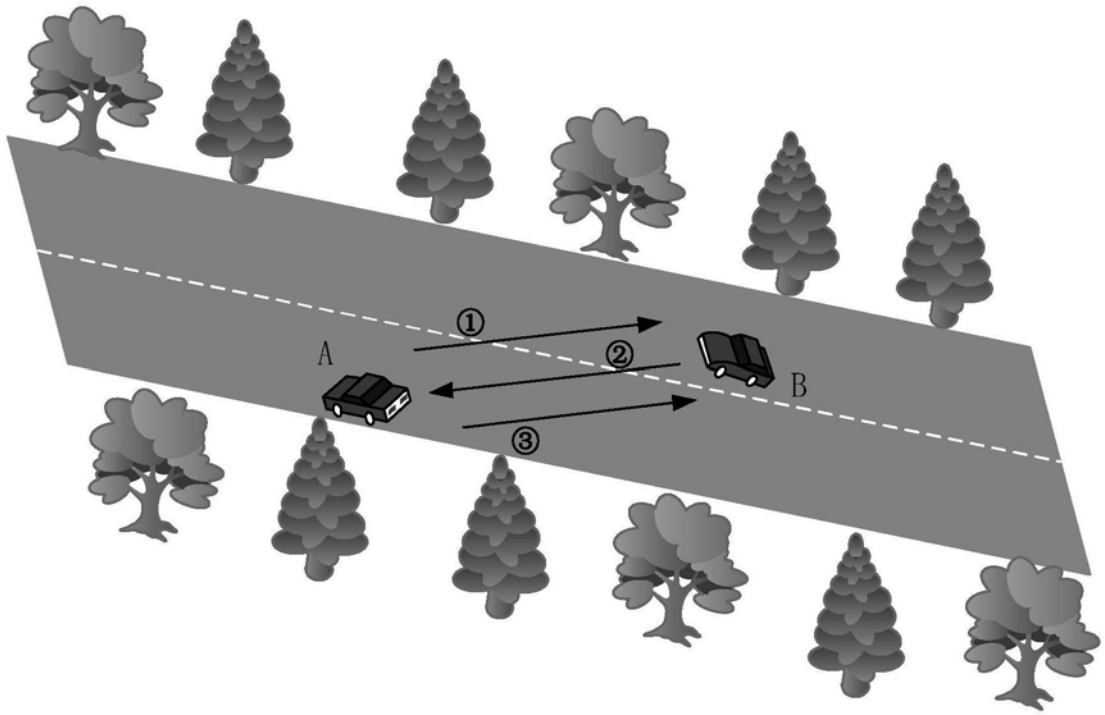

①
②
③
A
B

图1

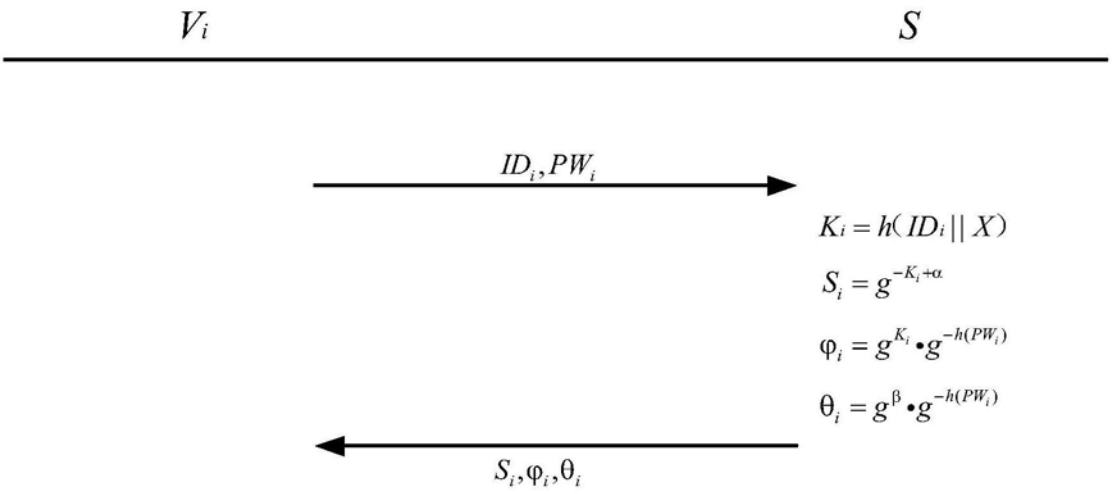

V_i
S
ID_i, PW_i
$K_i = h(ID_i || X)$
$S_i = g^{-K_i+\alpha}$
$\varphi_i = g^{K_i} \bullet g^{-h(PW_i)}$
$\theta_i = g^{\beta} \bullet g^{-h(PW_i)}$
S_i, φ_i, θ_i

图2

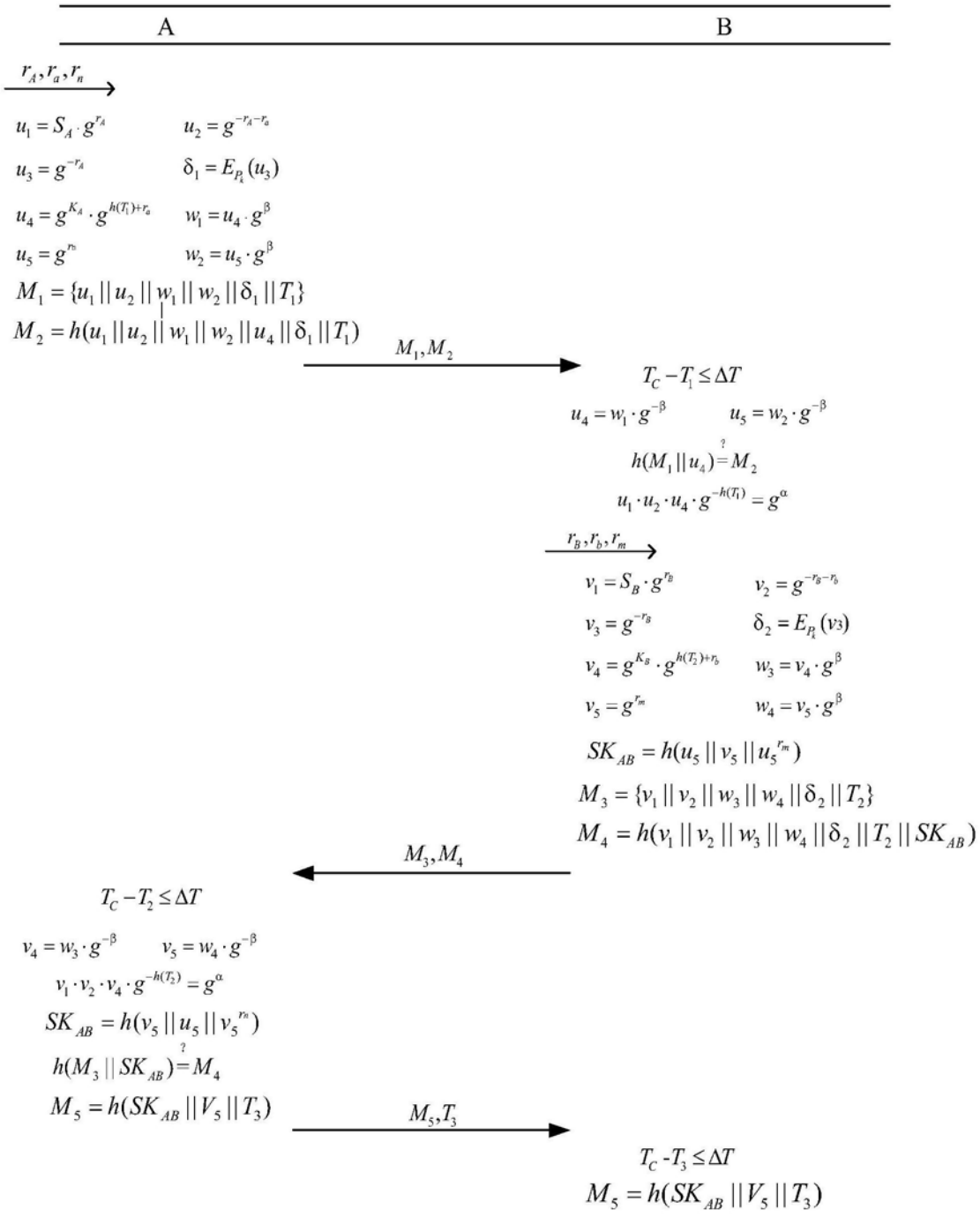

A
B
r_A, r_a, r_n
$u_1 = S_A \cdot g^{r_A}$
$u_2 = g^{-r_A - r_a}$
$u_3 = g^{-r_A}$
$\delta_1 = E_{P_k}(u_3)$
$u_4 = g^{K_A} \cdot g^{h(T_1)+r_a}$
$w_1 = u_4 \cdot g^{\beta}$
$u_5 = g^{r_n}$
$w_2 = u_5 \cdot g^{\beta}$
$M_1 = \{u_1 || u_2 || w_1 || w_2 || \delta_1 || T_1\}$
$M_2 = h(u_1 || u_2 || w_1 || w_2 || u_4 || \delta_1 || T_1)$
M_1, M_2
$T_C - T_1 \le \Delta T$
$u_4 = w_1 \cdot g^{-\beta}$
$u_5 = w_2 \cdot g^{-\beta}$
$h(M_1 || u_4) \stackrel{?}{=} M_2$
$u_1 \cdot u_2 \cdot u_4 \cdot g^{-h(T_1)} = g^{\alpha}$
r_B, r_b, r_m
$v_1 = S_B \cdot g^{r_B}$
$v_2 = g^{-r_B - r_b}$
$v_3 = g^{-r_B}$
$\delta_2 = E_{P_k}(v3)$
$v_4 = g^{K_B} \cdot g^{h(T_2)+r_b}$
$w_3 = v_4 \cdot g^{\beta}$
$v_5 = g^{r_m}$
$w_4 = v_5 \cdot g^{\beta}$
$SK_{AB} = h(u_5 || v_5 || u_5^{r_m})$
$M_3 = \{v_1 || v_2 || w_3 || w_4 || \delta_2 || T_2\}$
$M_4 = h(v_1 || v_2 || w_3 || w_4 || \delta_2 || T_2 || SK_{AB})$
M_3, M_4
$T_C - T_2 \le \Delta T$
$v_4 = w_3 \cdot g^{-\beta}$
$v_5 = w_4 \cdot g^{-\beta}$
$v_1 \cdot v_2 \cdot v_4 \cdot g^{-h(T_2)} = g^{\alpha}$
$SK_{AB} = h(v_5 || u_5 || v_5^{r_n})$
$h(M_3 || SK_{AB}) \stackrel{?}{=} M_4$
$M_5 = h(SK_{AB} || V_5 || T_3)$
M_5, T_3
$T_C - T_3 \le \Delta T$
$M_5 = h(SK_{AB} || V_5 || T_3)$

图3