基于簇的水声传感器网络的安全认证协议

任超群[1] 徐 明[1,2]
(上海海事大学信息工程学院 上海 201306)[1] (同济大学电子与信息工程学院 上海 201804)[2]

摘 要 近年来,基于簇的水声传感器网络得到广泛应用。由于水声传感器多用于军事行业,使得提高水声传感器网络的安全性变得十分重要。针对提高水声传感器网络安全性这一问题,提出了结合ECC Diffie-Hellman密钥交换、一元高阶多项式、双线性映射和哈希函数的安全认证协议。经过分析,该协议满足了认证、访问控制、数据保密性、数据完整性和不可否认性等安全需求。结合BAN逻辑进行形式化分析,证明该协议是安全的;同时,将协议的两个阶段分别与同类型认证协议进行对比,实验结果表明,所提协议的性能在时间或者空间上有所提升。

关键词 水声传感器,认证协议,双线性映射,BAN逻辑
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.031

Security Authentication Protocol Based on Cluster for Underwater Acoustic Sensor Networks

REN Chao-qun[1] XU Ming[1,2]
(College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China)[1]
(College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)[2]

Abstract In recent years, the application of underwater acoustic sensor networks based on cluster is widely used. The underwater acoustic sensor is mainly used in military industry, which emphasizes the importance of safety. In order to improve the safety of underwater acoustic sensor networks, this paper presented a secure authentication protocol, which combines the ECC Diffie-Hellman key exchange, single variable higher order polynomial bilinear mapping and hash function. After analyzing, this protocol satisfies safety requirements in authentication, access control, data confidentiality, data integrity and non-repudiation. This protocol is proved to be secure when combined with BAN logic formal analysis. In addition, the two stages of this protocol are compared with the same type certification protocol separately. The comparison results show that the performance of this protocol is improved in time and space.

Keywords Underwater acoustic sensor, Authentication protocol, Bilinear mapping, BAN logic

1 引言

无线传感器网络主要由大量资源有限的传感器节点和基站组成,网络中的传感器节点被部署到大面积地理区域来感知和收集各种信息,包括温度、湿度、入侵检测、车辆运动等。水声传感器网络是用来收集水下环境数据、监测水下环境的无线传感器网络,由于水下环境的恶劣性未知以及无线传感器网络的大规模性等各方面原因,使得水声传感器网络安全变得非常重要,近年来水声传感器的广泛应用使得水声传感器网络的安全性得到逐步优化,本文就此目的结合双线性映射、一元高次多项式、ECC Diffie-Hellman密钥交换提出一种基本安全的基于簇的认证协议,结合BAN逻辑非形式化分析,本协议能提供多种安全需求。

2 系统模型

在一个基于簇的水下传感器网络中,一个网络有多个簇,且每个簇有一个簇头节点,簇头聚合由簇成员(即非簇头节点)节点收集数据发送给陆地上的基站。本文的环境基于以下几点假设:

(1)假设簇头节点与成员节点在功能上没有什么不同。

(2)假设基站的安全级别非常高,基站是可信的,不考虑基站被盗用的可能。

(3)假设所有的网络实体通过一些现有时间同步机制保持松散的时间同步。

(4)假设生存周期合理,不会过短影响正常通信,不会过长引起非授权节点重放已经发送过的消息。生存周期的详情不在本文的讨论范围之内。

3 协议设计

3.1 系统参数标记表

本文所提方案将用到的符号标记如表1所列。

到稿日期:2015-09-26 返修日期:2016-03-06 本文受国家自然科学基金项目(61202370),上海市教委科研创新项目(14YZ110),中国博士后科学基金资助项目(2014M561512)资助。

任超群(1991—),女,硕士生,主要研究方向为水声传感器网络、网络安全,E-mail:chaoqunren@foxmail.com;徐 明(1977—),男,博士,副教授,主要研究方向为水声传感器网络、网络安全与隐私保护、智能信息处理。

表1 系统参数表

字符	含义
parameters	系统公共参数
n, p, q	大素数
P	G_1 的生成元
Z_p	模为 p 的有限域
$E_p(a,b)$	模为 p 的有限域
G	Ep(a,b)的基点
GF(p)	阶为 p 的有限域，p 为素数，域定义为 Z_p 及其上模 p 的算术运算
Z_p^*	乘法群
f(x)	有限域 Z_p 上的多项式
G_1	一个 q 阶循环加法群
G_2	一个 q 阶循环乘法群
e	一个双线性映射$G_1 \times G_1 \rightarrow G_2$
H	从{0,1}* 到G_1 中的哈希映射函数
h	能将任意长度输入映射一个固定长度输出
t_i	i 的时间戳
N_i	i 的随机数
$E_k(\cdot)$	表示使用密钥 k 的对称加密算法
CA	可信的认证机构
$K_x^- K_x^+$	x 的私钥、公钥
K_{sk}	会话密钥
$D_k(\cdot)$	表示使用密钥 k 的对称解密算法

3.2 簇头与基站之间的通信设计

假设簇头 i 向基站发送消息。将这个协议设计过程描述为以下几个步骤。

3.2.1 协议初始化

(1)基站产生安全认证系统的公共参数 $parameters(p,q,a,b,n,G,Zp,G_1,G_2,e^{[13,14]},Z_p^*)$。

(2)基站选定阶 r 和 $f(x)$的系数为 $a^*=(a_0,a_1,a_2,\cdots,a_r)$，用来确定 $f(x)$并为每个簇头节点分配身份 ID_i。

$$\Phi_i=f(ID_i) \tag{1}$$

基站以身份 ID_i 为因变量代入 $f(x)$，按照式(1)计算 Φ_i，并在节点部署前将 Φ_i 分发给簇头节点，簇头存储自己的身份密钥(ID_i,Φ_i)对，基站建立身份密钥(ID_i,Φ_i)对列表。

(3)选定一个哈希函数 H，可以将任意长度的字符串映射到G_1 中的数值。选定一个函数 h 可以将任意长度的输入映射到固定长度的输出。

(4)基站更新安全认证系统的公共参数[1] $parameters(p,q,a,b,n,G,Z_p,G_1,G_2,e,H,h,f,Z_p^*)$。

3.2.2 簇头 i 与基站之间共享密钥交换[2]

$$P_s=n_s\times G \tag{2}$$

(1)基站选择一个小于 n 的整数 n_s 作为它的私钥，然后按照式(2)计算公钥 P_s，这个公钥 P_s 是 $E_p(a,b)$中的点，并将它广播给所有簇头节点。

$$P_i=n_i\times G \tag{3}$$

$$K=n_i\times P_s \tag{4}$$

$$M_1=P_i \parallel K \parallel t_i \parallel ID_i \parallel lt \parallel N \parallel h(t_i \parallel ID_i) \tag{5}$$

(2)簇头 i 选择一个小于 n 的整数 n_i 作为 i 的私钥，然后按照式(3)计算公钥 P_i，按照式(4)计算共享密钥 K。这个公钥 P_i 同样也是 $E_p(a,b)$中的点，簇头将式(5)发送给基站。

$$t_s-t_i>lt \tag{6}$$

$$K'=n_s\times P_i \tag{7}$$

$$K=n_i\times P_s=n_i\times n_s\times G=K'=n_s\times P_i=n_s\times n_i\times G \tag{8}$$

$$h'(t_i \parallel ID_i)=h(t_i \parallel ID_i) \tag{9}$$

(3)基站收到后首先检查 N 的新鲜性，如果随机数不新鲜，那么基站将丢弃这条消息；如果随机数新鲜，基站继续检查式(6)是否成立。如果成立则该消息过期，基站将其丢弃；如果不成立，基站将按照式(7)计算 K'。比较这个 K'与收到的 K 是否相等，由于对于合法簇头，式(8)必然成立，因此如果不相等，直接将这个消息丢弃并认为簇头是恶意节点；如果相等，则基站取出式(5)中得到的 ID_i 并检查是否存在自己的身份列表里。若不存在则将这条消息丢弃；若存在则取出 ID_i 与 t_i 进行计算并得到 h'[3]。检查式(9)是否成立，如果不成立则认为这个节点是伪造节点，基站将整个消息丢弃；若成立则基站存储 P_i。这个密钥交换方法是用椭圆曲线密码实现 Diffie-Hellman 密钥交换方法，由于大素数求椭圆曲线离散对数问题在计算上是不可行的，且 Diffie-Hellman 交换方法经过改进后能抵御中间人攻击，因此我们认为密钥交换是安全的。

3.2.3 簇头节点 i 与基站之间发送消息

$$M_3=E_{\Phi_i}(M_2) \tag{10}$$

$$M_2=(t_i \parallel lt \parallel N_i \parallel SIG_i \parallel auth) \tag{11}$$

$$auth=E_K(ID_i \parallel t_i \parallel C_m \parallel h(C_m)) \tag{12}$$

$$C_m=\{k_iG,M+k_iP_s\}=\{C_1,C_2\} \tag{13}$$

$$SIG_i=\langle s,\theta_i\rangle \tag{14}$$

$$s=H(n_iP_s)+\alpha_i \tag{15}$$

$$\theta_i=e(P,P)^{\alpha_i} \tag{16}$$

其中，M 是簇头 i 要发送给基站的原始消息，C_m 是加密消息，SIG_i 是簇头签名，k_i 是一个随机正整数，$auth$ 是认证部分。

(1)簇头对原始消息 M 产生加密消息 C_m。簇头从 Z_p^* 中随机选择一个正整数 k_i，按照式(13)产生一个密文 C_m，该密文是一个点对。

(2)簇头 i 产生对原始消息的簇头签名。簇头 i 从 Z_p^* 中随机选择 α_i，按照式(16)计算 θ_i。传感器节点进一步按照式(15)计算 s。$\langle s,\theta_i\rangle$作为其签名[4]，即 $SIG_i=\langle s,\theta_i\rangle$。

(3)簇头 i 按照式(12)计算产生认证器 $auth$。

(4)簇头用 Φ_i 加密 M_2 生成 M_3 并将其发送给基站。这里 Φ_i 充当簇头与基站之间的会话密钥，由于 Φ_i 是基站产生并分发给簇头节点并存储起来的，因此仅有基站和簇头有 Φ_i。

3.2.4 基站收到簇头 i 发送的消息后，对消息进行处理

$$M_2=D_{\Phi_i}(M_3) \tag{17}$$

(1)基站从自己的存储列表中取出 Φ_i，按照式(17)将收到的消息 M_3 进行解密得到 M_2，如果基站找不到对应的正确的密钥来解密这个消息，则这个消息不合法，将它丢弃。

(2)基站取出 N 检查它的新鲜性，如果不新鲜则将其丢弃；如果新鲜继续下一步。

(3)基站检查式(6)是否成立，如果成立则该消息超时，基站丢弃这条消息；如果不成立则继续下一步。

$$ID_i \parallel t_i \parallel C_m \parallel h(C_m)=D_K(auth) \tag{18}$$

(4)基站再次通过认证器互相认证身份[3]。首先基站用自己的私钥和簇头的公钥计算得到 K 并按照式(17)来解密认证器，从而得到簇头 i 的身份和时间戳 $ID_i \parallel t_i \parallel h(C_m)$。然后比较式(18)和式(11)里面的时间戳是否一致，如果不一致则基站将消息丢弃；如果一致，继续比较式(18)里的 ID_i 是否存在于基站本身存储的簇头预分配身份表中，如果存在，将这个 ID_i 按照式(1)计算得到 Φ_i'，比较其与基站存储的$(ID_i,$

Φ_i)是否一致。如果不一致，基站丢弃这个消息；如果一致，基站将式(18)里得到的 C_m 进行哈希得到 $h'(C_m)$ 并比较它与式(18)的 $h(C_m)$ 是否一致。若不一致，基站将它丢弃，否则基站认为它是合法的，继续下一步。

(5)基站验证簇头对 i 对消息的签名[8]。

$$\theta_i' = e(s,p)e(-H(n_sP_i),p) \tag{19}$$

基站按照式(19)计算得到 θ_i'，比较 θ_i' 与 M_2 中 SIG_i 里的 θ_i 是否相等。如果不相等则认为这个签名不合法，将这个消息丢弃；如果相等则认为这个签名合法，继续下一步。

$$M = C_2 - n_s \times C_1 \tag{20}$$

(6)基站通过处理 C_m 获得原始消息 M。基站通过用接收到的 C_m 和自己的私钥计算得到 M。

3.3 簇成员节点与簇头之间的通信设计

3.3.1 协议初始化

(1)在系统部署之前，基站为每一个簇成员节点分配身份 ID_j，并计算

$$\Phi_j = f(ID_j) \tag{21}$$

将 Φ_j 作为成员节点 j 的身份标识，与身份 ID_j 有同等的标识身份的作用。通过 ECC Diffie-Hellman 密钥交换方法实现基站与簇成员节点 j 交换共享秘钥 K_{sj}，即成员节点 j 产生了私钥 n_j 和公钥 $P_j = n_j \times G$，并且有

$$K_{sj} = n_s \times P_i = n_s \times n_j \times G = n_j \times n_s \times G = n_j \times P_s \tag{22}$$

基站与成员节点均将(ID_j，Φ_j，K_{sj})存储在自己的列表中。

(2)设有一个可信认证机构 CA 在系统部署之前为簇成员节点和簇头节点分发节点证书[6]。对于成员节点 j 和簇头节点 i 分别有：

$$Cert_j = E_{K_{CA}^-}(ID_j \| \Phi_j \| t_{CA} \| lt) \tag{23}$$

$$Cert_i = E_{K_{CA}^-}(ID_i \| \Phi_i \| t_{CA} \| lt) \tag{24}$$

可信认证机构将它的公钥 K_{CA}^+ 广播给所有节点，即系统中每个节点有 CA 的公钥 K_{CA}^+。

(3)系统部署之后，任意一个簇成员节点 j 广播它的基本信息 BI_j 给这个簇里面其它簇成员节点。

$$BI_j = (ID_j, \Phi_j, Cert_j) \tag{25}$$

它的任意一个邻居节点 j' 收到 j 发送的基本信息之后检查 $Cert_j$。

$$ID_j \| \Phi_j \| t_{CA} \| lt = D_{K_{CA}^+}(Cert_j) \tag{26}$$

$$t_j' - t_{CA} < lt \tag{27}$$

$$f(ID_j) = \Phi_j' = \Phi_j \tag{28}$$

解密 $Cert_j$，检查这个基本信息是否过期，如果式(27)成立，则没有过期；如果不成立，则过期将其丢弃。没有过期则先检查式(28)是否成立，若不成立则该节点是伪结点；若成立则继续比较 Φ_j 与解密证书得到的 Φ_j 是否一致。若不一致，则判断该节点是伪结点并将这个基本信息丢弃，若一致，则该节点的基本信息通过检查。

$$\Phi_j < \Phi_{j'} + H(P) \tag{29}$$

所有其他成员节点 j' 检查式(29)是否成立，若成立，则 j' 存储 j 的基本信息并回复它的基本信息给 j，$BI_{j'} = (ID_{j'}, \Phi_{j'}, Cert_{j'})$。$j$ 以同样的方式核实 j' 的基本信息，并判断是否要存储 j' 的基本信息。最终这个过程的每个簇里面每个成员节点都有自己证人节点的基本信息列表，将每个成员节点的基本信息作一个备份[5]以防止伪造节点攻击。

3.3.2 成员节点 j 的注册过程设计

(1)簇成员 j 向簇头节点 i 发送消息

$$I_1 = N_j \| Cert_j \tag{30}$$

$$ID_j \| \Phi_j \| t_{CA} \| lt = D_{K_{CA}^+}(Cert_j) \tag{31}$$

$$f(ID_j) = \Phi_j' = \Phi_j \tag{32}$$

$$t_j - t_{CA} < lt \tag{33}$$

N_j 是由簇成员节点 j 随机产生的随机数。簇头节点 i 收到消息后验证 N_j 的新鲜性，若随机数不新鲜则将其丢弃；否则簇头节点按照式(31)解密 $Cert_j$ 得到 ID_j、Φ_j、t_{CA}、lt。首先检查簇成员节点 j 的身份 ID_j 的合法性，若不合法，则将这个消息丢弃；若合法，则继续按照式(32)比较簇头节点计算的 Φ_j' 与解密证书得到的 Φ_j 是否一致。若不一致，则该证书不合法，将整个消息丢弃，若一致则判断式(33)是否成立，若不成立则该证书过期，若成立则认为该消息合法。簇头节点 i 存储 N_j 和 $Cert_j$。

(2)簇头节点 i 向基站发送消息

$$I_2 = E_{K_{is}}(ID_j \| N_j \| N_i) \| Cert_i \tag{34}$$

$$ID_j \| N_j \| N_i = D_{K_{is}}(E_{K_{is}}(ID_j \| N_j \| N_i)) \tag{35}$$

基站收到消息首先如同式(34)解密并检查 $Cert_i$ 的合法性，若合法则按式(35)解密消息的前半部分来获得 ID_j、N_j、N_i，基站首先检查 i 和 j 是否是合法用户，若是则继续检查 N_j 和 N_i 的新鲜性，若不新鲜则将这个消息丢弃，否则基站认为该消息合法存储(ID_j N_j)和(ID_i N_i)对。

(3)基站向簇头 i 发送消息

$$I_3 = E_{K_{js}}(ID_i \| N_j \| N_i \| N_s \| K_{ij}) \| E_{K_{js}}(ID_j \| N_i \| N_s \| K_{ij}) \tag{36}$$

$$ID_j \| N_i \| N_s \| K_{ij} = D_{K_{js}}(E_{K_{js}}(ID_j \| N_i \| N_s \| K_{ij})) \tag{37}$$

K_{ij} 是基站产生的簇头 i 和簇成员节点 j 的会话密钥。簇头 i 收到消息后按式(37)解密消息的后半部分到 ID_j，N_i，N_s，K_{ij}。由于本文假设基站是可靠的且不是恶意的，因此簇头检查 ID_j 与式(31)的 ID_j 是否一致，若不一致则认为簇头节点是恶意节点并丢弃；若一致则继续比较解密得到的 N_s 的新鲜性。若不新鲜则丢弃这个消息；若新鲜则保存 K_{ij}。

(4)簇头 i 向簇成员节点 j 发送消息

$$I_4 = E_{K_{js}}(ID_i \| N_i \| N_s \| K_{ij}) \| E_{K_{ij}}(N_j \| N_i \| N_s) \| Cert_i \tag{38}$$

$$ID_i \| N_j \| N_s \| K_{ij} = D_{K_{js}}(E_{K_{js}}(N_j \| N_i \| N_s \| K_{ij})) \tag{39}$$

$$N_i \| N_s = D_{K_{ij}}(E_{K_{ij}}(N_i \| N_s)) \tag{40}$$

簇成员节点 j 首先按照式(31)解密证书，然后检查它的合法性，若不合法则丢弃整个消息，若合法则按照式(39)解密消息的第一部分。首先检查 N_s 的新鲜性，然后将解密获取的 K_{ij} 按照式(40)来解密消息的第二部分。将式(40)得到的 N_i 和 N_s 与式(39)里得到的进行对比，若不一致则丢弃整个消息，若一致则保存 K_{ij} 和 N_s。

(5)簇成员节点 j 向簇头节点 i 发送消息

$$I_5 = E_{K_{ij}}(nonce_s) \tag{41}$$

$$nonce_s = D_{K_{ij}}(I_5) \tag{42}$$

簇头节点 i 收到消息后按照式(42)解密消息得到 N_s，与自己本地存储的 N_s 进行比较，若不一致则丢弃该消息；否则簇成员节点注册过程完成。

成员节点 j 注册的目的就是得到由基站分配的仅合法的该成员节点和该成员节点与之通信的簇头节点 i 所共享的会话密钥 K_*，这个会话密钥用于成员节点与簇头节点之间通信的加密消息。成员节点注册过程如图 1 所示。

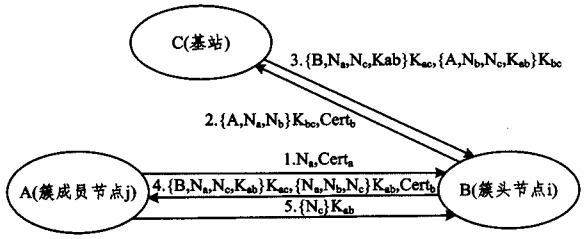

图 1　成员节点的注册流程

4　协议分析

4.1　簇头与基站之间协议分析

4.1.1　正确性分析

(1)公式 $\theta_i'=e(s,p)e(-H(n_sP_i),p)=\theta_i$ 是成立的。证明如下：

$$\begin{aligned}\theta_i' &= e(s,p)e(-H(n_sP_i),p)\\ &= e(H(n_sP_i),p)e(\alpha_i p,p)e(-H(n_sP_i),p)\\ &= e(H(n_in_sG),p)e(n_sP_i,p)e(-H(n_sn_iG),p)\\ &= e(H(n_in_sG),p)e(H(n_sn_iG),p)^{-1}e(p,p)^{\alpha_i}\\ &= e(p,p)^{\alpha_i}\end{aligned}$$

(2)公式 $M=C_2-n_s\times C_1$ 是成立的。证明如下：

$$\begin{aligned}M &= C_2-n_s\times C_1\\ &= M+k_iP_s-n_sk_iG\\ &= M+k_in_sG-n_sk_iG\\ &= M\end{aligned}$$

4.1.2　安全性分析

无线传感器网络在具体的应用过程中，需要进行数据采集、数据融合、处理以及任务的协调控制等。为了抵御各种安全攻击和威胁，保证任务执行的机密性、数据的可靠性、数据融合的正确性以及数据传输的安全性等，对于无线传感器网络提出了主要的安全需求，本文提出的协议能提供以下安全服务。

认证：密钥交换阶段，簇头发送 $M_1=P_i\parallel K\parallel t_i\parallel ID_i\parallel lt\parallel N\parallel h(t_i\parallel ID_i)$ 给基站来交换共享密钥，基站通过取出收到的 M_1 里的 ID_i 查找自己为节点分配的身份列表，判断其身份的合法性来保证通信的实体的合法性，其次通过计算和比对式(9)来保证通信的实体就是它所声称的通信实体。通信阶段，基站用来解密 M_3 的密钥 Φ_i 是基站 ID_i 分配的，只有合法的 ID_i 才有对应的 Φ_i。其次基站解密式(17)得到 ID_i，基站比对该 ID_i 再次保证了收到的信息来源是所声称的来源。

访问控制：本文的水声传感器网络环境只考虑了通信双方是否合法，由于没有优先级或访问权限的限制，因此只要保证通信双方合法，就保证了提供访问控制服务。通信双方通过了身份认证就已经保证了提供访问控制服务，如根据以上分析所提方案确实提供了身份认证，所以这个方案提供了访问控制。

数据保密性：对于消息通信阶段，首先基站收到的 M_3 是 M_2 用 Φ_i 加密过的，因为这个 Φ_i 是由基站计算并分发的，只有与之通信的簇头和基站才有，所以这个消息 M_2 是保密的。$auth$ 是用簇头和基站之间的共享密钥 K 加密的，通过 ECC Diffie-Hellman 密钥交换实现 K 的交换，ECC Diffie-Hellman 密钥交换是安全的，所以 K 是保密的且 C_m 也是保密的。由于要传输的消息 M 在 C_2 之中，因此 M 是保密的。

数据完整性：要传送的 M 在 C_m 中，如果 C_m 被修改、插入或者删除过，那么在基站把收到的 C_m 进行哈希得到的 $h'(C_m)$ 与 $auth$ 后面附带的 $h(C_m)$ 进行比对时就会出现不一致，基站丢弃整条信息，通信失败。如果消息被重放，那么基站在解密 M_3 得到 M_2 进而得到 N_i 就会不新鲜，基站会丢弃整条消息通信结束，所以数据完整性得到了保证。

不可否认性：密钥交换阶段，基站收到 M_1 且获得 ID_i 后比对它的合法性以确保该发送消息实体身份的合法性，确保发送者的身份合法后，通过比对附带的哈希函数值来确保身份没有被伪造过，以此来确保发送消息的实体不可否认地发送了消息。通信阶段，基站除了验证发送者实体的身份，还主要验证发送者的签名，即验证式(16)等于式(19)来确保发送消息的实体不可否认地发送了消息。式(16)等于式(19)的证明是基于双线性映射的，对于双线性映射，如果 $\forall U,V,W\in G_1$，找到一个 $X\in G$ 使得 $e(U,V)=e(W,X)$ 是很难的，事实上是计算上不可行的，所以签名是安全的。所以我们认为签名可以进一步保证发送消息实体的不可否认性。

4.1.3　空间复杂度分析

身份认证协议是保护系统的第一道重要屏障，对于系统安全起着不可或缺的作用。1978 年 Needham-Schroeder 提出了具有认证功能的密钥分配协议，许多学者对身份认证协议做了大量的研究，如文献[9,10]等。随着身份认证协议的发展和优化，按是否依赖第三方可分为：基于可信第三方认证协议和双方认证协议。同时也出现了一些著名的身份认证方案和基于 ID 的身份认证方案。椭圆曲线加密由于有更小的密钥长度、更小的带宽且实现速度快，受到了众多学者的关注和研究[8]。2000 年，Sakai、Ohgishi 和 Kasahara 分别独立地利用双线性配构造了基于身份密钥共享方案，使得 Shamir 猜想的基于身份的公钥密码体制变为现实。此后许多学者将双线性应用到身份认证中，提出了许多新颖有效的认证协议，如文献[2,4]。

簇头与基站之间协议是一种基于双线性映射、一元高次多项式、ECC Diffie-Hellman 密钥交换的双方认证协议。我们对此协议进行空间复杂度分析，并将其与同类的新颖的协议(文献[14])作比较，结果如表 2 所列。

表 2　空间复杂度分析表

步骤	文献[14]	簇头与基站之间的协议
第一步	$S_K+S_{ID}+2S_H$	S_K
第二步	$3S_K+S_{ID}+S_L+S_T+S_{SG}$	$2S_K+S_{ID}+S_T+S_H+S_N+S_{LT}$
第三步	$S_K+S_M+S_T+S_{SG}$	$S_K+S_{ID}+2S_T+S_H+S_N+S_{SG}+S_{LT}$
总开销	$5S_K+2S_{ID}+2S_T+2S_{SG}+2S_H+S_M+S_L$	$5S_K+2S_{ID}+3S_T+S_{SG}+2S_N+2S_{LT}$

文献[14]没有明确说明认证阶段。我们取车辆发送消息给认证中心为第一步，车辆发送消息给路边单元为第二步，路边单元发送消息给认证中心为第三步。这三步已完成车辆到认证中心的身份认证和传递原始消息 M 的完整过程，本协议也证明了上述功能有可比性。双线性对采用 Miyaji-Nakabayashi-Takano(MNT)曲线，生成元为 160 位长。循环群元素长度为 161 位[10]。表 2 中，S_K 为密钥所占空间，长度为 21 字节；

S_{ID}为身份所占空间，文献[14]取4字节，但现在的无线传感器网络节点数不超过200个只需要2字节[4]，考虑到将来数量会变大也取4字节；S_T为时间戳所占空间，4字节；S_{SG}为椭圆曲线签名所占空间，20字节；S_H为哈希结果所占空间，20字节(SHA-1)；S_M为原始消息所占空间，20字节；S_L为载荷，100字节；S_N为随机数所占空间，2字节；S_{LT}为生存周期，1字节。文献[14]的总开销与本协议的总开销之差为：

$$\Delta S = S_M + S_L + S_{SG} - S_T - 2S_N - 2S_{LT}$$
$$= 20 + 100 + 20 - 4 - 2*2 - 2*1 = 130$$

因此本协议较节约空间开销。由于文献[14]的载荷过于大，对结果计算造成大的影响，假设没有S_L，则$\Delta S=30$，不影响本协议较其节约空间开销的结果。

4.2 簇成员与簇头之间的协议分析

本文用BAN逻辑[13]对簇成员节点j的注册过程进行形式化分析。

将簇成员节点j、簇头节点i、基站分别用A,B,C通信主体来代替，可信认证机构用T来代替，以便进一步分析。协议过程如下：

(1)$A\rightarrow B:N_a, Cert_a$

(2)$B\rightarrow C:\{A,N_a,N_b\}K_{bc}, Cert_b$

(3)$C\rightarrow B:\{B,N_a,N_c,K_{ab}\}K_{ac},\{A,N_b,N_c,K_{ab}\}K_{bc}$

(4)$B\rightarrow A:\{B,N_a,N_c,K_{ab}\}K_{ac},\{N_a,N_b,N_c\}K_{ab}, Cert_b$

(5)$A\rightarrow B:\{N_c\}K_{ab}$

4.2.1 BAN逻辑形式化分析

BAN逻辑在对协议进行形式化分析时，主要解决4个方面的问题：1)认证协议是否正确；2)认证协议的目标是否达到；3)认证协议的初设是否合适；4)认证协议是否存在冗余。

本文只用BAN逻辑分析所提安全协议的前3个问题，第4个问题有待进一步研究。

BAN逻辑中安全目标的一般形式如下：

$$B|\equiv A \overset{K_{ab}}{\longleftrightarrow} B$$

$$B|\equiv A|\equiv A \overset{K_{ab}}{\longleftrightarrow} B$$

$$A|\equiv A \overset{K_{ab}}{\longleftrightarrow} B$$

$$A|\equiv B|\equiv A \overset{K_{ab}}{\longleftrightarrow} B$$

4.2.2 初始化假设

A_1 $A|\equiv A \overset{K_{ac}}{\longleftrightarrow} C$

A_2 $B|\equiv B \overset{K_{bc}}{\longleftrightarrow} C$

A_3 $C|\equiv A \overset{K_{ac}}{\longleftrightarrow} C$

A_4 $C|\equiv B \overset{K_{bc}}{\longleftrightarrow} C$

A_5 $C|\equiv A \overset{K_{ab}}{\longleftrightarrow} B$

A_6 $A|\equiv C\Rightarrow A \overset{K_{ab}}{\longleftrightarrow} B$

A_7 $B|\equiv C\Rightarrow A \overset{K_{ab}}{\longleftrightarrow} B$

A_8 $A|\equiv \#(N_a)$

A_9 $B|\equiv \#(N_b)$

A_{10} $C|\equiv \#(N_c)$

A_{11} $C|\equiv \#(A \overset{K_{ab}}{\longleftrightarrow} B)$

A_{12} $B|\equiv \#(A \overset{K_{ab}}{\longleftrightarrow} B)$

4.2.3 协议理想化

省略对协议分析意义不大的部分，协议理想化如下。

$(1')B\lhd N_a$

$(2')C\lhd \{N_a,N_b\}K_{bc}$

$(3')B\lhd \{N_a,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{ac},\{N_b,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{bc}$

$(4')A\lhd \{N_a,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{ac},\{N_a,N_b,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{ab}$

$(5')B\lhd \{N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{ab}$

4.2.4 逻辑推论规则

$$R_1 \quad \frac{P\lhd (X,Y)}{P\lhd (X)}$$

$$R_2 \quad \frac{P|\equiv P \overset{K}{\longleftrightarrow} Q, P\lhd \{X\}_K}{P|\equiv Q|\sim X}$$

$$R_3 \quad \frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$$

$$R_4 \quad \frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

$$R_5 \quad \frac{P|\equiv Q|\equiv (X,Y)}{P|\equiv Q|\equiv X}$$

$$R_6 \quad \frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$$

$$R_7 \quad \frac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$$

4.2.5 逻辑推理

由$(3')$应用规则R_1得到

$$B\lhd \{N_b,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{bc} \tag{43}$$

由假设A_2和式(43)，应用规则R_2得到

$$B|\equiv C|\sim \{N_b,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{44}$$

由式(44)应用规则R_7得到

$$B|\equiv C|\sim A \overset{K_{ab}}{\longleftrightarrow} B \tag{45}$$

由假设A_9和式(45)应用规则R_4得到

$$B|\equiv C|\equiv A \overset{K_{ab}}{\longleftrightarrow} B \tag{46}$$

由假设A_7和式(46)，应用规则R_6得到

$$B|\equiv A \overset{K_{ab}}{\longleftrightarrow} B \tag{47}$$

由$(5')$和式(47)，应用规则R_2得到

$$B|\equiv A|\sim \{N_c,A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{48}$$

由式(48)应用规则R_7得到

$$B|\equiv A|\sim A \overset{K_{ab}}{\longleftrightarrow} B \tag{49}$$

由式(49)和假设R_1应用规则R_4得到

$$B|\equiv A|\equiv A \overset{K_{ab}}{\longleftrightarrow} B \tag{50}$$

由$(4')$应用规则R_1得到

$$A\lhd \{N_a,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\}K_{ac} \tag{51}$$

由式(51)和假设A_1应用规则R_2得到

$$A|\equiv C|\sim \{N_a,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{52}$$

由假设A_8应用规则R_3得到

$$A|\equiv \#\{N_a,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{53}$$

由式(52)和式(53)应用规则R_4得到

$$A|\equiv C|\equiv \{N_a,N_c,A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{54}$$

由式(54)应用规则R_5得到

$$A|\equiv C|\equiv A \overset{K_{ab}}{\longleftrightarrow} B \tag{55}$$

由式(55)和假设 A_6 应用规则 R_6 得到

$$A|\equiv A \overset{K_{ab}}{\longleftrightarrow} B \tag{56}$$

由(4′)应用规则 R_1 得到

$$A \lhd \{N_a, N_b, N_c, A \overset{K_{ab}}{\longleftrightarrow} B\} K_{ab} \tag{57}$$

由式(56)和式(57)应用规则 R_2 得到

$$A|\equiv B|\sim \{N_a, N_c, A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{58}$$

由假设 A_8 应用规则 R_3 得到

$$A|\equiv \#\{N_a, N_b, N_c, A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{59}$$

由式(58)和式(59)应用规则 R_4 得到

$$A|\equiv B|\equiv \{N_a, N_c, A \overset{K_{ab}}{\longleftrightarrow} B\} \tag{60}$$

由式(60)应用规则 R_5 得到

$$A|\equiv B|\equiv A \overset{K_{ab}}{\longleftrightarrow} B \tag{61}$$

综上所述，本文提出的协议达到了 4.2.1 节中的前 3 个安全目标[13]，所以本协议是安全的。

4.2.6 时间复杂度分析

近年来出现了基于 ID 的身份认证方案的形式化定义和严格的安全证明[6,13]。随后提出了众多的形式化分析方法，由 Burrows 等提出的 BAN 逻辑最具影响力，广泛用于认证协议的分析中。本文提出的簇成员与簇头之间的协议是基于可信第三方的认证协议，并且采用 BAN 逻辑形式化分析语言证明其安全性。我们对此协议进行时间复杂度分析并将其与文献[6]中的同类型身份认证协议进行比较。文献[6]中的协议有数个多重加密，有较多冗余，本协议添加了基于身份的高阶多项式值作为身份验证和时间戳，在降低冗余的情况下没有对安全性造成破坏。时间复杂度分析结果如表 3 所列。

表 3 时间复杂度分析

步骤	文献[6]	簇成员与簇头之间的协议
第一步	$3T_N+2T_H+3T_{XOR}$	$T_N+T_{SD}+2T_{XOR}$
第二步	$2T_{SE}+2T_{SD}+2T_H+3T_{XOR}+T_{DD}$	$T_N+T_{SE}+T_{SD}+2T_{XOR}$
第三步	$T_N+3T_{SE}+2T_{SD}+2T_{AE}+T_{AD}+5T_{XOR}+T_{DD}+2T_K$	$T_N+2T_{SE}+T_{SD}+T_{XOR}+T_K$
第四步	$T_{SD}+T_{AD}+2T_{XOR}$	$T_{SE}+3T_{SD}+4T_{XOR}$
第五步	$2T_H+2T_{XOR}$	$T_{SE}+T_{SD}+T_{XOR}$
总时间	$4T_N+5T_{SE}+5T_{SD}+15T_{XOR}+2T_{AE}+2T_{AD}+2T_K+6T_H+2T_{DD}$	$3T_N+5T_{SE}+7T_{SD}+10T_{XOR}+T_K$

表 3 中每一步时间计算包括发送者的操作时间和接收者的验证时间，即开始下一步发送消息之前的所有时间开销。其中，TN 为产生一个随机数的时间；T_{SE} 为作一次非对称加密的时间；T_{SD} 为作一次非对称解密的时间；T_{AE} 为作一次对称加密的时间；T_{AD} 为作一次对称解密的时间；T_{XOR} 为作一次异或操作的时间；T_K 为产生一次会话密钥的时间；T_H 为作一次哈希操作的时间；T_{DD} 为验证一次数字签名的时间。

将文献[6]方案的总时间与本方案的总时间作差，得：

$$\Delta T = T_N + 5T_{XOR} + 2T_{AE} + 2T_{AD} + T_K + 6T_H + 2T_{DD} - 2T_{SD}$$

显然，ΔT 为正值，所以本方案较文献[6]节约了计算时间，对于水声传感器网络，计算时间越短越有利于节约传感器节点的能量，能节约能量的认证方案非常有利。

结束语 多项式求根问题、离散对数问题、椭圆曲线离散对数问题、Diffie-Hellman 和双线性映射是计算上的难解问题，结合这几种难解问题来提高认证协议在数学意义上的复杂程度，从而提高协议的安全性是可取的。BAN 逻辑形式化分析对于协议安全性分析是很好的工具，传统的 BAN 逻辑受到过许多学者的进一步研究，本文用 BAN 逻辑分析证明了所提协议是安全的。

参 考 文 献

[1] Li L C, Liu R S. Securing Cluster-Based Ad Hoc Networks with Distributed Authorities[J]. IEEE Transactionson on Wireless Communications, 2010, 9(10): 3072-3081

[2] Guo M H, Liaw H T, Deng D J, et al. Cluster-based securecommunication mechanism in wireless ad hoc networks[J]. Net Information Security, 2010, 4(4): 352-360

[3] Islam M R, Azad S, Morshed M M. A Secure Communication Suite for Cluster-based Underwater Surveillance Networks[C]// 2014 International Conference on IEEE Electrical Engineering and Information & Communication Technology (ICEEICT). 2014: 1-5

[4] Lu H, Li J, Guizani M. Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(3): 750-761

[5] Zhang Rui, Shi Jing, Zhang Yan-chao, et al. Secure Top-k Query Processing in Unattended[J]. IEEE Transactions on Vehicular Technology, 2014, 63(9): 4681-4693

[6] Vaidya B, Pyun J Y, Pan S, et al. Secure framework for intergrated multipath MANTE with internet[C]// Internation Symposium on Application and the Internet. 2008: 83-88

[7] Bellare M, Namprempre C, Neven G. Security Proofs for Identity Based Identification and Signature Schemes[J]. Journal of Cryptology, 2009, 22(1): 1-61

[8] Yasmin R, Ritter E, Wang G. An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures[C]// 2010 IEEE 10th International Conference on Computer and Information Technology (CIT). IEEE, 2010: 882-889

[9] Kiliani H. An Efficient and Transparent One-Time Authentication Protocol with Non-interactive Key Scheduling and Update [C]// IEEE International Conference on Advanced Information Networking & Applications. IEEE, 2014: 351-358

[10] Krishna R. Cookie-based acceleration of an authentication protocol: US, US8887233[P]. 2014

[11] Guo C, Zhang Z J, Zhu L H, et al. A novel secure group RFID authentication protocol[J]. Journal of China Universities of Posts & Telecommunications, 2014, 21(1): 94-103

[12] Yang Shi-ping. Security protocol and BAN Logic [D]. Guiyang: Guizhou University, 2007(in Chinese)
杨世平. 安全协议及其 BAN 逻辑分析研究[D]. 贵阳：贵州大学，2007

[13] Yang Tao. Based proxy signature vehicle from research networking privacy [D]: Beijing: Beijing University, 2013(in Chinese)
杨涛. 基于代理签名的车辆自组网的隐私保护研究[D]. 北京：北京大学，2013

[14] He Dao-jing. Key Technology of wireless network security [D]. Hangzhou: Zhejiang University, 2012(in Chinese)
何道敬. 无线网络安全的关键技术研究[D]. 杭州：浙江大学，2012