基于对的无线 Ad hoc 网络可追踪邻居匿名认证方案

周 曜 平 萍 徐 佳 刘凤玉
(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 为解决传统无线 Ad hoc 网络邻居匿名认证方案容侵性不佳以及难以锁定恶意节点身份的问题,提出一种基于双线性对的无线 Ad hoc 网络可追踪邻居匿名认证方案。采用基于身份的公钥系统,节点随机选择私钥空间中的数作为临时私钥,与身份映射空间的节点公钥以及一个公开的生成元模相乘得到临时公钥,利用双线性映射的性质协商会话密钥并实现匿名认证。通过在随机预言机模型下的形式化分析,表明本方案在 BCDH 问题难解的假设下可对抗攻击者的伪装行为,同时利用认证过程中交互的临时公钥可有效锁定恶意节点真实身份。

关键词 计算机应用,匿名认证,双线性对,可追踪,无线 Ad hoc 网络
中图法分类号 TP309.7 **文献标识码** A

Pairing-based Traceable Neighborhood Anonymous Authentication Scheme for Wireless Ad hoc Networks

ZHOU Yao PING Ping XU Jia LIU Feng-yu
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract To improve the disadvantage in traditional anonymous authentication schemes for wireless ad hoc networks which are vulnerable to nodes intrusion and unable to trace malicious nodes, a pairing-based traceable neighborhood anonymous authentication scheme was proposed. Using an ID-based public key system, the authenticating node chooses a random number from the private key space as its temper private key, and then multiplies this temper private key with his ID-based public key and an all-known generator respectively to create its temper public key. Using such temper keys pair, the node can establish anonymous authentication with its neighbors in a secure and efficient way. By formally analyzing this scheme under random oracle model, it is shown that this scheme can efficiently resist the impersonation attacks as long as the BCDH problem is hard and the hostile nodes can be traced through their temper public keys by the network manager.

Keywords Computer application, Anonymous authentication, Bilinear pairing, Traceable, MANET

1 引言

无线 Ad hoc 网络(Wireless Ad Hoc Networks, MANET)是一种由多个移动节点组成的自组织无中心无线网络,用于满足战场、灾区等环境恶劣场合的联网需求。当 MANET 用于军事用途时,出于保护关键节点身份的目的,通信匿名性是必须考虑的问题。但由于 MANET 在节点资源、物理层防御等方面的局限,匿名安全易遭受节点入侵攻击威胁。作为匿名安全的基本保证机制,匿名认证同样不可避免地要面对此类挑战。

MANET 的邻居匿名认证是实现网络通信匿名性与秘密性的关键。邻居间通过匿名认证确认对方为合法节点并秘密协商会话密钥,非邻居间的通信安全可通过逐跳加密通信内容得到保证。业界已经就 MANET 中的邻居匿名认证问题开展了多角度研究,文献[1-5]是一些典型解决方案。Ciszkowski 等[1]通过为节点生成多个不可比较公钥实现邻居间匿名认证;Misra 等[2]提出基于预分配注册伪名的匿名认证方案,其计算复杂度低于文献[1];Kim 等[3]改进了文献[2]中的伪名分配机制,降低了节点伪名存储成本;Wu 等[4]提出基于共享公钥的盲签名方案,使得认证过程不需第三方参与;Zhang 等[5]利用双线性对的性质设计了基于预注册伪名的匿名密钥协商机制。这些方案虽然实现了它们各自所定义的匿名性与安全性指标,但在容侵性、可追踪性和性能方面均存在局限,而被侵蚀节点的秘密暴露会对整个任务的可靠性造成威胁[6]。在文献[2,3]中,邻居匿名认证过程需在线第三方参与,第三方一旦被侵蚀,整个系统的匿名性完全失去;文献[1]方案容侵性虽较好,但其公钥证书的生成与验证开销过高;文献[4]方案同样存在计算开销过高的问题,且对于被侵蚀节点

到稿日期:2008-12-04 返修日期:2009-02-25 本文受国家自然科学基金资助项目(90718021),"十一五"重点研究项目"无线自组网自适应架构及安全性研究"资助。

周 曜 男,博士,主要研究方向为无线自组织网络技术、加密理论、入侵检测,E-mail:zhouyao@mail.njust.edu.cn;平 萍 女,博士生,主要研究方向为信息安全、元胞自动机、加密技术理论与算法设计等;徐 佳 男,博士生,主要研究方向为无线网络路由技术;刘凤玉 女,教授,博士生导师,主要研究方向为信息安全、入侵检测等。

的真实身份不具可跟踪性；文献[5]方案伪名列表预存于节点中，节点被侵蚀会导致以往通信中的匿名性丧失。因此，如何在 MANET 中设计高容侵与可追踪的高效匿名认证方案仍然是待解决的问题。

本研究提出一种新的基于双线性对的 MANET 可追踪邻居匿名认证方案，并对方案安全性给出了随机预言机模型(Random Oracle Model，ROM)下的形式化证明。本文方案具有以下特点：①认证伪名由节点自主生成，不需第三方参与，伪名的随机性保证了无法从以往通信内容中推测出节点的真实身份。②认证双方所协商密钥在节点私钥泄漏的情况下仍具有保密性，即满足前向安全性。③有效对抗对手的伪装行为，对于被侵蚀节点可根据认证脚本追踪其真实身份。④同以往基于对的认证方案相比，具有较低的计算开销。本方案与现有的其他方案相比，能够更加有效地抵抗攻击者的入侵行为，从而更适用于 MANET 这一特殊应用环境。

2 方案描述

2.1 预部署阶段

在部署 MANET 节点前，由离线的密钥分配中心(KDC)确定公开的系统参数 $params=\{p,q,E/F_p,G_1,G_2,H_1,H_2,P,P_{pub},\hat{e}\}$，其中 p,q 为满足安全强度要求的两个大素数；E/F_p 为定义在有限域 F_p 上的椭圆曲线，G_1 为 E/F_p 上点所构成加群的一个 q 阶子群；G_2 为乘群 F_p^* 的一个 q 阶子群；$H_1:\{0,1\}^*\rightarrow G_1^*$ 和 $H_2:\{0,1\}^*\rightarrow\{0,1\}^n$ 为单向抗碰撞散列化函数，分别将任意长度字符串随机映射为 G_1^* 中的点和长度固定为 n 的字符串；P 为 G_1 中任选生成元，$P_{pub}=tP$ 为系统公钥，$t\in Z_q^*$ 为秘密的系统主密钥；$\hat{e}:G_1\times G_1\rightarrow G_2$ 为 G_1、G_2 上的双线性映射，并具有以下重要性质[8]：

对于任意的 Q_1、$Q_2\in G_1$，a、$b\in Z_q^*$，都有 $\hat{e}(aQ_1,bQ_2)=\hat{e}(Q_1,Q_2)^{ab}$。

KDC 为网络中每个节点，比如 X，分配唯一身份 ID_X 以及对应私钥 $S_X=tH_1(ID_X)$，X 的公钥为 $Q_X=H_1(ID_X)$。由于 G_1 中的离散对数难解，每个节点只知道自己的私钥，而无法得到系统主密钥。

2.2 邻居匿名认证

邻居节点间通过互相交换临时公钥与伪名完成匿名认证和会话密钥协商。认证过程节点在本地发起，触发条件为：①节点被首次部署到网络以及漫游到一个新的位置；②节点改变目前所使用的伪名；③节点判断需要重新认证的其他情况(比如会话密钥泄漏)。

以节点 A 为例，当 A 需同邻居发起认证时，A 随机选择临时私钥 $a\in Z_q^*$，计算 $T_A=aQ_A$ 和 $W_A=aP$，以 (T_A,W_A) 作为临时公钥(这样的临时公钥可在 A 空闲时预计算多个，以提高效率)。之后，A 对外广播认证请求报文 AREQ(Authentication Request)，格式为：

$[\mathrm{AREQ},seq,T_A,W_A,TS_A,VS_A]$

其中，seq，TS_A，VS_A 分别为本次认证序列号、时间戳和 AREQ 报文校验和。同时，A 在一张临时表中记录 $\langle seq,H_2(T_A,W_A)\rangle$，该记录被保持到 A 下次发起认证时为止。

当邻居 B 收到该请求时，判断是否

$$|time-TS_A|\leqslant\Delta T \tag{1}$$

其中，$time$ 为 B 的本地时间，ΔT 为预设的最大时间偏离。若上式不满足，B 丢弃该报文；否则 B 检查报文校验和。若无误，B 缓存 seq、$H_2(T_A,W_A)$、该报文的散列值，对以后收到的相同 seq 的报文，B 简单丢弃。该机制与时间戳协同，防止重放攻击。然后 B 使用它上次发起本地认证时所生成的临时公钥，即 (T_B,W_B)，其中 $T_B=bQ_B$，$WB=bP$，$b\in_R Z_q^*$，计算

$$K_{BA}=H_2(\hat{e}(T_A,bS_B),bW_A) \tag{2}$$

其中，$S_B=tQ_B$ 为 B 的长期私钥。以及

$$MAC_B=H_2(T_A,T_B,W_A,W_B,K_{BA},1) \tag{3}$$

完成上述计算后，B 广播一个认证响应报文 AREP(Authentication Response)，格式为：

$[\mathrm{AREP},seq,H_2(T_A,W_A),T_B,W_B,MAC_B,TS_B,VS_B]$

其中，seq 与 AREQ 报文中相同，TS_B 和 VS_B 分别为 B 的时间戳和 AREP 报文校验和。

A 通过 $H_2(T_A,W_A)$ 和 seq 的组合确认 AREP 为先前发出的请求响应，并检查 TS_B 和 VS_B 的合法性。若所有检查通过，A 计算

$$K_{AB}=H_2(\hat{e}(aS_A,T_B),aW_B) \tag{4}$$

其中，$S_A=tQ_A$ 为 A 的长期私钥。验证

$$MAC_B=H_2(T_A,T_B,W_A,W_B,K_{AB},1) \tag{5}$$

若相等，A 通过对 B 的认证，并在本地邻居表中增加记录：

$\langle PS_B=H_2(T_B,W_B,K_{AB}),K_{AB},ValidTime\rangle$

其中，$ValidTime$ 为记录有效时间。之后 A 计算

$$MACA=H_2(T_A,T_B,W_A,W_B,K_{AB},2) \tag{6}$$

广播响应确认报文(Response Acknowledge，RACK)

$[\mathrm{RACK},seq,H_2(T_A,W_A),MAC_A,TS_A',VS_A']$

其中，TS_A'为新的时间戳，VS_A'为 RACK 报文校验和。

B 检查时间戳与校验和无误后，验证

$$MAC_A=H_2(T_A,T_B,W_A,W_B,K_{BA},2) \tag{7}$$

若验证无误，则 B 通过对 A 的认证，并在本地邻居表中增加记录：

$\langle PS_A=H_2(T_A,W_A,K_{BA}),K_{BA},ValidTime\rangle$

至此，A 与 B 之间的双向匿名认证过程完成。在之后的通信中，A、B 分别以 PS_A 和 PS_B 作为自己的伪身份标识，并以 K_{AB}(或 K_{BA})为通信会话密钥。

A 同其他邻居间的匿名认证与 B 类似。图 1 是 A 同其邻居的匿名认证示例。

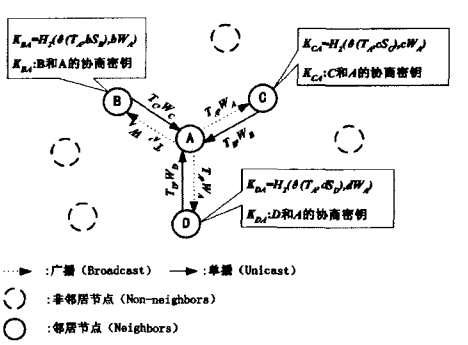

图 1 邻居匿名认证

认证的正确性：当 A 和 B 拥有由同一 KDC 分发的公私

钥对时，下面的等式成立

$$K_{BA}=H_2(\hat{e}(T_A,bS_B),bW_A)$$
$$=H_2(\hat{e}(aQ_A,b(tQ_B)),b(aP))$$
$$=H_2(\hat{e}(a(tQ_A),bQ_B),a(bP))$$
$$=H_2(\hat{e}(aS_A,T_B),aW_B)=K_{AB} \quad (8)$$

即 A 和 B 分别计算出的共享密钥相等，因此双方可通过验证对方 MAC 确认其为合法节点。

认证的匿名性：认证中与节点身份相关的公开信息仅有临时公钥。以 A 为例，窃听者如果要从 A 的临时公钥（$T_A=aQ_A, W_A=aP$）得到其真实公钥 Q_A，则面临着解决 G_1 中的离散对数问题，这是计算不可行的。

不可连接性：由于 G_1 为素数 q 阶循环群，根据素数阶群性质，G_1 中每一非零元素均为生成元。而临时公钥由 Z_q^* 中随机数与 G_1 生成元 Q_A 和 P 相乘得到，根据生成元的性质，临时公钥随机分布于 G_1 中，不同认证轮次生成的临时公钥不具比较性，即认证通信内容满足不可连接匿名（Unlinkable Anonymity）[7]。

与传统的基于预注册伪名列表的 MANET 匿名认证方案[1-3,5]相比，本方案具有良好的扩展性和容侵性。首先，每个节点只需拥有唯一的私钥即可完成匿名认证；其次，认证是完全分布式的，不需要与在线第三方进行实时交互；最后，部分节点被侵蚀不会导致其他节点的匿名性失去。

3 会话密钥安全性分析

认证的一个重要目的是协商安全的会话密钥。下面分析方案中密钥协商机制的安全性。

结论 1（方案满足已知密钥安全） 此类安全表明某一轮次会话密钥泄漏不会导致其他轮次的会话密钥也连带泄漏。在本方案中，由于临时私钥独立生成，每一轮次生成的会话密钥相互独立，某一轮次密钥泄漏不会危及到其他轮次密钥的安全。

结论 2（方案满足完美前向安全） 前向安全指节点的长期秘密泄露不会使之前会话密钥连带泄漏；完美前向安全指即使系统主密钥泄漏，也不会使之前的会话密钥泄漏。在本方案中，会话密钥由两部分共同散列得到。以前述 A、B 间密钥为例，第一，假设某个时刻节点 A 和 B 的长期私钥 S_A 和 S_B 泄漏给攻击者 C，C 要计算密钥的第一部分 $\hat{e}(T_A,bS_B)$ 或 $\hat{e}(aS_A,T_B)$，需由 $W_A=aP$ 或 $W_B=bP$ 得到 a 或 b，这相当于解决 G_1 中离散对数问题；第二，假设某个时刻系统主密钥 t 泄漏给 C，C 虽然可以通过下式计算出第一部分

$$\hat{e}(T_A,bS_B)=\hat{e}(aS_A,T_B)=\hat{e}(T_A,T_B)^t \quad (9)$$

但它还必须由 $W_A=aP$ 和 $W_B=bP$ 计算出第二部分，即 abP，这相当于解决 G_1 上计算 Diffie-Helleman 问题（CDH 问题），同样计算不可行。因此，无论何种长期密钥泄漏均不会导致之前所协商的共享密钥也连带泄漏，方案是完美前向安全的。

结论 3（方案满足密钥支配安全） 此类安全指任何一方均无法单独决定会话密钥。本方案中会话密钥由双方的临时公钥、长期私钥和临时私钥共同决定，任何一方都不具备对密钥的单方面支配权。

4 恶意节点追踪

由于 MANET 节点的资源有限，在一个长的时间窗里，节点被侵蚀是不可避免的。对于此类情况，必须存在有效机制以追踪到被侵蚀节点真实身份，即实现可追踪性。在方案中，可由系统管理者 KDC 根据认证方的临时公钥追踪其真实身份。

定义 1（可跟踪性） 设 T 为成员 u 和 u^* 之间的匿名认证通信脚本，若 u 和 u^* 的真实身份可由 T 得到，则称匿名认证方案满足可跟踪性。

定理 1 本方案满足可跟踪性。

证明：设 u 为被侵蚀节点，u 在认证过程中发送的临时公钥为 $T_u=hQ_u$ 和 $W_u=hP$，其中 $h\in_R Z_q^*$。则 u 的真实身份可通过以下方法确定：

密钥分配中心 KDC 从其掌握的节点私钥列表中随机选择某一私钥，比如节点 $\hat{u}$ 的私钥 $S_{\hat{u}}$，判断下式

$$\hat{e}(S_{\hat{u}},W_u)=\hat{e}(T_u,P_{pub}) \quad (10)$$

是否成立。

易见，当且仅当 $\hat{u}=u$ 时，有

$$\hat{e}(S_{\hat{u}},W_u)=\hat{e}(tQ_{\hat{u}},hP)=\hat{e}(tQ_u,hP)=\hat{e}(hQ_u,tP)$$
$$=\hat{e}(T_u,P_{pub}) \quad (11)$$

因此，KDC 可通过式(10)判断是否选择了正确的节点 u。若式(10)不成立，KDC 另选一个节点检验，直至发现 u 的真实身份。设网络中节点数为 n，追踪方案以不超过 n 次比对即可锁定 u 的身份。

5 形式化安全分析

5.1 相关定义

所使用模型借鉴文献[7]中匿名认证协议框架，其中攻击者的行为被设定为可无限制窃听与篡改通信内容，但无法在有限时间内解决 G_1 和 G_2 上的离散对数与双线性计算 DH 问题（BCDH 问题）。

对随机多项式时间（Probabilistic Polynomial Time，PPT）对手 A，定义以下成员伪装游戏（Member Impersonation Game，MIG）：

step 1 设所有合法成员集合为 G，A 随机选择 G 中一部分成员进行查询，得到它们的真实身份与长期私钥，设这些成员的集合为 U。

step 2 A 任选一个成员 $u^*\notin U$ 作为目标。

step 3 A 试图向 u^* 证明 $A\in G$，也就是说，A 试图在匿名认证过程中做出正确的响应。若 A 成功，则赢得游戏。

设 A 的伪装优势为

$$AdvMIG_A=\Pr[A\text{ 赢得 MIG}]$$

其中，$\Pr[.]$ 表示事件概率；并设 A 在事件 E 发生时的伪装优势为：

$$AdvMIG_A=\Pr[A\text{ 赢得 MIG}\mid E]$$

定义 2（成员伪装安全） 称匿名认证方案满足成员伪装安全，当对任一 PPT 对手 A，$AdvMIG_A^{U=\emptyset}$ 是可忽略的。

定义 2 说明以下安全性：当某个 PPT 对手未攻破 G 中任何一个节点时，它即便可以监听与分析足够多的匿名认证信

息，也无法以不可忽略的概率伪装 G 中成员成功。

5.2 安全分析

本文方案的成员伪装安全性基于以下双线性计算 DH (Bilinear Computing Diffie-Helleman, BCDH)困难问题：

定义 3(BCDH) 设 G_1，G_2 为素数 q(长度为 k)阶群，$\hat{e}$：$G_1\times G_1\to G_2$ 为双线性映射，P 为 G_1 生成元，x、y、$z\in_R Z_q^*$，则 $\langle G_1, G_2, \hat{e}\rangle$ 上的 BCDH 问题为：由 (P, xP, yP, zP) 计算 $\hat{e}(P, P)^{xyz}$。

称 BCDH 问题是困难的，若对任一 PPT 对手 A，其解决 BCDH 问题的优势

$$AdvBCDHA=\Pr[A(P,xP,yP,zP)=\hat{e}(P,P)^{xyz}]$$

在安全参数 k 下是可忽略的。

设方案中的散列函数 H_1 和 H_2 为随机预言机，以下定理说明了对手赢得 MIG 游戏优势与解决 BCDH 问题优势之间的关系。

定理 2 设 A 为 MIG 的 PPT 对手，Q_E 为 A 在 MIG step1 中执行查询的次数，Q_{H2} 为 A 查询 H_2 的次数，则存在 BCDH 的 PPT 对手 B，满足

$$AdvMIG_A^{U=\emptyset}\leqslant e\cdot(1+Q_E)\cdot Q_{H_2}\cdot AdvBCDH_B+\varepsilon(k)$$

其中，$\varepsilon(k)$为关于安全参数 k 的可忽略函数，$e\approx 2.72$ 为自然对数底。

为证明定理 2，首先对 PPT 对手 A 定义以下 GetPair 游戏。

step 1 A 对团体 G 中某些成员执行查询操作，获得它们的身份及私钥。设这些成员集合为 U。

step 2 A 任意选择成员 $u^*\notin U$ 作为目标。

step 3 A 利用自己身份生成临时公钥的第一部分 T_A 发送给 u^*，并从 u^* 处获得其生成的临时公钥第一部分 T_B，之后 A 输出 e_0。

设 t 为系统主密钥，若 $e_0=\hat{e}(T_A, tT_B)$，则 A 赢得游戏，A 在游戏中的优势为

$$AdvGetPair_A=\Pr[A\text{ 赢得 GetPair 游戏}]$$

引理 1 对 GetPair 游戏的 PPT 对手 A，存在 BCDH 的 PPT 对手 B，满足

$$AdvGetPair_A\leqslant e\cdot(1+Q_E)\cdot AdvBCDH_B+\varepsilon(k)$$

其中，Q_E 为 A 在 GetPair step1 中的查询次数，$\varepsilon(k)$对于安全参数 k 可忽略。

证明：B 仿真 A 的运行环境，利用 A 在 GetPair 游戏中的优势解决 BCDH 问题，即由 (P, xP, yP, zP) 解出 $\hat{e}(P, P)^{xyz}$。

预言机：B 按如下设定随机预言机 H_1 的输出，对于查询输入 d，B 首先运行一个概率函数 $Guess(.)$，满足

$Guess(d)=0$，以概率 δ；

$Guess(d)=1$，以概率 $1-\delta$。

当 $Guess(d)=0$ 时，B 任选 $r\in Z_q^*$，并返回 $H_1(d)=r(xP)$；当 $Guess(d)=1$ 时，B 返回 $H_1(d)=rP$。

仿真：B 选择辅助参数 $t_r\in_R Z_q^*$，以 t_ry 作为系统主密钥(注意 B 并不知道 y 的值)，仿真 A 在 GetPair 游戏中的运行环境：

step 1 A 对节点 u_i($1\leqslant i\leqslant Q_E$)执行查询，$B$ 返回 ID_{ui} 为任意字符串。对于 u_i 的私钥，B 首先执行上述 H_1，若 $Guess(ID_{ui})=0$，B 报错退出；否则，由于此时 $Guess(ID_{ui})=1$，B 得到 $H_1(ID_{ui})=r_iP$，$r_i\in_R Z_q^*$，以 $S_{ui}=r_it_r(yP)$作为 u_i 的私钥返回给 A。由于

$$S_{ui}=(t_ry)r_iP=(t_ry)H_1(ID_{ui})$$

因此，以 A 的视角，仿真环境与真实环境无异。

step 2 A 选择未查询过的节点 u^*，B 为 u^* 分配 G_1 中点 $T_B=b(zP)$，其中 $b\in_R Z_q^*$。

step 3 B 选择 $a\in_R Z_q^*$ 以及 $ID_A\neq ID_{ui}$($1\leqslant i\leqslant Q_E$)。对于 A 的 $H_1(ID_A)$查询，若 $Guess(ID_A)=1$，B 报错并退出；否则，由于此时 $Guess(ID_A)=0$，B 返回 $H_1(ID_A)=r_A(xP)$，其中 $rA\in_R Z_q^*$。A 以 $T_A=a\,H_1(ID_A)$作为临时公钥第一部分发送给 u^*，B 以 T_B 作为 u^* 的临时公钥第一部分返回给 A。由于 a，b，r_A 均随机分布于 Z_q^*，以 A 的视角，仿真环境与真实环境无异。最后 A 输出 e_0。

若 A 赢得游戏，注意 t_ry 为此时的系统主密钥，则

$$e_0=\hat{e}(T_A, t_ryT_B)=\hat{e}(ar_AxP, t_rybzP)$$

B 可由 e_0 得到 BCDH 问题的解为

$$\hat{e}(P,P)^{xyz}=(e_0)^{(a\cdot b\cdot r_A\cdot t_r)^{-1}}\tag{12}$$

若 B 在整个过程中未报错退出，则以 A 的视角，除了一个可忽略的概率 $\varepsilon(k)$之外，仿真环境对于 A 来说与真实环境一致。设 E 为事件“B 未退出”，则

$$AdvGetPair_A=(AdvBCDH_B/\Pr[E])+\varepsilon(k)\tag{13}$$

在 GetPair step1 中，B 未退出的概率为 $(1-\delta)^{Q_E}$；在 GetPair step3 中，B 未退出的概率为 δ。则在整个过程中，B 未退出的概率为

$$\Pr[E]=(1-\delta)^{Q_E}\cdot\delta$$

使等式右边导数为 0 的 δ 值为使得 $\Pr[E]$取得极大的最优 δ 值，设为 δ_{opt}，易知 $\delta_{opt}=1/(1+Q_E)$。将 δ_{opt} 代入上式，可得

$$\Pr[E]=(1-1/(1+Q_E))^{Q_E}/(1+Q_E)$$

设 $n=1+Q_E$，因为

$$(1-1/(1+Q_E))^{Q_E}=(1-1/n)^{n-1}=((1+1/(n-1))^{n-1})^{-1}\geqslant e^{-1}$$

所以

$$\Pr[E]\geqslant 1/e\cdot(1+Q_E)\tag{14}$$

由式(13)、(14)，可得

$$AdvGetPair_A\leqslant e\cdot(1+Q_E)\cdot AdvBCDH_B+\varepsilon(k)$$

证毕。

引理 2 对任一 MIG 游戏的 PPT 对手 A，存在 GetPair 游戏的 PPT 对手 B，满足：

$$AdvMIG_A^{U=\emptyset}\leqslant Q_{H_2}\cdot AdvGetPair_B+\varepsilon(k)$$

证明：B 仿真 A 的运行环境，利用 A 在 MIG 游戏中的优势赢得 GetPair 游戏。B 按如下设定随机预言机 H_2 的查询输出：若 x 为新查询，B 生成随机字符串 y，返回 $H_2(x)=y$，并记录(x, y)；若 x 已被查询，B 从记录中检出 y 作为输出。

仿真 MIG：在 MIG step1 中，B 将 A 的查询传送到 GetPair step1 中，并将 B 在 GetPair 中的查询结果返回给 A，设 A 所查询节点集合为 U；

在 MIG step2 中，B 以自己在 GetPair 中选择的 u^* 作为 A 在 MIG 中选定的目标；

在 MIG step3 中，A 发送 T_A、W_A 给 u^*，B 返回 $T_B=bQ_{u^*}$、$W_B=bP$，A 输出字符串 K 作为认证密钥。设 $D=(\hat{e}(T_A, tT_B), bW_A)$，则当 $U=\emptyset$，且 $K=H_2(D)$时，A 赢得 MIG 游戏。设事件 T 为“$U=\emptyset$ 且 $K=H_2(D)$”，则

$$AdvMIG_A^{U=\emptyset}=\Pr[T] \quad (15)$$

设 T_1 为事件："A 曾经向 H_2 查询过 D"，则

$$\Pr[T]=\Pr[T|T_1]\Pr[T_1]+\Pr[T|\neg T_1]\Pr[\neg T_1] \quad (16)$$

若 A 未向 H_2 查询过 D，此时 $K=H_2(D)$ 的概率为一可忽略值 $\varepsilon(k)$，即

$$\Pr[T|\neg T_1]=\varepsilon(k) \quad (17)$$

若 A 曾经向 H_2 查询过 D，则 B 从查询记录中随机选择某一 (x,y)，以 x 的前 q 位作为 e_0，以 e_0 作为它在 GetPair step3 中的输出。假如 A 执行 Q_{H2} 次 H_2 查询，则 $x=D$ 的概率为 $1/Q_{H2}$，此时 B 赢得 GetPair 游戏，即

$$\Pr[T|T_1]=Q_{H_2}\cdot AdvGetPair_B \quad (18)$$

由式(15)—式(18)，可知

$$AdvMIG_A^{U=\emptyset}\leqslant Q_{H_2}\cdot AdvGetPair_B+\varepsilon(k)$$

证毕。

定理 2 的证明：由引理 1、2 可直接推出定理 2。

由于 BCDH 问题是困难的，$AdvBCDH_B$ 可忽略，则由定理 2 可得以下推论：

推论 1 对任意的 PPT 对手 A，$AdvMIG_A^{U=\emptyset}$ 可忽略。

根据推论 1 和定义 2，知本方案满足成员伪装安全性。

6 性能分析

通信复杂度：每个节点需要发送临时公钥和 MAC 结果给对方，临时公钥长度为 $2q$，MAC 输出长度为 n，则通信复杂度为 $2q+n$。

计算复杂度：每个节点需要进行 4 次 G_1 中点乘运算、一次双线性对运算，2 次 H_2 散列运算。

本方案在提供了较好的匿名性的同时也具有较低的开销。表 1 为本方案与其他基于对的非匿名认证方案的性能比较(散列运算由于计算开销低而不加考虑)，其中 Pair 表示双线性对运算，Mul 表示 G_1 中点乘运算，Plus 表示 G_1 中点加运算。从表中可以看出，同现有基于对的认证方案相比，本方案双线性对和 G_1 中点加运算次数最少，点乘运算次数与文献[10]和文献[11](方案 2)相同，但高于文献[9]和文献[11](方案 1)。考虑到对运算的开销远高于点乘运算开销[11]，而本方案对运算次数较少，因此本方案总的计算开销仍然低于文献[9]和文献[11](方案 1)。通信开销方面，本方案高于文献[9]和文献[11](方案 2)，但计算开销比它们要少一次对运算。

表 1 本文方案与其他基于对的认证方案的性能比较

方案	Pair	Mul	Plus	通信复杂度
文献[9]	2	3	0	q+n
文献[10]	1	4	1	2q+n
文献[11]方案 1	2	3	0	2q+n
文献[11]方案 2	2	4	0	q+n
本文方案	1	4	0	2q+n

本方案基于双线性对，对于双线性对在 MANET 中的应用问题，已有研究提出了很多优化算法以降低对运算开销。比如 Scott 等[12]的研究表明，利用优化算法和特定椭圆曲线，可在主频为 32MHz 的智能卡上以不高于 0.2s 的时间完成一次对运算。由于基于双线性对的密码算法具有许多传统加密机制所没有的优点，比如公钥分配简单、无需验证证书等[13]，此类算法在 MANET 中具有良好的应用前景。

结束语 MANET 中的匿名安全和可认证安全的结合一直是研究的难点与热点问题。基于双线性对的可追踪匿名认证方案，具备可认证密钥协商方案主要安全特性，并且解决了传统 MANET 匿名认证方案中存在的容侵性差和难以追踪恶意节点等问题。本方案在随机预言机模型下具有可证明的成员伪装安全性，在认证开销方面也优于以往基于对的认证方案。

参 考 文 献

[1] Ciszkowski T, Kotulski Z. ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks[C]//Proc of the 10th Domestic Conference on Applied Cryptography ENIGMA. Warsaw, Poland, May 2006

[2] Misra S, Xue Guoliang. SAS: A Simple Anonymity Scheme for Clustered Wireless Sensor Networks[C]//Proc of the Communications, 2006 IEEE International Conference. Volume 8, June 2006: 3414-3419

[3] Kim Dong Myung, Ho Byeong, Lee Sang Ho. Privacy for Low-power Sensor Node based on Alias in Ubiquitous Network[C]// Proc of the Software Engineering Research Management and Application. 2006, Fouth International Conf. Aug 2006: 144-149

[4] Wu Qianhong, Chen Xiaofeng, Wang Changjie. Shared-key Signature and its Application to Anonymous Authentication in Ad Hoc Group[J]. Lecture Notes in Computer Science, Information Security, 2004, 3225: 330-341

[5] Zhang Yanchao, Liu Wei, Lou Wenjing, et al. Anonymous Handshakes in Mobile Ad Hoc Networks[C]//Proc of Military Communications Conference 2004. IEEE, 2004: 1193-1199

[6] 王昌达，鞠时光. 无线组网技术中的安全问题[J]. 计算机科学，2006, 33(7): 121-126

[7] Balfanz D, Durfee G, Shankar N. Secret Handshakes from Pairing-based Key Agreements[C]//Proc of the 2003 IEEE Symposium on Security and Privacy(SP. 03). May 2003: 180-196

[8] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]//Proc of the CRYPTO 01. LNCS 2139. Springer-Verlag, 2001: 213-229

[9] Smart N P. An ID-based Authenticated Key Agreement Protocol Based on the Weil Pairing[J]. Electron. Lett, 2002, 38(13): 630-632

[10] Chen L, Kudla C. Identity based Authenticated Key Agreement Protocols from Pairing[C]//Proc of the 16th IEEE Security Foundations Workshop. IEEE Computer Society Press, 2003: 219-233

[11] Choie Young Ju, Jeong Eunkyung, Lee Eunjeong. Efficient Identity-based Authenticated Key Agreement Protocol from Pairings [J]. Applied Mathematics and Computation, 2005, 162: 179-188

[12] Scott M, Costigan N, Abdulwahab W. Implementing Cryptographic Pairings on Smartcards[J]. Lecture Notes in Computer Science, Cryptographic Hardware and Embedded Systems-CHES Volume, 2006, 4249: 134-147

[13] 田野，张玉军，李忠诚. 使用对技术的基于身份密码学研究综述[J]. 计算机研究与发展，2006, 43(10): 1810-1819