一种无线传感器网络匿名安全路由协议 *

章志明[a], 邓建刚[b], 邹成武[c], 余 敏[c]
(江西师范大学 a. 软件学院; b. 科技处; c. 计算机信息工程学院, 南昌 330022)

摘 要: 为了能在有限资源的无线传感器网络上进行安全的匿名通信,使用双线性函数的双线性对和异或运算提出了一种匿名安全路由协议,与目前现有的无线网络匿名通信方案相比,协议不仅能提供身份的机密性、位置隐私性和路由的匿名性,而且还满足前向和后向安全性,并且大大提高了系统的计算复杂度和带宽消耗,更适合无线传感器网络。

关键词: 无线传感器网络; 匿名路由; 节点身份; 双线性函数对
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)04-1477-04
doi:10.3969/j.issn.1001-3695.2010.04.076

Anonymous secure routing protocol for wireless sensor network

ZHANG Zhi-ming[a], DENG Jian-gang[b], ZOU Cheng-wu[c], YU min[c]
(*a. School of Software, b. Science & Technology Research Place, c. College of Computer Information Technology, Jiangxi Normal University, Nanchang* 330022, *China*)

Abstract: In order to support anonymous secure communications in resource restricted wireless sensor network, this paper proposed an anonymous secure wireless sensor network routing protocol based on bilinear pairings and different operation. Comparing with previous wireless network anonymous communications schemes, this protocol not only can provide identity confidentiality, location privacy and routing anonymity, but also can ensure the backward and forward security, and improve distinctly in computation and bandwidth consumption, this protocol is more suitable for the wireless sensor network.

Key words: wireless sensor network(WSN); anonymous routing; node-ID; bilinear pairings

0 引言

随着传感器技术与计算机等技术的发展,无线传感器网络(WSN)的应用已越来越广泛。在无线传感器网络上,传感器节点之间的彼此通信是借助于公开的媒介来完成的。由于无线传感器的存储、计算和通信资源等方面严格受限的特点,每个传感器节点的无线信号传输范围是有限的,任意两个节点之间的通信常常必须借助其他节点来完成,也就是说每个节点都可能是某次通信的中间节点,都需要为其他节点转发数据包。

不幸的是无线传感器网络上任何节点都有可能是恶意节点,它们会发起流量分析等攻击,从而得到网络上通信双方的信息,并通过分析节点间的通信获得节点的身份等信息,从而摧毁或捕获被标志的节点,最终使整个网络瘫痪。因此无线传感器网络节点之间的通信安全不仅涉及到通信内容的机密性、完整性、鉴别与可用等安全特性,还因为敌手通过流量分析与报文分组追踪会对通信节点本身及其所要完成的秘密使命造成威胁,所以系统需要提供匿名通信的支持,具有匿名通信能力。

关于传统网络匿名通信问题的研究,近年来已成为国内外研究的热点并取得了丰硕的研究成果,但由于无线传感器网络(WSN)的能量、存储和带宽都严格受限,传统的基于洋葱(onion)路由等匿名通信协议都无法在无线传感器网络中直接应用。对于如何保护无线传感器网络和无线移动自组(Ad hoc)网络的匿名通信,近年来已成为国内外研究的热点。2004 年,Zhu 等人[1]提出一个移动自组网络的匿名路由通信方案,该方案能提供源和目的端节点的匿名性,并且方案抗攻击性强,但这个方案要求每对通信节点需要预存共享密钥,并且不能满足前向和后向安全性。2006 年,Zhang 等人[2]提出一个 MASK 移动自组网络匿名路由协议,然而,Li 等人在文献[3]中指出他们的方案由于目的节点的身份在 RREP 包中泄露而不满足匿名性。Seys 等人[4]于 2006 年提出了一个 ARM 的匿名通信方案,但这个方案不仅需要预置共享会话密钥,而且需要预置共享假名列表,需要很大的存储空间。Lu 等人[5]在 2007 年提出了一个能提供从源节点到目的节点匿名性,并且具有可认证的密钥交换的匿名路由协议,但是在他们的方案中,当节点广播一个数据包时,它的身份会被其前驱和后继节点记录下来,这使得信息的传送具有可跟踪性。文献[6]利用假名机制提出了两个无线传感器网络匿名通信方案,方案一为每个节点提供了一个伪名集合,当节点需要发送信息时,从伪名集合中随机选取一个假名作为它的身份,另一个方案利用哈希函数产生节点的假名身份。这两个方案在假设节点之间共享的密钥不会被窃听者捕获的情况下,都能提供很好的安全匿

收稿日期: 2009-07-18; **修回日期**: 2009-08-28 **基金项目**: 国家"973"计划资助项目(2007CB316505, 2006CB303000); 国家科技型中小企业技术创新基金资助项目(07C26213600564); 江西省科技支撑计划资助项目

作者简介: 章志明(1978-),男,江西临川人,讲师,硕士,主要研究方向为网络信息安全、无线传感器网络(zzm_9650@163.com); 邓建刚(1977-),男,江西高安人,讲师,硕士,主要研究方向为信息安全、网络计算技术; 邹成武(1980-),男,江西临川人,助教,硕士,主要研究方向为网络信息安全、无线传感器网络; 余敏(1964-),女,江西南昌人,教授,博士,主要研究方向为网络信息安全、无线传感器网络.

名性,并且每个节点为了达到匿名通信目的,需要存储许多参数。文献[7]提出一种分层传感器网络安全匿名路由协议,协议使用簇密钥代替簇首与各个传感器间的两两共享密钥,减少簇首的密钥存储量,从而放宽异构层次化的要求,并允许存在内部攻击者,但该方案仍然是基于洋葱路由算法,大大增加了网络的计算负担。

为了保持较高安全匿名性的同时,提高系统的性能,本文使用双线性函数的双线性对和异或运算提出了一种安全有效的无线传感器网络匿名安全路由协议,协议采用对称密钥机制替代公钥签名机制,采用异或运算替代模指数运算,大大降低了通信所需的能耗。

1 双线性函数

1.1 双线性对

双线性对是基于身份的密码体制中非常重要的概念 ,双线性映射可以从椭圆曲线中的 Weil Pairing 或 Tate Pairing 构造得到,设 G_1 和 G_2 是阶为素数 q 的群。其中 G_1 为加法群,G_2 为乘法群,P 为 G_1 的生成元,设群 G_1 和 G_2 中离散对数问题是困难的。双线性对是指满足以下性质的一个映射 e: $G_1 \times G_1 \rightarrow G_2$。

a)双线性。对任意 $P,Q,R \in G_1$,有 $e(P,Q+R)=e(P,Q)e(P,R)$,$e(P+Q,R)=e(P,R)e(Q,R)$;对任意 $P,Q \in G_1$,$a,b \in Zq$,有 $e(aP,bQ)=e(P,Q)^{ab}=e(abP,Q)$。

b)非退化性。存在 $P,Q \in G_1$,满足 $e(P,Q) \neq 1$。

c)可计算性。对任意 $P,Q \in G_1$,存在有效的多项式时间算法计算 $e(P,Q)$。

1.2 双线性对难解问题

1)离散对数问题(discrete logarithm problem, DLP) 对任意 $P,Q \in G_1$,求解一个整数 n, 满足 $Q=nP$,称为离散对数问题,假设在群 G_1 和 G_2 中离散对数问题是困难的。

2)判定 Diffie-Hellman 问题(decision Diffie-Hellman problem DDHP) 对任意 $P,a,b,c \in G_1$,给定(P, aP, bP, cP),决定 $c = ab \bmod q$ 是否成立。

3)计算 Diffie-Hellman 问题(computational Diffie-Hellman problem CDHP) 对任意 $P,a,b \in G_1$,给定(P, aP, bP),计算 abP。

如果在群 G 中 DDHP 是易解的而 CDHP 是难解的,那么群 G 称为 Gap Diffie-Hellman 群。因为可以通过 $e(P,cP)=e(aP,bP)$来决定 DDHP, 但没有有效的算法来计算 abP,所以 G_1 是一个 Gap Diffie-Hellman 群。

2 基于双线性对的无线传感器网络匿名安全路由协议

2.1 系统网络模型

系统由 N 个传感器节点和一个基站组成。基站一般作为无线传感器网络的控制中心,而且处理能力、内存及无线发射功率都不受限制。系统为每个节点分配一个身份随机数 ID_i 作为惟一身份标志。节点之间的无线信道是对称和双向的,也就是说,如果节点 i 是在节点 j 的通信范围内,那么节点 j 也是在节点 i 的通信范围内。敌手具有无限窃听能力,但只具有有限的计算能力与捕捉节点的能力。当源节点需要与目的节点进行安全匿名通信时,需要经过路由请求、路由回复和数据传送三个阶段。

2.2 符号说明

q:一个大素数

G_1:大素数 q 的加法群

G_2:大素数 q 的乘法群

e:满足 $G_1 \times G_1 \rightarrow G_2$ 的一个双线性映射

Q_i: 表示节点 i 的公钥

S_i:表示节点 i 的私钥

BS:表示基站

ID_i:节点 i 的惟一身份标志

ID_{BS}:表示基站的惟一身份标志

$h(\cdot)$:一个强密码 hash 函数,该函数把节点 ID 映射到 G_1 中的一个元素

$\|$:表示串接

K_{ij}:表示节点 i 与 j 之间的共享密钥

$E_{Ki,j}(m)$:表示用密钥 K_{ij} 加密信息 m

SK_{ij}:表示节点 i 与 j 之间共享的一次会话密钥

$\oplus$:表示异或运算

2.3 系统初始化

系统初始化步骤如下:

a)BS 选择系统参数为 $q,G_1,G_2,e:G_1 \times G_1 \rightarrow G_2$ 以及一个强密码 hash 函数 $h(\cdot):\{0,1\} \rightarrow G_1$。

b)产生一个系统私公密钥对(S,Sq),S 为系统私钥,Sq 为系统公钥。

c)为每个节点 i 选择一个身份随机数 ID_i 并计算其公钥为 $Q_i=H(ID_i)$,私钥为 $S_i=SQ_i$。

2.4 路由请求阶段

当源节点 i 需要与目的节点 j 进行安全通信时,源节点 i 首先构造路由请求包, 然后进行广播。具体步骤如下:

a)源节点 i 选取两个随机数 R_1 和 R_2,并计算 R_1Q_i, $K_{ij}=H(e(S_i, Q_j))$,$H(ID_i) \oplus H(e(Sq, Q_j))$。

b)产生路由请求 M,具体格式为 $M=[\text{RREQ\_id}, R_1Q_i, H(ID_i) \oplus H(e(Sq, Q_j)), E_{Ki,j}(R_2 \| H(ID_j) \| T_i)]$。其中:RREQ_id 表示本次路由请求包的惟一标志; R_1Q_i 表示节点在路由回复阶段判断是否处理过此路由请求包的标志;$H(ID_i) \oplus H(e(Sq, Q_j))$ 表示用源节点 i 的身份 ID 与 $H(e(Sq, Q_j))$ 作异或运算;$E_{Ki,j}(R_2 \| H(ID_j) \| T_i)$ 表示用源节点 i 和目的节点 j 之间的共享密钥加密随机数 R_2、目的节点身份 ID 和一个时间戳。把路由请求包广播给所有通信范围内的邻居节点。

c)当中间节点收到此路由请求包时,首先检查节点路由表中是否存在路由标记 RREQ_id。若存在,则表示已收到过此请求包,并丢弃此包;否则,节点把 R_1Q_i 存入路由表中,并计算 $H(e(q, S_j))$。因为 $H(e(q, S_j)) = H(e(q, SQ_j)) = H(e(q, Q_j)^S) = H(e(Sq, Q_j))$,所以通过计算 $H(ID_i) \oplus H(e(Sq, Q_j)) \oplus H(e(q, S_j))$ 可得到源节点的身份 $H(ID_i)$,然后计算与源节点共享的密钥 $K_{ji}=H(e(H(ID_i), S_j)) = H(e(H(ID_i), SQ_j)) = H(e(H(ID_i), Q_j)^S = H(e(SH(ID_i), Q_j)) = H(e(S_i, Q_j)) = K_{ij}$,用 K_{ij} 解密 $E_{Ki,j}(R_2 \| H(ID_j) \| T_i)$,若能正确解密出信息,并且时间戳在一定的合理范围内,则表示自己就是目的节点,并开始执行路由回复操作;否则,自己是中间路由节点,需把路由请求包继续广播给通信范围内的邻居节点。

d)返回到 c)重新执行。

2.5　路由回复阶段

当目的节点 j 收到路由请求包,并确定自己就是目的节点后,知道节点 i 需要与自己进行安全通信,节点 j 则构造路由回复包, 然后广播出去。具体步骤如下:

a)目的节点 j 选取一个随机数 RRER_id 作为路由回复包的惟一标志,通过解密得到随机数 R_2,并计算与源节点 i 此次通信的会话密钥 $SK_{ji}=H(e(R_1Q_i,R_2S_j))$。

b)广播路由回复包 $M'=[\text{RRER\_id},R_1Q_i,R_2Q_j]$ 给通信范围内的邻居节点。其中:RRER_id 表示回复包的惟一标志,R_1Q_i 表示路由请求包是由源节点 i 发出的;R_2Q_j 表示路由回复包是由目的节点 j 发出的。

c)当节点收到路由回复包后,首先检查节点路由表中是否存在路由标记 RRER_id。若存在,则表示已收到过此回复包,并丢弃此包;否则,检查节点路由表中是否存在 R_1Q_i,若存在,表示它不是源节点就是此路由的中间节点。如果它是源节点,可计算出与目的节点共享的此次通信的会话密钥 $SK_{ij}=H(e(R_1S_i,R_2Q_j))=H(e(R_1SQ_i,R_2Q_j))=H(e(R_1Q_i,R_2Q_j)^S)=H(e(R_1Q_i,R_2SQ_j))=H(e(R_1Q_i,R_2S_j))=SK_{ji}$,如果是中间路由节点,继续把路由回复包广播给通信范围内的邻居节点。

d)返回到 c)重新执行。

2.6　数据传送阶段

当源节点 i 和目的节点 j 通过路由请求和路由回复阶段成功建立起通信路径后,节点之间可通过下面步骤进行数据传送:

a)源节点 i 使用会话密钥 SK_{ij} 产生数据包 $M=[E_{SK_{i,j}}(\text{data}\|T_{i+1}),R_1Q_i]$ 并广播出去。其中:$E_{SK_{i,j}}(\text{data}\|T_{i+1})$ 表示用源节点 i 和目的节点 j 此次会话密钥加密要传送的数据和一个时间戳,R_1Q_i 表示此次通信路由路径的标志。

b)节点收到此数据包,首先检查节点路由表中是否存在 R_1Q_i,若存在,表示它不是目的节点就是此路由的中间节点。如果它是目的节点,可使用与源节点共享的此次通信的会话密钥 SK_{ji} 解密出源节点传送的数据 data;如果是中间路由节点,继续把路由数据包广播给通信范围内的邻居节点。

c)返回到 b)重新执行。

3　路由协议性能分析

3.1　匿名性分析

根据文献[7],匿名路由要达到如下目标:

a)身份机密性。任何中间路由节点都不知道通信的发送方(源)与接收方(目的)的真实身份,并且发送方和接收方也不知道中间路由节点的真实身份。

b)位置机密性。发送方与接收方的位置不会被其他节点知道,路由节点不能得到源与目的节点之间的距离,即中间转发节点不可判断发送方和接收方节点的跳数。

c)路由的匿名性。不能通过追踪发送信息包来发现发送方和接收方的节点,即第三方难以推断源与目的之间的通信传输模式。

下面分析本文方案的匿名性。

本方案源节点的真实身份是用源节点 i 的身份 ID 作哈希映射后与 $H(e(Sq,Q_j))$ 作异或运算进行隐藏,目的节点的真实身份是用源节点 i 和目的节点 j 之间的共享密钥加密后进行隐藏,任何中间路由节点都不知道通信的发送方(源)与接收方(目的)的真实身份,并且发送方和接收方也不知道中间路由节点的真实身份,从而保证了路由节点的身份机密性。

当中间路由节点取得源节点 i 发送的路由信息包 $M=[\text{RREQ\_id},R_1Q_i,H(\text{ID}_i)\oplus H(e(Sq,Q_j)),E_{Ki,j}(R_2\|H(\text{ID}_j)\|T_i)]$,由于不知道目的节点 j 的私钥以及源节点 i 与目的节点之间共享的密钥 K_{ij},中间路由节点不能得到源节点和目的节点的任何信息,从而保证源节点和目的节点的位置机密性,即中间转发节点不可判断到发送方和接收方节点的跳数。

只有目的节点 j 才能通过计算 $H(\text{ID}_i)\oplus H(e(Sq,Q_j))\oplus H(e(q,S_j))$ 得到源节点的身份 $H(\text{ID}_i)$,然后计算与源节点共享的密钥 $K_{ji}=H(e(H(\text{ID}_i),S_j))=H(e(H(\text{ID}_i),SQ_j))=H(e(H(\text{ID}_i),Q_j))^S=H(e(SH(\text{ID}_i),Q_j))=H(e(S_i,Q_j))=K_{ij}$,解密得到正确的路由信息,其他任何节点都不能得到正确路由信息,从而保证了路由的匿名性。不能通过追踪发送信息包来发现发送方和接收方的节点,即第三方难以推断源与目的节点之间的通信传输模式。

3.2　安全性分析

1)抗中间人攻击　当窃听者获得路由信息包 $M=[\text{RREQ\_id},R_1Q_i,H(\text{ID}_i)\oplus H(e(Sq,Q_j)),E_{Ki,j}(R_2\|H(\text{ID}_j)\|T_i)]$ 时,由于不知道目的节点 j 的私钥以及源节点 i 与目的节点之间共享的密钥 K_{ij},不能解密信息 $E_{Ki,j}(R_2\|H(\text{ID}_j)\|T_i)$ 得到 R_2,从而不能得到此次通信的会话密钥 $SK_{ij}=H(e(R_1S_i,R_2Q_j))=H(e(R_1SQ_i,R_2Q_j))=H(e(R_1Q_i,R_2Q_j)^S)=H(e(R_1Q_i,R_2SQ_j))=H(e(R_1Q_i,R_2S_j))=SK_{ji}$,所以本方案能抵抗中间人攻击。

2)后向安全性和前向安全性　后向安全性是指当节点 i 与节点 j 此次通信的会话密钥 SK_{ij} 被泄密,它们以前使用的会话密钥 SK_{ij}' 仍然是安全的。前向安全性是指当节点 i 与节点 j 以前的通信会话密钥 SK_{ij} 被泄密,它们以后使用的会话密钥 SK_{ij}' 仍然是安全的。在本方案中,节点之间的通信密钥 $SK_{ij}=H(e(R_1S_i,R_2Q_j))=H(e(R_1SQ_i,R_2Q_j))=H(e(R_1Q_i,R_2Q_j)^S)=H(e(R_1Q_i,R_2SQ_j))=H(e(R_1Q_i,R_2S_j))=SK_{ji}$ 的计算是依赖于两个随机数 R_1、R_2 和两个节点的公私密钥,每次产生的随机数 R_1、R_2 保证了每次通信的会话密钥是相互独立的,某次会话密钥的泄密不会影响其他会话密钥的使用,所以本方案具有后向和前向安全性。

3.3　复杂度分析

本节将从计算复杂度方面与其他方案进行分析比较。分析比较中使用的符号如表 1 所示。假设在源节点和目的节点之间有 n 个中间路由节点。

表 1　分析比较中所使用的符号及含义

符号	含义
$\oplus$	表示异或运算
BP	表示双线性对运算
exp	表示计算临时公钥所需要进行的模指数运算
asym	表示用非对称密钥进行加/解密运算
sym	表示用对称密钥进行加/解密运算
H	表示进行哈希运算
n	表示所有中间路由节点数
cmp	比较次数
crte	创建实体表的次数
mul	在 G_1 上的一个点乘操作

在本方案中,每个双线性对运算都能在协议运行之前进行运算,所以,在本文方案中不考虑双线性对运算。本方案与其他方案计算开销如表 2 所示。当一个源节点想传送一个请求

包给目的节点,它需要进行一次8 运算、一次 mul 操作(计算 R_1Q_i)、一次 sym 运算,对于其他 n 个中间节点,每个节点需要进行一次8 运算、一次 sym 运算,目的节点需要进行一次8 运算、一次 sym 运算,在路由请求阶段总计需要($n+2$)次8 运算、($n+2$)次 sym 操作和一次 mul 操作。在路由回复阶段,目的节点需要进行一次 mul 操作(计算 R_2Q_j)、一次 BP 运算(计算会话密钥),源节点需要进行一次 BP 运算(计算会话密钥),其他 n 个中间节点只需要进行包的转发、丢弃等操作,所以在路由回复阶段总计需要两次 BP 和一次 mul 操作。在文献[1]中,为了传送一个请求包,源节点和目的节点都需要进行一次 H 操作、一次 asym 和一次 exp 运算,其他每个中间节点需要一次 asym 运算,在路由回复阶段,总共需要($n+2$)次 cmp、($n+1$)次 asym 和($3\times n+5$)次 sym 运算。在文献[2]中,源节点、目的节点和所有 n 个中间节点在路由请求阶段总共需要($n+2$)次 crte 操作,在路由回复阶段源节点、目的节点和所有 n 个中间节点在路由请求阶段总共需要($n+2$)次 crte 和($n+2$)次 sym 操作。在文献[4]中,在路由请求阶段,源节点需要执行一次 asym 操作、两次 sym 操作和一次 exp 操作来计算自己的公钥,所有 n 个中间节点需要执行 n 次(sym + asym)操作,目的节点需要执行两次 sym 和 $n+1$ 次 asym 操作,在路由回复阶段,源节点需要执行两次 sym 操作、一次 cmp 操作,所有中间节点需要执行 n 次(sym + cmp)操作,目的节点需要执行 $n+1$ 次 asym 和四次 sym 操作。在文献[5]的路由请求阶段,源节点需要进行一次(asym + H + exp)操作,每个中间节点需要进行一次 asym 运算,目的节点需要进行一次(asym + H + cmp)操作,在路由回复阶段,目的节点需要进行一次 asym、一次 H 和两次 exp 操作,每个中间节点需要进行两次 asym 运算,源节点需要进行两次 asym、一次(H + exp + cmp)次操作。从表 2 可知,本方案只需进行一些基本可以忽略不计的异或运算和对称加密运算,而其他方案大多都使用了昂贵的模指数运算和非对称加密运算,所以本方案具有较好的计算复杂性。

表 2 本方案与其他方案计算开销比较

阶段	本方案	ASR[1]	MASK[2]	ARM[4]	SARPAKE[5]
路由请求	8 :$n+2$ sym:$n+2$ mul:1	asym: $n+2$ exp:2 H:2	crte: $n+2$	asym: $2n+2$ sys:$n+4$ exp:1	asym:$n+2$ exp:1 exp: 1 H: 2
路由回复	BP:2 mul:1	asym:$n+1$ sym:$3n+5$ cmp:$n+2$	sym:$n+2$ crte: $n+2$	asym:$n+1$ sym:$n+6$ cmp:$n+1$	asym:$2n+3$ exp:3 cmp:1 H:2
总计算开销	8 :$n+2$ sym:$n+2$ mul:2 BP: 2	asym: $2n+3$ sym:$3n+5$ cmp:$n+2$ exp:2 H:2	sym:$n+2$ crte:$2n+4$	asym:$3n+3$ sym:$2n+10$ cmp:$n+1$ exp:1	asym:$3n+5$ exp:4 cmp:2 H: 4

3.4 带宽消耗分析

低带宽消耗能使整个网络电能消耗降低,数据传输速度加快,从而有效提高网络寿命。假设对称密码系统使用 AES-192,非对称密码系统使用 RSA-1024。对于 RSA 和 Elgamal 密码系统,密钥长度一般是 1 024 bit,基于椭圆曲线密码体制的计算性能要优于 RSA 和 Elgamal 密码系统,它只需要长度为 160 bit 的密钥就能提供等强度的安全性。本方案的双线性对是基于椭圆曲线密码体制,在路由请求阶段传送的信息为 $M=[\text{RREQ\_id}, R_1Q_i, H(\text{ID}_i)8\ H(e(Sq, Q_j)), E_{Ki,j}(R_2 \| H(\text{ID}_j) \| T_i)]$,需要传送 160 ×4 bit 的信息量,路由回复阶段传送的信息为 $M'=[\text{RRER\_id}, R_1Q_i, R_2Q_j]$,需要传送 160 ×3 bit 的信息量。在文献[1]中,在路由请求阶段总共需要传送 192 × 2 + 1024 + 128 bit 信息量,在路由回复阶段总共需要传送 1024 + 192 bit信息量。在文献[2]中,匿名路由发现阶段需要传送 128 ×2 bit 的信息量,在回复阶段需要传送 192 + 128 bit 信息量。在文献[4]中,路由发现阶段需要的带宽为 2 × (128 + 160) + 192 + 1024 bit,在回复阶段需要的带宽为 192 × 2 bit。在文献[5]中,路由请求阶段需要的带宽为 1 024 bit,在路由回复阶段需要的带宽为 1024 ×2 bit。表 3 为本方案与其他方案带宽开销的比较,从表中可知,只有文献[2]中的方案带宽开销比本文的方案小,其他方案的带宽消耗都比本方案要大,所以本方案具有较低的带宽消耗。

表 3 本方案与其他方案带宽开销比较

阶段	本方案	ASR[1]	MASK[2]	ARM[4]	SARPAKE[5]
路由请求	160 ×4 bit	192 ×2 + 1024 + 128 ×2 bit	128 ×2 bit	2 ×(128 + 160) + 19 +2 +1024 bit	1 024 bit
路由回复	160 ×3 bit	1024 + 192 bit	192 + 128 bit	192 ×2 bit	1024 ×2 bit
总带宽开销	1 120 bit	2 752 bit	576 bit	2 176 bit	3 072 bit

4 结束语

本文使用双线性函数的双线性对提出了一种无线传感器网络匿名安全路由协议,协议不仅能提供身份的机密性、位置隐私性和路由的匿名性,而且还具有后向安全性和前向安全性,协议采用对称密钥机制替代公钥签名机制,采用异或运算替代模指数运算,大大提高了系统的计算复杂度和带宽消耗,更适合无线传感器网络。笔者的下一步工作将进一步在网络仿真平台上对路由建立时间与数据包发送迟延进行仿真,以全面评价该机制的性能。

参考文献:

[1] ZHU Bo, WAN Z, KANKANHALLI M S, *et al*. Anonymous secure routing in mobile Ad hoc networks[C]//Proc of the 29th Annual IEEE Conference on Local Computer Networks (LCN2004). New York: ACM Press, 2004: 102-108.

[2] ZHANG Yan-chao, MEMBER S, LIU Wei, *et al*. Anonymous on-demand routing in mobile Ad hoc networks[J]. IEEE Trans on Wireless Communications, 2006, 5(9):2376-2385.

[3] LI Song, EPHREMIDES A. Anonymous routing: a cross-layer coupling between application and network layer[C]//Proc of the 40th Annual Conference on Information Sciences and Systems (CISS 2006). Princeton, NJ:ACM Press, 2006:783-788.

[4] SEYS S, PRENEEL B. An anonymous routing measure for mobile Ad hoc networks[C]//Proc of the 20th International Conference on Advanced Information Networking and Applications (AINA 2006). New York: ACM Press, 2006:133-137.

[5] LU Rong-xing, CAO Zhen-fu, WANG Li-cheng, *et al*. A secure anonymous routing protocol with authenticated key exchange for Ad hoc networks[J]. Computer Standards & Interfaces, 2007,29(5):512-527.

[6] MISRA S, XUE G. Efficient anonymity schemes for clustered wireless sensor networks[J]. International Journal of Sensor Networks, 2006, 1(1/2):50-63.

[7] 张炜承, 章洋, 胡晓蕙. 一种分层传感器网络安全协议的分析与改进[J]. 计算机仿真, 2008, 25(5):154-158.