软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(Suppl.(1)):49−57

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种异构传感网认证密钥协商方案*

王九如[1,2], 丁林花[1,2], 刘 丽[1,2], 王海峰[1,2]

[1](临沂大学 信息学院,山东 临沂 276000)

[2](山东省网络环境智能计算技术重点实验室(济南大学),山东 济南 250022)

通讯作者: 王九如, E-mail: wangjiuru@lyu.edu.cn

摘 要: 把集合论思想引入异构传感网认证密钥方案设计中,提出一种基于双线性对动态累加器的异构传感网认证密钥协商方案.已往基于经典随机图等理论的安全方案主要实现了节点间密钥协商,使身份认证和密钥协商割裂开来;新方案则从集合论的角度把异构传感网认证密钥协商转化为集合元素关系认证,实现了身份认证和密钥协商的有效融合.方案包括异构传感网身份认证、密钥协商和广播认证这3部分.节点通过交换ID与证人信息相互验证身份合法性;合法节点协商生成共享密钥;利用广播消息动态增加/删除节点,更新节点证人信息.实验分析表明,该方案不但实现了身份认证、密钥协商和广播认证的有效融合,而且具有良好的安全性、扩展性和网络结构变化的自适应性,适用于节点性能和安全性需求较高的场景中.

关键词: 认证密钥协商;动态累加器;双线性对;异构传感网

中文引用格式: 王九如,丁林花,刘丽,王海峰.一种异构传感网认证密钥协商方案.软件学报,2015,26(Suppl.(1)):49−57. http://www.jos.org.cn/1000-9825/15006.htm

英文引用格式: Wang JR, Ding LH, Liu L, Wang HF. Authenticated key agreement scheme for heterogeneous sensor networks. Ruan Jian Xue Bao/Journal of Software, 2015,26(Suppl.(1)):49−57 (in Chinese). http://www.jos.org.cn/1000-9825/15006.htm

Authenticated Key Agreement Scheme for Heterogeneous Sensor Networks

WANG Jiu-Ru[1,2], DING Lin-Hua[1,2], LIU Li[1,2], WANG Hai-Feng[1,2]

[1](School of Informatics, Linyi University, Linyi 276000, China)

[2](Provincial Key Laboratory for Network Based Intelligent Computing (University of Ji'nan), Ji'nan, 250022, China)

Abstract: In this paper, set theory is introduced to the design of authenticated key agreement scheme for heterogeneous sensor networks, and a scheme based on bilinear dynamic accumulator is proposed. The previous schemes based on classical random graph and others mainly achieve key agreement between nodes, and separate authentication and key agreement. From the perspective of set theory, this work transforms authenticated key agreement into set element relationship certification, and integrates identity authentication and key agreement. It includes identity authentication, key agreement, and broadcast authentication. Sensors verify the identity of each other by exchanging ID and witnesses. Legitimate nodes generate a shared key. Broadcast messages are used to dynamically add/delete nodes, and update witness. Experimental results show that the new scheme not only achieves effective integration of authentication, key agreement and broadcast certification; but also has better security, scalability, and adaptive changes in the network structure. It is suitable for higher node performance and security requirements scenarios.

Key words: authenticated key agreement; dynamic accumulator; bilinear pairing; heterogeneous sensor network

近年来异构传感网(heterogeneous sensor network,简称 HSN)安全方案研究已取得许多显著成果[1,2].从所依

* 基金项目: 国家自然科学基金(61170241); 山东省自然科学基金(ZR2014FL012); 山东省自主创新及成果转化重大专项(2014ZZCX02702); 山东省科技发展计划(2013GGB01332); 山东省网络环境智能计算技术重点实验室开放基金; 临沂大学 2014 年博士科研启动基金(LYDX2014BS006)

收稿时间: 2015-04-15; 定稿时间: 2015-07-20

据的理论基础来看,主要分为以下几类:(1) 以随机图理论为基础,把节点映射为随机图中顶点,部署前每个节点预置一定数量密钥,部署后协商生成通信密钥,网络运行过程中不考虑密钥更新和撤销问题.典型方案有:以 E-G 方案[3]为基础后续发展起来的基于部署知识的密钥管理方案[4]、路由驱动的密钥管理方案[5]、基于时间部署的密钥管理方案[6]等.(2) 以组合设计理论为基础,把节点看作集合中的元素,利用元素排列组合关系及时排除受损节点,使网络处于动态安全中.典型方案有:以 EBS 方案[7]为基础后续提出的了动态密钥管理方法[8]和优化改进方案[9,10]等.(3) 以单项哈希函数为基础,实现用户身份合法性认证.典型方案有:轻量级用户认证方案[11]以及优化改进方案[12].以上方案主要有以下 3 个特点:(1) 无论基于随机图理论还是组合设计理论,均是节点间偏序关系的描述,未深入研究节点间身份认证问题.(2) 相对于基于随机图理论而言,以组合设计理论为基础的动态密钥管理方案因"共谋"问题难以解决而发展缓慢.(3) 已取得的研究成果主要集中在通信密钥管理方法,认证密钥方面研究相对较少,把两者结合起来研究更显薄弱[13].

认证密钥协商方案由认证密钥和通信密钥两部分组成,认证密钥解决节点身份认证问题,通信密钥解决通信安全问题.在信息监测、医疗卫生、交通管理等安全性要求较高的应用中,作为各种安全机制的基础,认证密钥协商是关系到 HSNs 能否走向实用的关键性问题,必须首先解决.本文以集合论为基础,利用双线性对设计一种异构传感网认证密钥协商方案.主要贡献在于:(1) 把集合论思想引入异构传感网认证密钥协商中,把节点间认证密钥协商问题转化为集合中元素间身份认证和密钥问题,为异构传感网认证密钥管理方案研究提供新的研究思路;(2) 把双线性对和动态累加器技术相结合,构造基于双线性对的动态累加器,为双线性对和动态累加器的应用提供参考.(3) 方案实现了身份认证和密钥协商的有效融合,运行中可以随时部署新节点、排除受损节点,使网络处于动态安全中,有效抵抗仿冒攻击.

本文第 1 节介绍相关理论模型,并构建基于双线对的动态累加器.第 2 节阐述密钥管理方案.第 3 节从安全性、可扩展性等方面分析方案性能.第 4 节总结全文提出下一步研究工作.

1 理论模型

本节首先阐述全文的理论基础,从集合论角度分析异构传感网认证密钥协商问题的转化;再进一步介绍与集合论相适应的动态累加器及其性质;最后基于双线性对构造一个动态累加器.

1.1 问题转化

定义 1(集合). 具有某种属性的对象的总体(通常用大写字母表示,如 A,B 等),这些对象称为其元素或点(通常用小写字母表示,如 x,y 等).

集合的表示:$\{x\in A|P(x)\}$,表示集合 A 中满足条件 $P(x)$的 x 的集合.集合中元素具有如下性质:

① 确定性:$x\in A$ 或 $x\notin A$,必居其一;

② 互异性:$x_1\in A$ 且 $x_2\in A$,则 $x_1\neq x_2$;

③ 无序性:集合中元素是"平等"的,无先后次序.

定义 2(偏序关系). 设 A 是一个非空集,元素 $a,b\in A$,R 是 A 上的一个关系,$\langle a,b\rangle\in R$,若关系 R 是自反的、反对称的和传递的,则称 R 是集合 A 上的偏序关系,用 $a\preccurlyeq b$ 表示$\langle a,b\rangle\in R$.

一个典型的异构传感网如图 1 所示.网络由 1 个 Sink 节点、m 个 H-sensor 节点和 n 个 L-sensor 节点组成($m<<n$).Sink 节点安全可信;H-sensor 通常配备防篡改器件;L-sensor 不配备防篡改器件.每个 L-sensor 和 H-sensor 拥有唯一 ID 标示,并均由电池供电.L-sensor 和 H-sensor 部署位置相对静止,借助定位算法可以确定相对位置.部署完成后,L-sensor 围绕性能较优的 H-sensor 成簇,被选中的 H-sensor 称为簇头(cluster-heads,简称 CH).网络中 Sink 节点通信范围覆盖整个监测区域,H-sensor 通信范围可以覆盖自己所在的簇,L-sensor 只能与邻居节点通信.L-sensor 通过多跳与簇头通信,同样簇头经过多跳到达 Sink.Sink,H-sensor 和 L-sensor 形成层次式拓扑结构.

从逻辑上看,如果以 V 表示节点集合(包括 Sink,H-sensor 和 L-sensor),以 R 表示合法节点间链路关系,则异构传感网可表示为

$HSN=(V,R)$;

$V=\{S, H_1,\ldots,H_m, L_{11},\ldots,L_{mn}, m\geqslant 1, n\geqslant m\}$, $R=\{R_1,R_2,R_3\}$;

$R_1=\{\langle S,H_i\rangle|m\geqslant i\geqslant 1\}$, $R_2=\{\langle H_i,L_{ij}\rangle|m\geqslant i\geqslant 1,n\geqslant j\geqslant 1\}$, $R_3=\{L_{ij}\preccurlyeq L_{it}|m\geqslant i\geqslant 1,n\geqslant t\geqslant 1\}$.

因此,从集合论的角度,以数据为中心的异构认证密钥协商问题可以分解为如下 3 个问题:(1) 元素与集合间身份合法性问题,即身份认证问题;(2) 元素与元素间偏序关系问题,即密钥协商问题;(3) 元素与集合间消息合法性问题,即广播认证问题.

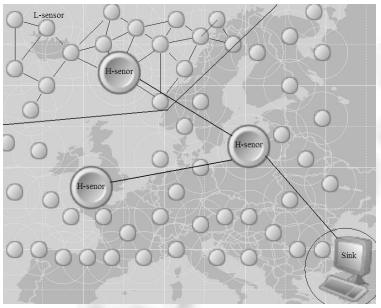


Fig.1 Heterogeneous sensor networks model

图1 异构传感网模型

1.2 动态累加器及性质

Camenisch 和 Lysyanskaya 改进的动态累加器技术[14]恰是解决以上问题的有效办法.

定义 3(动态单向累加器(dynamic accumulator)). 将集合中所有累加元聚合为一个累加值,为每个累加元提供一个证人信息以证明该元素参与了聚合运算,并以与集合大小无关的代价增加/删除累加元.其性质如下:

① 可生成性:存在概率算法 G,以安全参数 1^l 为输入,输出函数 $f: X\times Y\to Y, x\in X, y\in Y$ 和辅助信息 t_f.

② 可计算性:存在一个多项式算法 P,对给定的整数 $l, \forall x\in X, \forall y\in Y, f(y,x)$ 在多项式时间内 $P(l,|x|,|y|)$ 是可计算的.

③ 准交换性:对 $\forall x_1,x_2\in X, y\in Y$ 有 $f(f(y,x_1),x_2)=f(f(y,x_2),x_1)$.

④ 动态增加:设 $v=f(y,X), X'=X\cup\{x'\}$, 则 $f(v,x')=f(y,X')$.

⑤ 动态删除:存在算法 D 和 W,对于 $v=f(y,X), x,x'\in X, f(w,x)=v$, 有 $D(t_f,v,y')=v', W(f,v,v',x,x',w)=w'$, 其中 $, v'=f(y,X\setminus\{x'\})=f(w',x)$.

1.3 基于双线性对的动态累加器

本文以文献[15,16]为基础构建基于双线对的动态累加器:

① 可生成性:以安全参数 1^l 为 BPG(bilinear pairing instance generator)输入,生成元组 $t=(p,\mathbb{G}_1,\mathbb{G}_M,e,P)$. $\mathbb{G}_1$ 是阶为 p 的加法循环群,其生成元为 P; $\mathbb{G}_M$ 是阶为 p 的乘法循环群;e 是满足双线性、非退化性和可计算性的双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_M$; 依据网络规模 $q(q>>(m+n+1))$选择辅助信息为 $a_f=s\in_R\mathbb{Z}_p^*$. 定义函数 $(f,g)\in_R F_l$ 如下: $f:\mathbb{Z}_p\times\mathbb{Z}_p\to\mathbb{Z}_p$, $g:\mathbb{Z}_p\to\mathbb{G}_1$, 即, $f:(u,x)\to(x+s)u, g:u\to uP$. 其中,累加元定义域为 $\mathbb{Z}_p\setminus\{-s\}$.

② 可计算性:对 $u\in\mathbb{Z}_p$, $X=\{x_1,\ldots,x_k\}\subset\mathbb{Z}_p\setminus\{-s\}, k\leqslant q$,函数 $g(f(u,X))=\prod_{i=1}^k(x_i+s)uP$, 在多项式时间 l 内是可计算的.

③ 准交换性: $g(f(f(u,x_1),x_2))=g(f(u,\{x_1,x_2\}))=(x_1+s)(x_2+s)uP$.

④ 动态增加:假设 $V=g(f(u,X)), x\in X, g(f(g^{-1}(W),x))=V$, V 是累加和,W 是 x 的证人信息,新增元素 $x'\notin X$, 则新累加和 $V'=g(f(u,X\cup\{x'\}))=(x'+s)V$. x 元素对应的证人信息 W 更新为 W', 且满足 $g(f(g^{-1}(W'),x))=V'$, W'可做如下计算,求得 $W'=V+(x'-x)W$.

⑤ 动态删除:假设 $V=g(f(u,X)), x,x'\in X, x\neq x, g(f(g^{-1}(W),x))=V$, 删除元素 x', 则新的累加和为 $V'=g(f(u,X\setminus\{x'\}))=1/(x'+s)V$, x 的证人信息 W', 且满足 $g(f(g^{-1}(W'),x))=V'$, W' 可做如下计算,求得 $W'=(1/(x'-x))(W-V')$.

2 认证密钥协商方案

如图 1 所示,HSN 路由包含两个部分:1) 簇内路由,L-sensor 向 CH 发送数据;2) 簇间路由,CH 融合 L-sensor 发送的数据,经 CH 骨干网络发送至 Sink.因为 CH 是高能节点,CH 间路由相对简单,同样地,CH 间的认证密钥协商也相对容易.比如,为每个 H-sensor 预置一个由防篡改器件保护的特殊密钥 K_H,部署后 CH 利用 K_H 实现安全通信.本文主要研究 L-sensor 之间的认证密钥协商问题,考虑到簇内建立路由结构之后,每个 L-sensor 只需与其邻居节点建立共享密钥,也就是父节点和孩子节点,假设同簇内的 L-sensor 和 H-sensor 拥有邻居节点列表.

2.1 密钥预分配

假设网络存在可信第三方(比如由 Sink 担任),为网络规模为 q 的异构传感网配置密钥原材料.可信第三方中输入安全参数 1^l,执行 BPG 算法,生成元组 $t=(p,\mathbb{G}_1,\mathbb{G}_M,e,P)$. 其中,$\mathbb{G}_1$ 是阶为 p 的加法循环群,其生成元为 P;$\mathbb{G}_M$ 是阶为 p 的乘法循环群;e 是双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_M$;依据网络规模 $q(q>>(m+n+1))$选择辅助信息为 $a_f=s\in_R\mathbb{Z}_p^*$. 定义函数 $(f,g)\in_R F_l$ 如下: $f:\mathbb{Z}_p\times\mathbb{Z}_p\to\mathbb{Z}_p, g:\mathbb{Z}_p\to\mathbb{G}_1$, 即, $f:(u,x)\to(x+s)u, g:u\to uP$. 其中,累加元定义域为 $\mathbb{Z}_p\setminus\{-s\}$. 每个节点(包含 Sink,H-sensor 和 L-sensor)以(x_i+s)作为节点 Id_i 值,$(x_i+s)^{-1}$ 作为节点私钥,其余 $q-1$ 个节点的累加和 $W_i=g(f(...f(u,x_1)...,x_q))=\prod_{j=1,j\neq i}^{k}(x_j+s)uP=\prod_{j=1,j\neq i}^{k}Id_juP$ 作为证人信息,把 $\langle Id_i,W_i\rangle$和私钥预置到节点中.

2.2 身份认证

部署完成后,节点成簇构建层次式拓扑结构.如果两个节点在路由结构中是父子关系,则它们将尝试建立安全通信链路[17].为防止恶意节点访问网络,在进行密钥协商之前,节点间将进行身份认证.假设节点 a 和 b 在路由结构中有父子关系,则认证过程如图 2 所示.

$1: a\to *: Id_a \| W_a \| nonce_a$
$2: b:$ if $Id_aW_a == Id_bW_b$ then
add a into neighbor list
$b\to a: Id_b \| W_b \| nonce'_a$
$3: a:$ if $nonce_a == nonce'_a$ &&$Id_bW_b == Id_aW_a$ then
add b into neighbor list

Fig.2 Identity authentication
图 2 身份验证

节点 a 广播包含节点 Id_a、证人信息 W_a 和随机数 $nonce$ 的信息包.邻居节点 b 收到该广播消息后,首先验证 a 是否同属于一个集合.如果满足 $Id_aW_a=Id_bW_b=\prod_{i=1}^{k}(x_i+s)uP$, 则说明节点 a 与节点 b 同属一个集合,并参加了累计和运算,b 将把 a 存入邻居节点列表中.验证为合法节点后,b 将反馈 a 一个包含 Id_b、证人信息 W_b 以及原随机数 nonce 的信息包.同样,节点 a 也将验证信息的合法性,合法节点将存入 a 邻居节点列表中.

2.3 密钥协商

完成身份认证之后,通信半径内的合法节点间将完成密钥协商.节点 a,b 分别选择随机数 $n_a,n_b\in_R\mathbb{Z}_p^*$ 交换 n_aId_b 与 n_bId_a. 由双线性映射 e 和节点私钥 a_{pri},b_{pri} 求得共享密钥 k_{ab}=k_{ba}.过程如图 3 所示.

$$a\to b: n_aId_b$$
$$b\to a: n_bId_a$$
$$a: k_{ab}=e(n_bId_a,a_{pri})^{n_a}=e(n_b(x_a+s)P,(x_a+s)^{-1}P)^{n_a}=e(P,P)^{n_an_b}$$
$$b: k_{ba}=e(n_aId_b,b_{pri})^{n_b}=e(n_a(x_b+s)P,(x_b+s)^{-1}P)^{n_b}=e(P,P)^{n_bn_b}$$

Fig.3 Key agreement
图 3 密钥协商

虽然其他节点也可以解密此交换信息,但不能生成共享密钥.比如此处第三方节点可以获取 n_aId_b 和 n_bId_a,但不能计算共享密钥,因为计算共享密钥是一个 $\mathbb{G}_1$ 群上的计算 DH 问题(computational diffie-hellman problem,简称 CDHP)[18].

2.4 广播认证

由于 HSN 规模大、部署环境复杂难于人工维护,当有节点 a 退出网络时,依据不同退出原因将采用不同的处理措施.本文假设网络可以发现妥协节点并上报至控制节点(通常为 Sink).假设 Sink 节点的 Id 与证人信息分别为 Id_s 和 W_s.(1) 若因能量耗尽而消亡(或节点捕获但未泄露内部消息),则控制节点只需采用广播认证方式删除与该节点相关的密钥链路.广播信息为:① $Id_s \| W_s \| W_a$,② $Id_s \| W_s \| Id_a$.所有节点接收到信息后,验证如果 $Id_sW_s = Id_aW_a$,即可删除与 Id_a 节点相关的密钥链路.(2) 若节点被捕获且可能泄露内部信息,则不但要删除与节点相关的密钥链路还需要更新全网证人信息.广播消息为:① $Id_s \| W_s \| W_s'$,② $Id_s \| W_s \| Id_a$,③ $Id_s \| W_s \| V'$.接收节点判定 $Id_sW_s \neq W_s'Id_a$,进而验证 $Id_sW_s' = V'$,删除与 Id_a 节点相关的密钥链路,并更新证人信息 $W' = (1/(Id_a - Id_i))(W - V')$.

2.5 节点加入

随着时间的推移,一部分节点将失效或因能量耗尽而消亡.为了维持网络正常运转,需要部署新的节点.新节点 b 部署前从预置元素集合 q 中任选一组$\langle Id_b, W_b\rangle$和相应的私钥 a_{pri}.部署后,首先按照第 2.2 节对节点 b 进行身份认证,通过认证的节点则按照第 2.3 节所示过程完成密钥协商加入网络.不能通过身份认证的节点则判定为恶意节点,不与之进行密钥协商.

3 实验分析

异构传感网密钥管理方案性能评价主要由安全性、连通性与扩展性和能耗这 3 个方面来决定.本文首先从密码学角度分析所提方案的安全性,然后以经典 E-G 方案、EBS 方案为参照分析方案的完整性,最后与 E-G 方案对比分析方案的连通性与扩展性和能耗.

3.1 安全性分析

定义 4(可忽略函数). 对于函数 $f:\mathbb{N}\to\mathbb{R}^+$,如果对任意正整数 α,都存在正整数 l_0,使得 $l > l_0$,满足 $f(l) < l^{-\alpha}$,则 f 是可忽略函数.

定义 5(q-SDH 假设(q-strong Diffie-Hellman assumption)). $\mathbb{G}_1$ 是阶为 p 的加法循环群,其生成元为 P;$\mathbb{G}_M$ 是阶为 p 的乘法循环群;e 是满足双线性、非退化性和可计算性的双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_M$;$s\leftarrow\mathbb{Z}_p^*; Adv_A^{q\text{-SDH}}(l) = \Pr\left[A(t,P,sP,...,s^qP) = \left(c,\frac{1}{s+c}P\right)\right]$ 是可忽略的.

定理 1. 如果 q-SDH 假设是不可破解的,则累加器 $DA1$ 是抗碰撞的,其中 q 是累加器元素上界.

证明:假设存在概率多项式时间对手 A 可以破坏 $DA1$ 抗碰撞性,则可以构建概率多项式敌手 B,可以破解 q-SDH 假设.

假设已知挑战元组 $challenge = (P, zP, ..., z^qP), z\in_R\mathbb{Z}_p^*$,则 B 可以以不可忽略概率计算 $(c, 1/(z+c)P), c\in\mathbb{Z}_p$.设 $u\in_R\mathbb{Z}_p^*$,因为 A 可以破坏 $DA1$ 抗碰撞性,则它可以计算出 $X = \{x_1,...,x_k\}\subset\mathbb{Z}_p\setminus\{-z\}, x\in\mathbb{Z}_p\setminus(\{-z\}\cup X)$ 和 $W\in\mathbb{G}_1$,使得 $k\leqslant q$,且 $(x+z)W = \prod_{i=1}^k(x_i+z)uP$.从这个等式和挑战元组 $challenge$,可以计算 $(1/(x+z))P$,因此,q-SDH 是可破解的. □

定理 2. 身份认证过程中,认证密钥协商方案可以抵抗中间人攻击.

证明:在节点加入过程中,敌手有能力截获节点间广播信息: $Id_a \| W_a \| nonce$.① 若敌手篡改 $Id_a\to Id_a'$ 或 $W_a\to W_a'$,因为 $Id_a'W_a \neq Id_bW_b, Id_aW_a' \neq Id_bW_b$,所以 a 节点不被认为是 b 的邻居.② 若敌手修改 $nonce\to nonce'$,虽然通过 $Id_aW_a == Id_bW_b$ 验证,a 节点被认为是 b 的邻居,但是在 a 节点收到 b 节点的反馈信息时会发现

$nonce_a \neq nonce'_a$, 所以 b 节点不被认为是 a 的邻居.因此,如果身份认证信息发生篡改,则无法完成身份认证不会发生密钥协商,从而可以抵抗中间人攻击. □

定理 3. 若网络运作中发生节点妥协,则可以通过广播认证删除妥协节点满足向后安全性.

证明:在网络运行过程中,如果发生节点妥协,则按照第 2.4 节发送广播认证信息删除妥协节点.依据定义 3, $V \neq V'$ 且 $W \neq W'$, 网络仍然是安全的,即具有向后安全性. □

3.2 完整性分析

表 1 比较了 E-G 方案、EBS 方案以及本文方案的完整性.E-G 方案通过共享密钥发现与路径密钥建立完成实现身份认证和密钥协商,但方案本身没有涉及广播认证内容;EBS 方案是群组动态密钥管理方案,没有身份认证和密钥协商内容;本文方案把集合论引入异构传感网密钥管理中,基于双线性对动态累加器,部署前每个节点预置一定的密钥原材料,部署后节点相互验证是否属于同一个集合实现身份认证,合法节点生成通信密钥完成密钥协商,运行中借助广播认证随时部署新节点、排除受损节点,使网络处于动态安全中.

Table 1 Scheme integrity analysis

表 1 方案完整性分析

	E-G	EBS	本文方案
身份认证	√	×	√
密钥协商	√	×	√
广播认证	×	√	√

3.3 连通性与扩展性分析

在 E-G 方案[3]中,由于普通节点在密钥池中随机选取等额密钥作为本节点密钥环,节点间连通概率相同且与密钥池 P 的大小以及节点密钥环 k 的长度有关.节点间共享至少一个密钥的概率为

$$p = 1 - \frac{\left(1-\frac{k}{P}\right)^{2\left(P-k+\frac{1}{2}\right)}}{\left(1-\frac{2k}{P}\right)^{\left(P-2k+\frac{1}{2}\right)}} \tag{1}$$

显然,节点间连通概率与密钥环 k 的长度成正比,与密钥池 P 的大小成反比.新节点能否加入网路,取决于节点间能否发现共享密钥或建立路径密钥.假设每个节点周围平均有 d 个邻居节点,则建立密钥链路的概率为 $P_s = 1-(1-p)(1-p^2)^d$.因此,网络扩展性与邻居节点个数和节点间至少共享一个密钥的概率成正比.本方案从集合论的角度建立密钥链路,节点的存储需求不依赖于累加元集的变化而变化,节点存储量是恒定的.簇内节点完成第 2.2 节身份认证之后通过密钥协商建立共享密钥,由第 2.3 节可知,通信半径的合法节点都可以建立唯一共享密钥,所以本方案节点间连通概率恒等于 1.由于本方案从集合论的角度考虑节点能否加入,只要与原部署节点属于一个集合,只需按照第 2.2 节和第 2.3 节通过身份认证和完成密钥协商即可,所以网络的可扩展性恒等于 1.

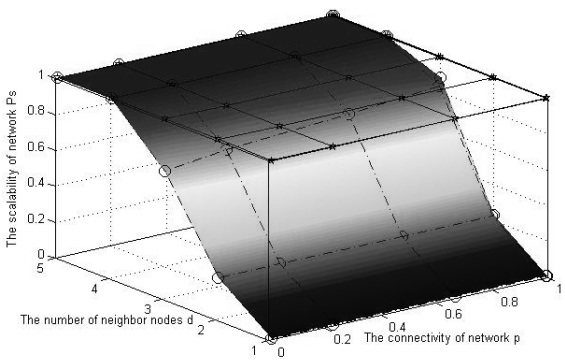


Fig.4 Comparison of connectivity and scalability

图 4 连通性与扩展性对比

假设密钥池 P=100,节点密钥环长度 k=[1,5,10,20,30],节点周围平均邻居节点个数 d=[1,2,3,4,5],网络连通性与可扩展性如图 4 所示.由于本方案从集合论的角度完成密钥协商,节点存储量恒定,可扩展性和连通性恒为 1.而在 E-G 方案[3]中,节点密钥

环长度越长,节点间联通概率就越大;节点在相同密钥环时,邻居节点数目越多,可扩展性就越好.

3.4 能耗分析

采用 Omnet++ 4.0 仿真实验平台,设定为 200×200m^2 的正方形区域.网络配置一个 Sink 节点,区域内分别随机部署 20、40、60、80 和 100 个节点,其中,H-sensor,Low-sensor 分别为 4,5,6,7,8 和 16,35,54,73,92.节点状态在空闲、接收和发送之间转换,节点性能参数参照 MICA2 Mote[19]配置.在相同部署情况下,采集不同数目网络节点自节点部署完成至建立共享密钥之间(不考虑数据通信能耗),E-G 方案与本文方案平均能耗变化情况.由图 5 可以看出,本文方案平均能耗明显比 E-G 方案[3]要高,且随着网络节点数目的变大,能耗差距明显增大.其原因在于,E-G 方案[3]本身不包含身份认证功能,且共享密钥建立也相对比较简单,只需比对密钥环是否有相同密钥 ID 即可,因此功耗较小.而本文方案首先采用动态累加器完成身份认证,再利用椭圆曲线计算共享密钥,算法时间复杂度相对较高,所以更适用于有较高安全性需要的环境中.

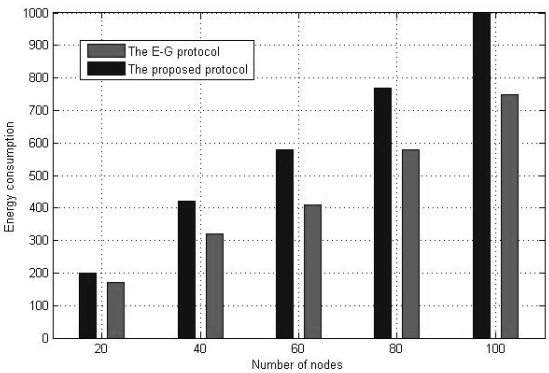


Fig.5 Comparison of energy consumptions

图 5 能耗分析

4 结束语

通过分析异构传感网已有安全方案,提出一种基于双线性对动态累加器的异构传感网认证密钥协商方案.该方案把集合论思想引入异构传感网认证密钥协商方案设计中,把节点间身份认证和密钥协商转化为集合元素间的关系认证.借助双线性对累加器技术实现了异构传感网身份认证、密钥协商和广播认证功能.实验分析表明,该方案不但实现了身份认证、密钥协商和广播认证的有效融合,而且具有良好的安全性、扩展性和网络结构变化的自适应性.但是,双线性对效率和能耗相对较高,较适用于节点性能和安全性需求较高的场景中.下一步,将一方面把本方案配置到传感器实验网络中观测性能;另一方面,将优化尝试采用 Ate 配对优化双线性对提升计算效率,并以认证密钥协商为基础,开展与时空相关的传感网隐私保护研究.

致谢 在此,我们感谢哈尔滨工程大学计算机科学与技术学院马春光教授对本课题研究给予的指导,感谢各位审稿专家给予的支持和建议,感谢《软件学报》编辑部编辑付出的辛勤劳动.

References:

[1] Zhao J, Li X, Deng LJ, Li XH, Ma JF. A selection method for user authentication protocols in wireless networks. Journal of Computer Research and Development, 2015,52(3):671−680 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2015.20131376]

[2] Reegan AS, Baburaj E. Key management schemes in wireless sensor networks: A survey. In: Proc. of the IEEE Int'l Conf. on Circuit, Power and Computing Technologies (ICCPCT 2013). Washington: IEEE Computer Society, 2013. 813−820. [doi: 10.1109/ICCPCT.2013.6528861]

[3] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2002. 41−47. [doi: 10.1145/586110.586117]

[4] Lee JH., Kwon T. GENDEP: Location-Aware key management for general deployment of wireless sensor networks. Int'l Journal of Distributed Sensor Networks, 2014, 2014:1−17. [doi: 10.1155/2014/490202]

[5] Lata BT, Raghavendra M, Tejaswi V, Shaila K, Venugopal KR, Iyengar SS, Patnaik LM. SSEGR: Secure single-copy energy efficient geographical routing algorithm in wireless sensor networks. IOSR Journal of Computer Engineering, 2014,16(6):37−49.

[6] Yuan T, Ma JQ, Zhong YP, Zhang SY. Key management scheme using time-based deployment for wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2010,21(3):516−527 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3457.htm [doi: 10.3724/SP.J.1001.2010.03457]

[7] Eltoweissy M, Moharrum M, Mukkamala R. Dynamic key management in sensor networks. IEEE Communications Magazine, 2006,44(4):122−130. [doi: 10.1109/MCOM.2006.1632659]

[8] Kong FR, Li CW. Dynamic key management scheme for wireless sensor network. Ruan Jian Xue Bao/Journal of Software, 2010,21(7):1679−1691 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3585.htm [doi: 10.3724/SP.J.1001.2010.03585]

[9] Zeng WN, Lin YP, Yu JP, Wang L. Group key management based on random perturbation in wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2013,24(4):873−886 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4270.htm [doi: 10.3724/SP.J.1001.2013.04270]

[10] Erfani SH, Javadi HHS, Rahmani AM. A dynamic key management scheme for dynamic wireless sensor networks. Security and Communication Networks, 2015,8(6):1040−1049. [doi: 10.1002/sec.1058]

[11] Wang JR., Zhang WY. One-Way accumulator based random key pre-distribution protocol for sensor networks. Journal of Information and Computational Science, 2012,9(18):5561−5569.

[12] Zhong XR, Ma CG. Dynamic accumulators-based authenticated group key management scheme for heterogeneous wireless sensor network. Journal on Communications, 2014,35(3):124−134 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-436x.2014.03.014]

[13] Ren YJ, Wang JD, Xu DZ, Zhuang Y, Wang J. Key agreement protocol for wireless sensor networks using self-certified public key system. Journal of Computer Research and Development, 2012,49(2):304−311 (in Chinese with English abstract). http://crad.ict.ac.cn/CN/Y2012/V49/I2/304

[14] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials. Lecture Notes in Computer Science, 2002,2442:61−76.

[15] Nguyen L. Accumulators from bilinear pairings and applications. Lecture Notes in Computer Science, 2005,3376:275−292.

[16] Tartary C, Wang HX. The bilinear pairing-based accumulator proposed at CT-RSA'05 is not collision resistant. Cryptology ePrint Archive, 2006. http://eprint.iacr.org/2006/426

[17] Seung-Hyun S, Jongho W, Salmin S, Elisa B. Effective key management in dynamic wireless sensor networks. IEEE Trans. on Information Forensics and Security, 2015,10(2):371−383.[doi: 10.1109/TIFS.2014.2375555]

[18] Yacobi Y. A note on the bilinear Diffie-Hellman assumption. Cryptology ePrint Archive, 2002. http://eprint.iacr.org/2002/113

[19] MICA2 mote datasheet. http://www.moog-crossbow.com

附中文参考文献:

[1] 赵婧,李鑫,邓凌娟,李兴华,马建峰.无线网络中身份认证协议选择方法.计算机研究与发展,2015,52(3):671−680. [doi: 10.7544/issn1000-1239.2015.20131376]

[6] 袁斑,马建庆,钟亦平,张世永.基于时间部署的无线传感器网络密钥管理方案.软件学报,2010,21(3):516−527. http://www.jos.org.cn/1000-9825/3457.htm [doi: 10.3724/SP.J.1001.2010.03457]

[8] 孔繁瑞,李春文.无线传感器网络动态密钥管理方法.软件学报,2010,21(7):1679−1691. http://www.jos.org.cn/1000-9825/3585.htm [doi: 10.3724/SP.J.1001.2010.03585]

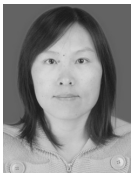
[9] 曾玮妮,林亚平,余建平,王雷.传感器网络中基于随机混淆的组密钥管理机制.软件学报,2013,24(4):873−886. http://www.jos.org.cn/1000-9825/4270.htm [doi: 10.3724/SP.J.1001.2013.04270]

[12] 钟晓睿,马春光.基于动态累加器的异构传感网认证组密钥管理方案.通信学报,2014,35(3):124−134. [doi: 10.3969/j.issn.1000-436x.2014.03.014]

[13] 任勇军,王建东,徐大专,庄毅,王箭.自认证公钥的无线传感器网络密钥协商协议.计算机研究与发展,2012,49(2):304−311. http://crad.ict.ac.cn/CN/Y2012/V49/I2/304

王九如(1983－),男,山东临沂人,博士,讲师,CCF 会员,主要研究领域为网络信息安全,传感网与物联网.

刘丽(1981－),女,讲师,CCF 会员,主要研究领域为网络信息安全,传感网与物联网.



丁林花(1979－),女,讲师,CCF 会员,主要研究领域为网络信息安全,分布式计算.

王海峰(1976－),男,博士,副教授,CCF 会员,主要研究领域为分布式计算,传感网与物联网,复杂系统分析.