ISSN 1000-1239/CN 11-1777/TP
50(10): 2109-2116, 2013

基于 M-IBE 的异构传感网密钥管理协议

马春光[1,2,3] 王九如[1] 武 朋[1] 张 华[2]
[1](哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)
[2](网络与交换技术国家重点实验室(北京邮电大学) 北京 100876)
[3](哈尔滨工程大学国家保密学院 哈尔滨 150001)
(machunguang@hrbeu.edu.cn)

M-IBE Based Key Management Protocol for Heterogeneous Sensor Networks

Ma Chunguang[1,2,3], Wang Jiuru[1], Wu Peng[1], and Zhang Hua[2]
[1](*College of Computer Science and Technology, Harbin Engineering University, Harbin* 150001)
[2](*State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), Beijing* 100876)
[3](*College of National Secrecy, Harbin Engineering University, Harbin* 150001)

Abstract To address intra-group and inter-group communication issues arising from function heterogeneity in heterogeneous sensor networks (HSNs), the applications of public-key cryptosystem, especially identity-based encryption (IBE), is studied, and a key management protocol for HSNs based on multi-domain identity-based encryption (M-IBE) is proposed. In the protocol, one group of HSNs is analogized to one domain in M-IBE from a logical point of view. Before deployment, a trusted third party generates global public parameters for the HSN, selects public and private keys for each group, and extracts private key for each sensor within the group. After deployment, neighbor sensors within the same group set up shared-key through the exchange of sensor identity; neighbor sensors in different groups establish shared-key after getting authorized from cluster heads. The proposed protocol is composed of four parts: key material pre-distribution, shared-key establishment within group, shared-key agreement between two groups, and adding new sensors and removing sensors. The security analysis and performance evaluation show that the protocol has high security, which can resist against high-end sensors and low-end sensors capture attacks. It also has low storage requirements and constant connectivity probability. It can satisfy the demand for higher security application scenarios.

Key words heterogeneous sensor network; key management; public key cryptosystem; multi-domain identity-based encryption; security

摘 要 为解决异构传感网(heterogeneous sensor networks, HSN)因功能异构而导致的组内通信和组间通信安全问题,研究了公钥密码体制尤其身份基密码体制(identity-based encryption, IBE)在异构传感网中的应用,提出了基于多域身份基加密(multi-domain identity-based encryption, M-IBE)的异构传感网密钥管理协议.从逻辑上把 HSN 中的一个组类比于 M-IBE 的一个域.部署前由可信第三方为 HSN 生成全局公共参数、选取各组公私钥、抽取组内各节点私钥;部署后同组内邻居节点通过交换身份

收稿日期:2011-09-15;**修回日期**:2012-04-23
基金项目:国家自然科学基金项目(61073042,61170241);博士后科研人员落户黑龙江科研启动资助金项目(LBH-Q10141);网络与交换技术国家重点实验室(北京邮电大学)开放课题基金项目(SKLNST-2009-1-10);黑龙江省教育厅科学技术研究项目(12513049);黑龙江省自然科学基金项目(F201229)
通信作者:王九如(jiuruwang@163.com)

标识建立共享密钥;不同组内邻居节点在获得簇头授权后协商建立共享密钥.协议由密钥预分配、组内共享密钥建立、组间共享密钥协商、新节点加入、节点移除5部分组成.实验分析表明:该协议具有较高的安全性,可以抵抗高端节点和低端节点俘获攻击,较低的存储需求和恒定的连通概率适用于安全需求较高的应用场景中.

关键词 异构传感网;密钥管理;公钥密码体制;多域身份基加密;安全

中图法分类号 TP393.08

由多种不同类型的传感节点构成的异构传感网[1](heterogeneous sensor networks, HSN)尤其作为物联网感知层而存在时,往往需要不同组监测不同区域或者不同组监测不同内容,因此异构传感网中组内通信和组间通信不可偏废.但是因为节点资源受限、缺乏基础设施、部署环境复杂等异构传感网固有特性,使得许多研究成果(如KDC技术、PKI/CA技术等)不能直接应用[2],所以在军用信息监测等私密性要求较高的应用场景中,安全问题成为一个瓶颈问题.而作为各种安全机制的基础,密钥管理问题必须首先解决[3].

虽然异构传感网密钥管理已经取得许多良好成果,但已有的密钥管理协议均无法有效解决异构传感网组内通信和组间通信问题.造成这一现象的原因主要有以下3个方面:1)早期的研究主要基于网络同构性假设,即构成异构传感网的节点是低功耗的、无差异的[4],网络功能相对简单,主要解决组内通信问题,未考虑组间通信;2)当前异构性研究局限于节点能量、通信能力和计算能力3方面,对节点功能异构研究不足,仍以组内通信研究为重点[5],忽略了组间通信问题;3)公钥密钥体制在异构传感网密钥管理中的应用研究不够深入,已提出的对称密钥管理协议虽然在一定程度上解决了组内通信和组间通信问题,但存在网络抗俘获性差[6]、存储空间大等不足[7].2004年Lauter证明经优化设计的非对称密钥系统,不仅可以应用于传感器,而且椭圆曲线密码(elliptic curve cryptography, ECC)系统在计算量和存储需求方面有一定优势[8],从而逐渐引起科研人员重视并把基于ECC的密钥算法(如elliptic curve digital signature algorithm, ECDSA[9])用于传感网中.

本文提出一种基于多域身份基加密(multi-domain identity-based encryption, M-IBE)的异构传感网密钥管理协议.该协议使组内通信和组间通信有效融合,解决了组内通信和组间通信问题,为异构传感网乃至物联网的广泛应用提供安全保障;将M-IBE运用到异构传感网中,深化了公钥密码体制尤其身份基密码的应用研究;把节点功能异构纳入到异构性研究之中,拓展了异构性研究范围.实验分析表明与已有典型协议相比该协议优势主要体现在:1)具有较高的安全性,可以有效抵抗节点俘获攻击;2)较低的存储需求、恒定的连通性和高效的计算效率;3)适用于军用信息监测等安全需求较高的环境中.

1 M-IBE方案

为简化公钥密码系统中的密钥管理过程,1984年Shamir[10]首次提出了身份基密码学概念.在身份基密码系统中,用户的公开身份信息(如IP地址、Email等)即可作为公钥.隶属于同一管理域的多个用户从同一个域私钥生成中心(域-PKG)处获得私钥,整个系统对证书或目录的依赖程度显著降低[11].2001年Boneh和Franklin[12]基于椭圆曲线上双线性配对设计了安全实用的身份基加密(identity-based encryption, IBE)方案(BF-IBE方案).2003年Sakai和Kasahara等人[13]同样基于双线性配提出了一个约减的身份基加密方案(SK-IBE方案).2007年杨庚等人[14-15]将BF-IBE方案用于同构传感网中,表明协议在复杂性、安全性、健壮性和内存需求等方面,与随机协议等相比有一定的优势.同年,王圣宝等人[16-17]提出多域环境下的高效身份基加密方案(M-IBE方案),并指出在多域环境下,SK-IBE方案扩展性远不如BF-IBE方案和M-IBE方案,BF-IBE方案的计算效率不及M-IBE.本节将对M-IBE方案作简要描述.

令G_1表示一个由P生成的加法循环群,阶为素数p;G_2表示一个阶同样为p的乘法循环群;一个可容许的配对$\hat{e}$是满足双线性、非退化性和可计算性的双线性映射$\hat{e}:G_1\times G_1\rightarrow G_2$.假设群$G_1$,$G_2$上的离散对数问题都是困难的.M-IBE方案的安全性基于MBDH问题(modified BDH问题)难解性,即

给定$\langle P,aP,bP,cP\rangle$(其中,$a,b,c\in\mathbb{Z}_p^*$),计算 $\hat{e}(P,P)^{a^{-1}bc}\in G_2$ 是难解的[16-17]. M-IBE 方案与 BF-IBE 方案不同之处主要在于特别提炼出一个额外的全局初始化算法——G-setup,负责生成全局公共参数 *params*. 在获得全局参数之后,每个域-PKG 生成各自的主密钥(包括主私钥、主公钥),避免每个域独立设置并维护各自的域-PKG,从而有效降低跨域运行复杂度. 具体的 M-IBE 方案由以下 5 种算法组成.

1) 全局初始化(G-setup):由全局可信第三方运行的一个概率算法,输入安全参数 k,输出全局公共参数 *params*. 具体包含以下内容:

① 两个阶为素数 p 的循环群 G_1 与 G_2,群 G_1 的生成元为 P,以及一个可容许的双线性映射 $\hat{e}:G_1\times G_1\to G_2$.

② 两个整数 $k_0,n(k_0<n)$和 3 个密码 Hash 函数 $H_1:\{0,1\}^*\to G_1$, $H_2:G_2\to\{0,1\}^n$ 和 $H_3:\{0,1\}^n\to\mathbb{Z}_p^*$.

从而,全局公共参数 *params* 可表示为$\langle p,G_1,G_2,\hat{e},P,n,k_0,H_1,H_2,H_3\rangle$. 其中,明文空间为 $M=\{0,1\}^{n-k_0}$,密文空间为 $C=G_1^*\times\{0,1\}^n$.

2) 域初始化(setup):由每个域-PKG 运行的概率算法,输入全局参数 *params*,输出该域的主密钥,即一对公私钥(P_{pub},s). 域-PKG 公布主公钥,保密主私钥. 具体过程如下:

① 每个域-PKG 随机选取整数 $s\in\mathbb{Z}_p$作为主私钥.

② 计算主公钥 $P_{\text{pub}}=s^{-1}P\in G_1$.

注意,在 BF-IBE[12,14-15]中,域-PKG 的主公钥是 $P_{\text{pub}}=sP\in G_1$.

3) 私钥抽取(key-extraction):域-PKG 运行密钥生成算法,输入全局公共参数 *params*、域主私钥 s 以及用户身份标识 ID,输出用户的私钥 S_{ID}. 具体描述为:给定一个身份标识 $ID\in\{0,1\}^*$,域-PKG 首先计算 $Q_{ID}=H_1(ID)\in G_1^*$,再计算用户私钥 $S_{ID}=sQ_{ID}$,其中,s 为不同域主私钥.

4) 加密(encryption):执行一个概率算法,输入全局公共参数 *params*、接收者身份标识 ID、明文 m,输出为密文 C. 详细描述如下:

为加密一个明文消息 $m\in\mathbb{M}$,发送者随机选取 $\sigma\in\{0,1\}^{k_0}$,利用接收者的身份标识 ID,计算 $Q_{ID}=H_1(ID)\in G_1^*$,计算 Hash 值 $r=H_3(m\|\sigma)\in\mathbb{Z}_p^*$. 最后,求得密文设置 $C=\langle U,V\rangle=\langle rP_{\text{pub}},(m\|\sigma)\oplus H_2(g_{ID}^r)\rangle\in C$,其中,$g_{ID}=\hat{e}(P,Q_{ID})\in G_2^*$.

5) 解密(decryption):运行一个确定性算法,输入用户私钥 S_{ID}、密文 C,输出明文 m 或者一个区分标识符号 $\perp$(当 C 为不合法密文时). 具体过程为

① 计算 $m'\|\sigma'=V\oplus H_2(\hat{e}(U,S_{ID}))$;

② 计算 $r'=H_3(m'\|\sigma')$,然后检验式 $U=r'P_{\text{pub}}$是否成立;

③ 如果成立,输出明文 m';否则输出 $\perp$.

一致性条件:接收者能够正确解密密文 C 以获得明文 m,因为:

$$\hat{e}(U,S_{ID})=\hat{e}(rP_{\text{pub}},sQ_{ID})=\hat{e}(rs^{-1}P,sQ_{ID})=\hat{e}(P,Q_{ID})^r,$$

即若 C 是对应于明文消息 m 的合法密文,则解密算法能够保证 $m'=m$.

2 基于 M-IBE 的 HSN 密钥管理协议

本节首先介绍 HSN 部署模型和体系结构,再进一步阐述基于 M-IBE 的 HSN 密钥管理协议.

2.1 HSN 网络模型

部署前先将 HSN 所有的节点依据节点功能和监测任务分成分组,每组由 n 个节点组成. 分组完成后将节点按分组部署到预期位置. 通常同一分组的所有节点会在同一时间部署在同一地点. 比如,使用部署直升机在指定地点投放同一分组的所有节点. 可以预期,属于同一个分组的节点在地理位置上会相互更靠近,通常认为满足均匀分布或者二维高斯分布.

HSN 采用层簇式拓扑结构如图 1 所示,整个网络划分为多个组,每个组内分为若干簇. 在物理结构上,HSN 由大量低端节点(low-end sensor, L-Sensor)、少量高端节点(high-end sensor, H-Sensor)和一个基站(Sink)节点组成. 其中,H-Sensor 在通信能力、存储能力、计算能力和能量方面优于 L-Sensor,不同组 L-Sensor 之间可能配备不同的感知原件执行不同监测任务. 从逻辑层次看,网络划分为感知层、簇头层和基站层. 同组内 L-Sensor 选择信噪比(SRN)较优的 H-Sensor 为中心成簇,被选中的 H-Sensor 也称为簇头(cluster head, CH),簇头间相互通信构建组内骨干网络. 基站是数据信息的最终收集者,假设具有无限制的资源,能向整个网络发布命令和进行广播. 簇头是簇中的数据汇聚节点,负责数据的融合和转发. 簇成员节点是数据的采集节点,由普通传感节点组成,负责将监测到的信息在规定的时间转发给簇头. 在信任程度上,通常认为基站是完全可信的,簇头是不完全可信的,感知节点是不可信的.

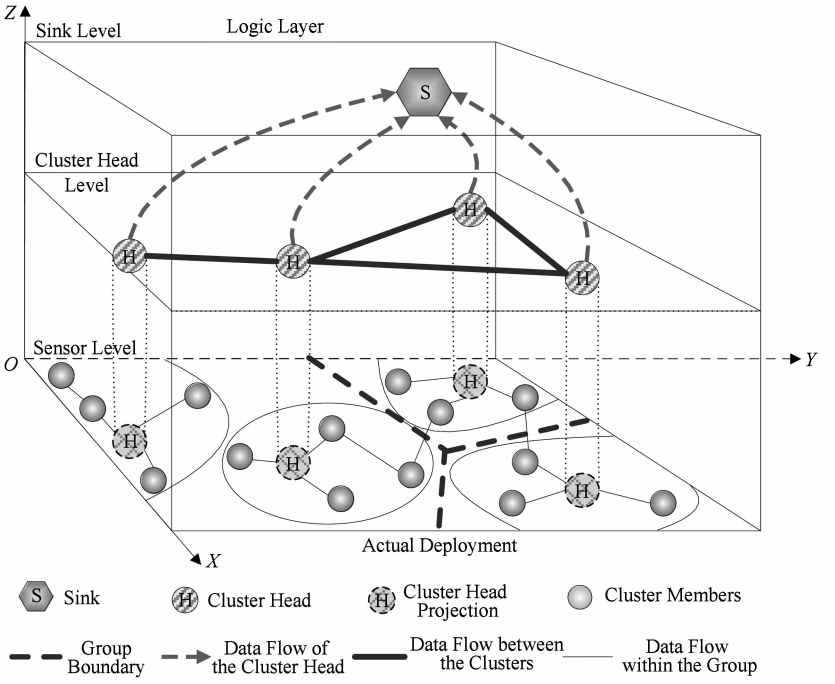

Fig. 1 Heterogeneous sensor network architecture.

图 1 异构传感网体系结构

可以看出,M-IBE 和 HSN 逻辑结构类似,M-IBE 的一个域可类比于 HSN 的一个组,因而启发探索 M-IBE 在异构传感网中的应用问题.

2.2 基于 M-IBE 的 HSN 密钥管理协议

该协议主要包括组内共享密钥建立和组间共享密钥建立 2 部分. 其基本思想是部署前可信第三方(通常由基站担任)构建全局公共参数 $params$,为不同组选择不同的主私钥 s. 部署后同一分组内邻居节点交换身份 ID,建立共享密钥;不同组邻居节点获得簇头授权后建立共享密钥. 如图 2 所示,A_1,B_1 是地理位置邻近的不同组具有较大通信半径的簇头节点,A_2,A_3,B_2,B_3 是通信半径较小的 L-Sensor 节点,A_1,A_2,A_3 属于组 A,节点 B_1,B_2,B_3 属于组 B. 各组首先建立组内共享密钥,在获得簇头授权后 A_3,B_3 建立组间共享密钥.

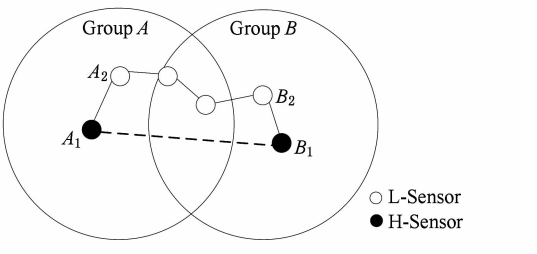

Fig. 2 Protocol schematic.

图 2 协议示意图

2.3 协议过程

1) 密钥预分配

① 给定一个安全参数 k,可信第三方运行全局初始化(G-setup)算法,输出全局公共参数 $params$ 为$\langle p,G_1,G_2,\hat{e},P,n,k_0,H_1,H_2,H_3\rangle$. 其中,明文空间为 $M=\{0,1\}^{n-k_0}$,密文空间为 $C=G_1^*\times\{0,1\}^n$.

② 根据预期部署位置(或功能)将节点分组,可信第三方运行域初始化(setup)为每个组(域-PKG)选取主私钥 $s\in\mathbb{Z}_p$,计算主公钥 $P_{pub}=s^{-1}P\in\mathbb{Z}_p$.

③ 执行私钥抽取(key-extraction)算法为各组内节点计算各自私钥 $S_{ID}=sQ_{ID}$,其中,s 为各组主私钥.

④ 将全局公共参数 $params$、所在组主公钥 P_{pub}、节点 ID、节点私钥 S_{ID} 预置到节点中(包括 H-Sensor,L-Sensor),并为 H-Sensor 装载本组所有节点 ID(包含为补充网络节点而预留的 ID)和其他组 H-Sensor 节点 ID. 其中,所在组主公钥 P_{pub} 用于验证可信第三方发送的广播数据. 当可信第三方广播数据包时(如节点移除),可信第三方借助 ECDSA 算法[9] 用组主私钥生成的数字签名,节点在收到数据包后利用预置的组主公钥验证签名.

2) 组内共享密钥建立

在密钥预分配完成之后,将 HSN 各分组部署到相应监测区域中. 每个分组内都有少量 H-Sensor

节点和大量 L-Sensor 节点,假设分组内 L-Sensor 以簇头为中心采用贪婪路由算法形成树型路由结构,L-Sensor 仅需要与邻居节点建立共享密钥,即与该节点的双亲和孩子节点建立共享密[5].

在获得邻居节点 ID 后,彼此加密交换密钥公共参数,计算共享密钥.如图 2 以 A_2,A_3 为例,A_2,A_3 为同属分组 A 的邻居节点.A_2 计算 $s_2=\eta^{r_2} \bmod q$ ($x_2<q$),A_3 计算 $s_3=\eta^{r_3} \bmod q$ ($x_3<q$).A_2 执行 Encryption 算法对 ID_{A_3},ID_{A_2},s_2 进行加密发送给 A_3,A_3 执行 Decryption 算法解密数据,获得 ID_{A_2} 和 s_2.同理,A_2 获得 ID_{A_3} 和 s_3.A_2 计算共享密钥 $K=s_3 \bmod q$,A_3 计算 $K=s_2 \bmod q$.双方应用对称密钥 K 安全通信.由于该协议满足 MBDH 安全假设,不同组内节点私钥在不同组主私钥下抽取,所以不同组节点之间不能相互解密数据,从而有效实现了组间信息隔离.

3) 组间共享密钥协商

在分组成簇时,节点间相互广播身份 ID,不同分组的相邻节点(如图 2 中 A_3,B_3)也可以相互获取身份 ID.如果节点收到来自不同分组邻居节点建立共享密钥的请求,则一方面向簇头发送利用簇头 ID 加密的通信授权请求信息,一方面利用对方 ID 生成准备应答的加密数据;簇头收到通信请求信息后,利用通信距离比较远的优势,与源请求节点所在组的簇头相互通信,验证源请求节点身份.验证通过后簇头则加密发送授权应答数据,节点间建立共享密钥.

如图 2 以 A_3,B_3 为例,A_3,B_3 为同分属组 A、组 B 的邻居节点.假设 B_3 向 A_3 发送建立共享密钥请求,则 A_3 一方面执行 Encryption 算法对 ID_{A_1},ID_{A_3},ID_{B_3} 加密,向 A_1 通信授权请求信息,另一方面 A_3 执行 Encryption 算法对 ID_{B_3},ID_{A_3},s_3 加密准备发送给 B_3.簇头 A_1 执行 Decryption 算法解密数据,获得 ID_{A_3} 和 ID_{B_3},并利用通信能力强的异构特性,A_1 执行 Encryption 算法对 ID_{B_1},ID_{A_1},ID_{B_3} 进行加密发送至 B_1.B_1 解密信息,利用预置的全组节点 ID 验证节点 B_3 身份并反馈验证结果至 A_1.若通过验证,B_1 把 ID_{B_3} 用 B_1 私钥加密广播告知全组所有 H-Sensor,A_1 执行 Encryption 算法对向 A_3 单播授权信息,A_3 解密获取授权,执行与组内共享密钥建立类似过程,与 B_3 建立共享密钥.

由于 M-IBE 方案加密算法中,配对运算为 $g_{ID}=\hat{e}(P,Q_{ID})$,独立于域-PKG 的主公钥 P_{pub}.因此,发送方无需获得接受者所在域-PKG 信息,即可完成信息加密,所以可以实现高效的组间信息交互.

4) 新节点加入

由于 HSN 通常由电池供电,部署在无人值守环境中,难于人工维护.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.新节点部署前首先预配置全局公共参数 $params$、所在组主公钥 P_{pub}、节点 ID、节点私钥 S_{ID}.部署完成后,执行组内共享密钥建立过程,即可验证节点身份加入网络中.

5) 节点移除

当发生节点妥协时,所有与妥协节点相关的节点需要停止与妥协节点的数据通信.假设网络具有入侵检测功能,并把检测报告上传至可信第三方.可信第三方广播包含该节点 ID 的节点移除数据包,并附上用 ECDSA 算法[9]和节点所在组主私钥生成的数字签名($sign$).数据包格式为:节点 ID+$sign$.节点(L-Sensor 和 H-Sensor)收到信息后,可以检查自己的链路中是否包含妥协节点.如果有则移除与妥协节点连通的链路(如果该节点与邻近分组有共享密钥,簇头需告知邻组删除该节点).因为每个节点具有组主公钥,所以当节点收到移除节点数据包时,可以通过签名验证数据包的完整性,从而阻止对方发送虚假移除数据包.

3 实验分析

本节将从安全性、存储及连通性和效率 4 个方面,以经典随机密钥管理协议(E-G 协议)[4]为参照,对新提出的协议进行深入分析.

3.1 安全性分析

定理 1. L-Sensor 妥协不影响网络安全.

证明. L-Sensor 妥协将泄漏全局公共参数 $params$、组主公钥 P_{pub}、节点 ID 和节点私钥 S_{ID}.从协议设计可以看出本协议的安全性基于 M-IBE 方案的安全性.文献[17-18]已经详细证明 M-IBE 方案是安全的,其安全性基于 MBDH 问题的困难性,能抵抗适应性选择密文攻击.本协议发生 L-Sensor 节点妥协时,等价于随机预言模型 ROM 中,查询阶段对特定 ID 的解密查询,对未捕获节点的推测等价于猜测查询.所以由文献[17]结论可知,L-Sensor 妥协不影响网络安全. 证毕.

定理 2. H-Sensor 妥协不会影响网络安全.

证明. H-Sensor 妥协将泄漏全局公共参数 $params$、组主公钥 P_{pub},ID,S_{ID} 以及本组所有

L-Sensor 的 ID. 由文献[17]可知,在 ROM 模型中,ID 的泄露不会给攻击者增加猜测优势. 结合定理 1 可知,H-Sensor 妥协不会影响网络安全. 证毕.

定理 3. 仅可信第三方可执行密钥重构解密密文.

证明. 由 2.3 节协议过程中密钥预分配可知,可信第三方知晓不同组主私钥 s,所以可信第三方可以重构节点自私钥 $S_{ID}=sQ_{ID}$,从而可以正确解密密文. 另一方面,由定理 1、定理 2 可知 L-Sensor 与 H-Sensor 的妥协不会影响网络安全,即恶意节点不能重构其他节点私钥解密密文. 所以仅可信第三方可以执行密钥重构并正确解密密文. 证毕.

3.2 存储及连通性分析

假设由 M 个 H-Sensor 和 N 个 L-Sensor 随即部署在观测区域中($M\ll N$). 基于 M-IBE 的 HSN 密钥管理协议,H-Sensor 存储全局公共 $params$、组主公钥 P_{pub}、ID、节点私钥 S_{ID}、以及本组所有 L-Sensor 的 ID;L-Sensor 存储全局公共 $params$、组主公钥 P_{pub},ID 和节点私钥 S_{ID}. 各组存储需求为 $M(4+N)+4N$. 路由选择之后,节点间通过交换公共参数建立密钥链路,连通概率为 1.

在 E-G 协议[4]中,由于 H-Sensor 和 L-Sensor 存储能力互不相同,且与密钥池和节点间连通概率相关. 假设密钥池大小为 S,H-Sensor 密钥环长度为 H,L-Sensor 密钥环长度为 $L(H\geqslant L)$,则各组存储需求为 $MH+NL$,L-Sensor 间的连通概率(p_{LL})为

$$p_{LL}=1-\frac{\left(1-\frac{L}{S}\right)^{2\left(S-L+\frac{1}{2}\right)}}{\left(1-\frac{2L}{S}\right)^{\left(S-2L+\frac{1}{2}\right)}}. \tag{1}$$

H-Sensor 与 L-Sensor 的连通概率(p_{HL})为

$$p_{HL}=1-\frac{\left(1-\frac{H}{S}\right)^{\left(S-H+\frac{1}{2}\right)}\left(1-\frac{L}{S}\right)^{\left(S-L+\frac{1}{2}\right)}}{\left(1-\frac{H+L}{S}\right)^{\left(S-H-L+\frac{1}{2}\right)}}. \tag{2}$$

假设 $M=4$,$N=16$,密钥池 s 分别为 10,20,30,40,50,60,70,80,90,100,则所提协议连通概率恒为 1,存储需求恒为 144. E-G 协议[4]中存储需求与连通概率相关,假设 $p_{LL}>0.9$,$p_{HL}>0.95$,则 L-Sensor 与 H-Sensor 存储需求如表 1 所示,全组存储需求变化如图 3 所示. 可以看出,本协议连通概率、节点存储需求和总存储需求均恒定不变,而 E-G 协议[4]随着密钥池的增大节点存储需求和总存储需求均变大.

Table 1 Relationship Between Key Pool and Storage Requirements of Sensor

表 1 密钥池与节点存储需求对照表

S	$L(p_{LL}>0.9)$	$H(p_{HL}>0.95)$
10	4	5
20	6	7
30	8	9
40	9	11
50	10	12
60	11	14
70	12	15
80	13	16
90	14	17
100	15	17

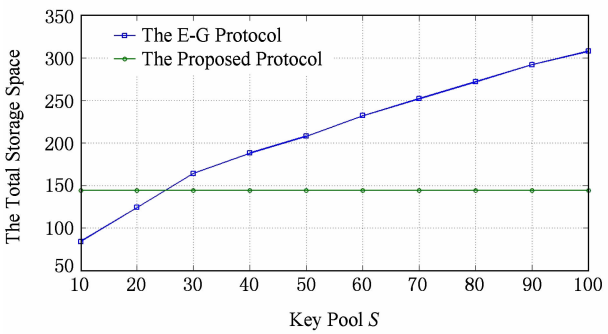

Fig. 3 Relationship between key pool and total storage requirements.

图 3 密钥池与总存储需求变化关系

3.3 效率分析

如第 1 节所述,BF-IBE 和 M-IBE 均可用于多域环境,但是 BFM-IBE 方案不及 M-IBE 方案高效,比较结果如表 2 所示. 两个方案安全性都基于 BDH 假设,域-PKG 私钥、公钥长度相同、加密解密计算负荷相等. 但 BF-IBE 方案中,配对运算为 $g_{ID}=\hat{e}(P_{pub},Q_{ID})$,其中,$P_{pub}$ 是解密者所属域的主公钥. 因此在多域环境下,BF-IBE 方案要求发送者必须事先获得接受者所在域-PKG 主公钥. 而 M-IBE 方案加密算法中,配对运算为 $g_{ID}=\hat{e}(P,Q_{ID})$,独立于域-PKG 的主公钥 P_{pub}. 因此,发送方无需获得接受者所在域-PKG 信息,具有较高的通信效率.

在 Omnet 4.1 平台下仿真运行本协议和 E-G 协议[4],分析通信密钥建立过程能耗情况. 仿真环境大小设定为 200 m×200 m 正方形区域,网络节点配置情况如表 3 所示. 节点在空闲、接收和发送 3 种状态间转换,参照 MICA2 Mote[19]配置相关参数. 如

图 4 所示本文新协议比 E-G 协议[4]能耗要高.原因在于新协议节点之间通过 IBE 加密交换公共参数,利用 Diffie-Hellman 方式建立共享密钥.而 E-G 协议[4]中节点以明文方式交换密钥 ID 完成发现共享密钥.所以整个网络构建过程中新协议以较高的能耗换取较高的安全性,较适用于对安全性要求较高的环境中.

Table 2 Efficiency Comparison Between M-IBE Scheme and BF-IBE Scheme Under Multi-Domain Environments

表 2 多域环境下 M-IBE 方案与 BF-IBE 方案效率比较

Algorithm	Theoretical Basis	Domain Private Key	Domain Public Key P_{pub}	Pairings Operation g_{ID}
BF-IBE	BDH	s	sP	$\hat{e}(P_{pub},Q_{ID})$
M-IBE	MBDH	s	$s^{-1}P$	$\hat{e}(P,Q_{ID})$

Table 3 Simulation Platform Sensor Configuration

表 3 仿真平台节点配置

Item	Number of Times				
	1	2	3	4	5
Sink	1	1	1	1	1
H-Sensor	4	5	6	7	8
L-Sensor	16	35	54	73	92

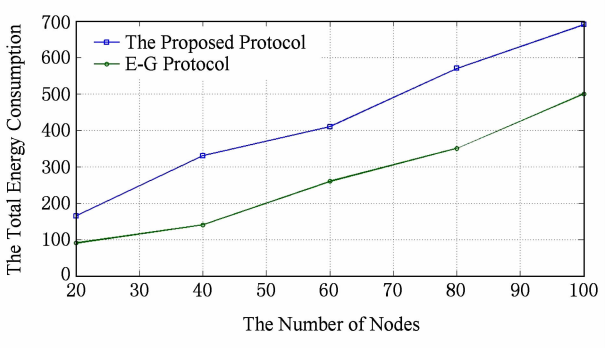

Fig. 4 Energy consumption comparison.

图 4 能耗对比

4 结 论

本文将公钥密码体制与网络异构、节点异构相结合,针对当前异构传感网密钥管理所面临的问题,提出了基于 M-IBE 的异构传感网密钥管理协议.有效解决了异构传感网组内通信与组间通信问题,具有良好的安全性、较低的存储需求和恒定连通性,适用于军用信息监测等私密性要求较高的应用中.

由于异构传感网具有大规模、自组织、资源受限等特性,使得传统网络上密钥管理已经取得的很多好的研究成果无法直接应用.要从根本上解决密钥管理问题,必须充分研究和利用异构传感网中客观存在的各种异构性,指导实用化的、与应用场景相关的密钥管理协议设计.在下一步的工作中,将一方面研究 M-IBE 方案的约减与改进问题,从而有效均衡安全与能耗;另一方面将完善属性基加密(attribute-based encryption, ABE),研究属性的描述方法设计高效地支持否定属性的非单调访问结构与高效的属性撤销机制.

致谢 感谢《计算机研究与发展》审稿专家对本文提出的修改意见!

参 考 文 献

[1] Reza A, Arash R M. Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks [J]. Eurasip Journal on Wireless Communications and Networking, 2010, 2011: 893592-1-12

[2] Boujelben M, Youssef H, Mzid R, et al. IKM—An identity based key management scheme for heterogeneous sensor networks [J]. Journal of Communications, 2011, 6(2): 185-197

[3] Rathod V, Mehta M. Security in wireless sensor network: A survey [J]. Ganpat University Journal of Engineering & Technology, 2011, 1(1): 35-44

[4] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks [C] //Proc of the 9th ACM Conf on Computer and Communications Security. New York: ACM, 2002: 41-47

[5] Du X J, Guizani M, Xiao Y, et al. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks [J]. IEEE Trans on Wireless Communications, 2009, 8(3): 1223-1229

[6] Traynor P, Choi H, Cao G, et al. Establishing pair-wise keys in heterogeneous sensor networks [C] //Proc of the 25th IEEE Int Conf on Computer Communications (INFOCOM 2006). Piscataway: Institute of Electrical and Electronics Engineers Inc, 2006: 1-12

[7] Chen Haikun, Shi Shengfei, Li Jianzhong. A key management scheme based on variable transmission range in wireless sensor networks [J]. Journal of Computer Research and Development, 2008, 45(1): 165-171 (in Chinese)
(陈海坤,石胜飞,李建中. 基于通信半径动态调整的无线传感器网络密钥管理协议[J]. 计算机研究与发展, 2008, 45(1): 165-171)

[8] Lauter K. The advantages of elliptic curve cryptography for wireless security [J]. IEEE Wireless Communications, 2004, 11(1): 62-67

[9] Blake I, Seroussi G, Smart N. Elliptic Curves in Cryptography [M]. Cambridge: Cambridge University Press, 1999: 159-170

[10] Shamir A. Identity-based cryptosystems and signature schemes [G] //LNCS 196: Proc of Advances in Cryptology (CRYPTO'84). Berlin: Springer, 1985: 47-53

[11] Libert B. New secure applications of bilinear map in cryptography [D]. Louvain: University of Catholique, 2006

[12] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [G] //LNCS 2139: Proc of Crypto 2001. Berlin: Springer, 2001: 213-229

[13] Sakai R, Kasahara M. ID based cryptosystems with pairing on elliptic curve [EB/OL]. [2011-07-05]. http://eprint.iacr.org/2003/054.pdf

[14] Yang Geng, Yu Xiaojie, Wang Jiangtao, et al. A novel encryption scheme for wireless sensor networks based on identity-based encryption [J]. Journal of Nanjing University of Posts and Telecommunications: Natural Science, 2007, 27(4): 1-7 (in Chinese)
(杨庚, 余晓捷, 王江涛, 等. 基于IBE算法的无线传感器网络加密方法研究[J]. 南京邮电大学学报: 自然科学版, 2007, 27(4): 1-7)

[15] Yang Geng, Wang Jiangtao, Cheng Hongbing, et al. A key establish scheme for WSN based on IBE and Diffie-Hellman algorithms [J]. Acta Electronica Sinica, 2007, 35(1): 180-184 (in Chinese)
(杨庚, 王江涛, 程宏兵, 等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报, 2007, 35(1): 180-184)

[16] Wang Shengbao. Practical identity-based encryption (IBE) in multiple PKG environments and its applications [EB/OL]. (2007-03-22) [2011-07-19]. http://arxiv.org/pdf/cs.cr/0703106.pdf

[17] Wang Shengbao. Research on cryptosystems and key agreement protocols from bilinear pairings [D]. Shanghai: Shanghai Jiao Tong University, 2008 (in Chinese)
(王圣宝. 基于双线性配对的加密方案及密钥协商协议[D]. 上海: 上海交通大学, 2008)

[18] Lal S, Sharma P. Security proof for Shengbao Wang's identity-based encryption scheme [EB/OL]. [2011-08-26]. http://eprint.iacr.org/2007/316.pdf

[19] Crossbow. MICA2 Mote Datasheet [EB/OL]. [2011-07-15]. https://www.eol.ucar.edu/

Ma Chunguang, born in 1974. PhD, professor and PhD supervisor of Harbin Engineering University. Senior member of China Computer Federation, Chinese Association for Cryptologic Research. His main research interests include cryptology, information security, Ad hoc & WSN, and network coding.

Wang Jiuru, born in 1983. PhD. His research interests include information security and Ad hoc & WSN.

Wu Peng, born in 1974. Master and technician of Harbin Engineering University. Her research interest includes information security(wupeng@hrbeu.edu.cn)

Zhang Hua, born in 1978. PhD and lecturer of Beijing University of Posts and Telecommunications. Her research interests include cryptographic protocol and information security(zhanghua_288@bupt.edu.cn).