

WSN 中一种优化的混合密钥分配方案

沈明玉, 刘 腾

(合肥工业大学 计算机与信息学院, 安徽 合肥 230009)

摘 要: 由于对称加密算法不能很好地解决无线传感器网络中存在的安全问题, 本文对对称加密算法和非对称加密算法进行了优化; 采用对称多项式建立通信路径, 椭圆加密算法进行认证, 认证后节点间将会产生较短的会话密钥, 节点间相互通信时可以使用该会话密钥进行通信. 通过随机图理论对该分配方案的连通性进行了分析, 在研究敌手攻击过程的基础上证明了该方案在实际应用中具有很高的安全性; 在对该方案的详细分析和比较的基础上, 进一步证明了该方案的可行性以及安全性.

关键词: 无线传感器网络; 对称加密算法; 非对称加密算法; 计算开销; 通信开销

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2013)09-0086-04

A Kind of Optimization of the Mixed Key Management Scheme for Wireless Sensor Networks

SHEN Ming-yu, LIU Teng

(School of Computer & Information, Hefei University of Technology, Hefei 230009, China)

Abstract: Symmetric encryption algorithm can not solve the security problems effectively existing in the wireless sensor networks. This paper proposes a key distribution scheme based on symmetric encryption algorithm and elliptical encryption algorithm, which is optimized by asymmetric encryption algorithm and utilizes communication path created by symmetric polynomials and authenticate used by elliptical encryption algorithm, and which can bring shorter session key after the mutual authentication between nodes. This work analyses connectivity of the allocation scheme by the random graph theory and we proved the scheme has very high security in the practical application which is based on the research of the enemy attack process. The scheme proves feasibility and security based on the scheme detailed analysis and comparison.

Key words: wireless sensor network (WSN); symmetric encryption algorithm; asymmetric encryption algorithm; computing overhead; communication overhead

1 引言

WSN 的需求在很大一方面表现在安全的需求上, 它主要包括数据的机密性、完整性、真实性、新鲜性、不可伪造性. 因此一个安全的密钥管理协议应当具有以下特征: 可用性、自组织、强大的加密保证和数据的完整性.

针对 WSN 的特点, Perrig 等人提出了基于可信基站的 SPINS (Security Protocols for Sensor

Network) 协议, 以及闫丽丽等人对该协议的改进分析^[1-2]; Sencun Zhu 等人针对大规模分布式传感器网络提出了 LEAP 协议^[3], LEAP 协议支持各种通信模式和网内数据处理, 引入了单独密钥、组密钥、簇密钥、成对共享密钥. 虽然增加了存储开销但是减少了通信开销提高了网络安全性. 典型的无线的传感器网络密钥管理方案还有 E-G 随机密钥预分配方案, 对 E-G 的改进方案 q-Composite 随机密钥预分配方案, 基于 EBS 的动态密钥管理方案等.

收稿日期: 2012-11-08; **修回日期:** 2012-12-14

基金项目: 合肥工业大学博士专项基金(GDBJ2009-005)

一些研究表明非对称加密算法经过优化后适用于无线传感器网络^[4-7],从安全角度来看,非对称加密体制的安全强度在计算上要远优于对称密码体制。然而目前基于非对称的无线传感器网络加密方案的研究发展较缓慢。本文利用椭圆加密算法及对称多项式相关理论,在保证节点资源消耗尽可能低的情况下最大程度上解决无线传感器网络中存在的安全问题。

2 公钥的密钥分配方案

把无线传感器网络中节点分为基站节点和传感

$$S = \begin{pmatrix} ID_{11}PK_{11} \sum_{i,j=0}^t a_{i,j}x^i y^j & ID_{12}PK_{11} \sum_{i,j=0}^t a_{i,j}x^i y^j & \cdots & ID_{1n}PK_{11} \sum_{i,j=0}^t a_{i,j}x^i y^j \\ ID_{21}PK_{21} \sum_{i,j=0}^t a_{i,j}x^i y^j & ID_{22}PK_{22} \sum_{i,j=0}^t a_{i,j}x^i y^j & \cdots & ID_{2n}PK_{2n} \sum_{i,j=0}^t a_{i,j}x^i y^j \\ \vdots & \vdots & & \vdots \\ ID_{m1}PK_{m1} \sum_{i,j=0}^t a_{i,j}x^i y^j & ID_{m2}PK_{m2} \sum_{i,j=0}^t a_{i,j}x^i y^j & \cdots & ID_{mn}PK_{mn} \sum_{i,j=0}^t a_{i,j}x^i y^j \end{pmatrix}$$

这是一个 $n \times n$ 的矩阵, $PK_{i,j}$ 表示公钥, $ID_{i,j}$ 表示对应节点的身份, $\{f_i(x,y)\}_{i=1,2,\dots,s} = \sum_{i,j=0}^t a_{i,j}x^i y^j$ 是对称多项式。本文采用椭圆加密算法,公钥 $PK_{i,j}$ 对应私钥为 $RK_{i,j}$ 。

基站首先生成公钥矩阵,然后基站计算每个公钥对应的私钥,并从矩阵中选择一个元素 $ID_{ij}PK_{ij}$ 分配给节点 n_k ,而且每个元素不会被重复选择,分配完成后每个节点都将有一个有别与其它节点的身份标志ID、公钥和私钥。部署前,基站在有限域 F_q 上随机生成 s 个 t 阶对称多项式 $\{f_i(x,y)\}_{i=1,2,\dots,s}$;然后每一节点随机选取 s' 个多项式共享。子集 s' 中可能会存在相同的共享多项式,分配完成后每个节点将会得到公钥、私钥、对称多项式池。本方案是基于可信基站的,节点对基站是完全信任的,所以节点不需要对基站进行认证可以省去不必要的计算、通信、能量开销。节点部署前公钥、私钥、多项式池是由基站统一分配,因此节点无需利用基站的公钥对其合法性进行认证。节点间进行通信时也不需要身份认证,如果节点A能够与节点B进行通信说明节点A与节点B具有相同的多项式,而且节点B只有在具有基站分配的私钥情况下才可以对密文进行解码。

2.2 邻居发现阶段

传感器节点受到自身特点的限制其传播距离一般较近,节点 i 将自己的ID和多项式集合 s'_i 以明文

器节点两种类型。其中基站节点不受能量、存储、计算能力的限制。基站存储信息包括:基站 ID_B ,基站的公钥 PK_B ,基站的私钥 RK_B 。每个传感器节点存储信息包括:节点ID,节点的公钥 PK ,节点的私钥 RK ,计时器,对称多项式。本文将从以下两个方面对该方案进行描述:公钥、私钥和节点ID建立阶段,邻居发现阶段。

2.1 公钥、私钥和节点ID建立阶段

假设待部署无线传感器节点数量为 N ,在私钥产生及公钥、私钥分配前首先生成节点ID及节点公钥集合 S :

的形式广播出去,接收到节点 i 的ID信号的节点 j 查询其保存的多项式集合 s'_j 。如果多项式集合 s'_i 和 s'_j 存在相同的多项式,则节点 i 是节点 j 的邻居节点 j 节点可以将数据发送给节点 i ,反之亦然。节点 i 和节点 j 在互换了ID号以后可以根据对方的ID号通过查询保存得多项式池找出对方的公钥 PK ,所有节点成功广播ID和多项式集合 s'_i 以后整个无线传感网络将构成一个无向连通图。当节点A与节点B通信时节点A产生会话密钥 $K_{A,B}$;然后,用节点B的公钥对会话密钥进行加密,节点B对 $MAC_{A,B}(ID_A, PK_B(K_{A,B}))$ 认证后得到认证密钥 $K_{A,B}$ 。在会话过程中A,B节点使用 $K_{A,B}$ 进行加密会话。

3 网络连通性分析

由于无线传感器网络自身的特点,每个节点只能接收通信半径内的节点发送的信号。节点A接收到节点B广播的ID及多项式池 s'_B ;然后,节点A接收这些节点后与其多项式池 s'_A 进行比较,如果接受到的 s'_B 与节点A的多项式池 s'_A 存在相同的对称多项式则节点A与节点B互为邻居,同理可以找到节点A的其它邻居节点,节点A可以将收集到的数据传给节点B、C、D,反之亦然如图1。邻居发现阶段完成后整个无线传感器网络将形成一个随机无向图联通图。

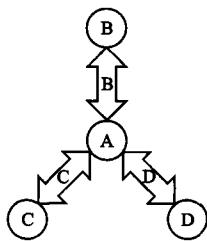


图1 直接通信节点的无向链路

在无线传感器网络中,假设节点的数量为 N ,基站存储的公钥总数为 $n \times n$,一个节点存储另一个节点公钥的概率为 p ,由此可得该节点的度 $d = (n-1)p$,当 $p=0$,任何节点都没有邻居, $p=1$ 时每个节点都有由 $(n-1)$ 个邻居.在此要选择一个最佳的度使得任何一个节点成为独立节点的概率很小.

根据经典的随机图理论,节点的度 d 与网络节点总数 N 存在下列关系: $d = \frac{N-1}{N}(\ln N - \ln(-\ln P_c))$,其中 P_c 为全网连通概率.图2可直观的对上式进行描述.

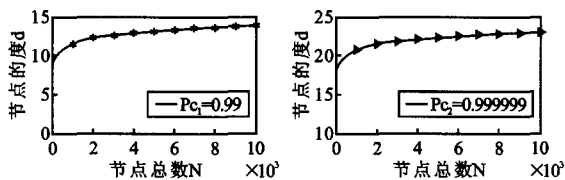


图2 节点总数与节点的度之间关系

在图2中 $P_{c1}=0.99, P_{c2}=0.99999$.由图可得当 $P_c=0.99, n=2000$ 时 $d \approx 12$;当 $n=10000$ 时 $d \approx 14$.当 $P_c=0.99999, n=2000$ 时 $d \approx 22$;当 $n=10000$ 时 $d \approx 22$.由上述分析可得当节点的规模变化很大时每个节点所保存的公钥数变化很小,即每个节点的邻居节点增加的不明显.这是因为每个传感器节点所能传输信号的距离都是有限的,每个节点周围的邻居节点 g 是远小于总节点数 N 的.如果想要调整整个网络的连通性,可以通过调节单位空间的节点数目也可以通过调节对称多项式的域来进行调节.根据经典随机图理论得出每个节点 i 保存其周围节点 j 的公钥的概率 μ 与该节点的度 d 成正比,与周围节点总数 n' 成反比,即 $\mu = \frac{d}{n'-1}$.由图3可以看出,当 $n'=60, d=10$ 时, $\mu \approx 0.2$, $d=40$ 时, $\mu \approx 0.7$;当 $n'=100, d=10$ 时, $\mu \approx 0.1$, $d=40$ 时, $\mu \approx 0.4$.而节点 i 为非孤立节点的概率.

$$\theta = \sum_{i=1}^n \mu^i (1-\mu)^{(n'-i)}$$

$$\begin{aligned} &= \sum_{i=1}^{n'} \left(\frac{d}{n'-1} \right)^i \left(\frac{d}{n'-1} \right)^{n'-i} \\ &= \sum_{i=1}^{n'} \left(\frac{(N-1)(\ln N - \ln N(P_c))}{N(n'-1)} \right)^i \\ &\quad \left(\frac{(N-1)(\ln N - \ln N(P_c))}{N(n'-1)} \right)^{n'-i} \end{aligned}$$

由上式可以得出,节点 i 与其它节点关联的概率与节点总数 N 、节点的密度 n' 、全网连通概率 P_c 有关.

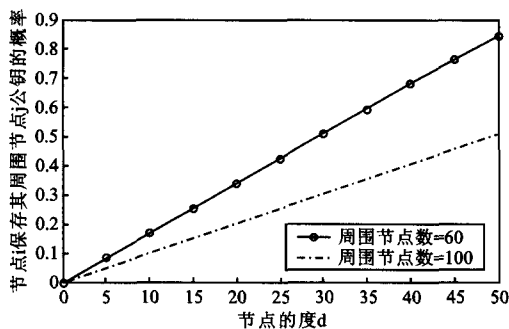


图3 节点保存其周围节点公钥的概率

4 网络的可扩展性和安全性分析

如果有新的节点需要加入网络,基站只需要从 $n \times n$ 个元素中选择一个未被分配的ID号、对应的公钥、私钥、多项式池和计时器对新的节点进行分配.理论上讲多项式的域 F_q 及在 F_q 域上产生的 t 阶多项式 s 所包含的元素越多网络的可扩展性越好,但在每个节点所选多项式个数 s' 不变的情况下节点间成为邻居的概率将会降低,从而导致整个网络的连通性将会降低.因此在增强网络可扩展性的同时需要综合考虑网络的连通性,使得网络的总体性能达到最优.

假设整个网络中包含6250个节点且节点 i 与节点 j 成为邻居的概率相同,每个节点保存密钥的数量 $\lambda=50$ 时,本方案中节点 i 与节点 j 互为邻居的概率 $P_i \approx 0.22$; $\lambda=75$ 时,节点 i 与节点 j 互为邻居的概率 $P_i \approx 0.31$; $\lambda=100$ 时,节点 i 与节点 j 互为邻居的概率 $P_i \approx 0.41$;在E-G方案中当 $\lambda=50$ 时,节点 i 与节点 j 互为邻居的概率 $P_i \approx 0.02$; $\lambda=75$ 时,节点 i 与节点 j 互为邻居的概率 $P_i \approx 0.1$; $\lambda=100$ 时,节点 i 与节点 j 互为邻居的概率 $P_i \approx 0.15$.通过比较可以得出本方案与E-G方案相比可扩展性更好.

WSN面临的几种典型的攻击方式包括:欺骗、篡改或重发路由信息、虫洞攻击、黑洞攻击、女巫攻击、拒绝服务攻击.本方案能够部分抵御拒绝服务攻

击,有效地抵御上述攻击其它攻击.攻击者通过伪造节点身份 ID 进行攻击,将是不可行的;这是由于攻击者不知道被攻击者的私钥所以本文所述的方案能够抵御欺骗、篡改、女巫攻击.当传感器节点受到虫洞攻击、黑洞攻击、拒绝服务攻击时可以向基站请求更新多项式 s' ,从而可以改变节点的邻居节点从而达到抵御的目的.

4.1 抵抗节点妥协

假设网络中已经有多个传感器节点妥协,敌手可获得妥协节点的所有信息.由于节点只存有基站的公钥、传感器节点的身份标志 ID、公钥和私钥邻居认证公钥、等公开信息,敌手如果想得到基站或其他邻居节点的私钥,其难度等同于解决椭圆曲线离散对数问题.当有多个节点妥协时敌手也只能得到相关节点得公钥信息,无法伪造未公布的私有信息.因此,妥协节点数目的增加无助于敌手生成正常节点的合法签名.妥协节点的增加可以增大虚假信息

的覆盖范围,但是,非妥协节点可以通过查询邻居节点表或散列运算过滤虚假信息,防止带来过高的消耗.

4.2 抵抗主动攻击

本方案在妥协节点较多并且进行大规模多次广播非法信息时,本方案在整个网络能耗方面的优势更加明显.

表 1 为本方案与 SPINS 方案在计算开销、通信开销以和安全性能方面的比较.其中 ENC 代表加密函数计算开销,MAC 代表人证函数计算开销.不难看出,本方案可扩展性较好安全性有了显著提高,计算、通信、存储开销有所增加;本方案中 加密函数和解密函数虽然各有两个但在不同情况下使用所以计算代价并未明显增加,存储需求与 SPINS 相比明显增高,在两个节点正常通信过程中通信负荷同样为所选会话密钥长度.

表 1 性能分析

安全方案	计算代价	存储需求	通信负荷	可扩展性	Sinkhole 攻击	Sybil 攻击	Wormholes 攻击	Dos 攻击
SPINS	一个 ENC、MAC	基站 8nB 节点 8B	会话密 钥长度	一般	不抵御	不抵御	不抵御	不抵御
本文方案	两个 ENC、MAC	多项式池 公钥、私钥	会话密 钥长度	好	抵御	抵御	抵御	部分 抵御

5 结束语

本文给出的密钥分配方案经过对非对称加密方案的优化,在保证资源消耗尽可能低的前提下使得无线传感器网络具有很高的安全性.随着科学技术的发展无线传感器网络节点的资源将不再严格受到限制,其应用也将更加广泛对安全性的要求也将更高.非对称加密方案和非对称对称混合加密方案也必将成为研究的重点.

参考文献:

[1] Perrig A, Szewczyk R,Victor W, et al. SPINS: security protocols for sensor networks [J]. Wireless Networks, 2002, 8(5):521-534.

[2] 闫丽丽,彭代渊,高悦翔. 传感器网络安全协议的分析和改进[J]. 通信学报, 2011, 32(5):139-145.

[3] Zhu S, Setia S, Jajodia S. LEAP: efficient security mechanisms for large-scale distributed sensor networks [C]//Proceeding of the 10th ACM Conference on

Computer and Communications Security. [s. l.]:ACM, 2003:62-72.

[4] Roman R, Alcaraz C. Applicability of public key infrastructures in wireless sensor network [J]. Lecture Notes in Computer Science,2007(4582):313-320.

[5] 温涛,张永,郭权,等. WSN 中同构模型下动态组密钥管理方案[J]. 通信学报, 2012, 33(6):164-173.

[6] 陈燕俐,杨庚. 适用于无线传感器网络的混合式组密钥管理方案[J]. 通信学报, 2010, 31(11):56-64.

[7] 胡宇舟,王雷,陈治平,等. 传感器网络中对偶密钥的动态密钥路径建立机制及算法[J]. 通信学报, 2008, 29(2):52-58.

作者简介:

沈明玉 男,(1962—),博士,副教授,硕士生导师.研究方向为网络与信息安全.

刘 腾 男,(1987—),硕士研究生.研究方向为无线传感器网络安全协议分析.